FMDB *Transactions on Sustainable Intelligence and Security*

Cybersecurity Governance: Toward an Institutional and Legislative Framework for Protecting the National Digital Space

Ivan Tan Wei Han[1], Jouma Ali Al-Mohamad[2,*], Deepa Indira Nair[3], Alexander Garcia[4], Yuto Okuda[5], Jovan Zigic[6]

[1]Department of Computing and Information Systems, Singapore Management University, 81 Victoria Street, Singapore.
[2]Department of Computer and Mobile Communication Engineering, Faculty of Information Engineering, Al-Shahbaa Private University, Aleppo, Syria.
[3]Department of Engineering Technologies, Swinburne University of Technology, Melbourne, Victoria, Australia.
[4]Department of Mathematics, Texas A&M University, College Station, Texas, United States of America.
[5]Department of Information and Communication Engineering, The University of Tokyo, Bunkyo-ku, Tokyo, Japan.
[6]Department of Mathematics and Statistics, McMaster University, Hamilton, Ontario, Canada.
ivan.t.2025@phdcs.smu.edu.sg[1], jalmohamad@su.edu.sy[2], dnair@swin.edu.au[3], alexandergarcia3@tamu.edu[4], yutookuda@logos.t.u-tokyo.ac.jp[5], zigicj@mcmaster.ca[6]

Abstract: The fall of the Assad regime in December 2024 and the emergence of a transitional government under Ahmed al-Sharaa have placed Syria at a critical juncture in redefining its approach to cybersecurity governance. This paper provides a comprehensive analysis of Syria's cybersecurity governance framework, examining the institutional, legislative, and operational dimensions of protecting the national digital space in the post-conflict era. Through documentary analysis of Syria's cybersecurity laws and regulations, assessment of institutional capacities, and examination of the transitional legal challenges facing the new government, this study identifies critical gaps and opportunities in Syria's cybersecurity governance architecture. The analysis shows that while Syria has made significant legislative progress since 2022, including the Cybercrime Law (No. 20 of 2022), the National Authority for Information Technology Services (Law No. 7 of 2023), and the Personal Data Protection Law (No. 12 of 2024), these instruments were developed under the previous authoritarian regime and present complex challenges for the transitional government. Cybersecurity requires institutional reform, legal revision, capacity building, international cooperation, and digital rights protection. The Cybercrime Law's vague and overly broad provisions threaten freedom of expression, the concentration of cybersecurity authority in a single state entity, the legacy of regime-focused rather than nationally oriented cybersecurity, and the lack of a comprehensive national cybersecurity strategy with clear implementation mechanisms.

Keywords: Transitional Government; Cybersecurity Governance; Information Technology Services; Cybercrime Law; Post-Conflict; Multi-Dimensional Framework; International Cooperation; Digital Ecosystem.

Received on: 22/09/2025, **Revised on:** 01/12/2025, **Accepted on:** 06/01/2026, **Published on:** 11/09/2026

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

DOI: https://doi.org/10.69888/FTSIS.2026.000806

Cite as: I. T. W. Han, J. A. Al-Mohamad, D. I. Nair, A. Garcia, Y. Okuda, and J. Zigic, "Cybersecurity Governance: Toward an Institutional and Legislative Framework for Protecting the National Digital Space," *FMDB Transactions on Sustainable Intelligence and Security*, vol. 1, no. 3, pp. 199–210, 2026.

Copyright © 2026 I. T. W. Han *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.

[*]Corresponding author.

1. Introduction

Post-conflict governance of cybersecurity presents a unique set of challenges as states are tasked with rebuilding damaged digital infrastructure, restoring institutional authority, creating effective legal structures, and managing ongoing security threats all at once [1]. As opposed to stable states, post-conflict countries often have limited financial resources, damaged administrative structures, a shortage of skilled personnel, and low public trust. These conditions render cybersecurity governance inseparable from broader state-building and institution-building processes [2]. Thus, the fall of the Assad regime in December 2024 has created a very significant context in which to study how Syria can transform its cybersecurity governance architecture. The establishment of a transitional government under the leadership of Ahmed al-Sharaa has provided an opportunity to revisit the institutional and legislative legacy of the previous political system and to tackle immediate vulnerabilities in the country's digital space. In this sense, cybersecurity governance must go beyond technical protection to include institutional accountability, legislative clarity, digital rights, public-private cooperation, international engagement, and sustainable capacity development [3]. Cybersecurity governance post-conflict needs a coordinated relationship between the state, private-sector organisations, civil society, technical communities and international partners. While government institutions set national priorities and legal requirements, a significant portion of the infrastructure supporting national digital services is often operated by private organisations [4]. Civil society organisations and independent technical communities can contribute to the protection, awareness and monitoring of digital rights, while international organisations can offer technical assistance, training and institutional support. Thus, the effectiveness of cybersecurity governance hinges on whether these actors can operate within a coherent national framework. Responsibilities divided can lead to overlapping mandates, unclear accountability and inefficient response to cyber incidents [5].

This problem is especially salient for Syria, where years of conflict have led to institutional fragmentation and less coordination across government agencies. Post-conflict cybersecurity governance has been studied, and a number of key factors that may affect successful reconstruction have been identified. Research conducted based on the Cybersecurity Capacity Maturity Model for Nations (CMM) emphasises the importance of a systematic assessment of national cybersecurity capabilities, identification of institutional and technical vulnerabilities, and the development of strategies in accordance with internationally recognised standards. Such approaches are useful for countries with emerging cybersecurity institutions as they provide a structured basis for measuring progress in policy, legal, organisational, technical and capacity-building dimensions [6]. For Syria, a maturity-based approach could identify the most pressing weaknesses in government networks, critical infrastructure protection, incident response, cybersecurity education, legal enforcement and national coordination. However, the implementation must consider the specificities of Syria post-conflict and not simply replicate models designed for stable countries [7]. Comparative research has also identified a number of core components of a working national cybersecurity framework. These include secure identification systems, public key infrastructure, computer incident response teams, electronic transaction legislation, cybercrime legislation and data protection laws. Together, these elements provide the institutional and technical basis for a secure digital economy. Identification systems allow trusted access to public services [8]. Public key infrastructure allows authentication and secure electronic communication. Computer incident response teams provide ways to detect and respond to cyber incidents and cybercrime, and data protection laws provide legal limits to digital activity and protections for individuals and organisations [9].

Electronic transaction laws are particularly important for economic recovery, as secure digital commerce can facilitate financial activity, government services, and private-sector growth. It is therefore important to assess Syria's cybersecurity governance framework not only in terms of the existence of individual laws and institutions, but also in terms of the effectiveness of their cooperation. The concept of cyber peacebuilding offers another perspective to understand cybersecurity governance in post-conflict Syria [10]. Cyber peacebuilding links cybersecurity with the broader goals of sustainable peace, human rights, social stability and inclusive governance. Its four priorities—access and cybersecurity, human rights, multi-stakeholder governance and stability—are interrelated. This is especially important for Syria, where cybersecurity institutions cannot be legitimate in the long term unless they are perceived as instruments of surveillance or political power [11]. A rights-respecting cybersecurity framework should protect citizens from cybercrime and malicious activity, as well as establish safeguards against unlawful surveillance, censorship, arbitrary data collection and misuse of government information systems. Such an approach could help restore public confidence in digital institutions and differentiate the emerging cybersecurity framework from the practices of the previous regime [12]. To understand the development of cybersecurity governance in Syria, the context of the country's conflict and authoritarian political structure is required. Academic research on cybersecurity governance in Syria has been limited, partly because of the difficulty of conducting research during the conflict and partly because of the slow development of formal cybersecurity institutions [13]. Earlier evaluations of Syria's digital environment documented the formation of a National Computer Incident Response Team (CIRT) within the National Agency for Network Service (NANS).

But these assessments also revealed important weaknesses in the area of formal cybersecurity regulation and the absence of well-documented national cybersecurity strategies [14]. This historical condition matters because it shows that Syria entered its post-conflict transition without a fully developed national cybersecurity governance framework. This authoritarian legacy

further complicated the development of public trust in digital institutions. Under the Assad regime, state control of communication infrastructure was coupled with extensive surveillance practices. Research has documented the use of deep-packet inspection to monitor and analyse the activities of Syrian Internet users. These capabilities are indicative of how technical infrastructure can be used for purposes beyond legitimate cybersecurity and into political surveillance [15]. The legacy of such practices poses a major governance challenge to the transitional government. National cybersecurity could benefit from the existing technical systems and institutional expertise, but the public's confidence can be damaged by their past applications. Institutional reform thus has to deal with both the technical functioning and the historical perception of cybersecurity institutions. This shift is based on a distinction between national cybersecurity and regime security. In authoritarian governance, the protection of the political leadership can be equated with the protection of national security [16]. However, a democratic or transitional approach to cybersecurity requires a broader approach, where the main objectives are the protection of citizens, critical infrastructure, public institutions, economic systems and sovereignty.

This change will require clear institutional mandates and legal protections. Sufficient authority is needed for cybersecurity agencies to respond to real threats, but they also need to operate within transparent legal boundaries [17]. Independent oversight, judicial mechanisms, parliamentary review where appropriate, and clear procedures for accessing sensitive information can help ensure that cybersecurity powers are not transformed into instruments of political repression. Another key dimension is the legislative evolution of Syria's cybersecurity framework. The Syrian state has issued several important legal instruments, such as the Cybercrime Law No. 20 of 2022, the establishment of the National Authority for Information Technology Services through Law No. 7 of 2023, and the Personal Data Protection Law No. 12 of 2024. These instruments are important steps toward the formalisation of digital governance. But their development under the previous political system creates challenges for the transitional government. The mere fact that there is legislation does not mean that cybersecurity governance is effective [18]. Laws must be clear, enforceable, consistent with broader legal principles, and supported by institutions capable of implementation. Transitional authorities therefore face the difficult task of reviewing inherited legislation while ensuring sufficient legal continuity to prevent the creation of regulatory gaps [1]. Researchers are especially worried about the Cybercrime Law because its broad or vague provisions could be interpreted to suppress legitimate expression. But in a post-conflict society, with its political uncertainty and heated public debate, it is particularly important to draw the line between real cybercrime and legitimate political speech [2].

Cybersecurity legislation should clearly define prohibited conduct and impose proportionate penalties while protecting legitimate expression, journalism, research and civil society activities [3]. Broad provisions may create uncertainty for citizens and businesses and may deter legitimate activity in the digital environment. This implies that legislative reform should seek to strike some balance between security needs and digital rights. Data protection is an additional essential component of cybersecurity governance. With more and more services being digitised by governments, public bodies are collecting and processing large amounts of personal data. Databases are vulnerable to attack by cybercriminals, foreign intelligence services, politically motivated actors or unauthorised insiders if they are not properly protected [4]. A strong data protection framework should set out principles for the lawful collection, storage, processing, sharing, retention and protection of personal information. It should also establish responsibilities for organisations that handle sensitive data, and provide ways in which individuals can challenge misuse [5]. Better data protection in Syria could help build public confidence in the digital government and facilitate the development of secure electronic services. Institutional concentration is another major issue in Syria's emerging cybersecurity governance structure. Having cybersecurity authority located in a single state agency can facilitate coordination and decision-making, particularly during emergencies. But over-concentration can also lead to risks of institutional dependency, limited oversight and abuse of power [12]. Good cybersecurity governance generally requires a distributed model, where strategic policy, technical incident response, law enforcement, critical infrastructure protection, data protection and digital rights responsibilities are appropriately coordinated, but not overly centralised.

The transitional government must therefore clarify institutional mandates and set up cooperation mechanisms between the relevant ministries, cybersecurity authorities, telecommunications providers, security institutions and private sector organisations [9]. International frameworks offer useful benchmarks for this institutional development. Important international approaches to cyber governance are the cybersecurity frameworks of the International Telecommunication Union [12] and the Budapest Convention on Cybercrime of the Council of Europe. Regional strategies on communications and information technology also provide an opportunity for Syria to engage with neighbouring states and regional institutions. International frameworks can help to harmonise legislation, promote technical cooperation, facilitate the sharing of information, build capacity and improve professional development [18]. But Syria's alignment with international approaches has to be customised to its domestic legal and institutional circumstances. International cooperation should strengthen national capacity, not create over-dependence on external institutions or technology providers. Comparisons show the importance of international cooperation and building up institutional capacities. Colombia's experience in developing cybersecurity in a post-conflict environment provides a useful example of how a developing country can embed cybersecurity within the broader national development agenda. Its experience emphasises the necessity of institutional strengthening, international cooperation, and the integration of cybersecurity policy with broader development strategies. The takeaway for Syria is that cybersecurity should

not be developed as a standalone technical sector [3]. Instead, it should be integrated into economic reconstruction, digital government development, telecommunications modernisation, education, financial reform and critical infrastructure rehabilitation.

Such integration can ensure that investments in information security directly contribute to the overall national recovery. Human capital is another basic requirement for good cybersecurity governance. No laws and institutions can be operated effectively without trained personnel to run them. The protracted Syrian war has displaced technical professionals and eroded educational and professional development systems [14]. The country could, therefore, find itself deficient in areas like network security, digital forensics, incident response, risk management, secure software development, cyber policy and critical infrastructure protection. Capacity building should be done through university education, professional certification, specialised government training, international exchanges and partnerships with private technology organisations. Syrian professionals abroad could also contribute to the country through knowledge transfer, remote collaboration, training, investment and eventual return to the country. Building a comprehensive national cybersecurity strategy is especially important to deal with these issues. A national strategy should set forth specific objectives, assign institutional responsibilities, identify critical infrastructure, set security standards, develop incident-response capabilities, and create mechanisms for cooperation between government and private-sector organisations [5]. It should also cover cybersecurity education, workforce development, research and innovation, international cooperation and digital rights. Crucially, the strategy must have measurable implementation mechanisms, instead of being a broad policy document. Clear timelines, institutional responsibilities, performance indicators, funding arrangements and review procedures can translate cybersecurity objectives into operational programs [11]. The transitional context also offers an opportunity to reconsider the relationship between cybersecurity and digital sovereignty. Digital sovereignty requires that the state exercise meaningful control over strategically important digital infrastructure, data and cybersecurity decision-making. But sovereignty doesn't mean technological isolation [6].

Outside assistance might be needed to modernise infrastructure, develop capabilities in security operations, obtain advanced cybersecurity technologies and train specialists. The challenge is to design external cooperation so that it builds domestic capacity, rather than substituting for it. Diversifying vendors, transferring technology, developing local expertise, securely hosting data and having transparent procurement can all help reduce dependency while enabling access to international technologies. However, the literature reveals important gaps in understanding the evolving cybersecurity governance framework in Syria. The current research considers separate aspects like cybercrime law, surveillance, institutional capability, international cooperation, or digital infrastructure [4]. However, there is a gap in holistic analysis of the integration of these aspects within the framework of Syria's post-2024 transition. The institutional, legislative and operational aspects of cybersecurity governance are interrelated, and weaknesses in one area can compromise progress in another [16]. Strong legislation cannot replace weak enforcement capacity, and advanced technical infrastructure cannot replace sufficient legal authority and trained personnel for sustainable protection [2]. The study thus fills an important gap by analysing Syria's cybersecurity governance as a multi-dimensional aspect of post-conflict state-building. It looks at the changing nature of cybersecurity institutions, the legal environment for cyber activities, the legacy of authoritarian surveillance, the problem of institutional concentration, the importance of capacity building, and international cooperation [14].

The analysis also explores how cybersecurity governance can be integrated with digital rights and public accountability. The study employs documentary evidence and comparative insights from other post-conflict contexts to identify weaknesses in Syria's existing governance architecture and to point to opportunities for institutional transformation. Ultimately, Syria's transition offers a unique chance to rebuild its cybersecurity governance system based on the principles of security, resilience, sovereignty, accountability, and digital rights [11]. The goal should not be to merely rebuild the cybersecurity institutions that were in place before the political transition, as this could lead to the re-emergence of the structural weaknesses and legitimacy problems of the previous system. Instead, the interim government must establish a mechanism that can protect national infrastructure, protect the rights of citizens, and maintain institutional accountability [9]. Such a framework needs legislative review, institutional restructuring, technical modernisation, professional capacity development, international cooperation and sustained investment in digital resilience. When these elements are developed together, cybersecurity can become a foundation for broader state reconstruction, rather than a source of institutional fragmentation. A secure and rights-respecting digital environment can foster public trust, support economic recovery, protect essential services and contribute to national sovereignty [10]. Therefore, the rebuilding of Syria's cybersecurity governance should be seen as part of the country's broader transition to stable, resilient and accountable state institutions.

2. Literature Review

Institutions, legislation, technical infrastructure, human capacity, international cooperation, and digital rights are increasingly mentioned in the literature on cybersecurity governance as dimensions of a multi-dimensional cybersecurity issue. These dimensions are especially relevant in post-conflict countries, where digital systems and governance institutions, as well as political and economic structures, often need to be rebuilt. Emergency Telecommunications Cluster [6] claims that

cybersecurity policies are often influenced by political priorities and may put national security in conflict with individual rights, of particular relevance for Syria, where the post- political transition requires revisiting the cybersecurity institutions created in an authoritarian system. Abdulghany [7] also describes how governments can use digital technologies for surveillance and political control. This is why cybersecurity reform in transitional states must address both technical capabilities and institutional legacies. Securitisation theory provides a powerful lens through which to view the politics of cybersecurity. Noone [4] argues that security problems are constructed through political processes where particular threats are presented as existential dangers, demanding exceptional responses. Applied to Syria, this perspective allows us to differentiate between cybersecurity designed to protect the state and cybersecurity designed primarily to protect a ruling regime. During the Assad era, digital security was tightly linked to regime stability and political control. The transition thus requires a shift toward a nationally focused cybersecurity that protects citizens, government institutions, critical infrastructure, and the broader digital ecosystem. Emergency Telecommunications Cluster [6] also notes that over-securitization may increase government control without necessarily improving overall social security. The other important research area is the protection of critical infrastructure and cybersecurity. More and more modern states rely on telecommunications, energy, financial services, health care, transportation and digital government systems.

International Telecommunication Union [12] defines cybersecurity resilience as the ability of systems to withstand, recover from and adapt to cyber disruptions. The relevance of this approach for Syria is that the long-lasting conflict has affected physical infrastructure and institutional capacity. Syrian Arab Republic [9] points out the damage to infrastructure in a wide range of areas due to the conflict. Al-Modon [2] refers to the need to rebuild the digital infrastructure of Syria for economic and social recovery. These studies suggest that cybersecurity should be incorporated into broader reconstruction policies, not treated as a standalone technological issue. The international cybersecurity capacity-building literature also stresses the importance of combining legal, technical, organisational and human capabilities. For example, the International Telecommunication Union [12] acknowledges legal measures, technical capacity, organisational development, skills and cooperation as key components of national cybersecurity readiness. This framework shows that legislation alone cannot develop an effective governance system of cybersecurity. Countries require capable institutions, trained personnel, technical infrastructure, incident-response capabilities, and cooperation between government and private-sector stakeholders. These dimensions are particularly important for Syria, where institutional reconstruction needs to be combined with technological modernisation. Comparative experiences shed light on cybersecurity governance in fragile and post-conflict contexts. Estonia shows how cybersecurity can be merged with digital transformation, secure public services and institutional development. Abdulghany [7] underscores the need for institutional coordination and public trust in Estonia's digital transformation. The Estonian experience demonstrates that cybersecurity can be the foundation for broader digital governance, even when the Syrian context is quite different in political and economic terms. Experiences from Iraq, Libya and Palestine also provide similar examples of the limitations that fragmented institutions, infrastructure weaknesses, political instability and dependence on external support can place on the development of cybersecurity.

Such cases suggest that post-conflict cybersecurity needs to focus on coordinated institutional reconstruction rather than isolated technical interventions. Thus, the authoritarian inheritance of Syria's former cybersecurity apparatus is of primary concern. During the Assad era, cybersecurity mechanisms were closely connected to surveillance, political control and regime security. Among the more visible examples of the regime's offensive cyber environment was the Syrian Electronic Army, which showed how cyber capabilities could be wielded against political opponents and perceived threats. Emergency Telecommunications Cluster [6] describes the tension between state security and individual rights, and Abdulghany [7] discusses how digital technologies can be leveraged by authoritarian governments to enhance political control. Therefore, the transitional government must endeavour to transform cybersecurity institutions from tools of regime protection into institutions of national security, public safety, and citizen protection. Cybersecurity legislation is another key element of governance. Effective legal structures usually cover cybercrime, e-transactions, protection of personal data, digital identity, information security and institutional responsibilities. Significant developments in the formal architecture of Syria's cybersecurity are Law No. 20 of 2022 on Cybercrime, Law No. 7 of 2023 establishing the National Authority for Information Technology Services, and Law No. 12 of 2024 on the Protection of Personal Data. But the suitability of these instruments for the transitional political environment should be scrutinised, as they were drafted under the previous authoritarian regime. Emergency Telecommunications Cluster [6] observes that broadly defined cybersecurity precautions can pose risks to freedom of expression and civil liberties. Legislative reform should therefore ensure that the provisions on cybercrime are precise, proportionate, transparent and consistent with digital rights. Another important governance issue is the concentration of institutions.

The International Telecommunication Union [12] identifies organisational capacity and cooperation as important elements of national cybersecurity. Centralisation of authority can make coordination easier, but too much concentration in one institution can create vulnerabilities in accountability and oversight. Syria needs clear roles and responsibilities for government ministries, regulatory bodies, telecom providers, critical infrastructure operators, private companies, academic institutions and civil society. A multi-stakeholder approach, coordinated across sectors, can improve information sharing, incident response,

transparency and national resilience. Finally, international cooperation, human capital and digital sovereignty are increasingly recognised as essential to cybersecurity development. The Carnegie Endowment for International Peace notes the need for post-conflict states to find a balance between international technological cooperation and the preservation of digital sovereignty [5]. While Syria may need foreign investment, technical expertise and cybersecurity partnerships, over-reliance on specific external technology providers could create strategic vulnerabilities. The International Telecommunication Union considers skills and capacity development to be central to sustainable cybersecurity [12]. Reducing reliance on external support over the long term can be achieved by building domestic expertise through education, professional training, research and engagement with Syrian technical professionals. Overall, the literature suggests that Syria's shift to cybersecurity cannot be accomplished with legislation and technology alone. Mnejja and Fatafta [1] emphasise the necessity of rebuilding Syria's digital future with rights protection. SANA [17] points out the significant challenges in rebuilding Syrian cyber power post-conflict. But few studies combine institutional reform, legislative review, technical resilience, human-capital development, international cooperation and digital rights in a post-conflict cybersecurity governance framework. This study takes up that gap by looking at these interconnected dimensions and proposing a governance approach that can enable a secure, resilient and rights-respecting digital environment in post-conflict Syria.

3. Methodology

The study employs a mixed-method research methodology that includes documentary analysis, institutional assessment, case study analysis, and comparative analysis to give a thorough assessment of cybersecurity governance in post-conflict Syria. In combination, these methodological approaches allow the study to investigate cybersecurity governance from legal, institutional, practical and comparative perspectives. The research does not depend on a single source of information but on legislative documents, institutional frameworks, practical situations and experiences from other post-conflict and developing nations. The objective of this method is to identify the institutional and legal gaps that exist and to examine the opportunities that exist to improve the cybersecurity governance of Syria during the transitional phase. A key part of the research is the examination of the documentary sources. It addresses key legal and policy tools shaping Syria's cybersecurity governance architecture. These include Law No. 20 of 2022 on Cybercrime, Law No. 7 of 2023 on the establishment of the National Authority for Information Technology Services (NAITS), Law No. 12 of 2024 on Electronic Personal Data Protection, Law No. 30 of 2024 amending the Telecommunications Law, and the Constitutional Declaration of March 2025. Where appropriate, national cybersecurity strategy documents, regulatory materials, policy statements and other relevant governmental documents are also evaluated, and the analysis focuses on detecting changes in Syria's cybersecurity legislation and outlining the distribution of responsibility between the various agencies.

Special attention is paid to legislative measures on cybercrime, information technology, telecommunications, personal data protection and cybersecurity administration. Moreover, the documentary analysis assesses the appropriateness of inherited legal structures for Syria's transitional era and whether existing laws offer enough means to manage developing cybersecurity concerns and to safeguard legal and digital rights. The second methodological component is an institutional analysis of organisations responsible for cybersecurity and related digital governance. This report analyses the mandates, organisational arrangements, duties, coordination arrangements and institutional capacities of major cybersecurity organisations. Specific focus is laid on the National Authority for Information Technology Services (NAITS), National Computer Incident Response Team (CIRT), Ministry of Communications and Technology and the Personal Data Protection Authority. The study takes stock of the situation of these institutions in the wider framework of cybersecurity governance and the interaction between their responsibilities. It also considers the possible overlaps, institutional gaps, coordination issues and capacity constraints that may influence the effectiveness of cybersecurity governance. The study will examine institutional responsibilities and legal structures to evaluate whether Syrian cybersecurity institutions have clear mandates and sufficient capacity to respond to cyber incidents, defend digital infrastructure, process personal data and enforce cybersecurity policies during the transition period.

A case study technique is also applied to discuss how cybersecurity legislation is implemented in practice. The article uses the instance of content creator Hassan Akkad, arrested in June 2026 under the Cybercrime Law, as a lens to highlight the broader challenges of the application of inherited cybersecurity legislation. The case provides a practical perspective to understand how the law requirements concerning cybercrime could be used in Syria's shifting legal and political climate. The study attempts to look beyond the case as an isolated incident and examine broader issues concerning the interpretation and application of cybersecurity legislation, the responsibilities of relevant institutions, legal accountability and the relationship between cybersecurity regulation and individual rights. The case study thus complements the documentary and institutional analysis by demonstrating how legal and institutional arrangements may function in practice during a moment of political and institutional transition. In addition, the paper adopts comparative analysis to derive useful lessons from the experiences of cybersecurity governance in other post-conflict and developing nations. In particular, Somalia, Colombia and Ukraine are chosen as comparative instances, as their experiences provide useful perspectives on cybersecurity governance in the midst of conflict, political instability, institutional reconstruction or wider country upheaval. Comparative analysis points to topics including

institutional reconstruction, legislative reform, capacity building for cybersecurity, digital infrastructure protection, inter-agency collaboration, and the establishment of accountable governance mechanisms.

The experiences of these countries are not referred to as models for Syria, but instead are investigated for approaches, problems and lessons that could be relevant to the specific transitional circumstances in Syria. The comparison allows the study to go beyond an evaluation of existing Syrian systems and to discuss new ways to improve cybersecurity governance. Together, these four methodological components enable a holistic assessment of post-conflict cybersecurity governance in Syria. Documentary analysis provides the legislative and regulatory framework. Institutional assessment provides the evaluation of the organisations responsible for implementing and administering the framework. The case study gives practical insights into the application of cybersecurity legislation, and the comparative analysis provides an external perspective on institutional rebuilding and governance change. The results of these methodologies are synthesised to identify places where legal rules may be confusing, outdated, overlapping or improperly fitted to the transitional setting. Likewise, institutional inadequacies, restricted capacities, coordination problems and accountability issues can be studied within the framework of the broader cybersecurity governance environment. The methodology framework overall seeks to examine the current issues and possible prospects related to cybersecurity governance in post-conflict Syria. The study aims to establish a holistic picture of the changing cybersecurity governance system in Syria by integrating legal analysis, institutional review, practical case examination, and international comparison. Ultimately, the approach allows for an assessment of how legislative reform, institutional strengthening, capacity building, and accountable governance mechanisms can contribute to the development of a secure, resilient, effective, and legal- and digital-rights-respecting cybersecurity framework during Syria's transition.

4. Results and Discussions

4.1. The Institutional Architecture of Cybersecurity Governance in Syria

The cornerstone of Syria's cybersecurity institutional architecture is the National Authority for Information Technology Services (NAITS), established by Law No. 7 of 2023. NAITS replaced the earlier National Agency for Network Service (NANS), which had been the officially recognized agency responsible for implementing "a national cybersecurity strategy, policy and roadmap". The establishment of NAITS represented a significant expansion of institutional capacity for cybersecurity governance. The law mandated NAITS to "keep pace with progress and development in the field of Internet and hosting services, support the national software industry, regulate digital signature services and the multi-purpose electronic card, and achieve information security in light of the widespread use of smart applications". Law No. 7 of 2023 granted NAITS significant authority, including the "exclusive right to provide information security services to public entities and to supervise the fulfillment of information security requirements in the private sector". This concentration of authority in a single state entity reflects a centralized approach to cybersecurity governance that may limit the development of a diverse and competitive cybersecurity ecosystem. In 2025, following the regime change, the Syrian government further consolidated NAITS's authority. A directive from the General Secretariat of the Presidency established NAITS as the "sole entity responsible for information security at a national level, granting it the power to regulate the private sector through accreditation." In February 2026, NAITS revoked the information security accreditations of several firms, including XTECH LLC, Smart Systems Solutions, and Talal Abu-Ghazaleh and Co., for "failure to comply with the regulations governing information security service providers."

4.2. The National Computer Incident Response Team (CIRT)

Syria has an officially recognized National CIRT, which was part of the National Agency for Network Service (NANS) and has continued under NAITS (Figure 1).

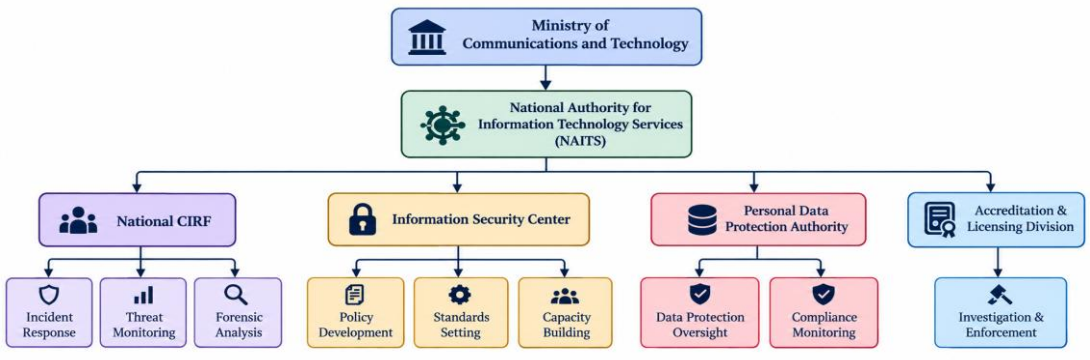


Figure 1: Institutional structure of cybersecurity governance in Syria

The CIRT is responsible for responding to cybersecurity incidents and coordinating national cybersecurity defense. However, the operational capacity of Syria's CIRT remains limited. As documented by the ITU, there is "no available information concerning any officially recognized national (and sector-specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards". The absence of established frameworks for certification, accreditation, and benchmarking indicates significant gaps in the CIRT's operational capabilities.

4.3. The Personal Data Protection Authority

Law No. 12 of 2024 established a dedicated Personal Data Protection Authority as an independent administrative body. The law mandates the authority to oversee the protection of electronic personal data, including the regulation of data collection, processing, use, and transfer. The establishment of a dedicated data protection authority represents an important institutional development. However, questions remain about the authority's operational independence, resourcing, and enforcement capacity. The law provides for "financial penalties that may reach 12 million Syrian pounds and imprisonment of up to three years", but the effectiveness of these enforcement mechanisms depends on the authority's institutional capacity.

4.4. Institutional Gaps and Challenges

Despite these institutional developments, significant gaps remain in Syria's cybersecurity governance architecture:

- **Fragmented Institutional Mandates:** The concentration of cybersecurity authority in NAITS, while providing clarity, may also create bottlenecks and limit the development of specialized capabilities.
- **Limited Operational Capacity:** Syria's cybersecurity institutions lack the technical capacity, skilled personnel, and resources necessary for effective cybersecurity governance. As noted in the post-conflict analysis, "national cybersecurity capabilities remain insufficient to protect even the most basic systems."
- **Absence of Independent Oversight:** The concentration of cybersecurity authority in executive branch institutions raises concerns about the absence of independent oversight mechanisms.
- **Human Capital Deficit:** The conflict has resulted in a significant brain drain of skilled cybersecurity professionals. As one analysis noted, "The potential return of syrian exiles with technical skills would enable the government to address vulnerabilities in the country's critical digital infrastructure" (Figure 2).

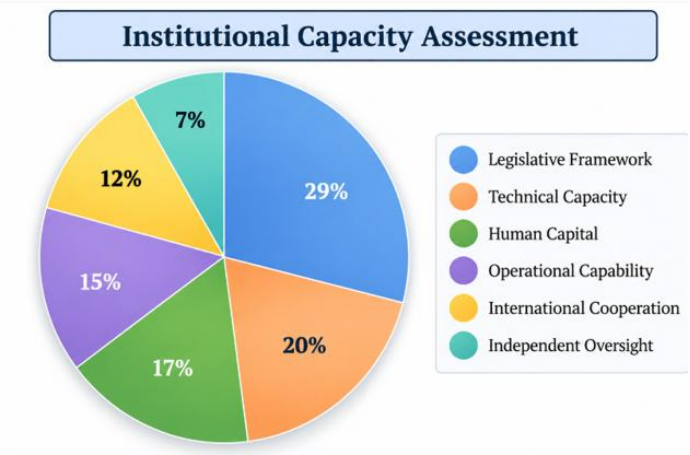


Figure 2: Institutional capacity assessment matrix

4.5. The Legislative Framework for Cybersecurity in Syria

4.5.1. The Cybercrime Law (Law No. 20 of 2022)

Law No. 20 of 2022 represents Syria's primary legislative instrument for addressing cybercrime. The law "reorganizes the penal rules for cybercrime" previously contained in Legislative Decree No. 17 of 2012. Its stated objectives include "combating cybercrime in line with technological developments and the high rate of its spread in society, protecting legal interests, regulating freedoms in the virtual world, and limiting the misuse of technical means". The law covers a wide range of cyber offenses, including "information fraud, privacy violations, electronic defamation, insult and contempt, crimes against modesty or decency, crimes against the constitution and attacks on the dignity or financial position of the state, as well as the unauthorized publication of audio or visual recordings, and crimes related to electronic cards and information theft". Penalties

under the law range from "one month to 15 years of imprisonment, with fines ranging from 200,000 to 15 million Syrian pounds". The law provides for enhanced penalties "if the crime is committed against a public entity".

4.5.2. The Personal Data Protection Law (Law No. 12 of 2024)

Law No. 12 of 2024 on Electronic Personal Data Protection was issued "with the aim of preserving the privacy of citizens' data and regulating the process of collecting, processing, using, and transferring personal information on the network in a manner that ensures its confidentiality and deters perpetrators of illegal acts". The law provides definitions of key concepts, including "personal data" (information relating to a specific natural person, directly or indirectly identifiable) and "sensitive personal data" (data revealing psychological, mental, physical, or genetic health, biometric data, financial data, religious beliefs, political opinions, criminal status, or data of children and those lacking legal capacity). The law establishes a Personal Data Protection Authority and provides for "financial penalties that may reach 12 million Syrian pounds and imprisonment of up to three years". Executive instructions for the law were issued in July 2024.

4.5.3. The National Authority for Information Technology Services Law (Law No. 7 of 2023)

Law No. 7 of 2023 established NAITS and provided its institutional mandate. The law grants NAITS the "exclusive right to provide information security services to public entities and to supervise the fulfillment of information security requirements in the private sector". The law also "imposed new penalties and tightened previous penalties" to ensure compliance with NAITS regulations. This concentration of regulatory, enforcement, and service provision authority in a single entity raises questions about the separation of functions and potential conflicts of interest.

4.5.4. Telecommunications Law Amendments (Law No. 30 of 2024)

Law No. 30 of 2024 amended the Telecommunications Law (No. 18 of 2010) to "increase fines and penalties for all acts that lead to damage to the telecommunications network, sabotage of its structure, misuse it for illegal purposes, or provide communications services whose content violates public order or public morals". There are a number of major problems with the legislative framework for cyber security in Syria in the transitional period. One important worry is the legacy of cyber security legislation adopted under the Assad administration that has been marked by an authoritarian approach to digital governance. One study notes that cybersecurity under former President Bashar al-Assad was largely concentrated on safeguarding regime-related assets, leaving the country’s wider digital infrastructure exposed. This legacy is challenging for the transitional government because the existing laws and institutions were created in a different political and legal context. Another key problem is the imprecise and overbroad provisions of the Cybercrime Law. Such regulations may provide extensive discretion in criminalisation and enforcement and may generate a chilling effect in the public domain, particularly for journalists, content creators, researchers and ordinary citizens. The very presence of broadly drafted criminal laws in existence may drive individuals to reduce their online expression out of fear of how the law will be construed or implemented. Another key difficulty is the link between the Cybercrime Law and constitutional and international human rights norms. Any restrictions on freedom of expression under article 19(3) of the International Covenant on Civil and Political Rights must in principle be specified with clarity, pursue a legitimate aim, and be necessary and reasonable. This has prompted concerns as to whether certain of the elements of Syria’s cybersecurity legislation meet these requirements and respect the notion of criminal legality.

The March 2025 Constitutional Declaration also generates a legal issue about the continued applicability of existing legislation. Article 48 provides for the abrogation of exceptional laws which are irreconcilable with human rights. Article 51 provides that previous legislation should remain in force unless and until altered or repealed. This raises an important transitional legal dilemma as to how to treat inherited laws while fresh constitutional and legal standards are being developed. Moreover, although a national cybersecurity plan was adopted in June 2023, this has not yet been implemented, and the development and revision of a subsequent National Cybersecurity plan has been reported to be under way in 2026. The cyber security threat environment in post-conflict Syria is just as complex. But the end of the Assad regime does not mean that cyber assaults by actors linked with the former government or other hostile parties would end. The civil war's legacy continues to impact Syria's cybersecurity environment, especially as parties linked to the former regime have previously shown cyber skills.

The Syrian Electronic Army, a hacker group aligned with the Assad government since 2011, engaged in cyber activities throughout the civil conflict and targeted groups like X (previously Twitter) and The New York Times. As such, the threat of attacks against transitional government institutions remains a significant cybersecurity risk, especially when rebuilding of government infrastructure is underway. The Syrian Ministry of Information said in June 2025 that a coordinated cyberattack targeted government websites and social media accounts. The ministry blamed the behaviour on remnants of the former Assad administration. Syria is also a target for state-sponsored cyber espionage activities. Researchers at Bitdefender reported in

September 2025 that they uncovered a cyber-espionage campaign targeting victims in Turkey and Syria and linked it to StrongPity, also known as Promethium, an organization followed by researchers since 2012.

This activity reveals that Syria's cybersecurity issues are related not only to domestic political actors, but also to sophisticated overseas threats. The post-conflict atmosphere has also bred conditions for deception and information warfare. Digital platforms have been utilised by various players to disseminate narratives that shape public opinion and political developments. Coordinated or deceptive online content can exacerbate sectarian tensions. These concerns are particularly acute in situations of political transition, when the rapid spread of false or manipulative information can impair public trust, institutional legitimacy and social cohesiveness. Serious cybersecurity risks are also present in Syria's civil society organisations. They may be hampered in implementing effective digital-security measures by financial limits, low technological knowledge, political instability and logistical obstacles. A consequence of digital security not always being seen as a core organisational practice has been gaps in data protection, secure communication, access control and incident response. These vulnerabilities might result in exposure of critical organisational information, personal data and communications to cyber assaults. The strengthening of cybersecurity in civil society organisations is therefore not just about technical protection, but also about institutional resilience and the safety of persons who rely on these organisations. Geopolitical forces further hamper Syria's cybersecurity administration. International disputes over technology vendors and telecommunications infrastructure can impact decisions about equipment, networks, data management, and digital infrastructure. The US has reportedly warned Syria against using Chinese technology in the telecommunications sector, citing national security concerns. The Syrian Ministry of Communications has said decisions on equipment and infrastructure are made according to national technical and security standards, with data protection and service continuity taken into account. These conflicting factors highlight the challenge of establishing a cybersecurity system that can satisfy national security, technology, infrastructural, economic, and international linkages.

Therefore, the whole post-conflict cybersecurity governance architecture for Syria may be explained through multiple interconnected sectors. The institutional component needs clear mandates, effective coordination procedures, independent monitoring, accountability, and adequate resources and operational capacity. The legal aspect demands a single piece of legislation on cybersecurity, specific definitions of cybercrimes, well-defined sanctions, and adherence to constitutional and international human rights standards. The technical component is an operational national computer incident response team, sufficient cybersecurity standards, certification processes, digital-forensic skills, and effective incident-response procedures. Human-capital development is also important, because cybersecurity institutions need people qualified to deal with complex technical, legal and operational difficulties. Mechanisms for attracting and maintaining competent people, education, professional certification and specialised training are therefore crucial elements of national cybersecurity capabilities. International cooperation in the form of involvement in international cybersecurity efforts, technical support, capacity building, information sharing and coordination with regional and international partners adds another dimension. The transitional era also poses a fundamental problem for the link between legal continuity and legal reform. The continuous application of cybersecurity legislation adopted under the previous political regime gives rise to problems concerning the compatibility of current laws with the demands of the new constitutional framework and contemporary human rights norms. One illustration of these wider issues is the arrest in June 2026 of content creator Hassan Akkad under the Cybercrime Law on accusations that reportedly included electronic defamation, insult and slander. The importance of such a case is not limited to the particular facts, as it raises problems regarding the continuous application of inherited criminal legislation in a period of legal transition. The problems are the principle of criminal legality, the conditions for the restriction of freedom of expression, the risk of a chilling effect from broad criminal laws, and the relation between articles 48 and 51 of the Constitutional Declaration.

Such problems point to the need to evaluate inherited legislation before applying it in a radically transformed constitutional and political context. Digital sovereignty has become an integral part of Syria's cybersecurity government. The concept is that digital essential infrastructure and state data are under national control. "Government data should be hosted inside Syria and government sector systems should not be hosted outside Syria," said Jihad Alala, director of the Information Security Center. Local hosting can help to preserve national control over sensitive information and decrease some external dependencies. Still, it requires stable domestic infrastructure, appropriate technological competence, high security standards, and good backup and recovery mechanisms. Too much technological isolation could also hamper international cooperation, access to specialised cybersecurity services, and involvement in global digital-security networks. So, digital sovereignty is a balance between national control and the actual realities of international cooperation regarding cybersecurity and technical growth. The comparative experiences of Somalia, Colombia and Ukraine present further possibilities for Syria. Somalia's usage of the Cybersecurity Capacity Maturity Model for Nations (CMM) illustrates how a systematic assessment framework may identify cybersecurity gaps and establish capacity-building plans. Colombia's post-conflict experience underlines the need to mainstream cybersecurity with other national development and institution-building efforts, and to leverage international collaboration to enhance technological skills. Ukraine's wartime experience highlights the need for resilient digital infrastructure, continuous provision of critical digital services, and international alliances to ensure connectivity and cybersecurity in the face of high security challenges. Although these experiences are not directly transferable to the Syrian

context, given different political, institutional, economic and technological conditions, they offer comparative lessons on institutional development, legal reform, infrastructure resilience, professional capacity and international cooperation.

The study suggests that Syria has a centralised architecture for cybersecurity governance, including institutions such as NAITS, but its operational competence is still limited. Centralisation could ease administrative coordination, but too much concentration of responsibility can also create institutional dependencies and vulnerabilities if there is no appropriate monitoring and capability. Syria has also adopted numerous important cybersecurity laws, such as the Cybercrime Law (2022), the NAITS Law (2023) and the Personal Data Protection Law (2024). However, worries about imprecise or broad legislative rules remain, particularly when cybersecurity regulation interacts with freedom of expression and other fundamental rights. The ongoing application of inherited cybersecurity regulations in the transitional phase thus offers a major legal difficulty. Meanwhile, Syria continues to be exposed to cyber assaults from groups linked to the old regime, state-sponsored actors, espionage operations and disinformation networks. Limited technological and forensic capabilities may impede identification of attackers and effective response. The conflict has also produced a lack of experienced cybersecurity workers, while the inadequate execution of national cybersecurity strategy has limited long-term planning at the institutional level. There is also geopolitical competition around technology and telecommunications infrastructure. Overcoming these difficulties requires coordinated institutional, legislative, technical, educational and international action. The existing laws can be evaluated in a comprehensive analysis of cybersecurity legislation in comparison to the Constitutional Declaration and international human rights norms. Provisions that are ambiguous or contradictory to these criteria might be examined, and cyber offences and penalties can be clarified with greater detail. Adequate resources should be provided to NAITS, CIRT, the Personal Data Protection Authority and other relevant organisations to build institutional capacity. At the same time, procedures for inter-agency collaboration and independent oversight can be clearly established.

Institutions with specialised capabilities in cyber-threat intelligence, digital forensics and incident response can also improve their ability to detect and respond to cyber problems. A national cybersecurity plan must also include clear objectives, defined tasks, measurable timetables and monitoring methods to be implemented. Cybersecurity has to be included in broader digital-transformation and national-development plans and not just viewed as a technical problem. There is a need to focus on human-capital development through university programs, professional training, certification pathways, research possibilities and measures to encourage talented Syrian professionals to contribute domestically. International collaboration can assist these efforts through technical assistance, training, knowledge sharing, information exchange and institutional alliances. Further chances for capacity building and aligning with internationally accepted cybersecurity procedures can be provided through interaction with bodies such as the International Telecommunication Union [12]. Lastly, it has to incorporate civil society and the private sector, as well as government organisations. Civil society organisations and enterprises can be involved in consultations on cybersecurity laws, contribute to the development of technical standards, and raise awareness of digital-security issues. Organisations should strengthen internal cybersecurity rules, personnel training, data-protection practices, and incident-response protocols. Civil society can also help monitor implementation of cybersecurity precautions and promote transparency and accountability. International partners can support inclusive governance by supporting multi-stakeholder involvement and offering technical and legal knowledge. Syria can tackle the complex cybersecurity challenges in its post-conflict and transitional environment through integrated development of the appropriate legislation, competent institutions, resilient infrastructure, skilled professionals, international cooperation and mechanisms for safeguarding digital rights.

5. Conclusion

Syria's cybersecurity governance stands at a critical crossroads. The fall of the Assad regime has created an unprecedented opportunity to reshape the country's approach to protecting the national digital space, moving from a regime-centric model focused on surveillance and control to a nationally oriented framework that balances security with the protection of fundamental rights. The institutional and legislative foundations for this transition have been laid. The establishment of NAITS, the enactment of comprehensive cybersecurity legislation, and the development of a national cybersecurity strategy represent important steps forward. However, significant challenges remain. The legacy of authoritarian legislation, the limited operational capacity of cybersecurity institutions, the human capital deficit, and the persistent cyber threats from regime loyalists and other actors all present obstacles to effective cybersecurity governance. The path forward requires a comprehensive approach that addresses institutional, legislative, technical, and human capacity dimensions simultaneously. Legislative reform is essential to align Syria's cybersecurity laws with constitutional and international human rights standards. Institutional capacity building is necessary to enable effective cybersecurity governance.

Human capital development is critical to address the skills shortage. And international cooperation is vital to access the technical assistance and capacity building needed for sustainable development. The decisions made in the coming months and years will determine whether Syria's digital future is characterized by security and rights-respecting governance or by continued vulnerability and authoritarian control. The framework proposed in this paper provides a roadmap for navigating this transition, emphasizing the need for comprehensive, integrated, and rights-respecting approaches to cybersecurity governance. As Syria

rebuilds from the devastation of fourteen years of conflict, cybersecurity governance must be recognized not as a secondary concern but as a fundamental prerequisite for sustainable recovery, economic development, and the protection of citizens' rights in the digital age. The rebuilding of Syria's digital infrastructure must be accompanied by the rebuilding of Syria's digital governance—creating a secure, resilient, and rights-respecting digital ecosystem that can support the country's recovery and development for decades to come.

Acknowledgment: The authors gratefully acknowledge Singapore Management University, Al-Shahbaa Private University, Swinburne University of Technology, Texas A&M University, The University of Tokyo, and McMaster University for their academic support and institutional contributions.

Data Availability Statement: The data supporting this study are available from the corresponding author upon reasonable request.

Funding Statement: This research was conducted by multiple authors without any external financial support or funding.

Conflicts of Interest Statement: The authors declare no conflicts of interest, and all sources have been appropriately acknowledged and referenced.

Ethics and Consent Statement: The study followed applicable ethical guidelines, with informed consent obtained from participants and confidentiality maintained throughout the research.

References

1. K. Mnejja and M. Fatafta, "Reclaiming Syria's digital future," *Access Now*, 2025. [Accessed by 02/02/2026].
2. Al-Modon, "Internet shutdowns in large areas of northern Syria," *Al-Modon*, 2024. [Accessed by 06/07/2025].
3. D. Belson, "Exam-ining recent Internet shutdowns in Syria, Iraq, and Algeria," *Cloudflare Blog*, 2024. [Accessed by 08/07/2025].
4. G. Noone, "STC Group wins bid to run Syria's 'Silklink' telecoms infrastructure," *Data Center Dynamics*, 2026. [Accessed by 12/07/2026].
5. Digital Watch Observatory, "Syria," *Digital Watch Observatory*, 2026. [Accessed by 12/07/2026].
6. Emergency Telecommunications Cluster (ETS), "Syria Situation Report (July–August 2025)," *ReliefWeb*, 2025. [Accessed by 10/02/2026].
7. F. Abdulghany, "Suspending the Cybercrime Law: A constitutional test for the transitional phase in Syria," *Fadel Abdulghany*, 2026. [Accessed by 11/02/2026].
8. C. Teter, "Civil society's data in north and east Syria is not secure," *Global Voices*, 2025. [Accessed by 12/01/2026].
9. Syrian Arab Republic, "Draft new Resolution—Assistance and support to Syria for rebuilding its telecommunication networks," *International Telecommunication Union (ITU)*, 2017. [Accessed by 14/07/2025].
10. Syrian Arab Republic, "A paper on digital development in Syria and the current reality," *International Telecommunication Union (ITU),* 2024. [Accessed by 16/07/2025].
11. Syrian Arab Republic, "Cybersecurity strategy in Syria," *International Telecommunication Union (ITU)*, 2024. [Accessed by 18/07/2025].
12. International Telecommunication Union (ITU), "Cyberwellness profile: Syria," *International Telecommunication Union (ITU)*, 2014. [Accessed by 20/07/2025].
13. MENA Startup Digest, "Syria revokes cybersecurity accreditations in push for digital sovereignty," *MENA Startup Digest*, 2026. [Accessed by 20/07/2026].
14. H. El-Hitami, "Internet in Syrien: Eine fragile Verbindung," *netzpolitik.org*, 2026. [Accessed by 22/07/2026].
15. ReliefWeb, "ETS Syria Situation Report #75 (Final): January 2013 – December 2025," *ReliefWeb*, 2025. [Accessed by 16/02/2026].
16. M. Ourahli, "Post-Conflict Challenges for Syria's Reconstruction of Cyber Power," *S. Rajaratnam School of International Studies (RSIS)*, 2025. [Accessed by 24/02/2026].
17. SANA, "Presidential law on increasing fines and penalties for sabotage acts of telecommunications network," *Syrian Arab News Agency (SANA),* 2024. [Accessed by 26/07/2025].
18. SANA, "President al-Assad issues Law No. 12 on protecting E-personal data," *Syrian Arab News Agency (SANA),* 2024. [Accessed by 28/07/2025].

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 perspective.*