

Boris Kantsepolsky & Lev Topor

MANAGING INFORMATION SINGULARITY

AI, Quantum Technologies, and the
Future of Information Systems



Managing Information Singularity

Boris Kantsepolsky • Lev Topor

Managing Information Singularity

AI, Quantum Technologies, and the
Future of Information Systems

palgrave
macmillan

Boris Kantsepolsky
The Academic College of Tel Aviv-Yaffo
Tel Aviv-Yaffo, Israel

Lev Topor
Institute for the Study of Global Antisemitism
and Policy (ISGAP)
Cambridge, UK

ISBN 978-3-032-26222-6 ISBN 978-3-032-26223-3 (eBook)
<https://doi.org/10.1007/978-3-032-26223-3>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2026

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Cover image: BlackJack3D | Getty Images

This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

If disposing of this product, please recycle the paper.

This book is dedicated to our families, whose love, unwavering support, and encouragement sustained us throughout this journey.

Boris Kantsepolsky

Lev Topor

Foreword

There are moments when a field must admit that its familiar vocabulary is no longer enough. Information Systems is at such a moment now, not because we lack theories or methods, but because the object of our study is mutating. Systems that once stored, processed, and reported information are rapidly evolving to systems that infer, recommend, persuade, and decide. They do not simply support information processing and flow through an organization; they shape what counts as information in the first place.

This is the intellectual wager of *Managing Information Singularity: AI, Quantum Technologies and the Future of Information Systems*. The authors argue that we are approaching a threshold where the defining challenge is no longer “digital transformation” in the managerial sense, but epistemic transformation: who produces knowledge, how it is validated, how it flows, and how it is contested. In practical terms, this is already visible. Generative models draft reports and essays (in fact, this very foreword was co-authored with such a model), write code, summarize intelligence, generate synthetic media, and provide decision support at speed and scale. Recommender systems curate attention and, with it, public discourse. Automated agents execute tasks across workflows. The informational environment becomes less like a database and more like a continuously updated hypothesis about the world—useful, powerful, and sometimes dangerously wrong.

What makes this book particularly timely is its multidimensional analysis; rather than treating artificial intelligence (AI) as a standalone topic and quantum information science as a separate scientific and technological

advancement, the authors place both within the core of IS: the design, governance, and consequences of socio-technical systems that mediate work, markets, and institutions. AI changes the *logic* of information systems as it blurs the lines between data and interpretation, and between reporting and reasoning, between assistance and delegation. Quantum technologies change the *assumptions* underlying information systems, as they enable us to reimagine security, trust, and computational advantage. Along with the strategic asymmetries that will emerge as quantum capabilities will become unevenly distributed across states and firms, together, AI and quantum information systems (QIS) will manage both the production and the trustworthiness of knowledge.

Readers will find that the authors do not romanticize this shift. They acknowledge what many of us have observed in our own research and practice: that the benefits of advanced systems are inseparable from new forms of fragility. When systems generate outputs that appear authoritative, using confident language, plausible citations, and compelling imagery, the burden of validation shifts from the system to the user and the institution. This shift can take place in a gradual and unnoticeable manner, rendering the users unaware of their new responsibility. Furthermore, when automation accelerates action, it also accelerates error. When decision support becomes decision shaping, accountability becomes harder to locate, especially across supply chains of models, platforms, data brokers, and outsourced analytics. And when information becomes abundant, the scarce resource is no longer access, it is trust.

It is precisely here that the book makes a contribution beyond technical forecasting. It treats governance as part of system design rather than an afterthought. Regulation, standards, auditing, procurement rules, professional norms, and institutional ethics are not external constraints imposed upon technology; they are components of the socio-technical architecture that determine the extent of both the public value and the potential harm they introduce. In the coming years, organizations will be expected to justify not only what their systems do, but how they were trained, what data they relied upon, what risks were assessed, what safeguards were implemented, and how failures will be detected and corrected. The future of Information Systems will be shaped as much by ethics and accountability as by performance.

As a discipline, Information Systems has lived through waves of technological change that promised rupture from mainframes and time-sharing, personal computing, enterprise integration, to the web, platforms, cloud, and mobile. Each wave altered organizational life, but it also forced Information Systems scholars to clarify what we study and why it matters. This book continues in these lines; beyond discussing new tools and technologies, it asks

what kinds of systems we are building, what kinds of organizations these systems shape, and what kinds of societies these organizations sustain.

The authors' ambition to speak across audiences is noteworthy as well. Scholars will recognize core disciplinary concerns, related to data, infrastructure, organizational routines, decision processes, and the politics of technology, reframed for an era of AI-mediated knowledge and emerging quantum capabilities. Policymakers and regulators will encounter a nuanced account of why simplistic solutions, whether total permissiveness or blanket bans, fail to address the realities of complex socio-technical systems. Practitioners will find terminology extended for expressing what they are already experiencing: accelerating automation, expanding vendor ecosystems, mounting compliance expectations, and risk landscapes that no longer fit legacy governance structures.

On the note of terminology, the term "information singularity" can sound dramatic. In this book, it is carefully handled, serving for naming a convergence of forces that compresses time, amplifies scale, and destabilizes the traditional relationship between information, expertise, and authority. Whether we embrace this term or choose another, the underlying question remains: how do we design and govern information systems when the system is no longer a mere conduit of information, but a producer of meaning?

While we all hold our own perspectives on the questions explored in the book, and some may differ with the authors' specific analyses, one thing is certain: regardless of your background, this book will challenge you to reconsider your assumptions and reevaluate your vision of the future.

Professor Irit Hadar, Director, Center for Cyber, Law and Policy, University of Haifa.

Haifa, Israel
March 1st, 2026

Contents

1	Introduction	1
1.1	About the Book	1
1.2	The Challenges of Technological Progress	3
1.3	Methodology and Book Structure	5
1.4	Book Audience and Contribution	6
1.5	Debating on Information Singularity	7
2	A Brief History of Information Systems	9
2.1	Introduction	9
2.2	Capturing, Storing, Processing, and Disseminating Information	10
2.3	The Birth of Hardware, Software, and Communication	13
2.4	The Rise of Information Systems	21
2.5	Conclusions	26
3	The Current State of Information Systems	33
3.1	Introduction	33
3.2	Common Types of Information Systems	34
3.3	Emerging Technologies and Innovations (2000–2025)	42
3.4	Digital Transformation	46
3.5	Academic Perspectives	52
3.6	Conclusions	57

4	Challenges and Abuses of Information Systems	65
4.1	Introduction	65
4.2	Vulnerabilities of Information Systems	68
4.3	The Main Dilemmas/Challenges of Information Systems	70
4.4	Conclusions	86
5	Legal and Regulatory Frameworks for Information Systems	93
5.1	Introduction	93
5.2	Understanding Domestic and International Law	95
5.3	Overview of Major Legal Frameworks Governing IS	97
5.4	Regulatory Compliance, Standards, and Risk Management	118
5.5	Ethical and Social Considerations in IS Law	120
5.6	International and Cross-Border Regulatory Issues	123
5.7	Conclusions	127
6	Implications of Artificial Intelligence for Information Systems	135
6.1	Introduction	135
6.2	Artificial Intelligence: Evolution, Types, Functions, and Approaches	137
6.3	AI Agents and Agentic AI in Information Systems	149
6.4	AI Use Cases and Applications in Information Systems	152
6.5	How AI Enhances Information Systems	154
6.6	Challenges and Negative Implications	159
6.7	Conclusions	175
7	Introduction to Quantum Information Science	187
7.1	Introduction	187
7.2	Introduction to Quantum Theory	188
7.3	Quantum Information Science	194
7.4	The Second Quantum Revolution	198
7.5	Conclusions	213
8	Toward Information Singularity	225
8.1	Introduction	225
8.2	Defining Singularity	226
8.3	How AI Might Lead to Information Singularity	231
8.4	The Role of QIS	234
8.5	Are We Ready?	240
8.6	The Way Ahead: Future Trends and Applications	246
8.7	Conclusions	247
	Index	255

List of Abbreviations

AGI	Artificial General Intelligence
AI	Artificial Intelligence
AIS	Association for Information Systems
ANI	Artificial Narrow Intelligence
APPI	Act on the Protection of Personal Information
ASI	Artificial Superintelligence
ATT	App Tracking Transparency
AWS	Amazon Web Services
BBS	Bulletin Board Systems
BCPL	Basic Combined Programming Language
BI	Business Intelligence
BIS	Bureau of Industry and Security
BYOD	Bring Your Own Device
C2PA	Coalition for Content Provenance and Authenticity
CAC	Cyberspace Administration of China
CBPR	Cross-Border Privacy Rules
CCDCOE	Cooperative Cyber Defense Centre of Excellence
CCL	Commerce Control List
CCPA	California Consumer Privacy Act
CDO	Chief Digital Officer
CFO	Chief Financial Officer
CFPB	Consumer Financial Protection Bureau
CGA	Color Graphics Adapter
CIA	Confidentiality, Integrity, and Availability
CLOUD	Clarifying Lawful Overseas Use of Data

CMMC	Cybersecurity Maturity Model Certification
CMS	Content Management Systems
CNN	Convolutional Neural Network
COBOL	Common Business-Oriented Language
COPPA	Children's Online Privacy Protection Act
CPL	Combined Programming Language
CPRA	California Privacy Rights Act
CRM	Customer Relationship Management
CSL	Cybersecurity Law
CTSS	Compatible Time-Sharing System
CV	Computer Vision
DE-CIX	Frankfurt Internet Exchange
DMA	Digital Markets Act
DOE	Department of Energy
DOS	Disk Operating System
DPC	Data Protection Commission
DSA	Digital Services Act
DSL	Data Security Law
DSR	Design Science Research
DSS	Decision Support Systems
EAR	Export Administration Regulations
EC2	Elastic Compute Cloud
ECIS	European Conference on Information Systems
EDPB	European Data Protection Board
EDVAC	Electronic Discrete Variable Automatic Computer
EIS	Executive Information Systems
ENIAC	Electronic Numerical Integrator and Computer
ENISA	European Union Agency for Cybersecurity
ERP	Enterprise Resource Planning
ESS	Executive Support Systems
ETHICS	Effective Technical and Human Implementation of Computer-based Systems
EU	European Union
FAR	Federal Acquisition Regulation
FCA	Financial Conduct Authority
FHE	Fully Homomorphic Encryption
FISMA	Federal Information Security Management Act
FORTTRAN	Formula Translation
FTC	Federal Trade Commission
FTQC	Fault-Tolerant Quantum Computing
GDPR	General Data Protection Regulation
GIGO	Garbage In, Garbage Out
GLBA	Gramm-Leach-Bliley Act

GPS	Global Positioning System
GRC	Governance, Risk, and Compliance
GSP	Golden Shield Project
GUI	Graphical User Interface
HBS	Harvard Business School
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HTAP	Hybrid Transactional and Analytical Processing
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IBP	Integrated Business Planning
ICIS	International Conference on Information Systems
ICO	Information Commissioner's Office
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IFIP	International Federation for Information Processing
IRS	Internal Revenue Service
IS	Information Systems
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
IYQ	Year of Quantum Science and Technology
KMS	Knowledge Management Systems
LGPD	Lei Geral de Proteção de Dados
LSE	London School of Economics
MAXC	Multiple Access Xerox Computer
MDM	Mobile Device Management
MIS	Management Information Systems
ML	Machine Learning
MRI	Magnetic Resonance Imaging
NERC	North American Electric Reliability Corporation
NIN	National Information Network
NIS	Network and Information Security
NISQ	Noisy Intermediate-Scale Quantum
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
NSF	National Science Foundation
OECD	Organization for Economic Cooperation and Development
OES	Operators of Essential Services
OS	Operating System
OT	Operational Technology

PARC	Palo Alto Research Center
PC	Personal Computer
PIPEDA	Personal Information Protection and Electronic Documents Act
PIPL	Personal Information Protection Law
PPML	Privacy-Preserving Machine Learning
PPP	Public-Private Partnership
PQC	Post-Quantum Cryptography
PSD2	Payment Services Directive 2
QAI	Quantum Artificial Intelligence
QIS	Quantum Information Science
QKD	Quantum Key Distribution
QNN	Quantum Neural Networks
RAI	Responsible AI
RE	Requirements Engineering
RLS	Row-Level Security
RPS	Requests Per Second
RSI	Recursive Self-Improvement
SBU	Security Service of Ukraine
SCC	Supreme Council of Cyberspace
SCM	Supply Chain Management
SI	International System of Units
SSM	Soft Systems Methodology
TAM	Technology Acceptance Model
TIA	Transfer Impact Assessment
TPS	Transaction Processing Systems
TRADIC	Transistorized Airborne Digital Computer
TTF	Task-Technology Fit
UN	United Nations
UNCLOS	United Nations Convention on the Law of the Sea
UTAUT	Unified Theory of Acceptance and Use of Technology
UX	User Experience
WEEE	Waste Electrical and Electronic Equipment
WWII	World War II
WWW	World Wide Web
XAI	Explainable AI

List of Tables

Table 4.1	Main threats for information systems (A conceptual model)	68
Table 6.1	AI in Information Systems	176
Table 7.1	Common quantum sensing types: representative performance	210
Table 8.1	The Information Singularity Readiness Maturity Model (ISRMM)	245



1

Introduction

1.1 About the Book

Throughout modern human history, Information Systems (IS) have always been both mirrors and engines of change. They reflect the organization of knowledge, labor, and power at any given time, while simultaneously shaping new modes of coordination and decision-making, serving as enhancers and enablers of work. Today, however, IS stands at a juncture that demands more than incremental adaptation. The accelerating fusion of Artificial Intelligence (AI) and Quantum Information Science (QIS) is not merely adding computational horsepower to existing infrastructures, but it is altering the very fabric of how information is produced and managed. These two forces, AI and QIS, form the twin engines of what we term in this book as Information Singularity, a phase in which the velocity and autonomy of information processing exceed the capacities of human oversight and institutional control.

The central argument of this book is that AI and QIS together compress the information cycle: the span between input, inference, output, and, of course, decision. As information loops tighten and decisions become increasingly automated, the boundaries between data/information, knowledge, and action begin to blur. Traditional architectures of governance, audits, regulations, and ethical reviews operate too slowly to keep pace. Managing this compression responsibly requires a reimagined discipline of IS that integrates technical, organizational, and regulatory design—a socio-technical approach or alignment. Information Singularity, therefore, denotes not a distant

science-fiction event but a concrete managerial threshold: the point at which the tempo and complexity of information flows demand continuous verification, adaptive control, and cross-disciplinary governance and regulation. This book proposes a roadmap for reaching that threshold deliberately rather than stumbling into it. Of course, we cannot predict how this might develop, but we can plausibly and probably assume this stage is coming in the twenty-first century, and perhaps, we are already in its beginning.

Our book begins with history, because history offers both caution and guidance. The discipline of IS was built, layer by layer, at the intersection of computing, management, operations research, and social science. Each technological wave, from mainframes to client-server, from the Web to cloud and mobile, reconfigured the relationship between data and decision. Scholars such as Heinz K. Klein and Rudy Hirschheim have shown that IS evolved through multiple overlapping eras characterized by shifts in governance structures, research themes, and educational institutions. IS became pluralistic by necessity as it absorbed insights from engineering, sociology, even psychology and behavior, and management science because no single discipline could explain or manage the socio-technical complexity it confronted. This pluralism is the field's greatest strength and its enduring challenge. It allows IS to adapt, but it also demands constant negotiation of boundaries and purposes. That is, there is no point in computing power or complex systems if we, the people, cannot use them for our benefit, and, thus, IS can also be considered as a problem solver.

Revisiting the field's intellectual history is not an antiquarian exercise. Understanding how earlier generations defined the *information problem* helps us recognize our own blind spots. The transition from data processing to information management in the 1960s mirrored industrial modernization; the move toward decision support in the 1980s reflected the rise of strategic management; the subsequent turn to enterprise systems and business intelligence paralleled globalization and digitization, especially with the rise of the internet. Each stage carried its own assumptions about human judgment, organizational control, and technological determinism. Today's fascination with AI and automation revives similar hopes and anxieties, only now amplified by scale, speed, and even depth. By recovering the field's earlier debates about systems thinking along with the balance between design science and interpretive inquiry, we arm ourselves against the amnesia that often accompanies technological enthusiasm.

What, then, distinguishes IS as a discipline in the mid-2020s? Above all, it is its action-orientation, or usability. Unlike computer science, which focuses on the properties of artifacts, or management science, which often abstracts from the materiality of technology, IS studies the intertwined integration of

people, processes, data, and machines in real contexts. It produces knowledge that is both descriptive and prescriptive, grounded in practice yet theoretically aware. Hirschheim's and Klein's call for bridging the gap between disciplines and communities remains relevant precisely because it encourages the codification of process knowledge, the reusable insights about how systems are conceived, developed, implemented, and governed. Codifying such knowledge does not constrain pluralism, but rather channels it into patterns that practitioners and educators can use. This book continues that effort by articulating patterns and capabilities for AI-native and quantum-aware IS design.

In the context of product design, the present moment can be characterized as one of compressed complexity, meaning we now see a visible part with a hidden backend. Cloud computing, data pipelines, MLOps, and, generally, platform ecosystems have made organizations simultaneously more powerful and more fragile. Information now flows across global infrastructures with latency measured in milliseconds, yet governance mechanisms often lag by months or years. The GDPR, for example, was adopted only in 2016 and became effective in 2018, decades after the internet raised privacy-related issues. Now, IS professionals are tasked not only with implementing technologies but also with ensuring that they remain transparent, secure, and ethically aligned, which is a whole contested topic of its own.

Education must evolve accordingly, and now we see the beginning of effective programs that integrate technical proficiency with socio-technical awareness, teaching students not just how to build systems but how to anticipate their organizational and ethical consequences. We can attest to this firsthand, as Dr. Kantsepolsky is a scholar-practitioner and seasoned executive with over 30 years of experience leading strategy, business development, product innovation, and the development of Information and Communication Technologies (ICT) in multinational corporations. Dr. Topor served as the Head of Cybersecurity Studies at the School of Information Systems at the Academic College of Tel Aviv-Yaffo, where both are currently educating the next generation of IS specialists. While working on this book, we applied the logic of professional practice—every technical decision embeds a governance decision.

1.2 The Challenges of Technological Progress

Technological progress has always been a double-edged sword, where every leap in efficiency is shadowed by a growing “pathology” of security debt and algorithmic bias. The automation of information flows often outpaces the

automation of accountability. Machine-learning models trained on biased or low-quality data produce inequitable outcomes that undermine trust. Data pipelines designed for efficiency frequently sacrifice traceability, making post-hoc audits difficult. Organizational incentives, meanwhile, can encourage speed over safety. The result is a growing mismatch between the complexity of systems and the maturity of the institutions that rely on them. The financial aspect of IS is still premature in mid-2020, but this issue is outside of our research scope. One of the book's core claims is that governance itself must be treated as architecture—just like the concept of security by design, or objectivity by design. Legal obligations and ethical principles must be translated into system properties like auditability, explainability, and resilience, rather than appended as afterthoughts, just as software code should be written securely, and not patched afterward.

AI-enhanced IS is already well underway. AI reshapes every classical system type. For instance, transaction systems become self-monitoring and anomaly-detecting; management information systems evolve into predictive dashboards; decision support systems employ ensemble models to simulate strategic outcomes; executive systems ingest near-real-time intelligence from global data streams; and enterprise resource planning, customer relationship management, and supply-chain management platforms now incorporate generative and prescriptive analytics that automate planning and interaction. These capabilities expand organizational intelligence but also magnify risk. Bias, model drift, and lack of interpretability can undermine decisions at scale. The challenge is to integrate intelligence without losing control.

Still emergent but already influential are quantum technologies. Quantum Information Science promises revolutionary breakthroughs in optimization, simulation, sensing, communications, and cryptography. Even before these systems reach widespread practical advantage, their implications are immediate: classical cryptography will need to be replaced or augmented with post-quantum algorithms, demanding years of migration work across digital infrastructures. The governance dimension of this transition is critical. Asset inventories, key-management policies, and cryptographic agility must be treated as continuous capabilities, not one-time projects. Moreover, quantum-inspired and hybrid quantum-classical algorithms may soon redefine what is computationally feasible in machine learning, creating new opportunities for pattern discovery but also new challenges for verification. The prudent approach is scenario-based, where we should plan multiple options, define decision checkpoints, and maintain adaptability.

From these dynamics emerge three guiding questions. First, how do AI and QIS reconfigure classical IS types at the levels of architecture, workflow,

and control? Second, what design and governance patterns make AI/QIS-ready systems trustworthy and compliant in practice, or not? Third, what transition pathways allow organizations to capture the benefits of acceleration while minimizing technical and regulatory debt? Each question connects to a corresponding set of working propositions. We suggest, for example, that organizations embedding auditability-by-design will outperform those that rely on post-hoc audits in both incident response and regulatory exposure. We argue that human-in-the-loop oversight must evolve into human-on-the-loop governance, where people supervise systems rather than micromanage them. And we also suggest that crypto-agility, the ability to change cryptographic primitives rapidly, is the best leading indicator of quantum readiness, in the context of security.

1.3 Methodology and Book Structure

This book adopts a multidimensional, pragmatic framework to bridge the gap between technical complexity and regulatory oversight. The evidence base spans peer-reviewed IS scholarship, standards such as those from NIST and ISO/IEC, industry white papers, incident analyses, and regulatory documents. The approach combines literature synthesis, comparative case studies, design-science pattern mining, legal-doctrinal analysis, and scenario planning. The synthesis identifies convergences and divergences across IS, security, and policy research. Case studies, drawn from multiple sectors, are used to surface repeatable problem-solution patterns, each articulated with context, forces, and consequences. Legal and regulatory analysis translates obligations, such as transparency, robustness, and accountability, into technical requirements. Finally, scenario planning tests these patterns under varying technological and regulatory futures, ensuring that the recommendations remain robust amid uncertainty. We also avoid vendor-specific prescriptions and focus on capabilities, those architectural and managerial competencies that remain valid even as specific technologies evolve.

The eight chapters that follow are arranged as a coherent arc. The present introduction establishes the conceptual frame, definitions, guiding questions, and methodology. [Chapter 2](#) revisits the history of IS, tracing its evolution through successive technological and organizational paradigms and examining how its pluralistic identity took shape. [Chapter 3](#) surveys the current landscape, describing dominant technologies, industry practices, and educational trends. [Chapter 4](#) examines the dark side, security debt, bias, disinformation, and other abuses that test the limits of governance. [Chapter 5](#)

analyzes the often too many and too complex legal and regulatory frameworks that define what responsible practice means, translating their demands into system properties. [Chapter 6](#) explores the concrete implications of AI for traditional IS types, identifying both opportunities and systemic risks. [Chapter 7](#) introduces QIS, explaining its technical foundations and governance ramifications. Finally, [Chapter 8](#) synthesizes these thematic threads into a strategic roadmap toward the information singularity. By introducing the Information Singularity Readiness Maturity Model (ISRMM), the chapter provides a robust framework for capability assessment and a targeted research agenda. ISRMM may serve as a planning utility for both scholars and practitioners, facilitating the design of transition sequences for governing AI-enabled autonomy and navigating quantum-era security shifts.

1.4 Book Audience and Contribution

Designed as a bridge between technical and strategic disciplines, this book speaks to the diverse stakeholders tasked with building and regulating our digital future. Executives and architects will find actionable guidance for designing and governing next-generation systems. Policymakers will gain a translation layer between technical feasibility and legal obligation. Educators and researchers will encounter a conceptual framework that links historical foundations to emerging challenges. Each chapter is self-contained yet interdependent, allowing readers to enter through the pathway most relevant to their roles. For this reason, we include chapter introductions, conclusions, and some recurring examples. The style is deliberately integrative, where technical detail is paired with conceptual clarity, and theoretical discussion is grounded in practice.

The contribution of this work lies in four interlocking achievements. First, it offers a unified conceptual framework for understanding the convergence of AI and QIS as a single socio-technical phenomenon: the compression of information cycles that constitutes information singularity. Second, it suggests actionable design patterns for AI-native and quantum-aware IS, giving practitioners tools for building systems that are explainable, auditable, and resilient. Third, it advances the notion of compliance-as-architecture, demonstrating how legal and ethical obligations can be embedded into the technical and organizational layers of IS. Fourth, it proposes a research and education agenda that redefines what it means to teach and study IS in the age of AI and QIS, ensuring that future professionals are equipped not only to build systems but also to govern them.

The book's scope is ambitious but bounded. It does not aim to teach quantum mechanics or to catalog every AI algorithm or every possible risk and bias. Its focus is on implications, architectures, and governance—on the managerial and institutional challenges of integrating these technologies into the infrastructures of society. Where we generalize, we do so cautiously, acknowledging the diversity of organizational contexts and legal regimes. Where we prescribe, we label our guidance as design-and-action, open to empirical refinement. The pace of technological change guarantees that some details will age, but the underlying principles—responsibility, transparency, and adaptability—will remain.

1.5 Debating on Information Singularity

To understand the systems of tomorrow, we must first acknowledge the dual heritage of IS as a field built on the rigid feedback loops of early systems theory and the nuanced, even interpretivist, perspectives that followed. IS has always balanced the technical and the human. Early systems thinkers emphasized feedback and control; later waves incorporated interpretivist approaches that valued meaning and context. The coexistence of these paradigms, sometimes contentious, ultimately enriched the field. Pluralism, rather than fragmentation, is what allows IS to address complex real-world problems. The field's ongoing efforts to establish a coherent body of knowledge, seen in the IS literature and in comparative education studies, reflect its maturing professional identity. Meanwhile, contemporary research on IS education emphasizes the triad of learner, environment, and curriculum. Understanding who learns, where they learn, and what they learn in a digital age shaped by AI can indicate a lot. The same triad guides how institutions must now adapt their own IS to the coming quantum horizon.

From this vantage point, the integration of AI and QIS appears not as a rupture but as the next logical evolution in the co-development of technology and governance. Architecture and compliance emerge as the twin pillars of this evolution. Architecture determines where intelligence resides, at the edge, in the service layer, or in the enterprise core, and how it connects to data sources and human oversight. Compliance ensures that these architectures remain accountable to the societies that depend on them—somewhat of a social contract. Together, they define a new professional ethic, which means that technical design is a form of governance.

Skeptics may question whether talk of information singularity exaggerates near-term change. They may argue that both AI and QIS are still constrained

by technical and economic limits. Such caution is healthy, but it misses the point. The singularity, as used here, is not a prediction of runaway intelligence; it is a description of accelerating interdependence between human and machine decision loops. Even if full quantum advantage remains decades away, the preparation window for governance and migration is already open. Cryptographic standards are being rewritten as these lines are being written as well, and regulators are integrating AI risk management into law. Delay carries a cost. Proactive design is the rational form of skepticism, and we must learn from past delays, as with previous technologies.

Others may fear that efforts to codify patterns and bodies of knowledge risk freezing a dynamic field. Yet codification, if done correctly, is not ossification. Patterns do not prescribe a single method; they record problem-solution relationships that can be adapted to context. Our aim is not to standardize thought but to make learning cumulative. Similarly, design-and-action guidance will inevitably age, but by embedding scenario planning and capability thinking, we ensure that organizations can adapt their implementations as technologies evolve.

In practical terms, the message of this introduction is straightforward. The acceleration of information cycles is real and measurable. The risk of institutional lag—legal, organizational, or ethical—is likewise real. The task ahead is to build systems and organizations that can keep pace without losing coherence or legitimacy. That means embedding governance into design, cultivating crypto-agility and auditability as core capabilities, and educating a generation of professionals who can think simultaneously in technical, managerial, and ethical terms.

The chapters that follow elaborate this agenda in detail, but the orientation is clear from the outset, and we advise that information singularity is not destiny—it is design. Whether societies experience it as empowerment or as disruption depends on how deliberately we manage the convergence of intelligence and information. IS, as both a discipline and a practice, holds the keys to that management. By revisiting our history, refining our methods, and expanding our imagination, we can ensure that the next transformation of information serves human purposes rather than eroding them. This book is written in that spirit.



2

A Brief History of Information Systems

2.1 Introduction

This chapter contains a historical exploration of information systems, briefly from ancient times and pre-industrialization and digitization, and mainly from the twentieth century onward until the year 2000, when it became clear that the world was headed toward more reliance on IS. In addition, the chapter charts IS's institutional maturation, conferences, journals, curricula, and its shift from tool appraisal to theory about adoption, value, alignment, and change. Our purpose is twofold. First, we show how successive waves of technology, mechanization, mainframes, personal computing, and the internet reconfigured the basic informational functions of collection, storage, processing, and communication. Second, we situate these changes within the maturation of IS as a discipline, highlighting how its questions, theories, and methods differentiated it from adjacent fields such as computer science and management while remaining deeply intertwined with them. In doing so, we treat IS as a socio-technical endeavor: systems that succeed only when technical architectures, organizational routines, and human practices evolve together.

This chapter is organized into three main sections. We begin with the history of information practices to illuminate how enduring informational needs of early humans developed through time up to the Industrial Revolution, which introduced the first communication and information processing methods and technologies. Then we provide historical perspectives on the birth

of computers, and their deployment in organizations, along with the first managerial applications. This section also presents the development path and explains the information and communication technologies available by the late 1990s. Finally, we end with the internet's diffusion and the web's standardization to explain how, at the end of the twentieth century, formerly isolated applications became networked platforms serving global audiences, foreshadowing developments we cover in later chapters.

Following the explanations on the core technological components of IS, the last section deals with the rise and establishment of IS as a distinguished discipline. A part of this section, we present the initial IS schools of thought and academic programs of that time. The historical trajectory of IS reveals a field shaped by continuous technological advancements, shifting human, social, and organizational needs, and evolving academic perspectives. By examining IS as a socio-technical process, we set the stage for the subsequent chapters in this book, which also address human and technological factors.

2.2 Capturing, Storing, Processing, and Disseminating Information

2.2.1 Information Practices from Ancient Civilizations to the Middle Ages

The need to collect and share information has been fundamental to survival since the earliest days of human existence. Early humans used oral communication to transmit and share experiences and thus preserved vital knowledge about reaching food, survival strategies, and social hierarchies (Couch, 1989; Marlowe, 2005). The transition from oral to written communication constituted significant progress in social development. Writing as a method of information creation was used to record and document stories, laws, and economic activities. The literature and the archeological artifacts show that the Sumerians used cuneiform writing on clay tablets around 3200–3000 BCE (Kramer, 2010). Written records enabled the storage of information beyond the limitations of human memory and, consequently, its sharing across generations. Hence, cuneiform writing constitutes one of the earliest examples where information used for decision-making enabled advanced social structure development.

The importance of information in the governance and administration of ancient civilizations is often exemplified in the literature by referring to ancient Egypt. As part of their cultural tradition, Egyptians used temple

walls, tombs, statues, and papyrus scrolls to describe and document everyday life routines, important events, and even religious beliefs (Teeter, 2011; Lichtheim, 2019; Galán, 1994). Ancient Egyptians are also often credited for establishing the first bureaucratic systems that relied on information to manage resources, labor, and trade. One example is the construction of monumental architecture, including pyramids (Bard, 2005). The writings in the form of hieroglyphics, along with the information-based decision-making management practices, were vital for organizing information to coordinate large-scale labor, materials, resources, and timelines (Kahl, 2022).

In addition to governance and administration, the economic prosperity of ancient civilizations was also dependent on trading. Since the role of information in trade and commerce cannot be overestimated, the ability to disseminate information during Egyptian times was critical. To allow trading operations, there was a need for information about trade routes and market conditions, along with record-keeping about transactions, goods, and prices (Vasiljević, 2013). With the time and development of trade networks, the influence of information management practices extended beyond Egypt, where similar systems emerged, and the need for information exchange continued to grow.

The first alphabet was developed about 2000 years later, approximately 1050 BCE, by the Phoenicians, significantly simplifying writing and improving communication across cultures (Elayi, 2018). The economic development and rise of empires, such as Greece and Rome, enhanced the importance of and dependence on information management. In the fields of philosophy and science, the Greeks developed early forms of data organization and classification. Greek philosophers of that time laid the basis for systematic thinking about information and knowledge (Chondros, 2017). In turn, the Romans' sophisticated administrative systems for governing territories relied on written rules and protocols and served as the basis for hierarchical management practices with an emphasis on documentation and record-keeping (Haighton, 2010; Zhang, 2022). As the organization and retrieval of information became increasingly important, this period of human history marked the beginning of a structured approach to information management.

The Antikythera Mechanism, dating to approximately the second century BCE, serves as a profound historical precursor to the human drive to mechanize calculation and systematize information. Often described as the world's first mechanical calculator, its intricate assembly of bronze gears demonstrates an early mastery of converting complex celestial data into predictable, physical outputs, hinting at the human desire to calculate and control information (Seiradakis & Edmunds, 2018).

L

Landauer, Rolf 194
 Laser 18, 188, 193, 197, 199, 208
 Least privilege 83, 116, 136, 151, 166, 175
 Legal personhood 166, 167
 Light quanta 189
 Lineage views 40
 LISP 19, 20
 Lorenz cipher 13
 Low-code 40, 158

M

Machine learning (ML) 4, 36, 40, 56, 73, 138, 142, 143, 144, 145, 148, 152, 153, 154, 156, 158, 163, 170, 231, 232
 Magnetic resonance imaging (MRI) 147, 193
 Mainframe computing 2, 9, 22, 26
 Managed transitions 240
 Management information systems (MIS) 4, 22, 25, 35, 36, 38, 41, 55, 135, 154, 155, 156, 175, 247, 248
 Management Information Systems (MIS) 34
 Matrix mechanics 190, 191
 Metrology 197, 198, 199, 200, 201
 Microprocessors 193
 Microservices 43
 Microsoft Dynamics 39, 156
 Misinformation 72, 122, 168, 173, 233, 240
 Mobile computing 2, 22, 33, 42, 82
 Mobile Device Management (MDM) 44
 Model cards 136, 166, 175, 247
 Model flows 167
 Multi-cloud 43
 Multics 17
 Mutual Legal Assistance Treaties (MLATs) 126

N

National security 74, 78, 82, 97, 102, 104, 106, 107, 109, 121, 124, 126
 Natural language processing (NLP) 137, 138, 145, 147, 152, 154, 155, 156, 158, 170, 176
 Network and Information Security (NIS) Directive 109, 112, 117, 125
 NIST AI RMF 119, 166, 175, 247
 NIST CSF 126
 No-cloning theorem 195
 Noisy Intermediate-Scale Quantum (NISQ) 203, 204, 205, 239

O

Omnichannel strategies 44
 OpenAI 77, 138, 146, 148, 164
 Operational technology (OT) 46
 Order-to-cash 38, 39, 155
 Organizational challenges 170
 Over-reliance on AI 136, 160, 177

P

Paginated reports 40
 Papyrus 11
 Payment Card Industry Data Security Standard (PCI DSS) 35, 112, 119
 Personal computer (PC) 19, 20, 22, 26, 106
 Personal data 70, 71, 73, 75, 76, 78, 79, 81, 87, 96, 98, 99, 101, 102, 103, 104, 105, 109, 111, 114, 115, 117, 123, 126
 Personal Information Protection and Electronic Documents Act (PIPEDA) 98, 101, 102, 117
 Pervasive computing 44
 Phoenicians 11
 Photoelectric effect 189
 Photons 189, 195, 199, 205, 206

Planck constant (h) 188, 189
 Planck, Max 188, 189
 Platform as a Service (PaaS) 43
 Point-of-sale (POS) 34, 156
 Policy challenges 86
 Policy constraints 247
 Positive feedback loop 226, 238, 246
 Post-quantum cryptography (PQC)
 207, 243, 244, 245, 246
 Power BI 36, 39, 40, 158
 Power Platform 39
 Predictive analytics 36, 121, 136, 145,
 154, 156, 157, 158
 Printing press 12, 240
 Privacy 3, 54, 55, 65, 66, 67, 69, 70,
 71, 73, 74, 75, 76, 77, 78, 79, 80,
 81, 82, 84, 86, 87, 94, 95, 96, 98,
 99, 100, 101, 105, 111, 112, 113,
 115, 116, 117, 118, 119, 121,
 122, 123, 124, 126, 127, 128,
 160, 163, 164, 167, 168, 171,
 242, 245, 248, 249
 AI and 55
 laws and regulation 66, 70, 71, 95,
 96, 100, 101, 242
 Privacy Shield 115, 124
 Private cloud 43
 Procure-to-pay 38, 39
 Project Genesis 165
 Provenance 120, 128, 136, 150, 152,
 160, 161, 162, 165, 166, 175,
 248
 Public cloud 43
 Public sector 168, 171
 Punch cards 15

Q

QIS-AI feedback loop 235, 239, 246
 Qlik 158
 Quanta 198, 199
 Quantum 1.0 193
 Quantum 2.0 194, 201
 Quantum advantage 8, 204, 205, 213,
 235, 247
 Quantum AI (QAI) 238, 239, 246,
 247, 248, 249, 250
 Quantum coherence 192, 199
 Quantum communication 197, 207,
 208, 237
 quantum internet 207, 208, 237
 quantum teleportation 197, 207
 Quantum communications 176, 199,
 200, 213, 234, 236, 237
 Quantum computing 197, 203, 204,
 207, 234, 242
 current state of 27, 33, 203
 error correction 203, 204
 NISQ era 203, 204
 post-quantum implications 207, 242
 quantum volume 204
 role in information singularity 234
 superconducting qubits 204
 trapped ions 197, 203, 204, 208
 Quantum error correction 203, 204
 Quantum information science (QIS) 1,
 4, 42, 176, 187, 194, 195, 196,
 225, 226, 231, 233, 235, 243,
 244, 247, 249
 channel capacity 194
 mutual information 194
 no-cloning theorem 195
 Shannon entropy 196
 Quantum Internet 207, 208, 237
 Quantum Key Distribution (QKD)
 205, 206, 207, 213, 236
 Quantum mechanics 7, 187, 188, 193,
 194, 195, 199, 201, 202, 203,
 213, 236
 Quantum metrology 197
 Quantum Neural Networks (QNN)
 246
 Quantum sensing 198, 199, 200, 208,
 213, 234, 237
 Quantum simulation 200, 213