FMDB *Transactions on Sustainable Management Letters*

Digital Sovereignty in the Reconstruction Era: Balancing International Partnerships and Technological Independence

Jouma Ali Al-Mohamad[1,*], Omar Farouk Al Mashhour[2], Nakamura Manami[3], Muhammad Aidil Bin Hassan[4], Ng Wei Jie[5], Chloe Teo Wan Ting[6]

[1]Department of Computer and Mobile Communication Engineering, Faculty of Information Engineering, Al-Shahbaa Private University, Aleppo, Aleppo Governorate, Syria.
[2]Department of Business and Management, Faculty of Administrative Sciences and Economics, Tishk International University, Erbil, Erbil Governorate, Iraq.
[3]Department of Economics, Keio University, Minato, Tokyo, Japan.
[4]Department of Operations, Merlion Manufacturing, North Region, Singapore.
[5]Department of Human Resources, Clarke Quay Group, Central Region, Singapore.
[6]Department of Finance, Sentosa Exports Pte Ltd, Central Merlion Manufacturing Region, Singapore.
jalmohamad@su.edu.sy[1], omer.farouk@tiu.edu.iq[2], nakamura.manami@keio.ac.jp[3], aidil.hassan@merlionmfg.sg[4], ng.weijie@clarkequaygroup.com.sg[5], chloe.teo@sentosaexports.com.sg[6]

Abstract: This paper examines the complex interplay between digital sovereignty and international alliances in Syria's post-conflict infrastructure rehabilitation, focusing on the IT and telecoms industries. Syria has launched a massive infrastructure-based digital transformation plan after the December 2024 political transition. Key projects include the Silk Link fibre-optic network, the Medusa undersea cable, and the Barq Net last-mile project. Gulf states have invested heavily in these projects. These agreements call into question Syria's digital sovereignty, particularly its control over data, infrastructure, and technology policy. This paper contrasts the necessity for foreign finance and technology transfer with the need to maintain digital system autonomy. This study examines Syria's digital infrastructure agreements across three policy areas: standards and cybersecurity frameworks, data governance and localization, and dependency concerns related to long-term maintenance, upgrades, and finance. The paper analyses public pronouncements, industry reports, and scholarly literature. This paper argues that Syria's digital sovereignty is contested and negotiated, characterised by geopolitical rivalries, institutional capabilities, and agreement terms. The study concludes with recommendations for risk-governed international digital investment. This approach maximises Syrian ownership and profit while avoiding dependency risks.

Keywords: Digital Sovereignty; Post-Conflict Reconstruction; Telecommunications Infrastructure; Foreign Direct Investment; Data Governance; Techno-Politics; Silk Link; Digital Independence.

Received on: 23/02/2025, **Revised on:** 16/05/2025, **Accepted on:** 19/08/2025, **Published on:** 12/09/2026

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSML

DOI: https://doi.org/10.69888/FTSML.2026.000819

Cite as: J. A. Al-Mohamad, O. F. Al Mashhour, N. Manami, M. A. B. Hassan, N. W. Jie, and C. T. W. Ting, "Digital Sovereignty in the Reconstruction Era: Balancing International Partnerships and Technological Independence," *FMDB Transactions on Sustainable Management Letters*, vol. 4, no. 3, pp. 94–107, 2026.

Copyright © 2026 J. A. Al-Mohamad *et al.,* licensed to Fernando Martins De Bulhão (FMDB) Publishing Company. This is an open access article distributed under CC BY-NC-SA 4.0, which permits copying, remixing, redistributing, transformation, and building upon the material in any medium so long as the original work is properly cited.

1. Introduction

[*]Corresponding author.

As the Syrian Arab Republic [8] enters the post-conflict reconstruction phase, it faces one of the most difficult state-building tasks of the modern era [9]. Beyond the massive effort to rebuild physical infrastructure after more than thirteen years of fighting, the nation also faces the equally important task of rebuilding the digital foundations needed for efficient governance, economic recovery and social growth [1]. Unlike earlier post-disaster reconstruction efforts that focused on rebuilding roads, buildings, energy systems and industrial capacity, recovery in the twenty-first century increasingly relies on digital infrastructure, information systems, data governance and technological skills [2]. In this sense, reconstructing Syria is an opportunity and a necessity to build a modern digital state that can enable open governance, efficient public services, economic innovation and national resilience [10]. Syria's reconstruction challenge is unprecedented in scale [3]. The World Bank estimates total rehabilitation costs at about $216 billion, driven by extensive damage to public services, infrastructure, housing and productive sectors [4]. Telecommunications and Information and Communication Technology (ICT) infrastructure are two sectors of particular strategic importance, as digital connectivity is becoming a key element of almost all aspects of modern governance and economic activity [5]. Years of violence, including massive theft of technical equipment, destruction of transmission towers, disruption of fiber-optic links and direct attacks on telecommunications facilities, have severely damaged Syria’s communication networks [6]. It has been estimated that about half of Syria’s infrastructure has been damaged or rendered inoperable, including critical communication networks that support individuals, businesses and government functions [7].

The extent of the financial and physical damage to digital infrastructure is demonstrated by the fact that the theft of copper and fiber-optic cables in the Homs governorate alone led to losses of over one billion Syrian pounds in one year [18]. Despite these challenges, the ICT sector offers one of the most promising paths to a rapid, transformative recovery. Digital technologies offer Syria the chance to leapfrog traditional development barriers through more effective public administration, greater access to services, support for private-sector growth and stronger institutional openness. Digital reconstruction allows us to build a more complex and interconnected technical landscape, not simply to restore antique technologies [17]. All of these, like sophisticated telecommunications networks, national databases, cloud-based services, digital government platforms and means of electronic payment, could greatly improve administrative effectiveness and reduce institutional fragmentation. So digital rebuilding is a fundamental part of state modernisation and not just a technical procedure [19]. The growing importance of digital infrastructure reflects a broader shift in rebuilding itself. In the past decades, the country’s recovery was often associated with physical reconstruction—building up factories, roads, bridges, and public facilities. But modern rebuilding increasingly depends on the ability to collect, organise, protect and use information. As has been observed in discussions around Syria’s recovery, reconstruction in the twenty-first century is increasingly a competition of data and digital capabilities rather than simply “cement and iron”. A state's ability to govern digital infrastructure, regulate information flows, and build technological capacity directly affects its ability to plan, coordinate, and implement successful reconstruction programs. Since Syria's political transition in December 2024, the country has launched several key projects to repair and improve its digital infrastructure [16].

Key initiatives include establishing Syria’s first Tier III data center in partnership with Saudi cybersecurity firm Cypher, the Medusa undersea cable landing project, the Barq Net last-mile fibre network project, and the Silk Link national fibre-optic backbone program [11]. These programs are key steps toward modernising Syria’s telecom infrastructure and reconnecting the country to regional and international digital networks [12]. They have also drawn sizeable foreign investment, notably from Gulf states, indicating a change in Syria’s international technological and economic ties. But while international collaborations and foreign investment provide essential financial resources, technical know-how, and infrastructure capabilities, they also raise challenging issues about digital sovereignty. Syria's key challenge is to benefit from external technological assistance while retaining significant control over its digital infrastructure, national data and strategic technology choices [13]. As Access Now [1] notes, Syria’s digital infrastructure development is a cautionary tale of the balancing act between digital sovereignty and external dependency. Syria lacks the financial and technical resources to rebuild its digital ecosystem alone, so international cooperation is necessary [14]. However, overreliance on foreign suppliers may carry long-term risks for cybersecurity, infrastructure control, data ownership and technological autonomy [15]. Thus, digital sovereignty is an important concept for discussing the restoration of Syria’s technology. Digital sovereignty can be defined as a state's ability to control its digital infrastructure, data resources, technology regulations and strategic technical choices. It has several interrelated dimensions. The first dimension concerns sovereignty over physical infrastructure, including data centers, fiber-optic systems, telecommunications networks and submarine cables.

The second is data sovereignty – where national data is stored, who can access it, and how it is protected [20]. The third is technological sovereignty, including the ability to set standards, control technology procurement, and develop domestic expertise. The fourth dimension is institutional sovereignty, the capacity of government institutions to independently and successfully administer digital systems. Digital sovereignty is particularly challenging for post-conflict countries like Syria. Countries emerging from a conflict usually have weak institutions, limited financial resources, damaged infrastructure and a lack of skilled workers [21]. As such, they often rely heavily on foreign governments, international organisations and multinational technology companies for funding, knowledge and technological solutions. This dependence creates a fundamental dilemma: rapid recovery requires external help, but too much dependence could eventually undermine self-

sufficiency. The question then becomes not whether Syria should pursue international cooperation but how it can do so in a way that builds domestic capabilities rather than creating long-term technological dependence [22]. The shift from traditional administrative systems to digital governance has major institutional and political implications. Digitisation is often presented as a neutral technical process meant to increase productivity and reduce administrative problems. But digital transformation also reshapes the state's power architecture. Institutional power can derive from control of servers, databases, algorithms, and digital platforms. Traditional systems of administration offer paper trails, official seals and bureaucratic processes to track authority. In the digital state, authority increasingly relies on control of information systems and technology infrastructure. An analysis of Syria's digital transition argues that the shift from paper-based administration to data-driven governance moves influence from traditional administrative actors to those who control digital systems and technology infrastructure.

This change illustrates the relevance of the "platform state" idea. Recent governance literature uses the term "platform state" to refer to governments that use digital platforms for information management, public service delivery, institutional coordination and citizen interaction. Digital platforms can also reduce administrative inefficiencies, improve access to services, increase transparency and develop integrated information systems. Digital platforms may support better coordination and integration of government activity in Syria, where years of violence have heightened institutional fragmentation. But the platform state isn't risk-free either. Digital systems are not politically neutral; they contain decisions about control, security, access and governance [23]. Digital platform design determines who gets information, who decides, and who is held accountable. Digitalisation can either strengthen public trust or exacerbate existing vulnerabilities in a post-conflict setting undergoing institutional change, depending on how it is managed [24]. Therefore, Syria's digital reconstruction should also encompass institutional accountability, cybersecurity, data protection, and citizen participation in addition to technological capability. In Syria's complex geopolitical reconstruction context, digital sovereignty is particularly crucial. Further challenges are posed by international sanctions, limited access to international technological markets, conflicting external interests and the involvement of many international entities. Foreign investment can hasten infrastructure development, but different partners may have different governance models, strategic agendas and technology standards [25].

Syria should exercise institutional control and policy preparation carefully to ensure these alliances serve its long-term national interests [26]. The importance of digital sovereignty for post-conflict reconstruction is undeniable, but important research gaps remain. Existing studies tend to discuss digital transformation through an economic or technological lens, and offer limited understanding of how vulnerable and conflict-affected governments could balance reliance on technology with national sovereignty. Syria is a key case because it combines significant infrastructure damage, urgent reconstruction needs, geopolitical complexity, and new opportunities for digital transformation. This paper examines Syria's digital reconstruction through the lens of digital sovereignty [27]. It discusses the current state of Syria's digital infrastructure, including major projects and international partnerships. It identifies the main features of digital sovereignty undergoing technological rebuilding. It examines the geopolitical and techno-political factors shaping Syria's digital environment. It considers the dangers of foreign digital investment and technological dependence. It offers policy recommendations to balance international cooperation with national digital independence. By examining these problems, this paper argues that digital restoration is more than simply restoring telecom networks or applying new technology [29]. It's part of broader efforts to restore governmental capacity, protect national interests and lay the foundations for a modern digital society. Rebuilding connectivity is only part of the story; Syria's reconstruction will depend on how digital transformation supports resilience, transparency, sovereignty and sustainable national growth [28].

2. Review of Literature

Digital sovereignty has become a litmus test for current debates on tech governance, international relations, and state capacity. Over the past decade, the concept has shifted significantly, from concerns about dependence on dominant global technology companies to states' ability to maintain control over critical digital systems. While the initial controversies were largely focused on European concerns regarding technological dependence on foreign platforms, digital sovereignty has increasingly become relevant for countries around the world, particularly regarding developing and post-conflict countries that are attempting to reconcile technological modernisation and national autonomy. In essence, digital sovereignty is a state's ability to exercise meaningful control over its digital infrastructure, data resources, technology policies and regulatory environment. Current literature, however, stresses the multidimensionality of digital sovereignty, including infrastructure sovereignty, data sovereignty, technological sovereignty, and regulatory sovereignty. Infrastructure sovereignty is the control of physical digital resources such as telecommunications networks, fibre-optic systems, submarine cables and data centers [18]. In contrast, data sovereignty is the ownership, storage, processing and protection of national data. Technological sovereignty is a country's ability to produce, access, and control technologies in line with national interests. Regulatory sovereignty is the ability to create and enforce rules for digital activities on its territory. The importance of digital sovereignty is especially evident in post-conflict environments, where states have to rebuild digital systems under conditions of institutional fragility, financial constraints and technological dependence. Developing countries emerging from conflict often need foreign investment, international know-how and foreign technology partnerships to rebuild damaged infrastructure and create modern digital services [22].

But the external dependency that speeds up reconstruction may also reveal long-term weaknesses in infrastructure control, data access, cybersecurity and strategic decision-making. Digital reforms in fragile states can boost institutional legitimacy and improve public-service delivery [23]. However, they may create new forms of dependency or exclusion when governance structures are weak, and implementation strategies are poorly designed. Thus, digital sovereignty in post-conflict reconstruction is not simply a matter of technology ownership, but a broader challenge of sustaining political autonomy, institutional capacity, and public trust in an increasingly digitalised state. Beyond infrastructure development, digital sovereignty and post-conflict reconstruction are closely linked, as technological choices are often anchored in broader political and geopolitical interests. Decisions related to digital infrastructure such as technology standards, procurement agreements, telecommunications partnerships and data-management arrangements have strategic implications for state authority and future governance capacity [21]. Digital infrastructure differs from traditional infrastructure projects such as roads or bridges. Digital infrastructure is the foundation through which governments manage civil registries, monetary systems, taxation, public services, security operations and future democratic processes. Therefore, decisions about the ownership, operation, and control of digital systems directly shape power distribution within institutions. Countries emerging from conflict are especially vulnerable to digital dependence as immediate reconstruction needs often require rapid collaboration with foreign governments, multinational corporations and international financial institutions. These partnerships are critical for providing capital and technical expertise [29].

Still, they can also create dependence on external providers for system maintenance, software updates, cybersecurity services, and technology decisions. The challenge is especially critical for Syria, where the country is digitally rebuilding after years of destroyed infrastructure, economic restrictions, and limited access to international technology markets. A key policy challenge for Syria's reconstruction process is how to attract foreign investment while maintaining national control over strategic digital resources. Digital sovereignty is shaped by geopolitical competition and techno-political rivalry. Infrastructure has emerged as a strategic battleground where states and international actors increasingly compete for influence through investment, partnerships and technology transfer [2]. Syria's digital reconstruction will involve various actors, including Gulf countries, European technology companies and other international partners with different economic and geopolitical interests. Saudi investment in telecom infrastructure, European technology participation, and talk of Chinese participation show the complex geopolitical climate surrounding Syria's digital transformation. These dynamics demonstrate that digital infrastructure choices are not simply technical decisions but are embedded in broader international power relations. Techno-politics offers an important conceptual framework for understanding these developments [1]. Techno-politics studies the relationship between technological systems and political power, and between political interests and technological decisions. For example, Syria's choices of telecommunications providers, cloud infrastructure, cybersecurity systems, and data-storage locations could shape the country's future governance model and strategic independence. Digital reconstruction therefore requires not only technology upgrades but also careful consideration of sovereignty, security and long-term national interests.

Data governance is another core dimension of digital sovereignty, as the control of data is key to a state's ability to govern public administration, protect citizens and facilitate evidence-based policymaking. "The basic digital infrastructure, such as civil registration, land registries, commercial registries and national information systems, is essential for good governance and reconstruction planning [4]. Data localisation has become a mechanism through which states are seeking to increase digital sovereignty, requiring that certain categories of data be stored and processed within national territory. Localisation policies are used by governments to increase legal control over data, protect sensitive information and reduce exposure to foreign surveillance or unauthorised access. Syria has implemented several initiatives to enhance its national data governance capacity. The National Digital Transformation Strategy includes establishing a National Data Centre, a major hub for digital development, to integrate government databases and improve digital public services. The strategy also plans to link major government registries and build national digital infrastructure to underpin modern governance systems. Similarly, efforts to strengthen digital sovereignty standards are reflected in the creation of Tier III data-centre infrastructure with commitments to data protection and domestic data storage. Cybersecurity is deeply embedded in the concept of digital sovereignty, because a state cannot exercise true sovereignty over its digital systems without the ability to defend them from cyber assaults. Post-conflict States are particularly vulnerable to cyberattacks because of damaged infrastructure, limited institutional capacity and the rapid expansion of digital services [5].

Syria has made progress in strengthening cybersecurity governance, including developing cybersecurity strategies, enacting legislation on electronic personal data protection, and signing cooperation agreements with cybersecurity organisations [7]. This growing recognition of cybersecurity as a national security issue that affects government services, economic development and citizen protection is reflected in recent cybersecurity initiatives, including national cybersecurity programs and expert forums. Interest in digital sovereignty is growing, yet several research gaps remain. Existing literature on digital sovereignty, largely from developed countries with robust institutions, offers little to no insight into how post-conflict states manage digital sovereignty under dependency and reconstruction pressures. Second, little attention has been paid to the role of private telecommunications companies and foreign technology firms in shaping digital sovereignty outcomes. Third, the effects of sanctions and geopolitical restrictions on digital reconstruction have not been sufficiently investigated, though this is important for countries such as Syria. Finally, existing studies tend to emphasise state-led approaches and pay less attention to the role of

civil society, diaspora communities, local technology ecosystems and citizens in shaping a sovereign digital future. This study addresses these gaps by examining Syria's digital reconstruction through the lens of digital sovereignty, focusing on infrastructure control, data governance, cybersecurity, geopolitical dynamics, and institutional capacity. It highlights how post-conflict states can benefit from digital transformation while maintaining national autonomy and building resilient governance systems [2].

3. Methodology

This study uses qualitative policy analysis and conceptual synthesis to examine the challenges and potential of digital sovereignty in Syria after the political change of December 2024. The methodological approach is designed to reflect the multidimensional nature of digital sovereignty, which is not only about technical infrastructure, but also about issues of governance, institutional control, data handling, geopolitical dependence, regulatory control and strategic ownership of digital systems. The study therefore draws on a rich body of documentary data, rather than a single source, to provide a holistic understanding of Syria's developing digital ecosystem. Primary sources include official statements, government strategies, legislation, policy documents, institutional reports, publications from international organisations, academic literature, foreign media, industry publications, and publications from think tanks and research institutions. By drawing on multiple source types, the study compares official policy aims with broader external assessments and helps identify areas of convergence, divergence, and uncertainty. The documentary study relies mostly on official Syrian government sources, reflecting national priorities, regulatory reforms, infrastructural plans, international agreements and institutional tactics. Government policies and official pronouncements of the Syrian authorities are used to evaluate the conceptualisation of digital transformation, infrastructure development, cybersecurity, data governance, telecommunications and national control over digital systems.

These are reinforced by reports from international organisations and development institutions, which provide further insights on digital infrastructure, institutional capacity, regulatory development and rebuilding needs. The study's conceptual base is rooted in academic literature, especially digital sovereignty, post-conflict reconstruction, technology reliance, digital geopolitics, and techno-politics. The addition of media and industry publications provides information on key technology agreements, telecommunications advances, international alliances, investments, and infrastructure projects that may not be fully captured in academic research. Independent interpretations of changes in geopolitics and the strategic implications of Syria's expanding digital linkages are provided by think-tank and research-institution analyses. The study is basically documentary, qualitative and interpretative. Rather than measuring digital sovereignty through a single numerical indicator, the research combines information across multiple dimensions to identify the structural elements that shape Syria's ability to exercise meaningful control over its digital ecosystem. These dimensions include telecommunications infrastructure, digital platforms, data centers, cloud computing, data governance, cybersecurity, regulatory institutions, multinational technological collaborations, and the geographic and geopolitical position of essential digital infrastructure. Particular attention is paid to the distinction between digital transformation and digital sovereignty. Digital transformation may increase connectivity, government services, economic activity and technological capabilities, but alone does not ensure national digital sovereignty.

A country might build digital infrastructure but still rely on foreign technology providers, cloud platforms, equipment vendors, technical skills or external financing. Thus, the study evaluates not only whether Syria is building digital infrastructure, but also who controls it, where key data is held, who provides essential technology, and how much strategic autonomy Syrian institutions enjoy. The conceptual synthesis also explores the relationship between digital sovereignty and other policy areas. Digital sovereignty is intimately linked to cybersecurity, personal data protection, economic development, national security, and digital governance. However, this study intentionally focuses its main analysis on the infrastructure, governance and geopolitical dimensions of digital sovereignty. Cybersecurity and data protection are viewed as crucial components of the broader digital environment. Still, they are not studied as autonomous policy domains except to the extent that they directly impact national authority over digital infrastructure and information systems. Similarly, the role of economic development is highlighted, since digital infrastructure can affect investment, employment, innovation and access to markets. However, the study does not aim to provide a thorough economic assessment. The research delimitation enables a focused examination of the strategic and institutional conditions needed for Syria to gain greater autonomy over its digital systems, while recognising that digital sovereignty is linked to broader policy domains. The study covers the political transition period from December 2024 to August 2026. This period is particularly important because it reflects an early stage of institutional and infrastructural change in Syria.

The analysis consequently highlights developments after the political transition, such as national digital plans, telecommunications measures, data infrastructure initiatives, digital government services, international technological collaborations and new regulatory measures. Information is considered in the particular temporal context because the digital environment is continually changing. As reconstruction unfolds, policies, agreements, infrastructure projects, and institutional arrangements may shift, so the findings should be understood as a snapshot of Syria's digital-sovereignty landscape at the time of this study, rather than a permanent characterisation of the country's digital system. The study also uses conceptual

triangulation to enhance the robustness of interpretation. Wherever possible, evidence from government sources is contrasted with academic research, foreign reports, media coverage and independent policy analysis. This approach is particularly pertinent in the Syrian context, as information addressing infrastructure development, foreign alliances, institutional reforms and geopolitical linkages may be partial or perceived differently by different stakeholders. Therefore, triangulation enables the detection of repeated patterns, while diminishing reliance on a single story. When evidence is sparse or arguably contestable, the analysis acknowledges the uncertainty rather than presenting individual statements as final. The whole research process can be viewed as a sequence of: source identification, documentary evaluation, topic classification, comparative interpretation and conceptual synthesis. First, sources relevant to Syria's digital transformation beyond 2024 are selected based on their relevance.

Secondly, papers are screened to gather information on infrastructure, governance, legislation, international partnerships and geopolitical influence. Third, evidence is organised around key analytic themes. Fourth, similarities and discrepancies across sources are analysed to identify significant advancements and recurring issues. Finally, the data are synthesised into a conceptual framework for understanding Syria's digital sovereignty and policy aspirations. This enables the study to move beyond a descriptive account of individual infrastructure developments and instead reflect on how they collectively shape Syria's strategic digital autonomy. Since the political revolution of December 2024, Syria has launched an ambitious initiative to build its digital infrastructure and administration. This process is framed by the National Digital Transformation Strategy to 2030. The strategy has three general phases: a basic phase focused on building infrastructure and legislation; a transition phase, from 2025 to 2027, to deliver interactive digital services; and a final phase, from 2027 to 2030, to deliver greater integration and data-driven governance. During the study period, Syria is in the second phase, which focuses on growing interactive services and translating foundational digital investments into practical government and citizen applications. This shift is particularly relevant to digital sovereignty, as the rise of services creates new needs for secure infrastructure, in-country technical capability, data governance and institutional control. Therefore, the approach utilised in this study can be used to assess not only Syria's progress toward digital transformation but also whether this transformation is leading to a more independent, resilient, and domestically managed digital ecosystem.

4. Results and Discussions

The picture provides an integrated view of Syria's evolving digital infrastructure and the interaction between regulatory laws, mobile networks, international connectivity, the national backbone, and data infrastructure.

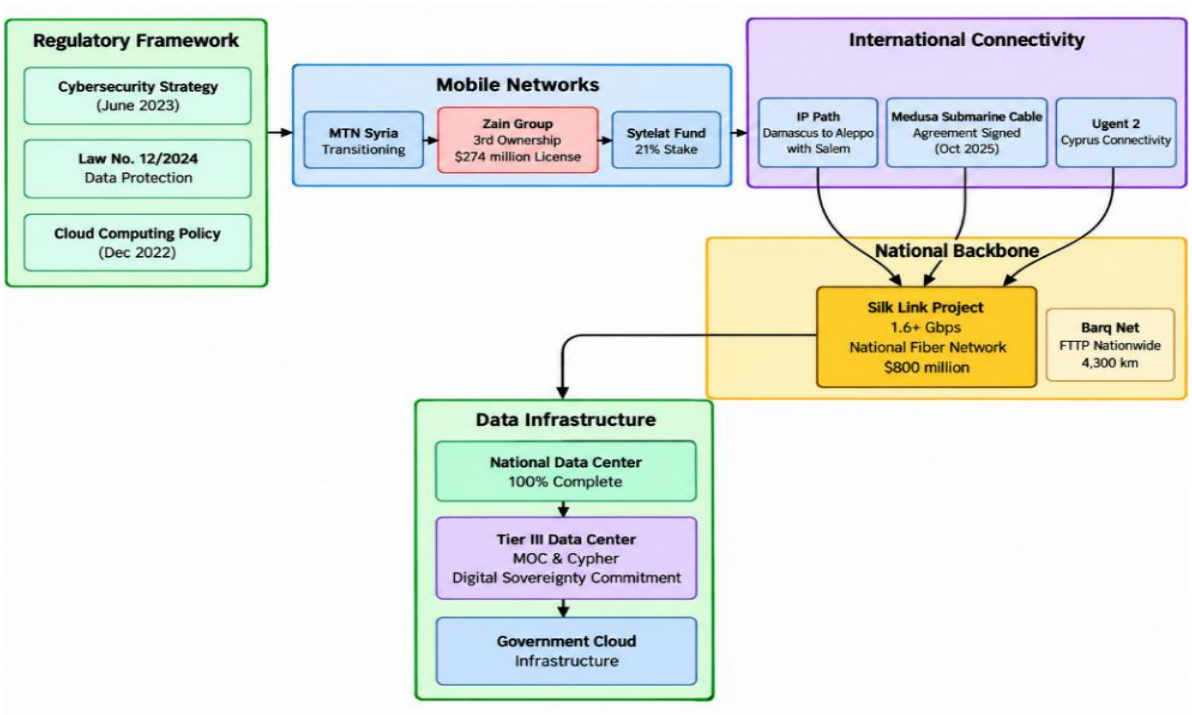


Figure 1: Syria's digital infrastructure ecosystem and key agreements

The institutional underpinning for digital development and data governance is a regulatory framework comprising the Cybersecurity Strategy, Data Protection Law No. 12/2024, and the Cloud Computing Policy. The mobile-network component identifies key telecommunications carriers and their ownership and investment patterns. International communication is via IP

channels from Damascus and Aleppo, the Medusa underwater cable and Ugarit 2 connectivity via Cyprus. These foreign links converge on the national backbone and include major projects such as the Silk Link Project, a national fiber-optic network with a projected investment of $800 million, and Barq Net's statewide FTTH network. The national backbone also supports the country's data infrastructure, including the National Data Center, Tier III Data Center and Government Cloud Infrastructure. The Tier III facility provides the latest data management and encryption capabilities and supports digital sovereignty. The picture depicts the interconnectivity of Syria's digital ecosystem, including its regulatory framework, telecommunications networks, international connection, fiber-optic backbone, and data centers, which can enable national digital transformation, secure data management, and enhanced connectivity. Figure 1 provides a visual overview of Syria's digital infrastructure ecosystem and the key agreements that shape it.

4.1. Silk Link: The Flagship Project

Silk Link is the centerpiece of Syria's digital infrastructure strategy. The paper aims to build a 4,500 km fiber-optic network across the country and establish data centers and international subsea cable landing stations. The paper will "provide high data transfer capacities and greater reliability, enabling telecom operators in Syria and the region to offer advanced communication services, and support digital applications, cloud services and the Internet of Things" (Developing Telecoms, 2026). In February 2026, Saudi Arabia's stc Group won the competitive tender to build the project, acquiring a 75% stake for SAR 3 billion ($800 million), with the Syrian Sovereign Fund holding the remaining 25%.

Table 1: Major digital infrastructure agreements in Syria (2025-2026)

Project/Agreement	Partner	Investment	Ownership Structure	Status	Sovereignty Implications
Silk Link	stc Group (Saudi)	$800 million	stc 75%, Syrian Fund 25%	Tender Won; Construction	Majority foreign ownership of backbone
Zain Mobile License	Zain Group (Kuwait)	$747 million + $10M fees	Zain 75%, Syrian Fund 25%	Awarded; Launch 2027	Majority foreign ownership of mobile operator
Tier III Data Center	MDC & Cypher (Saudi)	Undisclosed	Syrian-Saudi JV	Partnership Established	Data localization commitment
Medusa Cable	Medusa Submarine Cable System	Undisclosed	Syrian Telecommunications Co.	Agreement Signed	International connectivity
Barq Net	Syrian Ministry	Government-funded	100% Syrian	Deployment	National last-mile infrastructure
IP PoPs	Salam (Saudi)	Undisclosed	Partnership	MoU Signed	Direct global Tier-1 access

This represents "the first major foreign direct investment into the reconstruction of the country's telecoms network". The Silk Link project has sparked significant debate over its implications for Syrian digital sovereignty. As one analysis notes, the paper "was presented to the public as a technical investment to rehabilitate digital infrastructure under the umbrella of stc. But behind the reassuring investment language, a more complex geopolitical equation unfolds: whoever owns the code, owns the decision." Table 1 summarizes the key terms of the Silk Link agreement and other major infrastructure projects.

4.2. Mobile Network Licensing

In a significant development for Syria's telecommunications sector, the government launched an international tender for a new mobile network operator license valid for 20 years in March 2026. The government awarded the license to Kuwait's Zain Group for $747 million, with an additional $10 million paid in first-year optional spectrum fees. The paper is expected to attract around $800 million in direct and indirect investment over the next seven years, bringing the total value to more than $1.5 billion. The ownership structure mirrors that of Silk Link: Syria's sovereign wealth fund will hold a 25% stake, while Zain Group will own the remaining 75%. The license includes access to key frequency bands, including 800 MHz, 2600 MHz, and 3500 MHz, enabling 5G deployment. The new operator is expected to expand nationwide mobile coverage, improve service quality, and create jobs. The licensing process has been described as "a central component of Syria's broader telecommunications reform agenda and economic recovery strategy". The paper is linked to the Silk Link initiative, with both projects together forming "the foundation of Syria's long-term digital infrastructure strategy".

4.3. Data Center Infrastructure

Data center infrastructure is a critical component of Syria's digital sovereignty strategy. The National Data Center has been completed and is described as "one of the most important pillars of infrastructure". Government cloud services have been expanded, and digital signature systems have been rolled out. In a significant development, Syrian company MDC partnered with Saudi cybersecurity firm Cypher to establish Syria's first Tier III data center. According to web science and data management specialist Mohammad Tawfiq Nahlawi, this partnership "goes beyond being a commercial or technical agreement" and represents "a foundational step toward building a national digital infrastructure capable of supporting digital transformation, strengthening information sovereignty, and preparing the country for a data-based economy". Under the partnership, the center will provide "an integrated system of cloud hosting, cybersecurity, and round-the-clock digital security operations services for government bodies, banking institutions, and private companies". It also includes "a full commitment to digital sovereignty standards and keeping data inside Syrian territory".

4.4. International Connectivity

Syria has made significant progress in enhancing its international connectivity. In October 2025, Syria signed an agreement with Barcelona-based Medusa Submarine Cable System to land its first international undersea cable at the port of Tartous. The cable system will connect 12 countries across North Africa and southern Europe, "creating a corridor that links the Mediterranean to the Atlantic Ocean and the Red Sea". The Ugarit 2 project, launched to improve Syria's international digital connectivity through Cyprus, represents "an important step in strengthening Syria's communications infrastructure". In 2025, a Memorandum of Understanding with Saudi Arabia's Salam for establishing international IP Points of Presence (PoPs) in Damascus and Aleppo signaled "the potential to enhance Syria's direct access to global Tier-1 connections".

4.5. Regulatory Framework

Syria has established a regulatory framework to support its digital transformation. Key elements include a national cloud computing policy adopted in December 2022, a cybersecurity strategy adopted in June 2023, and Law No. 12 of 2024 on electronic personal data protection. The data protection law aims to "preserve the privacy of citizens' data and regulate the process of collecting, processing, and using it on the network", with financial penalties that may reach 12 million Syrian pounds and imprisonment of up to three years. The Ministry of Communications and Technology has emphasized that "the legal framework provides guarantees and exemptions designed to encourage long-term partnerships and promote knowledge transfer and innovation". The ministry is working to "improve the level of digital security in financial applications" and "enhance awareness and training in the field of cybersecurity".

4.6. Infrastructure Sovereignty

Infrastructure sovereignty refers to control over physical networks, data centers, and connectivity infrastructure. In Syria's case, this dimension is particularly salient given the scale of foreign investment in backbone infrastructure. The Silk Link project raises significant questions about infrastructure sovereignty. With stc Group holding a 75% stake, the paper represents majority foreign ownership of Syria's primary fiber-optic backbone. As one analysis notes, "when servers are managed through cross-border companies, and when operating systems are written outside borders, the question becomes legitimate: Does the state remain the owner of its platform, or does it become a user within a larger system?" The Zain mobile license follows a similar ownership structure, with Zain Group holding 75% and the Syrian Sovereign Fund holding 25%. While this brings needed investment and expertise, it also means that critical mobile infrastructure is controlled by a foreign entity. However, not all infrastructure projects follow this pattern. The Barq Net last-mile fiber initiative is government-funded and 100% Syrian-owned. The National Data Center is also fully Syrian-owned and operated. This mixed ownership structure reflects a pragmatic approach that balances the need for foreign investment with preserving sovereignty over critical infrastructure.

4.7. Data Sovereignty

Data sovereignty—control over data storage, processing, and transfer—is a critical dimension of digital sovereignty. Syria has taken steps to strengthen data sovereignty through data localization requirements and by building domestic data center capacity. The Tier III data center partnership between MDC and Cypher includes "a full commitment to digital sovereignty standards and keeping data inside Syrian territory". This matters because it ensures sensitive government and citizen data remains within Syria's legal jurisdiction, protected by Syrian law rather than foreign legal regimes. Law No. 12 of 2024 on electronic personal data protection provides a legal framework for data protection. The law regulates "the process of collecting, processing, and using data on the network" and establishes penalties for violations. However, the framework's effectiveness depends on implementation capacity, which remains limited. The National Data Center, which is 100% complete, serves as the central repository for government data.

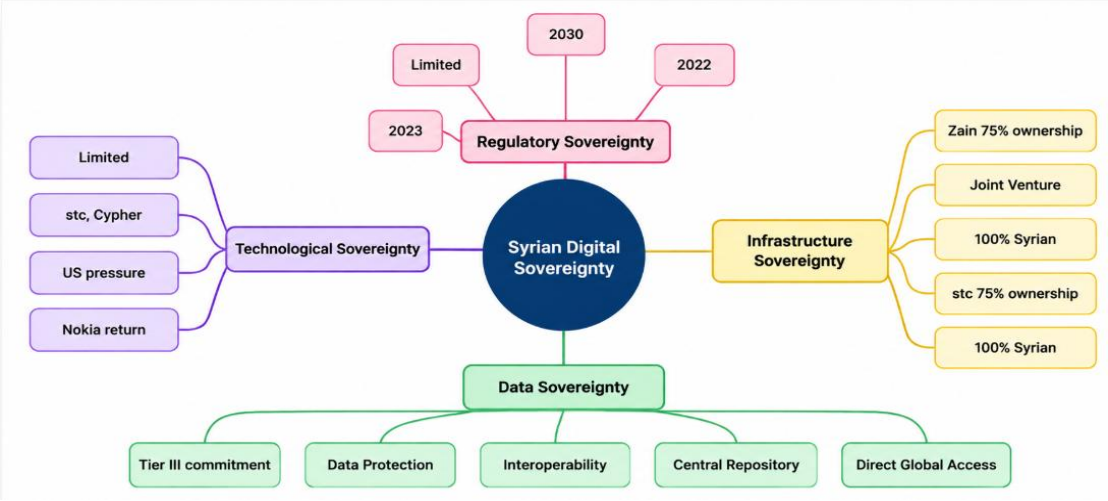


Figure 2: Dimensions of digital sovereignty in Syria

The strategy envisions a national database comprising at least eight government registries: civil registry, vehicle registry, family card registries, electronic registry, support registries, migration and passport registries, commercial registry, industrial registry, and a general registry of state employees. Figure 2 illustrates the key dimensions of digital sovereignty and their interconnections.

4.8. Technological Sovereignty

Technological sovereignty refers to the capacity to develop or procure technology on terms that serve national interests. This includes choices about technology standards, supply chains, and partnerships. Competition among foreign technology providers shapes Syria's technological sovereignty. Nokia's return to Syria has "opened the door for reintroducing European standards in equipment provision and knowledge transfer, particularly in cybersecurity and supply chain transparency". Meanwhile, Gulf technology providers from Saudi Arabia, Qatar, and the UAE play an increasingly prominent role. The United States has reportedly pressured Syria to avoid relying on Chinese telecommunications technology, arguing it conflicts with US interests and threatens US national security. Syria is reportedly "exploring the possibility of procuring Chinese technology to support its telecommunications base stations and local internet service providers' infrastructure". This pressure reflects broader US-China competition over technology standards and supply chains. The choice of technology partners has significant implications for technological sovereignty. Different providers offer different terms regarding technology transfer, local content requirements, and long-term maintenance and upgrade commitments. The risk-governed framework for digital-economy FDI emphasizes that investment must be "judged by quality rather than volume: technology transfer, local linkages, interoperability, competition, data protection, cybersecurity, financial integrity, human-capital development, and measurable reconstruction outcomes".

4.9. Regulatory Sovereignty

Regulatory sovereignty refers to the capacity to establish and enforce rules governing digital activities within national territory. This includes data protection laws, cybersecurity regulations, and competition policy. Syria has established a regulatory framework that includes a cybersecurity strategy, a cloud computing policy, and data protection legislation. However, the framework's effectiveness depends on implementation capacity, which remains limited. The Ministry of Communications and Technology continues to work on "improving the level of digital security in financial applications" and "enhancing awareness and training in the field of cybersecurity". The Syrian Cybersecurity Summit 2026, held in August 2026 with participation from more than 500 experts, addressed "cyber law, artificial intelligence, response to cyber threats, industrial systems security, human factors, and innovation".

The summit emphasized that "cybersecurity has become a national issue that affects the economy, government services, and the life of citizens". The Director General of the National Authority for Information Technology Services noted the continued activation of the National Security Operations Center (SOC) and the Computer Emergency Response Team (CERT), as well as the establishment of a backup data center in Aleppo to ensure business continuity. The author emphasized that "regional partnerships and support for entrepreneurship and specialized national companies are an essential path to building a Syrian cyber sector capable of producing digital solutions".

5. Geopolitical and Techno-Political Dynamics

5.1. The Geopolitical Landscape

Syria's digital transformation unfolds in a complex geopolitical environment. Multiple actors with competing interests are seeking to shape Syria's digital infrastructure:

- **Gulf States**: Saudi Arabia, Qatar, and the UAE have emerged as the dominant investors in Syria's digital infrastructure. The stc Group's $800 million investment in Silk Link, GO Telecom's agreement to modernize Syria's digital infrastructure, and the partnership between MDC and Cypher for the Tier III data center all reflect growing Gulf engagement. The Zain mobile license, awarded to Kuwait's Zain Group, represents another significant Gulf investment.
- **European Actors**: The easing of EU sanctions in May 2025 has opened the door for European engagement. Nokia's return to Syria has "opened the door for reintroducing European standards in equipment provision and knowledge transfer". The EU's removal of 24 entities from its sanctions list, including companies in the telecommunications sector, has created new opportunities for European investment.
- **US Pressure**: The United States has reportedly warned Syria against relying on Chinese technology in its telecommunications sector, arguing it conflicts with US interests and threatens US national security. This pressure reflects broader US-China competition over technology standards and supply chains.
- **Iranian Influence**: The involvement of Iranian-linked actors, such as the ownership structure of the third operator, Wafa Telecom, raises concerns. The presence of multiple, sometimes competing, international actors creates both opportunities and risks for Syria.

5.2. Techno-Political Rivalry

The concept of techno-politics helps explain the dynamics of Syria's digital transformation. Techno-politics refers to how technological choices and infrastructure decisions are shaped by, and shape, political power relations.

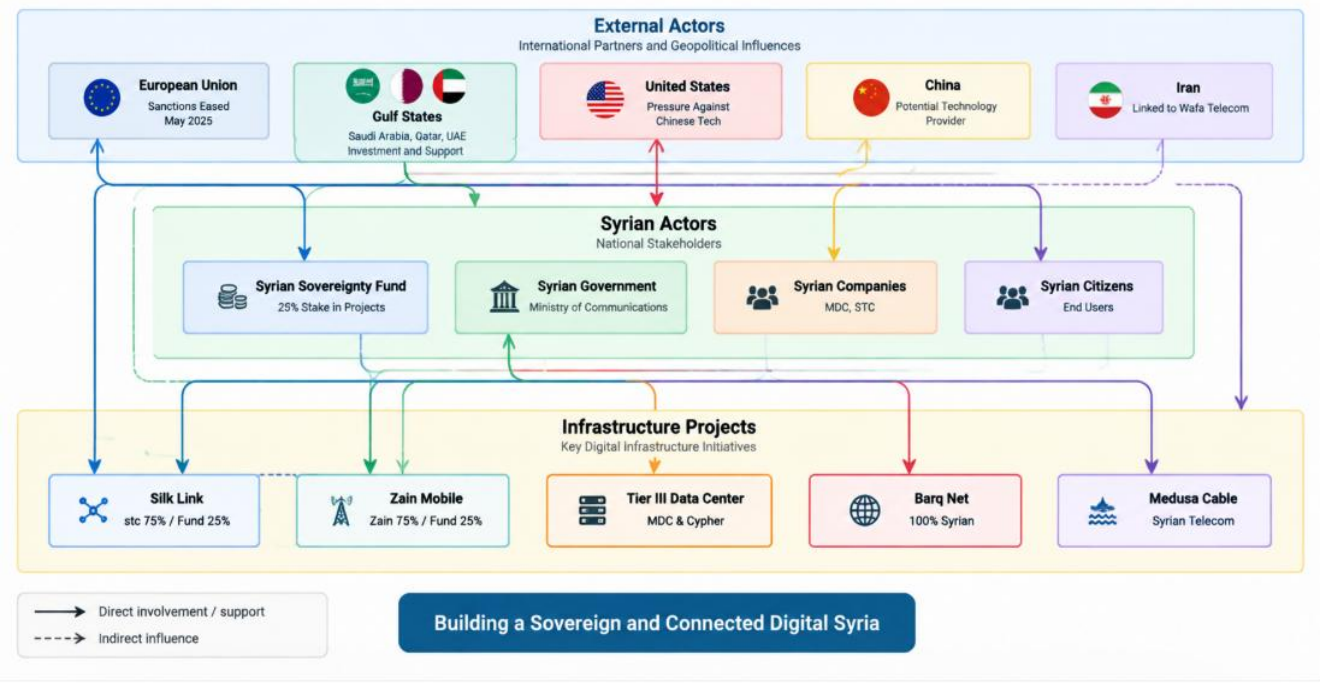


Figure 3: Geopolitical and techno-political dynamics

The Silk Link project exemplifies techno-political dynamics. As one analysis notes, "behind the reassuring investment language, a more complex geopolitical equation unfolds: whoever owns the code, owns the decision". The paper is not merely about connectivity; it is about "redefining the state in an era where power is shifting from geography to data". The competition among technology providers—Gulf, European, Chinese, and others—reflects broader geopolitical rivalries. Each provider offers different terms regarding technology transfer, local content, and long-term commitments. The choice among them has

significant implications for Syria's technological sovereignty. Figure 3 illustrates the geopolitical and techno-political dynamics shaping Syria's digital sovereignty.

5.3. The Sanctions Context

The easing of international sanctions has been a critical enabler of Syria's digital transformation. In May 2025, the EU adopted legal acts to lift nearly all economic sanctions on Syria. As part of the package, 24 entities, including the Central Bank of Syria and companies in key sectors such as oil production and refining, cotton, and telecommunications, were delisted from the EU's fund-freezing regime. The easing of sanctions has "opened future horizons for European investors to invest in Syria in various projects, especially in infrastructure and the telecommunications and technology sector". Saudi Arabia's GO Telecom agreement to modernize Syria's digital infrastructure was described as "one of the first major private sector initiatives following the recent easing of Western sanctions". However, the sanctions easing is not complete. The EU retained restrictions based on security grounds. The US has maintained pressure on Syria regarding technology choices, particularly regarding Chinese technology. The sanctions context thus creates both opportunities and constraints for Syria's digital transformation.

5.4. The Role of the Syrian Diaspora

The Syrian diaspora—estimated in the millions—represents a significant resource for digital transformation. Many Syrians abroad have technical expertise, entrepreneurial experience, and financial resources that could contribute to reconstruction. However, engaging the diaspora requires building trust and creating mechanisms for their participation. The diaspora's relationship with Syria is complex, shaped by the conflict, displacement, and political divisions. Digital platforms could facilitate diaspora engagement in reconstruction, but this requires careful attention to governance and inclusion.

5.5. Emerging Technologies and Future Challenges

Emerging technologies—including artificial intelligence, blockchain, and the Internet of Things—present both opportunities and challenges for Syria's digital sovereignty. These technologies could enhance service delivery, improve efficiency, and support economic diversification. However, they also create new dependencies and vulnerabilities. Syria has discussed AI governance in regional forums and presented AI as a tool to improve government performance. However, there is no standalone national AI strategy or AI law. Developing such frameworks will be important to ensure that emerging technologies serve Syrian interests rather than creating new dependencies. This paper has examined the complex interplay between digital sovereignty and international partnerships in Syria's post-conflict reconstruction. The analysis yields several key findings. First, Syria's digital infrastructure development has accelerated significantly since the political transition of December 2024. Major initiatives—Silk Link, Barq Net, Medusa submarine cable, and Tier III data centers—are underway, attracting substantial foreign investment, particularly from Gulf states. Second, these partnerships raise fundamental questions about Syria's digital sovereignty.

The ownership structures of major projects—with foreign entities holding 75% stakes in both Silk Link and the Zain mobile license—create dependencies that could constrain Syrian autonomy over critical digital infrastructure. Third, Syria has taken steps to safeguard digital sovereignty, including data localization requirements, building domestic data center capacity, and developing a regulatory framework that includes data protection and cybersecurity legislation. However, implementation capacity remains limited. Fourth, Syria's digital sovereignty is shaped by complex geopolitical and techno-political dynamics. Competing powers—Gulf states, the European Union, the United States, China, and Iran—seek to shape Syria's digital infrastructure in ways that serve their interests. Syria must navigate between these competing actors while safeguarding its own interests. Fifth, digital sovereignty in Syria is not binary but contested and negotiated. Different projects and agreements have different implications for sovereignty, and the overall trajectory depends on the cumulative effect of multiple decisions and partnerships.

6. Conclusion

Syria's digital transformation represents both an immense opportunity and a profound challenge for digital sovereignty. The opportunity lies in the potential to leapfrog traditional development pathways, to build a more efficient, transparent, and inclusive state, and to position Syria as a regional hub for technology and innovation. The challenge lies in navigating the complex geopolitical and techno-political dynamics that shape digital infrastructure development, balancing the urgent need for foreign investment and technology transfer with the imperative of protecting national sovereignty over critical digital systems. The foundation for this transformation is being laid. The Silk Link fiber-optic network, the Medusa submarine cable, the Tier III data center, and the Zain mobile license are tangible manifestations of a commitment to digital modernization. The National Digital Transformation Strategy provides a framework extending to 2030. Easing sanctions has opened the door to increased international engagement. However, infrastructure alone is insufficient. Syria's digital transformation will ultimately

depend on the quality of governance, the depth of human capital, and the effectiveness of efforts to safeguard digital sovereignty. As one analysis notes, "when servers are managed through cross-border companies, and when operating systems are written outside borders, the question becomes legitimate: Does the state remain the owner of its platform, or does it become a user within a larger system?" The path forward requires strategic sequencing, careful attention to governance and sovereignty, and a commitment to learning from both successes and failures in other contexts. The risk-governed approach to foreign investment, embedding cybersecurity as a design principle, and leveraging the Syrian diaspora's expertise offer pathways to navigate the tensions between urgency and sustainability, and between foreign engagement and national sovereignty. Syria's digital sovereignty is not merely about technology; it is about rebuilding the social contract between state and citizen, about creating opportunities for a generation that has known only conflict, and about re-establishing Syria's place in the regional and global economy. The stakes could not be higher. The opportunity, however, is real.

6.1. Recommendations

Based on the analysis, the following recommendations are offered for safeguarding Syria's digital sovereignty while enabling reconstruction:

- **Adopt a Risk-Governed Approach to Foreign Digital Investment:** Digital-economy FDI should be evaluated by quality rather than volume, with attention to technology transfer, local linkages, data protection, cybersecurity, and measurable reconstruction outcomes. Contract terms should protect Syrian interests and ensure long-term benefits. The 75% foreign ownership in major projects should be carefully reviewed, and future agreements should include stronger provisions for technology transfer and local capacity building.
- **Strengthen Institutional Capacity for Digital Governance:** The institutions responsible for digital transformation—particularly the Ministry of Communications and Technology and the regulatory authority—need stronger capacity in human resources, technical expertise, and coordination mechanisms. This includes building the capacity to negotiate, implement, and enforce complex technology agreements.
- **Diversify Technology Partners:** Reliance on a single foreign provider or group of providers creates dependency risks. Syria should diversify its technology partnerships across multiple providers and regions, including European, Gulf, and potentially Asian sources, to reduce vulnerability to any single partner's political or commercial decisions.
- **Prioritize Data Localization and Sovereignty:** The commitment to keeping data inside Syrian territory, exemplified by the Tier III data center partnership, should be maintained and strengthened. Clearly specify data localization requirements in all agreements, and develop enforcement mechanisms.
- **Develop Indigenous Technological Capacity:** Long-term digital sovereignty depends on indigenous technological capacity. This requires sustained investment in education and training, particularly in cybersecurity, data science, and network engineering. Expand the Digital Innovation Center (DIGIT) and strengthen partnerships with universities and research institutions.
- **Enhance Cybersecurity Posture:** Cybersecurity is both a component of and a prerequisite for digital sovereignty. The National Security Operations Center (SOC) and Computer Emergency Response Team (CERT) should be fully operationalized. The backup data center in Aleppo should be completed. Regular cybersecurity exercises and training programs should be conducted.
- **Strengthen the Regulatory Framework:** While Syria has established a regulatory framework including data protection and cybersecurity legislation, implementation capacity remains limited. Enforcement mechanisms should be strengthened, and public awareness of digital rights and responsibilities should be enhanced.
- **Engage the Syrian Diaspora:** The Syrian diaspora represents a significant resource for digital transformation. Develop mechanisms to engage the diaspora in knowledge transfer, mentorship, investment, and innovation. Digital platforms could facilitate diaspora engagement in reconstruction.
- **Develop a National AI Strategy:** While Syria has discussed AI governance in regional forums, there is no standalone national AI strategy or AI law. Developing such frameworks is important to ensure emerging technologies serve Syrian interests rather than creating new dependencies.
- **Monitor and Evaluate Digital Sovereignty:** Digital sovereignty is not static; it requires ongoing monitoring and evaluation. Syria should develop indicators to track its digital sovereignty across multiple dimensions—infrastructure, data, technology, and regulation—and use these indicators to inform policy decisions.

6.2. Limitations and Future Research

This paper has several limitations. The analysis is based on publicly available sources and may not capture all relevant developments, particularly those not reported in international media. Syria's rapidly changing political and economic situation means some findings may quickly become dated. The paper focuses primarily on state-level dynamics and does not fully explore the role of civil society, informal digital economies, or the private sector beyond major telecommunications companies. Future

research should address these gaps. Future research should examine the role of the Syrian diaspora in digital sovereignty; the potential of blockchain and other emerging technologies to enhance digital sovereignty; the gender dimensions of digital inclusion and sovereignty; the relationship between digital sovereignty and transitional justice; and a comparative analysis of digital sovereignty across Syria's governorates.

Acknowledgment: The authors gratefully acknowledge the academic support, institutional resources, and valuable contributions provided by Al-Shahbaa Private University, Tishk International University, Keio University, Merlion Manufacturing, Clarke Quay Group, and Sentosa Exports Pte Ltd. Their encouragement and support are sincerely appreciated throughout the research process.

Data Availability Statement: The corresponding author can provide the data upon reasonable request.

Funding Statement: This research received no external funding or financial support.

Conflicts of Interest Statement: The authors declare no conflicts of interest. All sources have been appropriately cited.

Ethics and Consent Statement: The study followed ethical standards. Informed consent was obtained, and participant privacy and confidentiality were maintained.

References

1. Access Now, "Reclaiming Syria's digital future," *Access Now*, 2025. [Accessed by 22/08/2025].
2. Arab News, "Saudi GO Telecom signs deal to rebuild Syria's telecom sector," *Arab News*, 2025. [Accessed by 01/09/2025].
3. J. Tanner, "Stc wins bid for Syria's US$800m Silklink fibre project," *Developing Telecoms*, 2026. [Accessed by 09/06/2026].
4. Enab Baladi, "Data, the silent engine of Syria's reconstruction," *Enab Baladi*, 2026. [Accessed by 17/06/2026].
5. European Council, "Syria: EU adopts legal acts to lift economic sanctions on Syria, enacting recent political agreement," *European Council Press*, 2026. [Accessed by 08/06/2026].
6. D. S. Haji, S. Mustafa, and K. M. Mousa, "Digital public administration and fiscal legitimacy in post-conflict settings," *Frontiers in Political Science*, vol. 8, no. 5, pp. 1–17, 2026.
7. B. Jansen, N. Kadenko, D. Broeders, M. van Eeten, K. Borgolte, and T. Fiebig, "Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions," *Government Information Quarterly*, vol. 40, no. 4, pp. 1–13, 2023.
8. Syrian Arab Republic, "A paper on digital development in Syria and the current reality," *ITU-D Study Group 2, Contribution 163, International Telecommunication Union (ITU)*, 2026. [Accessed by 26/06/2026].
9. Syrian Arab Republic, "Cybersecurity strategy in Syria," *ITU-D Study Group 2, Contribution 128, International Telecommunication Union (ITU*), 2024. [Accessed by 29/05/2024].
10. J. Edler, K. Blind, H. Kroll, and T. Schubert, "Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means, *Research Policy*, vol. 52, no. 6, pp. 1–13, 2023.
11. J. Pohle and T. Thiel, "Digital sovereignty," *Internet Policy Review*, vol. 9, no. 4, pp. 1–19, 2020.
12. A. C. Arslan, "Syria's Contested Digital Sovereignty: Technology Agreements and Techno-Political Rivalry in Syria's Reconstruction 2024–2025," *Post-Conflict Rebuilding in Syria Symposium*, İstanbul, Turkey, 2025.
13. F. Dalatey, "Washington presses Syria to shift from Chinese telecom systems," *Reuters,* 2026. [Accessed by 28/06/2026].
14. Syrian Arab News Agency (SANA), "Communication Ministry announces starting the first phase of Ugarit project '2'," *Syrian Arab News Agency (SANA)*, 2025. [Accessed by 01/08/2025].
15. Syrian Arab News Agency (SANA), "Minister: Syria to become regional data-transmission hub," *Syrian Arab News Agency*, 2025. [Accessed by 23/02/2026].
16. Syrian Arab News Agency (SANA), "Syria accelerates nationwide digital transformation across public institutions," *Syrian Arab News Agency (SANA)*, 2026. [Accessed by 30/06/2026].
17. Syrian Arab News Agency (SANA), "Syria signs first international submarine cable deal to strengthen connectivity," *Syrian Arab News Agency*, 2025. [Accessed by 29/01/2026].
18. Syrian Arab News Agency (SANA), "Syria launches international tender for 20-year mobile network license," *Syrian Arab News Agency (SANA)*, 2026. [Accessed by 30/06/2026].
19. Syrian Arab News Agency (SANA), "Syria's Zain mobile network to launch within six months, regulator says," *Syrian Arab News Agency (SANA)*, 2026. [Accessed by 30/06/2026].
20. The New Arab, "Syria signs landing deal for first international submarine cable," *The New Arab*, 2025. [Accessed by

25/01/2026].
21. United Nations Economic and Social Commission for Western Asia (UNESCWA), "Technology to reduce the generational impact of conflict," *United Nations Economic and Social Commission for Western Asia (UNESCWA)*, 2025. [Accessed by 05/02/2026].
22. World Bank Group, "Accelerating digital transformation in fragile and conflict affected situations," *World Bank Group*, 2025. [Accessed by 13/08/2025].
23. World Bank Group, "The Syrian conflict: Physical damage and reconstruction assessment (2011–2024)," *World Bank Group*, 2025. [Accessed by 31/11/2025].
24. K. Abedalrhman "Digital-economy FDI for post-conflict reconstruction: A risk-governed framework for investment quality, institutional trust, and technology transfer in Syria," *Zenodo*, 2026. [Accessed by 30/07/2026].
25. H. AbdulKader, E. ElAbd, and W. Ead, "Protecting online social networks profiles by hiding sensitive data attributes," *Procedia Computer Science*, vol. 82, no. 5, pp. 20–27, 2016.
26. S. Temara, "The ransomware epidemic: Recent cybersecurity incidents demystified," *Asian Journal of Advanced Research and Reports*, vol. 18, no. 3, pp. 1–16, 2024.
27. S. Temara, "Harnessing the power of artificial intelligence to enhance next-generation cybersecurity," *World Journal of Advanced Research and Reviews*, vol. 23, no. 2, pp. 797–811, 2024.
28. M. S. Miah and M. S. Islam, "Big data analytics architectural data cut off tactics for cyber security and its implication in digital forensic," in *Proc. 2022 Int. Conf. Futuristic Technol. (INCOFT)*, Belgaum, India, 2022.
29. C. R. Katru, S. Srinivasan, T. G. M. Kumar, S. Yadwad, G. Satish, and R. Maranan, "Enhancing sovereign allocation of resources in cloud milieus using a causal dilated geometric algebra approach for dynamic scalability," in *Proc. 2025 Int. Conf. Mach. Learn. Autonomous Syst. (ICMLAS)*, Prawet, Thailand, 2025.

Publisher's Note: *The publisher remains impartial concerning jurisdictional claims in published maps and institutional affiliations. Responsibility for the content rests entirely with the authors and does not necessarily reflect the publisher's perspectives.*