

Cybersecurity of cultural heritage: a reflection on SBN and Magazzini Digitali as critical infrastructures of Italian libraries

Chiara Storti^(a)

a) National Central Library of Florence, <https://orcid.org/0009-0005-1767-3425>

Contact: Chiara Storti, chiara.storti@cultura.gov.it

Received: 28 July 2025; Accepted: 14 October 2025; First Published: 15 January 2026

ABSTRACT

The contribution analyzes the escalating cyber risks for cultural heritage, driven by digitization and conflicts, highlighting severe incidents (e.g., British Library) causing economic and reputation damages, and data loss. It proposes considering these infrastructures as “critical” through the “C3E - *Cultural Cyber Critical Ecosystem*” model. Legal, managerial, and technological criticalities of SBN and Magazzini Digitali, as core components of this ecosystem, are then examined. The conclusion emphasizes the need to invest in cyber resilience and foster a cultural shift in risk management.

KEYWORDS

Cybersecurity implications; Cyberattack; Ransomware; SBN; Magazzini Digitali.

Cybersicurezza del patrimonio culturale: una riflessione su SBN e Magazzini Digitali come infrastrutture critiche delle biblioteche italiane

ABSTRACT

Il contributo analizza il crescente rischio cyber per il patrimonio culturale, determinato da fattori quali la forte accelerazione post-pandemica della digitalizzazione di processi e servizi e i conflitti in corso in Europa Orientale e nel Medio Oriente. A partire dal noto incidente occorso alla British Library, viene posto l'accento sui possibili danni economici e reputazionali, oltre che su conseguenze come la perdita irreversibile di dati. Alla luce del contesto delineato, si propone di considerare le infrastrutture del patrimonio culturale italiano, con particolare riferimento a quelle afferenti al dominio delle biblioteche, come “critiche”, analizzandole in relazione al modello recentemente definito di “C3E - *Cultural Cyber Critical Ecosystem*”. Vengono quindi esaminate le criticità legali, gestionali e tecnologiche di SBN e Magazzini Digitali, come componenti fondamentali dell'ecosistema. La conclusione sottolinea la necessità di investire nella resilienza informatica e di promuovere un cambiamento culturale nella gestione dei rischi.

PAROLE CHIAVE

Cybersicurezza; Cyberattacchi; Ransomware; SBN; Magazzini Digitali.

Perché dobbiamo occuparci di cybersicurezza delle infrastrutture del patrimonio culturale

Se sino a qualche anno fa il problema sembrava limitato alle sole “applicazioni informatiche”, in questi anni non esiste settore, dai sistemi industriali agli apparati medicali, che non sia stato intaccato da qualche forma di attacco informatico. [...]

In questo contesto, lo strumento di cui maggiormente disponiamo per fronteggiare il rischio informatico è la consapevolezza; è infatti decisamente diverso l'impatto di eventi pianificati rispetto a quello di eventi inattesi.

Queste parole, che risuonano ancora di straordinaria attualità, si possono leggere nell'introduzione al primo Rapporto Clusit sulla sicurezza ICT in Italia (Clusit 2012) che, nel 2012, conteggiava in 470 gli attacchi cyber avvenuti a livello globale l'anno precedente. In (Clusit 2025) il dato è considerevolmente più alto: 3.541 attacchi, di cui ben 357 ai danni del nostro Paese¹. Questa crescita molto consistente, concentrata negli anni 2020-2024, è dovuta in particolar modo a due opposte tendenze che si sono venute a delineare. Da una parte, la pandemia ha funto da acceleratore per la digitalizzazione dei processi e dei servizi a tutti i livelli, fenomeno che sta già subendo un'ulteriore crescita esponenziale a causa della diffusione degli strumenti di IA; dall'altra, i conflitti in corso, specialmente in Europa Orientale e nel Medio Oriente, hanno alzato il livello generale di tensione internazionale, e anche laddove tali conflitti non si trasformino in vere e proprie *cyberwar*, le infrastrutture informatiche sono obiettivi sensibili, alla stregua di altre infrastrutture strategiche. Non fanno eccezione nemmeno le infrastrutture del patrimonio culturale, pubbliche o private, come dimostrano i tanti incidenti registrati negli ultimi anni, di cui l'attacco ransomware² alla British Library dell'ottobre 2023 (The British Library 2024) è solo il più celebre.

Data	Istituzione	Tecnica di attacco	Conseguenze principali	Danni economici accertati
2018	Rijksmuseum Twenthe di Enschede (Paesi Bassi)	Man in the middle (Mitm) ³	Il museo ha versato 2.4 milioni di sterline per l'acquisto di un quadro ad un conto bancario falso creato da un hacker.	2.4 milioni £

¹ La grandezza di questo dato, come evidenziato nel Rapporto, è dovuta sia alla mancanza o forte carenza di cultura digitale e di cultura della cybersicurezza, soprattutto nel comparto pubblico, sia dalla diffusa obsolescenza dei sistemi hardware e software in uso.

² Per una definizione di Ransomware si veda <https://www.acn.gov.it/portale/csirt-italia/glossario>.

³ Per una definizione di Mitm si veda <https://www.acn.gov.it/portale/csirt-italia/glossario>.

Data	Istituzione	Tecnica di attacco	Conseguenze principali	Danni economici accertati
Maggio 2019	Asian Art Museum di San Francisco (USA) ⁴	Ransomware	Prolungata indisponibilità dei sistemi informatici del museo.	Costi di ripristino dei sistemi.
Dicembre 2021	Museum of Gloucester (Regno Unito) ⁵	Malware ⁶	Prolungata inaccessibilità del database contenente i dati relativi alle collezioni museali.	1 milione £ (la cifra complessiva spesa per il ripristino di tutti i servizi compromessi della Municipalità di Gloucester).
Novembre 2022	Archives départementales des Alpes-Maritimes (Francia) ⁷	Ransomware	Prolungata inaccessibilità degli inventari online e dei servizi digitali degli archivi. Circa 292 GB di dati rubati.	Costi di implementazione di un nuovo portale.
Dicembre 2022	Metropolitan Opera di New York (USA) ⁸	Non nota	Prolungata indisponibilità di tutti i sistemi di rete, compresi il sito web, la biglietteria, e il call center.	200.000 \$ di biglietti invenduti a causa dell'indisponibilità del sistema di biglietteria per quasi 30 ore.
Agosto 2023	MiBAC (Italia) ⁹	Ransomware	Violazione dei dati.	Non noti
Ottobre 2023	British Library (Regno Unito) (The British Library 2024)	Ransomware	600 GB di dati rubati; pubblicazione online di centinaia di migliaia di file sottratti, compresi i dati degli utenti e del personale. Prolungata indisponibilità di tutti i servizi e rallentamento di tutte le attività della biblioteca.	Tra i 6 e i 7 milioni £ per ricostruire la maggior parte dei servizi digitali (Uddin e Thomas 2024).

⁴ <https://abc7news.com/post/exclusive-cyberattack-launched-on-sf-museum-computers-/5399932/>.

⁵ <https://www.bbc.com/news/uk-england-gloucestershire-64917275>.

⁶ Per una definizione di Malware si veda <https://www.acn.gov.it/portale/csirt-italia/glossario>.

⁷ <https://www.rfgenealogie.com/infos/alpes-maritimes-un-site-refondu-en-totalite-apres-la-cyberattaque>.

⁸ <https://www.informationweek.com/cyber-resilience/the-metropolitan-opera-cyberattack-highlights-vulnerability-of-cultural-institutions>.

⁹ <https://www.redhotcyber.com/post/attacco-informatico-al-ministero-dei-beni-culturali-italiani-rivendicato-da-lock-bit-tra-9gg-la-pubblicazione-dei-dati/>.

Data	Istituzione	Tecnica di attacco	Conseguenze principali	Danni economici accertati
Ottobre 2023	Toronto Public Library (Canada)	Ransomware	Violazione dei dati personali di circa 8.000 tra dipendenti ed ex dipendenti, di circa 1.874 dei loro beneficiari e familiari a carico e di 4.100 tra utenti, donatori, appaltatori, volontari ecc. ¹⁰ e prolungata indisponibilità dei servizi ¹¹ .	Costi di ripristino di tutti i sistemi hardware e software, sostenuti dalla Municipalità di Toronto.
Ottobre 2023	Museum für Naturkunde Berlin (Germania) ¹²	Non nota, probabile ransomware	Data breach di dati personali di oltre 37.000 visitatori del Museo	Non noti
Dicembre 2023	Gallery Systems (USA) ¹³	Ransomware	Disservizi eMuseum.	Non noti
Maggio 2024	Seattle Public Library (USA) ¹⁴	Ransomware	Violazione dei dati di 27.000 persone e prolungata indisponibilità dei servizi.	1 milione \$ per coprire i costi dell'indagine forense, del ripristino dei sistemi e della consulenza legale per la gestione del data breach.
Maggio 2024	Internet Archive (USA) ¹⁵	DDoS ¹⁶ e accessi non autorizzati	Prolungata indisponibilità dei servizi.	Non noti
Maggio 2024	MiC - Direzione generale Educazione ricerca e istituti culturali (Italia) ¹⁷	Non nota	Compromissione di dati personali.	Non noti
Agosto 2024	Réunion des Musées Nationaux (Francia) ¹⁸	Ransomware	Rete dei pagamenti dei bookshop del sistema museale compromessa.	Non noti

¹⁰ <https://www.ipc.on.ca/en/cases-of-note/toronto-public-library-cyberattack>.

¹¹ <https://www.cbc.ca/news/canada/toronto/toronto-public-library-ransomware-employee-data-1.7028982>.

¹² <https://www.museumfuernaturkunde.berlin/en/information-about-cyber-attack-museum-fur-naturkunde-berlin>.

¹³ <https://apollo-magazine.com/art-news-cyber-attack-museums-ai/>.

¹⁴ <https://www.seattletimes.com/seattle-news/seattle-library-ransomware-attack-affected-nearly-27k-people/>.

¹⁵ <https://blog.archive.org/2024/05/28/internet-archive-and-the-wayback-machine-under-ddos-cyber-attack/>.

¹⁶ Per una definizione di Attacco DOS e DDOS si veda <https://www.acn.gov.it/portale/csirt-italia/glossario>.

¹⁷ <https://dgeric.cultura.gov.it/violazione-dei-sistemi-informatici-della-direzione-generale-educazione-ricerca-e-istituti-culturali/>.

¹⁸ <https://www.lesechos.fr/industrie-services/services-conseils/la-cyberattaque-contre-les-musees-francais-na-touche-que-36-boutiques-2112529>.

Data	Istituzione	Tecnica di attacco	Conseguenze principali	Danni economici accertati
Ottobre 2024	Internet Archive (USA) ¹⁹	DDoS e accessi non autorizzati	Violazione dei dati di 31 milioni di utenti e prolungata indisponibilità dei servizi.	Non noti
Novembre 2024	Library of Congress (USA) ²⁰	E-mail breach	Account mail compromessi.	Non noti
Dicembre 2024	National Museum of Royal Navy (Regno Unito) ²¹	Ransomware	Prolungata indisponibilità dei servizi del museo.	Non noti
Gennaio 2025	British Museum (Regno Unito) ²²	Sabotaggio interno dei sistemi IT	Parziale chiusura dei servizi museali.	Non noti

Tabella 1. Prospetto dei principali attacchi cyber noti a istituzioni culturali pubbliche e private, nel mondo, a partire dal 2018.

Rispetto alle tipologie di attacco, possiamo rilevare come la maggior parte sia perpetrato con l'uso di ransomware o malware di altra natura, seguono gli attacchi DDoS e quelli causati da vulnerabilità²³ sia conosciute che sconosciute dei sistemi (i cosiddetti *zero-day attack*²⁴), spesso in combinazione con tecniche di Phishing²⁵ e Social Engineering²⁶, che possono servire non solo a sottrarre dati alla vittima, ma anche ad introdurre malware nei sistemi attaccati²⁷. Per quanto riguarda le motivazioni degli attacchi, queste possono essere riconducibili ad alcune macrocategorie:

¹⁹ <https://www.washingtonpost.com/nation/2024/10/18/internet-archive-hack-wayback/>.

²⁰ <https://securityaffairs.com/171138/data-breach/library-of-congress-email-communications-hacked.html>.

²¹ <https://www.nmrn.org.uk/news/national-museum-royal-navy-statement>.

²² <https://www.theguardian.com/culture/2025/jan/24/british-museum-forced-to-partly-close-after-alleged-it-attack-by-former-employee>.

²³ Gli attacchi dovuti a vulnerabilità, soprattutto in Italia, non sono da sottovalutare. Nel 2020, ad esempio, il collettivo di hacktivisti *Anonymous* ha colpito diversi siti della PA italiana, tra cui quello di AgID, sfruttando una falla nel CMS sviluppato dall'azienda abruzzese ISWEB S.p.A.: <https://www.dire.it/17-06-2020/474702-anorc-attacco-hacker-al-sito-agid-non-e-una-burla-servono-competenze/>.

²⁴ Per una definizione di Attacco Zero Day si veda <https://www.acn.gov.it/portale/csirt-italia/glossario>.

²⁵ Per una definizione di Phishing si veda <https://www.acn.gov.it/portale/csirt-italia/glossario>.

²⁶ Nel contesto della sicurezza informatica, la Social Engineering o Ingegneria Sociale è l'uso dell'influenza psicologica sulle persone per indurle a compiere azioni o divulgare informazioni riservate. Per una definizione di Ingegneria Sociale si veda anche <https://www.acn.gov.it/portale/csirt-italia/glossario>.

²⁷ Il ransomware che ha colpito la British Library è stato introdotto, con grande probabilità, a seguito della compromissione delle credenziali di account con privilegi da amministratore, tramite attacchi di Phishing, Spear-Phishing (si veda <https://www.acn.gov.it/portale/csirt-italia/glossario>) o con un attacco di forza bruta (*brute force*), cioè con tentativi ripetuti di indovinare le password, facilitati da sistemi di autenticazioni poco solidi, vale a dire basati sull'utilizzo di password non forti o privi di Autenticazione Multi-Fattore (si veda <https://www.acn.gov.it/portale/csirt-italia/glossario>). Quest'ultima, sebbene, fosse stata introdotta nel 2020 per le applicazioni cloud adottate dalla Biblioteca, era stata esclusa per la connettività al dominio della British Library, inclusi l'accesso ai computer e ai server on-premise, per ragioni di praticità, costo e impatto sui programmi in corso (The British Library 2024).

- Motivazioni economiche (*cybercrime*): i cybercriminali possono ottenere guadagni diretti con strumenti quali i ransomware, anche se le istituzioni culturali, soprattutto pubbliche, tendono a non pagare i riscatti (o forse non ammettono pubblicamente di farlo). Guadagni indiretti possono, invece, derivare dai dati rubati sia utilizzando, ad esempio, le informazioni bancarie di utenti e donatori, sia rivendendo dati e informazioni a terzi, che potrebbero anche essere i reali committenti dell'azione criminale²⁸.
- Violazione della sicurezza informatica allo scopo di violare la sicurezza fisica: la compromissione dei sistemi di allarme, dei sistemi di monitoraggio ambientale o dei dati relativi alla dislocazione fisica di opere e documenti preziosi, nelle sale o nei magazzini di biblioteche, musei e archivi, possono dar luogo a danneggiamenti o furti di opere.
- Volontà di utilizzare una infrastruttura del patrimonio culturale come *backdoor*²⁹ per *attaccare infrastrutture collegate*.
- Volontà di aumentare il livello di tensione generale, come in caso di guerre e conflitti: l'obiettivo di questo di attacchi è, solitamente, quello di distogliere risorse destinate ad infrastrutture di altra natura e veri bersagli dell'azione criminale; le istituzioni culturali possono, quindi, essere vittime collaterali, come durante attacchi DDoS molto vasti.
- Volontà di colpire obiettivi simbolici: le infrastrutture del patrimonio culturale sono ormai anche obiettivi militari a tutti gli effetti nelle cosiddette *cyberwarfare*, come è stato evidente in particolare a partire dall'avvio del Conflitto in Ucraina nel febbraio 2022 (Neglia et al. 2024).
- Ricerca di visibilità: colpire istituzioni molto note, come nel caso della British Library, potrebbe far guadagnare notorietà e credibilità agli autori, singoli o gruppi, degli attacchi. È il caso dei *cyberactivists*, vale a dire di quei singoli o gruppi che utilizzano le tecnologie per promuovere cambiamenti a livello, politico, sociale e culturale.

Dai casi riportati nella Tabella 1 è possibile anche farsi un'idea delle principali conseguenze di un cyberattacco:

- Danni economici. In questa categoria, oltre alle perdite dirette causate dall'eventuale pagamento di un riscatto, rientrano anche le perdite indirette sia per mancati introiti (per tutti i luoghi ad accesso a pagamento, come musei, parchi archeologici o mostre temporanee), che derivanti dalla perdita di dati o informazioni, ovvero degli investimenti fatti nel corso del tempo. A ciò ci possono aggiungere i costi spesso molto alti per il ripristino dei sistemi e dei servizi.
- Perdita o fuga di dati. Considerata la specificità degli asset del patrimonio culturale, la perdita o fuga di dati può causare danni irreversibili. Si pensi, infatti, ai dati relativi al deposito legale digitale che potrebbero non essere più disponibili sul mercato editoriale o, semplicemente online, nel momento in cui i servizi vengono ripristinati³⁰.

²⁸ Nel 2024 i pagamenti provenienti da modelli RaaS - Ransomware as a Service hanno rappresentato oltre il 60% delle campagne ransomware: <https://www.onlinehashcrack.com/guides/cybersecurity-trends/ransomware-as-a-service-2025-market-analysis.php>.

²⁹ Per una definizione di *Backdoor* si veda <https://www.acn.gov.it/portale/csirt-italia/glossario>.

³⁰ Nel report pubblicato da Internet Archive, ad ottobre 2024, a seguito di due importanti attacchi DDoS che hanno reso

- Perdita reputazionale. L'interruzione di servizi per un tempo prolungato, la perdita o la fuga di dati, personali e non, sono un enorme danno di immagine per le istituzioni culturali, specialmente pubbliche.

Se gli attacchi al patrimonio culturale sono da considerarsi di estrema gravità non solo per il valore in sé dei beni che lo compongono ma, soprattutto, per quello che esso rappresenta per la società (Ovenden 2021), è necessario iniziare a ripensare le infrastrutture digitali del patrimonio culturale come infrastrutture critiche,³¹ definendo il perimetro³² da attenzionare. Negli ultimi anni, infatti, alle più tradizionali criticità legate alla sicurezza dei servizi informatici e di rete³³ e alla digital preservation³⁴, si sono affiancati i rischi derivanti da incidenti³⁵ che possono compromettere la cybersicurezza³⁶. A questo scopo, si propone una rilettura dell'ecosistema delle biblioteche italiane alla luce del modello "C3E – *Cultural Cyber Critical Ecosystem*", recentemente definito in (Bellini 2025).

indisponibili, per alcuni giorni, non solo i servizi agli utenti, come la Wayback Machine, ma anche i servizi di archiviazione web veri e propri, si legge: "When a library goes offline, it doesn't just interrupt research; it stifles educational progress, halts public access to information, and, in a new and chilling way, creates gaps in the public memory" (Messarra, Freeland, e Ziskina 2024).

³¹ La [Direttiva UE 2022/2557](#) (c.d. NIS2), all'Art. 2, ne fornisce la seguente definizione: «infrastruttura critica»: un elemento, un impianto, un'attrezzatura, una rete o un sistema o una parte di un elemento, di un impianto, di un'attrezzatura, di una rete o di un sistema, necessari per la fornitura di un servizio essenziale", dove si deve intendere per «servizio essenziale»: un servizio fondamentale per il mantenimento di funzioni vitali della società, di attività economiche, della salute e della sicurezza pubbliche o dell'ambiente.

Fino all'edizione di ottobre 2025, il rapporto Clusit non ha mai preso in considerazione le specificità delle infrastrutture del patrimonio culturale e dei cyber attacchi che le vedono come obiettivi. Tra le "vittime per categoria", infatti, non compare il settore cultura. Nell'edizione di ottobre 2025, è stato invece introdotto un Focus dal titolo "Analisi degli incidenti Cyber nel settore culturale italiano tra il 2020 e il 2024", a cura di un Gruppo di lavoro costituitosi all'interno del Corso di Alta Formazione Cyberhumanities for Heritage Security dell'Università di Roma Tre. Il Direttore del Corso è il prof. Emanuele Bellini (emanuele.bellini@uniroma3.it) che è stato tra i primi, in Italia, ad occuparsi delle problematiche legate alla cybersicurezza nel contesto del patrimonio culturale, e che si ringrazia per l'essenziale contributo alla redazione di questo lavoro.

³² Il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) è stato istituito con il [D.L. 21 settembre 2019, n. 105](#). Il successivo [D.P.R. 30 luglio 2020, n. 131](#) ha esplicitamente elencato i settori considerati di interesse nazionale. La [Direttiva UE 2022/2555](#) ha ulteriormente ampliato tale perimetro includendo nuovi settori critici.

³³ [Direttiva UE 2022/2555](#), Art. 6 – Definizioni: «Sicurezza dei sistemi informatici e di rete»: la capacità dei sistemi informatici e di rete di resistere, con un determinato livello di confidenza, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi.

³⁴ La Digital Preservation Coalition definisce la "Digital Preservation" come "the series of managed activities necessary to ensure continued access to digital materials for as long as necessary" e ne individua i principali rischi: "Rapid technological change may leave content unusable or unintelligible as the software that interprets it becomes obsolete. Without committed resources, the storage and management of digital content will not be possible. Organizational change might leave digital content without a committed custodian. Digital preservation requires a series of actions over time to ensure digital content remains alive, discoverable, accessible and usable": <https://www.dpconline.org/digipres/what-is-digipres>.

³⁵ [Direttiva UE 2022/2555](#), Art. 6 – Definizioni: «incidente»: un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi.

³⁶ [Regolamento UE 2019/881](#), Art. 2 – Definizioni: «cibersicurezza»: l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche e «minaccia informatica»: qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone.

Verso il riconoscimento del C3E italiano delle biblioteche

C3E is composed by complementary entities that are not only interconnected, but inter-reliant and work together to achieve a common value proposition or mission. C3E should be considered critical since “is crucial for the maintenance of vital societal functions” (Council Directive 2022/2557/EC on Resilience of Critical Entities). In fact, it is imperative to treat the (digital) Cultural Heritage as a critical infrastructure because of its role for the society’s identity and cohesion.
(Bellini 2025)

Un “C3E – *Cultural Cyber Critical Ecosystem*” è un ecosistema composto da più entità interconnesse e interdipendenti³⁷ tra loro, che lavorano insieme per il mantenimento della identità e della coesione sociale di una comunità. Tale *Mission*, che è anche la prima delle componenti del C3E, si può declinare nell’ecosistema biblioteche a partire dalle missioni della biblioteca pubblica definite in (IFLA, UNESCO 2022) cui si può aggiungere, più sul versante della tutela, l’istituto del Deposito Legale, che ha il precipuo fine di “conservare la memoria della cultura e della vita sociale italiana”.³⁸ La seconda componente del C3E è quella degli *agents*, da intendere sia come comunità e organizzazioni (enti e istituzioni culturali, operatori di settore, associazioni, imprese culturali e creative ecc. e tutti i loro utenti o clienti), che agenti software. Secondo l’Indagine ISTAT sulle biblioteche pubbliche e private 2022³⁹, le biblioteche italiane aperte al pubblico sono 8.131, di cui 6.453 pubbliche e 1.678 private. Gli utenti che hanno usufruito di almeno un servizio nel corso dello stesso anno sono quantificati in 5.7 milioni, ma sono oltre 35 milioni gli accessi fisici. I numeri assoluti sul personale impiegato nelle biblioteche non sono disponibili ma, considerate le percentuali di addetti riportate nell’ Indagine ISTAT sulle biblioteche 2023⁴⁰, possiamo certamente parlare di qualche decina di migliaia di operatori. D’altra parte, sappiamo che anche l’attenzione verso gli agenti software è in forte crescita. Lo dimostrano iniziative come il rilascio

³⁷ Esistono numerosi studi sulla interdipendenza delle infrastrutture critiche e sul conseguente “Effetto Domino” che può essere provocato dal fallimento di una o più di queste strutture, anche e soprattutto a seguito di un cyberattacco. Interessante, a questo proposito, il progetto DOMINO attivato nell’ambito del programma della Commissione Europea “*Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks*” 2007-2013, che ha sviluppato un modello di valutazione del rischio e di propagazione degli eventi di *failure* alle infrastrutture economiche e sociali che operano nella nostra società: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=SWD:2018:331:FIN>. Tra gli output del progetto, è stato realizzato anche il software di valutazione del rischio, la *DOMINO Platform*, che prende in considerazione tra gli item che caratterizzano il livello di qualità della vita anche “*Arts, sports, leisure and social activities, cultural traditions*”: https://home-affairs.ec.europa.eu/document/download/0f2758c0-3cb2-4d9e-adfd-a725450cee96_en?filename=Panel%20Luisa%20Franchina_DOMINO.pdf.

³⁸ Legge 15 aprile 2004, n. 106 - Art. 1: <https://www.normattiva.it/eli/stato/LEGGE/2004/04/15/106/ORIGINAL>.

³⁹ ISTAT - Statistiche culturali 2022 - Dati sulle Biblioteche - Tavola 4.12: <https://www.istat.it/tavole-di-dati/statistiche-culturali-anno-2022/>, citata in (MiC 2024). Se si considerano anche le biblioteche non stabilmente aperte al pubblico, il numero sale considerevolmente. L’Anagrafe delle Biblioteche Italiane, al 18/7/2025, ne censisce 13.685: <https://anagrafe.iccu.sbn.it/>.

⁴⁰ ISTAT - Statistiche culturali 2023 - Dati “Biblioteche” - Tavola 4.9: <https://www.istat.it/tavole-di-dati/statistiche-culturali-anno-2023/>.

di APIs da parte dell'ICCU⁴¹ o i servizi basati sui dati in corso di sviluppo da parte dell'ICDP – Digital Library⁴², nell'ambito del Piano nazionale di digitalizzazione del patrimonio culturale (PND)⁴³. Sembra poi superfluo ribadire come, in questo momento, una grandissima quantità di traffico verso qualsiasi tipologia di servizio digitale esposto in rete sia generata dai crawler, alla ricerca di dati per l'addestramento degli LLMs⁴⁴. Gli agenti interagiscono con i *Digital Cultural Assets* (DCA) ovvero con il Patrimonio culturale digitale nativo e non nativo, cuore dell'ecosistema. (Bellini 2025) identifica tre macro-criteri per la quantificazione del valore dei DCA:

- *Production Cost* (PC): il costo di produzione dei beni quindi i costi di digitalizzazione o i costi di produzione del bene nativo digitale.
- *Functional Value* (FV): una sorta di valore indotto dai possibili usi e riusi dei beni.
- *Cultural Value* (CV): il valore culturale e storico attribuito dalla comunità di esperti.

Il PC è in genere più facilmente quantificabile, almeno per i beni prodotti in tempi più recenti, mentre il FV e il CV possono chiaramente mutare molto in base al contesto, al tempo e ad altri fattori contingenti⁴⁵. Nel calcolo del valore dei DCA basato sul costo di produzione possono essere conteggiati, innanzitutto, gli investimenti fatti nel corso degli ultimi 40-50 anni nella catalogazione del patrimonio ovvero nella produzione di metadati descrittivi. Il solo Opac SBN indicizza 21.256.681 record per 125.675.014 localizzazioni⁴⁶. Vi è poi il costo della digitalizzazione del patrimonio delle biblioteche: le digitalizzazioni attualmente accessibili dall'Opac SBN sono 951.889⁴⁷, alle quali, entro il 2026, si aggiungeranno le digitalizzazioni provenienti dai cantieri del PND. Per la digitalizzazione di 107 mila microfilm conservati presso il Centro Nazionale per lo Studio del Manoscritto (CNSM) saranno spesi complessivamente 9.2 milioni di euro⁴⁸. Altri 27.9 milioni sono stati investiti per la digitalizzazione della documentazione catastale conservata negli Archivi di Stato e dei giornali quotidiani postunitari, appartenenti alle maggiori Biblioteche statali⁴⁹. Inoltre, Regioni e Province autonome hanno ricevuto 26 milioni di euro per la digitalizzazione di materiali cartacei e fotografici, e 650.000 euro per la digitalizzazione di microfilm di documenti archivistici e bibliografici di cui sono custodi⁵⁰.

⁴¹ <https://www.iccu.sbn.it/attivita-servizi/dati-aperti/>.

⁴² Si vedano il catalogo degli e-services di I.PaC sulla Piattaforma Digitale Nazionale Dati (PDND) e la piattaforma DPaaS “un ambiente di sviluppo e servizi tecnologici innovativi, per creare prodotti innovativi basati sui dati in modo semplice e scalabile”: <https://digitallibrary.cultura.gov.it/approfondimenti/ecomonic-dpaas/>.

⁴³ <https://digitallibrary.cultura.gov.it/il-piano/>.

⁴⁴ Sul tema si veda (De Robbio 2025).

⁴⁵ Si pensi, ad esempio, al dibattito sulla normativa sul riuso delle immagini dei beni culturali che vede contrapposti coloro che difendono gli incassi diretti derivanti dalla vendita delle licenze d'uso e coloro che sostengono che consentire il libero riuso genererebbe un indotto molto superiore; a questo proposito si veda (Modolo 2025).

⁴⁶ Dato al 14/7/2025: <https://opac.sbn.it/>.

⁴⁷ Dato al 14/7/2025: <https://opac.sbn.it/>.

⁴⁸ <https://digitallibrary.cultura.gov.it/avvisi/pnrr-digitalizzazione-del-patrimonio-culturale-online-la-procedura-di-gara-da-92-milioni-di-euro-per-la-categoria-microfilm-di-manoscritti-antichi/>.

⁴⁹ <https://digitallibrary.cultura.gov.it/avvisi/pnrr-digitalizzazione-del-patrimonio-culturale-online-la-procedura-di-gara-da-279-milioni-di-euro-per-la-categoria-carta-documentazione-catastale-registri-e-mappe-e-giornali-quotidiani/>.

⁵⁰ <https://pnrr.cultura.gov.it/gare-per-la-digitalizzazione-del-patrimonio-culturale-di-regioni-e-province-autonome-m1c31-1-strategie-e-piattaforme-digitali-per-il-patrimonio-culturale/>.

Il PC del Patrimonio nativo digitale per le biblioteche può forse essere inteso più come costo di acquisizione delle risorse native digitali, quali i costi per l'accesso permanente a repertori e banche dati, o quelli di acquisizione e gestione del deposito legale digitale.

Pur evitando di addentrarsi in analisi sul valore indotto dall'uso e riuso delle risorse e dei servizi delle biblioteche⁵¹, che esulerebbe forse le finalità di questo contributo, il FV dell'ecosistema delle biblioteche può essere, però, certamente ricondotto almeno ai servizi di consultazione e prestito delle risorse, sia digitali che no, tra i quali si annoverano anche servizi di rete come l'ILL e il Document Delivery. Infine, in relazione al processo che porta la comunità di esperti ad attribuire un CV ai DCA, sembra doveroso sottolineare il ruolo che ha la creazione del catalogo che, non a caso, è anche una delle *functions* principali che l'ecosistema svolge nei confronti dei DCA, durante tutto il loro ciclo di vita: "Il processo di contabilizzazione di un *heritage item* come *asset* necessita innanzitutto di una fase di rilevazione (*recognition*), che consiste nel raccogliere ed elaborare i dati disponibili al fine di rappresentarli nei prospetti contabili" (Aprile, Grandis, e Mocavini 2018). Altre funzioni sono quelle di digitalizzazione e/o acquisizione, metadattazione, accesso e fruizione, valorizzazione, conservazione e, non ultimo, cybersicurezza. Lo svolgimento di queste funzioni richiede chiaramente specifiche competenze e risorse tecnologiche. L'ultima componente del C3E sono gli *Hybrid Infrastructure Systems*, essenziali non solo per la tenuta degli asset digitali ma anche di quelli tradizionali. Essi comprendono una enorme varietà di infrastrutture e servizi cyber, come cataloghi e inventari online⁵², ILS e LSP⁵³, biblioteche e repository digitali⁵⁴, siti web, apps, sistemi di autenticazione, piattaforme per l'ILL, il Document Delivery e il prestito digitale, servizi basati su IA, sistemi di reportistica e di analisi dei dati, apparati di rete, sistemi di controllo degli accessi, sistemi di monitoraggio ambientale delle sale e dei magazzini, sistemi di allarme. Questa varietà è uno dei fattori che rende la sicurezza del C3E così difficile da proteggere, perché ciascuno di questi sistemi è potenzialmente anche un *single point of failure*⁵⁵. Di seguito, ci si soffermerà più nel dettaglio sulle infrastrutture che sottendono alcune delle funzioni chiave del C3E delle biblioteche italiane ma, intanto, è bene ricordare che, nell'ambito del PND, sono in corso di realizzazione una serie di infrastrutture e servizi che serviranno anche il comparto biblioteche (Cerullo et al. 2024). In ultimo, un C3E dovrebbe garantire il mantenimento nel tempo di tre *properties* caratterizzanti e interdipendenti (Bellini 2025):

- Affidabilità (*trust*): la capacità di preservare nel tempo le principali caratteristiche dei DCA ovvero accessibilità, autenticità, integrità, leggibilità⁵⁶.

⁵¹ A questo proposito, di sicuro interesse sarebbe una rassegna degli studi esistenti sul rapporto tra biblioteche e istruzione scolastica e formazione continua, e tra biblioteche e ricerca scientifica.

⁵² Nel 2023, il 72,6% delle biblioteche italiane aveva un catalogo in formato digitale: ISTAT - Statistiche culturali 2023 - Dati "Biblioteche" - Tavola 4.16: <https://www.istat.it/tavole-di-dati/statistiche-culturali-anno-2023/>.

⁵³ Nel 2023, il 45,6% delle biblioteche aveva una piattaforma web per l'erogazione di servizi on-line, <https://www.istat.it/tavole-di-dati/statistiche-culturali-anno-2023/>.

⁵⁴ Nel 2023, il 15,8% delle biblioteche aveva una teca digitale, propria o condivisa a livello locale o nazionale, <https://www.istat.it/tavole-di-dati/statistiche-culturali-anno-2023/>.

⁵⁵ https://en.wikipedia.org/wiki/Single_point_of_failure.

⁵⁶ Cfr. Glossario dei termini e degli acronimi allegato alle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici: <https://docs.italia.it/AgID/documenti-in-consultazione/lg-documenti-informatici-docs/it/bozza/allegati.html>.

- Resilienza (*resilience*): la capacità di prevedere e gestire i rischi cyber potenziali⁵⁷.
- Sostenibilità (*sustainability*): da intendersi come sostenibilità tecnica, ambientale, organizzativa, culturale ed economica.

SBN e Magazzini Digitali come componenti portanti del *Library Cyber Critical Ecosystem* nazionale

Nel contesto di quello che, a questo punto, potremmo definire il *Library Cyber Critical Ecosystem* italiano, le infrastrutture afferenti a SBN e al servizio Magazzini Digitali⁵⁸ non possono che essere considerate componenti portanti per l'assolvimento delle funzioni dell'ecosistema stesso, vale a dire:

- Censimento del patrimonio: 7.120 delle 8. 131 biblioteche aperte al pubblico sono parte della rete SBN⁵⁹. Ciò significa che, al netto del noto problema dei dati "sommersi"⁶⁰, la maggioranza delle informazioni sul patrimonio bibliografico o di altra natura delle biblioteche italiane è custodita all'interno dell'Indice SBN.
- Affidabilità delle informazioni sul lungo periodo: l'autorevolezza delle istituzioni che producono il censimento del patrimonio culturale è garanzia, nel lungo periodo, dell'affidabilità delle informazioni contenute.
- Tutela del patrimonio fisico: il catalogo SBN va considerato nella sua duplice veste di strumento di accesso e strumento di tutela. Esso, infatti, previene perdite e sottrazioni illecite e ne consente, laddove possibile, il ripristino.
- Circolazione dei documenti a livello locale, nazionale e internazionale: il catalogo SBN, come punto di accesso iniziale ai servizi di circolazione locale, e il servizio di ILL SBN sono infrastrutture essenziali per il prestito e la consultazione dei documenti.
- Supporto tecnologico al processo di patrimonializzazione⁶¹ dei documenti nativi digitali: Magazzini digitali, come servizio di conservazione e accesso di lungo periodo ai documenti nativi digitali, è attualmente l'unica infrastruttura bibliotecaria potenzialmente in grado di sostenere il processo di patrimonializzazione del nativo digitale che, viceversa, è soggetto a perdite più o meno accidentali dovute a cause come il mancato riconoscimento del valore del loro contenuto informativo⁶², l'obsolescenza tecnologica o la modifica unilaterale delle condizioni di accesso definite da editori, produttori o distributori dei documenti nativi digitali.

⁵⁷ Il primo documento che definisce ufficialmente il concetto di ciberresilienza è il Regolamento UE 2024/2847 c.d. Cyber Resilience Act: <http://data.europa.eu/eli/reg/2024/2847/oj>.

⁵⁸ <https://bncf.cultura.gov.it/servizi/magazzini-digitali/>.

⁵⁹ Dato al 25/7/2025: <https://www.iccu.sbn.it/it/SBN/poli-e-biblioteche/>.

⁶⁰ In questa dicitura è possibile far rientrare i dati non ancora recuperati dai cataloghi legacy, compresi quelli cartacei, il non catalogato e i dati presenti solo nei cataloghi di Polo.

⁶¹ "Per processo di patrimonializzazione si identifica l'insieme delle azioni, promosse su istanze sociali di tipo culturale, tecnico-scientifico e giuridico-amministrativo, attraverso le quali un qualsiasi oggetto, materiale, immateriale o digitale, viene considerato degno di sopravvivere al deperimento naturale per essere conservato nel tempo come testimonianza di civiltà" (ICDP 2023).

⁶² A questo proposito, si pensi in particolare all'attività di creazione e gestione degli archivi del Web.

I rischi specifici, reali o potenziali, per l'affidabilità, la resilienza e la sostenibilità di queste infrastrutture afferiscono a tre ambiti: quello legale, quello economico-gestionale e quello tecnologico.

Contesto legale

Nonostante SBN e Magazzini Digitali assolvano in tutto o in parte alle funzioni appena elencate, rispettivamente da 40 e 20 anni circa, un pieno riconoscimento del loro valore a livello istituzionale e legale non può dirsi compiuto. SBN è stata inserita tra le “basi dati di interesse nazionale” all’interno del Piano triennale per l’informatica nella Pubblica Amministrazione 2019-2021⁶³, ma nei successivi aggiornamenti il riferimento è stato espunto senza spiegazioni. Allo stesso tempo, la non esecutività dell’obbligo di deposito legale dei documenti nativi digitali⁶⁴ ha già causato e sta continuando a causare la perdita di moltissima documentazione di interesse nazionale. A ciò si aggiunge che nemmeno la più recente normativa comunitaria in materia di cybersicurezza, la Direttiva UE 2022/2555 (c.d. NIS2) e il D.lgs. 4 settembre 2024, n. 138 di recepimento della NIS2, sembra fornire indicazioni dirimenti per il settore cultura⁶⁵. Questo, infatti, non viene nominato né tra i settori ad alta criticità⁶⁶, come forse è normale che sia, né tra gli altri settori critici⁶⁷, tra i quali viene invece compreso quello della Ricerca. Tuttavia, il legislatore italiano dimostra una certa sensibilità alla questione nominando nell’Allegato III, dedicato alle Amministrazioni centrali, regionali, locali e di altro tipo, cui certamente moltissimi istituti e luoghi della cultura afferiscono, anche gli “Enti produttori di servizi assistenziali, ricreativi e culturali”; e includendo nell’Allegato IV, caso unico nel panorama europeo, “Soggetti che svolgono attività di interesse culturale”, qui da intendersi quindi come soggetti privati. Bisogna anche sottolineare che il Ministero della Cultura è Autorità di settore NIS⁶⁸ e, tra i suoi compiti di supporto all’Agenzia per la cybersicurezza nazionale (ACN)⁶⁹, vi è quello di convalidare l’elenco dei soggetti NIS per settore di competenza⁷⁰, proponendo eventuali ulteriori identificazioni governative. Purtroppo, il registro dei soggetti NIS non è pubblicamente disponibile, e non sappiamo se lo sarà mai, dal momento che, vigente la Direttiva NIS⁷¹, il registro era secretato.

Modello gestionale e di sostenibilità economica

Il modello gestionale e di sostenibilità economica di SBN, come ideato all’inizio degli anni ‘80

⁶³ https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2019-2021/05_dati-della-pubblica-amministrazione.html.

⁶⁴ Si veda infra (Bergamin e Messina 2025).

⁶⁵ www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/sg.

⁶⁶ I settori ad alta criticità sono elencati nell’Allegato I al D.lgs. 4 settembre, n. 138.

⁶⁷ D.lgs. 4 settembre, n. 138, Allegato II.

⁶⁸ D.lgs. 4 settembre, n. 138, art. 11.

⁶⁹ <https://www.acn.gov.it/>.

⁷⁰ Soggetti pubblici e privati appartenenti alle tipologie di cui agli allegati I, II, III e IV del D.lgs. 4 settembre 2024, n. 138. Tali soggetti, in base all’ art. 7 del medesimo decreto, sono tenuti all’obbligo di registrarsi sulla piattaforma dedicata della ACN: <https://www.acn.gov.it/portale/nis/registrazione>.

⁷¹ <http://data.europa.eu/eli/dir/2016/1148/oj>.

del '900 e consolidato nei due decenni successivi, rappresenta un *unicum* positivo, anche in una prospettiva allargata al contesto internazionale. Gli organi di governo SBN sono, però, in attesa di rinnovo da ormai quasi dieci anni⁷², e questo ha comportato un totale addossamento dell'onere decisionale e della responsabilità operativa sull'ICCU che, teoricamente, ne dovrebbe essere il "gestore"⁷³. Il venir meno del modello gestionale originale, a sua volta basato su una architettura tecnologica nativamente decentrata e distribuita, ha avuto un forte impatto anche sulla sostenibilità economica che ne discendeva. E le difficoltà di sostenere una infrastruttura così complessa hanno via via fatto propendere per un suo accentramento tecnologico. L'attuale modello di gestione e sviluppo sia del sistema Indice che dei sistemi di Polo, infatti, non sembra facilitare l'aggiornamento e l'innovazione, anche a causa di costi assai elevati, non più dettati dal mercato ma da situazioni di *lock-in* di fatto⁷⁴. Stessa sorte subisce anche il servizio "Magazzini Digitali". Nato come sperimentazione sulle base delle previsioni dell'art. 37 del D.P.R. 3 maggio 2006, n. 252, è stato inizialmente implementato grazie alla collaborazione tecnico-scientifica e il co-finanziamento non solo delle due Biblioteche nazionali centrali, ma anche della Biblioteca nazionale Marciana e della Fondazione Rinascimento Digitale⁷⁵. La prolungata assenza del regolamento tecnico attuativo del deposito legale digitale ha, tuttavia, distolto attenzione e fondi dal servizio per lunghi periodi, facendo convergere sulla Biblioteca nazionale centrale di Firenze la quasi totalità delle responsabilità tecnico-gestionali oltre che degli oneri finanziari, e rendendolo per questo non pienamente efficiente.

Potenziali criticità tecnologiche

La migrazione, in corso di completamento nel 2025, di tutte le infrastrutture e i servizi SBN⁷⁶ al Polo Strategico Nazionale (PSN)⁷⁷, per il tramite del Ministero della Cultura, ha avuto e avrà certamente un impatto fortemente positivo sulla questione della sicurezza. È bene specificare, però, che all'interno del PSN, l'approccio alla sicurezza è basato sullo *Shared Security Responsibility Model*, uno strumento attraverso il quale Cloud Service Provider (il PSN) e Cloud Service Customer (la PA che usufruisce dei servizi cloud) definiscono e regolano in che modo la responsabilità e l'accountability per la sicurezza dei dati e delle risorse venga suddivisa nell'ambito di uno specifico servizio Cloud⁷⁸. Ciò significa che per le biblioteche il problema della sicurezza non si esaurisce

⁷² <https://www.iccu.sbn.it/it/SBN/organi-di-governo-sbn/>.

⁷³ È doveroso sottolineare che coloro che si sono succeduti, in questi anni, alla direzione dell'Istituto centrale per il Catalogo Unico hanno più volte sollecitato, nelle opportune sedi, il rinnovo degli organi di governo SBN e che si sono fatti promotori della prima Assemblea dei Poli tenutasi nel 2015 e di quella in programma a dicembre 2025; purtroppo questi appelli sono rimasti evidentemente inascoltati.

⁷⁴ Nonostante l'attenzione sempre più diffusa per l'adozione di soluzioni hardware standard e software open source, sia oggettivi ostacoli tecnologici, quali la migrazione di grandi quantità di dati, che i costi del *reverse engineering* di soluzioni non largamente adottate e/o sostenute da una vasta community di sviluppo (spesso basate su linguaggi e formati estremamente customizzati), rendono di fatto la possibile concorrenza delle aziende sul mercato molto limitata.

⁷⁵ <https://wayback.archive-it.org/org-1284/20231204094728/https://www.depositolegale.it/accordo-mibac-editori/>.

⁷⁶ Indice e Opac SBN, SBNCloud, e altre banche dati come Manus e Edit XVI. Le infrastrutture per la gestione e conservazione del patrimonio digitalizzato, essendo parte del PND, sono ospitate dal Consorzio Cineca.

⁷⁷ <https://www.polostrategiconazionale.it/>.

⁷⁸ <https://www.polostrategiconazionale.it/chi-siamo/sicurezza/matrici-di-responsabilita-condivisa-della-sicurezza/>.

con il passaggio al PSN. Allo stesso modo, la scelta della BNCF, nel 2023, di entrare a far parte del Consorzio Cineca per la gestione dei servizi di Magazzini Digitali⁷⁹, dettata primariamente dall'esigenza di affidarsi ad un partner pubblico dotato di competenze specifiche e infrastrutture efficienti, si è rivelata vincente anche dal punto di vista della sicurezza⁸⁰. Se, però, si amplia la prospettiva all'intero *Library Cyber Critical Ecosystem* italiano, lo scenario tecnologico appare maggiormente problematico. Innanzitutto, se è vero che teoricamente tutti i dati e i servizi bibliotecari della PA centrale sono transitati o è previsto che transitino sul PSN, non è detto che questo passaggio copra davvero il 100% dei sistemi. Si pensi, ad esempio, a cataloghi e siti web, di istituzioni grandi e piccole, spesso non considerati critici, che vengono mantenuti in locale o in hosting a provider terzi non sempre dotati delle certificazioni previste da ACN. Dotati delle certificazioni previste ACN dovrebbero, invece, essere tutti i provider selezionati dalle PA locali per la migrazione ad ambienti cloud incentivata nell'ambito del Piano Nazionale di Ripresa e Resilienza⁸¹, e in parte già realizzata, anche prima del PNRR, soprattutto in alcune Regioni in cui sono storicamente presenti società e infrastrutture dedicate allo sviluppo e supporto ICT⁸². Così come la rispondenza ai requisiti di sicurezza dovrebbe essere imprescindibile nella scelta di fornitori di servizi ormai largamente diffusi nelle biblioteche, come il prestito digitale o l'accesso alle banche dati⁸³. Trattandosi di un caso che interessa il servizio di Web archiving di Magazzini Digitali, bisogna anche citare l'eventualità in cui l'hosting di taluni servizi sia affidato a provider terzi non certificati ACN, a causa dall'effettiva mancanza di alternative sul mercato, che equivarrebbe all'impossibilità di erogare i servizi stessi⁸⁴. Appare pertanto chiaro come anche sul piano delle soluzioni tecnologiche il panorama sia particolarmente variegato, e come da ciò possano dipendere livelli di cybersicurezza differenti. Certo, purché esistano dei backup e siano rispettate almeno le previsioni del GDPR, i potenziali

⁷⁹ Il Consorzio Cineca ospita già il servizio di conservazione e accesso alle tesi di dottorato (<https://tesidottorato.depositolegale.it>), ma è in corso di definizione anche l'affidamento per la reingegnerizzazione del servizio di rilascio del National Bibliography Number (NBN): <https://bncf.cultura.gov.it/servizi/magazzini-digitali/#cap-5>. Infine, è stato discusso il progetto di creazione di una infrastruttura per la conservazione e l'accesso di lungo periodo agli altri prodotti della ricerca.

⁸⁰ Le infrastrutture e i servizi cloud per la PA del Consorzio sono conformi a quanto previsto dal Regolamento ACN in materia: <https://www.acn.gov.it/portale/cloud>.

⁸¹ <https://padigitale2026.gov.it/misure>.

⁸² Si pensi a Lepida S.c.p.A. in Emilia-Romagna (<https://www.lepida.net/>) o a TIX in Toscana (<https://www.cloud.toscana.it/tix/>).

⁸³ Il principale riferimento in questo ambito è il Catalogo delle Infrastrutture digitali e dei Servizi cloud dell'ACN: <https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud>.

⁸⁴ Il servizio di Web archiving di Magazzini Digitali viene erogato attraverso la piattaforma Archive-it di Internet Archive che, seppure non certificata ACN, garantisce la conservazione di copie ridondate dei dati in datacenter indipendenti e la loro disponibilità per il download in qualunque momento: <https://archive-it.org/archive-it/>. Bisogna, però, ricordare che la tenuta di un servizio di conservazione non dipende solo dalle soluzioni tecnologiche adottate, ma anche dalla robustezza istituzionale ed economica del soggetto conservatore nonché dal contesto legale e culturale in cui il soggetto opera. Brewster Kahle, fondatore di Internet Archive, ha più volte dichiarato come una delle principali minacce alla loro attività derivi dalle battaglie legali intentategli dagli editori sulla liceità di alcuni servizi in relazione alle norme USA sul copyright. Per difendersi nei tribunali, infatti, la Fondazione ha perso centinaia di migliaia di dollari e rischia sanzioni milionarie, che minerebbero la capacità di Internet Archive di mantenere le proprie infrastrutture e i propri servizi così come fatto finora. A ciò, si aggiungono le attuali politiche del governo Trump che non solo hanno tagliato i fondi destinati alle istituzioni culturali e di ricerca, pubbliche e private, ma hanno anche creato un clima poco favorevole al lavoro di Internet Archive: <https://americanlibrariesmagazine.org/2025/06/04/newsmaker-brewster-kahle/#:~:text=Since%20founding%20the%20Internet%20Archive,him%20feel%20%E2%80%9Cvery%20encouraged.%E2%80%9D>.

danni materiali potrebbero essere ritenuti contenuti, ma la criticità di un servizio si misura anche e soprattutto in base alla mission dell'istituzione: la prolungata indisponibilità dell'accesso a siti web, cataloghi o repository di biblioteca può andare non solo a immediato discapito dell'attività di studenti e ricercatori, ma soprattutto della reputazione dell'istituzione⁸⁵. Per non parlare dei sistemi digitali per il controllo fisico degli ambienti che se non disponibili, anche per un breve periodo, possono costituire un problema per l'incolumità fisica delle persone e per la salvaguardia del patrimonio culturale. Se, ad esempio, ad essere attaccato fosse il sistema di controllo varchi di una biblioteca, l'istituto potrebbe non essere più nelle condizioni di sapere quante persone sono all'interno dell'edificio o quante di loro hanno lasciato la biblioteca con documenti rari o preziosi. Infine, in un ecosistema in cui tutte le componenti sono interdipendenti, non è possibile ignorare che, visto anche il contesto normativo descritto, le infrastrutture tecnologiche delle istituzioni culturali private possano essere ancora di più da attenzionare.

Conclusioni: dalla *Cyber security* alla *Cyber resilience*

Considerata la complessità del quadro fin qui delineato, che implica anche evidenti difficoltà nell'attribuzione univoca delle responsabilità in questo ambito, sarebbero innanzitutto auspicabili azioni di sensibilizzazione ed advocacy sul tema della cybersicurezza da parte delle istituzioni deputate alla tenuta delle infrastrutture bibliotecarie, come l'ICCU e le Biblioteche nazionali centrali, ma anche da parte delle associazioni professionali, come l'AIB o l'AIUCD. Azioni che dovrebbero essere seguite da una formazione specifica, da differenziare in base al livello di coinvolgimento nei processi che garantiscono la sicurezza di sistemi e servizi ma che tocchi, appunto, tutti i livelli. Sembra, infatti, di dover rilevare come proprio in un settore come quello delle biblioteche, che vanta una tradizione millenaria nella tutela del patrimonio culturale, si fatichi non poco ad affrontare un doveroso cambiamento culturale nella gestione del rischio cyber. Una formazione mirata degli addetti ai lavori, e degli utenti che interagiscono con il patrimonio, potrebbe sperabilmente almeno evitare le continue lamentele sulla richiesta di generare password "inutilmente complicate". Una volta acquisita consapevolezza dei rischi, però, per evitare danni economici e reputazionali talvolta molto ingenti, è necessario investire in sicurezza. L'elenco delle "misure tecniche, operative e organizzative adeguate [...] alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete [...] nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei [...] servizi", previste nel D.lgs. 4 settembre 2024, n. 138⁸⁶, mostra proprio l'importanza di approcciarsi alla gestione della cybersecurity come alla gestione di un processo articolato, che va dalla analisi delle vulnerabilità e dei rischi potenziali (c.d. *vulnerability assessment*) alla definizione delle azioni concrete afferenti ad una più ampia *cyber resilience strategy* in caso di attacco. Una rassegna delle misure di cybersicurezza specifica per biblioteche digitali si trova in (Tammaro e Bellini 2024). Ancor prima, sarebbe importante chiarire il quadro normativo illustrato e definire, quindi, per ciascuna funzione del C3E delle biblioteche quali sono i livelli di servizio che devono essere garantiti in termini di resilienza. Sulla base degli obiettivi, sarà possi-

⁸⁵ <https://www.ilpost.it/2024/05/22/british-library-conseguenze-attacco-informatico/>.

⁸⁶ D.lgs. 4 settembre 2024, n. 138, art. 24 commi 1 e 2.

bile scegliere il modello gestionale e le soluzioni tecnologiche adeguati. Ciò che desta maggiore preoccupazione sono ovviamente gli ingenti investimenti di cui necessita la cybersicurezza, per queste attività costanti di monitoraggio e aggiornamento di tutti i sistemi critici. Tuttavia, come ci insegna il caso della British Library, il costo della prevenzione è comunque sempre inferiore al costo del fallimento (The British Library 2024).

Riferimenti bibliografici*

Aprile, Rocco, Fabio Giulio Grandis, e Fabrizio Mocavini. 2018. «Heritage come asset nella contabilità economico-patrimoniale delle Amministrazioni pubbliche.» *Rivista della Corte dei conti* 3-4: 429–40. <https://www.corteconti.it/Download?id=7cbc64ff-575f-46fd-93a6-39dd52b6fb2f>.

Bellini, Emanuele. 2025. «Cyber Humanities for Heritage Security». *Commun. ACM* 68, 12 (December 2025), 112–117. <https://doi.org/10.1145/3735659>.

Cerullo, Luigi, Margherita Bartoli, Lina Antonietta Coppola, Costantino Landino, Antonio Davide Madonna, Antonella Negri, Giovanni Pescarmona, Chiara Fauda Pichet, Margherita Porena, e Valentina Rossetti. 2024. «Verso la creazione di un Ecosistema digitale nazionale per la Cultura.» *DigItalia* 19 (2): 11–48. <https://doi.org/10.36181/digitalia-00101>.

Clusit - Associazione Italiana per la Sicurezza Informatica. 2012. *Rapporto Clusit sulla sicurezza ICT in Italia*. https://clusit.it/wp-content/uploads/download/Rapporto_Clusit%202012.pdf.

Clusit - Associazione Italiana per la Sicurezza Informatica. 2025. *Rapporto Clusit sulla Cybersecurity in Italia e nel mondo*. <https://clusit.it/rapporto-clusit/>.

De Robbio, Antonella. 2025. «I bot dell'AI all'assalto delle biblioteche pubbliche.» *Il BO Live*. 26 luglio 2025. <https://ilbolive.unipd.it/it/news/societa/bot-dellai-allassalto-biblioteche-pubbliche>.

ICDP (Istituto Centrale per la Digitalizzazione del Patrimonio Culturale) - Digital Library. 2023. *Piano nazionale di digitalizzazione del patrimonio culturale (PND)*. <https://docs.italia.it/italia/icdp/icdp-pnd-docs/it/v1.1-febbraio-2023/index.html>.

IFLA (International Federation of Library Associations and Institutions) e UNESCO (United Nations Educational, Scientific and Cultural Organization). 2022. «Manifesto IFLA-UNESCO delle biblioteche pubbliche 2022.» *AIB studi* 62 (2): 431–34. <https://doi.org/10.2426/aibstudi-10097>.

Messarra, Luca, Chris Freeland, e Juliya Ziskina. 2024. «Vanishing Culture: A Report on Our Fragile Cultural Record.» *Internet Archive*. <https://blog.archive.org/2024/10/30/vanishing-culture-a-report-on-our-fragile-cultural-record/>.

MiC - Ministero della Cultura. 2024. *Minicifre della cultura. Una raccolta di dati statistici sulla cultura*. https://www.fondazione scuolapatrimonio.it/wp-content/uploads/2024/12/Minicifre-della-cultura_edizione-2024.pdf.

Modolo, Mirco. 2025. «Libero riuso delle immagini del patrimonio culturale pubblico: profili di compatibilità con il codice dei beni culturali e del paesaggio.» In *Strumenti del Dipartimento di Giurisprudenza di Siena*, a cura di Mario Perini, 3: 29–56. Florence: Firenze University Press, USiena Press. <https://doi.org/10.36253/979-12-215-0702-7.07>.

Neglia, Grazia, Mariarosaria Angrisano, Ippolita Mecca, e Francesco Fabbrocino. 2024. «Cultural Heritage at Risk in World Conflicts: Digital Tools' Contribution to Its Preservation.» *Heritage* 7 (11): 6343–65. <https://doi.org/10.3390/heritage7110297>.

* Ultima data di consultazione dei siti web: 26 luglio 2025.

Ovenden, Richard. 2021. *Bruciare libri: la cultura sotto attacco: una storia millenaria*. Tradotto da Luisa Doplicher e Daniele A. Gewurz. Milano: Solferino.

Tammaro, Anna Maria, e Emanuele Bellini. 2024. «Il ruolo della cybersecurity per le biblioteche digitali: sfide attuali e strategie di protezione.» *DigItalia* 19(2): 100–14. <https://doi.org/10.36181/digitalia-00104>.
The British Library. 2024. «Learning lessons from the cyber-attack. British Library cyber incident review.» *The British Library*. <https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf/>.

Uddin, Rafe, e Daniel Thomas. 2024. «British Library to burn through reserves to recover from cyber attack.» *Financial Times*, maggio.