From Threats to Sovereignty:

Managing Digital Risks and Preservation at the Bibliothèque nationale de France

Yannick Grandcolas

Digital Preservation Expert @ BnF

Director @ Open Preservation Foundation

The views and opinions expressed in this presentation are those of the author and do not necessarily reflect the official policy or position of the Bibliothèque nationale de France (BnF)

«Digital information lasts forever – or five years, whichever comes first.. »
Jeff Rothenberg

YG 2025

BnF | Bibliothèque nationale de France

From Threats to Sovereignty: Managing Digital Risks and Preservation at the Bibliothèque nationale de France

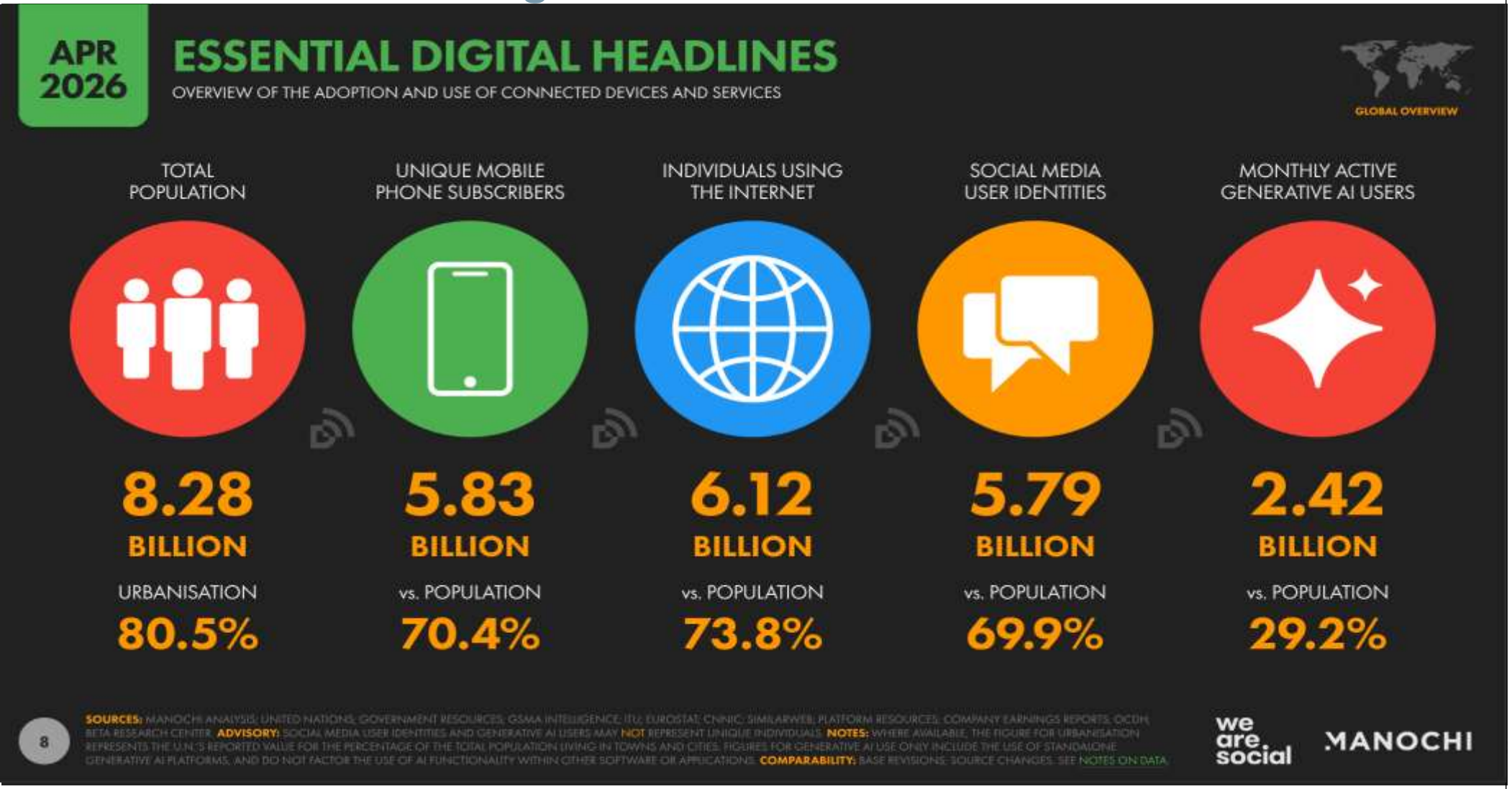
I. Context, definition and challenges

II. Security & Risk Assessment

III. Ensure Access To Preserved Digital Objects

BnF | Bibliothèque nationale de France

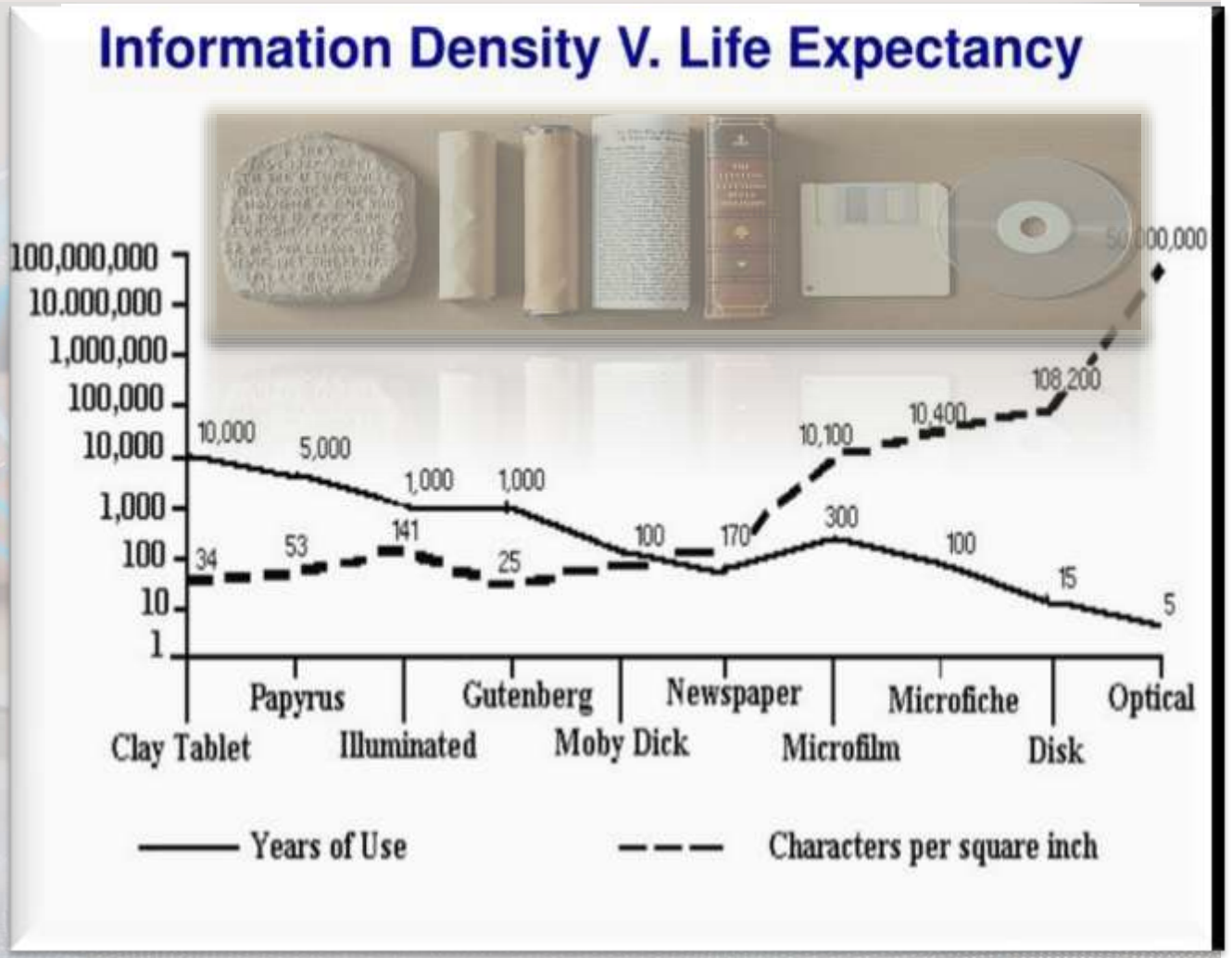
Context : The Global Digital Environment



Preservation in the Digital World [P.Conway, Yale U. 1996]

Sustainability at any cost?

- ✓ It is better to monitor the condition of media and replace them regularly or when too many errors are detected.
- ✓ A mix of media is recommended (but not heterogeneity!).



BnF Bibliothèque nationale de France

Context : Sovereignty

Digital Information, a paradigm shift: Sovereignty & Dependencies

II. Security & Risk Assessment

BnF Bibliothèque nationale de France

Risks Identification (BnF)

A list of existing risks and their assessment and impact.
A reference of the 72 risks identified to prioritise actions.

- ✓ Environmental risks:
- ✓ Security risks
- ✓ Organisational risks
- ✓ Technological risks
- ✓ Technical and semantic accessibility risks
- ✓ Risk management provides an overview of the preservation actions carried out on all digital objects

Identifying risks is an essential part of running any organisation.
It is important to understand the potential risks involved in order to make informed decisions and protect your digital archives.

BnF Bibliothèque nationale de France

Digital Roadmap

of the National Library of France

"The strength of the BnF lies in its harmony between knowledge and lightness of touch, that makes knowledge accessible to all!"

Laurence Engel, President of the National Library of France (BnF), April 2nd 2020

This quite unusual map was made possible through collective thinking about digital technologies and uses at the National Library of France. It follows two previous editions of the institution's Digital roadmap, which also aimed to visualise the strategic areas, the patterns, the distances, and the paths within the digital landscape of the Library and of its whole ecosystem.
This time, metaphor is used to bring humanity and poetry, to enable a common understanding of a complex subject and to promote the Library's vision for the future. This document, drawing its inspiration from the Library's collections of maps and plans which it will in its turn enrich, is a chance for you, Library staff, professionals from other organizations, partners, contractors, for all of you wherever you come from, to experience and truly explore its landscape.

The "digital world" which is thus unveiled in autumn 2020 is being released during an era – the global health crisis – that, in many respects, has upset the way we use and manage digital technologies. Adapting virtual content for different types of audience is more essential than ever, just like providing user-oriented and customized public services or remote working. Moreover, the digital divide has never been so relevant. The Digital roadmap takes into account these challenges within a renewed perspective, but it also suggests how valuable it can be for an institution to maintain a permanent, transversal and long-lasting critical reflection, enabling it to enrich its strategy and vision, and, above all, to face the most uncommon and unexpected situations. In this way, the digital working environment – of the staff as well as of the users – was identified long before March 2020 as a key field for changes to be initiated. This map is grounded on a strong base – including regions and geographic features, that echo the Library's missions. Since the Library's collective thinking about digital technologies and uses is bound to go on and because what we have learned from the health crisis will become clearer, it has also been designed to evolve over future editions. If you look closely, you will see the cartographers at work.

(BnF Bibliothèque nationale de France

NOVEMBER 2020

Legend

(BnF | Bibliothèque nationale de France

MAIN TYPES OF CYBERATTACKS

Malware (Malicious Software)

- Programs designed to :
  - Damage or infiltrate computer systems
  - Including viruses, worms, Trojan horses, ransomware, and spyware.

Denial of Service Attacks (DDoS)

- Attacks aimed at making an online service unavailable by overwhelming it with traffic from multiple sources.

Phishing

Fraudulent communications

- Often via email, that appear to come from trusted sources
- To trick victims into revealing sensitive information like passwords, credit card details...

SQL Injection Attacks

- **Attacks targeting databases by injecting malicious code into SQL queries to access, modify, or delete data.**

Zero-Day & Obsolescence Attacks

Attacks exploiting unknown software vulnerabilities for which no patch is yet available.

Man-in-the-Middle (MitM) & Internal Attacks

- **Attacks where the attacker intercepts and possibly alters communications between two parties without their knowledge.**

How can you manage your cyber security (1/2)

and what steps should you take to keep yourself safe online?

1 Inventory of digital assets and the people responsible for them.

2 The criticality of each system in the event of a cyber attack must be assessed.

3 Technical, organizational and contractual security measures.

4 Prioritisation of actions (Criticality/Cost/Effectiveness ratio).

5 Appointment of an internal consultant and choice of a specialist service provider.

6 Best cyber security practices and responses to cyber attacks.

7 Prepare for the worst, because you never know what might happen.

8 All must comply with the rules and decisions, and regular progress reviews must be carried out.

9 Verification of measures taken and technical and organisational audits.

10 Reapply the method. Do this for all new systems. Also do it every 2 to 3 years.

www.cybermalveillance.gouv.fr

How can you manage your cyber security (2/2)

and what steps should you take to keep yourself safe online?

Synthetic cybersecurity management methodology

1 TAKE STOCK OF THE SITUATION

The first step is to draw up the most exhaustive inventory possible of all your digital assets (internal networks, websites, messaging systems, social networks, outsourced applications and services, etc.) and those responsible for them (internal or external IT support).This should include all your digital assets, such as internal networks, websites, messaging systems, social networks, outsourced applications and services, and so on, as well as those responsible for them, whether internal or external IT support.

2 BE AWARE OF THE RISKS

For each system identified, assess how critical it would be to the functioning of your organisation if it were to be compromised or destroyed, or if the data it contains were to be stolen by cybercriminals.

3 EVALUATE YOUR LEVEL OF PROTECTION

Ask your internal and/or external IT support team about the appropriateness of the technical, organisational and contractual security measures applied in relation to the issues at stake, such as password policies, back-ups, updates and external access filtering. About whether the technical, organisational and contractual security measures applied are appropriate in relation to the issues at stake. These measures include password policies, back-ups, updates and external access filtering.

4 DEFINE AN ACTION PLAN

Eighty per cent of cyber-attacks could be avoided by implementing simple, low-cost measures such as good password management and regular backups., security updates, and access rights. Prioritise the actions to be taken according to their criticality/Cost-effectiveness ratio.

5 GET SUPPORT

If no one has been assigned to this role, appoint someone, a person to help you manage your organisation's cyber security plan. To assess the level of protection on your critical systems, call in a cyber security service provider.

6 RAISE THE STAFF'S AWARENESS

Your colleagues are an essential link in your cyber security chain. They play a vital role in both applying good cyber security practices and detecting and reacting to attempted cyber attacks.

7 PREPARE FOR THE WORST

There is no such thing as absolute cyber security; a successful cyber attack is always a possibility. Cyber attack is, unfortunately, always possible. We therefore need to prepare contingency plans for dealing with a crisis, including a crisis directory, downgraded operations and communication plans. We should also carry out exercises to assess their effectiveness.

8 GET INVOLVED

To ensure the success of the cybersecurity action plan, in order to implement it effectively, you, as a manager, need to get involved by providing regular status updates and progress reviews at your level. You must also lead by example and ensure that your managers and staff do not deviate from or circumvent the security measures put in place to protect the organisation.

9 REGULAR CHECKS

It is important to check that the decisions taken have been implemented. For the most critical systems, a technical and organisational audit may be necessary: it is advisable to call on a service provider specialising in cybersecurity.

10 REAPPLY

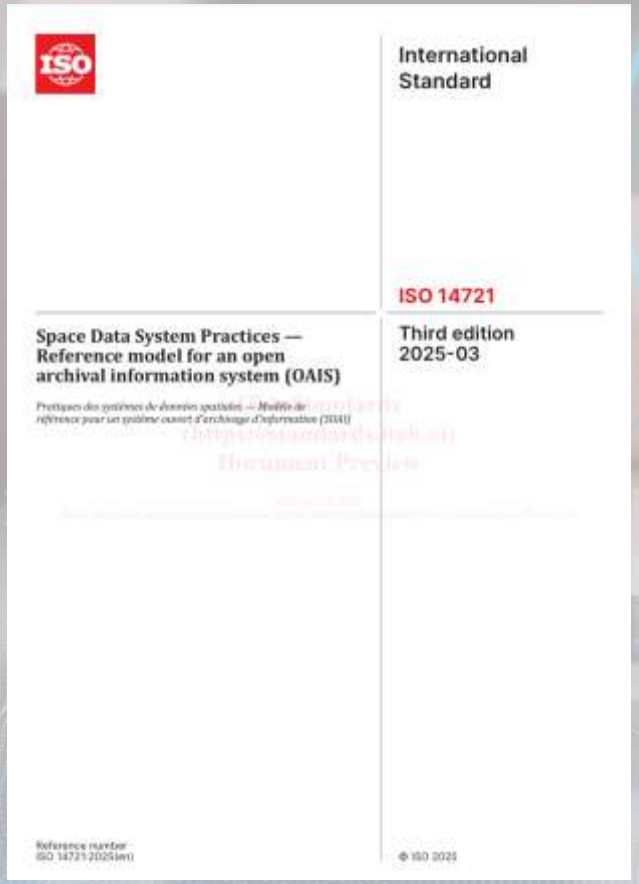
Digital services offered by organisations are constantly evolving, as are the ways in which they can be attacked. To take account of this, it is recommended that this method is 'reapplied' to all new digital services before implementation and every two to three years thereafter.

BnF Bibliothèque nationale de France

III. *Protect & Ensure Access to Preserved Digital Objects*

BnF | Bibliothèque nationale de France

A base: OAIS model & Security
Open Archival Information System


ISO

International Standard

ISO 14721

Space Data System Practices — Reference model for an open archival information system (OAIS)

Third edition
2025-03

- Reference model for an Open Information Archiving System
  Standard ISO 14721: 2025
- Issued by CCSDS (Consultative Committee for Space Data Systems)
- Conceptual model for perpetuating documents and data, particularly digital data
- A comprehensive, abstract overview of digital sustainability
  - Defines a set of concepts and functions
  - Provides a common terminology
  - Independent of any particular application and context
  - Applicable to the world of printed documents
  - Periodically revised (3rd version in 2025).

Open Preservation Foundation

Open software and standards are key to long-term digital access. The OPF provides expertise and support, empowering the digital preservation community to develop sustainable resources.

Tools

Explore our open source digital preservation toolset, our member-led development approach, and what's coming up in our next releases.

JHOVE

The file format identification, validation, and characterisation tool

veraPDF

The industry supported PDF/A validator

fido

Our file format identification tool

jpylyzer

JPEG2000 JP2 image validator

Our Github Repository

ViPER

A virtual machine with open source preservation software

Arlington PDF Model checker

Fixity Pro

CloudVIPER

ODF

Essential Strategies

Preservation means anticipating and therefore planning operations to ensure that access to digital information is maintained over the long term, and in particular to manage technological obsolescence.

- Transformation (or migration)
- Emulation

Key Strategies and Next Steps

France to ditch US platforms Microsoft Teams, Zoom for 'sovereign platform' citing security concerns

https://www.euronews.com/next/2026/01/27/france-to-ditch-us-platforms-microsoft-teams-zoom-for-sovereign-platform-amid-security-con

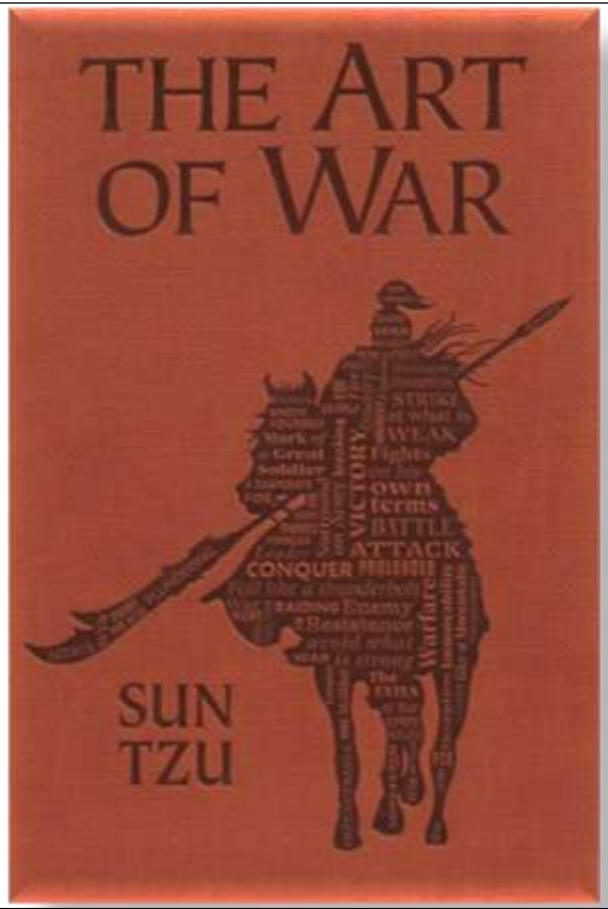
Updated 28/01/2026

Key Strategies, What's Next?

BnF Bibliothèque nationale de France

The Art of Digital Preservation is also the Art of War

and this is something that should be considered by anyone involved in the field.



THE ART OF WAR

By Sun Tzu
Translated with introduction and notes by
Lionel Giles, M.A.

19th May 2004

Contents

https://en.wikipedia.org/wiki/The_Art_of_War

BnF Bibliothèque nationale de France

Questions ?

Yannick Grandcolas
Digital Preservation Expert BnF
Director @ Open Preservation Foundation

YG 2025

BnF | Bibliothèque nationale de France