systems

MDPI

Article

Open Source as the Foundation of Safety and Security in Logistics Digital Transformation

Mihael Plevnik [1,†] and Roman Gumzej [2,*,†,‡]

[1] Ministry of Defence, Doctrine, Development, Education and Training Command, SI-2111 Maribor, Slovenia
[2] Faculty of Logistics, University of Maribor, SI-3000 Celje, Slovenia
* Correspondence: roman.gumzej@um.si; Tel.: +386-3-428-5314
† These authors contributed equally to this work.
‡ Current address: Faculty of Logistics, University of Maribor, Mariborska Cesta 7, SI-3000 Celje, Slovenia.

Abstract: In this article, we explored how open-source software serves as a strategic enabler for safety and security in the digital transformation of logistics systems. Open source is examined across multiple dimensions, including transparency, community collaboration, digital sovereignty, and long-term infrastructure resilience. The analysis focuses on the logistics domain, where interoperability, critical infrastructure protection, and supply chain continuity are essential. Key elements of open-source development—such as modular architectures, legal and licensing frameworks, and peer-reviewed codebases—support rapid vulnerability management, increased transparency, and the creation of sustainable digital ecosystems. Emphasis is placed on the role of open-source models in strengthening institutional trust, reducing dependency on proprietary vendors, and enhancing responsiveness to cyber threats. Our findings indicate that open source is not merely a technical alternative, but a strategic decision with legal, economic, and political implications, shaping secure, sovereign, and adaptive digital environments—particularly in mission-critical sectors.

Keywords: logistics; open-source software; digital transformation; safety; security

check for updates

Academic Editor: Ben Clegg

Received: 14 April 2025
Revised: 20 May 2025
Accepted: 28 May 2025
Published: 1 June 2025

Citation: Plevnik, M.; Gumzej, R. Open Source as the Foundation of Safety and Security in Logistics Digital Transformation. *Systems* **2025**, *13*, 424. https://doi.org/10.3390/systems13060424

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In an era of accelerating digitalization—especially in logistics and supply chain environments—ensuring trust, security, and system resilience has become a strategic imperative. Digital transformation in logistics and supply chain environments represents the transition towards new approaches and technologies, based on information and communication technologies, with the aim of increasing the efficiency, transparency, security, and resilience of systems [1,2]. More broadly, digital transformation can be understood as "an ongoing socio-structural change that leverages digital technologies to create new value toward sustained competitive advantage" [3], underscoring its strategic relevance beyond technological modernization. In logistics, this implies that transformation requires not only the adoption of new technologies, but also the development of dynamic capabilities—namely, the organizational capacity to anticipate, adapt to, and reconfigure systems in response to evolving threats and opportunities [4]. While digital transformation promises efficiency and agility, it also introduces new layers of complexity and risk. Many logistics domains—such as seaports, freight hubs, and warehouse operations—show uneven levels of digital maturity and face persistent challenges in integrating secure, interoperable systems [5,6]. Frameworks such as Logistics 4.0 emphasize the role of cyber–physical systems, IoT, and AI in enabling dynamic, real-time coordination across supply chains [7]. However, without foundational transparency and control, these systems risk

becoming opaque, siloed, and vulnerable. Within this context, open-source software is emerging as a strategic enabler of digital sovereignty and cybersecurity. Built on unrestricted access to source code, peer review, and collaborative development, the open-source model enables faster identification of vulnerabilities, flexible adaptation, and sustainable lifecycle governance [8–11]. Its transparent nature supports resilient digital infrastructures and reduces dependence on proprietary technologies—an increasingly critical concern for security in logistics.

Several unique features make the logistics industry a critical context for examining the role of open-source software in digital transformation. First, it involves highly interconnected and interdependent systems, where disruptions can have cascading effects across vast geographical areas and economic sectors. Second, it relies heavily on the real-time exchange of information among diverse stakeholders, including suppliers, manufacturers, distributors, and customers, necessitating robust and interoperable communication networks. Third, the increasing automation and digitization of logistics operations, driven by technologies like IoT, AI, and blockchain, generate massive amounts of data, raising concerns about data security, privacy, and control. Finally, the global nature of modern supply chains exposes them to a wide range of security threats, including cyberattacks, counterfeiting, and terrorism, which can have significant economic and social consequences. These characteristics highlight the need for digital solutions in logistics that prioritize security, resilience, transparency, and collaboration, qualities that open-source software is well positioned to provide.

Although open-source software has long been the subject of extensive debate, the literature still lacks comprehensive analyses that frame open source as a strategic foundation of digital security within the broader context of digital transformation, especially in mission-critical environments such as logistics, where failure or compromise can cascade across systems and borders. Its impact on the long-term resilience of digital systems, legal transparency, economic sustainability, and institutional trust, particularly in the public and security sectors, remains insufficiently explored. This article addresses this gap by offering an integrated examination of open-source practices, combining technological, legal, security, and societal perspectives to provide an in-depth understanding of their role in shaping trustworthy, secure, and sustainable digital infrastructures. We address the central research question: "Does the open-source development model offer greater security and reliability for digital systems compared to proprietary approaches?" To answer this, we conducted a thorough analysis of 115 scholarly, professional, and institutional sources that address open-source practices from various theoretical, legal, economic, and security standpoints.

This article explores how open-source software contributes to the development of secure, transparent, and resilient digital environments, with special attention given to the logistics sector, and identifies key research gaps and opportunities for further advancement. In this way, we aim to deepen the understanding of open-source practices as a comprehensive model of digital transformation—one that interweaves technology, law, economics, and society in pursuit of a more inclusive and sovereign digital future.

2. Materials and Methods

The methodological framework of this article is based on a combined analytical approach that reflects the complexity of the literature on open-source practices in the context of digital transformation and security. The review incorporates thematic content classification, chronological mapping, and multi-perspective analysis to capture the diverse roles of open-source software across logistics, governance, cybersecurity, and institutional domains. To investigate the strategic role of open-source software in secure digital transformation, we selected a narrative literature review as the most appropriate method. Given

the conceptual and interdisciplinary nature of the research question—how open-source software contributes to safety and resilience in logistics systems—this approach enabled the synthesis of diverse theoretical, legal, technical, and institutional sources. Unlike systematic reviews, which are oriented toward narrowly scoped empirical questions, the narrative method supports interpretive and critical engagement with heterogeneous literatures, aligning with the article's objective to evaluate both conceptual foundations and practical implications. We employed a structured search strategy using major academic databases: Scopus, Web of Science, IEEE Xplore, SpringerLink, ScienceDirect, JSTOR, and Google Scholar. The search was restricted to publications in English, covering the period from 2000 to 2024, with the inclusion of specific foundational works published before 2000, such as Cameron and McCormick [12], Winner [13], and Clift [14]. The following Boolean string was used in various combinations to reflect the interdisciplinary scope of the research: ("open source" OR "open-source software") AND ("digital transformation" OR "digitization") AND ("logistics" OR "supply chain") AND ("security" OR "cybersecurity" OR "resilience" OR "infrastructure protection"). Additional thematic refinements included legal terms ("licensing", "intellectual property", "GPL"), institutional use ("public sector", "government"), and defense-related keywords ("military systems", "national security"). Inclusion criteria prioritized peer-reviewed articles, institutional reports, and relevant conceptual or empirical studies addressing open-source software in relation to logistics, cybersecurity, digital sovereignty, or regulatory mechanisms. Exclusion criteria eliminated purely technical software development papers lacking strategic, legal, or operational context. The review integrated 115 sources, grouped into analytical clusters and development phases to ensure thematic consistency. To ensure transparency in the literature selection process, we adapted a PRISMA-style protocol to document the identification, screening, eligibility assessment, and final inclusion of sources. The initial search across academic databases yielded 356 records, with an additional 28 identified through manual citation tracking and institutional repositories. We used a custom Microsoft Access database to record and manage all references, including metadata such as author, year, topic, publication type, and thematic relevance. Relational constraints removed duplicate records (n = 54). We screened titles and abstracts of the remaining 330 sources, excluding 178 non-relevant or overly technical entries. Full-text reviews were conducted for 152 sources, of which 37 were excluded due to lack of peer review, conceptual redundancy, or insufficient analytical value. The final dataset comprised 115 sources, which were subjected to qualitative coding and thematic synthesis. To ensure analytical rigor, each source was assessed across three quality dimensions:

- Validity: Methodological transparency, theoretical grounding, peer-reviewed status;
- Reliability: Institutional affiliation, publication reputation, corroboration with the existing literature;
- Relevance: Direct contribution to the research themes (e.g., open source in logistics security).

The analytical framework of the study is structured around seven complementary analytical procedures applied to the reviewed literature: (1) thematic content analysis, (2) chronological mapping, (3) methodological assessment, (4) theoretical framing, (5) problematization, (6) discourse analysis, and (7) institutional analysis. The synthesis and analysis phase relied on thematic coding and qualitative clustering. We classified the literature into eight thematic clusters: (1) theoretical and conceptual foundations of open source; (2) digital transformation of logistics and open-source applications; (3) legal and licensing dimensions; (4) economics and business models of open-source solutions; (5) open source and digital security; (6) open-source practices in defense and public administration; (7) users, communities, and participation; and (8) open source, digital sovereignty, and democratization. Each thematic cluster aggregates and interprets content in direct rela-

tion to the central research question. The synthesis process built on the prior analytical steps and drew specifically on discourse analysis, institutional comparison, and problematization, enabling multidimensional interpretation. These interpretations were further supported by relevant theoretical frameworks, including co-creation, collective action, and legal-institutional theory. This integrated approach ensured both interpretive depth and analytical coherence, grounded in conceptually robust and context-sensitive critique.

3. Results

This section synthesizes findings from the thematic content and chronological analyses, enriched by methodological, theoretical, problematization, discourse, and institutional perspectives. The review of over one hundred scholarly, professional, and institutional sources identified key dimensions of open-source practices within digital transformation. Our findings reveal open source as a multifaceted phenomenon encompassing social, legal, security, and political dimensions, rather than a one-dimensional technological model. To provide a framework for understanding how open-source software, as a strategic enabler, addresses the research question of security and reliability in digital systems, the results are presented in a structured format. This structure enables a deeper interpretation of open-source practices as foundational elements in building trustworthy, sustainable, and sovereign digital infrastructures, particularly within the logistics sector, where the diverse impacts of open source on digital transformation are illustrated.

3.1. Thematic Content Analysis

Thematic categorization of the literature, which spans social theory, legal frameworks, security mechanisms, institutional practices, and defense strategies, enables a comprehensive and systematic examination of the diverse dimensions of open-source practices and their significance in digital transformation. This approach identifies research emphases, recurring themes, and divergences in approaches to open-source development. A prominent group of contributions establishes a theoretical and conceptual framework for understanding open-source development not merely as a technical model, but as an embodiment of broader values such as collaboration, transparency, community-driven regulation, and digital autonomy [11,15,16]. These authors view open-source development as a disruptive innovation model that, through institutional mechanisms of self-regulation, transparency, and collective knowledge, facilitates a secure, sustainable, and trustworthy digital transformation [17,18]. Theoretically, the open-source model demonstrates institutional resilience and strategic adaptability through modularity, community-driven peer review, and broad user participation, supporting robust and flexible digital systems and offering a more objective and stable security paradigm rooted in transparency and collaboration [12]. Diverse user approaches and the technological flexibility of open-source solutions further contribute to the development of inclusive and sustainable digital environments [19]. These contributions commonly understand open source as more than just a technical development model, but as an epistemological, legal, cultural, and political framework that enables the emergence of alternative modes of organizing and safeguarding digital systems, contributing not only to technical efficiency and innovation but also to the establishment of socially responsible, transparent, and resilient digital environments.

A distinct thematic group within the reviewed literature highlights the role of open-source software in the digital transformation of logistics and supply chain systems, emphasizing that open-source approaches constitute a strategic foundation for enhancing transparency, resilience, and long-term control over digital infrastructures—especially in mission-critical environments [20–23]. These contributions underscore open source's capacity to strengthen system security and reliability through publicly auditable code and

reduced vendor lock-in, promoting digital sovereignty in complex logistics environments, where operational flexibility and autonomy are paramount. From an institutional perspective, open-source models are increasingly seen as essential to managing cyber risks and ensuring the continuity of digital operations within supply chains, with governmental agencies like the Cybersecurity and Infrastructure Security Agency [8] recognizing open-source components as integral to resilient federal IT architectures, including logistics systems. The literature also identifies key architectural principles—such as modular design and interoperability [24,25]—as central to deploying open-source systems in logistics, supporting fast, secure communication and decision making. What unites these contributions is the recognition that open-source models offer a normative and strategic framework for shaping sovereign, robust, and ethically grounded logistics infrastructures as digital transformation accelerates.

A significant portion of the reviewed literature focuses on the legal and licensing aspects of open-source practices, with authors emphasizing the role of legal mechanisms as fundamental in ensuring transparency, accountability, and the long-term sustainability of open source [26–28]. These contributions demonstrate that legal regulation plays a constitutive role in shaping the open-source ecosystem as a trustworthy digital infrastructure, ensuring security, stability, and trust within digital transformation processes [29–31]. The deliberate selection of legal and institutional frameworks, including licensing, directly impacts the long-term stability and security of open-source solutions in security-sensitive contexts, while open source offers an alternative to traditional patent systems, which frequently hinder innovation [32,33]. A common theme across these contributions is the recognition of legal and licensing frameworks as key factors in ensuring the security and trustworthiness of open-source solutions, shaping stakeholder relationships and enabling transparent and accountable distribution of software. Independent code auditability, traceability of changes, and the potential for broad collaboration contribute to a well-founded trust in such solutions [34–36].

At the heart of the discourse on open source lies its economic rationale and business viability, with contributions highlighting that open source is not merely an alternative technical model but also a distinctive form of value creation and innovation [1,2]. Open-source solutions represent a significant economic alternative by promoting transparency and reducing transition costs, enabling the development of sustainable digital platforms [37,38]. The long-term sustainability of open-source software depends on positive user experiences and network effects [39–42]. Hybrid business models that combine open-source and proprietary elements allow companies to harness the advantages of open source while retaining existing systems [43–45]. These open-source strategies are reshaping competitive dynamics in the software industry as companies increasingly create value through integration and support [46–48]. A shared conclusion is that open-source approaches foster the emergence of alternative, more flexible, and collaborative business models, empowering companies with greater autonomy and faster innovation.

Security in digital transformation through open source is enabled by its transparency, modularity, and community-driven development, contributing to more reliable digital system security through open standards and transparent vulnerability management [49–52]. Tools like SBOM and static code analysis support scientifically grounded security management [9,53,54]. Open approaches also enable the development of reliable architectures in security-critical environments [55–57]. Developer communities that are both internally organized and connected to broader networks improve the security, adaptability, and long-term reliability of open-source solutions [58]. Open infrastructures prove particularly effective for managing the complexity inherent in modern digital ecosystems, offering targeted complexity management, transparent interconnections, and the repeatable use of

trusted building blocks [59–61], and enhancing resilience, transparency, and responsiveness during crises [62]. However, open source requires continuous support through verification and maintenance [63–66]. While not a guarantee of automatic security, open source necessitates transparent update processes and community auditing [10,20,67,68]. A key conclusion is that in the context of security, open source is a strategic decision demanding alignment between technical standards, legal regulation, institutional support, and community engagement.

A significant body of literature addresses the application of open-source approaches in sectors where security and technological control are critical, such as defense and public administration [69,70]. These contributions show that open source enhances digital sovereignty and improves responsiveness, offering public institutions greater control and reduced vendor lock-in [71]. Open-source practices promote transparency and accountability, contributing to more traceable and reliable infrastructure [72,73]. Strategic initiatives recognize open-source software as a cornerstone of secure and sustainable infrastructure in the public sector [8,74]. A unifying insight is that open-source software is a strategic instrument for strengthening sovereignty and long-term control over digital infrastructure in these critical sectors.

A particularly significant area of research concerns the role of users, communities, and participatory mechanisms in open-source development, emphasizing it as a broader social process rooted in voluntary participation and collective learning [75–77]. The effectiveness of open-source communities is built on collaboration and trust [78,79]. Peripheral developers facilitate rapid vulnerability detection [80]. User perception and an active community-based security culture are vital [81,82]. Long-term project sustainability hinges on social mechanisms like inclusivity [83,84]. Active participation is driven by shared intentions and a sense of belonging [85,86]. This literature understands the open-source community as a complex social system based on voluntarism and collaboration, underpinned by mechanisms ensuring quality and security, strengthening trust and long-term stability.

The final thematic cluster explores open source as a key driver of digital sovereignty and democratization [87,88]. By promoting decentralization and transparency, it creates conditions for the democratization of digital infrastructure [13,89]. Open source in education and research ensures transparency and accessibility [90–92]. It contributes to greater autonomy and reduces centralized control over information [93–95]. Open data and open-source software support digital democracy [96,97]. In this way, open-source approaches create the conditions for digital sovereignty and foster ethically grounded, transparent, and collaborative digital ecosystems—paving the way for a sustainable and democratic digital future [98,99]. However, transparency alone is not sufficient; open-source approaches also require institutional mechanisms for oversight, responsiveness, and participation in order to meaningfully advance digital security, accountability, and sovereignty [100–102]. F/OSS developer communities also play a crucial role through legal activism [103]. At the global level, open-source approaches enhance the resilience and strategic influence of the digital environment [104,105]. The overarching conclusion is that open source is not merely a technical tool but a carrier of political, ethical, and institutional values, emerging as a fundamental means of asserting digital sovereignty and establishing alternative models of managing digital infrastructure.

In conclusion, the thematic content analysis provides a multilayered understanding of open-source practices, spanning theoretical foundations to concrete applications. Open source increasingly transcends its technical definition, emerging as an analytical framework for examining core issues of digital transformation, including transparency, collaboration, digital sovereignty, and system resilience. The interconnectedness of legal mechanisms, security concerns, business models, political governance, and community involvement is

evident. This is particularly relevant in domains such as logistics, where the institutional integration of open-source technologies enhances interoperability and resilience. Open-source development is not merely an alternative model of software production but a structured and increasingly institutionalized approach to shaping secure, sustainable, and inclusive digital ecosystems.

3.2. Chronological Analysis

Spanning from the early 1990s to 2024, the development of open-source software reveals a significant evolution in its understanding and application. Initially conceived as an ideological movement centered on software freedom and collective creation, open source has progressively undergone institutionalization within industrial, governmental, and defense contexts, transitioning from an alternative approach to a strategically embedded component of digital infrastructure. To better understand this trajectory, the literature can be organized into four phases reflecting the developmental logic of open-source practices: the foundational phase (1990–2005); the industrial adoption phase (2005–2015); the governmental and defense integration phase (2015–2020); and the contemporary phase (2020–2024), raising questions of security and sustainability.

Between the early 1990s and mid-2000s, open-source software evolved from an ideologically driven initiative into a globally recognized development model rooted in the belief of universal source code accessibility to promote transparency and collaboration. This period saw the establishment of the legal and organizational foundations of the open-source movement, including the development of licenses like the GPL and the emergence of pivotal projects such as Linux and Apache [15,16,103]. Early theoretical contributions highlighted "peer production" as an alternative to market-based hierarchies, facilitating efficient knowledge sharing and enhancing digital system resilience, while also framing open-source development as a political and legal practice shaping interpretations of freedom and digital sovereignty. This formative stage established open source as an ethical infrastructure with security, political, and social implications, where security was understood through transparency and legal predictability, laying the groundwork for its subsequent institutionalization in both public and private sectors [17].

The period between 2005 and 2015 witnessed open source's transformation from an ideological movement to a broadly accepted practice within business and institutional environments, marked by a new equilibrium between market interests and community values [44,71,106]. No longer just an alternative to proprietary software, open source was increasingly recognized as a strategic resource for innovation and cost efficiency, facilitating its integration into diverse systems. Empirical studies highlighted the adoption of hybrid business strategies combining open-source and proprietary components, driven by factors like switching costs and network effects, while open source also gained prominence in information security through the emergence of open standards and tools, enhancing transparency and trust. This phase also saw continued debate on open source's role in the public sector's digital transformation, where its adoption fostered digital autonomy, particularly for developing nations, marking a shift from ideological to institutional acceptance, with technical and normative openness merging with economic pragmatism, firmly anchoring open source at the core of digital infrastructure.

The period from 2015 to 2020 marked a significant shift in the application and understanding of open source within governmental, security, and defense contexts, with it increasingly being treated as a strategic factor tied to national security and digital sovereignty [24,100,107]. The emergence of the Modular Open Systems Approach (MOSA) in the defense sector, built on openness and standardized interfaces, enabled faster technology integration and reduced vendor lock-in. Beyond defense, open source gained traction

across the public sector as a tool for achieving digital sovereignty, with agencies like the Cybersecurity and Infrastructure Security Agency [8] actively promoting open-source security standards. The strategic importance of open source also grew within diplomacy and international relations, becoming embedded in national digital agendas. This period signifies a shift in perspective from open source as a tool to recognizing it as strategic infrastructure, formalized and integrated into national planning as a core component for ensuring the resilience and independence of digital systems, explicitly linking security and interoperability to open development practices.

The period following 2020 has been characterized by rapid shifts in digital security, raising new questions about the resilience of open-source approaches and the ethical responsibility of its maintainers [9,67,108]. High-profile security incidents like Log4Shell exposed the vulnerabilities within critical open-source components reliant on volunteer labor with limited oversight. In response, institutional initiatives like the Cybersecurity and Infrastructure Security Agency have placed emphasis on a systemic approach, including SBOM, aiming to enhance transparency and accountability in the software supply chain [8]. Debates about responsibility and sustainability have intensified, alongside the ethical and political implications of companies benefiting from open source without adequate contribution [47]. A growing need for new forms of open-source governance integrating legal, ethical, and security standards is emerging, advocating for hybrid models involving communities, the public sector, and industry to ensure the robustness of digital solutions. This contemporary phase represents a moment of reflection and restructuring for open source to preserve its core values while ensuring systemic resilience in an increasingly complex digital environment.

The chronological analysis clearly illustrates the evolution of open-source practices from ideologically driven beginnings to strategically oriented operations, with each phase reflecting distinct priorities and challenges. The discourse surrounding open source has transformed from a marginal alternative to a central component of modern digital strategies, closely tied to sovereignty and resilience. However, the analysis also highlights that openness alone does not guarantee security, underscoring the necessity of robust institutional mechanisms and long-term support structures for a trustworthy digital future, particularly evident in the strategic integration of open-source frameworks within logistics and supply chain systems to enhance transparency and security.

3.3. Methodological Approach

The reviewed literature on open-source practices exhibits a pronounced methodological diversity, reflecting its multidimensional nature at the intersection of technology, law, economics, and society, with authors employing a wide array of research approaches for a comprehensive understanding. Some contributions utilize qualitative case studies to explore concrete examples of open-source implementation within institutional settings, such as Chan's [109] examination of a Peruvian legislative initiative applying open-source principles in public administration and Castelli's [24] analysis of MOSA adoption in the defense sector, providing insight into structural and contextual factors shaping practical use. Another set of contributions employs quantitative empirical analyses to test hypotheses about user, company, and community behaviors, exemplified by Bagozzi and Dholakia's [85] statistical examination of motivational factors in open-source communities and Lerner and Tirole's [39] modeling of the economic logic behind development model choices, supporting comparative and systematic analyses of open-source ecosystems.

A significant portion of the literature adopts a conceptual and theoretical approach, developing new frameworks for understanding open source as an institutional practice, including Benkler's [15] theory of "peer production" and Coleman's [103] ethnographic and

legal-theoretical work framing open-source communities as carriers of legal and political significance. Many contributions also engage in policy analysis, legal interpretation, and organizational case reviews, particularly concerning institutional documents and strategic reports, such as the Cybersecurity and Infrastructure Security Agency's [8] cybersecurity guidance and Couture's [100] historical overview of the FOSS movement, shedding light on the relationship between open-source solutions and state regulation, institutional resilience, and digital governance frameworks. This methodological diversity is a key strength, enabling a layered and holistic examination of open-source practices as not merely a technical phenomenon but also a social, legal, and political one, requiring interdisciplinary research sensitivity. Such a comprehensive methodology proves particularly valuable in domains like logistics, where technological decisions intersect with regulatory frameworks and institutional accountability, providing a more accurate assessment of how open-source models function in critical environments by incorporating legal analysis and institutional comparison.

3.4. Theoretical Approach

The reviewed literature approaches open-source practices through diverse theoretical frameworks, enabling a nuanced understanding of this multilayered phenomenon within technical, organizational, social, legal, and political contexts. One influential foundation is Benkler's [15] theory of "commons-based peer production", which posits open-source development as a result of voluntary, decentralized collaboration independent of traditional hierarchies, emphasizing distributed knowledge and community dynamics. Theories of "collective action" and "social capital" by Bagozzi and Dholakia [85] explain how identity and community shape individuals' voluntary contributions, crucial for the reliability of open-source communities. Institutional theory, as seen in Kologlugil [17] and von Krogh et al. [18], views open source as embedded within broader frameworks shaping digital norms and legitimacy, understanding open architecture as an institutional innovation influencing organizational resilience.

Theories of innovation also play a prominent role, particularly regarding open source's disruptive effects on markets, with von Krogh and von Hippel [16] highlighting user-driven innovation and collaboration as sources of competitive advantage. Legal-theoretical approaches, such as in Coleman [103] and Carver [110], interpret open source as a form of legal and political expression, with Coleman's "jurisgenesis" framework explaining how open-source communities actively shape legal meaning through code development. These theoretical approaches collectively recognize open source as a structural and ideological mechanism shaping digital space, power dynamics, and our understanding of trust and security. This theoretical diversity enriches our comprehension and invites interdisciplinary reflection, particularly applicable in logistics where open-source adoption affects infrastructure control and transparency, influencing the resilience and ethical structure of data-driven systems.

3.5. Problematization Analysis

A key dimension of the analyzed literature focuses on identifying specific problems and challenges that open-source approaches aim to address across diverse contexts, connecting openness as a development model with the mitigation of concrete risks in digital environments. One central issue is transparency and trust, with authors emphasizing the ability to look into the workings of software with open source, enhancing user trust in critical environments, where a lack of transparency is associated with security vulnerabilities and vendor lock-in [8,9,103]. Interoperability and standardization are also frequently highlighted, with open standards facilitating system integration and enhancing resilience in fragmented digital environments [8,67].

Vulnerability management is another recurring theme, examining open source in terms of response speed and community engagement, particularly critical when essential components rely on under-supported volunteers [108,111]. Digital sovereignty and technological dependency are also emphasized, framing open source as a means of reducing reliance on closed-source solutions, enabling greater control over technology and data [96,100,109]. From an ethical perspective, the literature raises questions about conflicts of interest and inequality, noting the paradoxes of openness, where actors may exploit open-source solutions without contributing, prompting calls for reflection on participation rules and governance [47,112].

Problematization analysis highlights open source as a targeted response to systemic challenges like opacity and vendor lock-in, positioning it as a practical mechanism for mitigating structural risks and enhancing digital resilience, particularly pertinent in the logistics sector for creating secure and transparent supply chains.

3.6. Discourse Analysis

Discourse analysis of the reviewed literature reveals that "open source" is not a singular concept but a polysemous category carrying diverse meanings and ideological projections across research and institutional contexts. Authors and organizations define open source in ways that reflect specific interests and interpretations of technological openness as a social phenomenon. In some works, particularly institutional documents like the Cybersecurity and Infrastructure Security Agency reports [8], open source is framed as a technical solution aimed at improving software quality and security, rationalized and integrated into existing governance structures. Conversely, authors like Benkler [15] and Coleman [103] interpret open source as a political project expressing freedom and resistance to centralized control, where code symbolizes decentralization and sovereignty, a counterforce to corporate dominance.

Other contributions emphasize open source as a community practice focused on collaboration and informal organization [83,84], where social dynamics are central. A critical discourse, found in works by Couture [103] and Birkinbine [47], highlights the risks of commodification, where openness is co-opted by corporate strategy without genuine community adherence. This plurality of interpretations shows open source as a discursive field intersecting technical, political, legal, and ethical perspectives, ranging from an optimization solution to a liberating practice. Acknowledging this is crucial for policy design, as it implies open-source solutions are context-dependent and shaped by discursive frameworks. Discourse analysis thus helps understand open source as a culture and ideology reflecting societal values, significant in domains like logistics where terms like "interoperability" carry institutional weight, and the language, used to justify open-source adoption, reflects priorities like security and trust.

3.7. Institutional Analysis

Institutional analysis of the reviewed literature reveals open source as increasingly a matter of institutional decision making and strategic positioning, involving government bodies, military organizations, corporations, NGOs, and academic institutions. Public authorities often adopt open source for cost efficiency and digital sovereignty, as seen in Peru [109] and Brazil [107], although this requires long-term commitment [100]. In defense and security, open source enhances interoperability and sustainability [14,24], exemplified by MOSA, with the Cybersecurity and Infrastructure Security Agency [8] highlighting the need for institutional capacities in managing associated security risks.

In the private sector, technology companies use open source for hybrid business models and ecosystem influence [44,106], though concerns about power asymmetry exist [47].

Communities and civil society are key drivers through project maintenance and norm establishment [84,103], with academic institutions contributing through research [39,113]. Open source operates at the intersection of formal and informal institutions, with its success depending on aligning goals and cooperation, emerging as an institutional infrastructure requiring balance between community autonomy and strategic interests.

The literature reveals open source as a complex phenomenon embedded in strategic debates about the digital future, evolving as a technological practice impacting security and innovation, and as a bearer of co-creation values like transparency and trust. Key research areas include legal regulation, business models, security, and institutional integration. The diverse methodologies and theoretical frameworks confirm open source's multidimensional character as a foundational tool for secure and inclusive digital infrastructure, particularly relevant in logistics, where data exchange and interoperability are essential, making it a critical area for further research into high-stakes environments.

3.8. Summary of Results

The reviewed literature demonstrates that open-source development is more than a technical paradigm; it is a complex institutional, legal, economic, and social phenomenon increasingly central to strategic debates about the digital future. The thematic and chronological review shows open source evolving along two lines: as a concrete technological practice with tangible impacts on digital systems' security, efficiency, and innovation; and as a carrier of values like transparency, collaboration, autonomy, and digital justice. Key research focal points include legal regulation and licensing, sustainable business models, the link between openness and digital security, and the integration of open-source solutions into defense and institutional systems. The literature uses diverse methodological approaches and theoretical frameworks, confirming open source's multidimensional character as both a research subject and a strategic instrument.

Clearly, open-source models are more than an alternative to proprietary software; they are foundational for building a more secure, resilient, and inclusive digital infrastructure. This is particularly relevant in logistics, where secure data exchange, system interoperability, and operational continuity are essential to mission success. The intersection of legal certainty, economic sustainability, and technological transparency is especially pronounced in this domain, making logistics a critical area for further empirical and policy-oriented research into open-source applications within high-stakes, mission-critical environments.

4. Discussion

The thematic and chronological analyses demonstrate that open-source software is more than a technical approach to software development. In the context of digital transformation—including that of logistics systems and supply chain operations—it is a multidimensional phenomenon with legal, organizational, security, economic, and political dimensions. The literature indicates that open source fosters collaboration, drives innovation, and reduces dependency on proprietary solutions, while also raising questions about responsibility, sustainability, and institutional support. Within digital sovereignty frameworks, open source is increasingly seen as a strategic response to geopolitical and technological challenges. Public and defense sector examples illustrate how open architectures enable greater operational independence and improved control over digital assets. Consequently, open source is increasingly used to advance political objectives like transparency, participation, and the decentralization of power. However, successful open-source implementation requires coordinated institutional backing, long-term strategic planning, and a view of openness as an organizational principle, not just a technical feature.

The diverse theoretical perspectives outlined in this study provide a robust framework for understanding how open-source principles can be applied to address the unique challenges and opportunities within the logistics sector. These theoretical perspectives connect to the practical applications of open-source in logistics as follows.

- Peer production and logistics collaboration: Benkler's [15] theory of peer production emphasizes decentralized collaboration and knowledge sharing. In logistics, this translates to the development of open-source platforms for supply chain management, where various stakeholders (suppliers, distributors, customers) can collaboratively contribute to and benefit from shared information and resources. For example, open-source platforms for tracking goods or managing inventory can facilitate real-time visibility and coordination across supply chains, enhancing efficiency and reducing costs.
- Institutional theory and logistics governance: Institutional theory, which highlights the role of norms, rules, and governance structures, is crucial for understanding the adoption of open source in logistics. As logistics increasingly relies on digital infrastructure, open-source solutions need to be embedded within clear legal and regulatory frameworks to ensure accountability, security, and trust. For instance, open-source licenses and standards can establish guidelines for data sharing, interoperability, and cybersecurity practices within the logistics ecosystem [17,40,41].
- Collective action and logistics communities: Theories of collective action and social capital [85] underscore the importance of community engagement and user participation. In logistics, this is evident in the formation of industry-specific open-source communities that collaborate on developing and maintaining software solutions tailored to their needs. These communities can foster innovation, drive the adoption of best practices, and provide mutual support, leading to more resilient and adaptable logistics systems.
- Innovation theory and logistics agility: Von Krogh and von Hippel's [16] work on open source as a driver of disruptive innovation is highly relevant to logistics, which requires agile and responsive solutions to manage disruptions, changing market conditions, and emerging technologies. Open-source software can accelerate the development and deployment of innovative logistics applications, such as predictive analytics tools, autonomous delivery systems, and blockchain-based supply chain platforms.
- Legal-theoretical approaches and trust in logistics: Legal-theoretical perspectives on open source, as seen in Coleman [103] and Carver [110], highlight the importance of legal frameworks in shaping trust and security in digital environments. In logistics, where the integrity and reliability of information are paramount, open-source licenses and legal mechanisms can ensure transparency, accountability, and compliance with regulations. This is crucial for building trust among stakeholders and facilitating seamless data exchange across complex logistics networks.

By connecting these theoretical perspectives to practical applications, we can see how open-source principles can address key challenges and opportunities in the logistics sector, leading to more efficient, secure, and resilient supply chains.

The literature indicates that open-source software presents a compelling economic alternative to proprietary models, offering several potential benefits for the logistics sector. Increased transparency, greater stability, and enhanced freedom of choice are some of these benefits, potentially leading to reduced transition costs and stronger user commitment [2]. In the logistics industry, where supply chains are often complex and involve numerous stakeholders, these factors can be particularly significant.

Open-source solutions, with their carefully designed architecture, can lower both risk and coordination costs, facilitating the development of sustainable digital platforms in

the long run [1]. This is crucial for logistics operations that require reliable and enduring digital infrastructures. Furthermore, when coupled with professional services, open-source approaches enable businesses to build robust and scalable systems [38]. This combination is relevant in logistics, where companies may require external support to implement and maintain open-source solutions effectively.

Moreover, open models and technologies can optimize knowledge and processes within logistics service networks, contributing to greater efficiency, adaptability, and organizational resilience [37]. This is particularly important within the dynamic and often unpredictable logistics environments, where organizations need to respond quickly to disruptions and changing market conditions. The long-term sustainability of open-source software in logistics depends on positive user experiences and network effects, which can foster the development of secure and technologically sovereign digital solutions [42].

Economic incentives, personal motivation, and community collaboration drive the development of high-quality, transparent, and stable digital solutions within open-source models [40,41]. This model can be especially attractive to logistics businesses, as it allows for collaboration without compromising competitive advantage, ultimately fostering the development of adaptable and trustworthy digital systems [48]. For example, companies can collaborate on developing open-source platforms for tracking goods or managing inventory, while still competing on service quality and other value-added offerings.

Hybrid business models, which combine open-source and proprietary elements, offer a pragmatic approach for logistics companies. These models allow businesses to leverage the developmental, infrastructural, and security advantages of open source while retaining their existing closed systems [44]. This strategy can help logistics firms reduce their dependence on proprietary vendors and enhance their innovation capacity, fostering the emergence of market-oriented and resilient digital ecosystems [43,45].

Open-source technological platforms, by promoting innovation and reinforcing network effects, support the development of open digital infrastructure that encourages broader participation and well-being within the logistics sector [114]. Digital transformation based on open-source solutions enables a shift from a production-centric to a service-oriented ecosystem, where free code is complemented by paid services, enhancing the global competitiveness of logistics businesses [115].

These open-source strategies are reshaping competitive dynamics in the logistics industry, as companies increasingly create value through integration, support, and related services, while open access to source code enhances the quality and resilience of their digital systems [46]. The case of Microsoft, which has transitioned from closed-source to hybrid software vendor, supporting open-source development, illustrates a broader recognition of the economic efficiency of open models, which offer greater interoperability, security, and agility than traditional proprietary approaches [47]. This shift is relevant to logistics, as it demonstrates the growing recognition that open-source can drive efficiency and innovation.

In summary, open-source approaches foster the emergence of more flexible and collaborative business models, which can be more resilient to changes in the technological landscape. In the context of logistics, this means that open source is not merely a technical decision but a strategic business direction, empowering companies and organizations with greater autonomy, faster innovation, and reduced dependency on centralized solutions. Further research could explore the specific economic impacts of open-source adoption in different segments of the logistics industry, such as warehousing, transportation, and supply chain management.

4.1. Novel Contributions of This Synthesis

This article offers several novel contributions to the understanding of open-source software, particularly in the context of digital transformation and logistics. First, it synthesizes a wide range of interdisciplinary literature, spanning technology, law, economics, and social science, to provide a holistic view of open-source practices. This approach moves beyond the primarily technical or legal perspectives that have often dominated previous discussions. Second, the article develops a framework that highlights the multidimensional nature of open source, demonstrating its relevance not only for technological advancement but also for addressing key challenges in security, governance, and institutional trust. By applying this framework to the logistics sector, the study elucidates how open-source principles can be leveraged to enhance the resilience, security, and efficiency of complex supply chain ecosystems. Finally, the article identifies several key research gaps, offering a roadmap for future inquiry into the long-term sustainability, governance, and ethical dimensions of open-source solutions in an increasingly interconnected and automated world.

4.2. Significance of Findings, Research Gaps, and Limitations

The analysis confirms that open-source software represents a foundational component of modern digital transformation—particularly in domains that prioritize transparency, sovereignty, and security. Open-source practices significantly influence how digital systems are governed, how information risks are managed, and how institutional resilience is achieved. In sectors such as public administration, digital infrastructure, and defense, this marks a shift away from centralized, proprietary control models toward more open, collaborative, and adaptive frameworks.

Despite the relevance of these findings, several limitations of the study also highlight important research gaps. The analysis relies predominantly on English-language secondary sources, which may exclude valuable regional and non-English-language perspectives. It does not include primary empirical data, case studies, or technical evaluations—such as source code audits or penetration testing—which limits the ability to validate specific claims about the comparative security or cost-efficiency of open-source versus proprietary software. Future research should therefore include longitudinal and technical assessments, particularly in mission-critical environments, where compliance, reliability, and resilience are paramount.

The diverse and decentralized nature of open-source ecosystems presents another challenge. These systems differ in licensing models, governance structures, development cultures, and institutional roles. While this study addressed representative cases, it did not examine localized, niche, or experimental projects. Furthermore, the growing involvement of commercial actors in open-source development raises questions about how corporate strategies affect community cohesion, transparency, and long-term project sustainability. The tension between commercial appropriation and community values remains insufficiently explored.

Adoption of open-source technologies by public and defense institutions is well documented in strategic and policy terms, but the internal organizational dynamics of this adoption, i.e., how decisions are made, how cultural or bureaucratic resistance affects implementation, and how national or institutional digital strategies shape open-source uptake, is less understood. Moreover, broader issues of governance—such as legal liability, ethical oversight, and accountability mechanisms within open-source ecosystems—are under-theorized, particularly in the context of high-risk or regulated domains.

Security within open-source development communities is often assumed to be enhanced by transparency and collective scrutiny, yet few studies empirically examine how

practices like peer review, automated testing, or community-driven bug resolution actually affect security outcomes. Legal and ethical accountability in the event of a security breach remains largely unresolved, particularly where responsibility is diffused across contributors, maintainers, and institutional users.

The review also faces limitations in temporal coverage. Although it spans the literature from the 1990s to 2024, the pace of technological change—especially in cybersecurity, AI integration, and regulatory development—means that some recent incidents or shifts may not yet be captured in peer-reviewed sources. This raises questions about the timeliness of some findings and highlights the need for continuous literature monitoring.

Additionally, while the study includes a variety of theoretical and critical sources, much of the existing literature frames open source in a normative and optimistic light. Although this work intentionally included contrasting views, some risks and structural weaknesses—such as governance failures, inconsistent support, or fragmentation—may be under-represented. Balanced and interdisciplinary approaches are needed to explore both the strengths and vulnerabilities of open-source models, especially as they become embedded in critical infrastructure.

In effect, these findings validate the strategic importance of open-source approaches for digital transformation and resilience, while also identifying key areas for further investigation. Future research should integrate technical, legal, organizational, and societal perspectives to ensure that open-source systems not only offer openness and accessibility but also meet the demands of security, accountability, and long-term sustainability. These issues are particularly relevant for the logistics sector, where digital transformation depends on infrastructures that are secure, interoperable, and resistant to disruption across complex supply chain networks.

4.3. Practical Applications and Use Cases

The literature and discourse on open-source development show its practical applications extend beyond technology, influencing the strategic, organizational, and political dimensions of digital transformation, especially in logistics. Open source is increasingly used to enhance security, digital sovereignty, transparency, and cross-sector collaboration among public institutions, private actors, and user communities. These applications are particularly relevant in contexts with high security demands, limited resources, or the need for long-term digital infrastructure sustainability.

In the public sector and defense, open source facilitates adaptable, controllable, and reliable systems. Modular architectures with open interfaces and standards enable efficient maintenance, interoperability, and easier integration of new functionalities without vendor lock-in. This is crucial in defense, where operational conditions change rapidly and systems must remain responsive, upgradeable, and secure throughout their lifecycles. Use cases like the MOSA illustrate how open-source architectures support cost-effective, long-term solutions based on reuse, standardization, and openness. However, the integration of open-source solutions in these sectors can be hindered by the need for rigorous security certifications and compliance with strict regulatory frameworks. Furthermore, the long-term maintenance and support of open-source systems may pose a challenge if in-house expertise is lacking, potentially requiring significant investment in training or external support.

From the viewpoint of digital security, open-source solutions offer transparency in critical components' operation, aiding code audits, faster vulnerability detection, and responsive incident handling. SBOM implementation and open-source security repositories show the potential for systemic security management using open standards, with collaboration among developers, institutions, and users. This framework establishes security

through verifiability, adaptability, and responsiveness—qualities inherent in open development. A key challenge, however, lies in ensuring the quality and reliability of community contributions. Open-source projects can suffer from a lack of consistent funding and developer attention, potentially leading to undiscovered vulnerabilities or delayed security updates. Moreover, the decentralized nature of open-source development can complicate efforts to establish clear lines of responsibility for security breaches.

In logistics, open-source solutions significantly aid the management of complex, interdependent systems like supply chains, transport networks, and inventory infrastructures. Open standards-based modular and interoperable architectures allow seamless integration between actors across the logistics ecosystem, from planning to tracking. Open platforms enhance data visibility, real-time auditability, and reduce reliance on proprietary vendors—essential for continuity, security, and sovereign control over data flows. Open-source logistics platforms (e.g., OpenLMIS, Odoo SCM) demonstrate achieving transparency, customization, and cost control without sacrificing performance. In military and humanitarian logistics, open-source technologies improve supply chain resilience, enable decentralized coordination, and ensure security compliance through verifiable and adaptable components. As logistics becomes increasingly cyber–physical, open-source development is key to secure, scalable, and ethically governed infrastructure (e.g., the physical Internet). Despite these advantages, the logistics industry's heavy reliance on real-time data and seamless integration presents significant challenges for open-source adoption. The lack of dedicated support and service-level agreements with open-source solutions can be a major concern for logistics providers, who require 24/7 system up-time and immediate technical assistance. Furthermore, the interoperability of open-source systems with existing proprietary logistics software can be complex and costly to achieve.

Open source also enhances digital autonomy. It offers countries and organizations a viable alternative to reduce vendor dependency and control long-term digital solution costs. Open-source platforms enable full control over data, source code, and system functionality, providing strategic independence—especially for sensitive information, defense data, or national infrastructure. However, the initial investment in developing and customizing open-source solutions can be substantial, and the long-term costs of maintenance and updates may be unpredictable. Moreover, the lack of a clear commercial roadmap or dedicated vendor support can create uncertainty for organizations that rely on these systems for critical operations.

Regarding digital inclusion and participation, open source enables engagement, local development, and collaborative innovation. Open-source tools facilitate the involvement of academia, civil society, businesses, and user groups in developing and maintaining digital solutions. This reduces informational inequality, strengthens local capacities, and fosters community-driven digital service environments. However, ensuring equitable participation and representation in open-source projects can be challenging. Digital literacy gaps and power imbalances within online communities can lead to the marginalization of certain groups and limit the diversity of perspectives contributing to the development process.

Finally, open source supports digital ethics. Its principles of transparent development, community-based maintenance, and collective responsibility offer alternatives to closed, opaque, and often monopolized software models. Organizations can use open source to strengthen internal security, support ethical technology use, and build trust among stakeholders in digital services' integrity and fairness. Nevertheless, the decentralized nature of open-source development can make it difficult to enforce ethical guidelines and ensure accountability for unethical behavior. The lack of clear legal frameworks and governance structures can also create challenges in addressing issues such as data privacy, intellectual property rights, and liability for software defects.

A practical example of the introduction of open-source principles in logistics is MOSA, originally from the U.S. Department of Defense. MOSA uses open interfaces and interoperable components to manage supply chains and weapon systems logistics. As Castelli [24] explains, this architecture allows rapid technology integration, long-term maintenance without vendor lock-in, and adaptability across operations. In logistics, MOSA supports scalable inventory control, transport modularity, and decentralized coordination, demonstrating how open-source design enhances security, flexibility, and efficiency in critical environments. However, the adoption of MOSA in complex logistics systems can be hindered by the need for extensive testing and validation to ensure compatibility and reliability across different systems and platforms. The integration of MOSA with legacy systems can also be a significant challenge, requiring substantial investment in software development and system reconfiguration.

The reviewed literature provides several examples of open-source systems used in real-world logistics, particularly in military, public health, and governance sectors. These cases highlight transparency, interoperability, and digital sovereignty's value in logistics applications.

In conclusion, open source's practical applications extend beyond software, enabling strategic digital solution management, security-resilient environments, and the promotion of collaboration, accountability, and fairness. For institutions seeking sustainable, inclusive, and secure digital systems, open source is a deliberate and progressive development path. However, its successful implementation requires careful consideration of the associated challenges and limitations, including the need for ongoing maintenance, security management, and addressing ethical considerations.

4.4. Comparative Contribution

This article contributes to the literature by systematically analyzing open-source software as a multidimensional infrastructure model relevant to the security, autonomy, and resilience of logistics systems, beyond just legal or technical concerns. While research has explored open-source practices in areas like public administration [71], national ICT strategies [54,100], and collaborative innovation [16], few studies focus on open-source adoption's concrete implications in mission-critical sectors like logistics.

Unlike prior work that primarily views open source as a tool for cost reduction or community empowerment, this article frames it as a strategic enabler of digital transformation in high-stakes environments. It integrates legal, economic, and cybersecurity dimensions, supported by institutional analysis and chronological mapping. In contrast to normative or ideological treatments [15,103], this study anchors its analysis in operational requirements and governance models relevant to supply chains, defense infrastructure, and critical digital platforms.

Furthermore, this research advances the respective research fields by comparatively synthesizing over 100 sources, classified across eight thematic categories and four developmental phases. Incorporating perspectives from defense institutions [8,24], security assessments [9,67], and global governance discourse [14,100] enhances the findings' practical relevance.

This study's originality is emphasized by its ability to bridge theoretical abstraction and applied strategy—connecting community-based development models with institutional digital sovereignty. By using the narrative review methodology combined with inductive thematic analysis, the article provides a unique framework for evaluating open-source practices' role in shaping secure and transparent digital infrastructures within logistics.

4.5. Answers to the Research Questions

This research addresses the central question: Does the open-source development model—characterized by open access to source code and community-based peer review—provide greater security and reliability for digital systems than proprietary approaches? Based on thematic and chronological analyses of over 100 scholarly and institutional sources, open source offers complex advantages if certain conditions are met.

The open-source model's transparency in source code is a significant advantage in security-sensitive environments. The literature emphasizes that open access enables faster vulnerability detection, easier validation of security mechanisms, and greater incident responsiveness. Compared to proprietary solutions with internal oversight, open-source projects use collective scrutiny and collaboration, enhancing digital systems' resilience.

However, the analysis reveals critical conditions for open source's effectiveness. Transparency and accessibility alone are insufficient; an active community, systemic support, and clear vulnerability management are essential. Without resources, governance, or institutional backing, open projects can become security liabilities, as shown by the Log4Shell vulnerability.

Therefore, open-source development offers security and reliability advantages over proprietary approaches if adequate support mechanisms exist. These include well-maintained infrastructure, institutional collaboration, standardization, and sustainable funding. When these conditions are met, such as in the defense sector's modular architectures or cybersecurity SBOM adoption, open-source solutions are more effective, adaptable, and transparent.

In conclusion, the answer is affirmative, with the qualification that the open-source model can provide greater security and reliability than proprietary approaches only with institutional support, clear regulation, and active community participation. Without them, open-source projects remain vulnerable. This research contributes to understanding open source not as inherently secure but as a strategic approach to digital security dependent on socio-technical alignment.

5. Conclusions

This analysis of over one hundred sources demonstrates that open-source development is a significant, multilayered approach to building digital systems focused on transparency, security, reliability, and sustainability. The research indicates that open source is more than a technical choice; it is an institutional, legal, economic, and political strategy that is increasingly integral to digital transformation across public and private sectors.

Open-source practices foster decentralized innovation, reduce dependence on closed systems, and enhance digital sovereignty of states and organizations. This thematic and chronological review reveals a shift from the movement's idealistic origins to its institutionalization within security-critical and strategic domains. However, this study also highlights challenges: unstable funding, a lack of formal accountability, and the vulnerability of many projects due to limited resources.

Our research question's answer confirms that, with the right institutional conditions and community support, open-source development can provide greater security and resilience of digital solutions. This is achieved through independent review, rapid vulnerability discovery, and broad collaboration. Yet, openness alone is insufficient; robust legal and security frameworks, responsible governance, and long-term strategic support are essential.

This study positions open source as a relevant methodological, strategic, and normative choice for shaping future digital infrastructure. The findings provide a basis for further research, especially in areas like comparative security analysis, the economic sustainability

of community models, and the design of public policies promoting open, inclusive, and trustworthy digital environments.

Extending these findings, domains like logistics show how open source can be operationalized where security, transparency, and control are vital. These insights are highly relevant to logistics, where the digital transformation increasingly converges with sovereignty, security, and continuity. As supply chains and transport infrastructures become more digital and interdependent, adopting open-source architectures can provide greater control, transparency, and adaptability, particularly in environments with high reliability needs and geopolitical sensitivity. Future research should investigate the systematic integration of open-source practices into logistics governance, cyber-risk management, and secure-by-design principles for critical infrastructure. It should also examine open-source governance under stress in military logistics and emergency supply chains. In this context, open source is not just a technical framework but a strategic enabler of resilient and trustworthy logistics systems.

Author Contributions: Conceptualization, M.P. and R.G.; methodology, M.P. and R.G.; validation, M.P. and R.G.; investigation, M.P. and R.G.; data curation, M.P. and R.G.; writing—original draft preparation, M.P.; writing—review and editing, M.P. and R.G.; supervision, R.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Tiwana, A. Platform desertion by app developers. *J. Manag. Inf. Syst.* **2015**, *32*, 40–77. [CrossRef]
2. Zhu, K.X.; Zhou, Z.Z. Lock-in strategy in software competition: Open-source software vs. proprietary software. *Inf. Syst. Res.* **2012**, *23*, 536–545. [CrossRef]
3. Saeedikiya, M.; Salunke, S.; Kowalkiewicz, M. The nexus of digital transformation and innovation: A multilevel framework and research agenda. *J. Innov. Knowl.* **2025**, *10*, 100640. [CrossRef]
4. Saeedikiya, M.; Salunke, S.; Kowalkiewicz, M. Toward a dynamic capability perspective of digital transformation in SMEs: A study of the mobility sector. *J. Clean. Prod.* **2024**, *439*, 140718. [CrossRef]
5. Egorov, D.; Levina, A.; Kalyazina, S.; Schuur, P.; Gerrits, B. The challenges of the logistics industry in the era of digital transformation. In *Technological Transformation: A New Role for Human, Machines and Management*; Schaumburg, H., Korablev, V., Ungvari, L., Eds.; Springer: Berlin/Heidelberg, Germany, 2021; pp. 201–209. [CrossRef]
6. Kern, J. The digital transformation of logistics: A review about technologies and their implementation status. In *Handbook of Smart Logistics*; Wiley: Hoboken, NJ, USA, 2021. [CrossRef]
7. Paksoy, T.; Ali, S.S.; Kochan, C.G. (Eds.) *Logistics 4.0: Digital Transformation of Supply Chain Management*; CRC Press: Boca Raton, FL, USA, 2021.
8. Cybersecurity and Infrastructure Security Agency. CISA Open Source Software Security Roadmap. 2023. Available online: https://www.cisa.gov/sites/default/files/2023-09/CISA-Open-Source-Software-Security-Roadmap-508c.pdf (accessed on 20 May 2025).
9. Ghalleb, W. Open-Source Security: Best Practices and Tools. Wiz. 2024. Available online: https://www.wiz.io (accessed on 20 May 2025).
10. Jones, B.R. Virtual neighborhood watch: Open source software and community policing against cybercrime. *J. Crim. Law Criminol.* **2007**, *97*, 601–629.
11. Kogut, B.; Metiu, A. Open-source software development and distributed innovation. *Oxf. Rev. Econ. Policy* **2001**, *17*, 248–264. [CrossRef]
12. Cameron, W.B.; McCormick, T.C. Concepts, of security and insecurity. *Am. J. Sociol.* **1954**, *59*, 556–564. [CrossRef]
13. Winner, L. Do artifacts have politics? *Daedalus* **1980**, *109*, 121–136.
14. Clift, A.D. National security and national competitiveness: Open source solutions. *Am. Intell. J.* **1993**, *14*, 25–28.
15. Benkler, Y. Coase's Penguin, or, Linux and "The Nature of the Firm". *Yale Law J.* **2002**, *112*, 369–446. [CrossRef]

16. von Krogh, G.; von Hippel, E. The promise of research on open source software. *Manag. Sci.* **2006**, *52*, 975–983. [CrossRef]
17. Kologlugil, S. Free software, business capital, and institutional change: A Veblenian analysis of the software industry. *J. Econ. Issues* **2012**, *46*, 831–858. [CrossRef]
18. von Krogh, G.; Haefliger, S.; Spaeth, S.; Wallin, M.W. Carrots and rainbows: Motivation and social practice in open source software development. *MIS Q.* **2012**, *36*, 649–676. [CrossRef]
19. Sacks, M. Competition between open source and proprietary software: Strategies for survival. *J. Manag. Inf. Syst.* **2015**, *32*, 268–295. [CrossRef]
20. Blair, G.; Chou, W.; Imai, K. List experiments with measurement error. *Political Anal.* **2019**, *27*, 455–480. [CrossRef]
21. Check Point Software Technologies Ltd. (n.d.). What Is Open Source Security? Available online: https://www.checkpoint.com/ (accessed on 20 May 2025).
22. Sipes, J.L. Software you can play with. *Landsc. Archit. Mag.* **2005**, *95*, 92, 94, 96, 98, 100–101.
23. Wheeler, D.A. Basics of Open Source Software. In *Using an Open Source Software Approach for Cybersecurity Technology Transition*; Institute for Defense Analyses: Alexandria, VA, USA, 2015; pp. 3-1–3-4. Available online: https://www.jstor.org/stable/resrep36511.6 (accessed on 20 May 2025).
24. Castelli, C.J. Future military innovations hinge on today's open systems work. *Inside Pentagon* **2008**, *24*, 6–7.
25. Romualdez, A.G., Jr.; dela Rosa, J.F.E.; Flavier, J.D.A.; Quimbo, S.L.A.; Hartigan-Go, K.Y.; Lagrada, L.P.; David, L.C. Organization and governance. In *The Philippines Health System Review*; Kwon, S., Dodd, R., Eds.; World Health Organization: Geneva, Switzerland, 2011; pp. 13–31. Available online: https://www.jstor.org/stable/resrep28459.9 (accessed on 20 May 2025).
26. Lemley, M.A.; Shafir, Z. Who chooses open-source software? *Univ. Chic. Law Rev.* **2011**, *78*, 139–164. [CrossRef]
27. Ricolfi, M. Consume and share: Making copyright fit for the digital agenda. In *The Digital Public Domain: Foundations for an Open Culture*; de Rosnay, M.D., Martin, J.C.D., Eds.; Open Book Publishers: Cambridge, UK, 2012; pp. 47–64. Available online: https://www.jstor.org/stable/j.ctt5vjsx3.8 (accessed on 20 May 2025).
28. Sen, R.; Subramaniam, C.; Nelson, M.L. Determinants of the choice of open source software license. *J. Manag. Inf. Syst.* **2008**, *25*, 207–239. [CrossRef]
29. Satchwell, M.D. The Tao of open source: Minimum action for maximum gain. *Berkeley Technol. Law J.* **2005**, *20*, 1757–1798.
30. Sauer, R.M. Why develop open-source software? The role of non-pecuniary benefits, monetary rewards, and open-source licence type. *Oxf. Rev. Econ. Policy* **2007**, *23*, 605–619. [CrossRef]
31. Scott, M.D. The FTC, the unfairness doctrine, and data security breach litigation: Has the Commission gone too far? *Adm. Law Rev.* **2008**, *60*, 127–183.
32. Cockburn, I.M.; MacGarvie, M.J. Entry and patenting in the software industry. *Manag. Sci.* **2011**, *57*, 915–933. [CrossRef]
33. Determann, L. What happens in the cloud: Software as a service and copyrights. *Berkeley Technol. Law J.* **2014**, *29*, 1095–1130.
34. Kwon, J.; Johnson, M.E. Meaningful healthcare security: Does meaningful-use attestation improve information security performance? *MIS Q.* **2018**, *42*, 1043–1068. [CrossRef]
35. Reber, P.A.; Graham, S.R. Evaluating system on a chip design security. *J. Inf. Warf.* **2017**, *16*, 63–78.
36. Veeraraghavan, S.; Bolisetti, C.; Slaughter, A.; Coleman, J.; Dhulipala, S.; Hoffman, W.; Kim, K.; Kurt, E.; Spears, R.; Munday, L. MASTODON: An open-source software for seismic analysis and risk assessment of critical infrastructure. *Nucl. Technol.* **2021**, *207*, 1073–1095. [CrossRef]
37. Dong, S.; Johar, M.S.; Kumar, R.L. A benchmarking model for management of knowledge-intensive service delivery networks. *J. Manag. Inf. Syst.* **2011**, *28*, 127–160. [CrossRef]
38. Suarez, F.F.; Cusumano, M.A.; Kahl, S.J. Services and the business models of product firms: An empirical analysis of the software industry. *Manag. Sci.* **2013**, *59*, 420–435. [CrossRef]
39. Lerner, J.; Tirole, J. Some simple economics of open source. *J. Ind. Econ.* **2002**, *50*, 197–234. [CrossRef]
40. Lerner, J.; Tirole, J. The economics of technology sharing: Open source and beyond. *J. Econ. Perspect.* **2005**, *19*, 99–120. [CrossRef]
41. Lerner, J.; Tirole, J. The scope of open source licensing. *J. Law Econ. Organ.* **2005**, *21*, 20–56. [CrossRef]
42. Sen, R. A strategic analysis of competition between open source and proprietary software. *J. Manag. Inf. Syst.* **2007**, *24*, 233–257. [CrossRef]
43. Ågerfalk, P.J.; Fitzgerald, B. Outsourcing to an unknown workforce: Exploring opensourcing as a global sourcing strategy. *MIS Q.* **2008**, *32*, 385–409. [CrossRef]
44. Bonaccorsi, A.; Giannangeli, S.; Rossi, C. Entry strategies under competing standards: Hybrid business models in the open source software industry. *Manag. Sci.* **2006**, *52*, 1085–1098. [CrossRef]
45. Fitzgerald, B. The transformation of open source software. *MIS Q.* **2006**, *30*, 587–598. [CrossRef]
46. August, T.; Shin, H.; Tunca, T.I. Licensing and competition for services in open source software. *Inf. Syst. Res.* **2013**, *24*, 1068–1086. [CrossRef]

47. Birkinbine, B.J. Shifting Toward the Commons: Microsoft and Competing Models of Software Production. In *Incorporating the Digital Commons: Corporate Involvement in Free and Open Source Software*; University of Westminster Press: London, UK, 2020; pp. 49–72. [CrossRef]
48. Kumar, V.; Gordon, B.R.; Srinivasan, K. Competitive strategy for open source software. *Mark. Sci.* **2011**, *30*, 1066–1078. [CrossRef]
49. Wheeler, D.A. What Is Open Security? Institute for Defense Analyses. 2013. Available online: https://www.jstor.org/stable/resrep36440 (accessed on 20 May 2025).
50. Wheeler, D.A.; Khakimov, S. Some past and current efforts to identify relevant OSS project metrics. In *Open Source Software Projects Needing Security Investments*; Institute for Defense Analyses: Alexandria, VA, USA, 2015; pp. 2-1–2-30. Available online: https://www.jstor.org/stable/resrep36518.5 (accessed on 20 May 2025).
51. Wu, Y. Developing a taxonomic framework of security methods for security management and information resource management. *J. Strateg. Secur.* **2020**, *13*, 64–77. [CrossRef]
52. Wu, Y.; Meng, F. Categorizing security for security management and information resource management. *J. Strateg. Secur.* **2018**, *11*, 72–84. [CrossRef]
53. Motogna, S.; Cristea, D.; Șotropa, D.; Molnar, A.-J. Formal concept analysis model for static code analysis. *Carpathian J. Math.* **2022**, *38*, 159–168. [CrossRef]
54. Nagaraju, V.; Fiondella, L.W.; Ji, T. An open-source tool to support the quantitative assessment of cyber security for software intensive system acquisition. *J. Inf. Warf.* **2017**, *16*, 31–50.
55. Hutton, W.J.; McKinnon, A.D.; Hadley, M.D. Software-defined networking traffic engineering process for operational technology networks. *J. Inf. Warf.* **2019**, *18*, 167–181.
56. Sovereign, B. Securing software defined networking. *J. Inf. Warf.* **2017**, *16*, 56–65.
57. Turner, M.; Jones, M.; Poschen, M.; Procter, R.; Rowley, A.; Schiebeck, T. Secure data sharing across portals: Experiences from OneVRE. *Philos. Trans. Math. Phys. Eng. Sci.* **2013**, *371*, 1–12. [CrossRef]
58. Singh, P.V.; Tan, Y.; Mookerjee, V. Network effects: The influence of structural capital on open source project success. *MIS Q.* **2011**, *35*, 813–829. [CrossRef]
59. Haefliger, S.; von Krogh, G.; Spaeth, S. Code reuse in open source software. *Manag. Sci.* **2008**, *54*, 180–193. [CrossRef]
60. Stewart, K.J. How hypertext links influence consumer perceptions to build and degrade trust online. *J. Manag. Inf. Syst.* **2006**, *23*, 183–210. [CrossRef]
61. Stewart, K.J.; Darcy, D.P.; Daniel, S.L. Opportunities and challenges applying functional data analysis to the study of open source software evolution. *Stat. Sci.* **2006**, *21*, 167–178. [CrossRef]
62. Ünver, H.A. Digital Open Source Intelligence and International Security: A Primer. Centre for Economics and Foreign Policy Studies. 2018. Available online: https://www.jstor.org/stable/resrep21048 (accessed on 20 May 2025).
63. Aho, A.V. Software and the future of programming languages. *Science* **2004**, *303*, 1331–1333. [CrossRef]
64. Canadian Centre for Cyber Security. Security Considerations When Using Open Source Software. Government of Canada. 2025. Available online: https://www.cyber.gc.ca (accessed on 20 May 2025).
65. Institution of Engineering and Technology. Open Source Software: A Factfile Provided by the Institution of Engineering and Technology. 2014. Available online: https://www.theiet.org/factfiles (accessed on 20 May 2025).
66. Worldwide Videotex. OpenSAMM consortium improves software security. *Comput. Secur. Update* **2015**, *16*, 5–8.
67. Crumpler, W.D.; Lewis, J.A. Cybersecurity and the Problem of Interoperability. Center for Strategic and International Studies (CSIS). 2020. Available online: https://www.jstor.org/stable/resrep29334 (accessed on 20 May 2025).
68. Petro, N., Jr. Software as a service. *GPSolo* **2007**, *24*, 28–31.
69. Tate, D.M. Software Productivity Trends and Issues (Conference Paper, IDA Document NS D-8367). Institute for Defense Analyses. 2017. Available online: https://www.jstor.org/stable/resrep22675 (accessed on 20 May 2025).
70. Wells, N.D. Government use of free software. *Public Contract Law J.* **2004**, *33*, 565–597.
71. FitzGerald, B.; Levin, P.L.; Parziale, J. Open Source Software & the Department of Defense. Center for a New American Security. 2016. Available online: https://www.jstor.org/stable/resrep06252 (accessed on 20 May 2025).
72. Butler, A. FBI searches offices, questions employees at Robins Air Force Base. *Inside Air Force* **2003**, *14*, 2.
73. Williams van Rooij, S. Adopting open-source software applications in U.S. higher education: A cross-disciplinary review of the literature. *Rev. Educ. Res.* **2009**, *79*, 682–701. [CrossRef]
74. Cybersecurity and Infrastructure Security Agency. CISA Announces New Efforts to Help Secure Open Source Ecosystem. 2023. Available online: https://www.cisa.gov (accessed on 20 May 2025).
75. West, Q. Librarians in the pursuit of open practices. In *Open: The Philosophy and Practices That Are Revolutionizing Education and Science*; Jhangiani, R.S., Biswas-Diener, R., Eds.; Ubiquity Press: London, UK, 2017; pp. 139–146. Available online: https://www.jstor.org/stable/j.ctv3t5qh3.15 (accessed on 20 May 2025).
76. Yeats, D. The role for technical communicators in open-source software development. *Tech. Commun.* **2008**, *55*, 38–48.

77. Yim, S.; Warschauer, M.; Zheng, B.; Lawrence, J.F. Cloud-based collaborative writing and the Common Core Standards. *J. Adolesc. Adult Lit.* **2014**, *58*, 243–254. [CrossRef]
78. Di Tullio, D.; Staples, D.S. The governance and control of open source software projects. *J. Manag. Inf. Syst.* **2013**, *30*, 49–80. [CrossRef]
79. Stewart, K.J.; Gosain, S. The impact of ideology on effectiveness in open source software development teams. *MIS Q.* **2006**, *30*, 291–314. [CrossRef]
80. Setia, P.; Rajagopalan, B.; Sambamurthy, V.; Calantone, R. How peripheral developers contribute to open-source software development. *Inf. Syst. Res.* **2012**, *23*, 144–163. [CrossRef]
81. Camp, L.J. Reconceptualizing the role of security user. *Daedalus* **2011**, *140*, 93–107. [CrossRef]
82. Johnston, A.C.; Warkentin, M. Fear appeals and information security behaviors: An empirical study. *MIS Q.* **2010**. [CrossRef]
83. Fang, Y.; Neufeld, D. Understanding sustained participation in open source software projects. *J. Manag. Inf. Syst.* **2009**, *25*, 9–50. [CrossRef]
84. Howison, J.; Crowston, K. Collaboration through open superposition: A theory of the open source way. *MIS Q.* **2014**, *38*, 29–50. [CrossRef]
85. Bagozzi, R.P.; Dholakia, U.M. Open source software user communities: A study of participation in Linux user groups. *Manag. Sci.* **2006**, *52*, 1099–1115. [CrossRef]
86. Davis, M. Conflict of interest revisited. *Bus. Prof. Ethics J.* **1993**, *12*, 21–41. [CrossRef]
87. Scott, S.; Brackett, S.A.; Gambrill, Y.; Nettles, E.; Herr, T. Dragon Tails: Preserving International Cybersecurity Research. Atlantic Council. 2022. Available online: https://www.jstor.org/stable/resrep42767 (accessed on 20 May 2025).
88. Zhou, Y. Against intellectual monopoly: Free software in China. *World Rev. Political Econ.* **2011**, *2*, 290–306.
89. Shoebridge, M. 5G futures: Why Huawei when open source may be the new black? In *Huawei and Australia's 5G Network*; Australian Strategic Policy Institute: Canberra, Australia, 2018; pp. 21–23. Available online: https://www.jstor.org/stable/resrep23079.13 (accessed on 20 May 2025).
90. Bliss, T.J.; Smith, M. A brief history of open educational resources. In *Open: The Philosophy and Practices That Are Revolutionizing Education and Science*; Jhangiani, R.S., Biswas-Diener, R., Eds.; Ubiquity Press: London, UK, 2017; pp. 9–27. [CrossRef]
91. Tuomi, I. Open educational resources and the transformation of education. *Eur. J. Educ.* **2013**, *48*, 58–78. [CrossRef]
92. Weijers, D.; Jarden, A. The International Journal of Wellbeing: An open access success story. In *Open: The Philosophy and Practices That Are Revolutionizing Education and Science*; Jhangiani, R.S., Biswas-Diener, R. Eds.; Ubiquity Press: London, UK, 2017; pp. 181–194. Available online: https://www.jstor.org/stable/j.ctv3t5qh3.18 (accessed on 20 May 2025).
93. Mackintosh, W. Open course development at the OERu. In *Open: The Philosophy and Practices That Are Revolutionizing Education and Science*; Jhangiani, R.S., Biswas-Diener, R., Eds.; Ubiquity Press: London, UK, 2017; pp. 101–114. [CrossRef]
94. May, C. Opening other windows: A political economy of 'openness' in a global information society. *Rev. Int. Stud.* **2008**, *34* (Suppl. S1), 69–92. [CrossRef]
95. McInerney, P.-B. Technology movements and the politics of free/open source software. *Sci. Technol. Hum. Values* **2009**, *34*, 206–233. [CrossRef]
96. Kalin, I. Open data policy improves democracy. *SAIS Rev. Int. Aff.* **2014**, *34*, 59–70. [CrossRef]
97. Munshi, U.M.; Verma, N. MEETING REPORT: Open data in education and research. *Curr. Sci.* **2014**, *107*, 167–168.
98. Rothschild, E. What is security? *Daedalus* **1995**, *124*, 53–98.
99. Schlicht, H. Open Access, Open Data, Open Software? Proprietary Tools and Their Restrictions. In *Digital Methods in the Humanities: Challenges, Ideas, Perspectives*; Schwandt, V.S., Ed.; Verlag/Bielefeld University Press: Bielefeld, Germany, 2021; pp. 25–47. Available online: https://www.jstor.org/stable/j.ctv2f9xskk.4 (accessed on 20 May 2025).
100. Couture, S. Free and open source software. In *The Handbook of Peer Production*; O'Neil, M., Pentzold, C., Toupin, S., Eds.; Wiley-Blackwell: Hoboken, NJ, USA, 2021; pp. 155–168. [CrossRef]
101. Noor, S. Cyber (in) security: A challenge to reckon with. *Strateg. Stud.* **2014**, *34*, 1–19.
102. Shkabatur, J. Transparency with(out) accountability: Open government in the United States. *Yale Law Policy Rev.* **2012**, *31*, 79–140.
103. Coleman, G. Code is speech: Legal tinkering, expertise, and protest among free and open source software developers. *Cult. Anthropol.* **2009**, *24*, 420–454. [CrossRef]
104. Benes, L. OSINT, new technologies, education: Expanding opportunities and threats. A new paradigm. *J. Strateg. Secur.* **2013**, *6* (Suppl. S3), 22–37. [CrossRef]
105. Fidler, D.P. A theory of open-source anarchy. *Indiana J. Glob. Leg. Stud.* **2008**, *15*, 259–284. [CrossRef]
106. August, T.; Tunca, T.I. Network software security and user incentives. *Manag. Sci.* **2006**, *52*, 1703–1720. [CrossRef]
107. Paiva, E. Use of Open Source Software by the Brazilian Government. Technology Innovation Management Review. 2009. Available online: https://timreview.ca/article/250 (accessed on 20 May 2025).

108. Herr, T.; Lee, J.; Loomis, W.; Scott, S. Attacks on the software supply chain. In *Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain*; Atlantic Council: Washington, DC, USA, 2020; pp. 10–23. Available online: https://www.jstor.org/stable/resrep26032.6 (accessed on 20 May 2025).
109. Chan, A. Coding free software, coding free states: Free software legislation and the politics of code in Peru. *Anthropol. Q.* **2004**, *77*, 531–545. [CrossRef]
110. Carver, B.W. Share and share alike: Understanding and enforcing open source and free software licenses. *Berkeley Technol. Law J.* **2005**, *20*, 443–481.
111. Gehem, M.; Usanov, A.; Frinking, E.; Rademaker, M. Response to cyber threats. In *Assessing Cyber Security: A Meta-Analysis of Threats, Trends, and Responses to Cyber Attacks*; Hague Centre for Strategic Studies: Hague, The Netherlands, 2015; pp. 57–72. Available online: https://www.jstor.org/stable/resrep12567.7 (accessed on 20 May 2025).
112. Carson, T.L. Conflicts of interest and self-dealing in the professions: A review essay. *Bus. Ethics Q.* **2004**, *14*, 161–182. [CrossRef]
113. Poritz, J.A. Information technology wants to be free. *Academe* **2012**, *98*, 18–23.
114. Economides, N.; Katsamakas, E. Two-sided competition of proprietary vs. open source technology platforms and the implications for the software industry. *Manag. Sci.* **2006**, *52*, 1057–1071. [CrossRef]
115. Campbell-Kelly, M.; Garcia-Swartz, D.D. From products to services: The software industry in the Internet era. *Bus. Hist. Rev.* **2007**, *81*, 735–764. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.