ANDORRA DIGITAL

ANC-AD Agència Nacional de Ciberseguretat d'Andorra

Informe de ciberintel·ligència

L'amenaça dels ciberatacs durant els processos electorals

TLP: WHITE

10/08/2023

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	18/08/2023	21/08/2023

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGÍA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). Es tracta d'un esquema creat per fomentar un millor intercanvi d'informació de caràcter delicat (però no classificada) en l'àmbit de la seguretat de la informació. A través d'aquest esquema, d'una forma àgil i senzilla, s'indica fins a on pot circular la informació més enllà del receptor en qüestió, i aquest ha de consultar a l'ANC-AD (Agència Nacional de Ciberseguretat d'Andorra) [https://www.anc.ad/] quan la informació necessiti ser distribuïda a tercers.

CODI	QUAN EMPRAR-LO	COM COMPARTIR-LO
TLP:RED	S'ha d'utilitzar **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, reputació o operacions si és mal utilitzada.	Els receptors no han de compartir informació designada com **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP:AMBER	S'ha d'usar **TLP:AMBER** quan la informació requereix ser distribuïda de manera limitada, però suposa un risc per a la privacitat, reputació o operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com **TLP:AMBER** únicament amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per a protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per a compartir aquesta informació.
TLP:GREEN	S'ha d'emprar **TLP:GREEN** quan la informació és útil per a totes les organitzacions que participen, així com amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP:WHITE	S'ha d'utilitzar **TLP:WHITE** quan la informació no suposa cap risc de mal ús, dins de 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

Si el passat 23 de juliol, dia en què es van celebrar les eleccions presidencials a Espanya, hi va haver un fet que va restar protagonisme als mateixos comicis, als partits polítics i als seus diferents candidats, foren els diversos ciberatacs que es van registrar.

Les pàgines web de l'Institut Nacional d'Estadística (INE), Casa Reial, Ministeri de l'Interior, la Moncloa o Correus, van ser algunes de les víctimes d'una campanya d'atacs de DDoS que va començar 96 hores abans del dia de les eleccions i es va prolongar fins uns dies després. Finalment, van ser fins a 27 les entitats afectades, incloent-hi organismes governamentals, mitjans de comunicació, empreses de telecomunicacions, de transport, hostaleria i banca.

Com es sap, els atacs DDoS es caracteritzen per provocar que la disponibilitat dels llocs web als quals es dirigeixen es vegi afectada. Si bé és cert que el seu impacte és limitat, no deixa de ser una mostra significativa de com els actors de l'amenaça intenten fer-se notar i influir en moments tan crítics per l'evolució política, econòmica i social d'una nació.

Ja sigui mitjançant campanyes de desinformació, atacs rupturistes de diferent índole o, fins i tot, mitjançant accions més complexes que han derivat en exfiltració de dades o en comprometre institucions o infraestructures crítiques, les ingerències dels cibercriminals en els processos electorals s'han tornat cada vegada més freqüents durant l'última dècada.

Per això, en el present document aprofundirem en les causes i motivacions d'aquest tipus d'accions i quins són els seus objectius. La finalitat no és una altra que donar a conèixer quines han estat les accions més rellevants en aquest sentit per, així, ajudar qualsevol organització que pugui ser susceptible de veure's afectada a prendre les mesures preventives oportunes.

3. CAUSES DE CIBERATACS DURANT ELS PROCESSOS ELECTORALS

Els comicis són un moment crucial per qualsevol país. Tenen un impacte important en l'àmbit econòmic i la millor mostra d'això és que els mercats sempre es mostren sensibles als resultats que es produeixen.

D'altra banda, en un món globalitzat com en el qual vivim, la política internacional juga un paper fonamental i, per això, és fàcil entendre com poden haver-hi interessos de tercers per influir en l'elecció d'un candidat polític o un altre.

Així doncs, les principals motivacions darrere les campanyes de ciberatacs de grups de cibercriminals patrocinats per un estat o hacktivistes durant els processos electorals són:

- Interessos geopolítics: amb l'objectiu de debilitar rivals o augmentar la mateixa influència global. Els ciberatacs s'utilitzen com a mecanisme que pretén aconseguir que l'elector es decanti pel líder que sigui més favorable a les polítiques i objectius del costat que implementa l'atac.
  D'altra banda, cal no oblidar la importància que ha adquirit actualment promoure determinades agendes ideològiques. Els ciberatacs poden ser usats per soscavar la confiança en els processos democràtics en si.
  En alterar els resultats o crear la percepció que les eleccions no són justes o legítimes, els atacants poden desestabilitzar la fe de la gent en la democràcia com a sistema.

- Desestabilització interna: alguns actors poden intentar debilitar o desestabilitzar un país o regió en sembrar discòrdia i desconfiança mitjançant ciberatacs. Això pot incloure fomentar la polarització política, promoure la radicalització o crear conflictes socials.

- Guanys financers: els ciberatacs també poden estar motivats pel desig de perpetrar furt d'informació confidencial relacionada amb el finançament de campanyes polítiques per, posteriorment, fer-la pública o utilitzar-la per extorsionar les parts afectades, sempre amb l'objectiu d'influir en els resultats electorals.

- Venjança política: en alguns casos, els ciberatacs poden ser una forma de venjança política, dirigida als candidats, partits o institucions que han pres decisions percebudes com a perjudicials pels mateixos atacants o els seus interessos.

És important tenir en compte que les motivacions darrere d'aquests ciberatacs poden variar segons el context i els actors involucrats. Les eleccions democràtiques són objectius atractius per als ciberatacs a causa de la seva importància política i social, i la comprensió d'aquestes motivacions és crucial per prevenir i mitigar els impactes negatius en els processos electorals.

4. TIPOLOGÍA DELS ATACS MÉS FREQÜENTS

No són poques les tècniques utilitzades pels actors maliciosos per influir en els processos electorals. Cadascuna d'elles, com és evident, està orientada a aconseguir diferents objectius:

- Campanyes de desinformació i *fakenews*: es basen en la creació i difusió de continguts falsos per influir en l'opinió pública. Les xarxes socials s'han convertit en una eina tant poderosa com perillosa on és fàcil trobar comptes creats ad hoc, secundats per quantitats enormes de bots automàtics, on els rumors, les narratives esbiaixades o directament les fal·làcies tracten d'arribar al màxim d'audiència possible. D'aquesta manera, es busca intervenir en l'elecció dels votants.

  De fet, han estat moltes les ocasions en què aquestes *fakenews* han arribat fins als mitjans de comunicació, per la qual cosa és fàcil d'entendre el gran impacte que poden arribar a tenir. A això s'ha de sumar el potencial de la Intel·ligència Artificial, que ha permès simular veus o crear imatges i vídeos falsos amb l'objectiu de fixar un discurs polític determinat.
- Manipulació de sistemes de missatgeria i comunicació: els atacants poden infiltrar-se en sistemes de comunicació utilitzats per candidats i equips de campanya per prendre informació estratègica o difondre missatges falsos en el seu nom.
- Campanyes de *phishing* i *spear-phishing*: l'enginyeria social és present també en els processos de votació. Molts actors maliciosos aprofiten les eleccions per crear campanyes que suplanten l'entitat d'institucions implicades en els comicis per enviar missatges o correus electrònics mitjançant els quals robar informació personal, credencials o propagar programari maliciós.
- Atacs DDoS: s'usen per aclaparar i desactivar llocs web i plataformes en línia relacionades amb el procés electoral. Això pot interferir amb la difusió d'informació i generar confusió entre el públic.
- Exfiltració d'informació i dades: aquests atacs es dirigeixen contra els sistemes dels partits polítics i els seus membres amb l'objectiu de prendre informació que pugui ser sensible i confidencial per intentar utilitzar-la posteriorment, sigui per divulgar-la o obtenir algun benefici a canvi mitjançant xantatge si aquesta pogués afectar la seva reputació, imatge o percepció pública.
- Atacs a la infraestructura electoral: l'objectiu és comprometre els sistemes fets servir en el registre de votants, l'emissió de vots o el recompte d'aquests. Els atacants poden intentar comprometre aquests sistemes per alterar els resultats o sembrar dubtes sobre la integritat del procés electoral.

5. IMPACTE I CONSEQÜÈNCIES

5.1. Impacte en la integritat electoral

Els ciberatacs en processos electorals poden tenir un impacte significatiu en la integritat de les votacions i en el funcionament adequat de la democràcia. La manipulació dels resultats de votació mitjançant intrusions en sistemes de votació electrònica o l'accés no autoritzat a bases de dades electorals pot alterar els resultats finals. Això no només distorsiona la voluntat de l'electorat, sinó que també sotmet la confiança pública en l'autenticitat i legitimació de les eleccions.

L'alteració de la confiança pública és un aspecte clau de l'impacte. Els ciberatacs que exposen informació sensible de candidats, partits o funcionaris electorals poden generar dubtes sobre la imparcialitat i la integritat dels involucrats. D'aquesta manera, els actors maliciosos poden arribar a aconseguir que es generi una creixent sensació de desconfiança entre els ciutadans i posar en perill la confiança en el procés electoral com a conjunt.

5.2. Impacte polític, social i de seguretat

En l'àmbit polític, els ciberatacs poden tenir efectes duradors. En influir en els resultats electorals o en la percepció dels votants, els atacants poden alterar l'equilibri del poder i afectar la direcció política d'un país. Això pot donar lloc a líders triats les agendes dels quals no representen genuïnament la voluntat de la població, la qual cosa, al seu torn, pot conduir a la implementació de polítiques que no reflecteixen els interessos de la majoria.

En l'àmbit social, poden ampliar la polarització. La difusió de desinformació i contingut enganyós pot fomentar la propagació de narratives extremes, creant un ambient en què els ciutadans s'enfrontin entre si en lloc de discutir de manera constructiva.

En termes de seguretat, els ciberatacs en eleccions poden desencadenar crisis internes i externes. En última instància, els cibercriminals poden arribar a tenir la capacitat de fer que els governs es vegin debilitats i que la confiança en les institucions democràtiques es dilueixi.

5.3. Impacte en la política internacional

Els ciberatacs en processos electorals també poden tenir implicacions significatives en la política internacional, arribant, fins i tot, a desencadenar conflictes o tensions diplomàtiques entre països si se'ls atribueix a actors estatals. La interferència en eleccions pot ser percebuda com una violació de la sobirania i la integritat del procés electoral d'un altre país, la qual cosa pot resultar en sancions, represàlies i deteriorament de les relacions bilaterals.

5.4. Conseqüències conjuntes i transversals

La interconnexió d'aquests efectes i conseqüències pot tenir un impacte en cascada que va molt més enllà dels resultats electorals en si mateixos. Els ciberatacs en eleccions són una qüestió que transcendeix la tecnologia i té profundes implicacions polítiques, socials i de seguretat.

A més a més, la política internacional també es veu afectada, la qual cosa subratlla la importància d'abordar aquests problemes mitjançant estratègies de ciberseguretat sòlides i esforços continus per preservar la integritat dels processos democràtics i mantenir la confiança de la ciutadania i la comunitat internacional.

6. CASOS MÉS RELELVANTS DE CIBERATACS A MODE D'INGERÈNCIA POLÍTICA

6.1. Eleccions presidencials dels Estats Units, 2016:

- Actor d'amenaça: es va atribuir a grups vinculats a Rússia, com APT28 (Fancy Bear) i APT29 (Cozy Bear).
- Mètode: els atacants van dur a terme atacs de *phishing* dirigits a comptes de correu electrònic de polítics i funcionaris demòcrates, i després van filtrar correus electrònics a través de llocs web com WikiLeaks.
- Impacte: els correus electrònics filtrats van exposar tensions internes en el Partit Demòcrata i van afectar la campanya de Hillary Clinton. Es van generar acusacions d'interferència russa en el procés electoral i es va qüestionar sobre la seguretat dels sistemes electorals.

6.2. Eleccions presidencials a França, 2017 i 2022:

- Actor d'amenaça: No es va identificar un actor específic.
- Mètode: es van detectar intents de *phishing* i campanyes de desinformació, incloent-hi la difusió de notícies falses.
- Impacte: encara que no es va confirmar una influència significativa en els resultats, hi va haver preocupacions sobre la desinformació i els intents de manipulació de l'opinió pública.

6.3. Eleccions a Ucraïna, 2014 i 2019:

- Actor d'amenaça: Es va atribuir a actors russos, concretant algun grup, com SandWorm.
- Mètode: es van dur a terme ciberatacs que van afectar la infraestructura electoral i les xarxes de comunicació en un intent de minar el procés electoral i la sobirania d'Ucraïna.
- Impacte: aquests atacs van generar desafiaments tècnics i polítics pel país, la qual cosa va conduir a una major consciència sobre la ciberseguretat en les eleccions.

6.4. Eleccions parlamentàries a Alemanya, 2017:

- Actor d'amenaça: No es va identificar un actor específic.
- Mètode: hi va haver preocupació sobre possibles intents de ciberatacs i campanyes de desinformació abans de les eleccions parlamentàries.
- Impacte: tot i que no es va confirmar una influència significativa en els resultats, el cas va posar de manifest la importància de la seguretat cibernètica en el procés electoral.

6.5. Eleccions al Brasil, 2018:

- Actor d'amenaça: No es va identificar un actor específic.
- Mètode: es va informar sobre la difusió de notícies falses i desinformació a les xarxes socials durant les eleccions presidencials.
- Impacte: la propagació de notícies falses va generar debats i tensions polítiques al país, posant de manifest els desafiaments de la desinformació en línia.

6.6. Eleccions al Regne Unit, 2019:

- Actor d'amenaça: No es va identificar un actor específic.
- Mètode: es van generar preocupacions sobre la propagació de desinformació i campanyes d'influència a les xarxes socials durant les eleccions generals.
- Impacte: encara que no es va confirmar una influència significativa als resultats, el cas va cridar l'atenció sobre la necessitat d'abordar la desinformació en línia.

6.7. Eleccions presidencials als Estats Units, 2020:

- Actor d'amenaça: Tot i que no es va identificar un actor específic com en 2016, l'enfocament principal es va centrar a prevenir qualsevol influència estrangera no desitjada.
- Mètode: les eleccions presidencials dels Estats Units al 2020 es van dur a terme en un entorn d'alta sensibilitat pel que fa a la seguretat cibernètica, després dels incidents d'interferència en l'anterior cursa electoral el 2016. Es van implementar mesures proactives per a reforçar els sistemes de votació, millorar la detecció de desinformació i augmentar la seguretat en línia.
- Impacte: en comparació amb les eleccions de 2016, les eleccions del 2020 als Estats Units van representar un enfocament més coordinat i proactiu per prevenir la interferència cibernètica i la desinformació. Els esforços de col·laboració entre el govern, els actors privats i les plataformes tecnològiques van ajudar a protegir la integritat del procés electoral i a mantenir la confiança del públic en els resultats.

6.8. Eleccions a Israel, 2019-2021:

- Actor d'amenaça: Tot i que no es va identificar un actor específic, es van informar intents d'interferència en diverses eleccions a Israel durant aquest període.
- Mètode: es van mencionar campanyes de desinformació i ciber-amenaces.
- Impacte: els intents d'interferència van destacar la necessitat de mantenir la seguretat cibernètica en eleccions i posar de manifest la vulnerabilitat dels processos democràtics a la manipulació.

6.9. Eleccions a l'Índia, 2019:

- Actor d'amenaça: no es va identificar un actor específic.
- Mètode: es va informar sobre intents de ciberatacs i campanyes de desinformació durant les eleccions generals.
- Impacte: es van generar preocupacions sobre la influència de la desinformació en línia en l'opinió pública i el procés electoral.

6.10. Eleccions a l'Equador, 2021:

- Actor d'amenaça: no es va identificar un actor específic.
- Mètode: es van detectar intents d'atacs cibernètics i campanyes de desinformació durant les eleccions presidencials.
- Impacte: encara que no es va confirmar una influència significativa en els resultats, l'incident va subratllar la importància de la ciberseguretat en els processos electorals.

6.11. Eleccions presidencials d'Espanya (23/07/2023):

L'Estat veí, Espanya també s'afegeix a la llista de països d'aquest punt, convertint-se en l'objectiu d'una campanya d'atacs DDoS contra diferents entitats públiques i privades, amb un total de 27 organitzacions afectades.

L'actor de l'amenaça en aquest cas va ser NoName057(16), un grup, el qual es creu que treballa sota les ordres del Kremlin i que va reivindicar cada una de les accions a mesura que es concretaven amb èxit. La motivació en aquest cas va ser totalment política, i en cada comunicat que va publicar després dels atacs perpetrats va deixar clar que es deuen al suport mostrat pel govern d'Espanya a Ucraïna.

Com és evident, la campanya de ciberatacs DDoS va tenir un impacte relativament baix. Les diferents entitats afectades no van trigar a recuperar-se i operar amb normalitat. No obstant això, el grup va aconseguir un ressò mediàtic més que notable. De fet, es creu que moltes d'aquestes campanyes, més enllà de buscar desestabilització al país atacat, pretenen animar que més cibercriminals s'uneixin a les files d'aquests grups per millorar la seva infraestructura humana i tècnica amb l'objectiu d'implementar atacs més crítics al futur.

Encara que, cal no oblidar, que qualsevol atac cap a un organisme governamental en aquest context en què la guerra entre Ucraïna i Rússia polaritza la política mundial, té també una finalitat col·lateral com és donar visibilitat a la debilitat de les Democràcies Europees occidentals i, per tant, desacreditar-les.

6.11.1. Cronologia de l'atac:

- 19 de juliol: el primer atac que va reivindicar el grup NoName057(16) en plena recta final de la campanya electoral, va ser el que va afectar la disponibilitat del lloc web de la Casa Reial.
- 21 de juliol: tan sols 48 hores abans que s'obrissin els col·legis electorals, van ser les entitats bancàries les que van patir les conseqüències dels atacs DDoS. Bankinter, Abanca, Grup Caja Rural i Banco Cooperativo van ser els objectius triats.
- 23 de juliol: durant els comicis va ser notícia la indisponiblitat temporal de les pàgines web del Ministeri de l'Interior, La Moncloa, la Junta Electoral, l'INE, Correus, l'Ajuntament de San Fernando de Henares, el consorci de transport de Madrid, la companyia Socibus.
- 25 de juliol: va ser el torn de Telefònica, Orange, Euskaltel, Jazztel, Barcelona Turisme, Reservalis o Triodos Bank Espanya.
- 28 de juliol: els atacs es van dirigir contra diversos mitjans en línia. El Mundo, El Español, ABC, La Razón o Expansión van ser alguns dels que van patir contratemps a causa de NoName057(16).

6.11.2. Sobre l'actor d'amenaça NoName057(16):

Es té constància de l'activitat del grup des de, com a mínim, març del 2022. És a dir, va sorgir durant els primers mesos de la invasió d'Ucraïna per part de Rússia. Des de llavors, han impulsat diferents campanyes d'atacs contra països europeus o pertanyents a l'OTAN. Generalment, com a resposta a les mostres públiques d'aquests de suport polític, militar o econòmic a Zelenski o, com a represàlia contra les diferents sancions que s'han anat imposant a Rússia com a conseqüència de la invasió.

De fet, la seva última amenaça dirigida contra occident es va produir el 30 de gener d'aquest mateix any. Mitjançant un comunicat, van manifestar la seva intenció d'orquestrar una sèrie d'atacs dirigits contra organitzacions del sector IT d'Ucraïna i d'Europa occidental, on els països pertanyents a l'OTAN, a priori, serien el seu principal objectiu.

A més, aquesta amenaça també va servir per donar visibilitat al "projecte DDosia", que en aquell moment es trobava en un estat prematur. Mitjançant aquest projecte, s'invita i s'encoratja a qualsevol ciberdelinqüent a fer-se voluntari i a unir-se per llançar atacs DDoS contra llocs web estratègics de nacions crítiques amb la invasió. Des de llavors, el grup ofereix fins a 80.000 rubles, que serien una mica més de 1.000€, per cada atac exitós.

- Modus operandi

El grup NoName057(16) està especialitzat en atacs DDoS per impulsar accions eminentment disruptives. Si bé és cert que aquest tipus d'atacs es caracteritzen per tenir un impacte limitat i les entitats afectades solen mitigar-los en períodes de temps relativament curts, no cal obviar que la seva repercussió pot ser important quan afecten la normal operativa d'institucions governamentals o infraestructures crítiques.

- Projecte DDosia

Com ja s'ha explicat anteriorment, aquest projecte consisteix a reclutar ciberdelinqüents que vulguin participar en els atacs de NoName057(16). Per fer-ho, el grup facilita un kit d'eines, que també es diu "DDosia", a tots els membres que s'hi adhereixin, per la qual cosa han aconseguit crear una *botnet* de servidors C2 molt àmplia.

Aquest kit d'eines, en els seus inicis, estava desenvolupat a Python. No obstant això, es té constància que les noves versions estan escrites en Go, aconseguint una major eficiència en els seus atacs, com es demostra amb l'èxit de la darrera campanya dirigida contra Espanya. A més, aquestes últimes versions són multiplataforma i treballen sobre els principals sistemes operatius (Windows, Linux, macOS, Android). Totes elles es distribueixen sota demanda mitjançant els canals de Telegram que opera el grup.

Encara que hi ha dificultats per quantificar quants membres formen part del projecte DDosia, s'estima que a començaments del 2023 la xifra podria estar entorn dels 2.000, i que abans de començar maig, la xifra podria haver ascendit a més de 7.000. Per tant, algunes empreses de seguretat creuen que ara mateix els atacs de DDoS de NoName057(16) podrien comptar amb l'ajuda d'uns 10.000 ciberdelinqüents.

7. CONCLUSIONS I RECOMANACIONS

La ciberseguretat s'ha convertit en un element fonamental per a qualsevol mena d'organització, però no hi ha dubte que hi ha moments crítics en què cal prestar atenció a les amenaces cibernètiques.

Els processos electorals són crítics per a qualsevol país i l'augment de l'intent d'influència dels actors d'amenaça en ells és una realitat. Per això, és important que qualsevol organisme o entitat estigui preparat per a qualsevol classe d'acció maliciosa que es pugui produir. Algunes de les mesures que haurien de tenir-se en compte abans de la celebració d'unes eleccions són:

- Avaluació de vulnerabilitats: realitzar avaluacions de seguretat cibernètica per identificar i abordar possibles vulnerabilitats en els sistemes electorals. Això inclou proves de penetració i anàlisis de riscos per anticipar i prevenir atacs.
- Educació i conscienciació en ciberseguretat: Oferir formació en ciberseguretat als candidats, funcionaris electorals i personal de campanya. Això ajudarà a reduir la probabilitat de caure en trampes de phishing i augmentar la consciència sobre amenaces cibernètiques.
- Monitoratge continu: implementar sistemes de detecció d'amenaces i monitoratge contínua per identificar patrons d'activitat sospitosa. La identificació primerenca d'atacs pot permetre una resposta ràpida i efectiva.
- Protecció de la Infraestructura Crítica: considerar la infraestructura electoral com un actiu crític que cal protegir. Això inclou la protecció de registres electorals, sistemes de votació electrònica i sistemes de comunicació.
- Resposta a incidents: desenvolupar plans detallats de resposta a incidents que establin com es manegaran i comunicaran els atacs cibernètics. La rapidesa i eficàcia en la resposta poden limitar el dany causat.
- Verificació d'informació: promoure l'ús de fonts fiables i verificar la informació abans de compartir-la en línia. L'educació del públic sobre la identificació de notícies falses és crucial per reduir la propagació de desinformació.
- Regulació, transparència i verificació de la informació compartida en plataformes: Les plataformes de xarxes socials i els mitjans de comunicació han de ser transparents en la seva gestió de contingut polític i desinformació. Es poden establir regulacions per evitar la difusió d'informació enganyosa.
- Col·laboració entre sectors: la cooperació entre governs, organitzacions internacionals, partits polítics, plataformes tecnològiques i experts en ciberseguretat és fonamental. La informació i l'intercanvi d'intel·ligència poden ajudar a identificar amenaces i respondre-hi de manera més efectiva. I la participació d'entitats especialitzades en ciberseguretat pot ser crucial perquè qualsevol organització estigui preparada davant qualsevol ingerència que es pugui produir amb motiu de les eleccions.

CLÀUSULA DE CONFIDENCIALITAT