

IDR

Romanian Diplomatic Institute



MINISTERUL AFACERILOR EXTERNE

POLICY BRIEF nr. 88/2026

Rolul operațiilor cibernetice în conflictul dintre Israel-SUA și Iran

Claudiu Codreanu





Rolul operațiunilor cibernetice în conflictul dintre Israel-SUA și Iran¹

Claudiu Codreanu²

Analist, Institutul Diplomatic Român

Policy Brief Series no. 88 / 2026

Published by: Romanian Diplomatic Institute

ISSN: 2066-5989

Abstract

Atacurile israeliano-americanе asupra Iranului din 28 februarie au condus la un război extins, existând riscul unei escaladări serioase din partea Teheranului după ce mai mulți oficiali iranieni au fost asasinați în bombardamente, inclusiv a Ayatollahul Ali Khamenei. În ceea ce privește operațiunile cibernetice, acestea nu au ieșit în evidență până în acest moment, fiind utilizate ca suport pentru operațiile militare cinetice. Niciuna dintre părți nu a lansat atacuri cibernetice distructive sau cu un impact ridicat, dar sunt șanse ridicate ca unele operațiuni cibernetice să fie încă în pregătire, să fi fost respinse, sau chiar să nu fi fost încă dezvăluite (cel puțin pentru perioada urmărită de această analiză, 28 februarie – 6 martie 2026). Astfel, operațiunile cibernetice par să aibă, cel puțin momentan, un rol de suport, și nu unul de atac sau un rol decisiv – similar cu intervenția americană din Venezuela din ianuarie 2026. Până la momentul acestei analize, Statele Unite au dezvăluit că au lansat atacuri cibernetice împotriva sistemului de comunicații al armatei iraniene pentru a pregăti bombardamentele, dar alte ținte din infrastructura critică nu au fost dezvăluite de niciuna dintre părți. Cu toate acestea, în perioada următoare va continua să existe posibilitatea unor operațiuni cibernetice iraniene împotriva unor sectoare critice, precum energia sau alimentarea cu apă potabilă, ținând cont de istoricul hackerilor Teheranului de a viza aceste sectoare în infiltrații cibernetice anterioare.

Cuvinte cheie: operațiuni cibernetice, Iran, Israel, Statele Unite, conflict.

¹ Această publicație se bazează exclusiv pe surse deschise. Opiniile exprimate aparțin în întregime autorului și nu reflectă neapărat poziția instituției.

² claudiu.codreanu@idr.ro



INTRODUCERE

Atacurile israeliano-americanе asupra Iranului din 28 februarie au condus la un război extins, existând riscul unei escaladări serioase din partea Teheranului după ce mai mulți oficiali iranieni au fost asasinați în bombardamente, inclusiv Ayatollahul Ali Khamenei. Operațiunile de intelligence ale Israelului și ale SUA au fost atât de complexe încât au reușit să identifice trei întâlniri ale liderilor politici și militari ai regimului iranian (Lieber, Ward & Norman 2026). În timpul primelor bombardamente, lansate în mod surprinzător pe lumină, au fost omorâți Liderul Suprem, Ali Khamenei, Ministrul Apărării, Amir Nasirzadeh, Ali Shamkhani, consilier pentru securitate al lui Khamenei, și comandantul Gărzilor Revoluționare, Mohammad Pakpour, printre alții.

Ca ripostă, **Iranul** a bombardat **Israelul**, dar și **state arabe din Golf** care găzduiesc **baze americane**, fiind avariate inclusiv ținte civile. Israelul a inițiat operațiuni și împotriva grupării **Hizbollah** din **Liban**, impunând, totodată, noi restricții pentru punctele de trecere din **Gaza**, inclusiv pentru asistența umanitară. Până în prezent, sunt peste o mie de persoane decedate în Iran (inclusiv la o școală din sudul țării), zeci de decese în Liban, Israel și alte state din zonă, dar și 6 militari americani care și-au pierdut viața.

Conflictul dintre Israel-SUA și Iran se află în plină desfășurare, iar scenariile privind modalitățile prin care ar putea să se încheie sunt incerte, la fel și scenariile post-conflict cu privire la șansele opoziției iraniene de a conduce la căderea regimului represiv. În ceea ce privește **operațiunile cibernetice**, acestea nu au ieșit în evidență până în acest moment, fiind utilizate ca suport pentru operațiile militare cinetice (analiza urmărește evoluțiile din prima săptămână a războiului). **Niciuna dintre părți nu a lansat atacuri cibernetice distructive sau cu un impact ridicat**, dar sunt șanse ridicate ca unele operațiuni cibernetice să fie încă în pregătire, să fi fost respinse, sau chiar să nu fi fost încă dezvăluite.

CONTEXT

Iranul și-a îmbunătățit capabilitățile cibernetice ofensive în ultimii 10 ani, de la campanii de spionaj, operațiuni de influență, cât și atacuri cibernetice. Țintele principale ale

Iranului sunt în Orientul Mijlociu, cu precădere Israel și Arabia Saudită, dar și Statele Unite și aliați din spațiul euro-atlantic. Principalele instituții care se ocupă de operațiuni cibernetice ofensive în Iran sunt Gărzile Revoluționare și Ministerul Informațiilor, acestea utilizând la rândul lor și diferite grupări de hackeri „activiști” pentru a încerca să ocolească atribuirea atacurilor direct către Teheran (Lim 2026).

De-a lungul ultimilor ani, Iranul a utilizat o gamă largă de operațiuni, de la spionaj cibernetic împotriva țintelor civile și militare din Israel, Orientul Mijlociu și SUA, la campanii coordonate de dezinformare, atacuri tip *ransomware*, până la atacuri cibernetice care au implicat utilizare de *wipers* – instrumente care distrug datele din sistemele țintite (SentinelOne 2026). Cele mai notabile operațiuni cibernetice ale Iranului includ atacul împotriva companiei saudite **Saudi Aramco** din 2012, operațiunile de influență în cadrul **alegerilor prezidențiale americane** din 2020 și 2024, dar și atacurile cibernetice împotriva **Albaniei**, lansate ca ripostă pentru găzduirea unei grupări de opoziție iraniene (Ross et al. 2026; Greenberg 2024).

Echipa de campanie a lui Donald Trump a anunțat în vara anului 2024 că a fost vizată de o infiltrare cibernetică iraniană, fapt confirmat ulterior atât de Google, cât și de autoritățile americane (Greenberg 2024). În august 2024, Google publica un raport cu privire la implicarea APT42 – un grup de hackeri coordonat de Gărzile Revoluționare Iraniene – într-o operațiune cibernetică care a vizat campaniile prezidențiale ale lui Donald Trump și a Partidului Democrat (Greenberg 2024). Același grup a vizat campaniile lui Trump și Joe Biden și în timpul alegerilor din 2020. Principalele agenții pentru securitate cibernetică din SUA, FBI (*Federal Bureau of Investigation*), CISA (*Cybersecurity and Infrastructure Security Agency*) și ODNI (*Office of the Director of National Intelligence*) **au atribuit operațiunile cibernetice Iranului** (Greig 2024a).

Există, de altfel, și un exemplu clar de utilizare a operațiunilor cibernetice ca armă principală în conflictul mai larg dintre Israel/SUA și Iran. **În perioada 2009-2010, Statele Unite și, cel mai probabil, Israel, au lansat un atac cibernetic distructiv împotriva Iranului**, reușind să perturbe programul nuclear iranian prin avarierea centrifugelor din centrul de îmbogățire a uraniului din Natanz – acum o țintă principală în campaniile de bombardamente din 2025 și 2026 (Shotter & Ghaffari 2026). Totuși, acțiunea din 2009-2010 a fost mai degrabă una de **sabotaj**, și nu avea rolul de a deschide un război cu Teheranul. Mai mult, impactul nu a fost unul decisiv, și nici nu a reușit să perturbe în totalitate programul nuclear iranian sau să afecteze regimul per ansamblu.

Rolul operațiilor cibernetice în Războiul de 12 Zile

Operațiuni cibernetice majore ale Iranului în perioada Războiului de 12 Zile dintre Israel-SUA și Iran (13-24 iunie 2025) ori nu au avut loc, ori nu au fost încă dezvăluite. **Autoritățile americane au avertizat în iunie 2025 că Iranul ar putea viza sistemele de transporturi sau de alimentare cu apă din SUA**, ținând cont că aceste sectoare au fost ținta mai multor intruziuni cibernetice iraniene în Statele Unite de-a lungul timpului (Miller 2025). Cu toate acestea, nu au avut loc incidente. Iranul a desfășurat **operațiuni de influență** care au constat în campanii de dezinformare concepute pentru a genera confuzie sau panică, dar și atacuri de tip DDoS (*Distributed Denial of Service*), care conduc la perturbarea unor site-uri sau platforme, sau chiar la trecerea lor în offline (Baram & Peer 2025). **În primele zile de la începutul bombardamentelor a avut loc o creștere de 700% a atacurilor cibernetice împotriva țintelor din Israel** (Baram & Peer 2025).

De cealaltă parte, au avut loc două operațiuni notabile. **Predatory Sparrow, un grup de hackeri afiliat guvernului israelian, a lansat două operațiuni cibernetice împotriva Iranului în acea perioadă**. Au fost vizate Bank Sepah, o bancă din Iran cunoscută pentru legăturile cu Gărzile Revoluționare, ale cărei servicii au fost paralizate, și Nobitex, cea mai mare platformă de schimb de criptomonede din Iran, fiind extrase și apoi distruse active crypto de peste 90 de milioane de dolari (Atlantic Council 2025; Baram & Peer 2025). În acest context, **Iranul a tăiat aproape complet accesul la internet** pentru a-și proteja sistemul financiar și restul sectoarelor critice de alte atacuri cibernetice care ar fi condus la pierderi considerabile (Baram & Peer 2025; Burgess 2025). Totodată, alte obiective ale opririi internetului au inclus **prevenirea unor eventuale demonstrații**, dar și **perturbarea eventualelor comunicații** sau activități de spionaj ale Statelor Unite și Israelului, în special cele legate de alegerea țintelor pentru rachete.

Represiune digitală și campanii de dezinformare

Iranul reprezintă una dintre principalele țări care au utilizat oprirea accesului la internet pentru populație ca măsură pentru a încerca stăvilirea protestelor anti-guvern. **Teheranul a restricționat accesul la internet pentru populație în timpul mai multor evenimente în**

ultimii ani, inclusiv în timpul protestelor din 2022-2023, după moartea Mahsei Amini în arestul poliției „moralității” (Burgess 2025). Totodată, **în contextul protestelor anti-regim din 2026, autoritățile iraniene au tăiat integral accesul la internet pentru populație timp de aproape două luni** (Newman & Burgess 2026). Măsura, care se integrează în politicile autoritarismului digital, a fost luată atât pentru a încerca oprirea demonstrațiilor prin perturbarea coordonării protestatarilor, dar și pentru a opri ca filmările cu masacrele produse de forțele de ordine să ajungă în internetul global. Mai mult, pe măsură ce restricțiile cu privire la internet au fost ridicate, autoritățile au înăsprit măsurile de supraveghere în masă a populației (Newman & Burgess 2026).

Totodată, un alt aspect notabil legat de protestele anti-regim și de actualul război lansat de Israel și SUA reprezintă o campanie coordonată de influență care a țintit populația iraniană începând cu 2025. Centrul *Citizen Lab* al Universității din Toronto dezvăluia în toamna anului trecut detaliile unei **operațiuni de influență care avea ca obiectiv înlăturarea regimului iranian** (Fittarelli et al. 2025). Conform analizei, campania coordonată de dezinformare a diseminat narațiuni care promovau revolte împotriva regimului și sprijin pentru Reza Pahlavi, fiul ultimului șah al Iranului și principala figură a opoziției. Totodată, cercetătorii au evaluat că, cel mai probabil, **operațiunea a fost desfășurată sau sprijinită de guvernul israelian**, fiind sincronizată inclusiv cu bombardamentele din iunie 2025.

ULTIMELE EVOLUȚII DIN ACTUALUL CONFLICT. ANALIZĂ

Generalul Dan Caine, șeful Statului Major Interarme al Statelor Unite, declara în 2 martie că s-au derulat acțiuni conduse de **Comandamentul Cibernetice, care a lansat atacuri cibernetice asupra comunicațiilor iraniene pentru a pregăti terenul campaniei de bombardamente**, afirmând că au fost desfășurate „efecte non-cinetice” pentru a sprijini operațiile (Matishak 2026). Totodată, media americană a relatat că și în timpul războiului din iunie 2025 au fost lansate atacuri cibernetice asupra sistemelor de rachete iraniene pentru a sprijini campania de bombardamente asupra instalațiilor nucleare (Matishak 2026). În același timp, Președintele Donald Trump și Dan Caine au sugerat în ianuarie 2026 că SUA au folosit atacuri cibernetice pentru a încerca provocarea unei pene de curent în Caracas și pentru a perturba sistemele de radare antiaeriene și comunicațiile în timpul misiunii pentru capturarea Președintelui venezuelean Nicolas Maduro (Matishak 2026).

Pe lângă atacurile cibernetice folosite în coordonare cu operațiile cinetice, nu au avut loc incidente majore. **Unul dintre cele mai vizibile atacuri cibernetice a ținut Iranul pe 28 februarie, imediat după primele rachete.** O aplicație de telefon pentru rugăciuni cu peste 5 milioane de descărcări, *BadeSaba Calendar*, a fost infiltrată cibernetic pentru a trimite mesaje de susținere a bombardamentelor și o promisiune pentru amnistierea celor care se predau – „ajutorul este aici” (Kumar 2026). Totuși, nu este clar ce impact a avut această operațiune, și nici care e proporția rezidenților din Iran care au primit mesajul. Astfel, **cel mai important element din zona cyber nu a fost reprezentat de atacuri cibernetice, ci de spionaj cibernetic** – acesta fiind esențial pentru pregătirea campaniei de bombardamente, atât pentru ținutarea clădirilor, cât și pentru asasinarea oficialilor iranieni (Shotter & Ghaffari 2026). De cealaltă parte, chiar dacă nu au fost înregistrate intruziuni semnificative până acum, mai multe **grupuri de hackeri „activiști” afiliați cu guvernul iranian au anunțat că vor lansa o serie de operațiuni cibernetice împotriva Israelului și a altor ținte din regiune** (Insikt Group 2026).

Potențialul rol decisiv al operațiunilor cibernetice în perioade de război deschis a fost chestionat în ultimii ani. **Există deja studii vaste cu privire la războiul rusesc din Ucraina, unde operațiunile cibernetice nu au jucat un rol strategic substanțial, având un rol și un impact limitat pentru ambele părți**, cu toate că în perioada anterioară invaziei totale Rusia a reușit să lanseze mai multe atacuri semnificative asupra infrastructurii critice ucrainene (Mueller et al. 2023; Maschmeyer & Dunn Cavelty 2023).

Mai mult, Lennart Maschmeyer argumenta într-un articol din 2021 că **utilizarea operațiunilor cibernetice se lovește de o trilemă operațională** – atacurile nu pot să fie în același timp executate într-un timp scurt, să aibă un impact puternic, dar și să fie controlabile și precise (Maschmeyer 2021). Totuși, atacurile israeliano-americeane asupra Iranului din 2026 sunt, practic, o continuare a celor din iunie 2025 – un timp aproape rezonabil pentru exploatarea unor breșe deja găsite anii trecuți în rețelele iraniene. Dar, măsurile de apărare cibernetică ale Iranului par să reprezinte un obstacol, la fel și faptul că lansarea de rachete și drone de atac este mult mai rapidă și are un impact mult mai mare în cadrul unui război deschis. La fel, Iranul, cel puțin până în prezent, pare să nu fi dezvoltat capacitățile necesare pentru a putea lansa rapid atacuri cibernetice substanțiale împotriva Statelor Unite, Israelului, sau asupra aliaților din Golf – dar acest lucru rămâne de văzut în săptămânile următoare, mai ales cu privire la Arabia Saudită și statele din Golf.

Astfel, **operațiunile cibernetice sunt utilizate pentru a sprijini acțiunile cinetice**, în primul rând pentru perturbarea comunicațiilor militare iraniene fie înaintea campaniei de bombardamente sau în timpul acesteia, dar și pentru **fructificarea unor campanii anterioare de spionaj cibernetic pentru a ținti precis** clădiri guvernamentale sau militare sau chiar a unor lideri politici sau militari. Totodată, alte obiective ar putea să fie țintirea sectorului financiar-bancar și a altor zone din **infrastructura critică** pentru a perturba regimul, dar și **diseminarea campaniilor informaționale** prin canale infiltrate cibernetic (ex. canale TV, aplicații mobile, social media). În schimb, **operațiunile cibernetice iraniene ori nu au avut succes, ori încă se află în desfășurare**, dar este posibil și ca acestea să nu fi fost dezvăluite până în acest moment – ceea ce implică, oricum, faptul că au avut un impact redus sau au fost desfășurate pe o scară redusă.

CONCLUZII ȘI RECOMANDĂRI

Compania americană de securitate cibernetică *SentinelOne* avertiza în 28 februarie că, este **probabil că operațiunile cibernetice iraniene să fie intensificate pe termen scurt**, ținând cont de istoricul utilizării acestora ca ripostă de către Teheran. Totuși, nu există riscuri majore cu privire la amenințările cibernetice iraniene pentru statele euro-atlantice. Spre exemplu, Centrul Național pentru Securitate Cibernetică al Regatului Unit (NCSC) a emis un comunicat în 2 martie, precizând că cel mai probabil, **nu există modificări semnificative cu privire la amenințările cibernetice iraniene pentru Regatul Unit**. Cu toate acestea, NCSC afirmă că Iranul și grupările legate de Teheran mențin capacități pentru a lansa operațiuni cibernetice, existând „aproape cu certitudine” un **risc ridicat de amenințări cibernetice indirecte pentru organizațiile care au o prezență în Orientul Mijlociu**.

Cel mai probabil, **operațiunile cibernetice vor continua să joace doar un rol de suport pentru toate părțile acestui conflict**. Totodată, Iranul va continua să impună **restricții aproape totale cu privire la accesul internetului** pe toată durata războiului, dar și în cazul unor eventuale proteste anti-regim care ar putea apărea după război. Totodată, **cel mai probabil România și alte state europene nu vor deveni ținte directe ale operațiunilor cibernetice, dar pot deveni ținte indirecte ale unor atacuri oportuniste care să vizeze ținte multiple**, dar sunt șanse reduse ca acestea să fie unele puternice sau fără precedent. Există un **risc scăzut pentru operațiuni cibernetice pe scară largă la un nivel fără precedent**, dar un risc crescut

pentru operațiuni oportuniste de tip **ransomware** (care blochează sistemele afectate prin criptarea datelor) sau atacuri de tip **wiper** (care șterg definit datele din sistemele vizate) și un **risc crescut pentru campanii de spionaj cibernetic**.

Totodată, **trebuie menținută atenția și în zona teritoriilor palestiniene**, mai ales în contextul deteriorării **situației umanitare** de acolo după restricționarea unor puncte de trecere de către Israel – există riscul impunerii unor **restricții pe termen lung cu privire la Internet** sau telecomunicații, similar cu cele implementate în Gaza în timpul Războiului de 12 Zile (Reuters 2025; Graham-Harrison & Tantesh 2026).

Chiar dacă războiul încă se află în desfășurare și pot avea loc schimbări cu privire la amenințările cibernetice, pot fi luate în calcul mai multe **recomandări** principale:

- Consolidarea securității cibernetice și monitorizarea rețelelor în **sectorul energetic și cel al alimentării cu apă**, ținând cont de istoricul hackerilor guvernamentali iranieni de a ținti aceste infrastructuri.
- Trebuie luată în calcul apărarea inclusiv împotriva unor **operațiuni cibernetice intruzive sau puternice care pot fi lansate de Iran** în perioada următoare.
- Trebuie luate măsuri și pentru prevenirea unor campanii iraniene de tip **ransomware în toate sectoarele critice**.
- Trebuie luate măsuri pentru **prevenirea campaniilor de dezinformare** sau a operațiunilor de tip *hack-and-lead* (sustragerea de informații prin atacuri cibernetice și publicarea lor *online*, de multe ori trunchiat).

Astfel, **operațiunile cibernetice par să aibă, cel puțin momentan, un rol de suport**, și nu unul de atac sau un rol decisiv – similar cu intervenția americană din Venezuela din ianuarie 2026. Totuși, acest lucru nu exclude în niciun caz posibilitatea unui astfel de atac cibernetic pe scară largă sau unul bine țintit dar cu un impact ridicat (ex. pene de curent, blocarea activității unor spitale etc.) Această analiză vizează doar informațiile existente până acum și evoluțiile din acest moment, urmărind perioada 28 februarie – 6 martie 2026. Nu este clar ce traiectorie va lua acest război, și nici dacă va rezista (sau nu) regimul actual în Iran, la fel cum nu este clar dacă vor fi implicate mai multe țări din spațiul euro-atlantic (fie prin atacuri cu drone sau rachete asupra unor baze americane, ori prin decizii de a se alătura eforturilor de apărare împotriva ripostelor iraniene).

Totodată, **eventualul final al actualului război nu trebuie considerat drept finalul tuturor ostilităților** – operațiunile cibernetice pot fi pregătite pentru perioada post-bombardamente. De aceea organizația AccessNow face apel la implementarea unui **armistițiu digital** pentru toate conflictele, ținând cont că operațiunile cibernetice și represiunea digitală continuă să fie utilizate și după oprirea acțiunilor cinetice (Coppi & Fatafta 2024). Atacurile cibernetice iraniene au continuat și după ce operațiunile cinetice au fost încheiate după 12 zile, grupări afiliate guvernului iranian încercând să exploateze o vulnerabilitate a Microsoft pentru a ținti serverele unor companii israeliene (Shotter & Ghaffari 2026).

BIBLIOGRAFIE

- 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., Michaelson, 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*. *RecordedFuture*. <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

Misiune. Institutul Diplomatic Român (IDR) își asumă misiunea de a contribui substanțial la creșterea calității diplomației românești prin formare, educare continuă, cercetare, prin dezvoltarea gândirii critice și strategice, prin conectare internațională. O politică externă bună servește unei politici interne benefice.

Principii: valorizarea resurselor umane, profesionalismul, respectul și dialogul, responsabilitatea pentru comunitate.

Pornind de la atribuțiile legale fondatoare ale IDR, dezvoltarea în continuare a institutului se realizează, în funcție de nevoile identificate în MAE, pe următoarele patru direcții:

- Formarea și educarea continuă a diplomaților și a altor categorii de cursanți;
- Aprofundarea dimensiunii de cercetare și expertiză pe spații regionale și problematice funcționale;
- Funcționarea IDR ca *think-tank* al MAE;
- Integrarea IDR în cadrul unei rețele internaționale de institute relevante similare.

Autor: Claudiu Codreanu (PhD) este analist la Institutul Diplomatic Român – Serviciul Furnizare de Expertiză pentru MAE.

Seria Policy Brief IDR
ISSN 2066-5989
ISSN-L 2066-5989

Editare, formatare și grafică: Claudiu Codreanu

Imagine copertă:

[https://commons.wikimedia.org/wiki/File:Frank_E_Petersen_Jr_Supports_Operation_Epic_Fury_\(9542620\).jpg](https://commons.wikimedia.org/wiki/File:Frank_E_Petersen_Jr_Supports_Operation_Epic_Fury_(9542620).jpg)

Institutul Diplomatic Român - IDR
<https://www.idr.ro/en/> | secretariat@idr.ro
Primăverii 17, sector 1, București, 011972