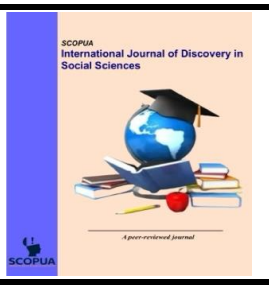
International Journal of Discovery in Social Sciences

Vol.2, Issue 1, February 2026
DOI: https://doi.org/10.64060/IJDSS.v2i1.4



Theory of Digitalization: Contemporary Theory of Digitalization

Jamil Afzal [1,2*]

[1]Southwest University of Political Science & Law, Chongqing, China
[2]International Islamic University Malaysia, Kuala Lumpur, Malaysia
* Corresponding Email: sirjamilafzal@gmail.com

Received: 03 January 2026 / Revised: 23 January 2026 / Accepted: 28 January 2026 / Published online: 01 February 2026

ABSTRACT

The Contemporary Theory of Digitalization (CToD) seeks to explain digitalization not merely as the adoption of digital technologies, but as a comprehensive, systemic, and evolving transformation that reshapes how organizations function internally and how they interact with other organizations across global networks. CToD provides a logical and conceptual framework that helps organizations to understand, design, govern, and sustain digital transformation in a rapidly changing technological, economic, and social environment. The theory recognizes digitalization as a multidimensional phenomenon involving technology, people, processes, institutions, and power relations rather than a purely technical upgrade. The innovation of CToD lies in its three-level structure, which reflects increasing degrees of digital maturity and complexity. Level 1 is a foundational digital order, whereas Level 2 is an operational digitalization, and Level 3 is Digital Connectivity and Global Interaction. This layered approach allows scholars and practitioners to analyze digitalization systematically, identify weaknesses, and design targeted interventions. It also facilitates empirical testing and comparative analysis across sectors and jurisdictions.

Keywords*:* Contemporary Theory of Digitalization; CToD; Theory of Digitalization; Layers of CToD; 3D; 5D; 7D

1. Introduction

Digitalization has emerged as one of the most transformative forces of the twenty-first century, reshaping economies, governance structures, social relations, and international systems(Afzal, 2024b; Grinin, 2022; Pfeiffer, 2021). Unlike earlier technological revolutions that primarily affected specific sectors or modes of production, digitalization permeates almost every dimension of modern life(Knell, 2021). From public administration and education to healthcare, finance, trade, diplomacy, and security, digital technologies have become deeply embedded in institutional and societal functioning. The contemporary digital era is characterized by the widespread adoption of technologies such as the Internet, cloud computing, big data analytics, artificial intelligence, blockchain, and platform-based systems(Shi et al., 2023; Tarumingkeng, 2025). These technologies enable real-time communication, automated decision-making, cross-border data flows, and unprecedented scalability of services. As a result, organizations and states increasingly rely on digital systems not merely as support tools but as core infrastructures of governance, service delivery, and strategic power. In its early conceptualization, digitalization was largely understood as a technological or operational process, digitizing records, automating workflows, or introducing information systems(Chisita et al., 2021; Gradillas & Thomas, 2025; Legner et al., 2017). Over time, it became evident that digitalization is not simply about converting analog processes into digital form but represents a structural transformation of institutions and power relations(Schröter, 2024). Digital systems increasingly shape how decisions are made, how authority is exercised, and how value is created and distributed(Snow et al., 2017). Algorithms influence administrative decisions, platforms mediate economic exchanges, and data has become a strategic asset

comparable to land, labor, or capital(Langley & Leyshon, 2017; Nayak & Walton, 2024). This shift has blurred traditional boundaries between public and private sectors, domestic and international jurisdictions, and physical and virtual spaces. One of the defining features of the contemporary digital era is the fragmentation of digital governance(Tan & Crompvoets, 2022). While digital systems operate globally, regulatory frameworks remain largely national or sector-specific(Panova & Lengyel, 2022). States adopt divergent approaches to data protection, cybersecurity, digital trade, and platform regulation(Mugamba, 2025). Organizations navigate a complex landscape of overlapping legal obligations, technical standards, and compliance requirements(Shandilya et al., 2024). International efforts to harmonize digital governance, through instruments such as the OECD Privacy Guidelines, the EU's General Data Protection Regulation (GDPR), WTO agreements (GATS and GATT), and emerging digital trade agreements, have made progress but remain incomplete(Afzal, 2024c). At the same time, geopolitical competition has intensified around digital technologies, infrastructure, and standards, giving rise to debates on digital sovereignty, technological decoupling, and cyber power(Chari, 2025; Mayer & Nock, 2025). A wide range of theoretical frameworks have been developed to study digitalization, including digital transformation models, socio-technical systems theory, platform theory, innovation diffusion models, and technology acceptance frameworks(Appelbaum, 1997; Cabral, 2019; Gray & Rumpe, 2017; Mahajan et al., 1990; Taherdoost, 2018). While these approaches offer valuable insights, they exhibit several limitations when applied to contemporary digital realities. First, many existing models are technology-centric, focusing on adoption, efficiency, or innovation outcomes while underestimating the role of law, governance, and institutional authority. Second, most frameworks are organization-centric, neglecting the broader inter-organizational and state-to-state dimensions of digital interaction. Third, issues of digital sovereignty, rights, and global power asymmetries are often treated as peripheral concerns rather than core analytical elements. Moreover, existing theories rarely provide a layered or sequential understanding of digitalization. They tend to treat digital transformation as a linear or holistic process, without distinguishing between foundational governance, operational rules, and external digital relations(Gradillas & Thomas, 2025; Sandberg et al., 2020). This lack of structural differentiation makes it difficult to diagnose failures, compare digital maturity across contexts, or design coherent digital strategies. Organizations face reputational, legal, and financial risks arising from digital failures, while states confront threats to national security and democratic governance(Kavanagh, 2022; Miller & Vaccari, 2020). Trust has thus emerged as a central challenge in the digital era. Trust cannot be sustained through technology alone; it requires clear rules, accountability mechanisms, enforceable rights, and legitimate governance structures. The absence of a coherent theoretical framework to integrate these elements has contributed to inconsistent policy responses and institutional uncertainty(Bylund & McCaffrey, 2017; Domorenok et al., 2021). This crisis of trust underscores the need for a theory that conceptualizes digitalization not as an inevitable technological trajectory but as a governable social and institutional process. In recent years, the concept of digital sovereignty has gained prominence in policy and academic discourse(Couture & Toupin, 2019). States and organizations increasingly seek to assert control over data, infrastructure, standards, and digital ecosystems(Holt & Malčić, 2015). Initiatives related to data localization, sovereign cloud infrastructure, national cybersecurity strategies, and digital industrial policy reflect this shift(Mitchell & Samlidis, 2021). At the same time, digitalization has become a domain of geopolitical competition. Control over digital infrastructure, platforms, and standards confers strategic advantages(Teece, 2017). Digital diplomacy, cyber defense, and digital alliances have become integral components of international relations. These developments highlight the inadequacy of frameworks that treat digitalization as a purely domestic or organizational phenomenon. Digitalization today operates at the intersection of governance, trade, security, and diplomacy, necessitating a theory capable of addressing these interdependencies in a structured manner(Alfarizi & Heryadi, 2024; Eriksson & Giacomello, 2007; Gatlin, 2024).

The Contemporary Theory of Digitalization (CToD) emerges in response to the conceptual, institutional, and governance gaps outlined above. CToD was developed to provide a comprehensive, layered, and governance-centric framework that captures the full complexity of digitalization in the contemporary era. The main focus of CToD is that digitalization must be understood as the construction of a regulated digital order rather than the mere adoption of digital technologies. It posits that effective and sustainable digitalization requires progression through distinct but interconnected levels: foundational digital governance, operational digital regulation, and external digital connectivity and sovereignty. CToD is explicitly designed to address the failures of fragmented digitalization by offering:

- Clear conceptual differentiation between internal and external digital processes

- Integration of law, governance, rights, and security into digitalization theory
- Applicability across organizational and state contexts
- Alignment with international legal and regulatory frameworks

2. An Insight to Contemporary Theory of Digitalization

The relevance of CToD is amplified by current global trends, including accelerated digitalization following the COVID-19 pandemic, the rapid deployment of artificial intelligence, growing concerns over data governance, and intensifying digital geopolitics. In this environment, organizations and states can no longer afford uncoordinated or purely technical digital strategies. CToD provides a theoretical foundation for responsible, sovereign, and rights-respecting digitalization, offering guidance for policymakers, institutional leaders, and researchers navigating the complexities of the digital age(Afzal, 2025).

2.1 Digitalization as an Organizational Logic

The Contemporary Theory of Digitalization positions digitalization as a new organizational logic. Traditionally, organizations were structured around hierarchical decision-making, linear workflows, and physical resources(Jerab & Mabrouk, 2023; Mihm et al., 2010). In contrast, digitalization introduces a logic based on data flows, connectivity, automation, and real-time decision-making(Isaksson et al., 2018; Kagermann, 2014). CToD explains how digital tools such as artificial intelligence, cloud computing, big data analytics, blockchain, and the Internet of Things (IoT) fundamentally alter organizational architecture. Under this theory, digitalization is not an add-on to existing systems but a transformative force that reshapes core organizational elements: strategy, structure, culture, and governance. Decision-making becomes more decentralized and evidence-driven, enabled by continuous data collection and analytics. CToD thus provides a framework to understand how organizations internalize digitalization as a guiding principle rather than a one-time project.

2.1 Integration of Technology, Strategy, and Human Capital

A key contribution of the Contemporary Theory of Digitalization is its emphasis on the integration of technology with organizational strategy and human capital. Many early digital transformation efforts failed because they focused excessively on technology without aligning it with organizational goals or workforce capabilities. CToD addresses this gap by highlighting that digitalization is successful only when technological adoption is synchronized with strategic intent and skills development. Within organizations, CToD explains how leadership plays a critical role in defining a digital vision, allocating resources, and fostering a culture of innovation. Employees are not passive recipients of technology but active participants who must adapt, reskill, and co-create digital solutions(Thomas, 2024; Whewell et al., 2022). The theory acknowledges the socio-technical nature of digitalization, recognizing that resistance, ethical concerns, and skill gaps can significantly influence outcomes. By offering a logical framework, CToD helps organizations balance efficiency gains with human-centered values such as inclusivity, transparency, and accountability.

2.3 Digitalization Across Organizational Boundaries

Beyond the internal dimension, the Contemporary Theory of Digitalization extends to organization-to-organization interactions on a global scale. In a digital economy, organizations no longer operate in isolation(Malecki & Moriset, 2007; Moriset & Malecki, 2009). They are embedded in complex ecosystems of partners, competitors, governments, and platforms. CToD explains how digitalization enables new forms of inter-organizational coordination, collaboration, and competition. Digital platforms, shared data infrastructures, and interoperable systems allow organizations across different countries to integrate operations, exchange information, and co-create value in real time(Abbate et al., 2022; Aksoy, 2023). CToD provides a conceptual lens to understand how trust, standards, and governance mechanisms evolve in these digitally mediated relationships.

2.4 Globalization and Digital Interdependence

The Contemporary Theory of Digitalization recognizes that digitalization is deeply intertwined with contemporary globalization. Unlike earlier phases of globalization driven primarily by trade and capital flows, the current phase is shaped by data flows, digital services, and virtual collaboration. CToD explains how organizations participate in global digital networks where geographical distance is less significant, but digital capabilities and institutional frameworks become decisive. Through this theory, digitalization is understood as a driver of global interdependence, enabling organizations in different regions to collaborate seamlessly while also exposing them to shared vulnerabilities. CToD provides a structured way to analyze how organizations navigate these risks while leveraging global digital opportunities.

2.5 Governance, Ethics, and Power in Digitalization

An important aspect of the Contemporary Theory of Digitalization is its attention to governance, ethics, and power dynamics. Digitalization redistributes power within organizations and across global systems(Pfeiffer, 2021). Data ownership, algorithmic decision-making, and platform control can concentrate power in the hands of a few actors while marginalizing others(Lee et al., 2020; Naudts, 2024). CToD incorporates these considerations into its logical framework, ensuring that digitalization is analyzed not only for its efficiency but also for its societal implications. Within organizations, governance mechanisms must evolve to address issues such as data privacy, algorithmic transparency, and accountability for automated decisions(Bibi, 2024; Coglianese & Lehr, 2019). Across organizations, global governance becomes critical to manage cross-border data flows, intellectual property, and digital competition(Rehman, 2023; Voss, 2019). CToD helps organizations understand the need for ethical digitalization, where technological advancement aligns with legal standards, human rights, and social responsibility.

2.6 Adaptability and Continuous Transformation

The Contemporary Theory of Digitalization emphasizes that digitalization is continuous rather than finite. Technologies evolve rapidly, and organizational environments are increasingly volatile(Day & Schoemaker, 2016). CToD provides a framework that values adaptability, learning, and resilience. Organizations are encouraged to view digitalization as an ongoing process of experimentation, feedback, and refinement. This perspective helps organizations avoid rigid digital strategies that quickly become obsolete. Instead, CToD promotes modular systems, agile governance, and continuous capability development. At the inter-organizational level, it supports flexible partnerships and adaptive standards that can respond to technological and regulatory changes(Liu et al., 2019; Martínez-Sánchez et al., 2009). By doing so, the theory equips organizations to remain competitive and relevant in a dynamic global digital landscape.

3. Conceptual Foundation of the Contemporary Theory of Digitalization

The Contemporary Theory of Digitalization (CToD) is proposed as a comprehensive, multi-level theoretical framework that conceptualizes digitalization as a governance-driven, rights-based, and sovereignty-aware process, rather than a purely technological or innovation-centric phenomenon. The theory responds to the growing recognition that digital transformation failures at organizational and state levels are primarily rooted in weak digital governance, fragmented regulations, unclear digital authority, and inadequate mechanisms for cross-border digital interaction. CToD advances the argument that digitalization must be understood as the construction of a regulated digital ecosystem, encompassing internal institutional order, operational digital practices, and external digital relations. It integrates insights from digital governance theory, international trade law, cybersecurity governance, and public administration to offer a unified analytical lens for understanding contemporary digital systems.

3.1 Theoretical Significance

CToD advances digitalization theory by reframing digital transformation as a regulated socio-technical order rather than a technological inevitability. It offers scholars and policymakers a structured lens to analyze digital governance, digital sovereignty, and cross-border digital relations in an increasingly interconnected world. The Contemporary Theory of Digitalization contributes to the literature by offering a holistic, layered, and governance-centric framework that integrates law, technology, rights, security, and international relations. It moves beyond fragmented digitalization models by systematically linking internal governance with global digital interaction. By addressing what digitalization is, why it is necessary, how it operates, who governs it, where it applies, and when it becomes critical, CToD provides a robust analytical foundation for empirical research, policy formulation, and institutional digital strategy.

3.2 CToD Level 1

Level 1 of the Contemporary Theory of Digitalization (CToD) represents the foundational layer upon which all higher levels of digital transformation are built. This level is concerned with establishing the basic digital order of an organization or a state by defining its digital boundaries, regulatory framework, and governance mechanisms. Because it addresses Digital Border, Digital Regulations, and Digital Governance, Level 1 is also referred to as the 3D Level of Contemporary Theory of Digitalization. Level 1 focuses on creating a secure, lawful, and governable digital infrastructure within which an organization or state operates. It answers the fundamental question: Where does the digital authority of an organization or state begin and end, under which rules does it function, and how is it governed?

Within the Contemporary Theory of Digitalization, Level 1 is strategically critical because it establishes digital legitimacy and authority. It ensures that digital transformation does not undermine institutional integrity, legal compliance, or

sovereignty. By clearly defining digital borders, regulations, and governance, organizations and states protect themselves against cyber threats, legal uncertainty, and governance failures. Moreover, Level 1 enables trust; internally, employees and users trust digital systems when rules and governance are clear. Externally, partners, regulators, and international actors are more willing to engage with organizations or states that demonstrate strong digital governance and regulatory clarity.

3.2.1 Digital Border: Defining the Digital Territory

The concept of the Digital Border is central to Level 1 of CToD. Traditionally, borders were physically defined by geography and jurisdiction. In the digital age, however, organizations and states operate in virtual environments where data, services, and interactions transcend physical boundaries(Chouliaraki & Georgiou, 2022; Churchill et al., 2012). Level 1 requires an organization or state to clearly define its digital area of operation, which includes digital assets, data repositories, platforms, networks, and virtual services. The defining characteristic of Level 1 is its focus on basic digital infrastructure within an organization or state. This includes hardware, software, networks, data systems, security architecture, and foundational digital platforms. However, CToD views infrastructure not only as physical or technical assets but as an institutional framework supported by borders, regulations, and governance. At this level, the goal is not innovation or advanced digital services, but stability, control, and readiness. An organization or state must first ensure that its digital environment is clearly defined, legally regulated, and effectively governed.

3.2.2 Digital Regulations: Establishing the Rules of the Digital Space

Once the digital border is defined, Level 1 emphasizes the creation of Digital Regulations, which function as the foundational legal and policy framework governing digital activities. Digital regulations include rules, laws, bylaws, policies, and standard operating procedures that guide how digital systems are designed, used, and managed within an organization or state(Beaumier et al., 2020; Hren, 2021). These regulations address key issues such as data protection, privacy, cybersecurity, access control, record management, intellectual property, digital conduct, and compliance obligations. For organizations, digital regulations ensure that employees, management, and stakeholders interact with digital systems consistently and lawfully(Omoseebi et al., 2024; Snow et al., 2017). For states, they form the backbone of national digital law, including cyber laws, data protection legislation, and electronic transaction regulations(Afzal, 2024a; Sarma, 2023).

3.2.3 Digital Governance: Managing and Enforcing the Digital Order

The third pillar of Level 1 is Digital Governance, also referred to as e-governance. While digital borders define where authority applies, and digital regulations define what rules apply, digital governance defines how decisions are made, implemented, monitored, and enforced in the digital domain. Digital governance includes institutional structures, decision-making mechanisms, accountability systems, and oversight processes related to digital operations(Erkut, 2020; Milakovich, 2012). In organizations, this may involve digital committees, IT governance frameworks, data governance boards, cybersecurity units, and compliance offices. In states, digital governance may include ministries of digital affairs, regulatory authorities, cybersecurity agencies, and digital public service platforms. Furthermore, digital governance enables accountability in digital decision-making(Sharma et al., 2021; Wang et al., 2018). As more processes become automated or data-driven, governance structures ensure that responsibility remains clearly assigned and that digital power is exercised ethically and transparently.

3.3 CToD Level 1

Level 2 of the Contemporary Theory of Digitalization (CToD) builds directly upon the foundational framework established in Level 1 and shifts the focus from digital order to digital operation. While Level 1 defines the digital borders, regulations, and governance mechanisms of an organization or state, Level 2 translates these foundational principles into day-to-day operational rules. This level determines how digital systems are used, what digital products and services are offered, what obligations exist for institutions and individuals, how privacy and security are ensured, and what digital rights are recognized and protected. Because it addresses five core operational dimensions, Level 2 is also known as the 5D Level of Contemporary Theory of Digitalization.

Level 2 occupies a crucial position within the Contemporary Theory of Digitalization by transforming foundational principles into operational reality. It ensures that digital borders, regulations, and governance mechanisms established in Level 1 are effectively implemented through concrete rules, systems, and responsibilities. This level bridges the gap between digital governance and practical digital functioning. It enables organizations and states to deliver digital goods and services,

operate secure digital infrastructure, enforce obligations, protect privacy, and uphold rights in a coherent and internationally aligned manner.

3.3.1 Digital Goods and Services: Defining Digital Output

The first dimension of Level 2 concerns Digital Goods and Services, which represent the tangible and intangible digital outputs of an organization or state. These include software, digital platforms, online services, data-driven products, cloud services, digital content, and electronically delivered public or private services(Dou et al., 2013; Laatikainen & Ojala, 2019). At this level, organizations must clearly identify and classify their digital goods and services in accordance with the digital regulations designed in Level 1. Within the Contemporary Theory of Digitalization, this classification is not merely administrative; it has legal, economic, and strategic implications. Digital goods and services must align with international trade norms, particularly major treaties such as the General Agreement on Trade in Services (GATS) and the General Agreement on Tariffs and Trade (GATT)(Fleuter, 2016; Oraegbunam & Onwuatuegwu, 2023). By explicitly defining digital goods and services, organizations ensure regulatory clarity, facilitate cross-border digital trade, and reduce legal uncertainty.

3.3.2 Digital Infrastructure: Operationalizing the Digital Framework

The second component of Level 2 is Digital Infrastructure, which translates regulatory and governance principles into functional technological systems. While Level 1 establishes the authority and governance of digital systems, Level 2 focuses on how these systems are designed, deployed, and maintained to support organizational operations. Digital infrastructure includes hardware, software, cloud platforms, data centers, networks, enterprise systems, and digital interfaces(Greenstein, 2019; Li et al., 2022). Under the Contemporary Theory of Digitalization, infrastructure must be developed in alignment with the digital borders, regulations, and governance mechanisms defined in Level 1. This ensures consistency, security, and compliance across the organization or state. At this level, infrastructure is not viewed as a neutral technical asset but as a regulated operational environment.

3.3.3 Digital Obligations: Institutional and Individual Responsibilities

After establishing basic digital regulations in Level 1, Level 2 specifies who must do what within the digital ecosystem. Digital obligations clarify duties, responsibilities, and liabilities related to the use, management, and protection of digital systems and data(Rim, 2024; Trier et al., 2023). At the organizational level, digital obligations may include ensuring system integrity, protecting user data, maintaining cybersecurity standards, complying with reporting requirements, and providing accessible and reliable digital services. At the individual level, covering employees, managers, users, and officials, obligations may involve responsible use of digital systems, compliance with security protocols, ethical handling of data, and adherence to internal digital policies.

3.3.4 Digital Privacy and Security: Protecting Digital Trust

Digital Privacy and Security form a critical pillar of Level 2, reflecting the central role of trust in digital operations. As organizations increasingly rely on data-driven systems, the protection of personal, institutional, and sensitive data becomes a fundamental operational requirement(Herath et al., 2024; Hiranandani, 2011). Level 2 requires organizations or states to clearly define and implement privacy and security regulations that govern data collection, processing, storage, and transfer. Within CToD, digital privacy and security must align with leading international standards and legal instruments, including the OECD Privacy Guidelines, the EU's General Data Protection Regulation (GDPR), and national laws such as China's Personal Information Protection Law (PIPL). These frameworks emphasize principles such as lawfulness, transparency, purpose limitation, data minimization, and security safeguards.

3.3.5 Digital Rights: Recognizing Entitlements in the Digital Space

Digital rights define what individuals and entities are entitled to in digital environments, including rights related to access, participation, privacy, data ownership, due process, and freedom from digital discrimination(Custers, 2022; Rusakova et al., 2020). At the organizational level, digital rights ensure that employees, users, and stakeholders are treated fairly and transparently in digital systems(Doerr & Lautermann, 2024). At the state level, they align digital governance with constitutional values, human rights standards, and democratic principles(AJUZIEOGU, 2025; Siur et al., 2024). Within CToD, digital rights serve as a counterbalance to digital power, preventing excessive control or arbitrary decision-making by institutions or automated systems.

3.4 CToD Level 3

Level 3 of the Contemporary Theory of Digitalization (CToD) represents a decisive shift from internal and operational digitalization toward inter-organizational and cross-border digital interaction. Level 3 focuses on how digitally mature entities connect, interact, cooperate, and protect their interests in the global digital environment. This level recognizes that digitalization today is inherently relational and transnational. Because it incorporates seven interrelated dimensions, Level 3 is also known as the 7D Level of the Contemporary Theory of Digitalization. At this stage, digitalization extends beyond organizational boundaries and enters the domain of digital ecosystems, global networks, and digital geopolitics. Level 3 provides a structured framework to manage connectivity, cooperation, exchange, and conflict in the digital sphere while preserving institutional autonomy and sovereignty.

Level 3 serves as the connective layer of the Contemporary Theory of Digitalization. It enables organizations and states to move from internal digital readiness to active participation in the global digital ecosystem. By integrating connectivity, relations, defense, diplomacy, exchange, and sovereignty, this level provides a comprehensive framework for managing digital interdependence.

3.4.1 Digital Relations: Structuring Inter-Organizational and State-to-State Interaction

Digital Relations form the core of Level 3 and refer to the structured digital interactions between organizations or between states. These relations determine how entities communicate, collaborate, share data, and coordinate policies using digital technologies(Luna-Reyes & Gil-Garcia, 2014; Verčič et al., 2015). In the Contemporary Theory of Digitalization, digital relations are not informal or ad hoc; they are governed by frameworks, protocols, and mutual understandings shaped by law, policy, and strategy. At the state level, digital relations influence international diplomacy, cyber cooperation, regulatory alignment, and multilateral governance. At the organizational level, they define partnerships, joint platforms, digital alliances, and cross-border operational integration. Level 3 emphasizes that digital relations increasingly shape power, trust, and influence in international and institutional settings, making them a central component of modern governance and cooperation.

3.4.2 Digital Connectivity: Enabling Cross-Border Digital Interaction

Digital Connectivity is the technical and functional enabler of Level 3. It refers to the ability of organizations or states to connect to external digital networks, including the Internet, mobile networks, satellite systems, cloud platforms, and cross-border data infrastructures(Gabarró, 2020; Lynn et al., 2022). Within CToD, digital connectivity is not treated as a purely technical feature but as a strategic capability. Connectivity determines access to information, participation in global digital markets, and integration into international digital ecosystems.

3.4.3 Digital Sovereignty: Preserving Control in a Connected World

As connectivity expands, Digital Sovereignty becomes a critical concern at Level 3. Digital sovereignty refers to the right and capacity of an organization or state to exercise control over its digital assets, data, technologies, standards, and digital infrastructure(Pohle & Thiel, 2020; Robles-Carrillo, 2023). In the Contemporary Theory of Digitalization, digital sovereignty does not imply digital isolation. Instead, it emphasizes controlled openness, where organizations and states engage globally while retaining authority over key digital resources. The mother organization or sovereign state has the right to implement legal, technical, and institutional measures to protect its digital sovereignty, including data localization, technology standards, and regulatory oversight.

3.4.4 Digital Defense: Safeguarding Digital Interaction

Digital Defense represents the protective dimension of Level 3. As organizations and states interact digitally, they are exposed to cyber threats, espionage, data breaches, and digital sabotage(Pelton & Singh, 2015; Williams, 2015). Within CToD, digital defense is recognized as a legitimate right of organizations and states. It includes cybersecurity frameworks, incident response mechanisms, threat intelligence sharing, and resilience planning. Level 3 emphasizes that digital defense is not purely reactive but strategic, enabling secure participation in global digital networks without compromising safety or integrity.

3.4.5 Digital Diplomacy: Advancing Interests through Digital Means

Digital Diplomacy reflects the use of digital technologies to advance diplomatic, strategic, and institutional objectives(Bjola, 2018; Rashica, 2018). This includes online engagement, digital negotiations, public diplomacy through social media, and participation in digital governance forums. At Level 3, digital diplomacy becomes a key instrument for shaping digital norms, standards, and cooperative frameworks. The Contemporary Theory of Digitalization views digital diplomacy as both

an opportunity and a responsibility. Organizations and states must develop mechanisms to communicate effectively, manage digital reputations, and engage foreign audiences while adhering to ethical and legal standards.

3.4.6 Digital Exchange: Facilitating Value Transfer Across Borders

Digital exchange platforms may include data-sharing systems, digital marketplaces, interoperable service platforms, or secure collaboration environments(Bolatbekkyzy, 2024; Lee & Milunovich, 2023). Within CToD, digital exchange must be governed by clear rules, technical safeguards, and trust mechanisms. When organizations or states interact digitally, digital exchange platforms provide structured environments for value creation while minimizing risk. Level 3 emphasizes that such platforms must respect digital sovereignty, protect digital assets, and comply with regulatory and governance standards established at earlier levels.

3.4.7 Digital Assets: Valuation and Protection in Digital Relations

Digital Assets include data, software, algorithms, intellectual property, digital platforms, and digital identities, any digitally created or stored resource that holds value(Jackson & Luu, 2023; Toygar et al., 2013). At Level 3, digital assets become particularly vulnerable because they are exposed through external digital interactions and shared platforms. The Contemporary Theory of Digitalization stresses that organizations and states must ensure the protection, classification, and controlled sharing of digital assets when engaging in digital relations. Safeguards must be in place to prevent unauthorized access, misuse, or destruction.

4. Evidence-Based Framework for the Contemporary Theory of Digitalization (CToD)

The Contemporary Theory of Digitalization (CToD) is a multi-level, governance-oriented theoretical framework that explains how digitalization should be defined, regulated, operationalized, and interconnected within and across organizations and states in the modern digital era. Unlike technology-centric or innovation-centric models (Table 1 & 2), CToD conceptualizes digitalization as:

- A legal–institutional process
- A governance and sovereignty issue
- A rights- and obligations-based system
- A globally interconnected digital order

4.1 Empirical and Practical Justification

Evidence from global digital transformation shows that:

- Organizations fail digitally due to weak governance, not lack of technology.
- States face cyber risks due to undefined digital borders and sovereignty.
- Digital conflicts arise from absence of rules, rights, and obligations.
- Cross-border digital trade suffers from regulatory fragmentation.

Existing Models	Limitation
Technology Acceptance Models	Ignore law, sovereignty, governance
Digital Transformation Frameworks	Organization-centric, not global
Innovation & Platform Theories	Underestimate rights and security
Cybersecurity Models	Focus on defense, not governance

Table 1*: Limitation of Existing Models*

The above table 1 shows Limitation of Existing Models. CToD responds to these failures by offering a structured and staged theory. CToD fills this gap by integrating Law, Governance, Trade, Security, Rights and Diplomacy.

4.2 Evidence-Based Value Proposition of CToD

Primary Actors of Contemporary Theory of Digitalization are Governments and States, International Organizations, Universities and Research Institutes, Corporations and Digital Enterprises, and Regulatory Authorities. Whereas, secondary actors are Employees and digital users, Citizens and consumers, Civil society, and Digital platforms. The following Table 2 shows different dimensions and the value added by CToD.

Dimension	Value Added by CToD
Governance	Structured digital authority
Law	Compliance and legitimacy
Security	Defense with sovereignty
Trade	Regulated digital exchange
Rights	Human-centric digitalization
Diplomacy	Peaceful digital relations

Table 2*: Dimensions and the value added*

5. Discussion

The rapid expansion of digital technologies has fundamentally reshaped organizational structures, governance mechanisms, and global interactions(Luna-Reyes & Gil-Garcia, 2014). While existing theories of digitalization have contributed valuable insights into technological adoption, innovation diffusion, and socio-technical change, they remain insufficient to fully explain and govern the complex realities of the contemporary digital era. The Contemporary Theory of Digitalization (CToD) advances this literature by offering a comprehensive, governance-centric, and multi-level theoretical framework that responds directly to the limitations of earlier approaches. Traditional theories such as Technology Acceptance Models (TAM) and Diffusion of Innovations Theory primarily focus on user behavior, adoption rates, and perceived usefulness of digital technologies(Dearing & Cox, 2018; Marangunić & Granić, 2015). While useful at the micro level, these theories largely overlook institutional authority, legal frameworks, and cross-border digital interactions. Similarly, Digital Transformation and Industry frameworks emphasize efficiency, automation, and value creation but often treat governance, digital rights, and sovereignty as secondary or exogenous concerns(De Bem Machado et al., 2022; Misra et al., 2025). In contrast, CToD places governance, regulation, and legitimacy at the core of digitalization, recognizing that sustainable digital transformation cannot occur in the absence of structured authority and legal clarity.

Socio-technical systems theory and platform theory offer more holistic perspectives by acknowledging the interaction between technology, society, and institutions(Appelbaum, 1997; Hoffmeister & Ladd, 1944). However, these theories tend to conceptualize digitalization as an emergent or adaptive process rather than a governable and sequential one. They do not sufficiently differentiate between internal organizational digital order and external digital relations among institutions and states. CToD addresses this gap by introducing a layered progression of digitalization, distinguishing clearly between foundational governance (Level 1), operational regulation (Level 2), and inter-organizational or geopolitical digital engagement (Level 3). This structural clarity represents a significant theoretical advancement. Another critical distinction between CToD and existing theories lies in its treatment of digital sovereignty and global digital relations. Most digitalization theories remain organization-centric or domestically focused, offering limited tools to analyze digital diplomacy, digital defense, or cross-border digital exchange. CToD explicitly integrates these dimensions, recognizing that digitalization today operates within an international system shaped by geopolitical competition, legal pluralism, and transnational data flows. By doing so, CToD aligns digitalization theory with contemporary realities of digital geopolitics and international governance.

Moreover, unlike innovation-driven or market-oriented frameworks, CToD foregrounds digital rights, obligations, privacy, and security as essential components rather than compliance afterthoughts. This normative orientation enables CToD to bridge the gap between digitalization theory and international legal instruments such as GDPR, OECD Privacy Guidelines, and WTO digital trade regimes. As a result, CToD provides not only analytical value but also practical relevance for policymakers, regulators, and institutional leaders. The strength of the Contemporary Theory of Digitalization lies in its integrative and scalable design. It is equally applicable to private organizations, public institutions, and states, allowing for comparative analysis across sectors and jurisdictions. Its structured approach facilitates empirical testing, policy evaluation, and strategic planning, making it adaptable to evolving digital technologies and regulatory environments.

6. Conclusion

Earlier theories of digitalization have largely focused on technological change and organizational adaptation; the Contemporary Theory of Digitalization reconceptualizes digitalization as a governed, rights-based, and sovereignty-aware process. By systematically integrating digital borders, regulations, operations, connectivity, and global digital relations, CToD offers a robust theoretical foundation for understanding and managing digitalization in the contemporary era. As

digital technologies continue to redefine power, governance, and human interaction, CToD provides a timely and necessary framework for achieving sustainable, legitimate, and equitable digital transformation.

REFERENCES

Abbate, T., Codini, A., Aquilani, B., & Vrontis, D. (2022). From knowledge ecosystems to capabilities ecosystems: When open innovation digital platforms lead to value co-creation. *Journal of the Knowledge Economy*, *13*(1), 290-304.

Afzal, J. *Exploring the New Horizons of International Law Concerning Globalization of Economy*. Springer Nature.

Afzal, J. (2024a). Best Practice of Digital Laws and Digital Justice. In *Implementation of Digital Law as a Legal Tool in the Current Digital Era* (pp. 95-120). Springer.

Afzal, J. (2024b). *Implementation of digital law as a legal tool in the current digital Era*. Springer.

Afzal, J. (2024c). Legal challenges regarding digital operations. In *Implementation of Digital Law as a Legal Tool in the Current Digital Era* (pp. 23-45). Springer.

Afzal, J. (2025). Nomenclature of the Digital Economy and Contemporary Theory of Digitalization. In J. Afzal (Ed.), *Exploring the New Horizons of International Law Concerning Globalization of Economy* (pp. 125-146). Springer Nature Singapore. https://doi.org/10.1007/978-981-95-1312-3_9

AJUZIEOGU, U. C. (2025). Algorithmic Governance and Democratic Accountability: A Novel Framework for Constitutional Adaptation in the Digital State.

Aksoy, C. (2023). Digital business ecosystems: An environment of collaboration, innovation, and value creation in the digital age. *Journal of business and trade*, *4*(2), 156-180.

Alfarizi, B. Z., & Heryadi, D. (2024). Global Governance in the 21st Century: A Digital Trends and Transformation. *Global Local Interactions: Journal of International Relations*, *4*(1), 57-67.

Appelbaum, S. H. (1997). Socio-technical systems theory: an intervention strategy for organizational development. *Management decision*, *35*(6), 452-463.

Beaumier, G., Kalomeni, K., Campbell-Verduyn, M., Lenglet, M., Natile, S., Papin, M., Rodima-Taylor, D., Silve, A., & Zhang, F. (2020). Global regulations for a digital economy: Between new and old challenges. *Global Policy*, *11*(4), 515-522.

Bibi, P. (2024). Establishing Transparency and Accountability in AI: Ethical Standards for Data Governance and Automated Systems. In.

Bjola, C. (2018). Digital diplomacy: From tactics to strategy. *The Berlin Journal*, *32*, 78-81.

Bolatbekkyzy, G. (2024). Legal Issues of Cross-Border Data Transfer in the Era of Digital Government. *Journal of Digital Technologies and Law*, *2*(2), 286-307.

Bylund, P. L., & McCaffrey, M. (2017). A theory of entrepreneurship and institutional uncertainty. *Journal of Business Venturing*, *32*(5), 461-475.

Cabral, L. (2019). Towards a theory of platform dynamics. *Journal of Economics & Management Strategy*, *28*(1), 60-72.

Chari, S. G. (2025). Power, Pixels, and Politics: The Geopolitics of Emerging Technologies in the Digital Age. *London Journal of Research In Humanities and Social Sciences*, *25*(2), 1-99.

Chisita, C. T., Durodolu, O. O., & Ngoaketsi, J. (2021). Evaluating the processes and procedure of digitalization workflow. In *Digital Libraries-Advancing Open Science*. IntechOpen.

Chouliaraki, L., & Georgiou, M. (2022). *The digital border: Migration, technology, power* (Vol. 44). NYU Press.

Churchill, E. F., Snowdon, D. N., & Munro, A. J. (2012). *Collaborative virtual environments: digital places and spaces for interaction*. Springer Science & Business Media.

Coglianese, C., & Lehr, D. (2019). Transparency and algorithmic governance. *Administrative law review*, *71*(1), 1-56.

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305-2322.

Custers, B. (2022). New digital rights: Imagining additional fundamental rights for the digital era. *Computer law & Security review*, *44*, 105636.

Day, G. S., & Schoemaker, P. J. (2016). Adapting to fast-changing markets and technologies. *California Management Review*, *58*(4), 59-77.

De Bem Machado, A., Secinaro, S., Calandra, D., & Lanzalonga, F. (2022). Knowledge management and digital transformation for Industry 4.0: a structured literature review. *Knowledge Management Research & Practice*, *20*(2), 320-338.

Dearing, J. W., & Cox, J. G. (2018). Diffusion of innovations theory, principles, and practice. *Health affairs*, *37*(2), 183-190.

Doerr, S., & Lautermann, C. (2024). Beyond direct stakeholders: The extensive scope of societal Corporate Digital Responsibility (CDR). *Organizational Dynamics*, *53*(2), 101057.

Domorenok, E., Graziano, P., & Polverari, L. (2021). Introduction: Policy integration and institutional capacity: Theoretical, conceptual and empirical challenges. In (Vol. 40, pp. 1-18): Oxford University Press.

Dou, Y., Niculescu, M. F., & Wu, D. (2013). Engineering optimal network effects via social media features and seeding in markets for digital goods and services. *Information Systems Research*, *24*(1), 164-185.

Eriksson, J., & Giacomello, G. (2007). *International relations and security in the digital age* (Vol. 2). Routledge London.

Erkut, B. (2020). From digital government to digital governance: are we there yet? *Sustainability*, *12*(3), 860.

Fleuter, S. (2016). The role of digital products under the WTO: a new framework for GATT and GATS classification. *Chi. J. Int'l L.*, *17*, 153.

Gabarró, P. P. (2020). Digital connectivity: The infrastructure of the future.
Gatlin, K. (2024). Security Challenges in International Relations: Bridging Political Science and Economic Diplomacy.
Gradillas, M., & Thomas, L. D. (2025). Distinguishing digitization and digitalization: A systematic review and conceptual framework. *Journal of Product Innovation Management*, *42*(1), 112-143.
Gray, J., & Rumpe, B. (2017). Models for the digital transformation. *Software & Systems Modeling*, *16*(2), 307-308.
Greenstein, S. (2019). Digital infrastructure. *Economics of infrastructure investment () University of Chicago Press*.
Grinin, L. (2022). Revolutions of the twenty-first century as a factor in the World System reconfiguration. In *Handbook of revolutions in the 21st century: The new waves of revolutions, and the causes and effects of disruptive political change* (pp. 975-999). Springer.
Herath, H., Herath, H., Madhusanka, B., & Guruge, L. (2024). Data protection challenges in the processing of sensitive data. In *Data Protection: The Wake of AI and Machine Learning* (pp. 155-179). Springer.
Hiranandani, V. (2011). Privacy and security in the digital age: contemporary challenges and future directions. *The International Journal of Human Rights*, *15*(7), 1091-1106.
Hoffmeister, J. E., & Ladd, H. S. (1944). The antecedent-platform theory. *The Journal of Geology*, *52*(6), 388-402.
Holt, J., & Malčić, S. (2015). The privacy ecosystem: regulating digital identity in the United States and European Union. *Journal of Information Policy*, *5*, 155-178.
Hren, M. (2021). Understanding Standards, Regulations, and Guidelines. *Digital Transformation of the Laboratory: A Practical Guide to the Connected Lab*, 135-142.
Isaksson, A. J., Harjunkoski, I., & Sand, G. (2018). The impact of digitalization on the future of control and operations. *Computers & chemical engineering*, *114*, 122-129.
Jackson, A. B., & Luu, S. (2023). Accounting for digital assets. *Australian Accounting Review*, *33*(3), 302-312.
Jerab, D., & Mabrouk, T. (2023). The evolving landscape of organizational structures: A contemporary analysis. *Available at SSRN 4584643*.
Kagermann, H. (2014). Change through digitization—Value creation in the age of Industry 4.0. In *Management of permanent change* (pp. 23-45). Springer.
Kavanagh, C. (2022). *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?* Carnegie Endowment for International Peace.
Knell, M. (2021). The digital revolution and digitalized network society. *Review of Evolutionary Political Economy*, *2*(1), 9-25.
Laatikainen, G., & Ojala, A. (2019). Pricing of digital goods and services.
Langley, P., & Leyshon, A. (2017). Platform capitalism: The intermediation and capitalisation of digital economic circulation. *Finance and society*, *3*(1), 11-31.
Lee, J., Young, M., Krafft, P., & Katell, M. (2020). Power and technology: Who gets to make the decisions? *Interactions*, *28*(1).
Lee, S. A., & Milunovich, G. (2023). Digital exchange attributes and the risk of closure. *Blockchain: Research and Applications*, *4*(2), 100131.
Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N., & Ahlemann, F. (2017). Digitalization: opportunity and challenge for the business and information systems engineering community. *Business & Information Systems Engineering*, *59*(4), 301-308.
Li, X., Li, J., Yuan, C., Guo, S., & Wang, Z. (2022). Digital infrastructure. In *Development practice of digital business environment in China* (pp. 39-55). Springer.
Liu, Y., Esangbedo, M. O., & Bai, S. (2019). Adaptability of inter-organizational information systems based on organizational identity: Some factors of partnership for the goals. *Sustainability*, *11*(5), 1436.
Luna-Reyes, L. F., & Gil-Garcia, J. R. (2014). Digital government transformation and internet portals: The co-evolution of technology, organizations, and institutions. *Government Information Quarterly*, *31*(4), 545-555.
Lynn, T., Rosati, P., Conway, E., Curran, D., Fox, G., & O'Gorman, C. (2022). Infrastructure for digital connectivity. In *Digital towns: Accelerating and measuring the digital transformation of rural societies and economies* (pp. 109-132). Springer.
Mahajan, V., Muller, E., & Srivastava, R. K. (1990). Determination of adopter categories by using innovation diffusion models. *Journal of Marketing Research*, *27*(1), 37-50.
Malecki, E. J., & Moriset, B. (2007). *The digital economy: Business organization, production processes and regional developments*. Routledge.
Marangunić, N., & Granić, A. (2015). Technology acceptance model: a literature review from 1986 to 2013. *Universal access in the information society*, *14*(1), 81-95.
Martínez-Sánchez, A., Vela-Jiménez, M. J., Pérez-Pérez, M., & De-Luis-Carnicer, P. (2009). Inter-organizational cooperation and environmental change: moderating effects between flexibility and innovation performance. *British journal of management*, *20*(4), 537-561.
Mayer, M., & Nock, P. J. (2025). Digital fragmentations, technological sovereignty and new perspectives on the global digital political economy. *Global political economy*, *4*(1), 2-13.
Mihm, J., Loch, C. H., Wilkinson, D., & Huberman, B. A. (2010). Hierarchical structure and search in complex organizations. *Management science*, *56*(5), 831-848.
Milakovich, M. E. (2012). *Digital governance: New technologies for improving public service and participation*. Routledge.
Miller, M. L., & Vaccari, C. (2020). Digital threats to democracy: Comparative lessons and possible remedies. *The International Journal of Press/Politics*, *25*(3), 333-356.

Misra, S., Barik, K., & Kvalvik, P. (2025). Digital Sovereignty in the Era of Industry 5.0: Challenges and Opportunities. *Procedia Computer Science*, *254*, 108-117.
Mitchell, A. D., & Samlidis, T. (2021). Cloud services and government digital sovereignty in Australia and beyond. *International Journal of Law and Information Technology*, *29*(4), 364-394.
Moriset, B., & Malecki, E. J. (2009). Organization versus space: The paradoxical geographies of the digital economy. *Geography Compass*, *3*(1), 256-274.
Mugamba, E. (2025). Global Data Governance in Digital Law: A Comparative Analysis of EU and Global Approaches to Cybersecurity Legislation. *Journal of Smart Computing and Quantum Technologies*, *1*(1), 1-19.
Naudts, L. (2024). The digital faces of oppression and domination: A relational and egalitarian perspective on the data-driven society and its regulation. Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency,
Nayak, B. S., & Walton, N. (2024). The future of platforms, big data and new forms of capital accumulation. *Information Technology & People*, *37*(2), 662-676.
Omoseebi, A., Cole, W., & John, S. (2024). Compliance and Ethics: Ensure that digital initiatives comply with regulations and ethical standards.
Oraegbunam, I. K., & Onwuatuegwu, C. (2023). Addressing the challenges in the contemporary international trading system: the limitations of general agreements on tariffs trade (gatt) and general agreements on trade in services (GATS). *IJOCLLEP*, *5*, 64.
Panova, G. S., & Lengyel, I. (2022). Sector-Specific Regulation: Policy Proposals. In *The Platform Economy: Designing a Supranational Legal Framework* (pp. 271-282). Springer.
Pelton, J., & Singh, I. B. (2015). *Digital defense: A cybersecurity primer*. Springer.
Pfeiffer, S. (2021). The greater transformation: Digitalization and the transformative power of distributive forces in digital capitalism. *International Critical Thought*, *11*(4), 535-552.
Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Pohle, J. & Thiel*.
Rashica, V. (2018). The benefits and risks of digital diplomacy. *Seeu Review*, *13*(1), 75-89.
Rehman, Z. (2023). Beyond borders: International law and global governance in the digital age. *Journal of Accounting & Business Archive Review*, *1*(1), 1-12.
Rim, A. (2024). Obligations in the Digital Environment: Legal Doctrine. *Legal Issues in the digital Age*(3), 4-30.
Robles-Carrillo, M. (2023). Sovereignty vs. digital sovereignty. *Journal of Digital Technologies and Law*, *1*(3).
Rusakova, E. P., Frolova, E. E., & Gorbacheva, A. I. (2020). Digital rights as a new object of civil rights: issues of substantive and procedural law. 13th International Scientific and Practical Conference-Artificial Intelligence Anthropogenic nature Vs. Social Origin,
Sandberg, J., Holmström, J., & Lyytinen, K. (2020). Digitization and phase transitions in platform organizing logics: Evidence from the process automation industry. *MIS quarterly*, *44*(1), 129-154.
Sarma, A. (2023). *A Handbook on Cyber Law: Understanding Legal Aspects of the Digital World*. Authors Click Publishing.
Schröter, J. (2024). Analog and Digital Power. *Deleuze, Guattari and the Schizoanalysis of Post-Neoliberalism*, 93.
Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024). Navigating the regulatory landscape. In *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy* (pp. 127-240). Springer.
Sharma, S., Kumar Kar, A., & Gupta, M. (2021). Unpacking Digital Accountability: Ensuring efficient and answerable e-governance service delivery. Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance,
Shi, X., Yao, S., & Luo, S. (2023). Innovative platform operations with the use of technologies in the blockchain era. *International Journal of Production Research*, *61*(11), 3651-3669.
Siur, N., Kuzmenko, H., Pavlichenko, I., Malakhova, T., & Pravdiuk, A. (2024). Basic principles of the constitutional system of local self-government. *Multidisciplinary Reviews*, *7*.
Snow, C. C., Fjeldstad, Ø. D., & Langer, A. M. (2017). Designing the digital organization. *Journal of organization design*, *6*(1), 7.
Taherdoost, H. (2018). A review of technology acceptance and adoption models and theories. *Procedia Manufacturing*, *22*, 960-967.
Tan, E., & Crompvoets, J. (2022). A new era of digital governance. In *The new digital era governance* (pp. 13-49). Wageningen Academic.
Tarumingkeng, R. C. (2025). in the Digital Era.
Teece, D. J. (2017). Profiting from innovation in the digital economy: standards, complementary assets, and business models in the wireless world. *Research Policy (forthcoming)*.
Thomas, A. (2024). Digitally transforming the organization through knowledge management: A socio-technical system (STS) perspective. *European Journal of Innovation Management*, *27*(9), 437-460.
Toygar, A., Rohm Jr, C., & Zhu, J. (2013). A new asset type: digital assets. *Journal of International Technology and Information Management*, *22*(4), 7.
Trier, M., Kundisch, D., Beverungen, D., Müller, O., Schryen, G., Mirbabaie, M., & Trang, S. (2023). Digital responsibility: a multilevel framework for responsible digitalization. *Business & Information Systems Engineering*, *65*(4), 463-474.
Verčič, D., Verčič, A. T., & Sriramesh, K. (2015). Looking for digital in public relations. *Public relations review*, *41*(2), 142-152.
Voss, W. G. (2019). Cross-border data flows, the GDPR, and data governance. *Wash. Int'l LJ*, *29*, 485.
Wang, C., Medaglia, R., & Zheng, L. (2018). Towards a typology of adaptive governance in the digital government context: The role of decision-making and accountability. *Government Information Quarterly*, *35*(2), 306-322.
Whewell, E., Caldwell, H., Frydenberg, M., & Andone, D. (2022). Changemakers as digital makers: Connecting and co-creating. *Education and information technologies*, *27*(5), 6691-6713.

Williams, S. (2015). Digital defense: Black feminists resist violence with hashtag activism. *Feminist media studies*, *15*(2), 341-344.

Declaration

Consent to Publish: The author has agreed to publish this version of the manuscript in the International Journal of Discovery in Social Sciences (ISSN: 3105-6288).
Preprint Version: https://doi.org/10.2139/ssrn.6018858