

Toward a cultural cyber-critical ecosystem: concepts, threats and challenges

Emanuele Bellini 

Department of Humanities Studies, Roma Tre University, Rome, Italy, and

Emiliano Degl’Innocenti

*Opera del Vocabolario Italiano, Consiglio Nazionale delle Ricerche,
Sesto Fiorentino, Italy*

Digital Library
Perspectives

581

Received 27 January 2026
Revised 10 May 2026
Accepted 12 June 2026

Abstract

Purpose – The purpose of this paper is to introduce and formalize the Cultural Cyber-Critical Ecosystem (C3E) as a conceptual and operational framework for understanding Cultural Heritage as a cyber-critical domain. This study specifically addresses cyber-cognitive threats, identified as a pressing yet largely underexplored risk to the long-term preservation, integrity and intelligibility of Digital Cultural Assets (DCAs).

Design/methodology/approach – This paper adopts a conceptual and analytical approach grounded in systems theory, resilience engineering and digital heritage studies. Core C3E concepts are mapped against emerging cyber-cognitive threat vectors using dependency analysis and the Functional Resonance Analysis Method (FRAM). Hybrid Infrastructures, such as DARIAH-IT, are examined as empirical reference cases to illustrate how human, cyber and physical layers interact across the full DCA life cycle.

Findings – The analysis demonstrates that Cultural Heritage infrastructures exhibit critical dependencies not only at technical and organizational levels, but also at semantic, cognitive and trust levels. Cyber-cognitive dependencies – arising from human–AI interaction, distributed decision-making and semantic mediation – represent significant vulnerability channels capable of triggering cascading failures. At the same time, when properly governed, these dependencies enable resilience, adaptive capacity and long-term meaning preservation. The findings support the characterization of advanced heritage infrastructures as Hybrid Infrastructures with Critical Infrastructure properties.

Originality/value – The paper provides the first conceptualization of Cultural Heritage as a Cultural Cyber-Critical Ecosystem. By explicitly integrating cyber-cognitive threats, dependency taxonomies and resilience modeling, it extends existing digital heritage and FAIR-based approaches toward a critical-infrastructure perspective. The C3E framework offers scholars, cultural operators and policymakers a novel lens for analyzing risk, trust, resilience and sustainability of digital cultural heritage. The novelty of C3E lies in four distinct contributions that collectively go beyond any single predecessor: (i) it reconceptualizes Digital Cultural Assets as cyber-cognitive targets – not merely technical objects to be preserved – introducing an adversarial dimension absent from digital preservation frameworks such as OAIS (ISO 14721) and FAIR; (ii) it applies Critical Infrastructure Protection (CIP) logic to the cultural domain by formalizing dependency taxonomies, cascading failure paths and resilience engineering principles (AMRL) that are structurally absent from heritage-specific frameworks; (iii) it grounds socio-technical systems theory in an explicitly mission-driven, governance-accountable model, operationalizing the human–cyber–physical layers through FRAM-based functional analysis rather than treating them as purely descriptive categories; and (iv) it



© Emanuele Bellini and Emiliano Degl’Innocenti. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licenses/by/4.0/>

Digital Library Perspectives
Vol. 42 No. 3, 2026
pp. 581-606
Emerald Publishing Limited
2059-5816
DOI 10.1108/DLP-01-2026-0031

introduces analytically novel constructs that have no direct equivalents in OAIS, FAIR or conventional CIP frameworks.

Keywords Resilience, Trust, Sustainability, Cultural cyber critical ecosystem, Cyber cognitive operation, Digital cultural assets

Paper type Research paper

1. Introduction

The accelerating digital transformation and the convergence of cyber–physical systems are profoundly reshaping the cultural heritage and humanities domains. Libraries, archives and museums – traditional custodians of collective memory – are increasingly responsible for managing digital cultural assets, whether born-digital or produced through digitization. Digital objects have therefore become central to preservation strategies and essential instruments for ensuring long-term cultural accessibility across generations.

This transformation requires a redefinition of cultural heritage that extends the process of heritagization to digital artifacts (Musiani and Schafer, 2016) in their full technological, informational and cognitive diversity.

Cultural institutions now depend extensively on ICT infrastructures, digital platforms and cyber services to fulfill their missions of preservation, dissemination and access. While these technologies significantly enhance global reach and knowledge circulation, they simultaneously introduce new interdependencies, systemic complexity and exposure to cyber and hybrid threats that remain insufficiently addressed.

Cultural heritage increasingly exhibits the defining characteristics of complex socio-technical systems. First, operations are inherently underspecified, meaning that adverse events often arise from unexpected combinations of otherwise routine activities. Second, the ecosystem comprises multiple interconnected sub-systems with nonlinear and sometimes opaque interactions, requiring holistic approaches capable of coping with uncertainty and “unknown unknowns.” Third, the involvement of heterogeneous stakeholders – often operating with weak standardization, limited interoperability, fragmented governance and constrained resources – further amplifies systemic vulnerability and complicates decision-making.

Despite these conditions, prevailing approaches to digital cultural heritage management continue to prioritize access, curation and long-term preservation while underestimating issues of resilience, trust and adversarial risk. As a result, existing frameworks struggle to account for cascading failures, cyber–cognitive threats and the strategic manipulation of digital cultural assets.

To address these gaps, this paper introduces the *Cultural Cyber-Critical Ecosystem (C3E)* framework, conceptualizing digital cultural heritage as a *Networked Ecosystem of Ecosystems*. The framework integrates critical infrastructure theory, digital ecosystem modeling and the life cycle of digital cultural assets to capture the interdependent, dynamic and mission-oriented nature of the cultural heritage domain. C3E formalizes key components – including digital cultural assets, agents, resources, hybrid infrastructures, trust, resilience and sustainability – supporting both governance and long-term stewardship.

By establishing the theoretical foundations of *Cyber Humanities* as an emerging discipline (Bellini, 2025; Adorni and Bellini, 2025), C3E clarifies the interaction between cultural practices and cyber infrastructures and strengthens the science–policy interface.

2. Theoretical positioning of C3E

The Cultural Cyber-Critical Ecosystem (C3E) framework is positioned at the intersection of four established intellectual traditions while extending beyond the scope of each. This section makes explicit what C3E borrows from, and where it departs from, each tradition – a comparison that underscores the framework’s distinctive contribution.

2.1 Positioning against digital preservation frameworks: OAIS and FAIR

The Open Archival Information System (OAIS, ISO 14721) is the canonical reference model for long-term digital preservation. It defines the functional entities and information flows required to receive, archive and disseminate digital objects: Ingest, Archival Storage, Data Management, Administration, Preservation Planning and Access. OAIS is authoritative for describing what a preservation system must do and for establishing the Submission, Archival and Dissemination Information Packages (SIP, AIP, DIP). FAIR principles (Findable, Accessible, Interoperable, Reusable) complement OAIS by specifying data quality requirements for scientific and cultural data sets in networked environments ([Wilkinson et al., 2016](#)).

C3E is explicitly designed to incorporate both OAIS and FAIR principles: the DCA life cycle maps onto OAIS functional entities, and FAIR principles are embedded in C3E’s governance and sustainability requirements (see the MetaFAIR Ecosystem and FAIR-aware workflow orchestration discussed in Section 4.3.E). However, C3E departs from OAIS and FAIR in three critical dimensions. First, OAIS and FAIR treat digital objects as artifacts to be preserved and made accessible under safe or merely negligent conditions; C3E explicitly models an adversarial environment in which digital cultural assets are targets of cyber-cognitive operations designed to corrupt meaning and erode trust rather than destroy data. OAIS has no adversary model; C3E’s entire dependency taxonomy (Section 4.3.F) is organized around attack vectors. Second, OAIS is a static functional model: it defines roles and information flows but does not model dynamic system behavior, resource constraints or emergent failures under stress. C3E introduces Functional Metabolism (FM) precisely to model the stochastic, resource-dependent quality of outputs and to capture how adversaries can degrade trustworthiness by exploiting resource scarcity rather than technical failure. Third, OAIS and FAIR operate below the level of meaning: they ensure bit-level and metadata integrity but provide no framework for protecting validated meaning – the semantically interpreted, institutionally authorized understanding of a Digital Cultural Asset that C3E identifies as a strategic resource. These gaps justify C3E as an extension of, rather than a replacement for, OAIS and FAIR.

2.2 Positioning against critical infrastructure protection models

Contemporary Critical Infrastructure Protection (CIP) frameworks – including the EU NIS2 Directive (2022/2555), the Council Directive on Resilience of Critical Entities (CER, 2022/2557) and the NIST Cybersecurity Framework (CSF 2.0) – identify sectors whose disruption would have severe societal, economic or security consequences. These frameworks provide risk assessment methodologies, dependency analysis tools, incident reporting obligations and sector-specific resilience requirements. The NIST CSF in particular organizes protection activities around five functions: Identify, Protect, Detect, Respond and Recover. C3E draws extensively on CIP logic. Its argument that cultural heritage exhibits critical infrastructure properties – essential societal functions, cascading interdependencies and high-consequence failure modes – is grounded in the CER Directive’s criteria. The AMRL (Anticipate-Monitor-Respond-Learn) cycle used in C3E’s resilience modeling is directly aligned with Hollnagel’s resilience engineering precepts, which

underpin many CIP frameworks. However, C3E diverges from conventional CIP models in two fundamental respects. First, standard CIP frameworks define “criticality” in terms of service availability and physical continuity (e.g., energy supply, transport, water). C3E reconceptualizes criticality for a domain where the primary asset is not availability but meaning: the integrity, interpretability and trustworthiness of digital cultural assets across generational time horizons. A cultural heritage infrastructure may remain technically operational while being cognitively compromised – a failure mode for which CIP frameworks have no category. Second, CIP frameworks address cyber threats predominantly as technical attacks: intrusion, data exfiltration, ransomware. C3E introduces the cyber-cognitive operations (CCO) dimension, in which the objective is not system disruption but epistemic manipulation – corrupting the narratives and trust relationships that give digital cultural assets their societal significance (Adorni *et al.*, 2026). This adversarial model requires governance responses that CIP frameworks do not provide, including provenance-by-design, cognitive integrity monitoring and trust capital management.

2.3 Positioning against socio-technical systems theory

Socio-technical systems (STS) theory, originating with Emery and Trist (1960) and later extended by Kling (1980), Baxter and Sommerville (2011) and others, holds that organizations are jointly optimized systems in which social and technical subsystems must be designed together. The core principle is that technical efficiency cannot be achieved by optimizing the technical subsystem in isolation; the social subsystem – roles, norms, governance structures, knowledge practices – is equally constitutive of system performance. In information systems research, STS theory informs participatory design, requirements engineering and organizational change management.

C3E is consistent with STS theory in its tripartite Human–Cyber–Physical World (HCPW) ontology and in its insistence that governance, expertise and epistemic community are co-constitutive of infrastructure integrity – not merely contextual factors (Adorni *et al.*, 2026). The C3E Agent taxonomy (Human, Organizational and Software Agents) maps directly onto the social and technical subsystems of STS theory, and the FRAM-based functional analysis operationalizes the joint optimization principle at the level of individual workflow functions. However, C3E extends STS theory in three significant ways. First, STS theory was developed for design-time optimization of organizational systems; C3E applies the joint-optimization principle at runtime, modeling how dynamic resource flows, functional metabolism and adversarial perturbations jointly determine output quality and trustworthiness. Second, STS theory is descriptive and normative but not inherently adversarial; C3E explicitly models a threat environment in which the human (cognitive) layer is itself a primary attack surface. Third, STS theory has no category for long-duration identity preservation across generational time horizons – a requirement central to cultural heritage and one that forces C3E to operationalize identity in terms of mission continuity rather than structural stability (see Section 4). Table 1 summarizes the comparative positioning of C3E against the three predecessor traditions.

3. The fragility of digital cultural heritage: the emergence of hybrid threats

Escalating cyber risks expose an unsettling reality: the operating environment is becoming more contested, yet many societal sectors – especially cultural heritage – remain underprepared. Unlike domains formally classified as critical infrastructures (e.g., energy, transport), cultural heritage lacks an embedded culture of cybersecurity and resilience. Applying Hollnagel’s resilience framework (Hollnagel and Woods, 2006) – articulated around the capabilities to *anticipate*, *respond*, *monitor* and *learn* – highlights a set of

Table 1. Comparative positioning of C3E against predecessor frameworks

Dimension	OAIS/FAIR	CIP Models (NIS2, NIST CSF)	STS theory	C3E (this paper)
Primary goal	Long-term access and interoperability	Service availability and continuity	Joint optimization of social and technical subsystems	Preservation of ecosystem identity (meaning, trust and cognitive integrity under adversarial conditions)
Adversary model	None (benign environment assumed)	Technical cyber threats (intrusion, ransomware)	None (design optimization focus)	Cyber-cognitive operations targeting meaning, trust and institutional legitimacy
Unit of protection	Digital object (bits, metadata)	Service and system availability	Work system performance	Validated meaning, cognitive integrity of DCA and ecosystem trustworthiness
Dynamic modelling	Static functional roles (OAIS)	Risk registers and impact assessment	Design-time joint optimization	Runtime FRAM-based functional metabolism and dependency propagation
Temporal scope	Generational (preservation horizon)	Operational (incident recovery)	Project/organizational life cycle	Open-ended, identity preserved through mission continuity across technological and institutional change

characteristic “failures of knowledge” that render the cultural domain particularly fragile (Bellini, 2025):

- *Failure of “Knowing What to Expect” (Anticipate):* The sector underestimates potential sources of disruption and systemic pressure. A persistent *false sense of security* – rooted in assumptions of openness, stability and neutrality of cultural information systems – conceals structural vulnerabilities (Bellini and Degl’Innocenti, 2024). This perception has skewed attention toward “traditional” agendas (long-term preservation, curation, access) while overlooking adversarial risk.
- *Failure of “Knowing What to Do” (Respond):* When disruption occurs, institutions struggle to adapt at pace. Contributing factors include chronic *resource constraints*, *skills and awareness gaps* and the *slow cadence of organizational digital transformation*. Siloed, on-premises content architectures and entrenched legacy ICT further create *single points of failure*, elevating the likelihood and impact of cyber incidents and digital object loss. The costs of recovery and hardening often exceed the means of heritage organizations, which must rely on ad hoc or philanthropic support – a precarious foundation for resilience.
- *Failure of “Knowing What to Look For” (Monitor):* The complexity of the digital cultural heritage ecosystem amplifies *cascade effects*, distributing harm across systems and over time that are difficult to monitor. In fact, impacts can be read along three horizons that rewire different monitoring tools, procedures and skills:
 - *Short-term:* Immediate service disruption (e.g., sabotage, vandalism, ransomware) can curtail access to digitized collections and research infrastructure, with global repercussions and substantial recovery costs (e.g., the British Library attack).
 - *Mid-term:* *Cyber–Cognitive Operations (CCO)* degrade *reputation* and *trustworthiness* of digital assets, for example via man-in-the-middle compromises, interference with digital signatures or hash collisions – raising doubt about authenticity and provenance for materials retrieved online.
 - *Long-term:* Advanced persistent threats (APTs), as a form of CCO, target *cultural identity* and *collective memory*. By poisoning archives – through deepfaked imagery, counterfeit manuscripts, altered content and manipulated metadata/paradata – malicious actors can systematically distort historical narratives. The accelerating availability of *generative AI* and *large language models* intensifies this risk by blending authentic and synthetic content in ways that frustrate detection and verification.
- *Failure of “Knowing What Has Happened” (Learn):* Resilience requires rigorous, evidence-based learning from both failures and successes. Conflicts, disasters and accidents underscore the urgency and complexity of safeguarding tangible heritage (e.g., war-related damage to sites and institutions; the 1966 Florence flood; the Notre-Dame fire). However, despite rapid technological advances, the cultural heritage sector remains constrained by limited awareness, insufficient skills and a lack of institutional preparedness. In particular, the absence of dedicated training programs and structured learning pathways within responsible agencies hampers the ability to learn lessons and into timely adaptation. This gap significantly reduces the sector’s capacity to mitigate emerging risks in the short term and to operationalize learning as a driver of resilience.

3.1 Cognitive warfare and the cyber-cognitive continuum

According to NATO Report (Blatny, 2025) *Cognitive Warfare* extends conflict into the terrain of perception, trust and meaning. Combined with cyber capabilities, it manifests as *cyber-cognitive operations (CCO)*: coordinated actions that use digital infrastructures not only as targets and tools, but as *vectors for shaping belief, legitimacy and confidence*. The primary objective is not necessarily to destroy data, but to *undermine trust* in information, institutions and shared cultural reference points. Within this continuum, *digital cultural heritage* – digital libraries, museum repositories, archival platforms – becomes a privileged target. These assets embody symbolic authority, epistemic value and institutional credibility; attacks therefore reverberate far beyond technical harm, destabilizing social sense-making and collective memory.

Digital cultural heritage systems operate on assumptions of *authenticity, integrity* and *institutional reliability*. CCOs exploit these assumptions by subtly manipulating or casting doubt on assets and processes rather than overtly destroying them (Bellini, 2025). Typical vectors include:

- *Altering* or selectively corrupting digital artifacts and/or their metadata;
- *Injecting* plausible but false contextual and paratextual information exploiting advanced tools as deepfake;
- *Impersonating* heritage institutions or domain experts; and
- *Seeding narratives* that question the neutrality, competence or legitimacy of memory institutions.

Even when technically reversible, such actions inflict *lasting cognitive effects* by cultivating uncertainty and polarization around the interpretation of the past. From a Cognitive Warfare perspective, *trustworthiness* is the core asset under attack and heritage institutions function as trusted intermediaries between citizens and collective memory. CCOs target three interrelated dimensions:

- (1) *Epistemic trust* – confidence that digital objects are authentic, accurate and traceable;
- (2) *Institutional trust* – belief in the integrity, competence and independence of managing organizations; and
- (3) *Societal trust* – shared acceptance of cultural narratives as a basis for identity, cohesion and democratic life.

The *mere possibility* that records have been manipulated can degrade confidence – even absent definitive proof – eroding social resilience without triggering conventional cybersecurity thresholds.

For institutions stewarding digital cultural heritage, Cognitive Warfare *blurs the boundary* between cybersecurity, information integrity and societal resilience. Heritage infrastructures become part of a *cognitive battlespace* characterized by ambiguity, persistence and deniability. Defenders bear a disproportionate burden: they must *continuously demonstrate* authenticity and integrity, while attackers need only *introduce doubt*.

Strategically, erosion of trust in cultural heritage institutions undermines democratic values, pluralistic memory and public confidence in expertise. Spillover effects can propagate to *scientific bodies, public authorities* and *governance structures*, weakening the broader informational commons on which open societies depend.

To raise awareness of these emerging threats and to assess their systemic impact, it is necessary to adopt a domain model capable of capturing not only structural components and functional processes, but also the multi-layered interdependencies among ecosystem elements. The ecosystem metaphor highlights the deep interdependence of heterogeneous actors, technologies and resources within this informational environment, which Floridi conceptualizes as a constellation of “inforgs” operating within the broader “infosphere” (Floridi, 2014). Moreover, this type of ecosystem should not be understood as a merely spontaneous or emergent phenomenon to be passively observed. Rather, it constitutes an intentionally designed and governed system, explicitly conceived to confront hybrid threats and to manage the challenges posed by the accelerating digital transformation of the cultural heritage domain.

To this end, the following section refines the concept of the Cultural Cyber-Critical Ecosystem (C3E), recently introduced in the literature (Bellini, 2025; Bellini and Degl’Innocenti, 2025; Adorni and Bellini, 2025), by explicitly analyzing and strengthening it against the emerging landscape of hybrid threats.

4. Cultural cyber critical ecosystem (C3E)

As articulated in (Bellini, 2025) and (Bellini and Degl’Innocenti, 2024; Adorni and Bellini, 2025), the cultural heritage domain can be conceptualized as a complex human–cyber–physical ecosystem, reflecting both its multidimensional composition and its essential societal function. Within this perspective, it is framed as a *Cultural Cyber-Critical Ecosystem* (C3E): a system composed of complementary entities that are not merely interconnected but structurally interdependent, collectively oriented toward a shared mission and a common social value proposition.

More specifically, the C3E should be understood as a *Networked Ecosystem of Ecosystems* (NEoE). Its constituent parts can themselves be modeled as ecosystems, each characterized by internally coherent interactions among actors, technologies, roles and assets. A paradigmatic example is provided by digital libraries, in which tools, users, institutional roles and digital cultural assets interact according to an explicit mission and governance framework.

At the same time, each digital library operates within a broader relational context, maintaining functional, informational and institutional dependencies with other entities – such as additional digital libraries, museums, archives and research infrastructures. These relationships form a dense web of interdependencies, through which local ecosystem dynamics propagate across the wider cultural heritage domain, reinforcing the systemic nature of the C3E.

C3E should be also considered critical, as it “is crucial for the maintenance of vital societal functions” (Council Directive 2022/2557/EC on Resilience of Critical Entities).

Anyhow, ecosystems can be treated as coherent units of analysis only insofar as they retain a recognizable *identity* over time. Multiple approaches to defining identity have been proposed. Some authors, such as the philosopher Wiggins (1967), ground system identity in spatiotemporal continuity, emphasizing persistence as the defining criterion. By contrast, Varela’s formulation (1979) conceptualizes identity in terms of structure and organization. Structure denotes the concrete configuration of a system’s components and the relations among them at a given moment, while organization refers to the set of rules and constraints that define and sustain those components and their relationships. This perspective has been further developed within the Quantum Resilience framework (Roberts, 2015), which extends the structural–organizational view by explicitly introducing the notion of valuable function. From this standpoint, identity is not defined solely by what a system is (its structure), but also

by what it does – namely, its capacity to deliver functions that are meaningful and valuable within its operational and societal context. From this perspective, identity emerges from the joint contribution of structure and function, as it is through the sustained delivery of functions and services that a system remains recognizable and meaningful to other systems. However, the assumption of the persistence of the structure could be not necessary for the identity preservation in C3E. In fact, in *C3E the preservation of the functions with a purpose defined by the C3E mission, is the actual source for recognition and thus for identity*. Thus, C3E Identity has not any dependency from its internal structure that can (should) change across space and time because of its capacity to adapt to changing condition.

The mission of the C3E is to establish a trustworthy, resilient and sustainable environment in which the heritagization (Musiani and Schafer, 2016), preservation, protection, accessibility and intelligibility of digital cultural assets can be collectively ensured over the long term, safeguarding their continuity, authenticity and meaning for present and future generations alike. This mission is aligned with the UNESCO Guidelines (Boston, 1988) whose approach is “save history, not rewrite it” and get inspiration by the Moore’s theory of digital preservation (Moore, 2008) and by the perspective of “interoperability with the future” of digital objects defined in (Paskin, 2006; Rusbridge et al., 2005). Thus, even if structure and functions are preserved, a C3E that alters the scope of its action loses its identity and cannot be recognized as the same system over time. Accordingly, we explicitly posit that the identity of the C3E is grounded in the continuous realization, across space and time, of those Functions that enable the fulfillment of its mission. Once the mission and identity of an ecosystem are defined, one of the most challenging tasks is the delineation of its boundaries. This challenge is particularly pronounced in the Cultural Heritage domain, which is inherently fluid and characterized by significant variability across both space and time. As noted by Cumming and Collier (2005), determining system boundaries is complex, as is assessing the extent of change that can be accommodated before a system becomes fundamentally different in nature. Within the Cultural Cyber-Critical Ecosystem (C3E), boundary definition requires explicit consideration of scale along two dimensions: spatial and temporal. The spatial scale can be understood in relation to the highest level of governance and authority that provides coherence and accountability to the ecosystem. In the context of Cultural Heritage, the national level emerges as an appropriate scale of analysis, as it aligns institutional responsibility, legal frameworks and preservation mandates. The temporal scale, by contrast, cannot be bounded in conventional terms. Cultural Heritage is intended to be preserved across indefinite time horizons, extending beyond technological life cycles and institutional continuity. Consequently, the C3E must be conceived as a long-lived ecosystem, designed to absorb change while maintaining identity and purpose over time.

5. Cyber cognitive threats for C3E

This section aims to map the principal C3E concepts recently introduced by Bellini and Degl’Innocenti (2025) against cyber-cognitive threats, which represent one of the most pressing yet largely neglected risks to which the Cultural Heritage domain is currently exposed.

5.1 Digital cultural assets (DCAs) as cyber-cognitive targets

Within the Cultural Cyber-Critical Ecosystem (C3E), *Digital Cultural Assets (DCAs)* constitute a critical subclass of Cultural Assets. DCAs are digital objects that have undergone digital heritagization (Musiani and Schafer, 2016), acquiring cultural, epistemic and symbolic significance. They may be born-digital or derived from digitization and function as

intangible, trust-bearing assets embedded in institutional and societal memory systems. From a cyber-cognitive perspective, DCAs represent *high-value targets*. Their authority and legitimacy make them attractive for cyber-cognitive operations aimed at manipulating perception, eroding trust or distorting collective memory rather than causing overt technical disruption. In line with the IFLA Library Reference Model (LRM) (Riva et al., 2017), each DCA is treated as an *Item* (LRM-E5), while multiple DCAs may correspond to the same intellectual or artistic creation (LRM-E2). Interoperable persistent identifiers and co-reference mechanisms (Bellini et al, 2012) are therefore essential not only for preservation and access, but also for *resilience against hybrid attacks*. Diversity of formats, custodians and infrastructures helps confine both technical and cognitive impacts of localized compromise. According to Bellini and Degl'Innocenti (2025) each DCA is associated with a multidimensional *Value* (V) (Production, Cultural, Functional) that guides governance and protection priorities and correlates with *attack attractiveness*. High cultural and symbolic value increases the potential cognitive impact of manipulation, while functional value influences visibility and exposure. The Production value represents the actual amount of effort and resources used to produce the digital artefacts. Beyond the digital object itself, *metadata and paradata* are central to cognitive integrity.

Subtle alterations to provenance, context or curatorial decisions may undermine authenticity and institutional credibility without modifying the object's content. Consequently, DCAs must be protected as *cognitive assets*, requiring integrated technical, semantic and governance-level safeguards. In Table 2, a mapping between DCA Components and their related Cyber-Cognitive Attack Vectors is provided.

Cyber-cognitive operations rarely need to destroy DCAs. *Minimal, plausible manipulations* of metadata, paradata or high-value narratives are often sufficient to erode trust. Effective protection therefore requires treating DCAs as *cognitive-strategic assets*, not merely preserved digital objects.

5.2 Agents as cognitive and reputational actors in the C3E

Within the Cultural Cyber-Critical Ecosystem (C3E), *Agents* are entities capable of processing information, making decisions and assuming responsibility for functions that sustain the ecosystem's mission. Each agent is defined by Attributes (At), Type (Ty), Reputation (Rep) and Functions (Fs) (Bellini and Degl'Innocenti, 2025).

Attributes (At) uniquely identify an agent within the C3E and support accountability and traceability. They include identifiers, legal references, institutional affiliations and other credentials that ground the agent's authority and responsibility. From a cyber-cognitive perspective, attributes are also *identity anchors*: their manipulation or impersonation constitutes a primary vector for trust erosion. The Type (Ty) of Agents are classified as: *Human Agent*, *Organizational Agent* (include cultural institutions and GLAM organizations) and *Software Agent* (include ETL pipelines, Agentic AI components, LLM, etc.). A critical subclass of Organizational Agent is the *Institution* (e.g., library, archive, museum), which functions as a *trusted cognitive mediator* between Digital Cultural Assets (DCAs) and society (Bellini, 2025). These institutions do not merely store or deliver content; they curate meaning, validate authenticity and sustain trustworthy epistemic continuity in face of stressors. Actually, their role is analogous to that of *clearing houses* in other critical domains, managing complex exchanges through trusted intermediation. Technologies such as Distributed Ledger Technology (DLT) can further reinforce this role by supporting verifiability, provenance and auditability (Bellini et al., 2025). An agent's *Reputation* (Rep) reflects the accumulated perception of its reliability, competence and integrity (Luhmann, 1979). For cultural institutions, reputation is directly tied to their ability to prevent two

Table 2. Mapping DCA components to cyber-cognitive attack vectors

DCA component	Role in C3E	Typical cyber-cognitive attack vectors	Primary cognitive impact
DO – digital object	Digital manifestation of the cultural asset	Content manipulation, substitution, deep-fake injection, selective corruption	Distortion of historical evidence; confusion between authentic and falsified records
M – metadata	Describes identity, provenance, authenticity and access	Alteration of provenance records, timestamps, identifiers, authorship or rights metadata	Undermining authenticity, traceability and institutional reliability
P – paradata	Documents curatorial decisions, processes and context	Suppression, falsification or selective omission of decision trails	Loss of interpretability, weakened forensic reconstruction, erosion of epistemic trust
Vc – cultural value	Symbolic, identity-forming significance	Targeted narrative attacks exploiting high-value or contested heritage	Manipulation of collective memory and cultural identity
Vf – functional value	Utility and visibility through access and reuse	Disinformation through high-visibility platforms or reuse channels	Amplified cognitive reach and societal impact
Persistent identifiers/ Co-references	Ensure continuity across systems and institutions	Identifier spoofing, resolution hijacking, reference poisoning	Fragmentation of authority and confusion over canonical sources

existential failures: (a) the temporary or permanent loss of access to DCAs, and (b) the dissemination of inauthentic, corrupted or manipulated DCAs. Within the C3E, reputation is not a secondary attribute but a *core systemic property*. The establishment of untrustworthy relationships – whether through compromise, impersonation or narrative attack – constitutes an existential threat, as it collapses public confidence in the ecosystem’s capacity to preserve and transmit cultural memory. This vulnerability is the primary objective of *Cyber-Cognitive Operations (CCO)*. Rather than focusing solely on technical disruption, CCOs strategically target the *cognitive and reputational dimensions* of agents responsible for DCAs. By introducing doubt about authenticity, neutrality or competence, attackers can generate cascading effects that destabilize trust across the broader cultural heritage domain, even in the absence of irreversible technical damage. Finally, the *Functions vector (Fs)* represents the set of operational responsibilities assigned to an agent and defines its contribution to the overall *C3E metabolism*. Functions encompass activities such as digitization, curation, preservation, validation, access provision and narrative mediation. From a cyber-cognitive perspective, these functions are also *points of cognitive control*, where meaning is interpreted, contextualized and legitimized. Consequently, attacks on agents frequently aim to compromise functions that shape interpretation and trust, rather than those that merely process data. [Table 3](#) reported the results of the exercise mapping of Agent Types and Attributes to Cyber-Cognitive Attack Vectors.

5.3 Functions as cognitive control units in the C3E

Within the Cultural Cyber-Critical Ecosystem (C3E), a *Function* is defined as a dynamic operational unit that enables the transformation, interpretation, validation and delivery of *Digital Cultural Assets (DCAs)* by the system’s Agents. Functions span the entire DCA life

Table 3. Mapping agent types and attributes to cyber–cognitive attack vectors

Agent type/attribute	Role in C3E	Typical cyber–cognitive attack vectors	Primary cognitive impact
Human agents (experts,	Interpretation, validation and mediation of meaning	Social engineering, phishing, credential coercion, narrative manipulation, expert impersonation	Undermined expert authority; manipulation of interpretation and scholarly consensus
Organizational agents (GLAM institutions)	Trusted intermediaries between DCAs and society	Reputation attacks, disinformation campaigns, institutional impersonation, selective data leaks	Erosion of institutional legitimacy and public trust
Institutional agents (archives, libraries, museums)	Custodians of authenticity and epistemic continuity	Delegitimization narratives, forged endorsements, provenance disputes	Systemic loss of confidence in heritage governance
Software agents (AI, LLMs, ETL pipelines)	Automated processing, enrichment and dissemination	Model poisoning, prompt manipulation, hallucination seeding, biased training data	Distorted interpretive outputs; amplification of false narratives
Attributes (At)	Identity, authority, accountability	Identity spoofing, credential forgery, role confusion	Breakdown of accountability; misattribution of authority
Reputation (rep)	Accumulated trust and credibility	Long-term trust erosion, coordinated doubt campaigns, reputational laundering	Persistent epistemic uncertainty; distrust even after recovery
Functions (Fs)	Execution of core heritage processes (e.g., curation, validation)	Function hijacking, workflow manipulation, selective omission	Loss of narrative coherence and interpretive reliability

cycle (Higgins, 2008), from digitization and curation to preservation, access and narrative mediation. In a cyber–cognitive context, these Functions do not merely process data: they *shape meaning, legitimacy and trust*, making them strategic targets for cognitive manipulation. Cyber–cognitive operations rarely require the direct takeover of systems. *Targeting functions that mediate meaning, validation and authority* allows adversaries to exploit normal operational variability and degrade trust while remaining within acceptable performance envelopes. Functions are activated by internal or external triggers and operate through execution logics that depend on resources, timing and control mechanisms. The complex, non-linear relationships among Functions can be modeled and their contribution in the ecosystem understood by using the *Functional Resonance Analysis Method (FRAM)* (Hollnagel and Woods, 2006), which captures how normal performance variability can resonate and produce unintended systemic outcomes – an effect actively exploited by cyber–cognitive operations. Formally, a C3E Function is defined by *M (Metadata)*, *Aspects (A)*, *Functional Metabolism and P (Properties)*. Functional Metadata (M) can be considered *Identity and Accountability Anchors*. It includes a unique identifier, ownership by a responsible Agent and formal specifications (e.g., OpenAPI). From a cyber–cognitive perspective, functional metadata is an *identity layer*: its manipulation – through false ownership, opaque specifications or undocumented changes – can obscure accountability and enable covert cognitive interference in heritage workflows. The *Aspects* define the

operational boundaries of a Function (Bellini and Degl’Innocenti, 2025). Inputs (I) and Outputs (O) often include *semantic and interpretive elements*, not only technical artifacts. Preconditions (Pr), Resources (R), Control (C) and Time (T) determine when and how meaning is processed and validated. Cyber–cognitive attacks frequently target these aspects by subtly altering inputs, delaying execution, disabling controls or exploiting timing windows, thereby influencing outputs without triggering overt failures. The *FM (Functional Metabolism)* models the stochastic dynamics through which a Function consumes inbound resources – time, expertise, computation, energy – to produce Outputs. The metabolism operates around a nominal operating state McM_cMc and collapses below a minimum threshold $MminM_{\{min\}}Mmin$. Variations in resource availability or processing effort directly affect output quality and credibility. The significance of FM as an analytical construct is that it bridges the gap between technical availability (a function is running) and cognitive quality (outputs are trustworthy): a function can maintain nominal technical availability while operating in stressed metabolism, producing outputs that erode cognitive integrity without triggering standard monitoring thresholds.

In cyber–cognitive operations, adversaries can *indirectly degrade outputs* by inducing resource strain, increasing cognitive load or enforcing efficiency pressures, in line with the *Efficiency–Thoroughness Trade-Off (ETTO)* principle (Hollnagel, 2009). Finally the *P (Properties)* characterize each Function’s resilience and systemic importance (Bellini and Marrone, 2020):

- *Buffer Capacity* governs the ability to absorb variability without distorting outputs;
- *Margin* indicates how close a Function operates to failure boundaries;
- *Tolerance* defines whether degradation is graceful or abrupt; and
- *Centrality* expresses functional criticality within the C3E network.

Functions with high centrality and low tolerance are especially attractive targets for cyber–cognitive operations, as modest perturbations can propagate across the ecosystem and undermine trust at scale. To better highlight the threats associated to the function’s component, in Table 4, a Cyber–Cognitive Attack Vectors has been mapped to its relevant Function’s component.

5.4 Resources as cognitive enablers and attack surfaces in the C3E

Within the C3E, *Resources (R)* comprise all assets that are used or consumed by a *Function (F)* to produce an *Output (O)*. As the lifeblood of the C3E’s metabolism, resources are inherently scarce and unevenly distributed, making their availability, quality and governance decisive for the ecosystem’s capacity to process, preserve and legitimize *Digital Cultural Assets (DCAs)*. From a cyber–cognitive perspective, resources are not neutral inputs. They shape *what can be processed, how thoroughly it can be interpreted and which narratives can be sustained over time*. Consequently, cyber–cognitive operations frequently target resources indirectly, exploiting scarcity, dependency or asymmetry to degrade trust and meaning without triggering overt technical failures. Resources within the C3E are categorized according to their *dependency structure*:

- *External Dependencies*: are supplied by infrastructures or agents outside the C3E’s immediate governance domain. These include, for example, *energy* (e.g., electrical power for data centers), *communication infrastructures* (e.g., network connectivity and bandwidth), cloud services and third-party platforms. Disruptions or manipulations at this level may not directly alter DCAs, yet they can impair availability, timeliness and continuity – conditions that cyber–cognitive operations exploit to cast doubt on institutional reliability.

Table 4. Mapping function’s components to cyber–cognitive attack vectors

Function components	Role in C3E	Typical cyber–cognitive attack vectors	Primary cognitive impact
Function metadata (M)	Identity, accountability, ownership	Misattributed ownership, undocumented changes, opaque APIs	Loss of accountability; reduced institutional credibility
Inputs (I)	Semantic and informational inputs	Injection of biased data, manipulated metadata, poisoned training sets	Distorted interpretation and validation outcomes
Outputs (O)	Validated DCAs, narratives, services	Selective omission, subtle alteration, misleading contextualization	Erosion of narrative integrity and trust
Control (C)	Verification, review, governance checks	Bypassing human-in-the-loop controls, disabling audits	Undetected manipulation; false legitimacy
Time (T)	Sequencing, timeliness	Induced delays, premature executions	Loss of contextual coherence; decision misalignment
Functional metabolism (FM)	Resource transformation into outputs	Resource exhaustion, cognitive overload, efficiency pressure	Quality degradation masked as routine performance
Buffer/margin/tolerance (P)	Resilience under stress	Targeting low-tolerance, high-centrality functions	Cascading trust failures across the ecosystem

- *Internal Dependencies*: represent the essential flows between the C3E’s own Functions. These include *computational resources* (storage, processing capacity), *human expertise*, organizational capacity and – crucially – *validated meaning*. Validated meaning is produced by interpretive or curatorial (catabolic) functions and consumed by downstream (anabolic) functions such as dissemination, education and reuse. *Validated Meaning* can be defined as the semantically interpreted, institutionally authorized and contextually situated understanding of a Digital Cultural Asset, produced by curatorial and interpretive Functions (e.g., cataloguing, scholarly annotation, provenance verification) and certified through documented review processes. It is operationalized as the aggregate of:
 - authoritative metadata and paradata that have passed institutional review;
 - contextual annotations linking the DCA to verified knowledge structures (controlled vocabularies, ontologies, knowledge graphs); and
 - explicit provenance chains traceable to responsible agents.
- Validated meaning is a consumable resource: it flows from upstream interpretive functions to downstream dissemination, educational and reuse functions. Its degradation indicators include broken or unresolvable persistent identifiers, undocumented changes to metadata, orphaned provenance chains and divergence between institutional records and externally circulating descriptions of the same DCA. As such, meaning itself becomes a *strategic resource*: its degradation, delay or selective suppression directly affects cognitive integrity across the ecosystem. *Cognitive Integrity* is defined as the systemic property of a C3E whereby Digital Cultural Assets and the Functions that process them collectively sustain reliable, consistent and trustworthy representations of cultural knowledge across the DCA

life cycle. It is conceptually distinct from technical (bit-level) integrity, which concerns data correctness, and from informational integrity, which concerns metadata accuracy. Cognitive integrity operates at the level of meaning: it is compromised when the ecosystem's outputs – whether artefacts, interpretations or narratives – deviate from authoritative, institutionally validated understandings in ways that are not detectable through conventional checksums or schema validation. Cognitive integrity is operationalized through four measurable indicators:

- (1) provenance consistency (the degree to which an asset's documented history agrees across all systems that reference it);
 - (2) interpretive coherence (the extent to which descriptions of the same DCA issued by different C3E agents are mutually consistent);
 - (3) trust signal stability (the absence of unexplained fluctuations in trust scores assigned to agents and DCAs); and
 - (4) validation coverage (the proportion of disseminated DCAs for which full validated meaning is available and current).
- A system exhibiting high cognitive integrity can sustain its epistemic authority under adversarial pressure; one with degraded cognitive integrity may appear operationally functional while silently transmitting corrupted cultural knowledge.

By acting on resources rather than on data or systems directly, cyber-cognitive operations can induce *functional underperformance*, *interpretive shortcuts* and *narrative distortion*, all while remaining within nominal operational thresholds. Resource stress therefore becomes a powerful vector for long-term trust erosion. In [Table 5](#), Resource Types have been connected with their relevant Cyber-Cognitive Attack Vectors.

Cyber-cognitive operations rarely need to falsify content directly. *Constraining or manipulating resources – especially time, expertise and validated meaning – can systematically bias interpretation and degrade trust*, while preserving the appearance of normal operation.

5.5 Hybrid infrastructure as a cyber-cognitive battlespace

The hybridization of infrastructures reflects the convergence of the *Human-Cyber-Physical World (HCPW)* that characterizes contemporary socio-technical systems. Within the Cultural Cyber-Critical Ecosystem (C3E), *Hybrid Infrastructures (HI)* embody this convergence by integrating physical, cyber and human-organizational layers into a single operational and cognitive environment. SSH European Research Infrastructures such as *DARIAH* exemplify this model (Bellini & Degl'Innocenti, 2024). Hybrid Infrastructures in the C3E integrate:

- a *physical layer* (data centers, servers, networks, sensing and communication devices);
- a *cyber layer* (digital platforms, computing continuum, HPC and cloud services, digital repositories); and
- a *human layer* (governance arrangements, operational practices, norms, epistemic communities).

From a cyber-cognitive perspective, these layers are not merely interdependent; they are *co-constitutive of trust and meaning*. Attacks on any layer can propagate across the others, enabling CCOs to exploit infrastructural dependencies to undermine confidence, legitimacy and continuity without requiring full system outages. In a cyber-cognitive context, Hybrid

Table 5. Mapping resource types to cyber–cognitive attack vectors

Resource type	Role in C3E	Typical cyber–cognitive attack vectors	Primary cognitive impact
Energy/power	Enables continuous operation of infrastructures	Induced outages, unstable supply, targeted disruptions	Perceived institutional fragility; loss of reliability
Communication infrastructure	Connectivity, access, dissemination	Bandwidth throttling, selective degradation, platform dependence	Delayed or fragmented access; erosion of user trust
Computational resources	Storage, processing, preservation workflows	Resource exhaustion, forced efficiency trade-offs	Quality degradation masked as routine constraints
Human expertise	Interpretation, validation, curation	Skill depletion, cognitive overload, discrediting experts	Weakening of epistemic authority and interpretive depth
Financial resources	Sustainability and resilience investment	Budgetary pressure, dependency on external sponsors	Strategic vulnerability; constrained defensive choices
Validated meaning	Input for downstream cultural functions	Narrative suppression, reinterpretation, selective validation	Distortion of collective understanding and memory
Time	Thoroughness and sequencing of processes	Forced acceleration, artificial urgency	Shallow validation; increased error and bias

Infrastructures are not attacked to *be destroyed*, but to *be discredited and to propagate uncertainty*. Exploiting their layered dependencies allows adversaries to degrade trust, continuity and cultural authority while preserving an appearance of operational normality. As highlighted by Li (2024), such infrastructures operate across data *at rest*, *in transit* and *in use*, supporting a) interdisciplinary research, b) developing flexible digital research environments, c) supporting academic communication and collaboration and d) ethical governance.

Building on this, Bellini and Degl’Innocenti (2024) identify a *new mission* to be added to the existing ones: sustaining the *entire life cycle of digital cultural heritage*. This expanded mission underpins the evolution of *DARIAH-IT* from a research-oriented infrastructure into a *Hybrid Infrastructure with Critical Infrastructure characteristics* within the cultural heritage domain. In this role, DARIAH-IT assumes responsibility for the long-term preservation, protection and accessibility of *Digital Cultural Assets (DCAs)* across open-ended temporal horizons. Its disruption would therefore represent not only a technical failure, but a *strategic threat to cultural continuity* at national and European levels – precisely the type of asymmetric effect sought by cyber–cognitive operations. Initiatives such as the *MetaFAIR Ecosystem* and FAIR-aware workflow orchestration in DARIAH-IT and H2IOSC extend FAIR principles toward *critical-infrastructure requirements*, improving traceability, transparency and interoperability (Degl’Innocenti and Spinelli, 2025; Degl’Innocenti and Spadi, 2025). AI-enabled components (e.g., NLP and HTR) modularized under the *MPAI AIM/AIF* paradigm enhance reproducibility, explainability and auditability (Chiariglione et al., 2025). Platforms such as *AEON* further support federated orchestration through standardized manifests and distributed identity control (Degl’Innocenti and Pinna, 2025). Together, these mechanisms reinforce *modularity, redundancy and trust*, countering cyber–cognitive attempts to exploit opacity and dependency. Overall, *DARIAH-IT* exemplifies a Hybrid Infrastructure within the C3E: a *cognitive-infrastructure backbone*

whose security, resilience and governance directly condition the trustworthiness and sustainability of digital cultural heritage. In this perspective, it is critical to identify and raise awareness on the critical attack vectors affecting each element of the Hybrid Infrastructure, as reported in Table 6.

5.6 Dependencies as cognitive propagation channels

In the C3E, *dependencies* determine how effects – technical and cognitive – *propagate* across the human–cyber–physical (HCPW) layers and the DCA life cycle. Under CCO, adversaries exploit these linkages to amplify doubt, disrupt meaning-making and erode trust with minimal technical action. These interdependencies can have different natures and different attack vectors as reported in Table 7. In particular:

- *Structural* – Physical/architectural linkages (e.g., co-located repositories, specific storage stacks). Single points of failure become *single points of narrative leverage*.
- *Functional* – FRAM-style inter-function reliance (Inputs/Outputs/Preconditions). Subtle perturbations in upstream validation functions can produce *downstream interpretive drift*.
- *Data* – Availability, integrity, interoperability of data and schemas. Silent changes to schemas or registries trigger *invisible misinterpretation*.
- *Semantic (DCA-specific)* – Meaning depends on vocabularies, ontologies, knowledge graphs. Attacks target *contextual anchors* to induce *semantic obsolescence* despite bit-level availability.
- *Temporal* – Sequence, cadence and windows of validity. CCO leverages *timing asymmetries* to force premature decisions or delay critical validation.
- *Resource* – Scarce compute, finance, expertise. Constraint tactics induce *efficiency-over-thoroughness* trade-offs that reduce cognitive rigor.

Table 6. Mapping hybrid infrastructure layers to cyber–cognitive attack vectors

Infrastructure layer	Role in C3E	Typical cyber–cognitive attack vectors	Primary cognitive impact
Physical layer	Material continuity and availability	Targeted outages, localized disruptions, kinetic or environmental threats	Perceived institutional fragility; doubts over continuity
Cyber layer	Processing, storage, dissemination	Supply-chain compromise, platform dependency, integrity degradation	Questioning authenticity and reliability of digital heritage
Human layer	Governance, expertise, legitimacy	Governance manipulation, insider coercion, trust-delegitimization narratives	Erosion of institutional authority and epistemic trust
Cross-layer dependencies	Coordination across HCPW	Exploiting weak interfaces, timing mismatches, responsibility gaps	Cascading socio-cognitive failures
Federated services	Interoperability and scalability	Federation poisoning, selective denial of cooperation	Fragmentation of cultural authority
AI-enabled components	Automation and interpretation	Model manipulation, biased enrichment, opaque outputs	Distorted semantic interpretation and meaning drift

Table 7. Mapping dependencies to cyber–cognitive attack vectors

Dependency type	Role in C3E	Typical CCO vectors	Primary cognitive impact
Structural	Physical/architectural continuity	Co-location exploitation, targeted outages	Perceived fragility; fear of loss
Functional	FRAM I/O chaining	Upstream validation nudging, silent workflow skips	Cascading interpretive drift
Data	Interoperability, registries	Schema/registry tampering, identifier poisoning	Ambiguous provenance; broken traceability
Semantic	Meaning preservation	Ontology/vocabulary biasing, KG perturbation	Context loss; semantic obsolescence
Temporal	Sequencing/cadence	Forced acceleration, blocking time-windows	Shallow review; misaligned decisions
Resource	Capacity for thoroughness	Induced scarcity, budgetary pressure	ETTO bias; reduced cognitive depth
Control/Governance	Legitimacy and assurance	Policy ambiguity, pseudo-compliance	Delegitimized oversight
Cognitive/Cyber-cognitive	Sense-making layer	Model poisoning, expert smear campaigns	Distorted interpretation
Trust/Reputation	Systemic confidence	Coordinated doubt and impersonation	Ecosystem-level distrust

- *Control and Governance* – Policies, accreditation, compliance. Manipulating rules/interfaces (or their public perception) undermines *legitimacy*.
- *Cognitive and Cyber-Cognitive* – Human expertise + AI mediation (HTR/NLP/enrichment). Poisoning or overloading these layers distorts *sense-making*.
- *Trust and Reputation* – Confidence in agents/services. CCO focuses on *trusted nodes* to catalyze *ecosystem-wide distrust*.

6. C3E trust and reputation under cyber–cognitive operations

At the level of the *Cultural Cyber-Critical Ecosystem (C3E)*, *trust* emerges as a *collective property*, reflecting the aggregated confidence that the ecosystem’s agents – human, organizational and technological – will jointly support the mission of cultural preservation, protection and accessibility. This form of trust is not reducible to isolated bilateral relations; rather, it arises from the *coherence and reliability of the ecosystem as a whole*, as perceived by internal and external stakeholders. Within the C3E, *reputation* plays a pivotal role as a form of *social and institutional memory*, accumulated over time through observable and auditable behaviors, peer evaluations and formal institutional assessments (Resnick *et al.*, 2000; Bellini *et al.*, 2025; Bottoni *et al.*, 2024). Reputation anchors expectations about competence, integrity and neutrality, and thus conditions both individual trust decisions and the overall credibility of the ecosystem. Under *Cyber–Cognitive Operations (CCO)*, reputation and trust become *primary targets rather than collateral effects*. CCOs aim not necessarily to disrupt services or destroy assets, but to *introduce doubt*, delegitimize authoritative actors and erode confidence in the authenticity and reliability of digital cultural heritage. In this context, the mere *perception* of compromised integrity – whether or not technically substantiated – can be sufficient to degrade trust at scale.

While *agent-level trust* within the C3E may remain asymmetric, partial and heterogeneous, *ecosystem-level trust* depends on the stability of reputations and on the integrity of critical dependencies. If reputations are systematically undermined, or if key institutional or functional dependencies fail or are perceived as unreliable, *systemic trust may collapse even when some bilateral trust relationships persist*. This asymmetry is central to the effectiveness of CCOs: localized or ambiguous attacks can propagate cognitively across the ecosystem, producing disproportionate societal effects. This dual-level perspective highlights that trust in the C3E is simultaneously:

- a *relational property between agents*, enabling cooperation and delegation under uncertainty; and
- a *systemic property*, sustaining the ecosystem's capacity to fulfill its mission despite risks, disruptions and behavioral variability.

From a cyber-cognitive standpoint, protecting trust therefore requires more than securing individual interactions. It demands the *preservation of reputational continuity, transparency of governance and verifiability of processes* across the entire ecosystem. In the C3E, trust is not merely assumed; it must be *continuously demonstrated*, defended and renewed in the face of adversarial efforts to blur authenticity, legitimacy and institutional authority. In Table 8, Trust Constructs are identified and mapped to their related Cyber-Cognitive Attack Vectors.

7. C3E resilience under cyber-cognitive operations

According to Bellini (2025), *resilience* is one of the tree foundational property that the Cultural Cyber-Critical Ecosystem (C3E) must exhibit. The concept of resilience, however, is inherently multifaceted and subject to diverse interpretations (Alhidaifi et al, 2024). It has been defined as a system's ability to maintain functionality under adverse conditions (Björck et al., 2015), as the persistence of dependability in the presence of change (Laprie, 2008), and, more broadly, as a characteristic of complex socio-technical systems encompassing technical, cognitive and social dimensions (Linkov and Kott, 2019). Alternative perspectives, such as antifragility (Jones, 2014; Taleb and Douady, 2013), emphasize learning, adaptation and strengthening through disruption rather than mere recovery. Recent integrative approaches seek to reconcile functionality-based and capacity-based views within unified models, such as the *Synergistic Dynamic Dual System (SDDS)* framework (Bellini and Marrone, 2020). Complementary studies further stress adaptive principles such

Table 8. Mapping trust constructs to cyber-cognitive attack vectors

Trust construct	Role	Typical CCO vectors	Primary cognitive impact
Ra(t) – reputation	Backward credibility	Smear campaigns, selective leaks	Retrospective doubt; credibility loss
T _{ij} (t) – bilateral trust	Forward reliance	Impersonation, deepfaked endorsements	Misplaced reliance; authority confusion
D(t) – dependency graph	System interdependence	Targeting hubs, interface opacity	Cascading distrust
Provenance/audit trails	Verifiability	Incomplete/forged logs; audit fatigue	Contestable authenticity
Transparency/Explainability	Interpretability	Opaque AI pipelines	Epistemic opacity; user alienation

as *bounce-forward* or *Building Back Better*, highlighting evolvability and continual recalibration toward a dynamic equilibrium rather than restoration of a fixed prior state (Flammini *et al.*, 2024). Within the C3E, resilience is understood as the *capacity of the ecosystem to preserve its identity* – as defined by its mission-critical functions – while adapting to adverse, uncertain or evolving conditions (Cumming and Collier, 2005; Roberts, 2015, Bellini and Degl’Innocenti, 2025). *Adaptation is therefore meaningful only insofar as it safeguards the original mission of the C3E*. A system that adapts at the cost of its mission or legitimacy cannot be considered resilient, even if it remains operational. Under *Cyber–Cognitive Operations (CCO)*, this definition must be extended beyond technical robustness. In such contexts, attacks do not primarily aim at disrupting availability or performance, but at *eroding authenticity, interpretability, institutional legitimacy and trust*. Consequently, resilience in the C3E must explicitly incorporate *cognitive resilience*: the ability to sustain reliable meaning-making, epistemic authority and public confidence despite sustained adversarial pressure, ambiguity and deniability.

To operationalize cognitive resilience under CCO, we align resilience strategies with the *anticipate–monitor–respond–learn (AMRL)* capacities cycle and with a set of structural design principles that explicitly counter cyber–cognitive attack vectors. In Table 9, the Resilience capacities have related to their Cyber–Cognitive Attack Vectors.

Together, these principles frame resilience in the C3E not as resistance to disruption alone, but as the *active preservation of identity, meaning and trust* in an adversarial cyber–cognitive environment

8. C3E sustainability under cyber–cognitive operations

Sustainability in the C3E is the ability to *preserve ecosystem identity and calibrate metabolism* without depleting resources or breaking the relationships that sustain meaning. Under CCO, sustainability hinges on *stable trust capital*, diversified revenue and capacity and governance that incentivizes *integrity over speed*.

Key levers:

- *Financial pluralism for cultural institutions* (mix of public funding, mission-aligned services) to avoid dependence that can be weaponized;
- *Human capital pipelines* (training, communities of practice) to cope with expertise erosion and technology changes;
- *Energy/compute efficiency* to buffer scarcity shocks; and

Table 9. Mapping resilience constructs to cyber–cognitive attack vectors

Capacities	Focus	Typical CCO pressure	Resilience countermeasure
Anticipate	Foresight and red-teaming	Novel narrative vectors; model poisoning	Scenario libraries; value-aware prioritization of DCAs
Monitor	Multi-layer telemetry	Low-signal, slow-burn manipulations	Provenance anomaly detection; trust KPIs
Respond	Coordinated action	Ambiguity and deniability	Pre-authorized playbooks; crisis comms with evidence packets
Learn	Post-event sense-making	Narrative capture post-incident	Blameless reviews; open reports; data set and model hardening; continuous improvement culture

- *Open, auditable processes* to convert transparency into *trust compounding* over time.

Each level is affected by a specific pressure generated by COO. These adversarial pressures have been identified in [Table 10](#).

9. Challenges: Advancing C3E under hybrid cyber–cognitive threats

The evolution of hybrid cyber–cognitive threats fundamentally challenges how digital cultural heritage is protected, governed and trusted. In this emerging threat landscape, adversaries do not primarily aim to destroy digital cultural assets, but to *manipulate perception, erode trust and destabilize collective memory*. Addressing these risks requires a decisive shift from purely technical cybersecurity toward *cognitive resilience* embedded within the Cultural Cyber–Critical Ecosystem (C3E).

C3E must confront the fragmentation of authenticity in an era of generative AI, deepfakes and subtle context manipulation. Future protection strategies must therefore institutionalize *provenance-by-design*, verifiable authenticity mechanisms and transparent curation processes that allow cultural institutions to demonstrate – not merely assert – the integrity and legitimacy of digital cultural assets. Authenticity must become continuously verifiable, not episodically assumed.

Trust emerges as the principal battleground. Cultural institutions function as epistemic intermediaries between society and cultural memory; hybrid attacks deliberately target their reputation, authority and perceived neutrality. Consequently, communication strategies must evolve from reactive crisis management to *pre-emptive trust reinforcement*, supported by measurable trust indicators, public transparency reports and evidence-based incident communication. Sustained public confidence cannot be improvised during crises; it must be cultivated beforehand.

The growing reliance on AI-enabled workflows introduces additional cyber–cognitive risks. While automation enhances scalability and access, opaque or unverified AI processes may amplify bias, hallucinations or manipulated interpretations. Future C3E implementations must therefore enforce *explainability, auditability and human-in-the-loop validation* as first-class requirements, ensuring that computational efficiency does not come at the expense of epistemic reliability.

Resilience planning within C3E must explicitly recognize that *time, expertise, attention and meaning* are strategic resources. Adversaries increasingly exploit resource constraints to

Table 10. Mapping sustainability levers to cyber–cognitive pressures

Sustainability lever	Adversarial pressure	Governance/design countermeasure	Long-term cognitive benefit
Funding diversification	Conditional sponsorship, boycott	Mission-aligned revenue mix; transparency	Independence; narrative resilience
Human capital	Burnout, brain-drain	Fellowships; rotation; mentorship	Stable interpretive quality
Compute/Energy	Cost shocks; rationing	Efficiency baselines; green SLAs	Consistent service and access
Open governance	Policy capture	Public deliberation; external audits	Legitimacy and societal trust
Open standards/FAIR	Proprietary lock-in	Standards conformance; exit plans	Interop for verification

force efficiency-driven shortcuts that progressively degrade quality and trust. Countering this dynamic requires institutional commitments to redundancy, diversity of formats and workflows, modularity and adaptive capacity, enabling graceful degradation without compromising identity or mission.

Hybrid threats also expose the critical role of *cross-sector collaboration*. Cultural heritage security can no longer be addressed in disciplinary silos. Effective cognitive resilience depends on sustained cooperation among heritage professionals, cybersecurity specialists, legal scholars and cognitive scientists. Such collaboration is essential to anticipate emerging attack patterns, interpret weak signals and integrate socio-technical insights into governance and operational design.

Finally, long-term sustainability must be reframed through a resilience lens. Financial fragility, organizational dependency and chronic skill erosion can themselves become vectors of cognitive vulnerability. C3E sustainability therefore requires diversified funding models, investment in human capital and governance structures that balance efficiency with long-term cultural responsibility.

In an era of persistent cognitive competition, safeguarding digital cultural heritage is no longer a matter of protecting data alone. It is a strategic effort to *defend the integrity of collective memory, the legitimacy of cultural institutions and the trust that binds societies to their past*. The future of C3E lies in its capacity to integrate technological robustness with cognitive, institutional and societal resilience – ensuring that digital heritage remains not only accessible, but meaningful and trustworthy across generations.

10. Conclusion

This paper has advanced the *Cultural Cyber-Critical Ecosystem (C3E)* as a comprehensive conceptual framework for understanding and protecting digital cultural heritage in an era of hybrid cyber–cognitive threats. By framing cultural heritage as a *mission-oriented, hybrid socio-technical ecosystem*, the C3E moves beyond traditional preservation-centric approaches and foregrounds *trust, resilience and sustainability* as foundational properties of cultural stewardship in the digital age. The analysis demonstrates that contemporary threats to digital cultural heritage do not primarily aim at data destruction or service disruption, but at the *cognitive dimensions of authenticity, legitimacy and institutional credibility*. Cyber–cognitive operations exploit dependencies, resource constraints, functional variability and reputational dynamics to erode confidence in cultural records and the institutions that curate them. In this context, cultural heritage infrastructures emerge as part of a broader *cognitive battlespace*, where safeguarding collective memory requires continuous demonstration of integrity rather than episodic technical assurance.

By decomposing the C3E into digital cultural assets, agents, functions, resources, hybrid infrastructures, dependencies, metabolism, trust, resilience and sustainability, the paper provides a *systematic vocabulary and analytical structure* for identifying vulnerabilities and designing counter-measures. Positioned within this framework, *Cyber Humanities* emerges as an transdisciplinary field concerned with the interaction between cultural meaning, cyber infrastructures and cognitive security. It provides the intellectual space in which digital humanities, cybersecurity, resilience engineering and cognitive sciences converge to address the strategic risks facing cultural memory in networked societies.

Ultimately, safeguarding digital cultural heritage is no longer only a technical or curatorial challenge. It is a *societal responsibility* that involves defending the integrity of collective memory, the legitimacy of cultural institutions and the trust that sustains democratic knowledge ecosystems. By articulating the C3E, this paper offers a foundational

step toward ensuring that digital cultural heritage remains *authentic, intelligible, resilient and trustworthy across generations*.

Acknowledgements

During the preparation of this work, the authors used Claude Sonnet 4.6 in order to improve readability and language. After using this tool, the author(s) reviewed and edited the content as needed and take full responsibility for the content of the publication.

References

- Adorni, G. and Bellini, E. (2025), "Towards a manifesto for cyber humanities: Paradigms, ethics, and prospects", *2025 IEEE International Conference on Cyber Humanities (IEEE-CH), Florence, Italy*, pp. 1-8, doi: [10.1109/IEEE-CH65308.2025.11279659](https://doi.org/10.1109/IEEE-CH65308.2025.11279659).
- Adorni, G., Bellini, E. and Torre, I. (2026), "Reclaiming agency through cyber humanism: a European agenda for AI, education and culture", In: Hagedorn, L., Schmid, U., Winter, S., Woltran, S. (eds) *Digital Humanism. DIGHUM 2025. Lecture Notes in Computer Science*, vol 16319 Springer, Cham, doi: [10.1007/978-3-032-11108-1_31](https://doi.org/10.1007/978-3-032-11108-1_31).
- Alhidaifi, S.M., Asghar, M.R. and Ansari, I.S. (2024), "A survey on cyber resilience: Key strategies, research challenges, and future directions", *ACM Computing Surveys*, Vol. 56 No. 8, pp. 48, doi: [10.1145/3649218](https://doi.org/10.1145/3649218). 196 (August 2024)
- Baxter, G. and Sommerville, I. (2011), "Socio-technical systems: from design methods to systems engineering", *Interacting with Computers*, Vol. 23 No. 1, pp. 4-17, doi: [10.1016/j.intcom.2010.07.003](https://doi.org/10.1016/j.intcom.2010.07.003).
- Bellini, E. and Marrone, S. (2020), "Towards a novel conceptualization of cyber resilience", *2020 IEEE World Congress on Services (SERVICES), Beijing, China*, pp. 189-196, doi: [10.1109/SERVICES48979.2020.00048](https://doi.org/10.1109/SERVICES48979.2020.00048).
- Bellini, E. (2025), "Cyber humanities for heritage security", *Communications of the Acm*, Vol. 68 No. 12, pp. 112-117, doi: [10.1145/3735659](https://doi.org/10.1145/3735659).
- Bellini, E. and Degl'Innocenti, E. (2025), "Building the foundations of cyber humanities: Cultural Cyber-Critical ecosystem conceptualization", *2025 IEEE International Conference on Cyber Humanities (IEEE-CH), Florence, Italy*, pp. 1-8, doi: [10.1109/IEEE-CH65308.2025.11279317](https://doi.org/10.1109/IEEE-CH65308.2025.11279317).
- Bellini, E. and Degl'Innocenti, E. (2024), "Transitioning SSH European research infrastructures to critical infrastructure through resilience", *2024 IEEE International Conference on Cyber Security and Resilience (CSR), London, United Kingdom*, pp. 801-806, doi: [10.1109/CSR61664.2024.10679383](https://doi.org/10.1109/CSR61664.2024.10679383).
- Bellini, E., Luddi, C., Cirinnà, C., Lunghi, M., Felicetti, A., Bazzanella, B. and Bouquet, P. (2012), "Interoperability knowledge base for persistent identifiers interoperability framework", *2012 Eighth International Conference on Signal Image Technology and Internet Based Systems, Sorrento, Italy*, pp. 868-875, doi: [10.1109/SITIS.2012.130](https://doi.org/10.1109/SITIS.2012.130).
- Björck, F., Henkel, M., Stirma, J. and Zdravkovic, J. (2015), "Cyber resilience – fundamentals for a definition", In: Rocha, A., Correia, A., Costanzo, S., Reis, L. (eds) *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*, vol 353 Springer, Cham, doi: [10.1007/978-3-319-16486-1_31](https://doi.org/10.1007/978-3-319-16486-1_31).
- Blatny, J. (2025), "NATO chief scientist research report on cognitive warfare", NATO, available at: <https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitive-warfare-4.pdf>
- Boston, G. (1988), "Safeguarding the documentary heritage. a guide to standards, recommended practices and reference literature related to the preservation of documents of all kinds", Document code: CIL98/WS/4 UNESCO, available at: <https://unesdoc.unesco.org/ark:/48223/pf0000112676>

- Bottoni, M., Bellini, E. and Farinetti, E. (2024), "Towards a Reputational-Based trustworthy archaeological information system", *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, London, United Kingdom, pp. 795-800, doi: [10.1109/CSR61664.2024.10679376](https://doi.org/10.1109/CSR61664.2024.10679376).
- Chiariglione, L., Bellini, E., Degl'Innocenti, E., Mambrini, F., Pinna, F., Ribeca, P., Santucci, R., Spadi, A. and Spinelli, F. (2025), "Modular AI for the digital humanities: Applications of MPAI standards to DH research workflows", *2025 IEEE International Conference on Cyber Humanities (IEEE-CH)*, Florence, Italy, pp. 1-7, doi: [10.1109/IEEE-CH65308.2025.11279302](https://doi.org/10.1109/IEEE-CH65308.2025.11279302).
- Cumming, G.S. and Collier, J. (2005), "Change and identity in complex systems", *Ecology and Society*, Vol. 10 No. 1.
- Degl'Innocenti, E. and Pinna, F. (2025), "AEON: an innovative platform for workflow orchestration and service integration in digital humanities", *2025 IEEE International Conference on Cyber Humanities (IEEE-CH)*, Florence, Italy, pp. 1-7, doi: [10.1109/IEEE-CH65308.2025.11279606](https://doi.org/10.1109/IEEE-CH65308.2025.11279606).
- Degl'Innocenti, E. and Spadi, A. (2025), "How to structure a SSH dataset for FAIR and computational reuse", *2025 IEEE International Conference on Cyber Humanities (IEEE-CH)*, Florence, Italy, pp. 1-6, doi: [10.1109/IEEE-CH65308.2025.11279300](https://doi.org/10.1109/IEEE-CH65308.2025.11279300).
- Degl'Innocenti, E. and Spinelli, F. (2025), "Building a fair workflow in the social sciences and humanities research: the metafair ecosystem", in *2025 IEEE International Conference on Cyber Humanities*, p. in print, 2025.
- Emery, F.E. and Trist, E.L. (1960), "Socio-Technical systems", In Churchman, C. W., and Verhulst M. (Eds.), *Management Sciences: Models and Techniques*, Oxford Academic, Vol. 2, pp. 83-97.
- Flammini, F., Alcaraz, C., Bellini, E., Marrone, S., Lopez, J. and Bondavalli, A. (2024), "Towards trustworthy autonomous systems: Taxonomies and future perspectives", *Ieee Transactions on Emerging Topics in Computing*, Vol. 12 No. 2, pp. 601-614, doi: [10.1109/TETC.2022.3227113](https://doi.org/10.1109/TETC.2022.3227113). April-June.
- Floridi, L. (2014), *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press.
- Higgins, S. (2008), "The dcc curation lifecycle model", *International Journal of Digital Curation*, Vol. 3 No. 1.
- Hollnagel, E. and Woods, D. (2006), "Epilogue: Resilience engineering precepts", in *Resilience Engineering – Concepts and Precepts*, (Hollnagel N. L. E., Woods D.D., ed.). Ashgate Publishing, Ltd, pp. 347-358.
- Hollnagel, E. (2009), "The ETTO principle: Efficiency-Thoroughness Trade-Off", *Why Things That Go Right Sometimes Go Wrong*, Taylor and Frensis.
- Jones, K.H. (2014), "Engineering antifragile systems: a change in design philosophy", *Procedia Computer Science*, Vol. 32, pp. 870-875.2014. The 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), the 4th International Conference on Sustainable Energy Information Technology (SEIT-2014).
- Kling, R. (1980), "Social analyses of computing: Theoretical perspectives in recent empirical research", *ACM Computing Surveys*, Vol. 12 No. 1, pp. 61-110, doi: [10.1145/356802.356806](https://doi.org/10.1145/356802.356806).
- Laprie, J.-C. (2008), "From dependability to resilience", in *38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, IEEE*.
- Linkov, I. and Kott, A. (2019), *Fundamental Concepts of Cyber Resilience: Introduction and Overview*, Springer International Publishing, Cham, pp. 1-25.
- Luhmann, N. (1979), "Trust: a mechanism for the reduction of social complexity", " in *Trust and Power*, (Luhmann N., ed.). Wiley, pp. 4-103.
- Moore, R. (2008), "Towards a theory of digital preservation", *International Journal of Digital Curation*, Vol. 3 No. 1, doi: [10.2218/ijdc.v3i1.42](https://doi.org/10.2218/ijdc.v3i1.42).

- Musiani, F. and Schafer, V. (2016), "Digital heritage and heritagization", *REST*, Vol. 6, pp. 2016, doi: [10.3917/tdm.018.0170](https://doi.org/10.3917/tdm.018.0170).
- Paskin, N. (2006), "Digital object identifiers for scientific data", *Data Science Journal*, Vol. 4, pp. 12-20, doi: [10.2481/dsj.4.12](https://doi.org/10.2481/dsj.4.12). Volume Page DOI.
- Resnick, P., Kuwabara, K., Zeckhauser, R. and Friedman, E. (2000), "Reputation systems", *Communications of the Acm*, Vol. 43 No. 12, pp. 45-48, doi: [10.1145/355112.355122](https://doi.org/10.1145/355112.355122).
- Riva, P., Le Boeuf, P. and Žumer, M. (2017), "IFLA library reference model. A conceptual model for bibliographic information", tech. rep., IFLA, available at: <https://repository.ifla.org/handle/20.500.14598/40>
- Roberts, T. (2015), "Quantum resilience: a generalized theory", Doctoral dissertation, School of Sustainable Engineering DOI: [10.13140/RG.2.2.31172.48000](https://doi.org/10.13140/RG.2.2.31172.48000)
- Rusbridge, C., Burnhill, P., Ross, S., Buneman, P., Giarretta, D., Lyon, L. and Atkinson, M. (2005), "The digital curation Centre: a vision for digital curation", *2005 IEEE International Symposium on Mass Storage Systems and Technology, Sardinia, Italy*, pp. 31-41, doi: [10.1109/LGDI.2005.1612461](https://doi.org/10.1109/LGDI.2005.1612461).
- Taleb, N.N. and Douady, R. (2013), "Mathematical definition, mapping, and detection of (anti) fragility", *Quantitative Finance*, Vol. 13 No. 11, pp. 1677-1689.
- Wiggins, D. (1967), "*Identity and Spatio-Temporal Continuity*", Oxford University Press, Oxford.
- Wilkinson, M.D., Dumontier, M., Aalbersberg, I.J., Appleton, G., Axton, M., Baak, A., ... Mons, B. (2016), "The FAIR guiding principles for scientific data management and stewardship", *Scientific Data*, Vol. 3 No. 1, p. 160018, doi: [10.1038/sdata.2016.18](https://doi.org/10.1038/sdata.2016.18).
- Woods, D. (2006), "Essential characteristics of resilience", in Hollnagel, E., Woods, D.D., and Leveson, N. (Eds.). *Resilience Engineering: Concepts and Precepts*, (1st ed.) CRC Press, pp. 21-34. doi: [10.1201/9781315605685](https://doi.org/10.1201/9781315605685).

Further reading

- Bellini, E. (2019), "A blockchain based trusted persistent identifier system for big data in science", *Foundations of Computing and Decision Sciences*, Vol. 44 No. 4, p. 2019.
- Bellini, E., Damiani, E., Di Giovanni, M. and Marrone, S. (2026), "Performance-Security analysis in O2O interactions in future 6G communications", *Distributed Ledger Technologies: Research and Practice*, Vol. 5 No. 3, p. 35, doi: [10.1145/3716176](https://doi.org/10.1145/3716176).
- Bellini, E., Bergamin, G., Messina, M., Cirinna', C. and Messuti, R. (2014), "NBN: It the Italian trusted persistent identifier infrastructure", *International Journal of Knowledge and Learning*, Vol. 9 No. 4.
- Bellini, E., Ceravolo, P. and Nesi, P. (2017), "Quantify resilience enhancement of UTS through exploiting connected community and internet of everything emerging technologies", *ACM Transactions on Internet Technology*, Vol. 18 No. 1, p. 34, doi: [10.1145/3137572](https://doi.org/10.1145/3137572).
- BL (2024), "British library: Learning lessons from the cyber-attack", available at: www.bl.uk/stories/blogs/posts/learning-lessons-from-the-cyber-attack
- CCSDS (2012), *Reference Model for an Open Archival Information System (OAIS). Recommended Practice, CCSDS 650.0-M-2*, Consultative Committee for Space Data Systems. [ISO 14721:2012]. Washington, DC, D.C.
- Conti, M., Das, S.K., Bisdikian, C., Kumar, M., Ni, L.M., Passarella, A., Roussos, G., Tröster, G., Tsudik, G. and Zambonelli, F. (2012), "Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber-physical convergence", *Pervasive and Mobile Computing*, Vol. 8 No. 1, pp. 2-21, doi: [10.1016/j.pmcj.2011.10.001](https://doi.org/10.1016/j.pmcj.2011.10.001).
- Deloitte (2022), "The value of an iconic asset", available at: www.deloitte.com/it/it/services/consulting-financial/events/the-value-of-an-iconic-asset—deloitte-italy-eventi.html

- European Union (2022), “Directive (EU) 2022/2555 of the European parliament and of the council on measures for a high common level of cybersecurity across the union (NIS2 directive)”, *Official Journal of the European Union*, Vol. 333, pp. 80-152.
- Huvila, I. (2022), “Improving the usefulness of research data with better paradata”, *Open Information Science*, Vol. 6 No. 1, pp. 28-48.
- Li, Y. (2024), “New roles of research data infrastructure in research paradigm evolution”, *Journal of Data and Information Science*, Vol. 9 No. 2, pp. 104-119.
- NIST (2024), *The NIST Cybersecurity Framework (CSF) 2.0*, National Institute of Standards and Technology. doi: [10.6028/NIST.CSWP.29](https://doi.org/10.6028/NIST.CSWP.29).
- Varela, F. (1979), Vol. 2 “Principles of biological anatomy,” in *di The North Holland series in general systems research*. (Holland N., ed.). Studies in Integer Programming.
- Yager, R. (1987), “Cardinality of fuzzy sets via bags”, *Mathematical Modelling*, Vol. 9 No. 6, pp. 441-446.

Corresponding author

Emanuele Bellini can be contacted at: emanuele.bellini@uniroma3.it