IDR
Romanian Diplomatic Institute

Ministerul Afacerilor Externe

POLICY BRIEF no. 88/2026

The role of cyber operations in the conflict between Israel-U.S. and Iran

Claudiu Codreanu

The role of cyber operations in the conflict between Israel-U.S. and Iran[1]

Claudiu Codreanu[2]

Analyst, Romanian Diplomatic Institute

Policy Brief Series no. 88 / 2026

Published by: Romanian Diplomatic Institute

ISSN: 2066-5989

Abstract

The Israeli-American attacks against Iran on 28 February triggered a wider war, with a serious risk of escalation from Tehran after several Iranian officials were assassinated in the bombings, including Ayatollah Ali Khamenei. In the case of cyber operations, they have not stood out so far, appearing to have been used primarily in support of kinetic military operations. Neither side has launched destructive cyberattacks or operations with a significant impact. However, there is a strong possibility that certain cyber operations are still in preparation, may have been repelled, or have simply not yet been disclosed (at least for the period followed by this brief, February 28 – March 6). As such, cyber operations appear, at least for the moment, to play a supporting role, similar to the role they played during the U.S. intervention in Venezuela in January 2026. At the time of writing, the United States has revealed that it carried out cyberattacks against the Iranian military's communications systems in order to prepare the bombing campaign. However, other potential targets within critical infrastructure have not been disclosed by either side. Nevertheless, in the coming period there will likely remain a possibility of Iranian cyber operations targeting critical sectors such as energy or water supply, given Tehran-linked hackers' previous track record of targeting these sectors in earlier cyber intrusions.

Keywords: cyber operations, Iran, Israel, United States, conflict.

[1] This publication draws exclusively on open-source materials. The opinions expressed herein are solely those of the author and do not necessarily reflect those of the institution.

[2] claudiu.codreanu@idr.ro

INTRODUCTION

The Israeli-American attacks on Iran on February 28 triggered a broader war, with a serious risk of escalation from Tehran after several Iranian officials were assassinated in the bombings, including Ayatollah Leader Ali Khamenei. The intelligence operations conducted by Israel and the U.S. were so complex that they successfully located three meetings of the Iranian regime's political and military leaders (Lieber, Ward & Norman 2026). Multiple high officials were killed during the initial bombings (launched surprisingly during daylight): Supreme Leader Ali Khamenei, Defence Minister Amir Nasirzadeh, Khamenei's security advisor Ali Shamkhani, and Islamic Revolutionary Guard Corps (IRGC) commander Mohammad Pakpour, among others.

In retaliation, **Iran** bombed **Israel** as well as **Gulf Arab** states hosting **U.S. bases**, causing damage to civilian targets as well. Israel launched operations against **Hizbollah** in **Lebanon** while also imposing new restrictions on **Gaza** crossings, including humanitarian aid. To date, over a thousand people have died in Iran (including at a school in the country's south), with hundreds of deaths reported in Lebanon, Israel, and other states in the region, as well as six U.S. military personnel who lost their lives.

The conflict between Israel-U.S. and Iran is ongoing, and scenarios regarding its potential resolution remain uncertain, as do post-conflict scenarios concerning the likelihood of the Iranian opposition successfully challenging the repressive regime. Regarding **cyber operations**, they have not stood out so far and appear to have been primarily used in support of kinetic military operations (the brief follows the developments from the first week of the war). **Neither side has launched destructive cyberattacks or operations with a high or large-scale impact**, though there is a strong likelihood that certain cyber operations are still in preparation, may have been countered, or have not yet been disclosed.

BACKGROUND

Over the past ten years, Iran has enhanced its offensive military cyber capabilities, ranging from espionage campaigns and influence operations, to cyberattacks. Iran's primary

targets are in the Middle East, especially Israel and Saudi Arabia, as well as the United States and Euro-Atlantic allies. The main institutions responsible for Iran's offensive cyber operations are the IRGC and the Ministry of Intelligence, which also employ various "activist" hacker groups to obscure direct attribution to Tehran (Lim 2026).

In recent years, Iran has deployed a wide spectrum of cyber operations, from espionage against civilian and military targets in Israel, U.S., or the Middle East, to coordinated disinformation campaigns, ransomware attacks, which lock affected systems by encrypting data, and cyberattacks involving wipers, which permanently delete data from targeted systems (SentinelOne 2026). Notable Iranian cyber operations include the 2012 attack on the Saudi company **Saudi Aramco** (Shamoon), influence operations targeting the **U.S. presidential elections** in 2020 and 2024, and cyberattacks on **Albania** in retaliation for hosting an Iranian opposition group (Ross et al. 2026; Greenberg 2024).

Donald Trump's campaign team announced in the summer of 2024 that it had been targeted by an Iranian cyber intrusion, later confirmed by both Google and U.S. authorities (Greenberg 2024). In August 2024, Google published a report on the involvement of APT 42 – a hacker group coordinated by the IRGC – in a cyber operation targeting Donald Trump's and the Democratic Party's campaigns (Greenberg 2024). The same group had also targeted Trump's and Joe Biden's campaigns during the 2020 presidential elections. The main U.S. cybersecurity agencies – FBI (Federal Bureau of Investigation), CISA (Cybersecurity and Infrastructure Security Agency), and ODNI (Office of the Director of National Intelligence) – **attributed these cyber operations to Iran**, but the campaign had a very limited impact (Greig 2024a)

There is also a clear example of using cyber operations as a primary weapon in the broader Israel/U.S. and Iran conflict. **Between 2009 and 2010, the United States, and most likely Israel, conducted a destructive cyberattack against Iran**, successfully disrupting the Iranian nuclear program by damaging centrifuges at the Natanz uranium enrichment facility – now a major target in the 2025 and 2026 bombing campaigns (Shotter & Ghaffari 2026). However, the 2009-2010 action can be most accurately described as an act of **sabotage** rather than an effort to unleash a war with Tehran. Moreover, its impact was not decisive and did not full disrupt the Iranian nuclear program or affect the regime overall.

The role of cyber operations in the Twelve-Day War

Major Iranian cyber operations during the Twelve-Day War between Israel-U.S. and Iran (June 13-24, 2025) either have not yet been disclosed or did not occur. **In June 2025, U.S. authorities warned that Iran might target transportation or water supply systems in the United States**, given that these sectors had previously been the focus of past Iranian cyber intrusions in the country (Miller 2025). However, no incidents occurred. Iran did conduct **influence operations**, including disinformation campaigns designed to create confusion or panic, as well as DDoS attacks (Distributed Denial of Service) that disrupted or took offline websites or platforms (Baram & Peer 2025). **In the first days following the bombings, cyberattacks against Israeli entities increased by 700%** (Baram & Peer 2025).

On the other side, two notable cyber operations took place. **Predatory Sparrow, a hacker group affiliated with the Israeli government, launched two cyberattacks against Iran during that period**. Bank Sepah, an Iranian bank linked to the Revolutionary Guards, had its services paralysed, while Nobitex, Iran's largest cryptocurrency exchange, suffered the exfiltration and destruction of crypto assets exceeding $90 million (Atlantic Council 2025; Baram & Peer 2025). In this context, **Iran imposed a near-total internet shutdown** to protect its financial system and other critical sectors from additional cyberattacks that could have caused substantial losses (Baram & Peer 2025; Burgess 2025). Additional objectives for the internet shutdown included **preventing potential anti-regime demonstrations** and **disrupting potential U.S. and Israeli intelligence** and communications activities, particularly those related to missile targeting.

Digital repression and disinformation campaigns

Iran is one of the leading global abusers of country-wide internet shutdowns as a means of suppressing anti-government protests. **Tehran has restricted internet access during multiple events in recent years**, including the 2022-2023 protests following the death of Mahsa Amini while in the custody of the "morality police" (Burgess 2025). Moreover, **during the 2026 anti-regime protests, Iranian authorities completely cut internet access for nearly two months** (Newman & Burgess 2026). This measure, part of broader policies of

digital authoritarianism, aimed both to disrupt protesters' coordination and to prevent footage of massacres by security forces from reaching the global internet. As internet restrictions were gradually lifted, authorities intensified mass surveillance of the population (Newman & Burgess 2026).

Another notable aspect of the anti-regime protests and the ongoing Israel-U.S. war is a coordinated influence campaign targeting the Iranian population, beginning in 2025. Citizen Lab revealed in the fall of last year the details of an **influence operation aimed at toppling the Iranian regime** (Fittarelli et al. 2025). According to the analysis, the coordinated disinformation campaigns spreaded narratives encouraging revolt against the regime and support for Reza Pahlavi, heir of Iran's last Shah and a key opposition figure. Researchers assessed that **the operation was likely conducted or supported by the Israeli government**, as it was also synchronized with the June 2025 bombings.

RECENT DEVELOPMENTS IN THE CURRENT CONFLICT: ANALYSIS

On March 2, General Dan Caine, Chief of the U.S. Joint Chiefs of Staff, stated that U.S. **Cyber Command had conducted cyber operations against Iranian communications to prepare the bombing campaign**, describing the actions as "non-kinetic effects" supporting military operations (Matishak 2026). American media reported that cyberattacks targeted Iranian missile systems to assist the bombing campaign against nuclear facilities during the June 2025 war as well (Matishak 2026). In January 2026, President Donald Trump and General Caine suggested that the U.S. had used cyberattacks to attempt power outages in Caracas and to disrupt air defence radars and communications during the operation to capture Venezuelan President Nicolas Maduro (Matishak 2026).

Beyond cyberattacks coordinated with kinetic operations, no major incidents occurred **One of the most visible cyberattacks targeted Iran on February 28, immediately after the first missile strikes**. The prayer app *BadeSaba Calendar*, with over five million downloads, was infiltrated to send messages supporting the bombings and promising amnesty to those who surrender – "help is here" (Kumar 2026). However, the impact of this operation and the proportion of Iranian residents who received the message remain unclear. Thus, **the most significant cyber action was not launching attacks, but cyber espionage**, which was crucial for preparing the bombing campaign, both for targeting buildings, and for assassinating Iranian

officials (Shotter & Ghaffari 2026). On the Iranian side, although no significant intrusions have been recorded to date, **several "activist" hacker groups affiliated with the Iranian government have announced plans to launch a series of cyber operations against Israel and other regional targets** (Insikt Group 2026).

The potential decisive role of cyber operations in periods of war has been questioned in recent years. **Extensive studies of the Russian war in Ukraine show that cyber operations did not play a substantial strategic role, having limited impact for both sides,** despite several significant cyberattacks on Ukraine's critical infrastructure prior to the full-scale invasion (Mueller et al. 2023; Maschmeyer & Dunn Cavelty 2023).

Moreover, Lennar Maschmeyer argued in 2021 that **the use of cyber operations faces an operational trilemma**: attacks cannot simultaneously be executed quickly, have a strong impact, and remain controllable and accurate (Maschmeyer 2021). The Israeli-American attacks on Iran in 2026 are effectively a continuation of those in June 2025 – a timeframe sufficient to exploit previously identified vulnerabilities in Iranian networks. However, Iran's cyber defences appear to pose a hurdle, as does the fact that missile and drone strikes are much faster and have a far greater impact during war. Similarly, Iran, at least to date, appears not to have developed the capabilities necessary to rapidly launch powerful cyberattacks against the United States, Israel, or Gulf allies – though this remains to be seen in the coming weeks, particularly regarding Saudi Arabia and the Gulf states.

Thus, **cyber operations are primarily used to support kinetic actions**, mainly by disrupting Iranian military communications before or during bombing campaigns, as well as leveraging prior cyber espionage campaigns to pinpoint government or military buildings, or even political and military leaders. Other objectives may include targeting the financial sector and other critical infrastructure to disrupt the regime, as well as using cyber-infiltrated channels to deploy information campaigns (e.g., mobile apps, social media, TV stations). Conversely, Iranian **cyber operations have either failed, are ongoing, or have yet to be disclosed** – indicated that, in any case, their impact has been limited or conducted on a small scale.

CONCLUSIONS AND RECOMMENDATIONS

On February 28, the U.S.-based cybersecurity firm SentinelOne warned that **Iranian cyber operations were likely to intensify in the short term**, considering Tehran's past usage

of such operations as a form of retaliation. However, there are no major risks regarding Iranian cyber threats to Euro-Atlantic states. For example, on March 2, the United Kingdom's National Cyber Security Centre (NCSC) issued a statement indicating that, **most likely, there were no significant changes in Iranian cyber threats to the UK**. Nevertheless, the NCSC noted that Iran and Tehran-linked groups retain the capability to launch cyber operations, with "near certainty" of a **high risk of indirect cyber threats to organisations with a presence in the Middle East**.

It is **likely that cyber operations will continue to play only a supporting role for all parties in this conflict**. Iran will also continue to impose near-total **internet shutdowns** throughout the war and in the event of post-war anti-regime protests. **Romania and other European states are unlikely to become direct targets of Iranian cyber operations, but they could become indirect targets of opportunistic attacks aimed at a broad range of entities**, although the likelihood of unprecedented or high-impact attacks is low. There is a **low risk of high-impact, large-scale, or unprecedented cyber operations**, but a higher risk of opportunistic **ransomware** attacks, **wiper** attacks, and **cyber espionage** campaigns.

Attention should also remain focused on the Palestinian territories, particularly given the deteriorating **humanitarian situation** following Israel's restrictions on multiple crossings – there is a risk of **long-term restrictions on internet or telecommunications access**, similar to those implemented in Gaza during the Twelve-Day War (Reuters 2025; Graham-Harrison & Tantesh 2026).

Even though the war is ongoing the and cyber threats may evolve, several key **recommendations** can be made:

- Strengthen cybersecurity and network monitoring in the **energy and water supply sectors**, given the past targeting of these infrastructures by Iranian state-affiliated hackers.
- Prepare defences against **intrusive or high-impact cyber operations** that Iran could launch in the near future.
- Take measures to prevent Iranian **ransomware campaigns across all critical sectors**.

- **Prevent disinformation campaigns** and hack-and-leak operations, where stolen information is published online (oftentimes altered to fit a certain narrative).

Thus, **cyber operations currently appear to have a supporting role** rather than a decisive one – similar to the U.S. intervention in Venezuela in January 2026. However, this does not rule out the possibility of a large-scale cyberattack or a targeted, high-impact operation (e.g., power outages, disruption of hospital operations etc.). This analysis is based solely on information available to date and on current developments, following the period between February 28 and March 6, 2026. The trajectory of the war remains uncertain, as does the resilience of the current Iranian regime, and it is unclear whether additional Euro-Atlantic countries will become involved (either through drone or missile attacks on U.S. bases or by joining defensive efforts against Iranian retaliation).

Finally, **the eventual end of the current war should not be considered the end of all hostilities**, as cyber operations may be prepared for the post-bombing period. This is why AccessNow calls for the implementation of a **digital ceasefire** in all conflicts, given that cyber operations and digital repression continue even after kinetic actions cease (Coppi & Fatafta 2024). For instance, Iranian cyberattacks continued even after the kinetic operations ended after 12 days in June 2025, with government-affiliated groups attempting to exploit a Microsoft vulnerability to target servers of Israeli companies (Shotter & Ghaffari 2026).

BIBLIOGRAPHY

Baram, G., & Peer, N. (2025, July 18). How Israel and Iran brought cyber conflict to centre stage. *BindingHook*. https://bindinghook.com/how-israel-and-iran-brought-cyber-conflict-to-centre-stage/

Burgess, M. (2025, June 18). Iran's Internet Blackout Adds New Dangers for Civilians Amid Israeli Bombings. *Wired*. https://www.wired.com/story/iran-internet-shutdown-israel/

Coppi, G., & Fatafta, M. (2024, November 20). Toward a digital ceasefire. *Access Now*. https://www.accessnow.org/toward-a-digital-ceasefire/

Fittarelli, A., Deibert, R., Michaelsen, M., Scott, M., & Linvill, D. (2025, October 14). We Say You Want a Revolution: PRISONBREAK – An AI-Enabled Influence Operation Aimed at Overthrowing the Iranian Regime. *The Citizen Lab*. https://citizenlab.ca/research/2025-10-ai-enabled-io-aimed-at-overthrowing-iranian-regime/

Graham-Harrison, E., & Tantesh, S. (2026, March 3). 'We'll run out of food this week': Israel's Iran war brings new Gaza siege. *The Guardian*. https://www.theguardian.com/world/2026/mar/02/iran-attacks-gaza-under-siege

Greenberg, A. (2024, August 14). A Single Iranian Hacker Group Targeted Both Presidential Campaigns, Google Says. *Wired*. https://www.wired.com/story/iran-apt42-trump-biden-harris-phishing-targeting/

Greig, J. (2024, August 20). *US agencies attribute presidential campaign cyberattacks to Iran*. The Record. https://therecord.media/agencies-attribute-campaign-attacks-to-iran

Insikt. (2026, March 2). *Ongoing Iran Conflict: What You Need to Know*. RecprdedFuture. https://www.recordedfuture.com/blog/ongoing-iran-conflict-what-you-need-to-know

Kumar, R. (2026, February 28). Hacked Prayer App Sends 'Surrender' Messages to Iranians Amid Israeli and US Strikes. *Wired*. https://www.wired.com/story/hacked-prayer-app-sends-surrender-messages-to-iranians-amid-israeli-strikes/

Lieber, D., Ward, A., & Norman, L. (2026, March 1). Why the U.S. and Israel Struck When They Did: A Chance to Kill Iran's Leaders. *Wall Street Journal*. https://www.wsj.com/world/middle-east/why-the-u-s-and-israel-struck-iran-when-they-did-a-chance-to-kill-its-leaders-b0dbbc88

Lim, J. (2026, January 14). *Beyond Hacktivism: Iran's Coordinated Cyber Threat Landscape | Strategic Technologies Blog | CSIS*. https://www.csis.org/blogs/strategic-technologies-blog/beyond-hacktivism-irans-coordinated-cyber-threat-landscape

Maschmeyer, L. (2021). Why Cyber Operations Fall Short of Expectations. *International Security*, *46*(2), 51–90. https://doi.org/10.1162/isec_a_00418

Maschmeyer, L., & Dunn Cavelty, M. (2022). Goodbye Cyberwar: Ukraine as Reality Check [Application/pdf]. *Policy Perspectives*, *10*(3). https://doi.org/10.3929/ETHZ-B-000549252

Matishak, M. (2026, March 2). *Cyber Command disrupted Iranian comms, sensors, top general says*. The Record. https://therecord.media/iran-cyber-us-command-attack

Miller, M. (2025, June 17). *US critical networks are prime targets for cyberattacks. They're preparing for Iran to strike.* POLITICO. https://www.politico.com/news/2025/06/17/us-critical-networks-iran-israel-cyber-attack-00411799

Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023, July 13). Cyber Operations during the Russo-Ukrainian War. *CSIS*. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

NCSC. (2026, March 2). *Alert: NCSC advises UK organisations to take action following conflict in the Middle East | National Cyber Security Centre - NCSC.GOV.UK*. https://www.ncsc.gov.uk/news/ncsc-advises-uk-organisations-take-action-following-conflict-in-middle-east

New Atlanticist. (2025, July 30). What the Israel-Iran conflict revealed about wartime cyber operations. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/new-atlanticist/what-the-israel-iran-conflict-revealed-about-wartime-cyber-operations/

Newman, L. H., & Burgess, M. (2026, February 9). Iran's Digital Surveillance Machine Is Almost Complete. *Wired*. https://www.wired.com/story/irans-digital-surveillance-machine-is-almost-complete/

Reuters. (2025, June 12). UN says full internet blackout in Gaza, paralyzing aid operations. *Reuters*. https://www.reuters.com/world/middle-east/un-says-full-internet-blackout-gaza-paralyzing-aid-operations-2025-06-12/

Ross, T., Clark, S., Melkozerova, V., Boycott-Owen, M., Lunday, C., & Pollet, M. (2026, March 4). *Europe braces as Iran threatens to attack*. POLITICO. https://www.politico.eu/article/iran-war-europe-braces-tehran-attack-retaliate-threat-missiles/

SentinelOne. (2026, February 28). SentinelOne Intelligence Brief: Iranian Cyber Activity Outlook. *SentinelOne*. https://www.sentinelone.com/blog/sentinelone-intelligence-brief-iranian-cyber-activity-outlook/

Shotter, J., & Ghaffari, B. (2025, August 9). The other Israel-Iran war. *Financial Times*. https://www.ft.com/content/37f21221-a2c3-47c5-b337-7cd168becaf4

IDR
Institutul Diplomatic Român

Our mission. The Romanian Diplomatic Institute (RDI) has the mission to make a substantial contribution to increasing the quality of Romanian diplomacy through training, further education, research, the development of critical and strategic thinking and international networking. A good foreign policy serves as a beneficial domestic policy.

Guiding principles: human resource development, professionalism, respect and dialogue, and responsibility for the community.

Based on the founding legal attributions of the RDI, the further development of the Institute is carried out, according to the needs identified in the MFA, along the following four directions:

- Training and further education of diplomats and other trainees;
- Deepening the research and expertise dimension on regional and functional issues;
- Operating the RDI as a think-tank of the MFA;
- Integration of the RDI into an international network of similar relevant institutes.

Author: Claudiu Codreanu (PhD) is an analyst at the Romanian Diplomatic Institute – Department of Expert Analysis.

RDI Policy Brief Series
ISSN 2066-5989
ISSN-L 2066-5989

Editing, layout, and graphics: Claudiu Codreanu

Cover photo:
https://commons.wikimedia.org/wiki/File:Frank_E_Petersen_Jr_Supports_Operation_Epic_Fury_(9542620).jpg