IDSS PAPER

8 December 2025

Post-Conflict Challenges for Syria's Reconstruction of Cyber Power

Marine Ourahli

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Ponder the Improbable since 1996

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore
Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg No.114– 8 December 2025

The authors' views are their own and do not represent the official position of the Institute of Defence and Strategic Studies of the S. Rajaratnam School of International Studies, NTU. These commentaries may be reproduced with prior permission from RSIS and due recognition to the authors and RSIS. Please email to Editor IDSS Paper at RSISPublications@ntu.edu.sg.

Post-Conflict Challenges for Syria's Reconstruction of Cyber Power

Marine Ourahli

KEY TAKEAWAYS

- Rebuilding Syria's cyber ecosystem is essential for the country's stability under its new transitional government.
- The legacy of the civil war represents a significant challenge for the transitional government. It must redefine its alliances to protect itself from potential cyber threats originating from the Assad regime and its supporters.

COMMENTARY

Following the fall of the Assad regime and the rise of Ahmed al-Sharaa's transitional government, Syria's cyber future is once again at a critical juncture. The new administration must rebuild national cyber capabilities while managing the legacies of both pro- and anti-regime hacker networks.

In a country that is physically in ruins, cyberspace may appear secondary. However, 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.

From Rebelling to Governing: Rebuilding the Syrian State

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. National cybersecurity capabilities

remain insufficient to protect even the most basic systems. Under former leader Bashar al-Assad, cybersecurity focused narrowly on protecting regime-linked assets, leaving the wider national infrastructure exposed.

Gaining legitimacy is crucial for al-Sharaa's regime to secure international cooperation and assistance, as well as to convince Syrian exiles to return to their country. The potential return of Syrian exiles with technical skills would enable the government to address vulnerabilities in the country's critical digital infrastructure.

The collapse of the Assad regime has also left Syria without a unified national army and with adversaries within and at its borders to contend with. The military is currently a patchwork of loosely coordinated militias and remnants of al-Sharaa's Hay'at Tahrir al-Sham militant group.

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. The Syrian Electronic Army (SEA), a hacker group allied with the Assad government since 2011, forms a part of this ongoing threat. During the civil war, it demonstrated significant offensive cyber capabilities, targeting "X" (formerly Twitter) and *The New York Times*, and quickly became one of the FBI's most wanted cyber groups. Should hacker groups loyal to Assad decide to attack the interim government, they could cause enormous damage and deeply disrupt the digital and physical reconstruction of Syria.

Building Alliances and Infrastructure

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. This was not the first such incident of critical digital infrastructure being sabotaged: nationwide outages had previously disrupted communications after fibre-optic lines were cut across the country.

With limited digital forensic capabilities, Syria remains unable to trace or attribute cyberattacks. Given the growing importance of cyber operations as a key instrument of warfare, this gap undermines both Syria's defensive posture and its credibility as a sovereign digital actor.

To address these vulnerabilities, the government signed a strategic cooperation agreement in July 2025 with the Saudi cybersecurity firm Cypher. This partnership aims to rebuild Syria's cyber architecture and establish a national cyber institution capable of training a new workforce. In parallel, Saudi telecommunications companies have signed investment agreements with the Syrian government for a total of nearly US$1 billion to support the development of Syria's digital infrastructure and cybersecurity capabilities.

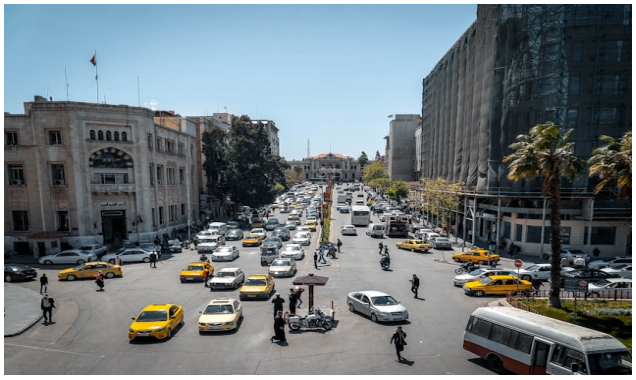
Domestically, the transitional government must address the presence of hacker groups whose agendas remain unclear. Hacker groups known for their opposition to Assad, such as the Supreme Council of the Revolution (SCR), the Free Syrian Army (FSA) and the Hackers of the Syrian Revolution (HSR), could be integrated into Syria's

cyber apparatus to protect against potential attacks and participate in the creation of a cyber arm of the national military. To achieve this, President al-Sharaa will have to convince them of his willingness to break with the Assad dictatorial regime and find ways to accommodate their requirements for aligning with the government.

Conversely, the fate of the pro-Assad SEA also remains uncertain. The SEA's advanced expertise could be both an asset and a challenge for the new government: could it be incorporated into a new cyber defence framework, or will it remain a potential threat aligned with the old regime? With Assad having fled the country, it is also conceivable that the organisation will evolve, splinter or even vanish entirely.

The question of the future of Assad's former supporters is not limited to the cyber realm. Some of Assad's collaborators have already joined al-Sharaa's government, and it would not be unrealistic to see a similar merger happening in the cyber realm as well. However, this naturally raises issues around legitimacy and trustworthiness. The SEA's stance on the new regime and their involvement in the March 2025 cyberattack are still unknown.

Rebuilding systems will not be enough; Syria would need to rebuild strategic alliances as well. To achieve this objective, the government is establishing a regional intelligence and cybersecurity network with Egypt, Turkey, Jordan and Iraq. Beyond enhancing cyber defences against Israel, this initiative aims to anchor Syria's position in the regional balance of power.



Rebuilding Syria's cyber ecosystem, as well as securing international cooperation and assistance, is crucial for the country's recovery. *Image source: Unsplash.*

This dynamic is part of a broader shift in geopolitical alignments. As Damascus redefines its position, its initial moves suggest that it has begun to turn towards Western and Arab partners, particularly the United States, Turkey, Saudi Arabia, Jordan and Qatar. In recent months, Damascus has shown signs of strategic realignment by distancing itself from Iran, whose influence and support were crucial for the previous regime, particularly in the cyber sphere.

Beyond this repositioning, Syrian Minister of Communications and Information Technology Abdulsalam Haykal has revealed his ambition to turn Syria into a "digital Silk Road". This begins with the installation of the country's first submarine cable, the Medusa Submarine Cable system, deployed in Tartus. It connects Syria to a larger network stretching across the Mediterranean and linking Europe, Asia and North

Africa, with the aim of strengthening data exchange, increasing bandwidth and promoting regional digital integration. This project aims not only to rebuild infrastructure, but also to establish Syria as a future regional cyber power.

Marine Ourahli *is a Senior Analyst with the Military Transformations Programme at the S. Rajaratnam School of International Studies (RSIS).*

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.