**FMDB** *Transactions on Sustainable Computer Letters*

# Rebuilding National Cybersecurity: The Challenge of Transitioning from Systems Protection to State-Level Defense

**Mihiro Otaki[1], Jouma Ali Al-Mohamad[2,*], Cheang Chi Seng[3], Mark Benjamin Kuhne[4], Lejla Skelic[5], Chang Shi Ying[6]**

[1]Department of Information and Communication Engineering, University of Tokyo, Bunkyo, Tokyo, Japan.
[2]Department of Computer and Mobile Communication Engineering, Faculty of Information Engineering, Al-Shahbaa Private University, Aleppo, Aleppo Governorate, Syria.
[3,6]Department of Computing and Information Systems, Singapore Management University, 81 Victoria Street, Singapore.
[4,5]Department of Computer Science, Secure and Trustworthy Systems Group, ETH Zurich, Zürich, Switzerland.
mihiro@logos.t.u-tokyo.ac.jp[1], jalmohamad@su.edu.sy[2], cs.cheang.2025@phdcs.smu.edu.sg[3], mark.kuhne@inf.ethz.ch[4], lejla.skelic@inf.ethz.ch[5], sy.chang.2025@phdcs.smu.edu.sg[6]

**Abstract:** This paper examines the profound challenges Syria faces in transitioning from a regime-centric cybersecurity paradigm to a comprehensive national defense framework following the fall of the Assad regime in December 2024. After nearly fourteen years of civil war that systematically degraded the country's digital infrastructure and institutional capacity, Syria stands at a critical inflection point where cybersecurity has emerged as a fundamental prerequisite for state legitimacy, economic recovery, and national sovereignty. This study examines five main challenges: regime-centric cybersecurity, fragmented hacker networks and persistent threats, degraded digital infrastructure and institutional capacity, sanctions-induced technological isolation, and the geopolitical dimension of digital sovereignty, using securitisation theory, critical infrastructure protection frameworks, and empirical evidence from Syria's post-conflict digital landscape. Cybersecurity was narrowly used for political repression and regime survival under the Assad dictatorship, leaving national infrastructure vulnerable. In the transitional government's digital ecosystem, national cybersecurity capabilities are insufficient to safeguard even basic systems, hacker organisations loyal to the past regime pose risks, and the military and security apparatus is fractured. The report also examines strategic relationships with regional cybersecurity providers, the establishment of a National Cybersecurity Strategy, revoking accreditations to enforce digital sovereignty, and the return of Syrian exile technical talent. This paper concludes with concrete advice for politicians, international partners, and cybersecurity practitioners working to build a robust national cybersecurity framework in one of the 21st century's most difficult post-conflict circumstances.

**Keywords:** National Cybersecurity; Digital Sovereignty; Critical Infrastructure Protection; Digital Infrastructure; Institutional Capacity; Political Repression; Transitional Government.

**Received on:** 14/09/2025, **Revised on:** 13/12/2025, **Accepted on:** 16/01/2026, **Published on:** 11/11/2026

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

**DOI:** https://doi.org/10.69888/FTSCL.2026.000843

**Cite as:** M. Otaki, J. A. Al-Mohamad, C. C. Seng, M. B. Kuhne, L. Skelic, and C. S. Ying, "Rebuilding National Cybersecurity: The Challenge of Transitioning from Systems Protection to State-Level Defense," *FMDB Transactions on Sustainable Computer Letters*, vol. 4, no. 4, pp. 227–243, 2026.

**Copyright** © 2026 M. Otaki *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

Academic research has increasingly examined the nexus between cybersecurity and state-building in post-conflict settings, as digital technologies have shifted from auxiliary governance tools to essential elements of state capacity [1]. Security studies have traditionally examined the main pillars of state power: territorial control, military strength, economic resources, political institutions, and diplomatic influence. But the rapid digitalisation of government administration, telecommunications, financial services, energy systems, health care, transportation, education and public communication has fundamentally changed this understanding. Modern states increasingly rely on secure digital networks to project authority and deliver essential services. Deibert and Rohozinski [4] argue that cyberspace has become a significant arena for state consolidation. Control over digital infrastructure gives governments substantial advantages in surveillance, information management, economic coordination and political influence. This relationship is especially relevant in post-conflict settings, where broken digital infrastructure and fragile cybersecurity institutions can impair governments' capacity to provide basic services and build political legitimacy. Cybersecurity should therefore be understood not merely as a technical issue but as an essential component of contemporary state-building, sovereignty, institutional resilience, and national security. The Syrian case provides a particularly important context for studying this relationship [5]. The collapse of the Assad regime in December 2024 ushered in a period of political change in Syria after nearly fourteen years of civil war. The conflict had broken state institutions, destroyed physical and digital infrastructure, displaced skilled professionals, eroded administrative capacity and created multiple competing security structures. These developments created a digital environment marked by technological vulnerabilities, institutional fragmentation, limited cybersecurity expertise, and exposure to domestic and foreign cyber actors. The transition therefore involves a complex process of reconstructing cybersecurity capabilities while redefining their political purpose.

The transitional state should not have to recreate a system that was built primarily to serve the previous regime, but rather create its own national cybersecurity system that is designed to protect the citizenry, government institutions, critical infrastructure, economic systems, and national sovereignty. Such transformation needs technological modernisation and institutional reform. Buzan et al. [2] securitisation theory offers a useful framework for understanding how cybersecurity is constructed as a national security priority. According to the Copenhagen School, securitisation is the process by which political actors present issues as existential threats that require urgent, exceptional measures. Thus, cybersecurity can be seen as a process that converts cyberattacks, espionage, infrastructure vulnerabilities, information manipulation, and technological dependence into national security issues. In fragile post-conflict states, this process can create a dual logic. One is that governments need to securitise cyberspace to protect their national networks from foreign intelligence agencies, cybercriminals, extremist organisations, hacktivists, and politically motivated groups. In contrast, over-securitization can be dangerous when cybersecurity institutions are granted wide powers without sufficient legal oversight. This can be a particular problem in countries transitioning from authoritarian rule, where citizens may link cybersecurity institutions to political oppression. Syria thus faces the difficult task of strengthening cybersecurity without replicating the practices that helped to delegitimise the previous regime. The notion of cyber resilience provides another theoretical basis for understanding this challenge. Traditional approaches to cybersecurity have generally focused on preventing attacks by identifying vulnerabilities and implementing protective controls. However, total prevention is increasingly unrealistic, as modern networks are constantly exposed to sophisticated, fast-evolving threats. Linkov et al. [8] highlight resilience as the capacity of systems to absorb shocks, respond, adapt to evolving circumstances and recover afterward.

This perspective is particularly relevant to Syria, where national reconstruction is underway amid diminished resources and ongoing uncertainty. Thus, a resilient cybersecurity system should be able to perform essential operations even when some networks are compromised. It must include backup systems, redundant communications, incident-response mechanisms, secure data storage, threat monitoring, digital forensics, recovery procedures, and trained personnel. In this way, cyber resilience offers a broader framework for Syria to develop cybersecurity capabilities that can support long-term national stability rather than simply responding to isolated incidents. Another reason cybersecurity must be part of post-conflict reconstruction is the need to protect critical infrastructure. Effective cybersecurity governance requires institutional capacity, technical infrastructure, skilled professionals and coordinated national cybersecurity strategies [9]. Post-conflict states face unique challenges, as physical infrastructure can be destroyed and existing digital infrastructure can be old, poorly maintained or not well protected. Telecom networks, electrical grids, banking systems, hospitals, transport networks, government records and educational institutions increasingly depend on interconnected digital infrastructure. Damage to any of these systems can have effects beyond cyberspace. For example, breaches of government databases may disrupt public administration, and telecommunications attacks may disrupt emergency services and humanitarian operations. Cybersecurity must be integrated into infrastructure reconstruction from the start, not addressed as a secondary concern once physical reconstruction is complete. Lessons from other post-conflict and transitional settings can offer helpful insights into the Syrian situation. Estonia's transition after the fall of the Soviet Union is often cited as a model of successful digital state-building [10]. The country invested heavily in digital infrastructure, electronic government services, secure identification systems, electronic signatures and cybersecurity institutions.

Estonia's experience, as noted by the e-Governance Academy Foundation [5], demonstrates the benefits of integrating digital security early in national reconstruction. Cybersecurity in Estonia was not an add-on; it was embedded in the broader development of government institutions and secure digital systems. This approach helped to create a highly digitalised state with strong cybersecurity capabilities. But the Estonian experience cannot be directly transplanted to Syria, as its geopolitical, economic, and institutional contexts differ sharply. Estonia has had relative political stability, European integration, institutional support and access to international financial and technological resources. Syria's transition takes place in a far more fractured and volatile regional environment, and involves rebuilding institutions that have been severely impacted by protracted conflict. A more cautionary analogy may be the post-2003 Iraqi experience. The dismantling of critical components of the previous security system resulted in institutional and security vacuums, which were subsequently exploited by various internal and external actors. It demonstrates the danger of dismantling existing structures without building up effective replacement institutions at the same time. Syria faces a similar dilemma in the virtual space. Some inherited capabilities may be dismantled because they are associated with political surveillance, repression or criminal activities. But losing all technical personnel and institutional knowledge could also create significant capability gaps. Effective cybersecurity rehabilitation, therefore, requires a carefully managed process to separate politically problematic structures from potentially valuable technical expertise. Professional screening, retraining, certification and institutional reintegration can help preserve legitimate expertise and avoid perpetuating harmful practices. Libya is another relevant comparison, as its post-2011 transition illustrated the challenges of building coherent national institutions amid competing armed groups and fragmented political authority. Without central control, it is hard to agree on common security standards, coordinate threat-intelligence sharing and protect national infrastructure.

If different political, military and security actors continue to run their own networks and technical resources, Syria's digital environment could face similar problems. The Palestinian case offers an alternative view: dire limitations on infrastructure, mobility, the economy, and political uncertainty are driving the development of adaptive, innovative technology ecosystems. However, these limitations also restrict scalability and make it difficult to build comprehensive cybersecurity systems. Taken together, these cases make clear that no cookie-cutter model exists for post-conflict cyber reconstruction. Syria needs a context-specific approach that combines institutional consolidation, technological modernisation, resilience and strategic cooperation. Another challenge is the authoritarian legacy of Syrian cybersecurity. Authoritarian regimes are increasingly utilising digital technologies for surveillance, repression, information control and regime survival [3]. Under Bashar al-Assad, Syria's cybersecurity was closely linked to the broader security apparatus and often focused on securing political authority rather than national digital infrastructure. One prominent example of offensive cyber capabilities used against perceived foes was the Syrian Electronic Army (SEA). The SEA's activities showed how relatively specialised cyber capabilities could be integrated into political strategies involving information control, intimidation and disruption. At the same time, the larger national digital environment remained vulnerable because resources and institutional attention were focused on regime security rather than comprehensive national protection. This regime-centric approach has several lasting consequences. First, the legitimacy deficit can be quite pronounced regarding cybersecurity institutions associated with the previous political order. People may not trust institutions they see as tied to surveillance and repression. Second, neglecting national infrastructure creates systemic vulnerabilities that outlast changes in government.

Third, politically affiliated hacker groups can fracture cyberspace, with ex-regime loyalists, opposition-affiliated groups, independent operators, and foreign actors continuing to operate beyond centralised government control. Fourth, personnel trained in the old system may have valuable technical capabilities but require institutional reassessment to ensure their expertise is applied to legitimate national defence. These legacies make reforming cybersecurity more complicated than routine technological modernisation. Another key issue in Syria's post-conflict reconstruction is digital sovereignty. It refers to a state's ability to exert real control over its digital infrastructure, data, technology resources and cybersecurity decisions. Feldstein [3] discusses the challenge of balancing international reliance on technology with efforts to develop local capacity in post-conflict environments. The years of war and economic sanctions have restricted access to cutting-edge technologies, cybersecurity tools and specialised services and placed Syria in an uncomfortable position. International partnerships can provide critical assistance, but relying on outside vendors may create new vulnerabilities. Foreign technology providers might control critical infrastructure, software platforms, data storage or security systems, possibly diminishing national autonomy. A sustainable approach therefore requires technology transfer, workforce development, vendor diversification, local data protection and clear regulatory authority. Syria's cyber threat environment is similarly complex. The transitional government has to deal with threats from former regime-connected actors, foreign state-linked groups, cybercriminals, hacktivists, and politically motivated organisations. The SEA's historical activities underscore the potential effects of politically motivated cyber groups, especially when they possess unique technical expertise and knowledge of domestic systems. Attacks on government websites, public databases, telecommunications infrastructure, or other critical services could complicate reconstruction. Another major concern is foreign actors.

Cyber threat intelligence research has identified activity by Chinese-aligned and other state-affiliated groups targeting Syrian interests, and espionage campaigns involving Syria show the country remains relevant to foreign intelligence operations. The

reconstruction process itself may make Syrian networks more attractive, as foreign actors may seek political intelligence, economic information, or strategic access to infrastructure as part of national development. Disinformation and information warfare compound the risks. Information manipulation is especially likely in post-conflict societies where public institutions may lack credibility, political identities may be polarised, and citizens may lack access to reliable information. These conditions can be exploited by foreign and domestic actors through coordinated disinformation, fabricated narratives, manipulated media, and social-media campaigns designed to increase distrust and social division. These activities can erode confidence in the transitional government and make it more difficult to establish political legitimacy. But responses to disinformation must be carefully calibrated, because overly broad restrictions on online information can mirror authoritarian patterns. More sustainable ways to build societal resilience include strengthening independent information sources, public communication, media literacy, digital awareness and transparent government communication. Institutional development is therefore essential to transform cybersecurity objectives into operational capabilities. Syria needs to define institutional roles, coordinate national incident-response mechanisms, establish cybersecurity standards, implement critical infrastructure protection procedures, develop digital forensic capabilities, and ensure effective cooperation between government and private-sector organisations. A national cybersecurity strategy can provide an overall framework for establishing these functions and identifying national priorities.

Such a strategy should identify critical information infrastructure, set security requirements for public institutions, establish incident-reporting procedures, strengthen security operations capabilities, foster cybersecurity education, and define the relationship between civilian cybersecurity organisations and military or intelligence entities. Cybersecurity institutions must also operate under clear legal mandates and appropriate accountability mechanisms so national security needs do not erode public trust or individual rights [11]. Another important element in the transition is human capital development. Effective cybersecurity requires specialists in network security, digital forensics, threat intelligence, incident response, secure software development, cryptography, infrastructure protection and cyber policy. The long conflict and displacement have depleted Syria’s pool of local technical talent, and economic problems could make it difficult to retain skilled professionals. But Syrian professionals living abroad represent a potentially important source of expertise. Engaging the diaspora could provide access to international technical knowledge, professional networks, research partnerships, training programs and investment opportunities. Universities can also help by embedding cybersecurity in computer science, engineering, information technology and public policy courses. In the long run, developing a sustainable homegrown workforce would reduce the country’s reliance on foreign consultants and improve its ability to maintain and adapt its cyber infrastructure. Despite growing scholarly attention to post-conflict cybersecurity, the literature still has significant gaps. First, empirical research on Syria’s cybersecurity transformation after the December 2024 regime change remains limited. Much of the existing scholarship focuses on the digital technologies used by the Assad regime or on cybersecurity in conflict-affected states more broadly. Second, the link between cybersecurity and state-building in Syria remains undertheorized [12].

Cybersecurity is often seen as a technical problem, not as a factor that affects state legitimacy, institutional capacity, sovereignty, and economic recovery. Third, little research examines the link between offensive and defensive cyber capabilities in the context of a political transition. Syria must simultaneously tackle inherited offensive capabilities, protect national infrastructure, and develop legitimate defensive institutions. Fourth, greater attention should be paid to international partnerships, sanctions relief, technology transfer, vendor diversification and diaspora expertise. These gaps matter because choices made during the transitional period could shape Syria's digital security environment for years. Rebuilding cybersecurity without addressing the authoritarian legacy risks undermining public confidence. And dismantling inherited capabilities without safeguarding legitimate technical expertise risks creating dangerous security gaps [13]. Similarly, overdependence on external technologies without developing internal capacity could endanger digital sovereignty. Syria therefore needs an integrated approach that pursues institutional reform, infrastructure modernisation, human-capital development, regulatory reform, cyber resilience and international cooperation simultaneously. The transition provides the country with an opportunity to shift from a regime-centric model of cyber security to a national framework based on protection, accountability, resilience and sovereignty. This study addresses the gaps identified by analysing the main challenges and opportunities in Syria’s cybersecurity reconstruction and assessing how theoretical perspectives on securitisation, critical infrastructure protection, cyber resilience, digital sovereignty and state-building may apply to Syria's changing post-conflict environment [14]. Ultimately, the literature indicates that cybersecurity should be considered an essential aspect of Syria’s reconstruction, rather than a peripheral technological one. A strong national cybersecurity framework can increase state legitimacy, protect vital services, support economic recovery, reduce external dependence and help build a more stable and sovereign post-conflict state.

## 2. Literature Review

The relationship between cybersecurity and state-building in post-conflict settings has become an important area of academic inquiry, as digital technologies have become more deeply embedded in governance, critical infrastructure, economic activity and public communication [15]. Traditional security studies have tended to prioritise territorial control, military capabilities, economic resources and political institutions, relegating cyberspace to a secondary dimension of state power. But modern states' increasing dependence on digital networks has fundamentally altered this view. As Deibert and Rohozinski [4] argue,

cyberspace has become a key terrain of state-building, where control over digital infrastructure enhances the state's capacity for surveillance, economic coordination, information management and political influence. This relationship is particularly relevant in post-conflict settings, where re-establishing secure digital infrastructure can facilitate rebuilding of government institutions and the provision of key public services. The Syrian case illustrates this challenge: prolonged conflict has eroded both physical infrastructure and institutional capacity, making cybersecurity central to national reconstruction. Securitisation theory, as developed by Buzan et al. [2], offers a useful framework for understanding how cybersecurity is constructed as a national security priority. The theory explains how political actors can frame particular issues as existential threats that demand immediate security responses. Thus, in fragile post-conflict states, cybersecurity may be securitised through two intertwined objectives: the protection of national digital infrastructure from external threats and the avoidance of political legitimacy being compromised by excessive surveillance or repression by cybersecurity institutions. This tension is especially relevant to Syria, as the inherited cybersecurity institutions from the previous regime may be associated with authoritarian practices [16]. The transitional government therefore needs to strengthen cybersecurity by rethinking it as a means of protecting national institutions, critical infrastructure, citizens and sovereignty, rather than protecting a specific political leadership.

Another important theoretical basis is the critical infrastructure protection framework. The International Telecommunication Union notes that post-conflict states face particular challenges in securing digital infrastructure due to compromised networks, limited human capital, institutional fragmentation, and inadequate technical resources. Challenges are particularly acute when critical services such as telecommunications, electricity, health, banking, transport and government administration rely on interconnected digital systems. Linkov et al. [8] extend this view by introducing the concept of cyber resilience, emphasising cybersecurity not only as attack prevention but also as the capability to withstand, respond to, recover from and adapt to cyber incidents. In the Syrian context, this means national cybersecurity rebuilding should focus on redundancy, incident response, digital forensics, recovery mechanisms, ongoing surveillance, and institutional coordination, rather than only preventive security controls. Lessons from comparative experiences can guide Syria's post-conflict cybersecurity development. Estonia is often cited as a leading example of digital state-building, incorporating digital infrastructure, e-government, secure identification, electronic signatures and cybersecurity into its post-Soviet transition [17]. The e-Governance Academy Foundation [5] explains that early investments in digital governance laid the foundation for a resilient, highly connected state. However, Estonia's experience differs sharply from Syria's because the former benefited from relative political stability, EU integration, institutional support, and access to international financial and technological resources. Rather, Syria's transition is occurring amid a backdrop of regional instability, economic and technological constraints, and the continued threat of actors associated with the previous regime. More cautionary lessons are available from the experiences of Iraq and Libya. Iraq's 2003 transition showed the dangers of dismantling existing security institutions without building effective replacements, leaving institutional and security voids [18]. Libya's post-2011 experience also illustrates the challenges of building coherent national institutions in contexts characterised by political fragmentation and competing armed groups.

These experiences suggest that Syria must strike the right balance between institutional reform and maintaining legitimate technical expertise. Another important perspective is the Palestinian case, where technological innovation has developed within severe constraints on infrastructure, movement, the economy and politics. But the same constraints can also hinder the scalability and resilience of cybersecurity systems [19]. Thus, Syria needs a context-specific model that includes institutional consolidation, technological modernisation, resilience, and international cooperation. The authoritarian heritage of cybersecurity is a particularly important challenge. Feldstein [7] shows that authoritarian governments increasingly use digital technologies for surveillance, repression, political control, and regime survival. In Syria, cybersecurity was deeply integrated with regime security under Bashar al-Assad, and the Syrian Electronic Army (SEA) operated as an offensive cyber capability against perceived enemies. This regime-centred approach had several long-term consequences. Cybersecurity institutions were linked to political control, the broader national infrastructure remained vulnerable, and politically aligned hacker groups contributed to a fractured cyber environment [20]. Such legacies can undermine public trust and make institutional reform harder after a political transition. Syria must therefore distinguish between technical capabilities that could be redirected to legitimate national defence and structures that could reproduce political repression. Digital sovereignty further complicates this reconstruction process. The Carnegie Endowment for International Peace highlights the tensions between relying on external technology and building domestic capacity in post-conflict environments. Syria may require foreign technologies, cybersecurity services, training, infrastructure investment, and technical expertise, especially given the degradation of domestic capabilities after years of conflict. However, reliance on external providers can create technology dependence and reduce national control over critical systems and data.

A sustainable cybersecurity framework should therefore combine international assistance with domestic workforce development, technology transfer, vendor diversification and institutional strengthening [21]. The post-conflict Syrian threat environment is extremely complex. The RSIS analysis notes that reconstituting national cyber capabilities is complicated by the ongoing legacy of pro- and anti-regime hacker networks. The Syrian Electronic Army has historically shown that politically motivated cyber actors can target high-profile organisations and shape information environments. Additional risks stem from foreign state-linked actors, with ESET [6] reporting on nation-state-aligned cyber activity targeting Syrians. Disinformation is

another element of the threat environment. Foreign and domestic actors could exploit political uncertainty to spread false information and undermine confidence in the transitional government. These concurrent threats show that Syria's cybersecurity challenge is not just a technical protection issue, but also one of political stability, information integrity, and national resilience. Despite growing interest, significant gaps remain in the post-conflict cybersecurity literature. However, empirical research analysing Syria's cybersecurity transition after the December 2024 regime change remains limited. Previous research has largely focused on the former regime's cyber activities or on broader cybersecurity challenges in conflict-affected states. Researchers have also paid insufficient attention to the relationship between cybersecurity and state-building, especially how digital security affects state legitimacy, sovereignty and economic recovery [22]. Moreover, the role of international partnerships, sanctions relief, institutional reform, technological diversification and human-capital development needs to be explored. This study fills these gaps by examining Syria's transition from a regime-centric cybersecurity model to a holistic national cybersecurity framework that safeguards critical infrastructure, strengthens institutional resilience, facilitates economic recovery, and reinforces national sovereignty.

## 3. Methodology

This work adopts a qualitative, exploratory and analytical research approach, reflecting the complex, rapidly changing nature of Syria's cybersecurity environment following the fall of the Assad administration in December 2024. This study examines the challenges Syria faces in transitioning from a regime-centric cybersecurity paradigm to an inclusive national cybersecurity paradigm that can safeguard the country's inhabitants, institutions, vital infrastructure, and digital resources. Rather than framing cybersecurity narrowly as a technical problem, the methodology treats it as a multifaceted aspect of post-conflict state-building and national resilience. Particular focus is consequently paid to the interaction between cybersecurity, state-building, national sovereignty, institutional capacity, critical infrastructure protection, technology development and post-conflict resilience. This approach fits because, in a post-conflict context, the configuration of cybersecurity institutions depends not only on available technologies but also on political institutions, legal frameworks, human resources, international relations, infrastructure conditions and public trust. Because Syria's political and cybersecurity landscape is unique, the study relies primarily on secondary sources and documentary analysis to build an integrated assessment of the emerging cybersecurity environment. Primary field data are not the core evidence base, given that institutional structures, regulatory arrangements, infrastructure conditions and cyber-threat trends change rapidly. Instead, the study collates and critically analyzes data and information from academic literature, government publications, international organizations, cybersecurity research organizations, technology organizations, civil society sources and credible media reporting. It sheds light on Syria's digital infrastructure, cyber threats, institutional developments, regulatory measures, technology restrictions, cybersecurity initiatives and international alliances.

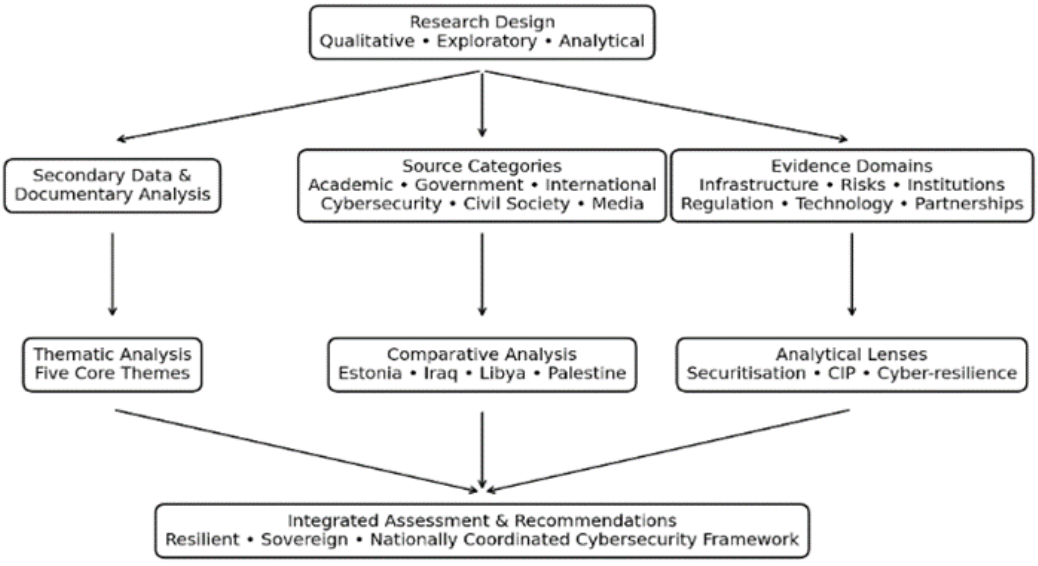



**Figure 1:** Integrated research methodology for assessing post-conflict cybersecurity in Syria

The documentary study also covers the legacy of regime-centric cybersecurity, fragmented hacker networks, weakened digital infrastructure, sanction-related technological constraints and new disputes over digital sovereignty. The aim is to bring together various sources and identify common patterns and links, rather than isolated instances or individual reports. The documentary

analysis is based on an organized process of identification, selection, extraction, comparison and interpretation of sources. The relevant documents are reviewed for relevance to the study's research topics and grouped into evidence on institutional, technological, infrastructural, legal, geopolitical and resilience-related dimensions. Information from multiple sources and source types is compared to avoid dependence on a single institutional or media perspective. Where reports conflict, the analysis considers each source's origin, purpose, breadth and evidentiary basis before integrating them into the overall assessment. This is especially true in post-conflict environments, where information may be sparse, quickly obsolete, politically contentious, or uneven across geographies. Hence, the study uses documentary evidence as contextual and interpretive material, using cross-source comparison to strengthen analytical reliability. The principal interpretive approach is thematic analysis. The collected material is organized into five broad categories that represent Syria's primary cybersecurity challenges. Theme 1: The legacy of regime-centric cybersecurity and political repression: the institutional outcome of security mechanisms that have traditionally privileged regime protection and surveillance over citizen-centred cybersecurity. The second theme concerns disjointed hacker networks and ongoing cyberattacks, with particular reference to the continued existence of decentralized cyber players, shifting threat trends and the challenge of developing coordinated systems for national cyber defence. The third theme addresses damaged digital infrastructure and institutional capacity, including damage to telecommunications and information systems, a lack of skilled personnel, fragmented institutional responsibilities and limitations in incident response and critical infrastructure protection.

The fourth theme explores the technological isolation caused by sanctions and the limitations on procuring cybersecurity technologies, software, hardware, cloud services, technical talent, and foreign technology alliances. The final subject looks at geopolitical issues of digital sovereignty, particularly Syria’s ability to develop independent national cybersecurity capabilities while working with international partners and external technology providers. Beyond these weaknesses, the theme analysis identifies promising prospects that could support institutional rebuilding. These include a national cybersecurity strategy; strategic international and regional alliances; institutional reform; accreditation and regulatory mechanisms; cybersecurity education and professional certification; and mobilizing Syrian technical expertise within the country and diaspora. The analysis explores how these options might help repair trust, improve institutional coordination, enhance technical capability, and create a more nationally coordinated cybersecurity ecosystem. The technique consequently avoids a strictly deficit-oriented perspective on Syria and includes both limits and viable avenues toward institutional rehabilitation. As a complementary strategy, a comparative analysis is utilized to find lessons that may be relevant to Syria. The study examines post-conflict or conflict-affected experiences in Estonia, Iraq, Libya and Palestine, considering disparities in institutional development, cybersecurity regulation, infrastructure resilience, external aid, digital sovereignty and human resource mobilization. Estonia is a benchmark of how digital governance and cybersecurity institutions can be built through strong national coordination and technological capacity. Iraq offers lessons on cybersecurity governance and institutional rehabilitation in a politically fractured, conflict-affected setting. Libya offers comparative insights into institutional fragmentation, infrastructure fragility and the difficulties of restoring governance systems after violence. Palestine offers evidence on cybersecurity in situations of political fragmentation, infrastructure limits, external dependence and challenged sovereignty. These scenarios are not directly translatable models, but cases from which ideas, risks and institutional practices can be critically adapted to Syria's specific context.

**Table 1:** Summary of the research methodology

| Methodological Component | Application in the Study | Analytical Purpose |
|---|---|---|
| Research design | Qualitative, exploratory, and analytical design focused on Syria’s post-conflict cybersecurity transition | Provides an integrated framework for examining complex and rapidly changing cybersecurity conditions |
| Secondary data and documentary analysis | Academic literature, government publications, international organisations, cybersecurity organisations, technology organisations, civil society, and credible media | Establishes the evidence base and triangulates information across different source categories |
| Evidence domains | Digital infrastructure, cyber risks, institutions, regulations, technological constraints, initiatives, partnerships, sanctions, and digital sovereignty | Identifies the principal structural and operational factors shaping cybersecurity reconstruction |
| Thematic analysis | Five themes: regime-centric cybersecurity; fragmented hacker networks; weakened infrastructure and institutions; sanctions-induced isolation; digital sovereignty | Reveals recurring patterns, vulnerabilities, relationships, and institutional challenges |
| Opportunity analysis | National strategy, strategic alliances, institutional reform, accreditation and regulation, and mobilisation of Syrian technical expertise | Identifies feasible pathways for capacity building and reform of cybersecurity governance |

| | | |
|---|---|---|
| Comparative analysis | Post-conflict or conflict-affected cases: Estonia, Iraq, Libya, and Palestine | Generates context-sensitive lessons without assuming foreign models are directly transferable |
| Theoretical interpretation | Draws on securitisation theory, critical infrastructure protection, and cyber-resilience frameworks | Connects political, institutional, infrastructure, and resilience dimensions of cybersecurity |
| Integrated assessment | Synthesis of vulnerabilities, institutional challenges, opportunities, and resilience requirements | Supports practical recommendations for a sovereign, resilient, and nationally coordinated cybersecurity framework |

Finally, the findings are evaluated through three complementary analytical lenses: securitization theory; critical infrastructure protection; and cyber-resilience frameworks. Securitization theory offers a way to study how cybersecurity threats are constructed, prioritized and integrated into national security agendas. The critical infrastructure protection perspective emphasizes protecting and strengthening vital digital and physical systems whose failure could affect public safety, economic activity, government services and national stability. Cyber-resilience offers a broader lens for measuring institutions' and infrastructure's ability to anticipate, withstand, recover from and adapt to cyber catastrophes. Together, these views allow the study to link political, institutional, technological and resilience characteristics rather than addressing them as distinct concerns. Figure 1 illustrates the technique, from research design and secondary data collection to documentary assessment, thematic and comparative analysis, theoretical interpretation and integrated assessment and practical recommendations. The key methodological components and their analytical aim are summarized in Table 1. The integrated design enables triangulation across multiple evidence sources and identifies linkages between institutional flaws, technological restrictions, geopolitical pressures and resilience requirements. It also helps differentiate urgent cybersecurity vulnerabilities from longer-term institutional and strategic concerns. In sum, the technique provides a systematic basis for understanding Syria's evolving cybersecurity environment within the post-conflict reconstruction framework. The study combines qualitative documentary analysis, thematic interpretation, comparative case analysis, and established theoretical frameworks to identify key cybersecurity vulnerabilities, institutional obstacles, technological constraints, and reform prospects. The assessment aims to provide practical recommendations for building a resilient, sovereign and nationally coordinated cybersecurity framework in post-conflict Syria, while recognizing that successful cybersecurity reconstruction will require parallel development of institutions, infrastructure, human capital, regulation, international cooperation and public trust.

## 4. Results

### 4.1. The Syrian Context: From Regime-Centric to National Cybersecurity

Syria's cybersecurity landscape has been fundamentally shaped by the country's authoritarian past. Under Bashar al-Assad, cybersecurity was not a national defense priority but a tool of political repression and regime survival (Figure 2).

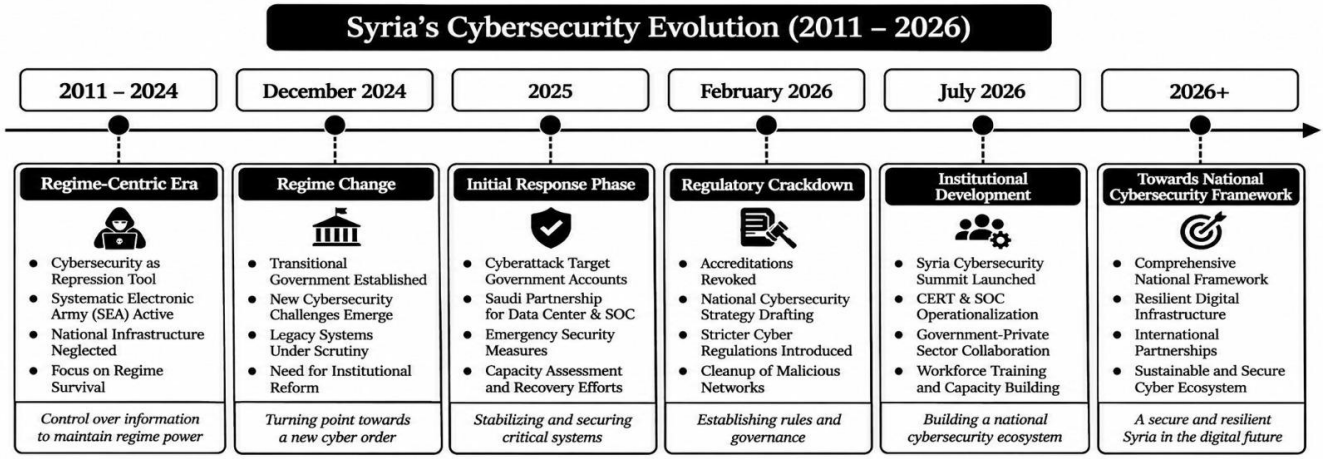



**Figure 2:** Timeline of Syria's cybersecurity evolution (2011-2026)

The regime's cybersecurity approach focused narrowly on protecting regime-linked assets, leaving the broader national infrastructure exposed. National cybersecurity capabilities remained insufficient to protect even the most basic systems. The

Syrian Electronic Army (SEA), a hacker group allied with the Assad government since 2011, exemplified this regime-centric approach. During the civil war, the SEA demonstrated significant offensive cyber capabilities, targeting major international media outlets and quickly becoming one of the FBI's most wanted cyber groups. While the SEA's activities were focused on attacking regime opponents and shaping international narratives, the broader national digital infrastructure was systematically neglected. The fall of the Assad regime in December 2024 marked a watershed moment, creating unprecedented opportunities for reimagining Syria's cybersecurity architecture. However, the new administration faces the daunting task of transitioning from leading a paramilitary opposition movement to becoming a legitimate head of state. The government's weakness is compounded by an equally vulnerable digital infrastructure, neglected for 14 years of civil war.

### 4.2. The Legacy of Regime-Centric Cybersecurity

The Assad regime's approach to cybersecurity left a complex and damaging legacy that the transitional government must address. Most fundamentally, the regime's conflation of regime security with national security means cybersecurity institutions remain associated with the previous regime. This association undermines their legitimacy and complicates institutional reform, as domestic and international actors may view inherited cybersecurity structures with suspicion (Figure 3).

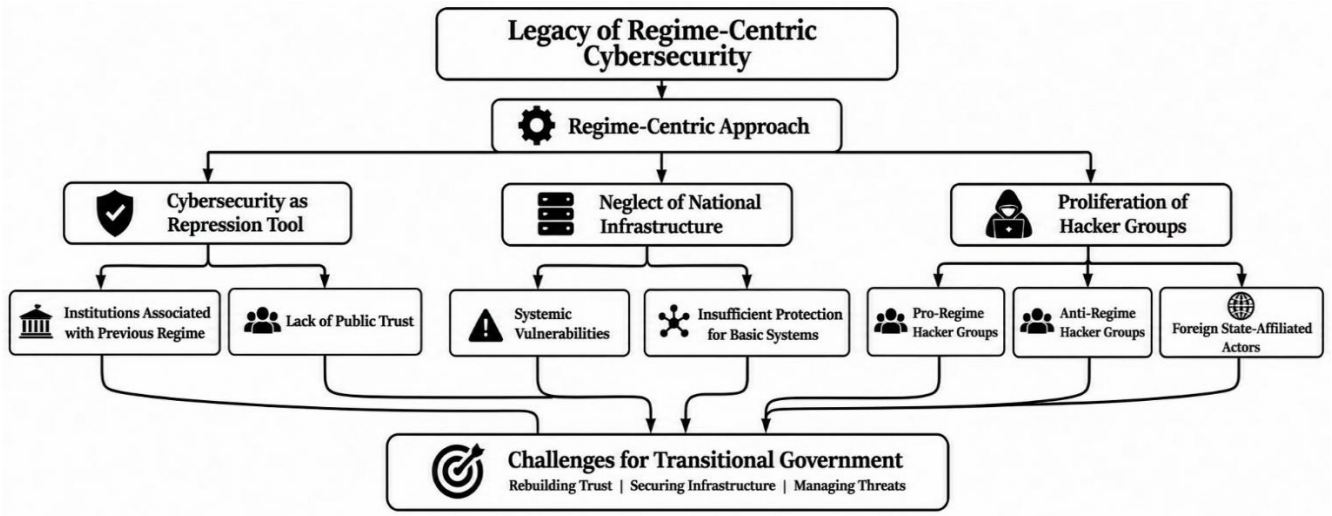



**Figure 3:** The legacy of regime-centric cybersecurity and its challenges

The neglect of broader national infrastructure under the Assad regime created systemic vulnerabilities that persist long after the regime's fall. As the RSIS analysis notes, "the civil war has demonstrated the centrality of cyberspace for regime survival and represents a real challenge to the legitimacy and stability of the new government." The new administration must not only secure its own digital systems but also address the accumulated vulnerabilities of a national infrastructure that was systematically neglected. The fragmentation of the military and security apparatus further complicates the cybersecurity transition. The military is currently a patchwork of loosely coordinated militias and remnants of the transitional government's militant group. This fragmentation is reflected in Syria's cyber environment, where hacker groups that supported the Assad regime, some of which are believed to be based in Russia, continue to pose a threat:

- The fragmented hacker network and Persistent Threats landscape confronting Syria's transitional government is unusually complex. The new administration must contend with multiple categories of cyber threats, each with distinct motivations, capabilities, and operational patterns.
- Pro-regime hacker groups represent perhaps the most immediate threat. The Syrian Electronic Army (SEA), which demonstrated significant offensive cyber capabilities during the civil war, remains a potent force. Should hacker groups loyal to Assad decide to attack the transitional government, they could cause enormous damage and deeply disrupt the digital and physical reconstruction of Syria. In June 2025, Syria's Ministry of Information reported a coordinated cyberattack targeting government websites and social media accounts, believed to have been orchestrated by remnants of the Assad regime.
- Foreign state-affiliated actors pose another significant threat. China-aligned groups have targeted Syrian government networks, with ESET researchers linking this activity to Chinese commercial interest in reconstruction work in Syria. Disinformation campaigns by foreign actors, including from Russia, China, Iran, and Israel, have flooded Syria's digital space with content aimed at destabilizing the fragile new order. Iranian, Russian, Israeli, and Chinese officials have been implicated in online disinformation and "weaponising narratives".

- Hacktivist groups add another layer of complexity. In March 2026, at least 10 official Syrian government accounts on X were compromised in a cyberattack that exposed vulnerabilities in the country's digital infrastructure amid rising regional conflict. The perpetrators, believed to be pro-Israel hackers, compromised accounts belonging to the General Secretariat of the Presidency, the Syrian Central Bank, and multiple ministries.
- The inability to trace or attribute cyberattacks compounds these threats. With limited digital forensic capabilities, Syria cannot trace or attribute cyberattacks. This attribution gap undermines Syria's ability to respond to threats and deter future attacks (Figure 4).

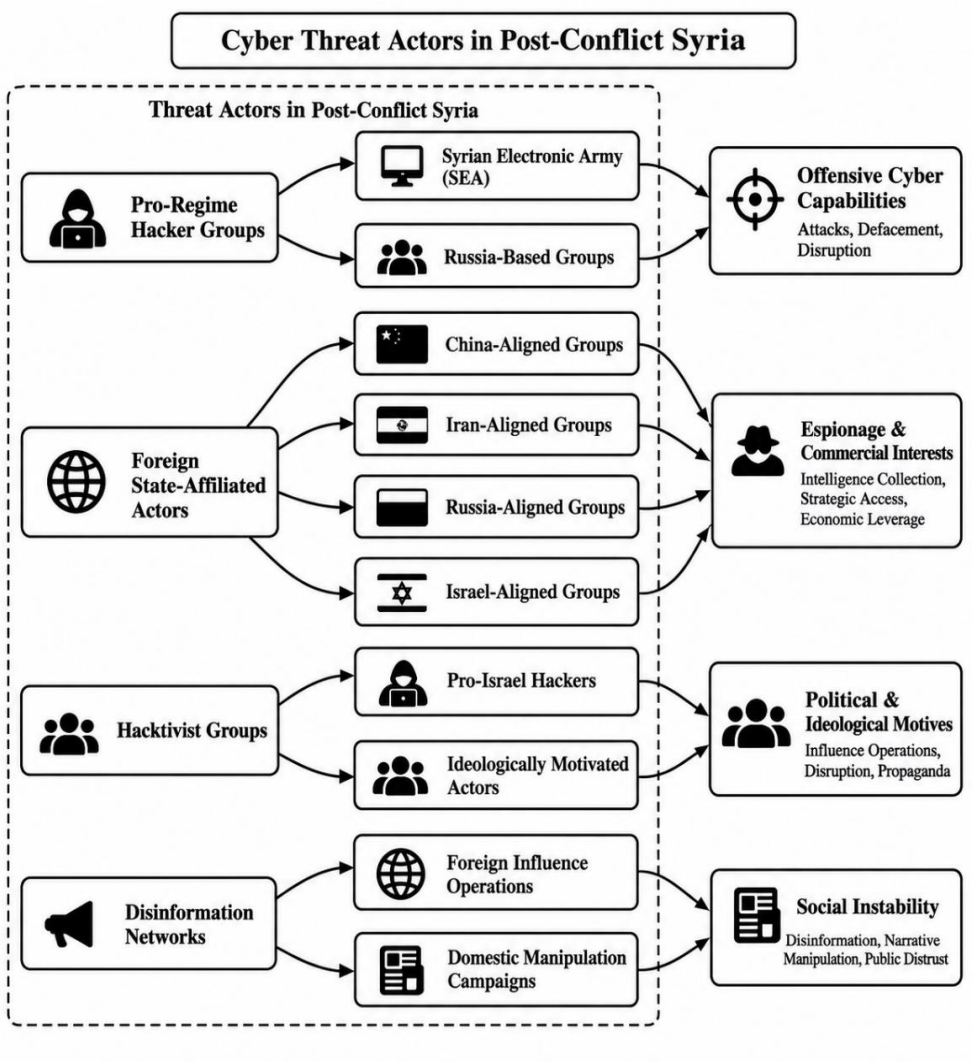



**Figure 4:** Cyber threat actors in post-conflict Syria

### 4.3. Degraded Digital Infrastructure and Institutional Capacity

Over a decade of conflict has devastated the physical and institutional infrastructure required to support national cybersecurity. Half of Syria's infrastructure is "destroyed or rendered dysfunctional," including its communication networks. This destruction is compounded by decades-long stifling sanctions that not only choke Syrians and hinder humanitarian assistance but also bar reconstruction and economic recovery, including the export of telecom and dual-use equipment. The transitional government's inherited digital infrastructure is marked by multiple vulnerabilities. Syria has inadequate telecommunications infrastructure, with weak network coverage outside city centers and connection speeds in many areas barely exceeding a few kilobits per second. The country's internet resilience score is only 31%, with a cybersecurity preparedness score of 51.55 on the 2024 Global Cybersecurity Index and an e-government systems preparedness score of 38.88. Institutional capacity is equally degraded. Under the Assad regime, cybersecurity focused narrowly on protecting regime-linked assets, leaving the wider national infrastructure exposed. National cybersecurity capabilities remain insufficient to protect even the most basic systems (Figure 5).

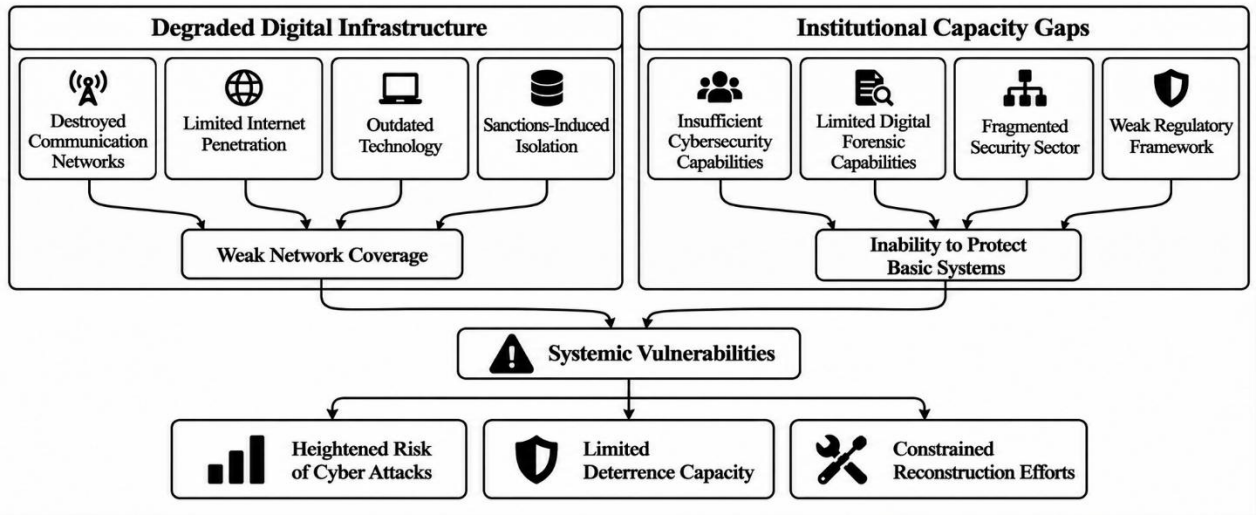



**Figure 5:** Degraded digital infrastructure and institutional capacity gaps

The government has inherited a digital infrastructure weakened by years of international sanctions, which deprived Syrian institutions of access to the latest global cybersecurity tools and protection licenses. Institutional fragmentation in the security sector further complicates cybersecurity governance. The collapse of the Assad regime has left Syria without a unified national army. This fragmentation is reflected in Syria's cyber environment, where multiple actors with varying capabilities and loyalties operate.

### 4.4. Sanctions-Induced Technological Isolation

International sanctions have significantly shaped Syria's cybersecurity vulnerabilities. Under the Assad regime, sanctions deprived Syrian institutions of access to the latest global cybersecurity tools and protection licenses. Syria's telecom infrastructure has relied heavily on Chinese technology due to US sanctions imposed on successive Assad governments over the civil war (Figure 6).

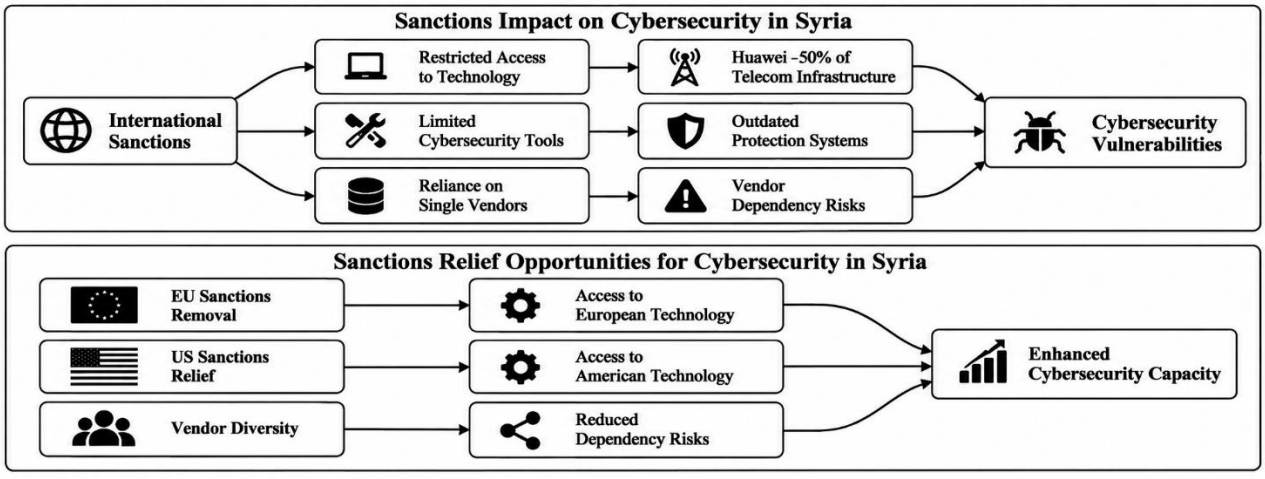



**Figure 6:** Sanctions impact on cybersecurity and relief opportunities

Huawei technology accounts for more than 50% of the infrastructure of Syriatel and MTN, the country's only telecom operators. This heavy reliance on a single vendor creates significant security risks and dependency concerns. The Syrian government acknowledges that US restrictions "hinder the availability of many American technologies and services in the Syrian market". Lifting major sector-specific sanctions in 2025 represents a significant opportunity. The EU announced it would remove all economic sanctions on Syria, and the US announced its intention to lift its sanctions. These welcome developments are critical first steps toward letting Syrians reclaim their digital future. However, challenges remain. Syrian officials say infrastructure development projects are time-critical and that Damascus is seeking greater vendor diversity, but export controls and "over-

compliance" remain an issue. The geopolitical dimension of technology procurement adds further complexity. The United States has warned Syria against relying on Chinese technology in its telecommunications sector, arguing it conflicts with US interests and threatens US national security. Syrian officials said infrastructure development projects were time-critical and that Damascus was seeking greater vendor diversity.

### 4.5. The Geopolitical Dimension: Digital Sovereignty and External Dependency

Syria's post-conflict cybersecurity reconstruction unfolds within a complex geopolitical environment characterized by competing international interests. The Syrian government's digital infrastructure agenda has been marked by a series of agreements that highlight the fragile balance between digital sovereignty and external dependency in the country's post-conflict reconstruction. Negotiations over the $300 million SilkLink project with Zain, e& stc, and Ooredoo have strengthened Syria's ambition to position itself as a terrestrial corridor for Asia-Europe data traffic. The Memorandum of Understanding with Saudi Arabia's Salam for establishing international IP PoPs in Damascus and Aleppo signaled the potential to enhance Syria's direct access to global Tier-1 connections. Meanwhile, 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. This landscape confirms the growing role of Gulf capital and technology providers (Saudi Arabia, Qatar, UAE) while also requiring caution about the continued influence of Iran-linked actors. Analyzing these agreements across three policy axes—standards and cybersecurity, data governance and localization, and dependency risks—underscores the need for strategic diversification and risk mitigation to ensure Syria's digital sovereignty during reconstruction (Figure 7).

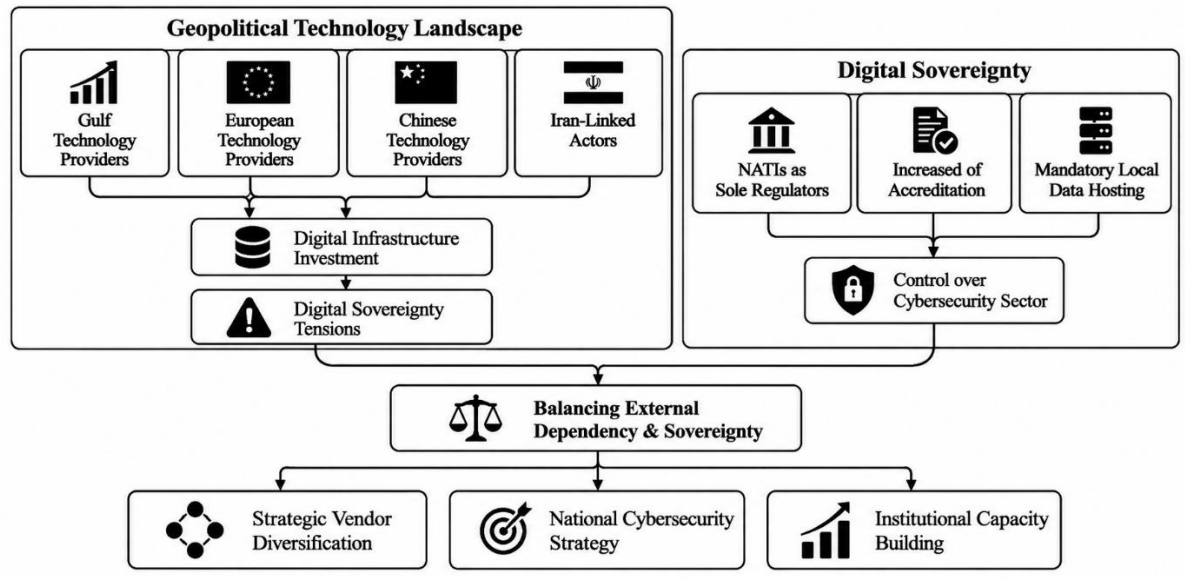



**Figure 7:** Geopolitical technology landscape and digital sovereignty assertion

The Syrian government has taken significant steps to assert digital sovereignty. In February 2026, the government revoked the information security accreditations of several local and regional firms, including XTECH LLC, Smart Systems Solutions, and Talal Abu-Ghazaleh and Co. The National Authority for Information Technology Services (NAITS) said the decision stemmed from the companies' failure to comply with regulations governing information security service providers. This action follows a directive that established NAITS as the sole national authority for information security. A core principle of Syria's digital sovereignty is the mandatory local hosting of all government data. "Hosting any data or systems belonging to the government sector outside the country is strictly forbidden," stated Jihad Alala, Director of the Information Security Center. This commitment to securing national data within its borders reflects a broader push for digital sovereignty.

### 4.6. Emerging Opportunities: The Turning Point

Despite the daunting challenges, significant opportunities for cybersecurity reconstruction have emerged since 2024. Strategic partnerships represent a critical opportunity. In July 2025, the Syrian government signed a strategic cooperation agreement with the Saudi cybersecurity firm Cypher to rebuild Syria's cyber architecture and establish a national cyber institution to train a new workforce. The partnership includes building Syria's first Tier III data center and establishing a Security Operations Center (SOC). This paper aims to accelerate the recovery of technical infrastructure and enhance Syria's capabilities in advanced

technologies, artificial intelligence, and cybersecurity. The partnership also includes a memorandum of understanding with the Syrian Scientific Society for Informatics to build technical capabilities through specialized training programs and transfer Saudi expertise to Syrian cadres. Institutional development is advancing on multiple fronts. The government is actively drafting a "National Cybersecurity Strategy". Jihad Alala confirmed that relevant government bodies are reviewing a draft and that it is expected to launch soon. Alala emphasized that this strategy is part of preparations for an upcoming "digital revolution" and aims to establish the necessary legal and legislative frameworks. The Syria Cybersecurity Summit 2026, which drew 500 experts, represents another significant institutional milestone. The summit focused on implementing an integrated national system to protect digital infrastructure. Officials reported that the SOC and Computer Emergency Response Team (CERT) are being operationalized, along with the creation of a backup data center in Aleppo. Regional partnerships and support for specialized national companies were emphasized as essential to developing Syria's cybersecurity sector. Regulatory reform is also underway (Figure 8).

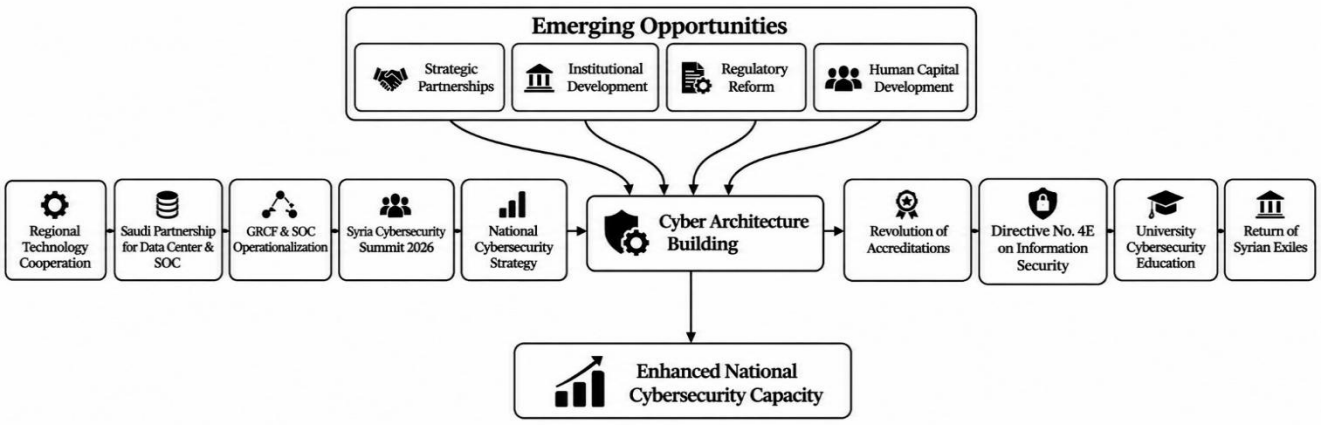



**Figure 8:** Emerging opportunities for cybersecurity development

In December 2025, the General Secretariat of the Presidency issued Directive No. 47 on organizing public entities' work in information security. The government has also revoked cybersecurity accreditations as part of a push for digital sovereignty. Human capital development represents another critical opportunity. The return of Syrian exiles with technical skills could help the government address vulnerabilities in the country's critical digital infrastructure. The Ministry of Higher Education is working with the National Authority for Information Technology to enhance cybersecurity education and integrate it into university curricula, toward a National Cybersecurity Framework: A Conceptual Model. Building a national cybersecurity framework in post-conflict Syria requires a multi-dimensional approach that addresses the interconnected challenges identified above (Figure 9).

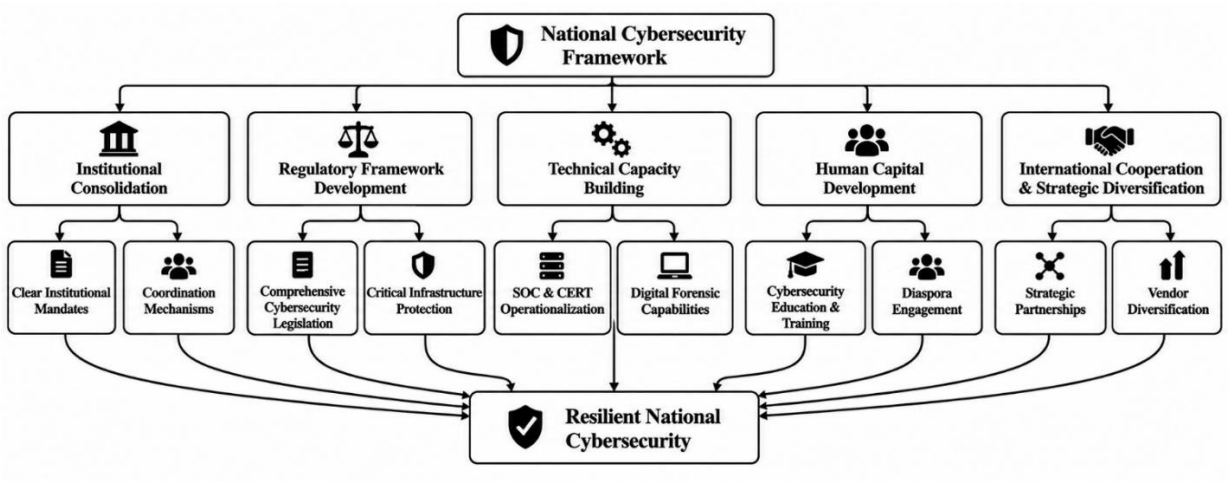



**Figure 9:** Conceptual model for a national cybersecurity framework

Drawing on securitization theory, critical infrastructure protection frameworks, and empirical evidence from Syria's post-conflict experience, we propose a conceptual model centered on five interrelated pillars, beginning with institutional

consolidation. This requires establishing clear institutional mandates for cybersecurity governance, including designating lead agencies, clarifying responsibilities, and developing coordination mechanisms. Establishing NAITS as the sole entity responsible for national-level information security is an important step in this direction. Second, regulatory framework development. This includes drafting and implementing comprehensive cybersecurity legislation, including data protection laws, critical infrastructure protection requirements, and incident reporting obligations. The National Cybersecurity Strategy currently under development provides a policy foundation. Third, technical capacity building. This involves investing in cybersecurity infrastructure, including Security Operations Centers (SOCs), Computer Emergency Response Teams (CERTs), and digital forensic capabilities. Operationalizing the SOC and CERT, along with establishing a Tier III data center, represents tangible progress. Fourth, human capital development. This includes cybersecurity education and training, developing professional certification programs and creating pathways for diaspora engagement. The potential return of Syrian exiles with technical skills and the integration of cybersecurity into university curricula are critical priorities. Fifth, international cooperation and strategic diversification. This involves building partnerships with international cybersecurity providers, diversifying technology vendors to reduce dependency risks, and participating in regional and global cybersecurity initiatives. The strategic cooperation agreement with Saudi Arabia's Cypher and negotiations with multiple international technology providers reflect this approach.

## 5. Discussions

The investigation reveals several key insights into the current state and trajectory of Syria's national cybersecurity reconstruction. One major challenge is the legacy of regime-centric cybersecurity. Cybersecurity, in the limited sense of a tool of political repression and regime survival, was a feature of Bashar al-Assad's rule. Still, the wider national digital infrastructure was nonetheless dangerously vulnerable. The fusion of regime security with national security has linked cybersecurity institutions to the old regime, impeding institutional transformation and eroding public confidence. Therefore, modernizing Syria's cybersecurity system requires not only technical upgrades but also institutional reform and building confidence in cybersecurity governance. Another major challenge is the threat landscape, which is characterized by atypical complexity and persistence. Syria is threatened by many types of players: pro-regime hacker groups, including the Syrian Electronic Army, foreign state-affiliated actors, especially those associated with China, hacktivist groups, and disinformation networks. This range of threat actors creates a layered security landscape, with cyberattacks driven by different motivations, targeting different objectives, and requiring varying skill levels. Limited digital forensics capacity constrains Syria's ability to investigate incidents, identify culprits and confidently attribute cyberattacks. To build a successful national cybersecurity system, Syria must improve forensic investigation, threat intelligence, monitoring, and incident-response skills. Cybersecurity growth is also severely constrained by deteriorating digital infrastructure and weak institutional capability. About half of Syria's infrastructure is categorized as destroyed or non-functional, posing serious problems to the preservation and continuity of digital services. The country's internet resilience score is a paltry 31%, showing serious flaws in the reliability and resilience of its digital connectivity. In this situation, national cybersecurity capabilities cannot consistently defend even the most basic systems.

Therefore, infrastructure rehabilitation must be central to rebuilding cyberspace, because cybersecurity institutions cannot do their work without secure telecommunications networks, data centers, power supplies, secure connectivity and supporting technical infrastructure. Sanctions-driven technological isolation has created risks. Syria's only telecom carriers reportedly have more than half of their infrastructure built on Huawei technology, highlighting the country's heavy reliance on Chinese telecoms technology. Such concentration increases dependency and may heighten security and continuity risks if access to certain technologies, maintenance services, software updates, or replacement components becomes limited. Hence, the findings highlight the need for a more diversified technology environment and stronger indigenous technical capabilities. Diversifying vendors can reduce dependence on a few and provide more flexibility in managing technology, operations and geopolitical concerns. The geopolitical nature of technology acquisition further complicates rebuilding Syria's cyber defenses. The government's digital infrastructure goal is a case study in a difficult balancing act: aspiring to digital sovereignty while still needing external technology, investment, knowledge and relationships. At the same time, governments are pursuing strategic diversification and tightening control over digital infrastructure and information. These include regulatory measures such as withdrawing accreditation and requiring local data hosting. Such developments suggest that rebuilding cybersecurity is not only a technical process but also tied to sovereignty, legislation, international collaboration, and control of the nation's data and digital infrastructure. At the same time, the findings reveal several opportunities to strengthen Syria's national cybersecurity capabilities. These include establishing strategic alliances with local cybersecurity providers, preparing a National Cybersecurity Strategy, strengthening institutions by operationalizing Security Operations Centers and Computer Emergency Response Teams, and encouraging the return or engagement of Syrian professionals with technical know-how.

Mobilizing Syrian technical expertise, especially from the diaspora, can address shortages of specialized human resources and support knowledge transfer and institutional development. These prospects pave the way for incremental progress from disjointed, reactive cybersecurity measures to a more cohesive national framework. From these findings, several recommendations can be made for politicians, foreign partners and cybersecurity practitioners. Syrian policymakers should

first focus on institutional consolidation by developing clear mandates for cybersecurity governance, naming lead agencies, and clarifying roles among relevant government bodies. In this regard, establishing NAITS as the sole organization responsible for information security is a major step and should be supported by institutional coordination mechanisms across government entities. Clear lines of responsibility help reduce institutional fragmentation, enhance accountability and promote coordination in cyber events. Institutional consolidation should also ensure that cybersecurity governance is supported by the right technological, legal and administrative capacities. Finalize and implement a National Cybersecurity Strategy to accelerate development of the regulatory framework. Comprehensive cybersecurity laws should cover data protection, protection of vital infrastructure, cybersecurity standards and mandatory incident-reporting duties. At the same time, regulations must balance legitimate security needs with respect for civil freedoms and human rights. Clear legal responsibilities for public institutions, telecommunications providers, technology companies and other providers of critical services would strengthen national cybersecurity governance and improve consistency in implementing security measures. Technical capacity building should also be recognized as a national priority. Syria needs to invest in security infrastructure, including setting up and operationalizing Security Operations Centers and Computer Emergency Response Teams, building digital forensic capabilities and establishing secure data centers.

These capabilities would improve Syria's ability to identify threats, investigate incidents, coordinate responses and recover from cyberattacks. Establishing national cybersecurity standards and professional certification programs would help advance common technological practices across government and critical infrastructure sectors. Developing human capital is also crucial. Syria should develop cybersecurity education and training programs at all levels, from basic education to university and professional levels. Universities and technical institutes can develop specialized cybersecurity courses, including network security, digital forensics, incident response, cloud security, critical infrastructure protection, and threat intelligence. Professional certification programs and specialized cybersecurity training facilities could also help develop skilled workers. Also, establish mechanisms for diaspora engagement so Syrian cybersecurity professionals working abroad can participate through training, research, advisory roles, remote collaboration and eventual institutional participation. Domestic capacity growth should be coupled with strategic supplier diversity. Syria needs to diversify away from dependence on a single technology source by working with several foreign vendors and building collaborations across different technological ecosystems. Vendor variety can increase technical resilience and lessen supply-chain, geopolitical and continuity concerns. At the same time, investment in domestic cybersecurity capabilities, software development, technical maintenance, research and specialized services can gradually reduce dependence on external partners and increase national technological sovereignty. International partners also play a vital role in helping restore cybersecurity. Support for sanctions relief and access to technology is especially important because rebuilding Syria's cybersecurity infrastructure requires cutting-edge technologies, security software, protection licenses, technical services, and specialist skills. Discussions must recognize that limitations on lawful technology transfer and capacity building may compound challenges to cybersecurity rebuilding for international partners.

Where appropriate, procedures that promote lawful access to cybersecurity technologies, technical help and protective services can support improved national resilience. Another key area for international cooperation is technical support and capacity building. International organizations, cybersecurity institutions, technology companies and academic partners can support the Syrian institutions through training programs, knowledge transfer, curriculum development and technical advisory assistance. Such cooperation could help establish SOCs and CERTs, strengthen digital forensic capabilities, set cybersecurity standards and improve incident-response protocols. Similarly, institutional development aid should focus on regulatory systems, law, standards, accreditation methods and organizational capability so that technological investments are supported by sustainable governance structures. International cooperation should also enable Syria to participate in regional and global cybersecurity initiatives. The availability of threat intelligence, technical expertise, best practices, training programs, and joint incident response capabilities can be improved by fostering collaboration between Syrian cybersecurity entities and their foreign counterparts. Such accords could strengthen Syria's ability to detect emerging risks and respond to cross-border cyber crises by enabling information sharing. Such cooperation should be designed to reinforce national capacities rather than create long-term institutional dependence. Respect for digital sovereignty should remain a key premise of international cybersecurity collaboration. "Syria has a legitimate interest in building the capacity to protect its own digital infrastructure and control national data. International aid should therefore focus on capacity building, knowledge transfer, institutional strengthening and access to technology to help Syrian institutions build sustainable domestic capacities while preserving constructive partnerships with international partners. Syria may benefit from global cybersecurity experience through a balanced strategy that avoids long-term dependence on external support. Complementing these institutional and international actions, cybersecurity practitioners must conduct comprehensive risk assessments across vital industries.

Systematic vulnerability assessments, threat modeling, infrastructure security evaluations and institutional gap analyses can help uncover weaknesses and set investment priorities. Incident response skills should be strengthened through improved procedures for detection, reporting, response and recovery. Government institutions and critical infrastructure operators should have clear incident-reporting procedures and coordination mechanisms in place so that cyber incidents may be addressed swiftly

and consistently. Fundamental flaws can be exploited by typical cyberattacks; therefore, basic cybersecurity hygiene should also be addressed immediately. Some of these measures are:

- Eliminating password reuse
- Enforcing multifactor authentication
- Strengthening access restrictions
- Regularly updating software
- Applying suitable backup procedures
- Enforcing secure account-management practices

These measures can greatly reduce exposure to preventable risks. These precautions should be supplemented by increasingly sophisticated cybersecurity technologies, and not be disregarded in favor of complicated systems. Develop threat intelligence capabilities to routinely gather, analyze, and share information on new and emerging cyber risks. Collaborate with global threat intelligence vendors and participate in data-sharing frameworks to improve visibility into attack methods, signs of compromise, malicious infrastructure, and emerging threat-actor activity. Finally, Syria should build a stronger cybersecurity culture across government, the commercial sector, educational institutions and civil society. Awareness initiatives, professional training, public education campaigns, and organizational cybersecurity policies can help make cybersecurity a collective duty, not a narrowly specialized technical function. Together, they map a holistic path to strengthening Syria's cybersecurity posture through institutional consolidation, regulatory development, technical modernization, human-capital development, international cooperation, vendor diversification, risk management, incident response, threat intelligence, and cybersecurity awareness.

## 6. Conclusion

Syria stands at a critical juncture in its post-conflict reconstruction. The fall of the Assad regime in December 2024 created unprecedented opportunities for reimagining the country's cybersecurity architecture, but the challenges are equally unprecedented. The new administration must rebuild national cyber capabilities while managing the legacies of both pro- and anti-regime hacker networks. It must transition from a regime-centric approach that treated cybersecurity as a tool of political repression to a national framework that protects the entire digital ecosystem. This paper identifies five principal categories of challenges: the legacy of regime-centric cybersecurity, fragmented hacker networks and persistent threats, degraded digital infrastructure and institutional capacity, sanctions-induced technological isolation, and the geopolitical dimension of digital sovereignty. These challenges are interconnected and mutually reinforcing, creating systemic vulnerabilities that require comprehensive solutions. The analysis also identified significant opportunities. Strategic partnerships with regional cybersecurity providers, drafting a National Cybersecurity Strategy, institutional development (including operationalizing SOCs and CERTs), and the potential return of Syrian exiles with technical skills collectively create a more enabling environment for cybersecurity development. The stakes could not be higher.

It has been remarked that "without appropriate digital infrastructure and an effective cybersecurity strategy, Syria's democratic transition will not succeed." Neglecting cybersecurity during post-conflict recovery risks pushing Syria back toward authoritarian practices marked by surveillance, data exploitation, foreign interference, and digital repression. The Syrian case offers lessons for other post-conflict settings. It demonstrates that cybersecurity is not a luxury to be addressed after physical reconstruction but a fundamental prerequisite for state legitimacy, economic recovery, and national sovereignty. It illustrates the profound challenges of transitioning from authoritarian cybersecurity practices to a national framework. It shows that international partnerships, institutional development, and investment in human capital are essential to building cyber resilience in fragile contexts. For Syria, the path forward requires sustained commitment from policymakers, international partners, and cybersecurity practitioners. It requires investment in institutional capacity, regulatory frameworks, technical infrastructure, and human capital. And it requires a vision of cybersecurity that serves not regime interests but the broader national interest—protecting Syria's digital future while respecting the rights and dignity of its citizens. The window of opportunity is narrow and closing rapidly. Delay increases the risk of irreversible cyber vulnerabilities and the consolidation of authoritarian digital practices. But with strategic investment, international cooperation, and sustained political will, Syria can build a national cybersecurity framework that lays the foundation for a resilient, democratic, and prosperous digital future.

**Acknowledgement:** The authors sincerely acknowledge the University of Tokyo, Al-Shahbaa Private University, Singapore Management University, and ETH Zurich for their valuable institutional support and academic encouragement.

**Data Availability Statement:** Access to the research data underpinning the findings of this study may be arranged through the corresponding author upon reasonable request.

**Funding Statement:** This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

**Conflicts of Interest Statement:** All authors confirm that they have no relevant competing interests associated with the research, analysis, or publication of this paper.

**Ethics and Consent Statement:** The research was carried out in compliance with established ethical standards, ensuring the privacy, confidentiality, and anonymity of all participants.

**References**

1. N. Aljizawi, "Syria's recovery depends on rebuilding its digital infrastructure," *Tech Policy Press*, 2025. [Accessed by 11/05/2026].
2. B. Buzan, O. Wæver, and J. de Wilde, "Security: A New Framework for Analysis," *Lynne Rienner Publishers*, Boulder, Colorado, United States of America, 1998.
3. S. Feldstein, "Digital democracy in a divided global landscape," *Carnegie Endowment for International Peace*, 2025. [Accessed by 12/06/2026].
4. R. J. Deibert and R. Rohozinski, "Risking security: Policies and paradoxes of cyberspace security," *International Political Sociology*, vol. 4, no. 1, pp. 15–32, 2010.
5. e-Governance Academy Foundation, "e-Estonia: e-Governance in Practice," *e-Governance Academy Foundation*, 2019. [Accessed by 15/07/2025].
6. ESET, "Newsroom," *Essential Security against Evolving Threats*, 2026. [Accessed by 17/09/2026].
7. S. Feldstein, "The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance," *Oxford University Press,* New York, United States of America, 2021.
8. I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, "Resilience metrics for cyber systems," *Environment Systems and Decisions*, vol. 33, no. 4, pp. 471–476, 2013.
9. M. Ourahli, "Post-conflict challenges for Syria's reconstruction of cyber power," *S. Rajaratnam School of International Studies, Nanyang Technological University*, 2025. [Accessed by 08/07/2026].
10. SANA, "Syria enhances cybersecurity infrastructure after detecting website vulnerabilities," *Syrian Arab News Agency*, 2025. [Accessed by 14/04/2026].
11. SANA, "Syria Cybersecurity Summit 2026 kicks off with more than 500 experts participating," *Syrian Arab News Agency*, 2026. [Accessed by 23/09/2026].
12. S. A. Mitoulis, S. Argyroudis, M. Panteli, C. Fuggini, S. Valkaniotis, W. Hynes, and I. Linkov, "Conflict-resilience framework for critical infrastructure peacebuilding," *Sustainable Cities and Society*, vol. 91, no. 4, pp. 1–19, 2023.
13. L. Tabansky and E. Lichterman, "PROGRESS: The sectoral approach to cyber resilience," *International Journal of Information Security*, vol. 24, no. 11, pp. 1–10, 2025.
14. M. D. Cavelty, C. Eriksen, and B. Scharte, "Making cyber security more resilient: Adding social considerations to technological fixes," *Journal of Risk Research*, vol. 26, no. 7, pp. 801–814, 2023.
15. L. Connolly and S. Igba, "Digital technology as a tool for peace interventions," *South African Journal of International Affairs*, vol. 33, no. 2, pp. 249–269, 2026.
16. M. Gustafsson, O. Matveieva, E. Wihlborg, Y. Borodin, T. Mamatova, and S. Kvitka, "Adaptive governance amidst the war: Overcoming challenges and strengthening collaborative digital service provision in Ukraine," *Government Information Quarterly*, vol. 42, no. 3, pp. 1–11, 2025.
17. L. Streltsov, "The system of cybersecurity in Ukraine: Principles, actors, challenges, accomplishments," *European Journal for Security Research*, vol. 2, no. 11, pp. 147–184, 2017.
18. P. Radanliev, "Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains, and quantum computing," *Journal of Cyber Security Technology*, vol. 9, no. 1, pp. 28–78, 2025.
19. D. Conduit, "Digital authoritarianism and the devolution of authoritarian rule: Examining Syria's patriotic hackers," *Democratization*, vol. 31, no. 5, pp. 979–997, 2024.
20. M. Rohde, K. Aal, K. Misaki, D. Randall, A. Weibert, and V. Wulf, "Out of Syria: Mobile media in use at the time of civil war," *International Journal of Human-Computer Interaction*, vol. 32, no. 7, pp. 515–531, 2016.
21. F. Thiel and R. Orabi, "Reviving Aleppo: Urban, Legal and Digital Approaches for Post-War Recovery," *Springer*, Cham, Switzerland, 2024.
22. Y. Saied, I. Rodionovskaya, M. Nassour, and R. Husen, "The role of smart city applications in the development of IDP areas in war countries," *IFAC-PapersOnLine*, vol. 52, no. 25, pp. 246–251, 2019.

***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.*