FMDB *Transactions on Sustainable Intelligence and Security*

Strengthening Offensive and Defensive Cyber Capabilities Through Unified Cybersecurity Strategies Against Evolving Threats

Jouma Ali Al-Mohamad[1,*], S. S. Rajest[2], C. Suvan Mathew[3], Tan Haoran[4], Fang Zihan[5], Ahmed J. Obaid[6]

[1]Department of Computer and Mobile Communication Engineering, Faculty of Information Engineering, Al-Shahbaa Private University, Aleppo, Syria.
[2]Department of Information Systems, Girne American University, University Avenue, Karmi Campus, Karaoğlanoğlu, Northern Cyprus.
[3]Department of Computer Science and Engineering, University of Galway, University Road, Galway, Ireland.
[4]Department of Information Technology and Engineering, Jingwei Software Co., Beijing, China.
[5]Department Research and Development, Taihu Advanced Materials, Jiangsu, China.
[6]Department of Computer Science, Faculty of Computer Science and Mathematics, University of Kufa, Kufa, Najaf Governorate, Iraq.
jalmohamad@su.edu.sy[1], suman.avancer@gmail.com[2], s.churchill1@universityofgalway.ie[3], tan.haoran@jingwei-software.cn[4], fang.zihan@taihu-materials.com.cn[5], ahmedj.aljanaby@uokufa.edu.iq[6]

Abstract: Syria's offensive and defensive cyber capabilities face significant and complex difficulties after the Assad regime's fall in December 2024. Syria is at a critical point where cyber power is essential for state sovereignty, economic recovery, and national security after nearly fourteen years of civil war that fragmented the country's security apparatus, depleted its human capital, and exposed its digital infrastructure to relentless exploitation. This study identifies and examines five main difficulties using securitization theory, state-building frameworks, and empirical evidence from Syria's post-conflict cyber landscape: The fragmented legacy of offensive cyber assets, the degraded defensive infrastructure, multifaceted external threats, institutional consolidation and regulatory reform, and geopolitical complexities of strategic alliance development. The SEA was the main example of offensive cyber capabilities developed and used by the Assad regime to survive rather than defend the nation. However, defense skills were ignored, exposing vital national infrastructure to threat. The transitional administration inherited a cyber environment where military fragmentation is replicated in cyberspace, pro-regime hacking organizations pose grave dangers, and state cybersecurity skills are insufficient to defend even basic systems. The study also examines strategic partnerships with regional cybersecurity providers, the creation of a National Cybersecurity Strategy, the creation of institutional frameworks like NAITS, and the return of Syrian exile technical talent. The paper ends with concrete advice for policymakers, foreign partners, and cybersecurity practitioners striving to develop a cohesive, resilient, and effective national cyber capability in one of the most difficult post-conflict circumstances of the 21st century.

Keywords: Cyber Capabilities; Offensive Cyber; Defensive Cyber; Syrian Electronic Army (SEA); National Security; State-Building; National Cybersecurity Strategy; Cyber Environment.

Received on: 11/09/2025, **Revised on:** 20/11/2025, **Accepted on:** 27/12/2025, **Published on:** 11/09/2026

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

DOI: https://doi.org/10.69888/FTSIS.2026.000805

Cite as: J. A. Al-Mohamad, S. S. Rajest, C. S. Mathew, T. Haoran, F. Zihan, and A. J. Obaid, "Strengthening Offensive and Defensive Cyber Capabilities Through Unified Cybersecurity Strategies Against Evolving Threats," *FMDB Transactions on Sustainable Intelligence and Security*, vol. 1, no. 3, pp. 182–198, 2026.

[*]Corresponding author.

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

1. Introduction

The sudden emergence of cyberspace as a critical theatre of national power has transformed the meaning of sovereignty, security and state capacity in the twenty-first century. Modern states are increasingly dependent on interconnected digital networks to deliver public services, regulate monetary systems, manage critical infrastructure, coordinate defence institutions, communicate with citizens and participate in the global economy. The ability to create, secure and manage digital infrastructure is thus inextricably linked to the wider process of state-building. Cybersecurity is no longer just a technical responsibility for IT experts; it is now a strategic part of national security that directly impacts political stability, economic development, institutional legitimacy and the protection of citizens [1]. This reality is especially relevant in countries emerging from protracted armed conflict, where physical destruction is compounded by institutional fragmentation, displacement of skilled professionals, technological dependence, and the emergence of competing security actors. Syria is one of the most complex examples of this challenge, as it enters a new political phase following the collapse of the Assad regime in December 2024, after almost fourteen years of civil war. The Syrian conflict has caused massive destruction, impacting almost all areas of national governance and security. Since 2011, the conflict has further eroded state institutions, weakened centralised authority, displaced millions of people, disrupted education and professional development, and damaged telecommunications and information infrastructure [2]. At the same time, the conflict created an increasingly sophisticated environment for digital surveillance, cyber espionage, information warfare, online propaganda, disruption and politically motivated cyber operations.

With the expansion and internationalisation of conventional warfare, cyberspace became another arena for the pursuit of strategic objectives by state and non-state actors [3]. Cyber activities may have targeted government agencies, opposition groups, journalists, activists, civil society organisations, businesses and foreign actors. The present digital environment in Syria, therefore, cannot be understood in isolation from its history of conflict. Its difficulties regarding cybersecurity are very much rooted in the political, military, institutional and geopolitical legacy of the last fourteen years. The demise of the Assad regime has therefore posed a major cybersecurity dilemma. Political transition presents an opportunity to rebuild national institutions and reshape the relationship between the state and cyberspace, but it also creates vulnerabilities that can be exploited during institutional uncertainty [4]. The transitional government inherited digital systems built under conditions of conflict, authoritarian governance, low investment in technology and international isolation. Some of the cyber capabilities developed under the old regime were primarily designed to protect political power, not national infrastructure or the public's welfare [5]. Other capabilities were spread among military, intelligence, political and non-state actors. At the same time, the defensive systems remain insufficient to protect the critical infrastructure against increasingly sophisticated threats. The transition therefore involves two simultaneous imperatives: restructuring the regime-survival cyber capabilities, and developing a legitimate national cybersecurity architecture to protect the emergent state. One of the biggest challenges is the legacy of Syria's offensive cyber capabilities.

Cyber operations were tightly integrated with political control and information management during the era of Assad. The Syrian Electronic Army (SEA) was the most visible face of this approach. The SEA, associated with pro-regime cyber activity, showcased how digital technologies could be weaponised against opposition movements, media organisations, political groups, and foreign entities. These activities were rooted in a model that treated cyberspace as an extension of political and security control [6]. The post-Assad government will therefore have to face the thorny question of how to deal with the personnel, technical knowledge, infrastructure, credentials, tools and organisational relationships linked to these capabilities. Simply transferring former cyber personnel to new institutions could recreate harmful practices and security vulnerabilities, while abandoning their expertise could lose valuable human capital. Rehabilitation therefore requires stringent screening, restructuring of institutions, accountability and a clear distinction between legitimate national cyber defence and politically motivated cyber activity [17]. The challenge is compounded by a fractured post-conflict security environment in Syria more broadly. Years of conflict resulted in the establishment of many military and political organisations with varying command structures, territorial scope, technological resources, and security priorities [7]. This Fragmentation is increasingly visible in cyberspace, where different actors can control separate networks, databases, communication systems and technical resources. Dispersed cyber assets hinder a transitional government from establishing centralised authority over national digital infrastructure.

Coordination is not effective, cybersecurity resources can stay in silos, threat intelligence may not be shared well, and cyber incidents may not be detected or responded to quickly. Former regime-aligned groups and independent actors may also maintain access to digital systems even after the political leadership that supported them has gone. Cybersecurity rehabilitation should therefore be part of broader security sector reform, not an isolated program of technological modernisation. The same is true of defensive cybersecurity [8]. Many systems are vulnerable to unauthorised access, malware, data theft, service disruption,

and other forms of cyberattack due to years of conflict and institutional disruption. Digital technologies are increasingly important to government databases, telecommunications networks, financial institutions, healthcare systems, energy infrastructure, transport services, universities, and other essential sectors. But many systems may be vulnerable because of outdated hardware, unsupported software, poor monitoring, weak security controls, insufficient backup capacity and a shortage of trained cybersecurity professionals. In a post-conflict setting, such weaknesses can have ramifications far beyond the realm of cyberspace [8]. A cyberattack against an electricity grid can paralyse hospitals and businesses; a breach of government databases can undermine public administration; an attack on financial institutions can undermine confidence in the economy; and disruption of telecommunications can interfere with emergency response and governance.

Digital resilience is therefore a fundamental component of national reconstruction. Syria's cybersecurity transition is made more complex by the external threat environment. Foreign intelligence services, state-sponsored cyber actors, criminal organisations, hacktivist groups, and other malicious actors are attracted to the country's digital infrastructure due to its strategic geographic location, political history, regional conflicts, and international significance. In times of political instability, adversaries may exploit institutional vulnerabilities to obtain intelligence, influence political processes, interrupt critical services, steal sensitive information, or establish enduring access to government systems. Syria's transition could therefore increase its cyber-attack surface at a time when its defensive capacity is at its most fragile [9]. Domestic instability and external cyber dangers can be mutually reinforcing, generating an environment in which attacks may exacerbate political uncertainty and economic disruption. The transitional government must therefore develop mechanisms for identifying critical assets, assessing cyber risks, strengthening incident response and coordinating national and international responses to emerging threats. Building effective cybersecurity institutions is at the core of addressing these vulnerabilities [10]. National cyber defences require clear institutional responsibilities and mechanisms for cooperation between government agencies, security organisations, telecommunications providers, private companies, academic institutions and other stakeholders. The establishment and strengthening of institutions such as the National Authority for Information Technology Services (NAITS) could provide an important basis for the coordination of information technology services and support for national digital governance.

However, the problems of cybersecurity in Syria cannot be solved only by creating institutions. Such institutions require: clear legal authority; sustainable funding; technically qualified personnel; operational independence; effective leadership and appropriate accountability mechanisms [22]. They should be detached from military and intelligence institutions to prevent the re-emergence of cyber capabilities focused primarily on political surveillance or domestic repression [23]. Regulatory reform is just as important, because technical controls alone won't maintain cybersecurity. Syria needs a modern legal framework for cybercrime, data protection, privacy, electronic transactions, digital evidence, protection of critical infrastructure, incident reporting, cybersecurity standards and responsible use of cyber capabilities by government institutions [24]. Laws enacted under authoritarianism may not constitute a proper basis for a new political order if they privilege state control over individual rights and institutional accountability. At the same time, a legal vacuum could allow cybercrime, unauthorised access, data exploitation and other forms of digital abuse to flourish. So the reconstruction of regulation must balance the national security needs of the state with privacy, civil liberties, transparency and the rule of law [25]. This balance may be particularly difficult to achieve in a political transition, during which legal and judicial institutions themselves may be undergoing reform. Another fundamental obstacle is human capital. Cybersecurity requires expertise in domains like network engineering, cryptography, threat intelligence, malware analysis, digital forensics, secure software development, incident response, risk management and cyber policy. The years of conflict have disrupted Syria's educational environment and caused the displacement and emigration of highly educated professionals.

The country could end up with a serious shortage of cybersecurity specialists at a time when demand for such expertise is growing. But the Syrian diaspora is a potentially valuable source of technical capacity. Syrian engineers, researchers, software developers, and cybersecurity professionals who have been living abroad have gained experience working in international universities, technology companies, research institutions, and professional organisations [11]. Policies permitting return (temporary or permanent), remote collaboration, knowledge transfer, professional exchanges and educational partnerships could allow the transitional government to make use of this expertise without requiring every specialist to return immediately. Strategic alliances will also be an important part of rebuilding national cyber capabilities. Syria may require technical assistance, training, cybersecurity technologies, threat intelligence, infrastructure modernisation, and institutional support from regional and international partners. Immediate access to expertise and technologies that are difficult to develop domestically could be gained through short-term cooperation with regional providers of cybersecurity expertise and technologies. International organisations and partner governments can also support capacity-building, cybersecurity education, governance reform, and critical infrastructure protection [12]. But partnerships can also be potential risks. Over-dependence on external suppliers might result in technological dependence, put sensitive government information at risk, or restrict Syria's ability to maintain independent control over key strategic systems. Thus, strategic alliances need to take into account sovereignty, transparency, technology transfer, interoperability, sustainability and data protection. International cooperation should complement, and not permanently replace, domestic capability.

These challenges are compounded by the economic stakes involved with cybersecurity [13]. Digital connectivity, electronic financial services, telecommunications, digital government platforms, online commerce and integration with international markets will be of increasing importance for the long-term recovery of Syria. For businesses, investors, humanitarian organisations and international institutions to be effective, they need reliable and secure digital infrastructure. Weak cybersecurity can discourage investment, disrupt critical services, lead to higher financial losses, and damage public confidence in the digital transformation. Conversely, a secure digital environment can support economic modernisation by enabling trusted electronic transactions, encouraging innovation, improving public administration, and facilitating international cooperation. Cybersecurity should therefore be built into national reconstruction planning from the outset and not be treated as an add-on technical requirement after digital infrastructure has been created. Securitisation theory offers a useful framework to understand the transformation of Syria's cybersecurity agenda [14].

Under the previous regime, cyber assaults were often seen as threats to the survival of the regime, with opposition activities and information warfare viewed as threats to the authority of the regime. Cyber capabilities might therefore be justified by exceptional security narratives and used to buttress centralised political control. The post-Assad transition offers the opportunity to reshape the object of cybersecurity. National cyber institutions should be committed to defending state sovereignty, public institutions, critical infrastructure, economic systems and citizens, not specific political leadership [15]. This is not only an institutional transformation, but also a conceptual one, because it implies redefining cybersecurity as a public good and as a part of legitimate state capacity and not as an instrument of political coercion. From a state-building perspective, the reconstruction of cybersecurity institutions should be seen as part of the broader rebuilding of state authority. A viable state needs to be able to exercise control over its territory, but also provide services, protect its citizens, manage information, maintain its economic systems and respond to new threats.

In a society that is becoming more and more digital, these functions rely on secure information systems. Even a government with conventional security capabilities may have trouble asserting effective authority if it is unable to secure its networks or critical infrastructure. So, cybersecurity directly supports institutional legitimacy and resilience [16]. So Syria's digital security environment will have to be rebuilt alongside reforms to public administration, telecommunications, security institutions, legal systems, and economic structures. A National Cybersecurity Strategy could provide the umbrella framework within which these requirements are coordinated. Such a strategy would need to set out national priorities, identify critical information infrastructure, set out institutional responsibilities, create cybersecurity standards, strengthen incident-response mechanisms, develop national cyber skills, promote public-private cooperation, and set out the governance of offensive cyber capabilities. It should also provide mechanisms for continuous evaluation as cyber risks evolve rapidly and cannot be addressed through a static policy framework [17].

A national overarching strategy could also facilitate international cooperation by spelling out Syria's cybersecurity priorities and setting out clear principles for engagement with external partners. Thus, rehabilitating Syria's cyber capabilities is a multidimensional challenge, involving technology, institutions, human resources, law, national security, economics and geopolitics. The country does not have an empty technological base to start from, but it cannot just re-establish the cyber institutions of the previous regime. Instead, it has to determine what existing capabilities can be transformed into legitimate national assets, what structures need to be dismantled, and what new institutions and capabilities need to be created. The essential challenge is how to transform a fragmented and politically charged cyber landscape into a unified, resilient, accountable, and nationally focused cybersecurity architecture. In this framework, this study addresses the most prominent challenges facing the rehabilitation of Syria's offensive and defensive cyber capabilities, after the fall of the Assad regime [18].

It is concerned with five interrelated matters: the broken heritage of offensive cyber assets, the broken-down state of defensive infrastructure, the continuing presence of hybrid external threats, the need for institutional consolidation and regulatory reform, and the geopolitical complexities of strategic partnership building. It also examines new opportunities within the framework of the development of a National Cybersecurity Strategy, the strengthening of institutions through bodies like NAITS, the cooperation with regional cybersecurity providers, and the mobilisation of Syrian technical expertise in the diaspora [19]. By analysing these factors through the frameworks of securitisation theory and state-building, the study demonstrates that cyber rehabilitation is not merely a technological recovery project, but a fundamental component of Syria's broader political and institutional reconstruction. Ultimately, the fate of Syria's cyber power will depend on the ability of the transitional state to convert a fractured and historically politicised cyber sphere into a coherent national capability focused on resilience, sovereignty, economic recovery, and public security [20].

This process requires investment in defensive infrastructure, professional human capital, institutional coordination, legal reform and strategic alliances while establishing safeguards against the misuse of cyber capabilities. If these elements are developed in an integrated way, Syria's post-conflict transition could offer a chance to build a cybersecurity architecture that is substantially different from the Assad era. Such an architecture would not only repair damaged systems, but also lay the foundation for a secure digital state, able to protect critical infrastructure, support economic recovery, strengthen institutional

legitimacy and respond effectively to future cyber assaults [22]. The rehabilitation of Syria's cyber capabilities should therefore be understood as a core component of twenty-first-century state reconstruction and a necessary precondition for a stable, sovereign and digitally resilient Syria.

2. Literature Review

The relationship between cyber power and state-building in post-conflict settings has emerged as an increasingly important subject of academic inquiry. Classical theories of state power, exemplified by the work of Morgenthau [11] and Waltz [21], focused on military capabilities, economic resources, territorial control, and diplomatic influence. But the rapid digitisation of governance, critical infrastructure, communication, and economic activity has shifted the foundation of national power. According to Nye [12], cyber power has emerged as an important tool for states to pursue national goals, to influence other actors and to exercise strategic power. This dimension is particularly salient in post-conflict societies, where the reconstruction of secure digital infrastructure is inextricably linked to the restoration of administrative capacity and national sovereignty. Thus, for states, the idea of cyber sovereignty comes to the fore, as they seek to reduce technological dependence while developing autonomous digital capacities. In post-conflict settings, the need to build domestic capabilities is at odds with reliance on external technology, especially when sanctions and political restrictions limit access to the most advanced technologies, according to a study by the Carnegie Endowment for International Peace [5]. These theoretical considerations are particularly applicable to the case of Syria, where the transitional government is expected to rebuild the national digital institutions, while protecting critical systems and gaining more control over its cyberspace. Securitisation theory is another theoretical framework to understand the definition of cyber capabilities as national security priorities. Securitisation theory, developed by Buzan et al. [4], explains how political actors convert certain issues into existential threats that require extraordinary security responses. In fragile and transitional states, cyberspace can be securitised through offensive and defensive methods. Offensive capabilities might be developed to deter external adversaries and respond to perceived threats, while defensive capabilities are needed to protect national infrastructure, government systems and citizens.

The Syrian case shows how cybersecurity can be tightly linked to the survival of a regime. Feldstein [8] reports on the wider adoption of digital technologies by authoritarian governments for surveillance, political control, repression and international influence. Syria's cyber capabilities under Bashar al-Assad also had a regime security focus, rather than a full national cybersecurity focus. This distinction is important for post-conflict reconstruction, because the transitional government must convert cybersecurity from an instrument of political control into a tool for protecting national sovereignty, public institutions, critical infrastructure, and citizens. The proliferation of offensive cyber capabilities under authoritarian governments has garnered significant scholarly interest. Syria is a good example, with the Syrian Electronic Army (SEA) becoming a pro-regime hacking group during the civil war. The SEA's cyber operations against opposition groups, journalists and media organisations, and foreign targets illustrated the potential of cyber capabilities to support political objectives and information warfare. SEA's activities have been the subject of reports that show the use of offensive cyber operations to shape narratives and intimidate perceived opponents [19]. Such capabilities, however, did not result in the development of a comprehensive national defensive architecture. This imbalance is all the more important in the post-Assad context, where the transitional authorities will need to find a way to manage inherited personnel, technical expertise, infrastructure and cyber tools, while preventing their reuse for political repression. Ourahli [13] points out the dilemma for the new administration to create legitimate national cyber capabilities, while handling the persistent legacy of pro- and anti-regime hacker networks in Syria. This difference makes post-conflict cyber rehabilitation distinct from traditional cybersecurity development in that reconstruction requires both capability creation and restructuring of inherited cyber assets.

A further major dimension of post-conflict cyber rehabilitation is defensive cyber capability and critical infrastructure protection. Adequate institutional capacity, technical infrastructure and skilled personnel are necessary to have effective national cybersecurity systems, according to the International Telecommunication Union [9]. In countries affected by conflict, these requirements are harder to meet, as physical networks may be damaged, information systems outdated, institutions fragmented, and trained professionals may have migrated. The concept of cyber resilience proposed by Linkov et al. [10] would be particularly relevant as it emphasises the ability of systems not only to prevent cyber incidents, but also to withstand, respond to and recover from attacks. Syria has been at war for years, and its digital infrastructure is therefore vulnerable, while its defensive capabilities are still in their infancy. The rebuilding of the digital infrastructure and the development of a comprehensive cybersecurity strategy are the basis for Syria's recovery, according to Aljizawi [2]. Similarly, access Now [1] emphasises the necessity of protecting Syria's digital future through stronger institutions and rights-based digital governance. These views imply that defensive cybersecurity should be embedded in broader reconstruction efforts and not treated as a stand-alone technical problem. Post-conflict Syria faces an especially complex threat environment, given its composition of domestic, regional and international actors. Pro-regime hacker groups are a possible threat, and other risks are presented by foreign state-linked groups and politically motivated groups. StrongPity, also known as Promethium, has been involved in cyber espionage activities with targets in Syria, demonstrating that sophisticated cyber assaults still exist against Syrian systems [3].

China-aligned cyber activity against Syrian government networks has also been found by research. Iranian-linked groups have a history of operating against individuals with ties to the Syrian opposition [7]. Repeated cyberattacks by hacktivist groups such as Sadeh et al. [6] have also played a role in the country's complex threat landscape. Syrian government reports have also documented coordinated attacks against government websites and information systems [14]; [15]. These developments demonstrate that the transitional government must confront cybersecurity in an environment of ongoing and overlapping threats, rather than assuming that political transition will automatically reduce cyber risks. Comparative experiences give further insights into the challenges of cyber rehabilitation in post-conflict settings. Estonia's post-Soviet development shows how early investment in digital infrastructure, cybersecurity institutions, and digital governance can maintain long-term state capacity. However, Estonia had relatively stable political conditions, European integration and access to international institutional and financial support, which makes direct comparison with Syria difficult. A cautionary example is Iraq, where the dismantling of established security structures after 2003 resulted in institutional disruption and opened up opportunities for internal and external actors. Libya has also demonstrated the difficulty of creating cohesive national institutions amid a landscape of competing armed groups and fractured authority.

The cases suggest the importance of balancing the institutional restructuring of Syria's cyber rehabilitation with the continuity of critical technical capabilities. While there is increasing research on cyber security and post-conflict reconstruction, there remain significant gaps. There is limited empirical analysis in the existing literature regarding Syria's cyber capability rehabilitation following the December 2024 political transition. Also, there is a lack of research on offensive and defensive capabilities as connected components of national cyber power. The role of international partnerships, sanctions, regulatory reform, institutional consolidation and diaspora expertise in rebuilding Syrian cybersecurity is also underexplored. Emerging institutional response. The Syrian Ministry of Communications and Information Technology has developed an ITU-D Cybersecurity [18], and there have been cybersecurity training initiatives and initiatives to introduce cybersecurity into higher education. Another example is the 2026 Syria Cybersecurity Summit, which demonstrates the increasing focus on national cybersecurity capacity-building [16]. These developments offer an important starting point for exploring how Syria can transform fragmented and historically politicised cyber capabilities into a coherent national cybersecurity architecture. This study seeks to address these gaps by examining the challenges, institutional requirements, external threats, and strategic opportunities within the framework of Syria's rebuilding of offensive and defensive cyber capabilities during the post-conflict transition phase.

3. Methodology

The present study adopts a qualitative research technique to examine the obstacles and opportunities that are present for the reconstruction of Syria's offensive and defensive cyber capabilities following the fall of the Assad regime in December 2024. Given the quickly evolving post-conflict cybersecurity environment in Syria, which remains under-researched in the existing academic literature, the study is designed as an exploratory and analytical piece of research. Instead of statistical measurement, the study focuses on reported developments, institutional adjustments, cyber events, rising threats, and foreign alliances to create a contextual picture of Syria's evolving cybersecurity needs. The qualitative approach is justified because many aspects of post-conflict cyber capability development involve institutional relationships, governance arrangements, political and security contexts, technological dependencies, and capacity-building processes that cannot be fully captured through quantitative indicators alone. The study methodology incorporates document analysis, theme analysis and comparative case analysis. Researchers rigorously analyze papers from academic publications, cybersecurity reports, government pronouncements, international organization documents, research-institution publications, technology-company reports, and reliable media sources. This analysis is based mainly on secondary data because of the lack of access to comprehensive primary cybersecurity datasets from Syria.

Key sources are publications and assessments from the International Telecommunication Union [9], United Nations Development Programme (UNDP) [20], Carnegie Endowment for International Peace [5], Ourahli [13], Access Now [1], and Salivio et al. [7], as well as key Syrian government entities. These sources cover cybersecurity occurrences, institutional advancements, digital infrastructure, cyber risks, legislative initiatives, and international collaboration. The employment of numerous categories of sources enables the study to triangulate developments and minimize dependency on a single institutional or media standpoint. The research is theoretically grounded in the existing academic literature on cyber power, securitization, state-building, cyber resilience and digital repression. The notion of cyber power offers a way of understanding how governmental institutions and others may utilize digital capabilities for the goals of security, governance, influence, intelligence, and strategy. Drawing on securitization theory, researchers analyze how cybersecurity risks are constructed as problems for which special attention, institutional response and resource allocation are warranted. State-building approaches offer useful insights into how cybersecurity institutions might play a role in legitimate governance, institutional consolidation and post-conflict national reconstruction. Cyber-resilience concepts are used to study the capacity of institutions and key digital infrastructure to resist, respond to, recover from, and adapt to cyber events. For further information on the history of state-

controlled cyber operations and the significance of moving toward accountable and domestically oriented cybersecurity organizations, see the literature on digital repression.

The documentary material is ordered both chronologically and thematically, with special emphasis on developments documented after 2024. Researchers evaluate government comments and cybersecurity reports to discover new threats, reported cyber events, institutional developments, and national cybersecurity strategies. The gathered material is then coded and classified along five main analytical dimensions: inherited offensive cyber capabilities, defensive infrastructure deficiencies, external and internal cyber threats, institutional and regulatory development and international strategic partnerships. The first dimension looks at the cyber capabilities and organizational legacies inherited from the former political system, particularly the consequences of moving from regime-oriented cyber operations to nationally responsible and legally governed cyber capabilities. The second dimension is the lack of defensive infrastructure, including security monitoring, incident response, digital forensics, critical-infrastructure protection, and data resilience. The third analytical dimension concerns external and internal cyber hazards. Outside dangers include foreign state-affiliated actors, cyber-espionage campaigns, hacktivist activity, harmful cyber operations, and other threats that may target Syrian government networks or persons. The internal hazards include: institutional fragmentation, lack of understanding of cybersecurity, poor control of access, poor reporting on incidents and limited technological competence. The fourth is institutional and regulatory development, such as the creation or strengthening of national cybersecurity authorities, the elaboration of cybersecurity strategies, regulatory standards, incident-response structures and coordination mechanisms among public institutions.

The fifth pillar is about worldwide strategic alliances, such as with technology providers, international organizations, bordering states, research institutes and cybersecurity groups. In the evaluation of these alliances, consideration is given to technical support, financing, transfer of technology, training, infrastructure development and any risks of external dependency. Thematic analysis is used to uncover repeating patterns, correlations and differences across the material collected. Evidence from diverse sources is evaluated to find areas of agreement and regions of disagreement, and ambiguous or disputed assertions are treated with caution. Thematic categories are evaluated not just in their own right but also in connection to the other dimensions. For example, flaws in defensive infrastructure may be related to a lack of trained staff, and institutional fragmentation may influence incident response and threat attribution. Likewise, international alliances may give key opportunities for capacity development, but also pose issues of data governance, dependence on technology, supply-chain security and digital sovereignty. This integrated analysis enables the study to go beyond a straightforward presentation of specific cybersecurity concerns and to analyze the structural relationships that shape Syria's cyber recovery. It also includes a comparative case study component that draws insights from various post-conflict and transition contexts. The choice of case studies (Estonia, Iraq, Libya and Palestine) is justified by the diverse insights they offer on digital state-building, institutional fragmentation, foreign help, cybersecurity capacity-development and the rebuilding of digital infrastructure.

The comparative analysis does not presume these situations are directly comparable to Syria. Rather, they serve as contextual points of reference for extracting transferable lessons, recurring institutional issues and techniques that may need to be adapted to Syria's particular political, technological and security situation. Special focus is given to how governments and organizations in these situations built cybersecurity governance, dealt with infrastructure constraints, controlled external aid, and attempted to develop resilient digital systems. The research also uses a structured source-evaluation method to enhance the trustworthiness of the qualitative findings. Academic research is evaluated for methodological integrity and relevance; institutional reports are evaluated for the authority and experience of the issuing organization. Government statements are used largely to document official stances and institutional developments, while cybersecurity industry reports include technical information about specific threats and occurrences. These are augmented by credible media sources and timelines where applicable. In cases when sources offer competing interpretations, the study distinguishes between documented facts and analytical interpretations, and refrains from classifying unconfirmed assertions as proven conclusions.

This technique is especially critical in a post-conflict environment because information may be fragmentary, politically contentious or fast-changing. Finally, the findings are analyzed via the lens of securitization theory and state-building frameworks to explore how cybersecurity might help toward sovereignty, institutional legitimacy, resilience and national regeneration. The analysis examines whether the creation of national cyber institutions may improve the capacity of states and guarantee that cyber capabilities are subject to proper legal and institutional supervision. Focus is given to the shift from regime-centric cyber operations to nationally accountable cybersecurity organizations that emphasize the protection of public institutions, key infrastructure, individuals and essential digital services. Thus, the research addresses cybersecurity rehabilitation not as an isolated technical modernization task, but as a component of a broader post-conflict institutional reconstruction. Finally, the technique integrates theoretical inquiry, documentary evidence, thematic analysis and comparative experience to generate pragmatic and context-aware recommendations for the reconstitution of Syria's offensive and defensive cyber capabilities. The framework is meant to guide future research, policy, institutional planning, capacity building and international cooperation, acknowledging the ambiguity and fast-changing character of Syria's post-conflict cybersecurity environment.

Table 1: Research methodological components and their purpose

Methodological Component	Data/Focus	Purpose in the Study
Document Analysis	Academic publications, government statements, cybersecurity reports, institutional and industry sources	Identify documented threats, incidents, policies, institutional changes, and cybersecurity initiatives.
Thematic Analysis	Post-2024 evidence organized into five analytical dimensions	Identify recurring patterns, relationships, challenges, and opportunities for cyber capability development.
Comparative Case Analysis	Estonia, Iraq, Libya, and Palestine	Provide contextual lessons on digital state-building, institutional development, external assistance, and capacity building.
Theoretical Analysis	Cyber power, securitisation, state-building, cyber resilience, and digital repression literature	Interpret cybersecurity developments within broader security, governance, and reconstruction frameworks.

Main methodological components used in the investigation are summarized in Table 1. The document analysis provides the empirical basis; thematic analysis structures the evidence into related analytical dimensions; comparative case analysis provides lessons from other transitional contexts; and theoretical analysis supports the interpretation of cybersecurity development in the broader processes of state-building, resilience, and institutional legitimacy.

Table 2: Five analytical dimensions for assessing Syria's cyber rehabilitation

Analytical Dimension	Key Issues Examined	Expected Analytical Contribution
Inherited Offensive Cyber Capabilities	Legacy capabilities, organizational structures, command arrangements, legal and ethical oversight	Assess the transition from regime-centric operations toward nationally accountable cyber capabilities.
Defensive Infrastructure Weaknesses	SOC/CERT capacity, digital forensics, critical infrastructure, monitoring, incident response, data resilience	Identify major defensive gaps and priorities for national cyber resilience.
External and Internal Cyber Risks	Foreign actors, espionage, hacktivism, malicious activity, institutional and human vulnerabilities	Map the principal threat environment and associated response requirements.
Institutional and Regulatory Development	National authorities, cybersecurity strategy, laws, standards, coordination and compliance	Assess progress toward coherent national cybersecurity governance.
International Strategic Alliances	Technical assistance, financing, technology transfer, training, infrastructure and dependency risks	Evaluate opportunities and risks associated with international cybersecurity cooperation.

Table 2 the five analytical dimensions used to structure the theme assessment. These characteristics taken together give a complete framework for analyzing both inherited shortcomings and emergent opportunities. The framework integrates the technological cybersecurity requirements with institutional governance, human capability, external collaborations and broader goals of the post-conflict state reconstruction.

4. Results and Discussions

4.1. The Syrian Context: From Fragmented Militias to Unified National Cyber Defense

Syria's cyber capability landscape has been fundamentally shaped by the country's authoritarian past and the protracted civil war that followed. Under Bashar al-Assad, cyber capabilities were developed and deployed not as instruments of national defense but as tools of regime survival. The Syrian Electronic Army (SEA), a hacker group allied with the Assad government since 2011, exemplified this approach, demonstrating significant offensive cyber capabilities while the broader national infrastructure was systematically neglected. The fall of the Assad regime in December 2024 marked a watershed moment, creating unprecedented opportunities for reimagining Syria's cyber architecture. President Ahmed al-Sharaa faces the daunting task of transitioning from being the leader of a paramilitary opposition movement, previously internationally designated as a

terrorist organisation, to that of a legitimate head of state. The weakness of the government is compounded by an equally vulnerable digital infrastructure, neglected by 14 years of civil war. The collapse of the Assad regime has left Syria without a unified national army. The military is currently a patchwork of loosely coordinated militias and remnants of al-Sharaa's Hay'at Tahrir al-Sham militant group (Figure 1).

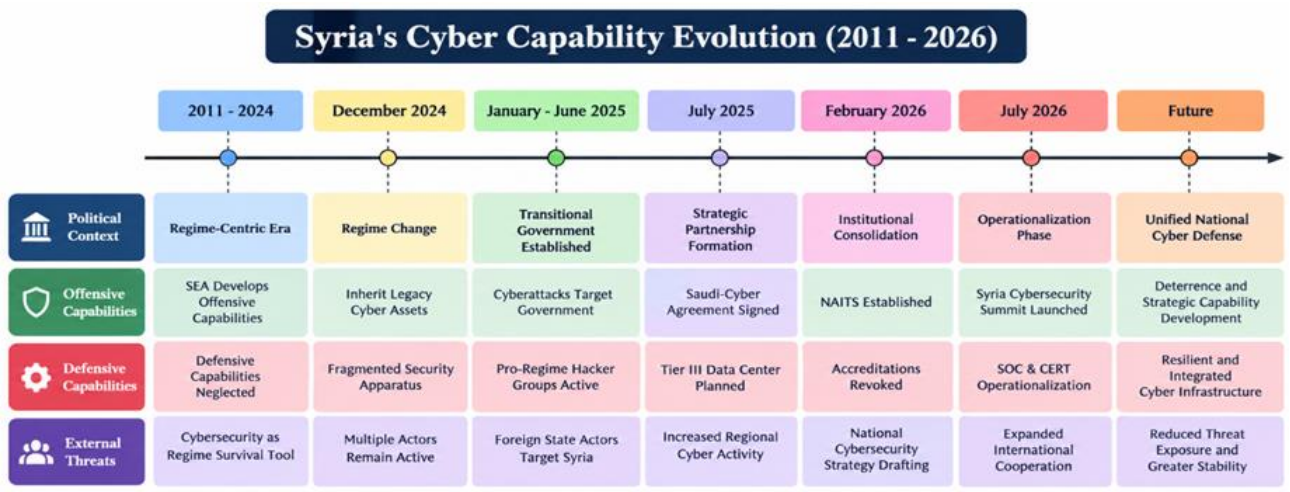


Figure 1: Timeline of Syria's cyber capability evolution (2011-2026)

This fragmentation is also 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.

4.2. The Fragmented Legacy of Offensive Cyber Assets

The Syrian Electronic Army (SEA) represents the most prominent legacy of Syria's offensive cyber capabilities. Formed in 2011 as a hacker group allied with the Assad government, the SEA demonstrated significant offensive cyber capabilities during the civil war. Its operations included targeting major international media outlets, including Twitter (now X) and The New York Times, and it quickly became one of the FBI's most wanted cyber groups. The SEA's operational capabilities were substantial and sophisticated. The group demonstrated the ability to conduct domain name system (DNS) hijacking attacks, compromising the digital infrastructure of major media organizations. Its attacks on Twitter, The New York Times, and The Huffington Post's UK website demonstrated both technical sophistication and strategic intent. The group's operations were focused on attacking regime opponents, shaping international narratives, and demonstrating the regime's cyber capabilities to both domestic and international audiences (Figure 2).

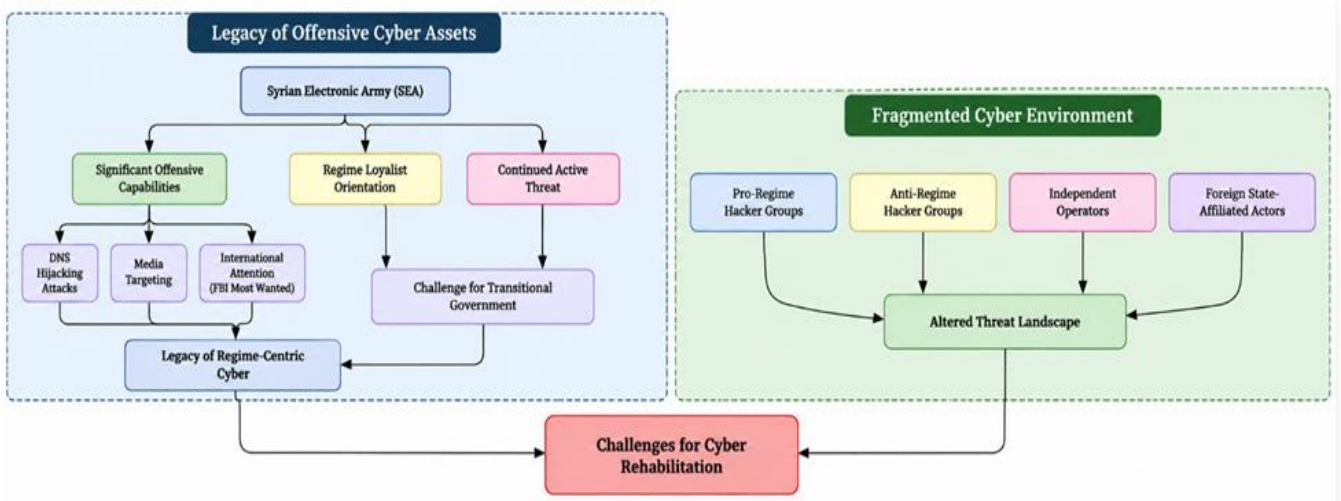


Figure 2: Legacy of offensive cyber assets and fragmented cyber environment

The legacy of the SEA presents multiple challenges for the transitional government. First, the group remains active and continues to pose a threat. 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. Second, the association of offensive cyber capabilities with the previous regime complicates efforts to develop new capabilities that serve national rather than regime interests. Third, the proliferation of hacker groups aligned with or opposed to the previous regime creates an atomized and potentially hostile cyber environment. The fragmentation of Syria's security apparatus is reflected in the cyber domain. The military's fragmentation into loosely coordinated militias is mirrored by the proliferation of hacker groups with varying loyalties and capabilities. Some groups remain loyal to the Assad regime, some have aligned with the transitional government, and others operate independently. This fragmentation complicates efforts to develop unified national cyber capabilities and creates vulnerabilities that can be exploited by external actors.

4.3. The Degraded State of Defensive Infrastructure

The defensive cyber capabilities inherited by the transitional government are characterized by profound degradation. Under Bashar al-Assad, 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. The physical infrastructure that underpins defensive capabilities has been devastated by over a decade of conflict. Syria's digital infrastructure has been neglected and damaged, with nationwide outages disrupting communications after fibre-optic lines were cut across the country. The country's internet resilience score is low, with network coverage weak outside city centers and connection speeds in many areas barely exceeding a few kilobits per second. Institutional capacity for defensive cyber operations is equally degraded. Under the Assad regime, cybersecurity institutions were subordinated to regime security priorities, resulting in a narrow focus on protecting regime-linked assets. The transitional 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. The consequences of this degradation are severe and ongoing. In June 2025, Syria's Ministry of Information reported a coordinated cyberattack targeting government websites and social media accounts. While it is believed to have been orchestrated by remnants of the Assad regime, no specific perpetrators were identified. The Ministry attributed the vulnerabilities to weak software infrastructure and shortcomings in applying necessary security protections. With limited digital forensic capabilities, Syria remains unable to trace or attribute cyberattacks (Figure 3).

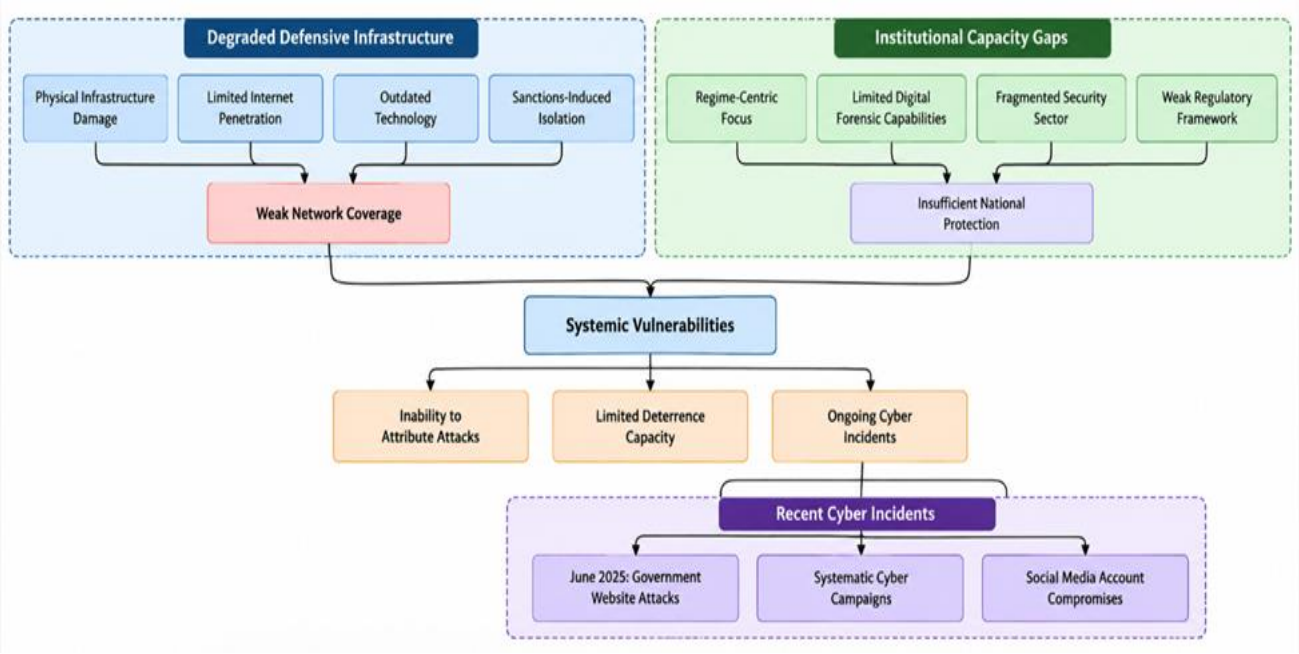


Figure 3: Degraded defensive infrastructure and recent cyber incidents

The cyber threat scenario facing Syria’s transitional government is complicated and persistent, with many types of actors with varied goals, capabilities, and operational patterns. A potential threat might stem from pro-government hacker organizations, including those linked to the former Assad regime and the Syrian Electronic Army (SEA), which exhibited offensive cyber skills during the Syrian civil war. If groups loyal to the former regime attack the transitional administration, attacks on government networks, essential infrastructure and digital services might impede restoration efforts and impair the reliability of emerging digital systems. Reporting has also connected some sections of these groups to areas outside of Syria, notably Russia,

which can complicate attribution, investigation, and coordinated responses. The second kind of cyber threat is actors associated with foreign states. ESET researchers have detected activity against Syrian government networks and linked some efforts to individuals with ties to China. StrongPity, also known as Promethium, has been active in cyber-espionage activities involving targets in Syria. Iranian-affiliated entities, including Group5, have also been linked to cyber operations that targeted individuals engaged with the Syrian opposition. Such initiatives illustrate how different geopolitical objectives might overlap with Syria's digital ecosystem at a time of institutional and infrastructure rebuilding.

Another complexity is the hacktivist side. Numerous cyberattacks have been attributed to Kurdish hacktivist organizations like Hezi Rash, while other actors like Predatory Sparrow have attacked digital resources affiliated with Syria. Disinformation and influence operations can also fuel instability by disseminating incorrect or manipulative information via digital means, beyond direct hacks. Individuals and businesses also face hazards from sophisticated cyber-espionage tools. ASO RAT is a custom-built Arabic-language Android remote-access trojan that has been observed in surveillance attacks against individuals with links to the Syrian conflict, including opposition Figures 1 and 2, journalists, NGO workers, and military personnel. The variety of these threats illustrates that the difficulty of cybersecurity in Syria extends beyond traditional network assaults to espionage, surveillance, disruption, hacktivism, manipulation of information, and attacks on individuals. Limited capacity to probe and attribute complex cyber incidents is another challenge. Limited digital-forensics capabilities can make it difficult to ascertain who carried out an attack, how they did so, what infrastructure was affected, and whether seemingly distinct occurrences are related. This attribution gap can weaken the government's ability to respond effectively, and can also hamper the development of evidence-based defensive measures and international collaboration (Figure 4).

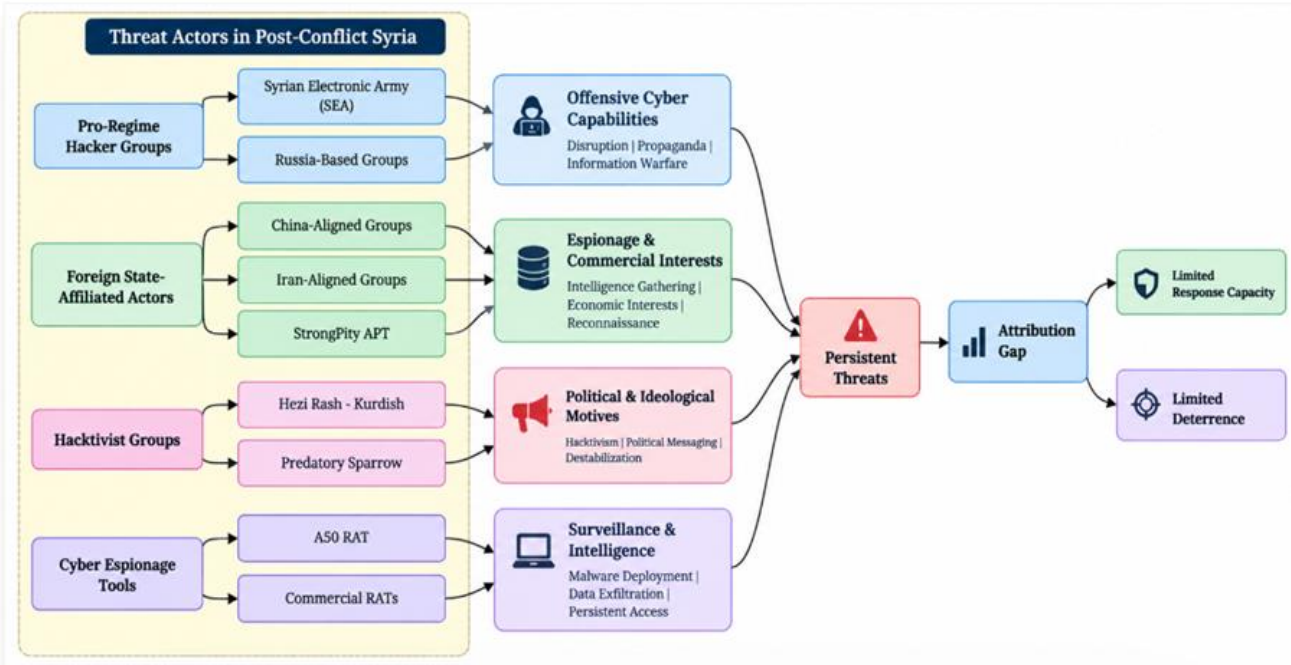


Figure 4: Threat actors in post-conflict Syria

The need for institutional consolidation and regulatory reform in an effort to build unified national cyber security capabilities." Regarding information security, Syria has made attempts to create more defined national structures, such as the establishment of the National Authority for Information Technology Services (NAITS) as the national body responsible for information security. In February 2026, the government withdrew the information-security accreditations of a number of local and regional companies, including XTECH LLC, Smart Systems Solutions and Talal Abu-Ghazaleh and Co., alleging their failure to meet the standards for information-security service providers. Such regulatory moves signal a drive to increase regulation of the cybersecurity industry and set clearer rules of compliance. "Researchers are also developing a National Cybersecurity Strategy. A draft strategy is under evaluation by the various government bodies and is expected to provide the legal and legislative framework for national cybersecurity, said Jihad Alala, Director of the Information Security Center. Directive No. 47 of the General Secretariat of the Presidency, released in December 2025, provides an additional regulatory framework for managing the activities of public organizations in the area of information security.

Collectively, these measures point toward a more formalized approach to national cybersecurity governance, but effective implementation, institutional coordination and enforcement will continue to be critical criteria. The Syria Cybersecurity Summit

2026 also shed light on the government's focus on establishing an integrated national cybersecurity system. The meeting, which gathered around 500 professionals, was dedicated to improving the protection of the national digital infrastructure. The government officials also said work continues on the operationalization of a Security Operations Center (SOC) and a Computer Emergency Response Team (CERT), as well as the establishment of a backup data center in Aleppo. These capabilities may enable ongoing surveillance, incident identification, coordinated response, and enhanced resistance to cyber incidents. The Ministry of Higher Education has been working with NAITS at the education level to improve cybersecurity education and to study the possibility of integrating cybersecurity into university curricula. The Ministry of Administrative Development also offered cybersecurity training in partnership with the King Salman Humanitarian Aid and Relief Center, with the participation of more than 30 personnel from various government agencies. Training was provided in account security, data security, network security, infrastructure security and application security, emphasizing the significance of building cybersecurity awareness and technical skills among public-sector staff (Figure 5).

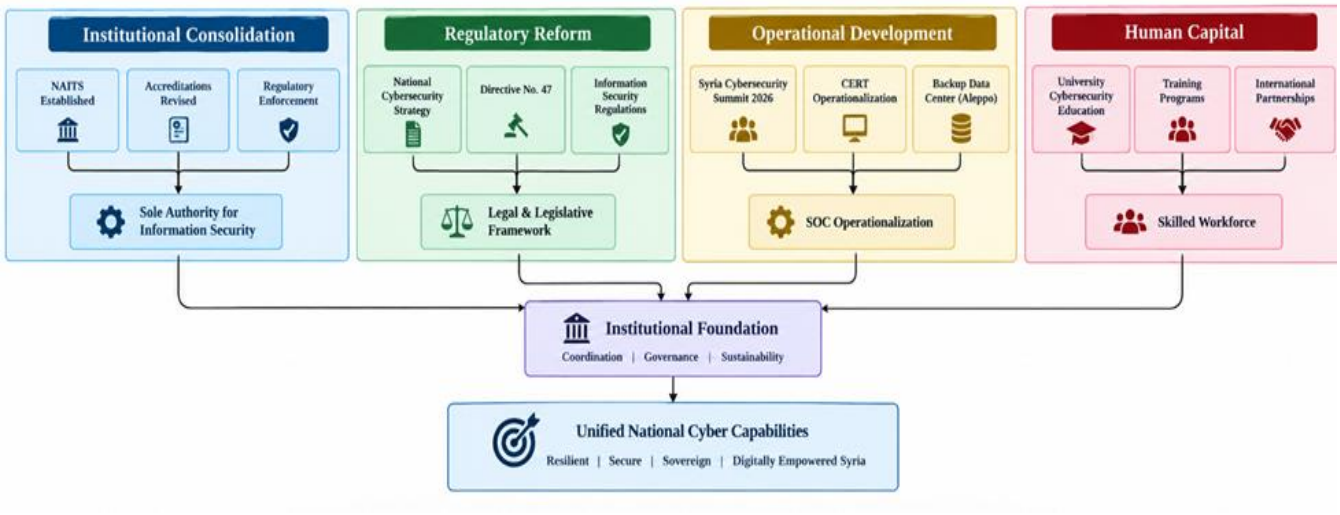


Figure 5: Institutional consolidation and regulatory reform

Strategic alliances and international cooperation provide further opportunity to develop Syria's cybersecurity capabilities. One notable development was the signing of a cooperation agreement between the Syrian government and the Saudi cybersecurity company Cipher in July 2025, which focused on rebuilding elements of Syria's cyber architecture and supporting the development of a national cyber institution and trained workforce. The agreement includes plans for a Tier III data center and a Security Operations Center, which could bolster national infrastructure resilience, data availability, monitoring and incident response capabilities.

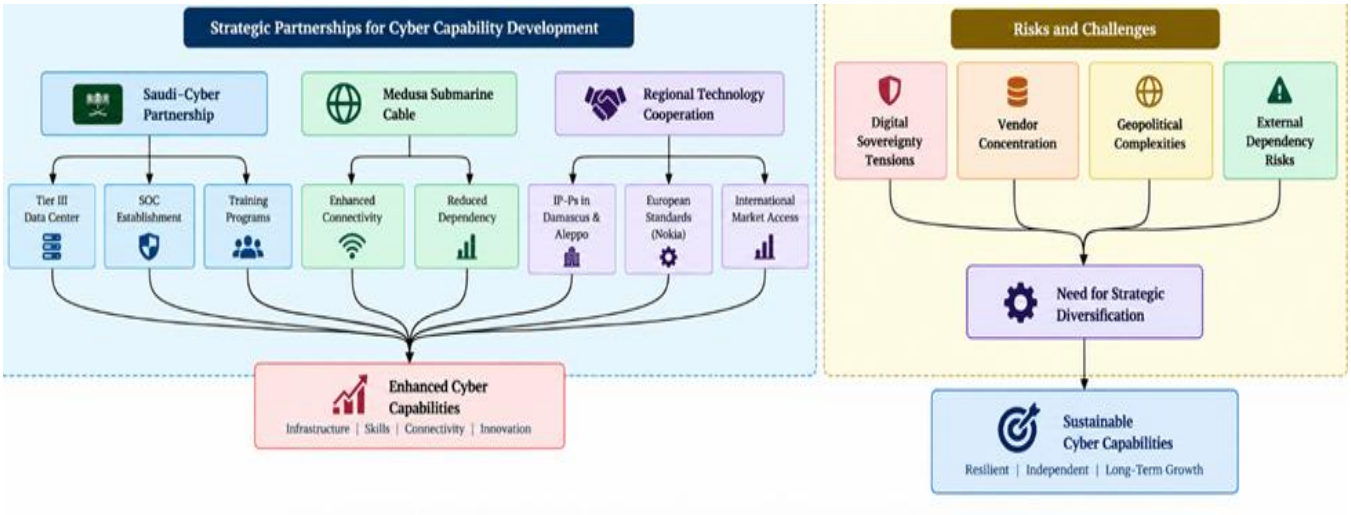


Figure 6: Strategic partnerships and associated risks

The memorandum of understanding with the Syrian Scientific Society for Informatics aims at improving technical capabilities through specialized training and knowledge transfer from Saudi professionals to Syrian staff. This knowledge transfer is vital, as long-term resilience for cybersecurity requires indigenous competence, not a perpetual reliance on external service providers (Figure 6). Connectivity infrastructure is also a key part of Syria's digital rebuilding. The development of the Medusa undersea cable in Tartus is a major investment in international communication and potentially minimizes reliance on terrestrial means. Better connectivity supports government digital services, business activity, cybersecurity operations, cloud services, research and international technology integration. There is also increasing regional technical cooperation, particularly with Saudi Arabia's Salam on international Internet Protocol points of presence in Damascus and Aleppo (Figure 7).

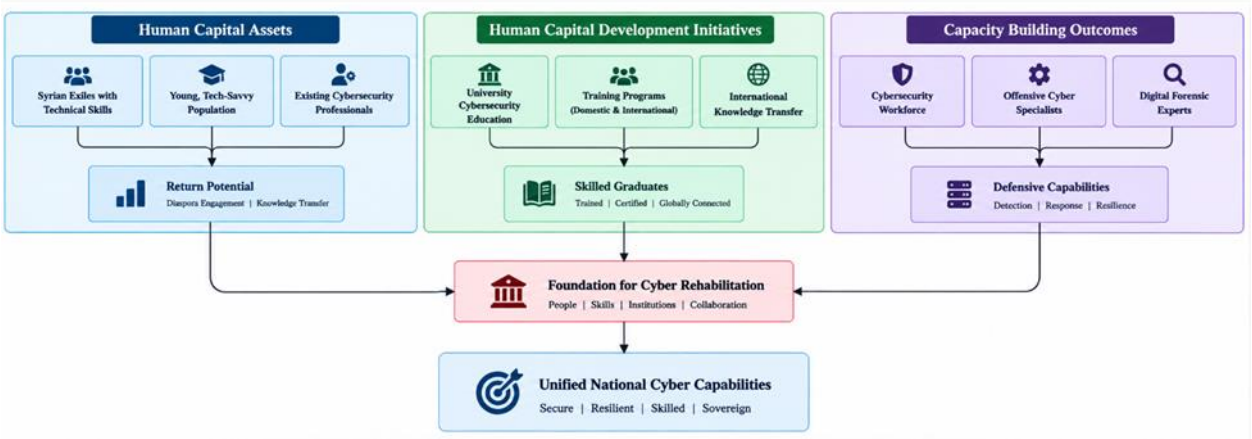


Figure 7: Human capital development for cyber capabilities

The return of Nokia to Syria is another potential conduit for the deployment of technology, supply of equipment, technical experience and adoption of internationally recognized techniques in telecommunications and cybersecurity. Syria's involvement in international technology events like GITEX Expand North Star with the slogan "Syria Is Online" also signals a growing interaction with worldwide technology networks and developing digital ecosystems. But these collaborations also entail possible dependency issues. An over-reliance on a small group of foreign technology suppliers, infrastructure operators or external technical partners could cause vulnerabilities relating to data governance, supply-chain security, technology lock-in, standards and digital sovereignty. Thus, international cooperation must be complemented by diversification, fair procurement, clear data-governance standards, security requirements and the development of home technical capabilities (Figure 8).

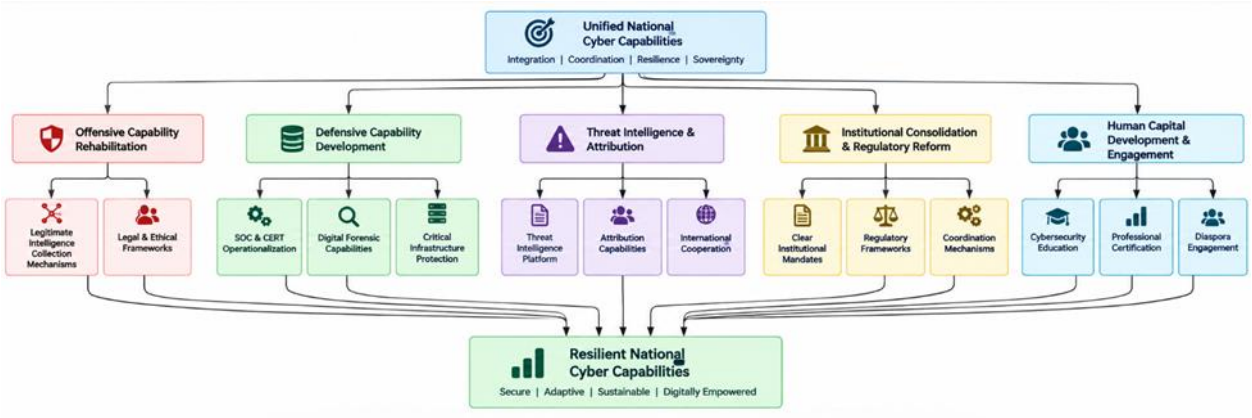


Figure 8: Unified national cyber capability framework

Rehabilitation of Syria's cybersecurity skills is highly dependent on the development of human capital. The conflict and relocation of around 13.5 million people have led to large losses of human capital and present major problems for education and skills development. Education disruption and the emigration of qualified professionals have limited the pool of competent technical personnel available to restore essential digital infrastructure. At the same time, the Syrian diaspora holds potential in terms of technical competence, professional networks, mentorship and institutional knowledge. Syrian professionals working in security, information technology, software engineering, telecommunications and related fields abroad could contribute to the

development of domestic capacity through temporary assignments, remote mentoring, academic collaboration, investment, training programs and eventual return. Therefore, university education should be enhanced through expanding cybersecurity courses, practical laboratory training, industry partnerships and internationally recognized educational and professional standards. In addition to university education, government training programs can provide practical skills to current public-sector employees, and specialized programs developed with international partners can address advanced areas such as security operations, digital forensics, incident response, threat intelligence, cloud security and critical-infrastructure protection. The establishment of a unified national cyber capacity involves a multidimensional framework that includes offensive capabilities, defensive capabilities, threat intelligence, institutional governance, and human capital. Offensive cyber capabilities should be separated from informal or politically motivated hacking activity and placed under legitimate state institutions with clear legal authority, oversight, accountability and appropriate ethical safeguards, when legally authorized and necessary for national security.

The development of defensive capabilities should focus on increasing the operations of SOC and CERT, strengthening incident response, protecting critical infrastructure, constructing secure government networks and establishing adequate backup and recovery systems. The capabilities of digital forensics should be improved to allow better investigation and attribution of cyber incidents, and methods for threat intelligence should allow the gathering, analysis and secure sharing of information on emerging threats. These capabilities can be developed with the support of international collaborations through intelligence-sharing arrangements, technical assistance, specialist training, and access to appropriate cybersecurity tools and standards. The governance basis for these technical skills should be regulatory reform and institutional consolidation. Clear mandates should be established for the authorities responsible for cybersecurity, telecommunications, digital services, critical infrastructure and incident response, with clear responsibilities and coordination procedures between institutions. In this regard, NAITS can be essential in promoting national information-security governance, standards, compliance and cooperation. Lastly, the national cybersecurity policy should emphasize human capital development and diaspora engagement. This should include university education, professional certification, government training, research programs, relationships with business and procedures for engaging Syrian technical workers abroad. A coordinated approach that includes institutional reform, defensive cybersecurity infrastructure, threat intelligence and forensic capabilities, responsible international partnerships, resilient digital infrastructure, and sustained investment in human capital can provide the foundation for the development of a more unified and sustainable national cybersecurity capability during Syria’s reconstruction.

5. Findings

The analysis yields several significant findings regarding the state and trajectory of Syria's cyber capability rehabilitation. The legacy of regime-centric offensive cyber capabilities represents a fundamental challenge. Under Bashar al-Assad, offensive cyber capabilities were developed and deployed as instruments of regime survival, embodied most prominently by the Syrian Electronic Army (SEA). The SEA demonstrated significant offensive cyber capabilities during the civil war, targeting major international media outlets and becoming one of the FBI's most wanted cyber groups. [186] The group remains active and continues to pose a threat to the transitional government. Defensive cyber capabilities are critically degraded. National cybersecurity capabilities remain insufficient to protect even the most basic systems. Under the Assad regime, cybersecurity focused narrowly on protecting regime-linked assets, leaving the wider national infrastructure exposed. The country's digital infrastructure has been neglected and damaged, with nationwide outages disrupting communications.

The threat landscape is characterized by unusual complexity and persistence. Syria faces threats from multiple categories of actors, including pro-regime hacker groups such as the SEA, foreign state-affiliated actors including China-aligned groups, Iranian-linked groups, and APT groups such as StrongPity, hacktivist groups, and sophisticated cyber espionage tools. With limited digital forensic capabilities, Syria remains unable to trace or attribute cyberattacks. Institutional consolidation is underway but incomplete. The establishment of NAITS as the sole entity responsible for information security, the revocation of accreditations, the drafting of a National Cybersecurity Strategy, and the issuance of Directive No. 47 represent significant institutional progress. However, much remains to be done to build effective coordination mechanisms and regulatory frameworks. Strategic partnerships offer significant opportunities but entail risks. The Saudi-Cypher partnership for a Tier III data center and SOC, the Medusa Submarine Cable System, and regional technology cooperation represent significant opportunities. However, the fragile balance between digital sovereignty and external dependency requires strategic diversification and risk mitigation. Human capital development is critical for sustainable cyber capabilities. The potential return of Syrian exiles with technical skills, university cybersecurity education, and training programs represents critical opportunities for building sustainable domestic cyber capabilities.

The analytical findings are concluded with a number of recommendations to policymakers, foreign partners and cybersecurity practitioners to enhance Syria’s national cyber capabilities. Syrian policymakers should first complete and enact a comprehensive National Cybersecurity Strategy that addresses both defensive and legally authorized offensive capabilities and covers the full spectrum of cyber operations, including threat intelligence, attribution, incident response and national cyber

resilience. Where offensive cyber capabilities are deemed necessary for national security, they should be placed under legitimate national command structures with clear legal, ethical and accountability frameworks, thus addressing the legacy of informal or politically affiliated cyber groups such as the Syrian Electronic Army. Simultaneously, it is imperative to emphasize the building up of defensive capabilities through operationalization of Security Operations Centers (SOCs) and Computer Emergency Response Teams (CERTs), development of digital-forensic capabilities, protection of critical infrastructure and continued development of resilient facilities such as Tier III data centers.

Syria should also strengthen its threat intelligence and attribution capabilities by investing in digital forensics, systematic threat collection and analysis, incident investigation, and international cooperation mechanisms that can help to identify the sources and characteristics of cyberattacks. The consolidation of institutions should be accelerated by strengthening the National Authority for Information Technology Services (NAITS) as a lead cybersecurity institution, establishing effective coordination mechanisms among government entities and enforcing regulatory compliance with the help of clearly defined cybersecurity standards, accreditation processes and certification requirements. Cybersecurity education at universities and professional institutions, specialized training programs, internationally recognized certification pathways and platforms for engaging Syrian professionals in the diaspora should continue to be a key goal to create human capital. The prospective return of Syrian cybersecurity and technology experts abroad, or their short-term involvement, might bring invaluable skills, mentoring, professional networks, and knowledge transfer.

Syria should also strive for strategic diversification, avoiding over-reliance on one technology source, infrastructure supplier or international partner. Diversifying vendors and international alliances, while building up domestic cybersecurity capabilities incrementally, can help mitigate foreign dependence and bolster long-term technological resilience. When considering Syria's cybersecurity reconstruction, international partners may help by providing suitable access to cutting-edge technology, security software, technical experience and capacity-building resources, while taking into account applicable legal and regulatory constraints. Where sanctions or technology limitations pose challenges to legitimate civilian cybersecurity capacity-building, foreign partners can support authorized methods to ensure access to required technologies and security services. Technical aid should be directed at training Syrian professionals, transferring necessary knowledge, developing cybersecurity curriculum, establishing and expanding SOC and CERT capabilities, boosting digital-forensic skills, and supporting secure critical infrastructure. International partners may also help promote Syria's involvement in regional and global threat-intelligence sharing agreements that would allow for the exchange of information about new threats, malicious infrastructure, attack strategies, and defensive measures.

Such cooperation can enhance attribution capabilities and improve coordination of responses to major cyber attacks. International assistance should also help with institutional development by providing experience on cybersecurity legislation, regulatory structures, technological standards, accreditation systems and organizational governance. At the same time, international partners should recognize Syria's legitimate interest in digital sovereignty and appropriate data governance, supporting capacity building that enables Syrian institutions to secure and manage their own digital infrastructure while maintaining constructive international cooperation. Long-term relationships should therefore be about knowledge transfer, domestic capability development, transparency and sustained institutional strengthening rather than generating permanent technical dependency. Such policy and international measures must be matched by thorough assessments of Syria's current cyber capabilities by cybersecurity practitioners. Such assessments should comprise a systematic review of defensive infrastructure, threat intelligence capability, digital forensic capacity, incident response methods, organizational readiness, critical infrastructure protection and other relevant areas.

Practitioners should develop standardized incident-reporting procedures, define response protocols, improve forensic processes and strengthen coordination among government institutions and other authorized organizations to build stronger incident detection, response, investigation and attribution capabilities. Basic cybersecurity hygiene should also be an immediate priority, as fundamental vulnerabilities like password reuse, lack of multi-factor authentication, over-privileged access, outdated systems, and insufficient controls over access can dramatically increase exposure to common cyberattacks. However, well-implemented strong authentication, least-privilege access, regular security upgrades, safe backups, network segmentation, and systematic vulnerability management can make considerable advances in overall cyber resilience. Building threat-intelligence capabilities requires a systematic approach to gather, analyze, and share information on cyber risks, indicators of compromise, attack methodologies, vulnerabilities, and malicious infrastructure. Working with well-regarded international threat intelligence bodies and entering into suitable information-sharing agreements may strengthen the capacity of Syrian institutions to detect new risks and act early, before incidents cause large-scale damage. Lastly, a broader cybersecurity culture must be cultivated in government institutions, corporate enterprises, educational institutions and civil society. Regular awareness programs, professional training, secure-technology practices, incident-reporting instruction, and public awareness campaigns can guarantee that cybersecurity is an organizational and societal obligation rather than a technical function. These measures can be integrated in a combination of institutional reform, defensive infrastructure, threat intelligence, human-capital development,

responsible international cooperation and practical cybersecurity practices to develop a more coordinated, resilient and sustainable cyber ecosystem in Syria.

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 cyber capabilities, but the challenges are equally unprecedented. The new administration must rehabilitate offensive cyber capabilities that serve national rather than regime interests while building defensive capabilities that can protect the entire digital ecosystem. It must contend with a persistent and multifaceted threat landscape while managing the legacies of both pro- and anti-regime hacker networks. The analysis presented in this paper has identified five principal categories of challenges: the fragmented legacy of offensive cyber assets, the degraded state of defensive infrastructure, the persistence of multifaceted external threats, the imperative of institutional consolidation and regulatory reform, and the geopolitical complexities of strategic partnership formation. These challenges are interconnected and mutually reinforcing, creating systemic vulnerabilities that require comprehensive solutions. Yet the analysis has also identified significant opportunities. Strategic partnerships with regional cybersecurity providers, the drafting of a National Cybersecurity Strategy, institutional development including SOC and CERT operationalization, and the potential return of Syrian exiles with technical skills collectively create a more enabling environment for cyber capability rehabilitation. The stakes could not be higher.

Neglecting cyber capabilities 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 cyber capability rehabilitation 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 cyber practices to a unified national framework. It shows that international partnerships, institutional development, and human capital investment are essential for building sustainable cyber capabilities in fragile contexts. For Syria, the path forward requires sustained commitment from policymakers, international partners, and cybersecurity practitioners. It requires investment in offensive and defensive capabilities, institutional capacity, regulatory frameworks, technical infrastructure, and human capital. And it requires a vision of cyber power 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 unified national cyber capabilities that serve as a foundation for a resilient, democratic, and prosperous digital future.

Acknowledgment: The authors sincerely acknowledge Al-Shahbaa Private University, Girne American University, University of Galway, Singapore Management University, Jingwei Software Co., Taihu Advanced Materials, and University of Kufa for their valuable academic support, research resources, and institutional collaboration.

Data Availability Statement: The authors confirm that the data supporting this study can be obtained from the corresponding author upon reasonable request.

Funding Statement: The authors declare that no external funding or financial assistance was received for conducting this research or preparing the manuscript.

Conflicts of Interest Statement: The authors declare that they have no competing interests or conflicts of interest related to this research or its publication.

Ethics and Consent Statement: The authors confirm that the study followed established ethical guidelines, with informed consent obtained from all participants.

References

1. Access Now, “Reclaiming Syria's Digital Future,” *Access Now*, 2025. [Accessed by 02/01/2026].
2. N. Aljizawi, “Syria's recovery depends on rebuilding its digital infrastructure,” *Tech Policy Press*, 2025. [Accessed by 05/01/2026].
3. R. Tudorica, C. Vatamanu, and A. Maximciuc, “StrongPity APT – Revealing Trojanized Tools, Working Hours and Infrastructure,” *Bitdefender White Paper*, 2025. [Accessed by 07/01/2026].

4. B. Buzan, O. Wæver, and J. de Wilde, "Security: A New Framework for Analysis," *Lynne Rienner Publishers*, Boulder, Colorado, United States of America, 1998.
5. Carnegie Endowment for International Peace, "New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms," *carnegieendowment*, 2023. [Accessed by 10/07/2025].
6. D. Sadeh, "Hezi Rash: Rising Kurdish Hacktivist Group Targets Global Sites," *Check Point Research*, 2025. [Accessed by 11/01/2026].
7. S. N. Salivio, "ESET links China-aligned hacks to oil, Syria & tech," *SecurityBrief Asia*, 2026. [Accessed by 12/01/2026].
8. 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.
9. International Telecommunication Union, "Global Cybersecurity Index 2024," 5th ed, *ITUPublications*, Geneva, Switzerland, 2024.
10. 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.
11. H. J. Morgenthau, "Politics Among Nations: The Struggle for Power and Peace," *Knopf*, New York, United States of America, 1948.
12. J. S. Nye, "The Future of Power," *PublicAffairs*, New York, United States of America, 2011.
13. M. Ourahli, "Post-Conflict Challenges for Syria's Reconstruction of Cyber Power," *S. Rajaratnam School of International Studies*, Singapore, 2025.
14. Syrian Arab News Agency (SANA), "Syria enhances cybersecurity infrastructure after detecting website vulnerabilities," *SANA*, 2025. [Accessed by 13/01/2026].
15. Syrian Arab News Agency (SANA), "Information Ministry: Coordinated electronic reporting campaign targets official government pages," *SANA*, 2025. [Accessed by 15/01/2026].
16. Dimasheq, "Syria Cybersecurity Summit 2026 Kicks Off with More Than 500 Experts Participating," *Dimasheq*, 2026. [Accessed by 17/01/2026].
17. Syrian Arab News Agency (SANA), "Administrative Development, KSRelief organize a training course in cybersecurity," *SANA*, 2026. [Accessed by 19/01/2026].
18. ITU-D Cybersecurity, "National Cybersecurity Strategies Repository," *ITU*, 2025. [Accessed by 20/01/2026].
19. L. Harding and C. Arthur, "Syrian Electronic Army: Assad's cyber warriors," *The Guardian*, 2013. [Accessed by 20/07/2025].
20. United Nations Development Programme (UNDP), "The Impact of the Conflict in Syria: A Preliminary Socio-Economic Impact Assessment," 2025. [Accessed by 21/01/2026].
21. K. N. Waltz, "Theory of International Politics," *Addison-Wesley*, Massachusetts, United States of America, 1979.
22. D. Makki, "The hack that exposed Syria's sweeping security failures," *Wired*, 2026. [Accessed by 22/07/2026].
23. World Bank, "Syria Economic Monitor, Spring 2024: Conflict, Crises, and the Collapse of Household Welfare," *World Bank*, 2024. [Accessed by 23/07/2025].
24. C. Arslan, "Syria's contested digital sovereignty: Technology agreements and techno-political rivalry in Syria's reconstruction 2024–2025," in *Post-Conflict Rebuilding in Syria Symposium*, Istanbul, Turkey, 2025.
25. Alikhbariah, "Syrian-Saudi partnership to build a global data center and advanced cybersecurity," *Alikhbariah*, 2026. [Accessed by 25/01/2026].

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.*