ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Ciberamenaces a les infraestructures crítiques

TLP: WHITE

MAIG 2025

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	29/05/2025	02/06/2025

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA **4**
2. INTRODUCCIÓ **5**
3. INFRAESTRUCTURES CRÍTIQUES **6**
3.1. Sector energètic 6
3.2. Sector sanitari 6
3.3. Sector financer 6
3.4. Sector de l'aigua i sanejament 7
3.5. Sector alimentari 7
3.6. Sector del transport 7
3.7. Sector de les telecomunicacions 7
3.8. Govern i administracions públiques 7
3.9. Defensa/militar 8
4. UN CLIC PER ALTERAR L'ORDRE DE LA NACIÓ **9**
5. PRINCIPALS TIPUS DE CIBERAMENACES A INFRAESTRUCTURES CRÍTIQUES **11**
5.1. Vectors d'atac més utilitzats 11
5.2. Tipologia dels ciberatacs més recurrents 13
6. ELS ACTORS D'AMENAÇA **15**
6.1. Ciberdelinqüents motivats pel lucre econòmic 15
6.2. Grups cibercriminals d'Estat (APT) 15
6.3. Hacktivistes: ciberatacs per motivació ideològica 16
6.4. Actors finançat per organitzacions terroristes 16
7. CONCLUSIONS I RECOMANACIONS **18**
8. CLÀUSULA DE CONFIDENCIALITAT **20**

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

L'any 2010 va suposar un punt d'inflexió en la percepció de la ciberseguretat industrial quan es va atacar la planta nuclear de Natanz, a l'Iran, amb el codi maliciós Stuxnet. Per primera vegada es va tenir consciència sobre l'impacte que podia tenir una acció cibernètica al món físic: un ciberatac havia estat capaç de paralitzar i danyar les centrifugadores per enriquir urani, cosa que suposava un perill greu.

Probablement, quan es parla d'una catàstrofe nuclear, es fa una associació d'idees amb el que va passar a Hiroshima i Nagasaki i, per això, tots ens podem fer una idea aproximada de quin podia haver estat el pitjor dels escenaris si no s'arriba a detectar Stuxnet a temps. Deu anys abans, però, ja s'havia produït la primera acció disruptiva mitjançant la manipulació de sistemes industrials.

L'any 2000, la planta de tractament d'aigües de Maroochy, a Queensland, Austràlia, va ser víctima d'un dels primers ciberatacs documentats contra una infraestructura crítica. L'atac va ser perpetrat per un exempleat que tenia un gran coneixement dels sistemes industrials de la planta. Amb l'ús d'un portàtil i un mòdem, l'exempleat va aconseguir accedir de manera remota al sistema de control industrial (SCADA) i va manipular vàlvules i bombes, cosa que va provocar l'alliberament de centenars de milers de litres d'aigües residuals a parcs, rius i zones urbanes, incloses comissaries de policia i habitatges.

Potser aquest primer incident no fa que s'associï un ciberatac a un escenari tan catastrofista com el que va passar a Natanz, però tots dos donen una mostra de la capacitat que té el món digital de generar danys importants al món real i, per tant, a la societat.

Des dels incidents comentats han transcorregut molts anys, és a dir, els coneixements, les tècniques i la capacitat dels atacants han evolucionat a nivells als quals, aleshores, seria gairebé impossible imaginar-nos-els. Internet pot esdevenir una arma efectiva i les infraestructures crítiques en un objectiu molt cobejat pels actors d'amenaça, atès que una única acció d'èxit podria arribar a tenir conseqüències inimaginables.

De fet, l'apagada històrica que es va viure a Espanya el 28 d'abril passat, va fer que totes les mirades s'adrecessin a l'ecosistema digital. La possibilitat que hagués estat el resultat d'un ciberatac va ser una de les hipòtesis principals que es van estudiar des d'un inici. Encara no se n'han confirmat les causes, però el simple fet que es valori l'opció que hagi estat la conseqüència d'un ciberatac ens diu molt de l'impacte que un incident cibernètic pot tenir al món físic i com pot arribar a afectar un país.

3. INFRAESTRUCTURES CRÍTIQUES

La protecció de les infraestructures crítiques és una de les prioritats estratègiques tant a nivell mundial, com europeu. De fet, **les diferents normatives i directrius que s'impulsen estan molt focalitzades a millorar la capacitat de resiliència de sectors clau** com ara l'energia, les comunicacions, el transport o la salut.

Per motius evidents de seguretat no hi ha un registre públic a nivell mundial, continental o nacional mitjançant el qual es comptabilitzin el total d'infraestructures crítiques, ni cap mena de mètrica estandarditzada. De fet, cada país és qui s'encarrega de determinar què s'ha de considerar infraestructura crítica i què no.

En el cas d'Andorra, se sap que té més de 100 infraestructures crítiques reconegudes oficialment, però no hi ha un llistat públic que permeti conèixer quins són.

En termes generals i a grans trets, es consideren infraestructures crítiques els sectors següents: energètic, sanitari, financer, aigua/sanejament, alimentari, transport, telecomunicacions, govern/AP, i defensa/militar.

3.1. Sector energètic

Inclou empreses de generació, distribució i comercialització d'energia com ara les elèctriques, les de gas i petroli. Aquesta indústria és essencial perquè sense energia no poden operar altres sectors, que abasten, per exemple, des d'hospitals fins a fàbriques. Les infraestructures com les plantes de producció o les xarxes de distribució són fonamentals i, si es produeix qualsevol esdeveniment que afectés la seva operativa normal, podria deixar milions de persones sense electricitat o gas, cosa que afectaria la vida diària i l'economia.

3.2. Sector sanitari

Inclou hospitals, centres de salut, entitats reguladores i proveïdors de serveis mèdics. Aquests organismes gestionen dades delicades de pacients i asseguren l'accés a atenció mèdica, medicaments i tecnologies sanitàries. Aquesta indústria és tan sensible que qualsevol acció disruptiva amb un impacte significatiu posa en risc vides humanes.

3.3. Sector financer

Bancs, borses de valors, asseguradores i empreses de pagaments electrònics gestionen l'estabilitat econòmica nacional i, per extensió, la global. Les infraestructures, com ara les xarxes de transaccions i els sistemes de gestió de comptes, són essencials per al funcionament diari de l'economia. Si es paralitzés el flux de diners, l'escenari de pèrdues econòmiques que es plantejaria seria molt complex d'abordar-se.

3.4. Sector de l'aigua i sanejament

El formen les empreses encarregades de la distribució de l'aigua potable, el tractament de les aigües residuals i les autoritats locals encarregades del sanejament. Aquests serveis són imprescindibles per a la salut pública. Qualsevol interrupció en el subministrament de l'aigua o en el tractament adequat de les aigües residuals pot generar una crisi fins i tot sanitària.

3.5. Sector alimentari

Inclou productors agrícoles, ramaders, processadors d'aliments, distribuïdors i organismes de control. La cadena de subministrament d'aliments és delicada i, si s'interrompés qualsevol dels elements que l'estructuren, provocaria que l'escassetat o l'augment de preus fessin col·lapsar el sistema.

3.6. Sector del transport

Inclou aerolínies, empreses de trens, metro, autobusos, operadors de ports i aeroports, i les autoritats de trànsit. Aquests actors són responsables de la mobilitat de les persones i les mercaderies. Interrompre les rutes de transport o, en definitiva, generar caos en el trànsit, afectaria directament tant l'economia com la vida quotidiana.

3.7. Sector de les telecomunicacions

Inclouen empreses que ofereixen serveis de telefonia mòbil, Internet i televisió per cable. Aquestes xarxes permeten la comunicació global i la connectivitat, i faciliten tota mena d'interaccions, des de les personals fins a les empresarials. L'apagada que es va viure a Espanya recentment va demostrar com pot afectar el funcionament correcte d'un país: famílies sense poder localitzar-se o empreses que van haver d'aturar la seva producció o deixar d'oferir els seus serveis.

3.8. Govern i administracions públiques

Engloba des de les autoritats locals fins als organismes nacionals encarregats de serveis essencials com ara la seguretat, la justícia i l'educació. El seu paper és tan rellevant que el caos social, polític o econòmic són els riscos principals als quals s'enfrontaria si es quedés paralitzat.

3.9. Defensa/militar

Està compost per les forces armades, les agències d'intel·ligència i les empreses que subministren tecnologies militars. Aquest sector s'encarrega de la seguretat nacional i la protecció davant d'amenaces externes i internes. Un incident en aquest sector pot afeblir les capacitats defensives d'un país, i posar en perill en darrer terme fins i tot la seva sobirania.

4. UN CLIC PER ALTERAR L'ORDRE DE LA NACIÓ

Històricament, el terrorisme, els conflictes armats, els actes de sabotatge, les vagues o les protestes socials eren les amenaces principals a l'estabilitat d'una nació. No obstant això**, Internet ha permès eliminar tota barrera física per aconseguir impactar en el funcionament normal d'un país**.

Mentre les amenaces tradicionals requerien presència física o accions directes sobre el terreny, la digitalització i l'ús massiu d'Internet han permès que actors remots, fins i tot des d'altres països, puguin atacar infraestructures crítiques sense necessitat de desplaçar-s'hi, cosa que augmenta la superfície de risc i la dificultat de defensa.

Un exemple clar de com les ciberamenaces poden influir en el funcionament d'un país són les campanyes de desinformació, com les que han afectat eleccions presidencials a diverses parts del món. Aquestes campanyes, que sovint es basen en la creació i la difusió de notícies enganyoses, són relativament senzilles, però extremadament eficaces. A través de les xarxes socials i les plataformes digitals, els actors maliciosos poden difondre informació errònia, **sembrar desconfiança en els processos democràtics, manipular l'opinió pública i, en molts casos, alterar el resultat d'una elecció**. El cas de **les eleccions presidencials als Estats Units el 2016 és un dels més notoris**, on es va al·legar que agents externs van utilitzar bots i comptes falsos per disseminar notícies falses, generar polarització i manipular el vot de milions de persones.

Tot i això, no totes les amenaces cibernètiques són tan visibles o fàcils de detectar. **També hi ha atacs més complexos, en els quals es fan servir eines avançades com ara codi maliciós (*malware*) per accedir, alterar o destruir infraestructures crítiques**. En aquesta mena d'atacs, l'objectiu no és només manipular l'opinió pública, sinó interferir directament en els sistemes que mantenen el funcionament bàsic d'un país, com ara el subministrament d'energia, les telecomunicacions, la gestió de l'aigua o el sistema bancari.

L'atac el 2015 a Ukrenergo, la companyia nacional d'electricitat d'Ucraïna, és un exemple alarmant de com un ciberatac pot deixar un país sense electricitat, i afectar no només la vida diària de milions de persones, sinó també les operacions econòmiques i la seguretat nacional. Aquest atac, que es va basar en la infecció de sistemes informàtics amb codi maliciós, demostra com les infraestructures crítiques poden ser l'objectiu de ciberatacs dissenyats per provocar caos i disrupció.

Un altre cas rellevant és **l'atac que es va produir el 2017 mitjançant el programari de segrest WannaCry, que va afectar hospitals, empreses i organismes governamentals a tot el món**. Al Regne Unit, el Servei Nacional de Salut (NHS) va patir paràlisi en els seus sistemes informàtics, fet que va comportar la cancel·lació de cites mèdiques i emergències, i va afectar l'atenció a milers de pacients. Tot i que el propòsit principal de WannaCry era obtenir guanys a través del pagament de rescats, les conseqüències per a la infraestructura pública i la vida de les persones van ser devastadores. Aquest tipus d'atacs demostra com, mitjançant l'ús de programari maliciós, es pot generar una interrupció massiva dels serveis que són vitals per a la salut i el benestar d'una nació.

A més dels atacs a infraestructures crítiques, els ciberatacs es poden centrar a desestabilitzar les relacions internacionals o soscavar la confiança en els governs i les seves capacitats. Els atacs dirigits a sistemes de comunicació, com els que afecten plataformes de votació electrònica o les bases de dades governamentals, poden comprometre la integritat de les eleccions o la legitimitat de les decisions polítiques. **El 2017, durant les eleccions a França, es va produir un atac massiu de pesca adreçat als sistemes de correu electrònic dels candidats**, cosa que va posar en perill la seguretat de la informació confidencial de les seves campanyes. Si bé aquest tipus d'atacs no va ser devastador en termes de danys immediats, sí que va servir per mostrar com un petit atac cibernètic pot posar en perill la seguretat política d'un país.

El fet preocupant de tot això és que **les ciberamenaces no només són un risc immediat, sinó que les seves conseqüències a llarg termini poden ser devastadores**. No es tracta únicament de la pèrdua d'informació o de la interrupció temporal de serveis; les repercussions poden afectar la confiança de la ciutadania a les institucions governamentals, l'estabilitat econòmica i les relacions internacionals. **Un atac ben coordinat que afecti les infraestructures crítiques d'un país pot generar un efecte dòmino**: des de la interrupció completa dels serveis essencials fins a la manipulació de l'opinió pública, passant per l'afebliment de la confiança en la democràcia i l'augment de la polarització social.

5. PRINCIPALS TIPUS DE CIBERAMENACES A INFRAESTRUCTURES CRÍTIQUES

Com ja hem exposat, un simple clic maliciós en un sistema adequat pot desencadenar conseqüències catastròfiques, com ja ha quedat demostrat en nombrosos incidents al llarg dels anys. Aquests ciberatacs van des de les manipulacions d'informació, com ara campanyes de desinformació, fins a atacs complexos dirigits a sistemes de control d'infraestructures essencials.

Les xifres més recents reflecteixen un creixement notable tant a la freqüència com a la sofisticació de les amenaces, amb variacions clares entre sectors. **El primer trimestre del 2025, la mitjana global de ciberatacs setmanals per organització va arribar als 1.925**, cosa que suposa un augment del **47 %** respecte del mateix període de l'any anterior. Si analitzem la distribució sectorial, **el sector educatiu/recerca lidera amb una mitjana de 4.484 atacs setmanals per empresa, seguit pel sector govern/militar amb 2.678 i telecomunicacions amb 2.664 atacs setmanals**, aquest últim amb un increment interanual del **94 %**.

En l'àmbit europeu, els atacs a sectors crítics presenten la proporció següent sobre el total d'incidents gestionats: el sector financer i tributari representa el **25,42 %** dels incidents, el transport el **25 %**, l'energia el **22,08 %**, les tecnologies de la informació i comunicació (TIC) el **18,33 %** i el sector aigua/sanejament el **4,58 %**.

5.1. Vectors d'atac més utilitzats

Els vectors d'atac són les vies a través de les quals els atacants aconsegueixen infiltrar-se a les infraestructures crítiques per comprometre els seus sistemes. Aquests vectors es basen en tècniques específiques que exploten vulnerabilitats o el comportament humà.

Una de les principals amenaces a les quals s'enfronten les infraestructures crítiques és el programari de segrest, un tipus d'atac que es basa a xifrar les dades i els sistemes de la víctima, i exigir un rescat per l'alliberament de la informació. Aquest tipus de ciberatac ha estat **particularment efectiu en sectors com l'energètic i el sanitari**, on les dades són extremadament delicades i la seva pèrdua o interrupció pot causar un dany significatiu. **El 2024, aproximadament la meitat dels atacs de programari de segrest van ser dirigits a infraestructures crítiques, amb un increment notable respecte a anys anteriors**.

Per exemple, el sector energètic va patir múltiples incidents que van afectar plantes d'energia a diversos països, fet que va comportar pèrdues milionàries. Segons les dades del 2024, **els costos globals del programari de segrest van assolir els 20.000 milions de dòlars, i es preveu que el 2025 aquesta xifra superi els 30.000 milions**. Les organitzacions, en enfrontar-se a la paralització dels seus sistemes, sovint es veuen obligades a pagar els rescats. De fet, **el 60 % de les empreses que pateixen atacs de programari de segrest acaben pagant la quantitat exigida** per recuperar les seves dades. Això no només té un impacte econòmic directe, sinó també de reputació i, en alguns casos, operatiu, especialment en sectors com el de la salut, on un atac pot afectar l'atenció de milers de pacients.

Una altra amenaça emergent que ha esdevingut forta en els darrers anys són els atacs a la cadena de subministrament. Aquest tipus de ciberatac explota la confiança que hi ha entre

una organització i els seus proveïdors, o entre diferents empreses que depenen de sistemes compartits. En comprometre un proveïdor de programari o maquinari, els atacants poden infiltrar-se a les xarxes internes dels seus clients, accedir a informació delicada o fins i tot prendre el control de sistemes crítics.

El 2024, els atacs a la cadena de subministrament **van representar un 30 % de tots els ciberatacs registrats a infraestructures crítiques**. Aquests atacs són especialment perillosos perquè poden obrir múltiples portes d'entrada a sistemes que normalment estarien protegits. Un exemple notori va ser l'atac al proveïdor de programari SolarWinds, que el 2020 va comprometre agències governamentals i empreses privades de gran rellevància. Tot i que l'atac va ser detectat a finals de l'any 2020, les repercussions es van continuar patint el 2024, amb un augment en els esforços dels ciberdelinqüents per atacar proveïdors en sectors com ara l'energètic, el tecnològic i el financer.

El 2025, la **Cybersecurity & Infrastructure Security Agency (**l'**Agència de seguretat cibernètica i d'infraestructures, CISA)** dels Estats Units preveu que els atacs dirigits a proveïdors d'infraestructures crítiques augmentin almenys en un **35 %**, amb un èmfasi especial en les empreses que proporcionen serveis de control remot a plantes d'energia o d'aigua, cosa que podria afectar milions de persones a nivell global.

La pesca i l'enginyeria social continuen sent vectors d'atac recurrents per la seva efectivitat i facilitat d'execució. Tot i que són tàctiques més antigues, els atacants perfeccionen constantment les seves tècniques per enganyar els empleats de les organitzacions i obtenir accés a xarxes internes o credencials d'accés. **El 2024, els atacs de pesca van representar més del 60 % de les violacions de seguretat en infraestructures crítiques**, d'acord amb l'Informe de Ciberseguretat Global 2024 d'IBM.

Aquests atacs són comuns en sectors com la salut i les finances, on els atacants suplanten identitats d'empreses o persones clau per robar informació confidencial. Al sector sanitari, per exemple, els hospitals han estat víctimes d'atacs de pesca (*phishing*) que van comprometre dades de pacients, cosa que no només genera pèrdues econòmiques sinó també un dany significatiu a la confiança pública. El 2025, s'espera que els atacs d'enginyeria social continuïn sent una de les principals portes d'entrada per als cibercriminals, atès que les tècniques d'engany estan esdevenint cada cop més sofisticades, cosa que en dificulta la detecció.

Finalment, **les vulnerabilitats de dia zero (zero-day) continuen sent un dels vectors més perillosos i difícils de defensar**. Aquestes són vulnerabilitats en programari o maquinari que són desconegudes per als fabricants i, per tant, no tenen pedaços disponibles en el moment que els atacants les descobreixen. Els atacants poden explotar aquestes vulnerabilitats per obtenir accés a sistemes crítics sense que siguin detectats.

El 2024, es van detectar i informar múltiples incidents en què els atacants van aprofitar vulnerabilitats de dia zero en sistemes de control industrial, que van afectar plantes d'energia i sistemes de distribució d'aigua. Aquests atacs no només són difícils de prevenir a causa de la manca de pedaços, sinó que, en molts casos, es desenvolupen de manera sigil·losa per evitar ser detectats durant mesos, cosa que pot tenir conseqüències devastadores a llarg termini. El 2025, **s'estima que els explotadors de dia zero augmentaran un 20 %**, a mesura que els atacants perfeccionen les seves tècniques i es dirigeixen a tecnologies emergents, com ara la intel·ligència artificial aplicada a la gestió d'infraestructures crítiques.

5.2. Tipologia dels ciberatacs més recurrents

Un cop compresos els vectors d'atac, és important abordar les tipologies o les formes dels atacs que es duen a terme per comprometre les infraestructures crítiques. Aquestes tipologies fan referència als mètodes específics que els ciberdelinqüents empren per fer l'atac un cop han identificat el vector d'accés adequat.

Si hi ha un tipus d'**atac que té un impacte especial, aquest atac és el programari de segrest**. El 2024, **el 50 % dels atacs de programari de segrest van ser dirigits a infraestructures crítiques**, i les organitzacions del sector energètic van ser les més afectades. A més de la xifra de les dades, els atacants també roben informació confidencial, cosa que augmenta les pressions sobre la víctima perquè pagui el rescat.

El **programari de segrest com a servei** també ha emergit com un model comú, on els atacants lloguen el programari de segrest a altres entitats, cosa que fa que aquest tipus d'atacs sigui més accessible i freqüent.

Tot seguit, els **atacs DDoS** són una altra de les amenaces principals que poden interrompre serveis crítics, especialment en xarxes de telecomunicacions o sistemes de monitoratge industrial. **El 2024, els atacs DDoS van ser responsables de 10 % de les interrupcions en infraestructures crítiques**, amb *botnets* cada cop més grans i sofisticades. Aquests atacs, encara que generalment són de curt termini, tenen un cost econòmic alt, perquè interrompen l'accés a serveis essencials.

Els codis maliciosos adreçats a sistemes de control industrial (ICS) són una altra tipologia de ciberamenaça especialitzada a comprometre les infraestructures crítiques. La seva funció és deshabilitar operacions industrials, robar dades de processos o fins i tot causar danys físics als equips. **El 2024, es van observar diversos incidents en els quals el codi maliciós ICS va afectar plantes d'energia i sistemes de distribució d'aigua, i va comprometre no només l'operació, sinó també la seguretat pública**. Stuxnet continua sent el cas més emblemàtic d'aquest tipus d'atac, però els atacs de codi maliciós a ICS són cada vegada més freqüents.

Els atacs MITM (man-in-the-middle) també són una altra de les amenaces més recurrents. Aquest tipus d'atac és especialment perillós quan els atacants manipulen les ordres enviades a sistemes de control industrial o xarxes de telecomunicacions. **El 2024, la CISA va registrar diversos incidents en què els atacants van interferir en les comunicacions de plataformes energètiques i sistemes de telecomunicacions, cosa que va causar interrupcions i vulnerabilitats potencials en els sistemes de seguretat**.

Per acabar, les infraestructures crítiques estan molt exposades a l'espionatge cibernètic. El seu objectiu pot ser el robatori d'informació confidencial o estratègica d'una organització amb finalitat intel·ligència econòmica o geopolítica. **El 2024, els sectors d'energia i salut van ser especialment vulnerables**, amb atacs que no sols buscaven accedir a dades financeres, sinó també a projectes de recerca o propietat intel·lectual. Aquest tipus d'atacs s'intensifiquen amb l'ús de programari maliciós avançat i tècniques d'enginyeria social, i poden ocasionar conseqüències greus per a la seguretat nacional o per a la competitivitat d'una empresa en mercats globals.

6. ELS ACTORS D'AMENAÇA

Els actors d'amenaça que dirigeixen ciberatacs a infraestructures crítiques són diversos, amb motivacions que van des d'interessos financers fins a objectius geopolítics i estratègics. Aquests actors utilitzen tècniques sofisticades, i la seva capacitat per penetrar xarxes i sistemes essencials posa en risc no només l'estabilitat de les organitzacions atacades, sinó també la seguretat de sectors clau com l'energia, les telecomunicacions, el transport i la sanitat.

El 2024 i el 2025, les amenaces provinents de diferents tipus d'actors han mostrat un increment en freqüència, complexitat i efectivitat. A continuació, s'exposa una anàlisi detallada dels actors d'amenaça principals, les motivacions i els objectius que persegueixen en atacar les infraestructures crítiques.

6.1. Ciberdelinqüents motivats pel lucre econòmic

Els ciberdelinqüents continuen essent els **actors més comuns en ciberatacs a infraestructures crítiques**. **La motivació principal d'aquests actors és el benefici econòmic**. Sovint, fan servir tàctiques com ara el programari de segrest, la pesca, o les estafes en línia per obtenir diners ràpids d'organitzacions compromeses.

A més del programari de segrest, els ciberdelinqüents també recorren a tècniques com ara el frau financer, la venda de dades robades (com ara credencials d'accés i dades personals) i l'exfiltració d'informació confidencial. **El 2024, els cibercriminals van aconseguir obtenir més de 18.000 milions de dòlars de guanys a través d'activitats relacionades amb el programari de segrest i els fraus en línia**, segons el Centre de Recerca de Ciberseguretat de l'ONU.

Els actors d'aquestes amenaces solen ser **grups altament organitzats, que sovint operen amb infraestructura global, cosa que els permet llançar atacs coordinats i dirigir-los a múltiples sectors crítics alhora**. Fan servir **el programari de segrest com a servei**, cosa que facilita la participació d'actors menys tècnics a l'atac, i així expandeixen la quantitat dels atacs dirigits a infraestructures crítiques. Les motivacions d'aquests actors solen centrar-se en el robatori de diners, el xantatge econòmic o la venda d'informació confidencial en els mercats foscos.

6.2. Grups cibercriminals d'Estat (APT)

Els grups **cibercriminals patrocinats per estats representen una de les amenaces més sofisticades i perilloses per a les infraestructures crítiques**. Aquests actors, coneguts com a APT (Amenaces persistents avançades), estan generalment **vinculats a governs que busquen assolir objectius geopolítics, econòmics o estratègics**. Aquests grups no només busquen obtenir informació delicada, sinó que també estan enfocats a desestabilitzar o desorganitzar infraestructures clau a l'enemic. Les APT tenen un **objectiu a llarg termini: infiltrar-se a les xarxes durant períodes llargs sense ser detectats, per tal de robar informació o manipular les operacions**.

El **APT33**, vinculat a l'Iran, i el **APT29**, que es creu que està patrocinat pel govern rus, són exemples d'actors que han dirigit ciberatacs a infraestructures crítiques. **El 2024, el 30 % dels atacs dirigits a infraestructures crítiques van ser atribuïbles a grups patrocinats per estats**.

Aquestes organitzacions no només ataquen per tal de robar informació, sinó també per interrompre o perjudicar les capacitats operatives dels enemics, i creen una vulnerabilitat estratègica en sectors vitals com ara l'energètic, el de comunicacions i el dels sistemes financers.

Els objectius darrere dels atacs dels actors estatals poden ser força variats. Des d'espionatge cibernètic i robatori de propietat intel·lectual fins a sabotatge d'infraestructures clau o desestabilització econòmica. Per exemple, els atacs a plantes nuclears o xarxes elèctriques poden ser part d'una estratègia per deshabilitar la capacitat operativa d'un país enemic i afectar-ne la seguretat nacional i l'economia. El 2024 es va observar un augment del 25 % en el nombre d'atacs APT dirigits a infraestructures crítiques comparat amb el 2023, amb un augment significatiu en atacs a sistemes de control industrial i plantes energètiques.

6.3. Hacktivistes: ciberatacs per motivació ideològica

El hacktivisme és un altre tipus d'actor que **ha guanyat protagonisme en els darrers anys**. Els hacktivistes són ciberactivistes que llancen ciberatacs **amb l'objectiu de promoure causes socials, polítiques o ideològiques**, més que per beneficis econòmics o estratègics. Sovint, els seus atacs són reivindicatius, busquen visibilitat per a la seva causa i volen desestabilitzar els sistemes associats a allò que consideren injustícies o abusos de poder.

El 2024, els hacktivistes van fer un 10 % dels atacs a infraestructures crítiques. Els seus objectius no solen ser tan destructius com els d'altres actors, però el seu impacte en la reputació i la credibilitat de les organitzacions atacades pot ser greu. Un exemple recent va ser l'atac als sistemes de control de plantes d'energia el 2024, dut a terme per grups de hacktivistes que s'oposen a l'explotació dels recursos naturals. En aquests casos, els hacktivistes apunten a interrompre operacions, fer públiques certes dades delicades o crear desestabilització mediàtica per generar consciència sobre les causes.

Solen utilitzar DDoS (denegació de servei distribuït) per generar interrupcions, o fins i tot vulnerabilitats de programari per filtrar informació confidencial, i fer servir els mitjans de comunicació per difondre els missatges.

6.4. Actors finançat per organitzacions terroristes

Un altre tipus d'actor que ha anat guanyant terreny en els darrers anys són els **grups terroristes que fan servir ciberatacs com una forma de lluitar contra governs o societats que perceben com els seus enemics**. El 2024, els atacs cibernètics associats a grups terroristes van ser més sofisticats i focalitzats, especialment després que algunes organitzacions terroristes adoptessin el **programari de segrest i la pesca com a eines per obtenir finançament i difondre la seva propaganda**.

El 2024, **la ciberseguretat global va informar d'un increment de 30 % en els atacs relacionats amb grups terroristes**, amb un augment en l'ús de codi maliciós adreçat a infraestructures crítiques. L'objectiu d'aquests actors no és només el sabotatge o l'obtenció de diners mitjançant extorsió, sinó també la creació de caos social i econòmic en regions específiques. La seva estratègia es basa a desestabilitzar governs i minar la confiança pública en els sistemes operatius vitals. Els sistemes d'energia, telecomunicacions i transport han estat particularment

amenaçats per aquests actors, que busquen maximitzar l'impacte dels seus atacs sobre la vida quotidiana.

7. CONCLUSIONS I RECOMANACIONS

A l'anàlisi detallada de les ciberamenaces dirigides a infraestructures crítiques durant el 2024 i el 2025, hem identificat patrons, actors i tècniques que estan redefinint la ciberseguretat global.

Les infraestructures crítiques, com ara les d'energia, telecomunicacions, transport i salut, es troben cada cop més al punt de mira d'actors de diversa mena: des dels ciberdelinqüents motivats pel benefici econòmic fins a grups patrocinats per estats amb objectius geopolítics. La sofisticació, la persistència i la complexitat d'aquests atacs estan en augment, cosa que planteja riscos greus tant a nivell nacional com global.

Alguns dels punts clau que val la pena destacar després de tota la informació aportada a l'informe, seria:

- **Diversificació d'actors d'amenaça**: els atacs dirigits a infraestructures crítiques provenen d'una àmplia gamma d'actors, que inclouen ciberdelinqüents, grups patrocinats per estats (APT), hacktivistes i, en alguns casos, grups terroristes. Cadascú té les seves motivacions i objectius específics, però tots coincideixen a fer servir tècniques cada cop més sofisticades i personalitzades, com el programari de segrest, els explotadors de vulnerabilitats zero-day i els atacs a la cadena de subministrament.

- **Impacte econòmic i geopolític creixent**: la magnitud dels ciberatacs, especialment els de tipus programari de segrest, continua augmentant. El 2024, els atacs a infraestructures crítiques van provocar pèrdues que van superar els 30.000 milions de dòlars, una xifra que s'espera que creixi exponencialment el 2025. A més, els grups patrocinats per estats estan jugant un rol més prominent, i afecten no només les economies, sinó també les relacions geopolítiques en exposar vulnerabilitats crítiques en sectors estratègics.

- **Vulnerabilitats específiques d'infraestructures crítiques**: a causa de la seva naturalesa i la seva integració amb tecnologies de control industrial, estan particularment exposades als atacs de codi maliciós especialitzat (com el dirigit a sistemes ICS). Aquests atacs poden no només paralitzar operacions, sinó també perjudicar físicament equips essencials i posar en risc la seguretat pública. A més, les infraestructures amb sistemes heretats o vulnerabilitats no aplicades són objectius freqüents per als atacants, cosa que assenyala la necessitat urgent d'actualitzar i enfortir les defenses.

- **Augment de la persistència dels atacs**: s'estan adoptant enfocaments més persistents, infiltrant-se en xarxes durant llargs períodes de temps abans de ser detectats. Això és particularment evident en els grups APT, que fan servir tècniques d'infiltració i exfiltració de dades a llarg termini, cosa que augmenta significativament el risc de filtració d'informació confidencial i sabotatge d'operacions crítiques.

- **Manca de preparació i resiliència en algunes àrees**: encara que les capacitats de ciberseguretat en infraestructures crítiques estan millorant, molts sectors continuen estant insuficientment preparats per fer front als atacs més sofisticats. La manca d'una estratègia de defensa integral, l'escassetat de formació continuada en ciberseguretat i les bretxes en

la cooperació pública-privada són factors que agreugen la vulnerabilitat davant dels ciberatacs.

8. 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.