ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

El paper del ciberespai en el conflicte de l'Iran

TLP: WHITE

MARÇ 2026

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	20/04/2026	21/04/2026

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

Codi	Com es fa servir	Com es comparteix
TLP: RED	S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament.	Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP: AMBER	S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació.
TLP: GREEN	S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP: WHITE	S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a les regles i procediments establerts per a la seva difusió pública.	La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de copyright.

2. INTRODUCCIÓ

El conflicte entre els Estats Units, Israel i l'Iran no es limita al pla militar convencional, el ciberespai ha esdevingut un domini estratègic clau, on es desenvolupen operacions de sabotatge, espionatge i propaganda.

Les guerres modernes es caracteritzen per combinar operacions en ambdós plans, en allò que s'anomena guerra híbrida.

En aquest informe s'analitzaran les capacitats dels principals actors involucrats, els incidents que s'han registrat fins ara, com també els actors d'amenaça més actius.

A més, s'exposarà el grau de risc a què s'exposa Europa perquè es considera aliada dels Estats Units, tot analitzant de manera individual el cas d'Espanya per la particularitat del seu posicionament davant del conflicte.

3. EL CIBERESPAI COM A FRONT PARAL·LEL DEL CONFLICTE

El ciberespai ha esdevingut un front paral·lel molt clau en el conflicte actual de l'Orient Mitjà. Els ciberatacs acompanyen i amplifiquen els atacs convencionals.

Tot seguit, s'exposaran les principals operacions cibernètiques que han donat suport als atacs militars, la tipologia d'atacs registrats i el seu impacte pels països de l'Orient Mitjà.

3.1. Operacions cibernètiques que complementen atacs militars

Des de l'inici del conflicte, que va començar amb l'atac militar impulsat entre els Estats Units i Israel contra l'Iran i que es va denominar Operació Fúria Èpica, **s'han succeït diverses operacions cibernètiques de manera simultània i que han complementat els atacs militars inicials**.

Entre els incidents registrats i documentats cal destacar els piratejos de llocs web de notícies iranians, el compromís de l'aplicació religiosa BadeSaba, amb milions d'usuaris, o els missatges inserits en diferents plataformes iranianes instant els seus militars a rendir-se.

Aquest tipus d'operacions **s'emmarca en el concepte d'operacions psicològiques digitals (PSYOPS)**, els objectius de les quals abasten des de desmoralitzar la població o les forces armades, fins a amplificar narratives internes d'oposició al règim i, fins i tot, generar confusió durant els atacs militars.

A més, s'han registrat ciberatacs típics en aquest tipus de contextos, com ara els DDoS o aquells mitjançant els quals s'han intentat infectar els sistemes dels adversaris.

Tot seguit, s'exposa una anàlisi de la informació més rellevant sobre incidents i actors identificats durant el conflicte.

3.1.1 Tipologia d'atacs i tècniques detectades durant el conflicte

Fins ara s'han reportat un total de **886 atacs associats a 3 tipus de tècniques** principalment:

	TÈCNIQUES	Nombre d'atacs
1	DDoS	808
2	No revelat	75
3	Múltiples tècniques	2

Taula 1 – Tècniques més utilitzades en el conflicte de l'Iran

Com es pot apreciar a la taula, hi ha un **predomini dels atacs DDoS**, la qual cosa indica que fins ara s'estan duent a terme campanyes àgils d'implementar i amb finalitats principalment

disruptives o propagandístiques, que **busquen més interrompre els serveis digitals que destruir infraestructura**.

El hacktivisme, la guerra psicològica i la demostració de capacitats són presumiblement les causes principals d'aquestes tendències, cosa que també permet establir que l'activitat cibernètica registrada busca més impacte mediàtic que no pas tècnic.

3.1.2 Impacte regional de l'Orient Mitjà per països

S'han reportat un total de **886 atacs dirigits contra 14 països de l'Orient Mitjà**. La distribució dels atacs rebuts per cada país és la següent:

	ACTORS D'AMENAÇA	Nombre d'atacs
1	**Israel**	**379**
2	Kuwait	109
3	Bahrain	73
4	Jordània	64
5	Xipre	61
6	Unió dels Emirats Àrabs	60
7	Qatar	46
8	Síria	28
9	**Iran**	**26**
10	Aràbia Saudita	16
11	Líban	9
12	Oman	7
13	Iraq	6
14	Iemen	2

Taula 3 – Països de l'Orient Mitjà amb més ciberatacs rebuts en el conflicte de l'Iran

Com es pot apreciar a la taula, Israel és amb diferència el país més atacat, i concentra més del 40 % del total de ciberatacs registrats, molt per sobre de l'Iran, que ha rebut 26 ciberatacs únicament.

Aquesta asimetria s'explica per l'elevat nombre de grups hacktivistes proiranians i propalestins que han dirigit múltiples campanyes contra objectius israelians amb l'objectiu de cercar impacte mediàtic. Per contra, quant a ciberatacs contra l'Iran, amb les dades de què es consta i han estat publicades, sembla que han estat menys freqüents però molt més selectives.

3.2. Hacktivisme i actors no estatals

Com hem comentat a l'apartat anterior, un element central d'aquest conflicte cibernètic és la **participació de grups hacktivistes pro-Iran i antioccidentals**.

Aquests actors duen a terme principalment:

- Atacs DDoS
- Desfiguració web
- Filtració o robatori de dades
- Campanyes de desinformació

Molts d'aquests grups operen amb suport indirecte estatal, encara que mantinguin una aparença d'independència.

3.2.1 Principals actors d'amenaça i grups identificats

Els actors d'amenaça més actius durant el conflicte són majoritàriament grups hacktivistes, i aquestes dades **reforcen la idea que el ciberespai l'utilitzen grups intermediaris o hacktivistes ideològics** i no és casualitat, perquè permet que els Estats externalitzin operacions ofensives, mantinguin negociacions en paral·lel i augmentin la pressió sobre els adversaris sense escalar militarment.

	ACTORS D'AMENAÇA	Nombre d'atacs
1	NoName057(16)	129
2	313 Team	96
3	Conquerors Electronic Army	83
4	DieNet	64

Taula 4 - Actors d'amenaça amb més atacs en el conflicte de l'Iran

A la taula principalment apareixen grups que es podrien considerar de l'ecosistema hacktivista pro-Iran o antioccidental. NoName057(16), el grup d'origen prorús lidera l'activitat amb 128 atacs, seguit pel 313 Team amb 96 atacs, Conquerors Electronic Army amb 83 atacs i finalment DieNet amb 64 atacs. Els grups, com ja hem indicat anteriorment, es caracteritzen principalment per l'ús d'atacs DDoS, amb finalitats disruptives i propagandístiques.

4. CAPACITATS DELS PROTAGONISTES PRINCIPALS

Cada país involucrat en aquesta guerra presenta capacitats cibernètiques molt diferents pel que fa a nivell tècnic, estratègic i de recursos.

A continuació, s'exposaran les capacitats cibernètiques de l'Iran, els Estats Units i Israel, amb les diferents estratègies, tàctiques i noves tècniques.

4.1. Iran

L'Iran ha invertit durant anys en capacitats de ciberguerra com a resposta asimètrica a la seva inferioritat militar convencional. Es caracteritza principalment pels elements que s'enumeren tot seguit.

4.1.1 Estratègia asimètrica

L'Iran fa servir el ciberespai per compensar la seva inferioritat tecnològica davant dels Estats Units i les seves limitacions en aviació o armament avançat. L'ús de ciberatacs forma part d'un patró de respostes no convencionals davant d'agressions militars.

4.1.2 Tàctiques habituals

Les operacions iranianes solen centrar-se majoritàriament en atacs DDoS, encara que les tàctiques de programari de segrest, espionatge industrial i sabotatge d'infraestructures també s'han vist entre les tècniques d'atac emprades.

4.1.2 Noves tècniques observades al conflicte

Durant la guerra actual es van detectar intents d'hackeig massiu de càmeres de seguretat a Israel i països del Golf per avaluar els danys d'atacs amb míssils.

Això demostra un ús tàctic del ciberespai per generar intel·ligència en temps real, avaluació de danys i planificació de nous atacs.

4.2. Estats Units

Els Estats Units posseeixen una de les capacitats cibernètiques més avançades del món. Les seves operacions se solen centrar en sabotatge d'infraestructures militars, atacs a sistemes de defensa i operacions d'intel·ligència.

El país considera els ciberatacs dels Estats rivals com a accions hostils equivalents a operacions militars, cosa que ha impulsat doctrines de resposta activa al ciberespai.

Històricament, Washington ha utilitzat els ciberatacs com a alternativa als atacs cinètics per evitar l'escalada militar.

4.3. Israel

Israel és considerat un dels actors més sofisticats en ciberguerra. Les seves capacitats es basen en intel·ligència tecnològica avançada, forta cooperació entre el sector militar i les empreses de ciberseguretat i unitats militars especialitzades.

Israel combina operacions cibernètiques amb operacions especials dins del territori enemic, cosa que ha estat clau en atacs contra infraestructures iranianes, fins i tot en conflictes que ja es van produir en el passat.

5. OBJECTIUS PRIORITARIS DE LA CIBERGUERRA

A la ciberguerra s'ataquen objectius concrets segons el seu valor estratègic. En aquest conflicte destaquen diversos sectors pel seu impacte militar i econòmic.

A continuació, es detallen els objectius prioritaris del conflicte, amb més èmfasi en les infraestructures crítiques, el sector financer, la infraestructura militar i els sectors més atacats.

5.1. Infraestructures crítiques

Que compten amb **sistemes especialment vulnerables perquè depenen de tecnologies industrials connectades (ICS/SCADA)**. Entre els sectors principals que conformen aquest tipus d'infraestructures cal destacar:

- Sector energètic.
- Aigua.
- Transport.
- Telecomunicacions.

5.2. Sector financer

De fet, després de l'inici de la guerra, **bancs nord-americans es van situar en alerta màxima davant de possibles ciberatacs iranians**.

A més, històricament ja s'han registrat al passat campanyes DDoS iranianes contra bancs nord-americans. Els principals motius són:

- Impacte econòmic immediat.
- Interrupció o alteració dels mercats financers.
- Pèrdua de confiança.

5.3. Infraestructura militar i logística

El ciberespai també s'usa per a:

- Interrompre comunicacions militars
- Recopilar intel·ligència

- Sabotejar logística.

5.4. Sectors més atacats al conflicte actual

Amb les dades més recents que s'expliquen des que va començar la guerra, els sectors més atacats han estat els que es mostren a la taula següent:

	SECTORS	Nombre d'atacs
1	Governamental	410
2	Financer / Assegurador	88
3	Mitjans de comunicació / Notícies / Multimèdia	71
4	Organitzacions (ONG, Fundacions, etc.)	51
5	Transport / Emmagatzematge / Logística	38

Taula 4 - Sectors amb més atacs en el conflicte de l'Iran

Aquestes dades confirmen diverses tendències importants:

- **Prioritat al sector governamental i militar**: el fet que gairebé la meitat dels atacs (410) s'adrecin a organismes governamentals o militars demostra que:
  - El ciberespai s'utilitza com a extensió directa del camp de batalla.
  - Es busca afectar capacitats de comandament, control i intel·ligència
- **Interès en el sector financer/assegurador, amb 88 atacs**: que aparegui en segon lloc reforça la idea que els actors del conflicte busquen generar inestabilitat econòmica, afectar la confiança en els sistemes financers i provocar efectes indirectes a l'economia.
- **Importància del sector mediàtic, amb 71 atacs**: la guerra informativa o mitjançant la desinformació és un altre dels pilars que es controlen des del ciberespai i des d'on es pot **exercir una gran influència, ja no directament sobre els estats, sinó sobre la població general i la seva opinió sobre el conflicte**. Les campanyes per manipular narratives, controlar el flux de la informació i influir en l'opinió pública estan directament relacionades amb operacions de propaganda digital i desinformació que caracteritzen la guerra híbrida moderna.

6. EL PAPER D'EUROPA EN EL CONFLICTE

Europa no és un actor directe del conflicte, però es pot veure afectada pels atacs indirectes o col·laterals.

L'agència europea de policia, Europol, ha advertit que el conflicte podria provocar un augment de ciberatacs a la Unió Europea, juntament amb amenaces terroristes i campanyes de desinformació.

Les motivacions principals apunten a represàlies contra aliats occidentals, atacs d'oportunitat i operacions de propaganda.

6.1. Possible impacte a Espanya

6.1.1 Probabilitat d'esdevenir objectiu directe

Espanya representa menys risc d'atac directe per diverses raons com:

- Postura política crítica amb la guerra.
- Menor implicació militar directa.
- Menys simbolisme estratègic davant dels EUA que davant d'Israel.

Tot i això, no es pot descartar que organitzacions espanyoles amb presència o entitats internacionals amb presència a Espanya puguin ser objectiu de campanyes cibernètiques associades al conflicte de l'Iran.

6.1.2 Sectors espanyols de més risc potencial

6.1.2.1 Sector energètic

S'entén que hi ha un risc més gran en aquest àmbit **pel fet que les infraestructures energètiques conformen un ecosistema que es connecta digitalment**, a més de la dependència que hi ha del mercat global de l'energia.

La tipologia d'accions que representen més risc i que es podrien esperar en un escenari com l'actual serien les relacionades amb sabotatges a xarxes elèctriques, intrusions en sistemes d'empreses energètiques o espionatge industrial.

6.1.2.2 Sector financer

La banca espanyola, com passa amb la resta de l'ecosistema financer a nivell mundial, podria veure's afectada per campanyes de DDoS, programari de segrest o robatori de dades.

El motiu principal es correspondria amb la **implicació d'actors estatals a les campanyes cibernètiques per generar un impacte econòmic indirecte** en un país que, simplement per formar part d'Europa, sigui considerat per l'Iran com a aliat occidental.

6.1.2.3 Indústria i manufactura

Les empreses industrials espanyoles podrien ser objectiu d'accions relacionades amb l'espionatge industrial o sabotatge a sistemes OT. Els sectors de defensa, l'aeroespacial, el de l'energia o el tecnològic es consideren els més susceptibles de veure's afectats per ciberatacs.

6.1.2.4 Transport i logística

En aquest sector cal destacar el transport marítim i portuari per la sensibilitat que s'està percebent davant el conflicte a causa de la seva implicació en el comerç global, que contempla les rutes energètiques.

Els atacs a sistemes logístics o les interrupcions de servei són les amenaces principals que cal tenir en compte pels precedents que hi ha derivats d'altres conflictes.

6.2. Riscos principals per a les entitats espanyoles

6.2.1 Atacs de baixa criticitat

Entre els que destacarien:

- Campanyes DDoS.
- Desfiguració.
- Propaganda.

6.2.2 Campanyes de desinformació

Amb l'objectiu de polaritzar l'opinió pública sobre el conflicte.

6.2.3 Atacs indirectes

Com es comentava anteriorment, les organitzacions espanyoles amb seus als Estats Units, Israel o l'Orient Mitjà, com també organitzacions d'aquestes regions amb seu a Espanya es podrien veure afectades per atacs cibernètics.

7. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.