STRATEGIER I CYBERDOMÄNEN

Välkommen till dystopia – den iranska regimens syn på cyberrymden

Erika Holmquist

Irans säkerhetspolitiska utveckling under 2026 är den mest turbulenta sedan Iran-Irakkriget, och har synliggjort vikten av cyberrymden som arena för iranska konflikter med både interna och externa fiender. Detta memo belyser aspekter av Irans cyberstrategi från 2022 i syfte att fördjupa förståelsen om hur den iranska regimen ser på cyberrymden och då främst ur ett inrikes perspektiv. Liksom i andra auktoritära länder är kontrollen över vilken information befolkningen får tillgång till av stor betydelse i Irans strategi i cyberdomänen.

Under de första dagarna av 2026 svepte den största vågen av protester under den islamiska republikens historia över Iran. Missnöjet tändes av den svåra ekonomiska situationen men övergick snabbt i kritik av regimen och krav på regimskifte.

Regimen antog en tvådelad motstrategi. Dels användes mer dödligt våld än någonsin tidigare, dels infördes den mest omfattande blockeringen av internet och telefoni i Iran dittills för att skära av iranierna från omvärlden. I slutet på februari 2026 angrep sedermera Israel och USA Iran militärt. Cyberförmågor har utgjort en viktig komponent i den efterföljande konflikten. Under krigets första dag användes underrättelseinhämtning via iranska trafikkameror för att lokalisera och döda Irans högste ledare Ayatollah Ali Khamenei. Attentatet visade att iransk cybersäkerhet har allvarliga brister. Iran stängde därefter ner internet ännu en gång med närmast total isolering av befolkningen som följd. Regimens omfattande blockering av internet skapar farhågan att tillgången till internet hädanefter kommer att

FOI Memo 9303
Projektnummer: E12626
Godkänd av: Karolina Gasinska Singh

Juni 2026

bli ett hårt reglerat privilegium. Irans cyberstrategi som kom ut 2022 visar att de betraktar cyberrymden som en högt prioriterad arena, vilket den säkerhetspolitiska utvecklingen under 2026 också understryker. Händelserna väcker frågan om vilken riktning Irans cyberrymd kommer att utvecklas i, och därigenom vilken slags framtid iranierna går till mötes.

- Irans syn på cybermakt har hittills framför allt formats av två erfarenheter: protestvågen 2009 som förstärktes av cyberbaserad kommunikation, och Stuxnetattacken mot Irans urananrikningscentrifuger vid ungefär samma tidpunkt. Sannolikt kommer även attentatet mot Ayatollah Khamenei att utgöra en tredje formativ erfarenhet för iransk cyberförmågeutveckling i framtiden.

- Iran definierar cyberområdet som den femte domänen för krigföring, och ser cybermakt som en av de viktigaste källorna till nationell makt eftersom den förstärker redan befintliga maktområden.

- Cyberstrategin från 2022 belyser att Iran har stora ambitioner på cyberområdet, och några av strategins viktigaste fokusområden är cyberförsvar, informationskontroll och övervakning, där alla syftar till att värna nationell säkerhet. Även om det inte skrivs ut explicit, så finns det också goda grunder för att anta att en satsning på offensiva förmågor ingår i Irans åtgärder för att stärka sin cybermakt. I detta memo ligger dock tyngdpunkten på hur Iran lägger upp sin inrikes cyberstrategi.

- Sitter regimen kvar vid makten är det sannolikt att cyberområdet kommer att få ännu större betydelse, och att potentialen för kontroll kommer att trumfa de ekonomiska möjligheter som cyberrymden också erbjuder.

Utvecklingen på cyberområdet sedan 2009

Irans cyberutveckling kan delas in i flera faser. 2009–2011 identifierade iranska beslutsfattare behovet av att stärka inhemska förmågor på cyberområdet. Proteströrelsen som uppstod 2009 efter misstankar om valfusk i presidentvalet gynnades av att tillgången till internet och sociala medier gjorde informationsspridning snabbare, och organiseringen av demonstrationerna enklare. Ordningsmakternas efterföljande övergrepp mot demonstranterna blev också svårare att dölja. Därigenom såg regimen ett ökat behov av att kontrollera information och övervaka medborgarnas kommunikations- och rörelsemönster. Den repressiva cyberverktygslådan har utökats stadigt sedan dess.

Stuxnetattacken mot kärnenergianläggningen i Natanz som upptäcktes 2010, gav insikten om att Iran behövde ett bättre cyberförsvar och bättre offensiva förmågor.[1] Under åren 2012–2018 etablerades nya strukturer och institutioner särskilt inriktade på cyberfrågor. Iran utvecklades också till en aktiv offensiv cyberaktör, som använder cyberförmågor för informationsinhämtning, spionerі och sabotage.[2] Under den här tidsperioden inleddes också samarbeten med Kina och Ryssland kring cyberfrågor. Sedan 2019 har satsningarna på att bygga ut infrastruktur och att öka cyberkapaciteten fortsatt.[3] 2022 rankades Iran på tionde plats i Belfer Centers National Cyber Power Index (NCPI).[4] Det innebar en förflyttning uppåt från plats 22 i den föregående mätningen från 2020, och visar att Iran har blivit en starkare cyberaktör.

Synen på cybermakt

> *Cyberrymden är lika betydelsefull som den islamiska revolutionen.*
>
> *Ali Khamenei*[5]

Citatet understryker hur viktigt Ali Khamenei, Irans föregående högste ledare ansåg att cyberområdet var. Han ville att Iran skulle bli en framstående cybermakt som skulle kunna mäta sig med världens mest inflytelserika stater.[6] En rapport från det iranska parlamentets

1 Chuck Freilich, *The Iranian Cyber Threat*, INSS, Memorandum 230 (Tel Aviv: INSS, 2024), 25.

2 Freilich, *The Iranian Cyber Threat*, 30.

3 Freilich, *The Iranian Cyber Threat*, 33–34.

4 Belfer Center, National Cyber Power Index 2022, Cambridge, MA: Harvard Kennedy School (2022), *CyberProject_National Cyber Power Index 2022_v3_220922.pdf*.

5 Mehr News, ”What are the important emphases of the Supreme Leader on the management of cyberspace?”, 24 mars 2024.

6 IRNA, *”Supreme Council of Cyberspace, a Council to Transform Iran into a Cyber Power”*, 9 mars 2024.

forskningscenter beskriver cybermakt som en av de viktigaste källorna till nationell makt under 2000-talet.[7] Det har med cyberområdets natur att göra. ”[Cybermakt] skiljer sig från traditionell makt på grund av dess spridning, låga inträdeskostnader, aktörers anonymitet och möjligheten till samtidig påverkan inom olika domäner.”[8] I cybermakt ingår både hårda och mjuka aspekter av nationell makt. Ett av rapportens viktigaste budskap är att ”cybermakt spelar en nyckelroll i nationell säkerhet och konkurrens globalt eftersom det kan användas för att skapa fördelar inom alla operationsområden/…/ och för att förstärka traditionella maktverktyg som ekonomi, försvar, diplomati och underrättelseverksamhet.”[9] Cyberrymden utgör den femte domänen för krigföring jämte land, luft, hav och rymd.[10] Att cyberrymden inte begränsas av geografi ger helt nya möjligheter till närvaro och påverkan nationellt och globalt.

Den iranska cyberstrategin

2022 antog Iran ett ”strategiskt dokument för cyberrymden” (hädanefter cyberstrategin/strategin) som sträcker sig fram till 2031. Dokumentet innehåller en vision för hur Irans cyberrymd ska se ut 2031, med 26 övergripande mål och 39 konkreta åtgärder som ska förverkligas.[11] Det finns ett antal tydliga teman i strategin. Det övergripande syftet är, i enlighet med Ayatollah Khameneis mål, att förvandla Iran till en ledande cybermakt. Dessutom finns en idé om att cybermakt förstärker redan befintliga maktverktyg och det förklarar många av prioriteringarna som görs i strategin. Många av Irans mål rör just att stärka traditionella källor till makt som ekonomi, försvar, diplomati och underrättelser. Den huvudsakliga drivkraften är att värna nationell säkerhet, vilket i mångt och mycket betraktas som synonymt med regimsäkerhet. Med det som utgångspunkt är det värt att lyfta fram några områden i strategin såsom cyberförsvar, kontroll över informationsmiljön och övervakning av befolkningen.

Cyberförsvar

Cyberstrategin innehåller flera ambitiösa målsättningar. Iran ska ta plats bland de globala cybermakterna och bli den ledande cybermakten i regionen, uppnå effektiv cyberavskräckning internationellt, säkerställa landets cybersäkerhet, och värna Irans nationella intressen samt skydda infrastruktur mot hot i cyberrymden.[12] I strategin finns en lång lista över åtgärder. Till exempel så ska ett cyberförsvarssystem (*nezam-e defa’ faza majazi*) utformas. Exakt vad som menas är inte tydligt i dokumentet, men enligt en artikel från den iranska försvarshögskolan bör cyberförsvar bygga på tre komponenter: resiliens, försvar och avskräckning.[13] Försvarskomponenten delas i sin tur in i aktivt (militärt) och passivt (civilt) försvar (*padafand-e amel* och *padafand-e gheir-e amel*).[14] Militärt cyberförsvar förutsätter cybervapen.[15] Därmed kan man anta att vidareutveckling av offensiva cyberförmågor också ingår i uppbyggnaden av cyberförsvarssystemet. Irans regering vidgår inte att de ligger bakom offensiva cyberoperationer, men det är väl belagt att såväl Iranaffilierade som statliga grupper från Iran har varit aktiva offensivt gentemot t.ex. USA och Israel.[16]

Iran rankas högt av NCPI vad gäller destruktiva cyberförmågor, men lågt vad gäller cyberförsvar och cybersäkerhet.[17] En delförklaring skulle möjligen kunna vara att de senare inte har varit högsta prioritet, trots Irans komplicerade säkerhetspolitiska situation. En intervju med chefen för den iranska civilförsvarsorganisationen (*sazman-e padafand-e gheir-e amel*) som har ett övergripande ansvar för Irans passiva cyberförsvar ger några ledtrådar. Som svar på frågan om varför Irans cyberförsvar inte verkar ha varit särskilt effektivt under tolvdagarskriget mot Israel 2025 uppgav han att hans

7 ”Cybermakt: Natur, dimensioner, komponenter och globala indikatorer”, forskningscentret vid islamiska republikens konsultativa församling, 8.

8 ”Cybermakt: Natur, dimensioner, komponenter och globala indikatorer”, 8.

9 ”Cybermakt: Natur, dimensioner, komponenter och globala indikatorer”, 7.

10 Mohammad Qasemi, Davood Azar, och Vahid Sajjadi, “Factors affecting the evaluation of the cyber defense power of the Islamic Republic of Iran Army”, (2022), *Warfare Study Quarterly*, *https://www.qjws.ir/issue_34895_34896.html*, (2022): 115-40, 118.

11 Irans högsta råd för cyberrymden,”Strategiskt dokument för cyberrymden”, 1401, جمهوري اسالمي ايران در فضاي مجازي سند راهبردي dotic..ir (hämtad oktober 2025)

12 ”Strategiskt dokument för cyberrymden”, 3–4.

13 Majid Haghi och Mehrdad Kargari, “Presenting a conceptual model of security-based cyber defense of the Islamic Republic of Iran”, *Quarterly Journal of Strategic Studies of Cyberspace*, Volume 2, Issue 3, 7-32, 29.

14 Haghi och Kargari, “Presenting a conceptual model”, 29.

15 Haghi och Kargari, “Presenting a conceptual model”, 28.

16 Eurepoc, Cyber incident dashboard, *https://eurepoc.eu/dashboard/*.

17 Belfer Center, *National Cyber Power Index 2022*, 11–12.

myndighet både saknar budget och personal.[18] Enligt iranska cybersäkerhetsexperter är dålig beredskap ytterligare en delförklaring. Iran har visserligen tagit fram regler och tekniska lösningar men inte kommit särskilt långt, varken när det gäller att implementera dem eller i att utbilda berörda organisationer och företag om cybersäkerhet.[19]

Iran har gjort framsteg på cyberområdet, men står även inför utmaningar. Enligt chefen för civilförsvarsorganisationen är ett grundläggande problem att Israel och USA har tillgång till långt mer avancerad cyberteknologi än vad Iran har. Ett annat är det som han ser som amerikansk dominans över teknologiutveckling, samt internets infrastruktur, innehåll och styrning.[20] Kombinationen av Irans svaga cybersäkerhet och fiendernas tekniska överlägsenhet har fått ödesdigra konsekvenser för den iranska regimen. På morgonen den 28 februari 2026 dödades Irans högste ledare Ali Khamenei av Israel och USA. Operationen möjliggjordes bland annat av underrättelseinhämtning via trafikkameror och manipulering av iraniernas kommunikation. [21]

Informationskontroll och övervakning

Vid sidan av våldsanvändning så hör övervakning, informationskontroll och propaganda till de viktigaste repressionsmedlen för auktoritära regimer.[22] Iran räknas som en av pionjärerna inom digital repression.[23] Därför är det kanske inte förvånande att kontroll över informationsmiljön och övervakning hör till de områden där Iran får högst poäng på NCPI:s ranking.[24] Cyberverktyg för informationskontroll, övervakning och censur spelar en grundläggande roll i den iranska regimens strategi för att förtrycka oliktänkande och bevara politisk stabilitet.[25]

Flera punkter i cyberstrategin syftar till att minska utländska beroenden, och att öka Irans inflytande över internets styrning. Det senare beskrivs som en strävan efter ökad multilateralism, vilket är en syn som Iran delar med både Ryssland och Kina. Syftet är stärkt kontroll. Ett av cyberstrategins explicita mål är att ”…konsolidera och stärka styrningen, utöva nationell suveränitet och auktoritet över alla dimensioner av landets cyberrymd.”[26]

Iran har länge arbetat på att skapa ett nationellt internet efter kinesisk modell, och i strategin understryks det att det projektet ska slutföras till 2031. Det finns flera syften med det. Å ena sidan handlar det om att reducera sårbarheten gentemot externa fiender, för man tänker sig att ett inhemskt kontrollerat internet samt minskat beroende av utländsk hård- och mjukvara leder till ett minskat antal externa attacker. Å andra sidan handlar det om att hantera interna hot och att stärka möjligheterna till att kontrollera och manipulera information. Under de senaste tio åren har det folkliga missnöjet ökat kraftigt och proteströrelser avlöst varandra nästan årligen. För varje omgång tycks cyberverktygen för repression bli fler och kontrollen över Irans cyberrymd bättre.[27]

I Iran är tillgången till internet i praktiken segregerad, både i fråga om internet i stort och vad gäller användning av utländska plattformar. Vanliga medborgare kan sedan länge inte använda sig av utländska plattformar utan VPN.[28] Särskilt utvalda personer kan använda internet utan begränsningar via så kallade ”vita SIM-kort”. Till de särskilt utvalda hör exempelvis statstjänstemän, myndighetspersoner och akademiker. Många politiska ledare har egna X-konton som de använder för att kommunicera med omvärlden. Att de icke-privilegierade behöver använda VPN för att nå utanför Irans gränser är både potentiellt lukrativt och användbart ur övervakningssynpunkt för staten, som utvecklar och säljer egna falska VPN-tjänster

18 Majeraa Media, ”Historien om tolvdagarskriget: Gholam-Reza Jalali”, Youtube, 2025 ماجرای جنگ دوازده روزه | به روایت جواد موگویی | قسمت یازدهم | غلامرضا جلالی

19 Peivast, ”Security in the age of successive attacks: why Iran is not yet ready for cyber warfare”, 29 oktober 2025. *https://peivast.com/p/246842*.

20 Majeraa Media, ”Historien om tolvdagarskriget: Gholam-Reza Jalali”, Youtube, 2025

21 Financial Times, ”*Inside the plan to kill Ali Khamenei*”, 2 mars 2026.

22 Edmarverson Santos, “The struggle for human rights in authoritarian regimes”, Diplomacy and Law, u.å., *https://www.diplomacyandlaw.com/post/the-struggle-for-human-rights-in-authoritarian-regimes.*

23 Shahram Akbarzadeh, Amin Naeni, Ihsan Yilmaz och Galib Bashirov, ”Cyber Surveillance and Digital Authoritarianism in Iran”, Global Policy, mars 2024, 4.

24 Belfer Center, *National Cyber Power Index 2022*, 11–12.

25 Anita Gohdes, *Repression in the digital age – Surveillance, censorship and the dynamics of state violence*, (Oxford University Press: 2024), 128.

26 ”Strategiskt dokument för cyberrymden”, 3.

27 Gohdes, ”Repression in the digital age”, 128.

28 VPN är en förkortning för virtuellt privat nätverk och det är en tjänst som skapar en krypterad anslutning mellan t.ex. en dator eller en mobil och internet, vilket gör det möjligt att kringgå statens restriktioner.

till medborgarna.[29] Liksom i andra auktoritära stater används också begränsningar av uppkopplingshastighet och blockeringar av internet som metoder för att kontrollera informationsflödet. Under demonstrationerna i januari 2026 och det efterföljande kriget med Israel och USA visade regimen upp sin kapacitet att genomföra en närmast total nedsläckning av både internet och telefoni, i syfte att stoppa informationsspridning både inom och utanför landet.[30] Tillvägagångssättet var också mer sofistikerat och precist än tidigare gånger. Förmågeutvecklingen vilar till del på fördjupade samarbeten med Kina och Ryssland som bidrar med expertis och teknologi.[31]

Övervakning nämns inte explicit i cyberstrategin men däremot i artikel 75 i den sjunde femårsplanen som godkändes 2024. Enligt den ska statens kapacitet för övervakning expandera kraftigt.[32] Till exempel är iranska företag som lagrar användardata skyldiga att dela dessa med staten, och särskilt flagga för kriminellt innehåll.[33] Formuleringarna antyder en del inspiration från Kina och dess omfattande sociala kreditsystem. I cyberstrategin används begrepp som ”smart governance” och ”smart cities” som möjligen anknyter till detta.

Förutom i syfte att stjäla information eller spionera på medborgarna så används cyberverktyg också mer praktiskt för att se till att lagar och regler efterlevs ute i samhället. Efter kvinna-liv-frihetprotesterna 2022–2023 så började man till exempel i Isfahan att använda falska basstationer och övervakningskameror för att identifiera kvinnor som rör sig i offentligheten med bristfällig hijab.[34] Mobilappen Nazer (ungefär ”Övervakaren”) används av på förhand godkända medborgare för att rapportera in bilar med bristfälligt klädda kvinnliga förare till polisen.[35] När en bil blir rapporterad så får bilägaren ett sms om att en förseelse begåtts, och ibland beslagtas även bilen. Appen är tänkt att i framtiden också användas för andra förseelser. [36] Under demonstrationerna i början av 2026 användes drönare för att övervaka folksamlingarna, och rikta in ordningsmakternas insatser.[37]

Slutsatser

Den iranska regimen är under stor press såväl externt som internt. Externt har Irans säkerhetspolitiska position försvagats, och försvarsstrategin som går ut på att hålla krig borta från iranskt territorium har fallerat.

Regimens interna legitimitet är mer ifrågasatt än någonsin efter åratal med ökat sanktionstryck, tilltagande vanstyre, och eskalerande brutalitet. Cyberverktygens roll i att upprätthålla regimens maktställning genom repression har växt över tid, liksom verktygens nivå av sofistikation. Detta sker mycket tack vare nära samarbete med likasinnade stater som Kina och Ryssland, som inte bara delar Irans dåliga relationer med väst utan också synen på den egna befolkningen som en potentiell fiende.

Israel och USA:s överlägsna cyberförmågeanvändning under kriget belyser dock att Iran har en bit kvar till målet att bli en global cybermakt. Strategin för att hitta och slå ut Irans ledarskap utgör ett skräckinjagande exempel för både Iran och många av världens auktoritära stater, som kan komma att motivera och driva på ansträngningar för utökad cybermakt och stärkt informationskontroll. För den iranska regimen var tillskansandet av cybermakt högsta prioritet redan före kriget. Givet motgångarna på andra områden är det nu troligt att cyberområdet med dess breda potential för maktutövning blir ännu viktigare framöver. Cybermakt utgör ett relativt kostnadseffektivt sätt att förstärka redan befintliga maktområden.

Irans cyberstrategi, varav enbart vissa delar har presenterats här, sätter upp höga mål. Hur förutsättningarna ser ut för att man ska uppnå strategins mål fram till 2031 kräver en egen studie. Men ett slags moment 22 är förmodligen hur utökad informationskontroll och isolering av befolkningen går ihop med målsättningen att ha en fungerande ekonomi. Irans katastrofala ekonomiska situation beror på en kombination av misskötsel och hårda sanktioner, och är en av kärnfrågorna som driver

29 Akbarzadeh et al., ”Cyber Surveillance and Digital Authoritarianism in Iran”, 6–7.

30 Filterwatch,”Total Blackout: A Technical Breakdown of the January 2026 Shutdown”, 16 januari 2026, *https://filter.watch/english/2026/01/16/investigative-report-technical-breakdown-of-the-january-2026-shutdown/*: netblocks.org.

31 Arash Beidollahkhani, ”The technology of repression: Iran re-engineers its security state”, Lowy Institute, 28 januari 2026.

32 Akbarzadeh et al., ”Cyber Surveillance and Digital Authoritarianism in Iran”, 5.

33 Khabar Online, ”Monitoring all the data of Iranian users on the agenda!”, 1 juli 2023, *KhabarOnline - Monitoring all the data of Iranian users on the agenda!*

34 Filterwatch, ”A battlefield named Isfahan: targeted use of IMSI-catchers and surveillance cameras to enforce chastity and hijab law”, 17 april 2025, *https://filter.watch/english/2025/04/17/investigated-report-isfahan-targeted-with-imsi-catchers-and-surveillance-cameras/*.

35 Filterwatch, ”Nazer app: How Iran is using technology to suppress Women’s rights”, 5 januari 2024 *https://filter.watch/english/2024/01/05/nazer-app-how-iran-is-using-technology-to-suppress-womens-rights/*.

36 BBC, ”Iran using drones and apps to enforce women’s dress code”, 14 mars 2025, *https://www.bbc.com/news/articles/c0kg15jkpdeo.*

37 Iranwire, ”Iranian protester: we heard the drones first, then they started to attack us”, 14 januari 2026, *https://iranwire.com/en/features/147636-iranian-protester-we-heard-the-drones-first-then-started-to-attack-us/*.

det utbredda missnöjet mot regimens styre. Avskärmningen från omvärlden skulle sannolikt göra ett redan dåligt läge ännu sämre, men för regimen går regimsäkerhet går före allt annat och det lär fortsätta diktera vägen framåt. Det återstår förstås att se hur kriget påverkar utvecklingen såväl ekonomiskt som politiskt, men sitter regimen kvar vid makten så antyder cyberstrategin att iranierna går en mer dystopisk framtid till mötes. ■

Referenslista

Akbarzadeh Shahram, Amin Naeni, Ihsan Yilmaz and Galib Bashirov, ”Cyber surveillance and digital authoritarianism in Iran”, *Global Policy*, mars 2024.

BBC, ”Iran using drones and apps to enforce women’s dress code”, 14 mars 2025, *https://www.bbc.com/news/articles/c0kg15jkpdeo*.

Beidollahkhani, Arash, ”The technology of repression: Iran re-engineers its security state”, *Lowy Institute*, 28 januari 2026, *https://www.lowyinstitute.org/the-interpreter/technology-repression-iran-re-engineers-its-security-state*.

Belfer Center, *National Cyber Power Index 2022*, Cambridge, MA: Harvard Kennedy School (2022), *CyberProject_National Cyber Power Index 2022_v3_220922.pdf.*
Chuck Freilich, *The Iranian Cyber Threat*, INSS, Memorandum 230 (Tel Aviv: INSS, 2024).

”Cybermakt: Natur, dimensioner, komponenter och globala indikatorer”, forskningscentret vid islamiska republikens konsultativa församling, *rc.majlis.ir/fa/report/show/1841364*.

Eurepoc, Cyber incident dashboard, *https://eurepoc.eu/dashboard/*.

Filterwatch,”Total Blackout: A Technical Breakdown of the January 2026 Shutdown”, 16 januari 2026, *https://filter.watch/english/2026/16/01/investigative-report-technical-breakdown-of-the-january-2026_shutdown/*.

Filterwatch, ”A battlefield named Isfahan: targeted use of IMSI-catchers and surveillance cameras to enforce chastity and hijab law”, 17 april 2025, *https://filter.watch/english/2025/17/04/investigated-report-isfahan-targeted-with-imsi-catchers-and-surveillance-cameras/*.

Filterwatch, ”Nazer app: How Iran is using technology to suppress women’s rights”, 5 januari 2024 *https://filter.watch/english/2024/05/01/nazer-app-how-iran-is-using-technology-to-suppress-womens-rights/*.

Financial Times, ”Inside the plan to kill Ali Khamenei”, 2 mars 2026, *https://www.ft.com/content/bf998c69_ab464_fa3_aae48_f18f7387836?syn-25a6b1a6=1*

Gohdes, Anita, *Repression in the digital age – Surveillance, censorship and the dynamics of state violence*, Oxford University Press: 2024.

Haghi, Majid och Mehrdad Kargari, ”Presenting a conceptual model of security-based cyber defense of the Islamic Republic of Iran”, *Quarterly Journal of Strategic Studies of Cyberspace*, Volume 2, Issue 3, 7–32 *https://ssc.sndu.ac.ir/article_2551.html?lang=en* (hämtad oktober 2025).

HRANA News agency, ”40th Day of Protests: From Domestic Positions to Continued Arrests and Forced Confessions”, 6 februari 2026, *https://www.hra-news.org/2026/hranews/a-58002/*

Irans högsta råd för cyberrymden, ”Strategiskt dokument för cyberrymden”, 1401, جمهوري اسلامي ايران در فضاي مجازي سند راهبردي dotic.ir (hämtad oktober 2025).

Iranwire, ”Iranian protester: we heard the drones first, then they started to attack us”, 14 januari 2026, *https://iranwire.com/en/features/147636_iranian-protester-we-heard-the-drones-first-then-started-to-attack-us/*.

IRNA, ”*Supreme Council of Cyberspace, a Council to Transform Iran into a Cyber Power*”, 9 mars 2024, *Supreme Council of Cyberspace, a Council to Transform Iran into a Cyber Power - IRNA.*

Khabar Online, ”Monitoring all the data of Iranian users on the agenda!”, 1 juli 2023, *KhabarOnline - Monitoring all the data of Iranian users on the agenda!*

Majeraa Media, Intervju med Gholam-Reza Jalali, Youtube, 2025 ماجرای جنگ دوازده روزه | به روایت جواد موگویی | قسمت یازدهم | غلامرضا جلالی

Mehr News, ”What are the important emphases of the Supreme Leader on the management of cyberspace?”, 24 mars 2024 *What are the important emphasis of the Leader of the Revolution on the management of cyberspace/ Serious demands that remain on the ground - Mehr News Agency | Iran and World News | Mehr News Agency.*

Netblocks.org.

Peivast, ”Security in the age of successive attacks: why Iran is not yet ready for cyber warfare”, 29 oktober 2025. *https://peivast.com/p/246842*.

Qasemi, Mohammad, Davood Azar och Vahid Sajjadi, ”Factors Affecting the Evaluation of the Cyber Defense Power of the Islamic Republic of Iran Army”, (2022), *Warfare Study Quarterly*, vol. 4, nr. 12, (2022): 115–40 *https://www.qjws.ir/article_253853.html* (hämtad oktober 2025).

Santos, Edmarverson ”The struggle for human rights in authoritarian regimes”, *Diplomacy and Law,* u.å., *https://www.diplomacyandlaw.com/post/the-struggle-for-human-rights-in-authoritarian-regimes.*

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Tel: +46 8 5550 3000
www.foi.se