# INFORME DE VIGILÀNCIA TECNOLÒGICA

# Ciberseguretat

hubb30.

Generalitat de Catalunya
Departament d'Empresa i Coneixement
Secretaria d'Universitats i Recerca

Unió Europea
Fons Europeu
de Desenvolupament Regional

INFORME DE VIGILÀNCIA TECNOLÒGICA

# Ciberseguretat


**Autors**

Roser Salvat Jofresa, Parc de Recerca UAB
Hafsa El Briyak Ereddam, Parc de Recerca UAB
Marta Tort Xirau, Oficina de Valorització i Patents UAB
Amb la col·laboració de Joan Caubet, d'Eurecat



**Edició i disseny**

Àrea de Comunicació i Promoció
Parc de Recerca UAB





Parc de Recerca UAB
Av. de Can Domènech s/n - Edifici Eureka - Campus de la UAB
08193 Bellaterra (Cerdanyola del Vallès) Barcelona · Spain
www.hubb30.cat

hubb30.

Una iniciativa de:

Projecte cofinançat per:

Generalitat de Catalunya
Departament d'Empresa i Coneixement
Secretaria d'Universitats i Recerca

Unió Europea
Fons Europeu
de Desenvolupament Regional

# 1
# Visió de síntesi sobre innovació i tendències en Ciberseguretat

La ciberseguretat engloba el conjunt de **mesures físiques, lògiques i administratives** destinades a la protecció digital d'empreses, sistemes i persones davant d'atacs digitals que en comprometen la confidencialitat, disponibilitat o integritat[1].

Aquest és un àmbit viu i en constant evolució; mantenir-se actualitzat és tot un repte per als emprenedors, els negocis i, en general, per al teixit empresarial.

## Magnitud del cibercrim

El cibercrim és un fenomen sense fronteres, i en expansió. Cybersecurity Ventures estima que en el 2021 el cibercrim representarà un **1% del PIB mundial** (xifra equivalent a un cost global de 6.000 milions de dòlars anuals), duplicant la xifra del 2015[2]. En consonància, la despesa mundial en ciberseguretat creix a un ritme anual de quasi el 15%.

Els **ciberdelinqüents** són els principals agents que ataquen les indústries, usualment motivats per l'enriquiment il·lícit o el frau, tot i que darrere el cibercrim també pot haver-hi **hacktivistes** que es mouen per causes polítiques o ideològiques, **hackers individuals** especialment interessats a crear moments de caos, i fins i tot agents patrocinats per estats.

Clonació de targetes de crèdit, atacs en caixers automàtics (ATM), transferències bancàries interessades, frau en assegurances i serveis mèdics, suplantació d'identitat a la xarxa amb finalitat comercial, robatori de criptomònades, obtenció il·lícita i venda d'informació a terceres parts... Els atacs són cada cop més complexos, i a mesura que els perpetradors es tornen més agressius i desenvolupen noves tècniques de pirateria, creen danys a major escala en l'economia domèstica i, sobretot, d'empreses.

En els darrers cinc anys, el nombre de ciberatacs a indústries i a xarxes informàtiques comercials ha augmentat notablement tant en freqüència com en intensitat [3]. Amb el temps, els pirates informàtics ciberdelinqüents han aconseguit crear un **ecosistema generalitzat** i nombrosos models de negoci, diversificant per exemple el Crime as a Service (CaaS) o el Pay Per Installs (PPI). Des de fa anys, la indústria de la ciberseguretat ha mantingut un status, pel qual tant els ciberdelinqüents com els venedors de seguretat estan constantment actualitzant les tàctiques per assolir els seus respectius objectius. L'èxit del cibercrim es deu, en part, al fet que la indústria de seguretat s'ha centrat més en protegir els clients dels atacs, que no pas en neutralitzar activament els atacants[4].

La identificació i el control dels pirates informàtics i de les seves accions ha estat, tradicionalment, una funció assumida per les agències policials, però les forces públiques de seguretat no sempre han demostrat ser eficients. En el **cicle continu d'iteració i millora** tant de solucions de seguretat

[1] ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic.

[2] ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic.

[3] Frost and Sullivan (2017) ) *Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment.*

[4] Frost and Sullivan (2019) *Technology Innovation award - The cyber intelligence industry: Europe & Israel.*

com de tàctiques de pirateria, l'avantatge queda en gran part del costat dels cibercriminals.

## Impacte a les empreses

Les empreses integren multitud de dispositius, sistemes, actius i recursos humans. Progressivament digitalitzen els seus negocis, i aquesta transformació genera **volums de dades sensibles**, com ara credencials d'empleats, informació sobre clients i propietat intel·lectual, que s'emmagatzemen en els punts finals connectats, al núvol i als centres de dades. Però sembla clar que com més depenem de la tecnologia connectada, més vulnerables som a les amenaces d'explotació de vulnerabilitats i fallades en el disseny de seguretat en dispositius.

Alguns estudis internacionals indiquen que Espanya va ser el país que més ciberatacs va patir a través de dispositius IOT el 2018[5]. La naturalesa crítica de les dades empresarials pot resultar atractiva per als pirates informàtics i els ciberdelinqüents. De fet, el **91% de les empreses de l'Estat admet haver patit un ciberatac** en el darrer any, i el 45% van haver de gestionar una interrupció de més de 5 minuts a causa d'un ciberatac l'any 2018, provocant danys per valor de més de 400.000 € [6].

El fet és que un error pot ensorrar la reputació en qüestió de segons. Per tant, és important que les organitzacions comptin amb **comunicacions fiables i segures**, així com amb una **identitat sofisticada** i una correcta **gestió d'accés al maquinari**. Sobre aquests actius, s'implementen capes de prevenció, protecció i resiliència a diversos nivells. No protegir-se efectivament contra les noves amenaces exposa les empreses a la **pèrdua d'informació confidencial**, a impactes negatius sobre la seva **marca**, a **sancions** per vulneració de lleis i, en definitiva, a dificultats per ser competitives.

És un fet que algunes busquen eines que els ajudin a **avaluar riscos** i intenten abordar de forma proactiva els problemes abans de ser piratejades. D'altres, regularment s'enfronten a pirates informàtics, i tendeixen a realitzar esforços sistemàtics per monitoritzar els seus empleats i ex-empleats, formar els treballadors, i a divulgar **protocols i eines** de seguretat. La planificació empresarial també hauria d'incloure una revisió de les **pòlisses d'assegurança** per comprovar la cobertura de ciberatacs.

En particular, les **grans corporacions són víctimes d'atacs dirigits**, conduïts per grups criminals experts, i és important que internalitzin capacitats per identificar els seus atacants i col·laborar amb les forces de seguretat per neutralitzar-los. Però les **empreses mitjanes i petites** també s'enfronten regularment a ciberatacs, i fan el que poden per defensar-se. Alguns dels incidents rauen en els seus propis treballadors, i sovint es descobreixen vulnerabilitats informàtiques després d'incidents. La compartició de **credencials** d'inici de sessió, així com la filtració accidental de dades sensibles als destinataris equivocats, són pràctiques que s'han de monitoritzar i preveure.

## Les amenaces que venen

Els errors humans, relacionats amb configuracions imprecises o amb males pràctiques, són i seguiran essent una causa freqüent de fuites d'informació. Però a les amenaces del factor humà se'n sumen altres, d'ordre molt divers, perquè els ciberatacants intenten incomplir les defenses de les empreses mitjançant **mètodes cada cop més sofisticats**.

[5] Centro de Ciberseguridad Industrial (2019) Incidentes de ciberseguridad industrial en Servicios esenciales en España. Edición 2019.

[6] ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic.

Els tipus de vulnerabilitats més reportades per l'Instituto Nacional de Ciberseguridad de España (INCIBE) el 2019[7] són el desbordament de memòria intermèdia, la gestió de paràmetres de forma incorrecta, el control d'accessos incorrectes i el *Cross-Site Scripting* (XSS).

Les **amenaces** es propaguen mitjançant noves formes innovadores de programari maliciós, a través del compromís de cadenes de subministrament globals i per sofisticats actors criminals i estats hostils[8]. D'entre les que són tendència, destaquen les següents:

- ***Botnets*:** Amb la proliferació de dispositius amb connectivitat, les xarxes de robots informàtics (bots) executades de forma autònoma i automàtica tindran un paper cabdal en la seguretat d'Internet i en la ràpida difusió de noves ciberamenaces.
- **Supply-chain attacks:** Els atacs a les cadenes de subministrament de proveïdors de productes i serveis amb l'objectiu d'afectar els seus clients seran una tendència habitual.
- **Atacs per correu electrònic:** Tècniques com ara el *BEC o el spear* ***phishing*** són cada vegada més elaborades, i seguiran demostrant un gran èxit per a enganyar, cometre frau o infectar amb ***malware*** (programari maliciós) o alguna de les seves varietats, com el *fileless malware*.
- ***Lateral movement*:** Els atacs laterals armats són una tècnica emprada pels ciberdelinqüents per desplaçar-se sistemàticament a través d'una xarxa a la recerca d'actius per fer inspeccions de memòria profunda.
- Atacs via xarxes socials, com l'***angler phishing***. En paral·lel, esdevenen un problema global com a mecanisme per influir a nivell polític o econòmic les ***fake news***.
- **Cryptojacking:** La mineria il·lícita apareix en moments d'alt valor de les criptomonedes, o bé de ràpida devaluació.
- **Fuites de dades a la "*dark web*":** El nombre d'incidents que acaben amb venda de dades personals creix cada any a causa del seu valor, així com de la proliferació de bases de dades al núvol.

## El *Ransomware* dirigit pren rellevància

Tot i que les organitzacions cibercriminals que utilitzen el *ransomware* se centren no en la quantitat sinó en la qualitat dels seus atacs, mesurada per la probabilitat de cobrar, els darrers tres anys ha hagut un augment significatiu del *ransomware* adreçat a governs estatals, provincials i locals, així com a les grans corporacions[9].

D'entre les amenaces que són tendència, aquesta variant de programari maliciós que infecta dispositius informàtics afectant la disponibilitat, integritat o confidencialitat de les dades, sol destacar-se particularment pel seu gran impacte. El motiu és que esdevé una forma d'atac a organitzacions amb **serveis crítics** que no poden permetre's aturar l'activitat, i que solen veure's forçats a **pagar rescats** per disposar de la clau criptogràfica de desxifratge. Els atacs de *ransomware* a les organitzacions el 2019 ha costat 10.450 milions d'euros[10].

[7] INCIBE (2020) Seguridad industrial en cifras 2019.

[8] Georges de Moura; World Economic Forum (2019) *The cibersecurity guide for leaders in today's digital world*.

[9] Sonicwall (2020) Cyber threat report 2020.

[10] Agència de Ciberseguretat de Catalunya (2020) Línies bàsiques d'un negoci cibersegur.

En el conegut ***Ransomware-as-a-service*** (RaaS), els atacants experts ofereixen els seus serveis per crear campanyes d'atac, comprats per ciberdelinqüents que executen fàcilment els atacs, eliminant barreres d'entrada al negoci del cibercrim. Els experts pronostiquen[11] que els atacs de *ransomware* augmentaran en un futur proper, i que en conseqüència és important que les empreses formin els treballadors sobre els seus riscos i activin plans específics.

## Sectors més vulnerables

L'Agència de Ciberseguretat de Catalunya alerta que el 40% de les empreses no es recuperen després d'un atac sever. Els sectors més vulnerables generalment es caracteritzen per la **presència d'informació sensible i d'actius crítics**:

- El **sector financer** i d'assegurances posseeix molta informació sensible que comporta la necessitat de defensar-se d'incidents derivats de la digitalització de serveis, dotant de seguretat els sistemes i aplicacions *fintech* (pagament online, comerç mòbil, NFC, o lectors de targetes per a mòbils basats en l'autenticació d'usuari), a vegades usant *big data analytics*.
- El **sector salut** (sanitat i farmàcia) disposa de dades molt preuades a la *dark web*, fet pel qual l'emmagatzematge xifrat i la transferència de dades mèdiques han de ser garantits. A aquest repte se suma la necessitat de protegir els dispositius mèdics connectats, així com la d'encriptar la recerca mèdica i farmacèutica.
- La **indústria** (indústria 4.0; *smart grids*,; infraestructures d'energia i *utilities*) sol sostenir-se d'informació crítica que requereix la protecció dels dispositius intel·ligents, sistemes i xarxes que conformen els sistemes de control industrial.
- El **sector de transport** ha d'atorgar seguretat als vehicles aeris i als vehicles terrestres autònoms i connectats, exposats a riscos de pèrdua de confidencialitat, integritat i disponibilitat de les dades, així com protegir-se de les vulnerabilitats dels sistemes de **telecomunicació** via satèl·lit.
- El **comerç**, en modalitat e-commerce, ha de trobar solucions per fer front al malware, a l'accés il·legal a canals com ara la missatgeria instantània o el correu electrònic, i als atacs de *phishing* (rèpliques de correus electrònics reputats amb sol·licitud d'informació sensible), alhora que es garanteixen les dades sensibles dels clients.
- El **sector educatiu**, que recentment ha virat decididament cap a l'*e-learning*, cal que protegeixi dades i que disposi de solucions als models pedagògics basats en la interacció, retroalimentació, ludificació o la simulació.
- El **sector de l'oci** i les xarxes socials exigeix la seguretat de dades privades i sistemes d'identitat digital.
- Finalment, el **sector públic** té vulnerabilitats derivades de la gestió de serveis als ciutadans, de l'intercanvi d'informació entre administracions (ciberintel·ligència) així com de la gestió de les ***smart cities***.

[11] Frost and Sullivan (2018) *Cyber Security Improvement Insights—Ransomware.*

## El mercat de la ciberseguretat

Segons Orbis Research, el mercat de la ciberseguretat es xifrarà en uns **164.000 milions de dòlars el 2024**, empès per l'increment d'atacs als serveis financers i bancaris, als governs, als serveis sanitaris i a les empreses, **el sector de la ciberseguretat està creixent**. Altres vectors d'impuls d'aquest mercat són l'augment de les aplicacions basades en el núvol, la telefonia intel·ligent i les tecnologies basades en la IoT.

Territorialment, el mercat mundial de la ciberseguretat ara per ara està concentrat a **EE.UU.**, especialment a Silicon Valley (25 % de share mundial), i a Europa destaca el Regne Unit, amb un 5%, però a mig termini la recent aprovació de legislació sobre seguretat cibernètica a la **Xina** pot comportar que emergeixi un significatiu mercat a Orient.

Quant als principals àmbits de negoci d'aquest sector, se solen classificar en tres categories:

- **Solucions de seguretat d'infraestructures:** seguretat al núvol, seguretat mòbil, seguretat de missatgeria, internet de les coses (IoT) i operacions de resposta d'incidents, entre d'altres.
- **Aplicacions** de gestió d'identitat i accessos, de seguretat web o a la xarxa, seguretat a l'extrem, MSSP i intel·ligència d'amenaces.
- **Serveis i consultoria** relacionats amb compliment de normativa, gestió del risc digital, protecció de sistemes i prevenció de frau en mitjans cibernètics.

A més de fer més segurs els sistemes empresarials, les **solucions de ciberseguretat de propera generació** podrien tendir a desencoratjar els hackers en les seves accions de disseny i execució d'atacs[12]. En aquest sentit, es preveu que la indústria d'intel·ligència cibernètica no només ofereixi solucions de protecció als seus clients, sinó també per frustrar ciberatacs en origen.

## Innovacions contextuals

El mercat de la ciberseguretat creix alhora que avança la transformació digital de la societat. S'espera que la indústria d'intel·ligència de seguretat evolucioni en els propers anys impulsada per innovacions relacionades amb l'automatització, l'aprenentatge automàtic i altres, que contribueixen a detectar atacs i a oferir-los millors respostes[13].

- **Computació en el núvol:** Suposa delegar la seguretat de dades i sistemes propis al núvol.
- **Industria 4.0:** Comporta la proliferació de dispositius de capacitat computacional menor, que cal protegir.
- **Internet of Things (IoT):** Suposa la proliferació de dispositius de capacitat computacional menor, amb una protecció crítica.
- **Big Data** (BD) i **Intel·ligència artificial** (IA): Potencien la capacitat de prevenció i detecció d'*Advanced Persistent Threats* (APT).
- **Blockchain:** Aporta integritat i alta disponibilitat de dades.
- **5G:** Possibilita la connectivitat segura d'un alt nombre de dispositius i comunicacions crítiques
- **Computació quàntica:** En pocs anys, permetrà desxifrar part dels actuals algoritmes de xifratge

[12] Frost and Sullivan (2019) *Technology Innovation award - The cyber intelligence industry: Europe & Israel.*

[13] Frost and Sullivan (2018) *Cyber Security Improvement Insights— Security Intelligence and Analytics.*

## El rol clau d'IoT

Sens dubte la tecnologia de computació en núvol està jugant un paper fonamental en l'abordatge dels reptes de gestió de dades i d'allotjament d'aplicacions, però els experts apunten que molts dels problemes de seguretat sorgeixen per una major adopció de IoT[14], una tecnologia revolucionària que afegeix una nova dimensió al món de les TIC.

El resultat de la seva implementació són els **ecosistemes connectats** que permet a cada dispositiu comunicar-se i compartir informació, aportant beneficis gens menyspreables relacionats amb l'eficàcia i l'eficiència de gestió de dades, processos i costos. La **seguretat transversal** i **integral de les infraestructures connectades**, en un context de manca d'estàndards de seguretat de perímetres, xarxes, *endpoints*, aplicacions i dades, pot ser un factor crític.

## Increment de l'adopció d'IA

També es preveu que la tecnologia d'Intel·ligència Artificial (IA) s'expandeixi en la defensa cibernètica per combatre les tècniques evolutives dels pirates informàtics[15] en seguretat de xarxa, gestió de vulnerabilitats i gestió d'accés a la identitat, igualment fonamentades en IA.

L'augment d'adopció d'intel·ligència artificial, combinada amb eines d'automatització i orquestració, aporta eficiència i redueix la necessitat i diversitat **d'analistes de seguretat**.

## Convergència i Internet of Everythig

La **convergència** d'aplicacions IoT amb tecnologies emergents com la intel·ligència artificial, el Big Data i la informàtica contextual, tendiran a contribuir a abordar alguns dels seus reptes de seguretat[16]:

- **Gestió d'identitats d'autoservei** en el núvol mitjançant sessions úniques centralitzades, en quatre segments: administració, autenticació, autorització i auditoria.
- **Representació visual interactiva** de dades (DV) de plataformes transversals.
- **Autenticació biomètrica** o tàctica d'*endpoints* per garantir l'accés a dispositius, serveis i zones restringides.
- **Monitoratge en temps real** mitjançant anàlisis predictives de patrons de comportament, *big data* i llenguatge natural (PNL).

En aquest context emergeix el concepte d'**Internet of Everything**, que en el futur emprarà una infraestructura de núvol segura, comuna amb una interfície de programació d'aplicacions (API) unificada. La perspectiva, així, és que s'eliminarà la necessitat de plataformes de seguretat específiques de sector, reduint en conseqüència els costos del desplegament i millorant les capacitats dels dispositius connectats amb múltiples fonts d'informació.

## El repte de la cibernètica en la Industria 4.0

La naturalesa interconnectada de les operacions basades en la indústria 4.0 i el ritme de transformació digital comporten escenaris de nous riscos cibernètics per als quals la indústria pot no estar preparada[17]. Tot i la progressiva incidència de l'IoT en les àrees d'operacions (OT) i malgrat el reconeixement generalitzat de la seva importància, el desafiament d'implementar estratègies de **seguretat cibernètica a la indústria** continua essent un repte en molts països[18].

[14] Frost and Sullivan (2018) *Asia-Pacific Cyber Security Trends into 2019.*

[15] Frost and Sullivan (2018) *Asia-Pacific Cyber Security Trends into 2019.*

[16] Frost and Sullivan (2017) *Cibersecurity Innovatons in the Connected world* .

[17] Waslo, Lewis, Hajj I Carton (2017) *Industry 4.0 and cibersecurity*: Deloitte

[18] Frost and Sullivan (2017) *Cyber Security In The Era Of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment*

Quan es connecten cadenes, fàbriques, clients i operacions de subministrament, els riscos són potencialment més importants. S'acumulen evidències de riscos d'interrupcions de producció, corrupció de dades i pèrdues financeres. Però aquesta indústria encara es mostra relativament escèptica, potser perquè fins ara el concepte seguretat s'ha associat a factors gens menors, com ara les vides humanes, les instal·lacions de les plantes, l'entorn operatiu i el medi ambient. En aquests entorns, la seguretat, la fiabilitat i la resiliència segueixen essent prioritats inqüestionables, però alhora emergeixen altres exemples de sistemes típics de risc, com ara els controladors lògics programables (PLC), els sistemes de control distribuït (DCS) o els dispositius electrònics intel·ligents (IEDs), específicament usats a la indústria elèctrica.

La manca de **coneixement de les direccions** comporta que la seguretat cibernètica s'assigni als departaments de TIC, sense assumir que l'aplicació de tecnologies en entorns industrials complexos ha de ser una responsabilitat d'**equips mixtos** integrats, també, per analistes, enginyers de seguretat i professionals d'intel·ligència. La ciberseguretat, la privadesa i la confiança digital es basen en la forma en què l'organització aconsegueix integrar la seguretat com a part inherent del seu ADN[19].

## Agudització en el sector d'energia

Segons el Centre Criptològic Nacional, dependent del Centre Nacional d'Intel·ligència (CNI), els sectors de l'Estat amb més incidents dels 33.000 informats el 2018 són l'elèctric, i el de gas i petroli[20]. En efecte, el **sector d'energia** concentra significatius reptes de conscienciació en matèria de seguretat, així com d'adopció a gran escala de tecnologies avançades, però la seguretat i la integritat dels diversos components de la cadena de valor no sempre posseeixen un marc de seguretat informàtica prou robusta com per a protegir-se de les intrusions[21]. Una infraestructura crítica com la xarxa elèctrica depèn de massives xarxes informàtiques, però els actuals mecanismes de defensa cibernètica poden estar obsolets i quedar exposats a la pirateria, causant destruccions a gran escala.

## Ecosistema dinàmic d'agents

Aquesta evidència sol relacionar-se amb una manca d'organismes reguladors i **d'aliances entre els participants d'aquestes indústries**[22], perquè per penetrar en mercats regulats o estratègics per les estratègies competitives dels territoris, les empreses han de treballar estretament amb els serveis públics, els reguladors i altres parts clau, a vegades inclús formant consorcis que els condueixin a guanyar projectes a llarg termini.

Amb l'augment de la consciència de risc i del desplegament de dispositius intel·ligents, la lògica indica que les **empreses públiques** i amb interessos públics es veuran progressivament obligades a invertir en solucions de protecció cibernètica. Però a no ser que el programari s'actualitzi sistemàticament, els ciberatacs són difícils de detectar i de prevenir. Com que la seguretat cibernètica és àmbit de despesa recurrent, els sectors públic i privat, sovint amb **limitacions pressupostàries** evidents, no sempre mantenen estratègies d'inversió incremental en aquest terreny.

Tot i així, es preveu un increment de la demanda de solucions de ciberseguretat en municipis i empreses, sovint amb el suport d'iniciatives governamentals. Així mateix, **creixeran els consorcis i les associacions públic-privades** participades per proveïdors de solucions

[19] Georges de Moura; World Economic Forum (2019) *The cibersecurity guide for leaders in today's digital world.*

[20] Centro de Ciberseguridad Industrial (2019) Incidentes de ciberseguridad industrial en Servicios esenciales en España. Edición 2019.

[21] Frost and Sullivan (2017) *Cibersecurity Innovatons in the Connected world.*

[22] Frost and Sullivan (2018) *Analysis of the North American Grids Cyber Security Market, Forecast to 2022. Growing Appetite for Automation Solutions Fuels Growth in Grid Cyber Security.*

de seguretat cibernètic i companyies d'assegurances amb l'objectiu d'oferir serveis de major valor afegit als clients i als ciutadans. Al cap i a la fi, treballar la ciberseguretat comporta **treballar la confiança en l'ecosistema digital** i en la fidelització de tots els actors implicats.

## Manca de talent

Per assegurar la ciberresiliència, els **serveis públics i les entitats** han de desenvolupar un marc de polítiques industrials i estratègies de mitigació del risc, i per fer-ho necessiten experts en ciberseguretat en nivells de direcció estratègica. En l'àmbit de les **empreses**, és igualment important recórrer a professionals de la ciberseguretat que ajudin a dissenyar xarxes segures, a fer anàlisis de vulnerabilitats i proves de penetració, a elaborar plans de continuïtat, i a oferir suport legal[23].

Però mentre la tecnologia i el paisatge amenaçador avancen ràpidament, els equips de seguretat dels sectors públic i privat s'enfronten constantment a desafiaments, un dels quals és la **manca de mà d'obra**[24]: moltes organitzacions no disposen d'executius de seguretat informàtica que contribueixin a canalitzar l'adopció de polítiques de ciberseguretat.

Tot i que la ciberseguretat esdevé un sector a l'alça pel que fa al seu creixement i a la seva projecció, segons ISC2, la **manca de professionals de la ciberseguretat assoleix els 3 milions** a tot al món, i les xifra de 142.000 persones a Europa. A l'Estat, per al 33% de les organitzacions un dels principals obstacles per a la seguretat és la **manca de personal especialitzat**[25], fins al punt que, un important volum d'empreses tenen llocs de treball vacants, pendents de cobrir. Essent aquest el context, no resulta sorprenent que aquest sigui l'àmbit TIC amb les remuneracions més elevades.

## Un paisatge cibernètic exigent

La **Directiva NIS imposa** a les entitats gestores de serveis essencials, així com als prestadors de certs serveis digitals clau, l'obligació d'establir sistemes de gestió de la seguretat de la informació en les seves organitzacions, així com de notificar a les autoritats els incidents d'especial gravetat. Així mateix, obliga als **Estats membres** a dotar-se dels mitjans per supervisar el compliment d'aquestes obligacions i a vetllar perquè hi hagi equips de resposta a incidents de seguretat amb capacitat per a protegir a les empreses de la propagació d'aquests incidents.

L'**interès geoestratègic** d'Internet conduirà alguns estats a desenvolupar iniciatives complementàries en matèria de ciberseguretat i ciberespionatge. Les noves tecnologies **requereixen adequar la normativa** per a protegir empreses i ciutadans, fet que quedarà patent en futures iniciatives reguladores sobre el ciberespai.

En definitiva sembla clar que el que abans era un espai definit i defensable, avui és un territori sense límits; una vasta i extensa petjada de dispositius, aplicacions, electrodomèstics, servidors, xarxes, núvols i usuaris. Malgrat les millors intencions de les agències de govern, els grups de control i la supervisió de la llei, el paisatge cibernètic actual és més àgil que mai[26]. Per sobreviure-hi **cal ser intel·ligent, ràpid i decidit**. Els incidents esdevenen fracassos si no són analitzats i aprenem per evitar-los i, sobretot, si no actuem per mitigar-ne les conseqüències i intentar depurar responsabilitats.

Però el risc augmenta exponencialment, l'escassetat de personal format es fa més aguda, i els recursos no són il·limitats per a la majoria d'empreses.

---

[23] Agència de Ciberseguretat de Catalunya (2021) Línies bàsiques d'un negoci cibersegur.

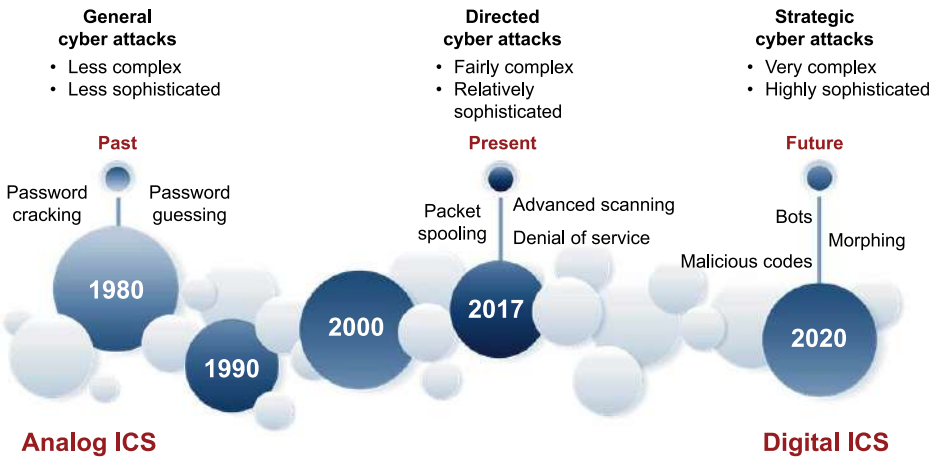
[24] Frost and Sullivan (2018) *Cyber Security Improvement Insights— Security Intelligence and Analytics.*

[25] ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic.

[26] Sonicwall (2020) Cyber threat report 2020.

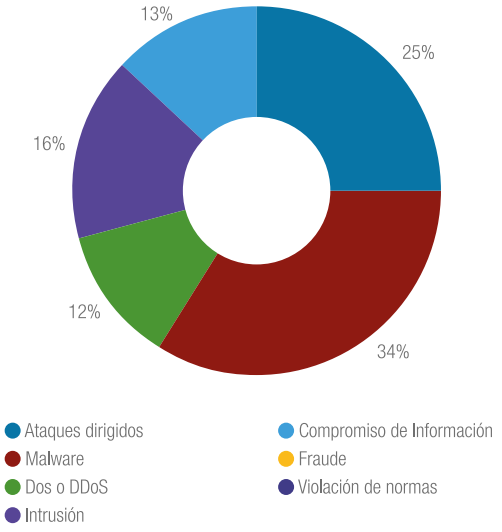
# 2
# Ciberseguretat: Infografies clau

## 2.1. Evolution of global cyber-attacks (1980-2020)



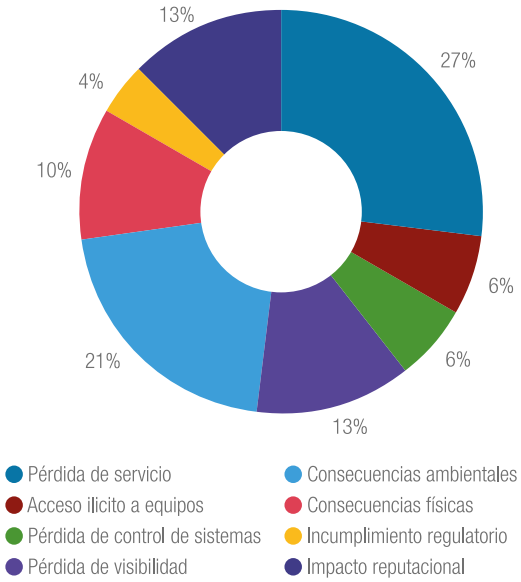

Font: Frost and Sullivan (2017) *Cyber Security In The Era Of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment*

## 2.2. Typology of industrial cybersecurity incidents in Spain (2019)



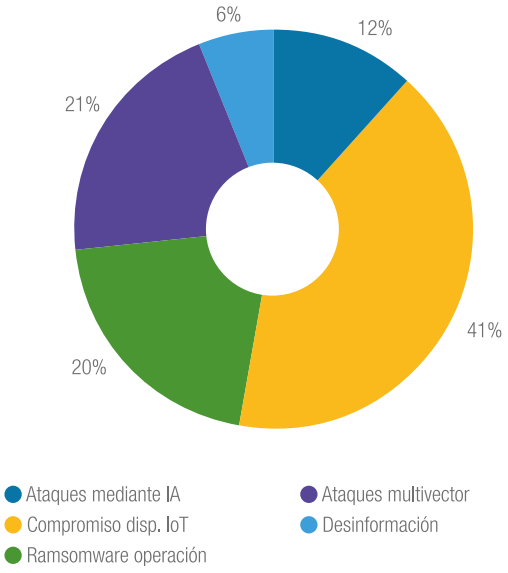

Font: Centro de Ciberseguridad Industrial (2019) *Incidentes de ciberseguridad industrial en Servicios esenciales en España. Edición 2019*

## 2.3. Consequences of industrial cybersecurity Incidents in Spain (2019)



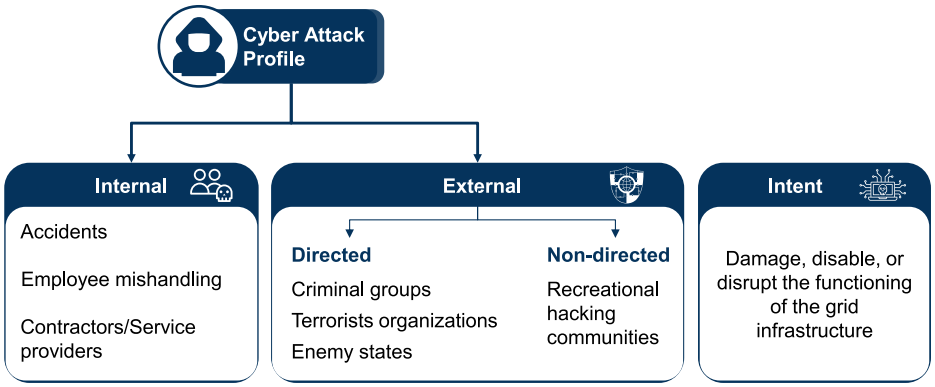

Font: Centro de Ciberseguridad Industrial (2019) *Incidentes de ciberseguridad industrial en Servicios esenciales en España. Edición 2019*

## 2.4. Outlook of future industrial cybersecurity incidents in Spain



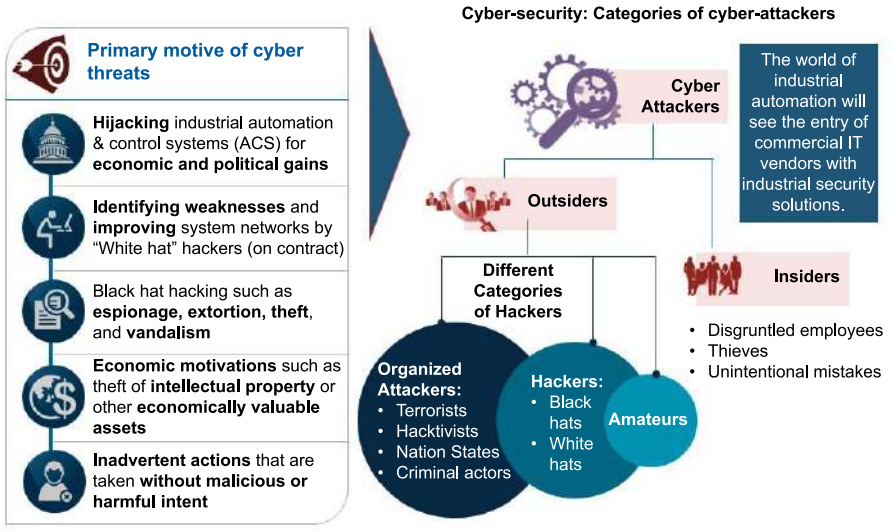

Font: Centro de Ciberseguridad Industrial (2019) *Incidentes de ciberseguridad industrial en Servicios esenciales en España. Edición 2019*

## 2.5. Typologies of cyber-attacks in the grid (2018)




Font: Frost and Sullivan (2018) *Analysis of the North American Grids Cyber Security Market, Forecast to 2022. Growing Appetite for Automation Solutions Fuels Growth in Grid Cyber Security.*

## 2.6. Cyber-attacks: Types and motives




Font: Frost and Sullivan (2017) *Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment.*

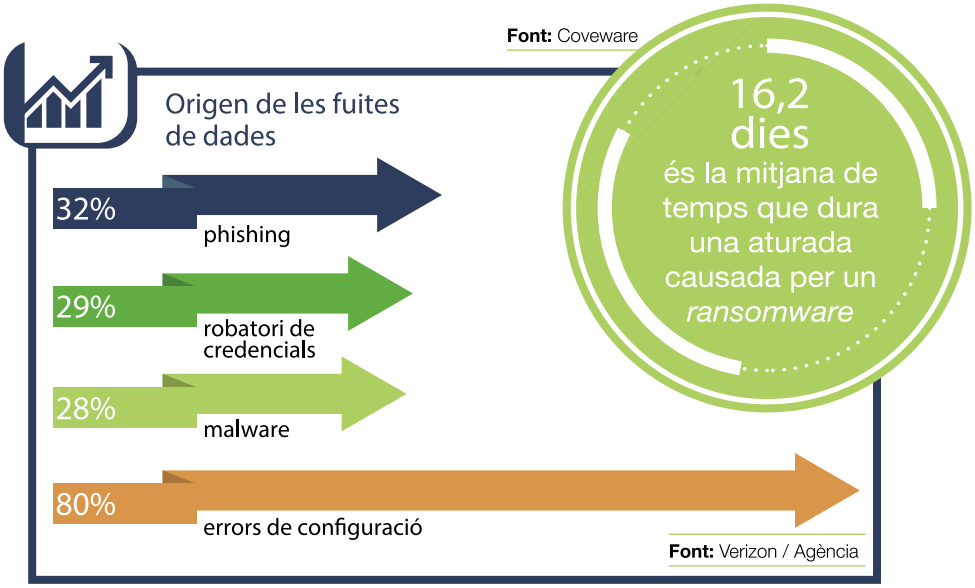
## 2.7. Agents behind cybercrime

| Agents | Motivacions | Vectors d'amenaça | Impacte |
|---|---|---|---|
| Estats/nacions | • Competició global<br>• Seguretat nacional<br>• Frau | • Cibercampanyes de llarga durada<br>• Persones infiltrades<br>• Proveïdors externs | • Pèrdua de propietat intel·lectual<br>• Disrupció d'infraestructures crítiques<br>• Pèrdues monetàries<br>• Legislatiu |
| Cibercriminals | • Enriquiment il·lícit<br>• Frau<br>• Suplantació d'identitat | • Robatoris individuals d'identitat<br>• Esquerdes de dades i robatori de propietat intel·lectual<br>• Persones infiltrades<br>• Per mitjà de proveïdors tecnològics | • Pèrdua d'identitat<br>• Pèrdues dineràries<br>• Pèrdua de propietat intel·lectual<br>• Privacitat<br>• Legislatiu |
| Ciberterroristes/ *hackers* individuals | • Ideològiques<br>• Polítiques<br>• Privació de drets<br>• Crear el caos | • Vulnerabilitats oportunístiques<br>• Persones infiltrades<br>• Per mitjà de proveïdors tecnològics | • Desestabilitzar, pertorbar i destruir actius d'institucions financeres<br>• Legislatiu |
| Hacktivistes | • Causa política abans que guany personal<br>• Ideològiques | • Organitzacions que s'interposen a la seva causa<br>• Persones infiltrades<br>• Proveïdors externs | • Disrupció d'operacions<br>• Desestabilització<br>• Vergonya/imatge<br>• Relacions públiques<br>• Legislatiu |

* Els cibercriminals són els principals agents que ataquen les indústries

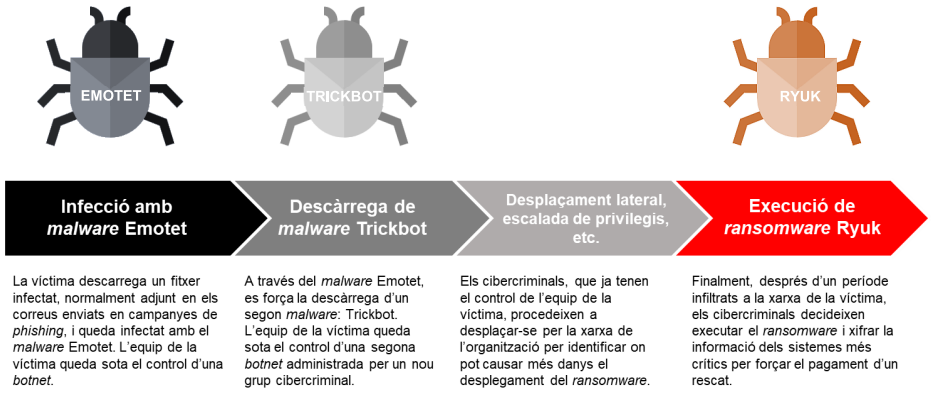
Font: ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic

## 2.8. Origin of data leaks




Font: Agència de Ciberseguretat de Catalunya (2020) Línies bàsiques d'un negoci cibersegur

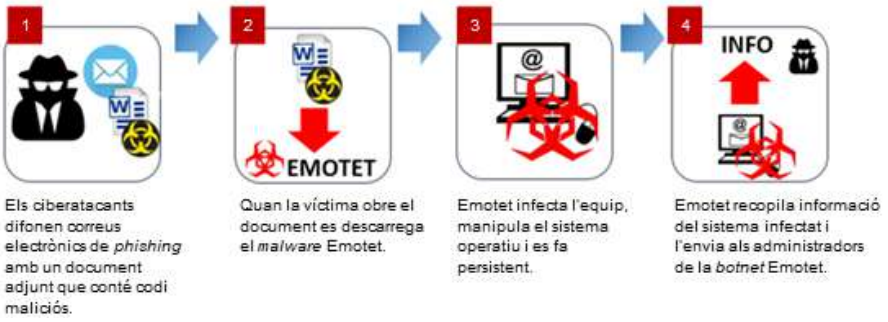
## 2.9. Stages of the attack in the ransomware dissemination campaign




*Il·lustració 1. Fases de l'atac en la campanya de difusió del* ransomware *Ryuk*

Font: Agència de Ciberseguretat de Catalunya (2019) Informe de tendències de ciberseguretat T3 2019: "La triple amenaça"

## 2.10. Phases of the triple threat: Emotet, Trickbot, Ryuk




*Il·lustració 9. Primera fase de l'atac amb la triple amenaça: Emotet*


*Il·lustració 10. Segona fase de l'atac amb la triple amenaça: Trickbot*


Il·lustració 11. Tercera fase de l'atac amb la triple amenaça: Ryuk

Font: Agència de Ciberseguretat de Catalunya (2019) Informe de tendències de ciberseguretat T3 2019: "La triple amenaça"

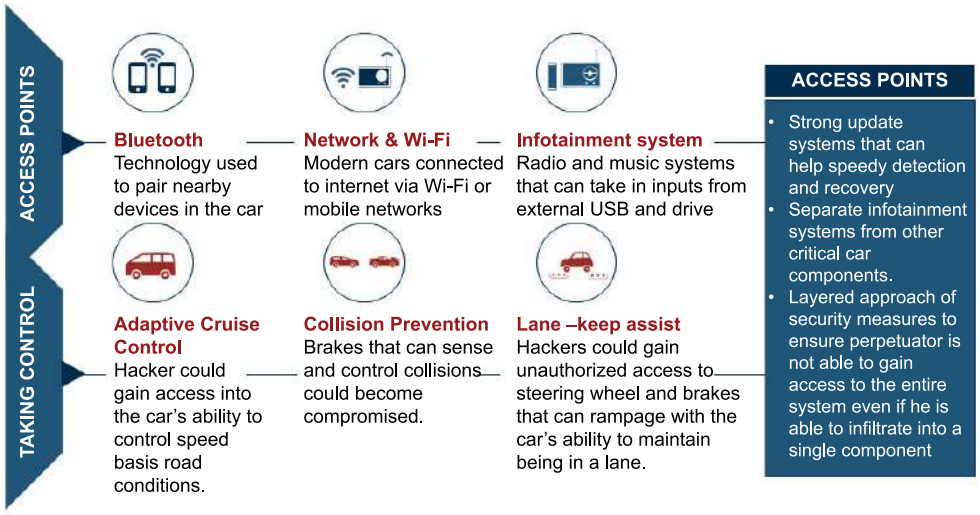
## 2.11. Monthly cost / benefit from exploiting a botnet

| | Atac DDoS | Frau bancari | Correu brossa | Frau de clics |
|---|---|---|---|---|
| Malware | variant de Mirai* | Zeus | ? | ZeroAccess |
| Nombre de bots | 30.000 bots | 30.000 bots | 10.000 bots | 140.000 bots |
| Cost del paquet demalware | -$30 | -$700 a -$10.000 | ? | -$700 a -$10.000 |
| Cost de distribució (PPI = 0,0935 $)** | -$2.805 | -$2.805 | -$935 | -$13.090 |
| Cost del hosting bulletproof | -$2.400 | -$70 | -$2.400 | -$70 |
| Manteniment | ? | -$5.167 | ? | ? |
| Màrqueting | -$2.400 | -$2.400 | ? | ? |
| Ingressos mensuals | $26.000 | $18.800.000 | $300.000 | $25.000.000 |
| Cost del moviment dels diners (3% de comissió) | -$780 | -$564.000 | -$9.000 | -$750.000 |
| Beneficis mensuals aproximats | ~20 K$ | ~18 M$ | ~290 K$ | ~24 M$ |

* El codi de Mirai es va fer públic el 2016 i és habitual l'aparició de noves variants.
** PPI = Pagament per Infecció; es considera que els bots s'han de reinfectar cada mes.

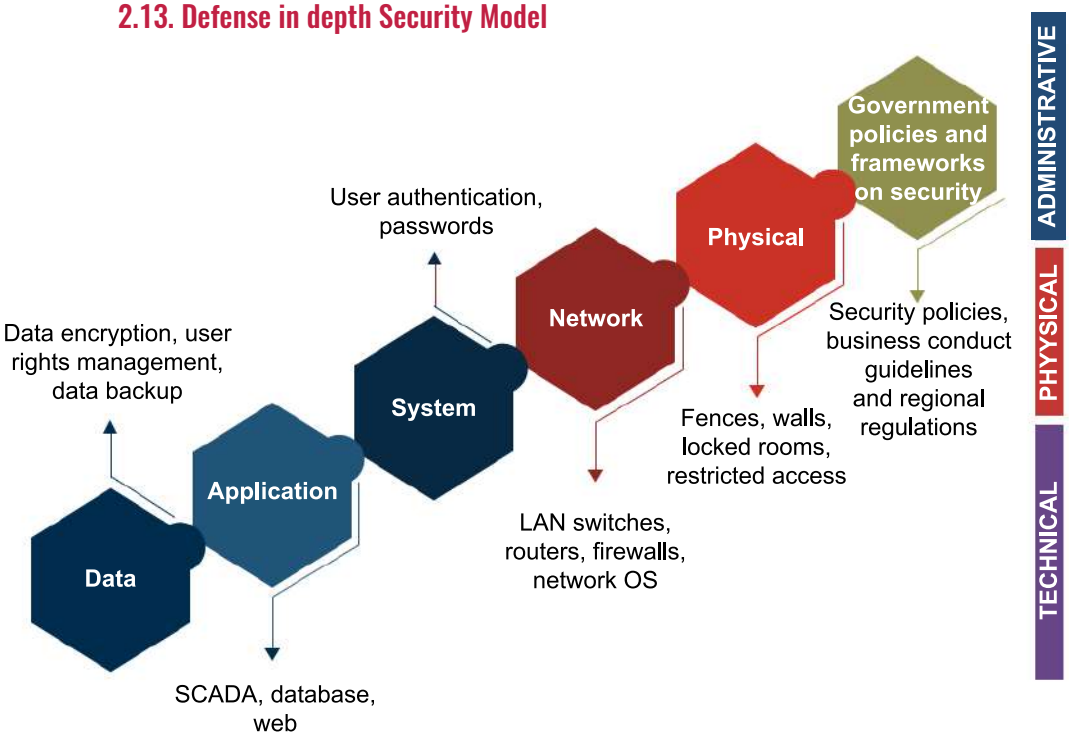
Font: Agència de Ciberseguretat de Catalunya (2019) Informe de tendències de ciberseguretat T3 2019: "La triple amenaça"

## 2.12. Potential cyber-threats in a connected car



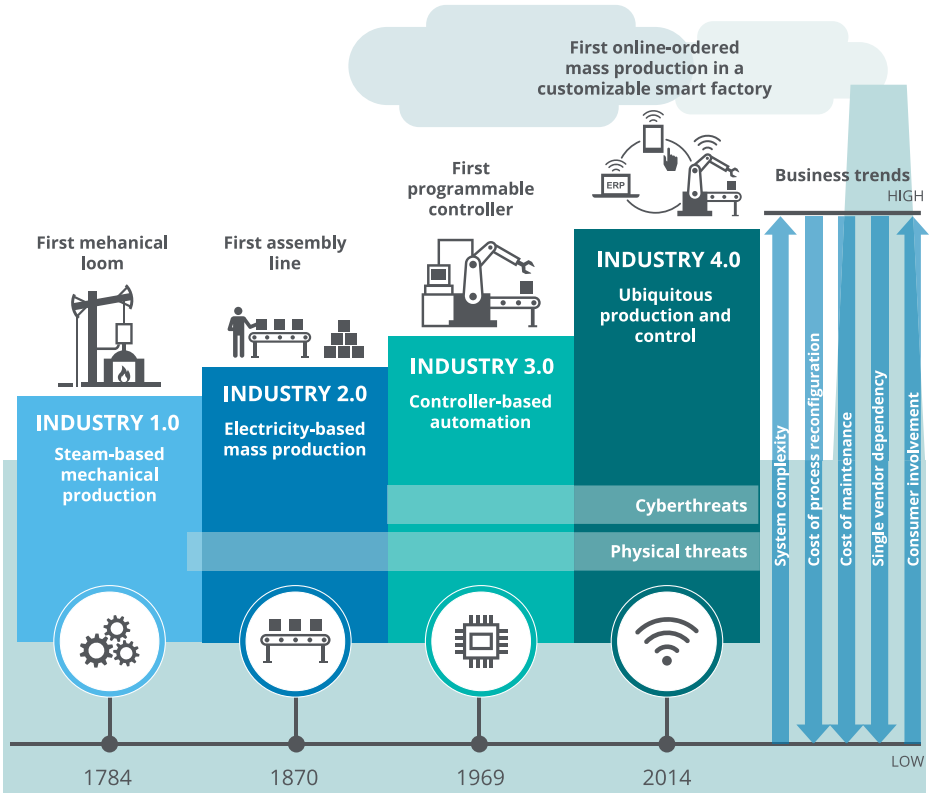

Font: Frost and Sullivan (2017) *Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment*

## 2.13. Defense in depth Security Model



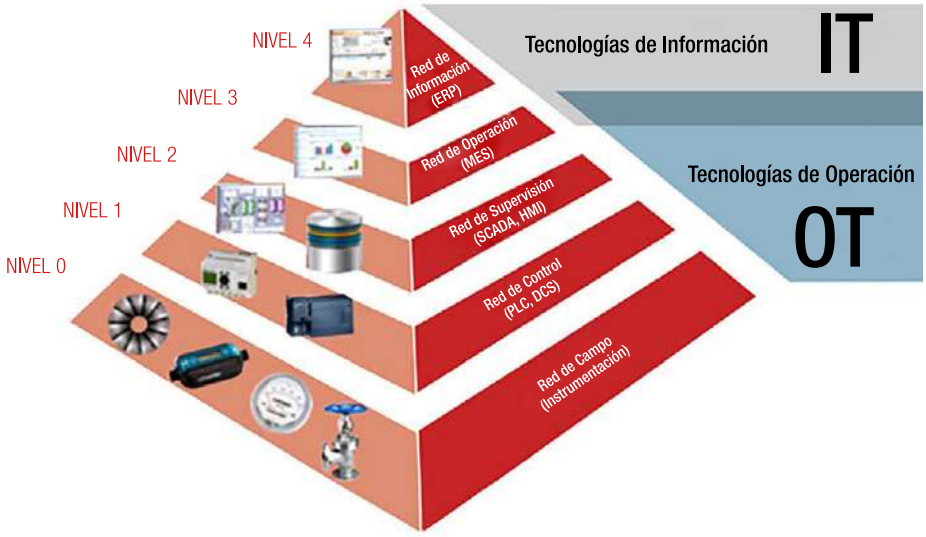

Font: Frost and Sullivan (2017) *Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment*

## 2.14. Progression of cyber and physical threats for each industrial revolution



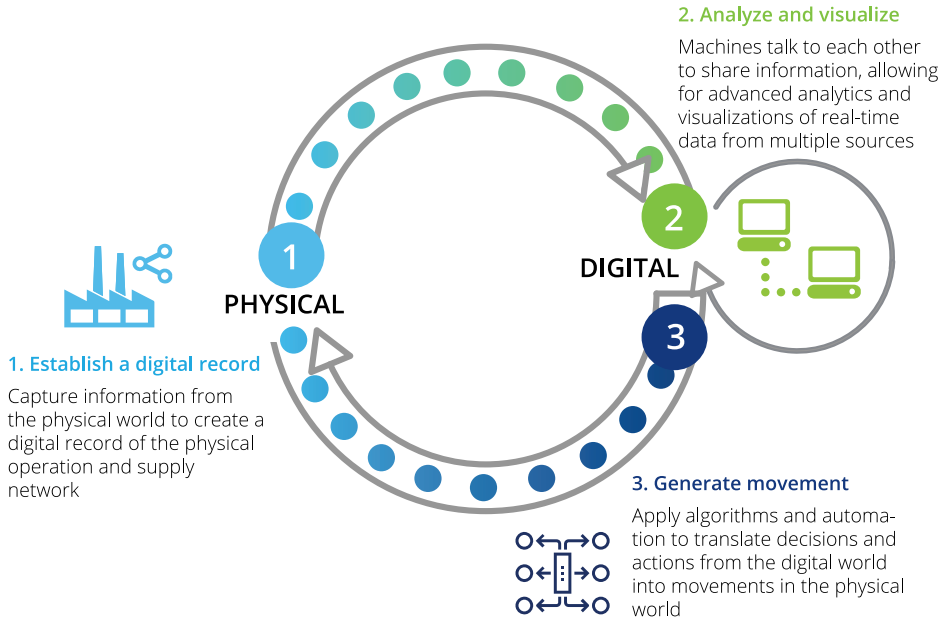

Font: Waslo, Lewis, Hajj i Carton (2017) *Industry 4.0 and cibersecurity: Deloitte*

## 2.15. Levels of industrial automation technologies



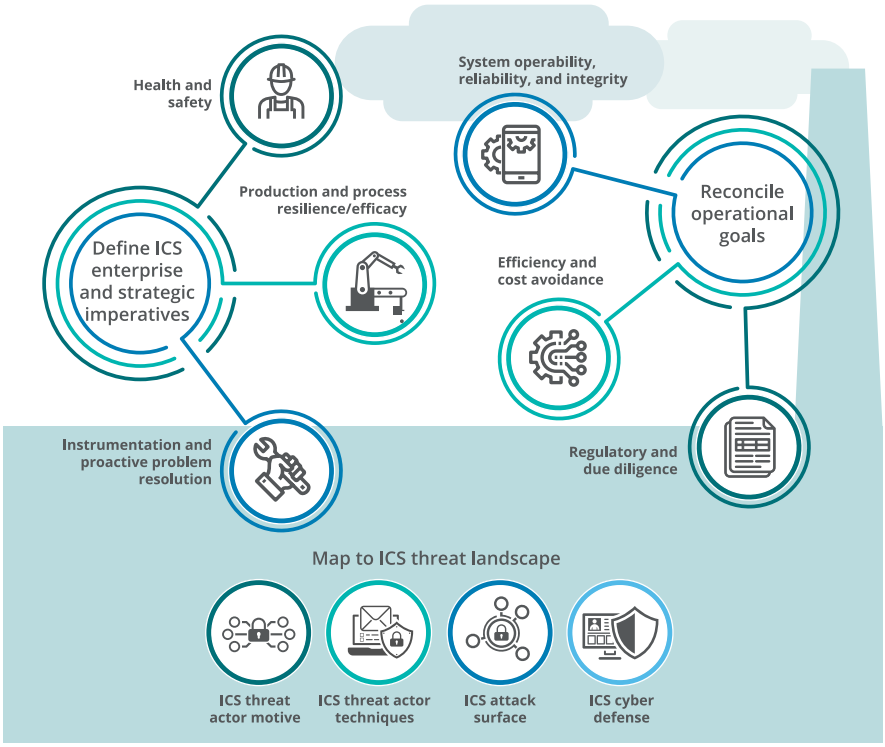

Font: Centro de Ciberseguridad Industrial (2019) *Incidentes de ciberseguridad industrial en Servicios esenciales en España. Edición 2019*

## 2.16. The physical-digital leap of industry 4.0



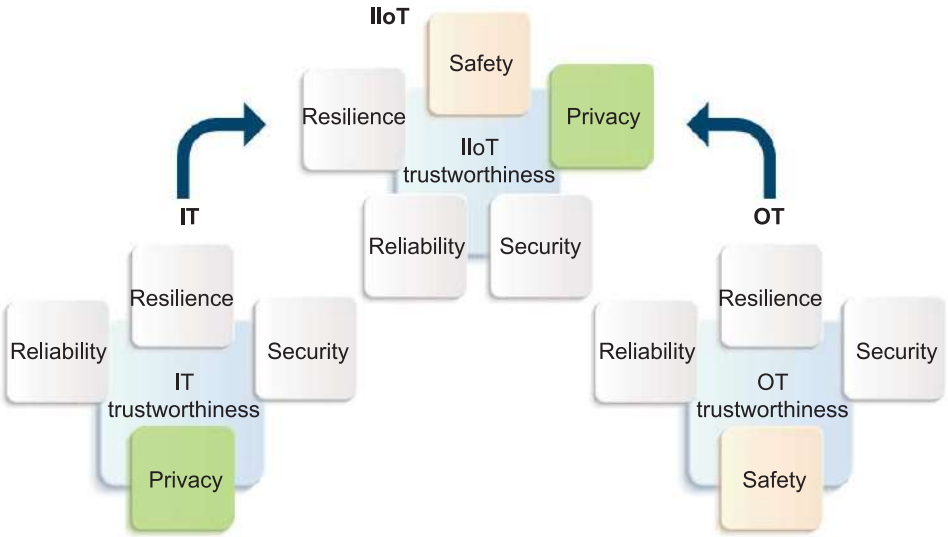

Font: Waslo, Lewis, Hajj i Carton (2017) *Industry 4.0 and cibersecurity: Deloitte*

## 2.17. Smart factory business divers and threat landscape



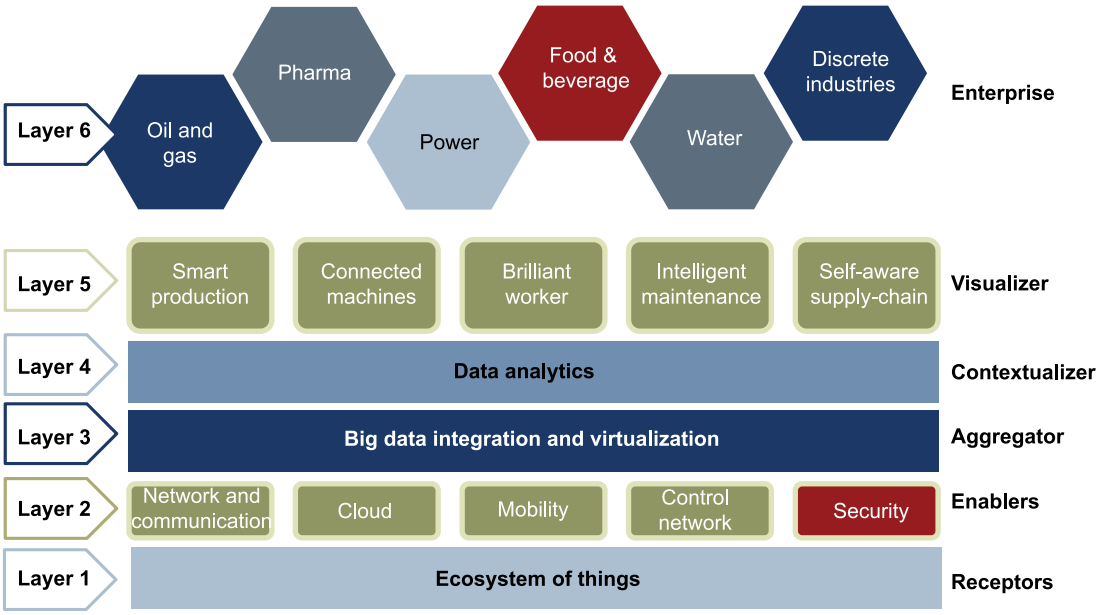

Font: Waslo, Lewis, Hajj i Carton (2017) *Industry 4.0 and cibersecurity: Deloitte*

## 2.18. Converging IT and OT for trustworthiness in Industrial Internet of Things (IIoT)



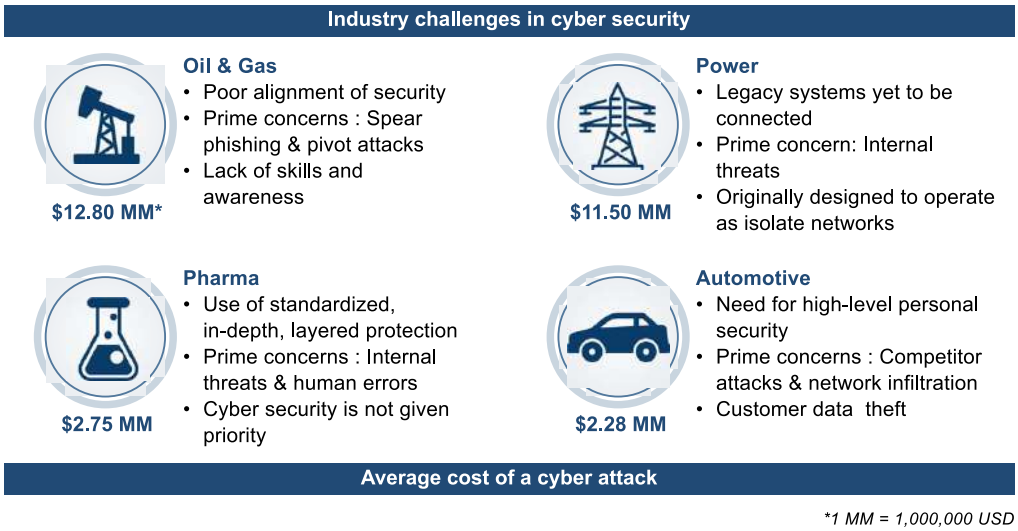

Font: Frost and Sullivan (2017) *Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment*

## 2.19. Cyber Security: A key enabler in the future industrial enterprise




Font: Frost and Sullivan (2017) *Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment*

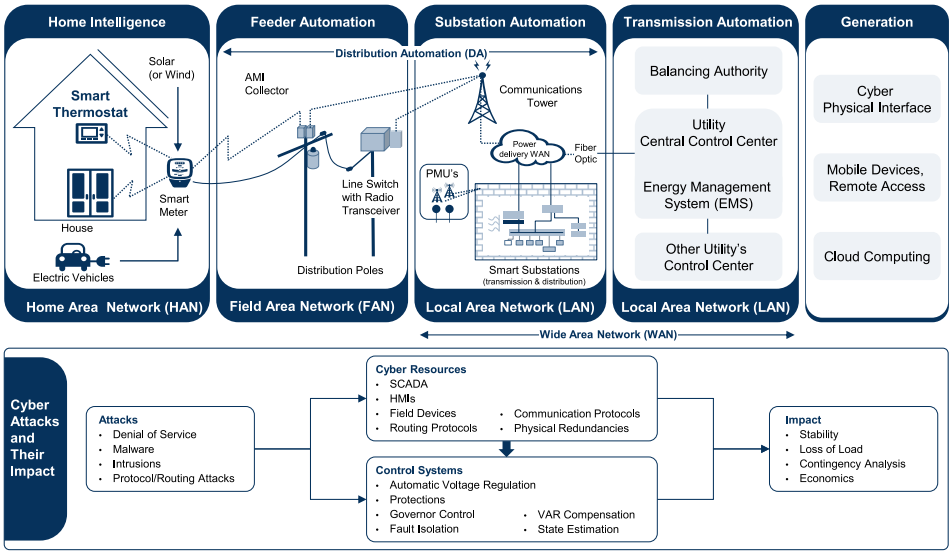
## 2.20. Challenges that plague critical infrastructures




**1 MM = 1,000,000 USD*

Font: Frost and Sullivan (2017) *Cyber Security In the era of Industrial IOT - Discerning implications of cyber security in a converged IT-OT environment*

## 2.21. Cyber Attacks on the grid and their impact

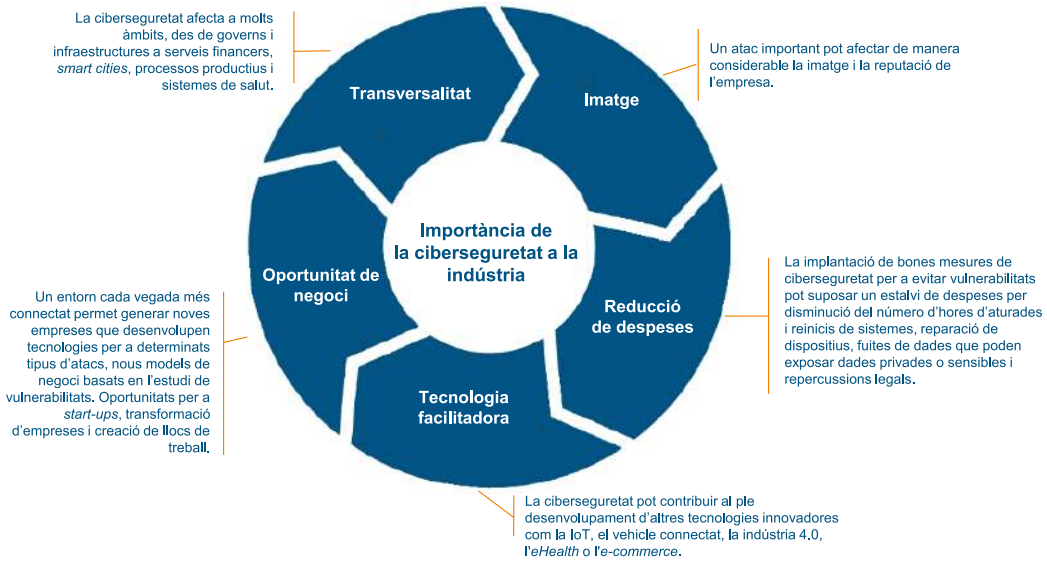



Font: Frost and Sullivan (2018) *Analysis of the North American Grids Cyber Security Market, Forecast to 2022. Growing Appetite for Automation Solutions Fuels Growth in Grid Cyber Security*

## 2.22. Main technological trends in cybersecurity

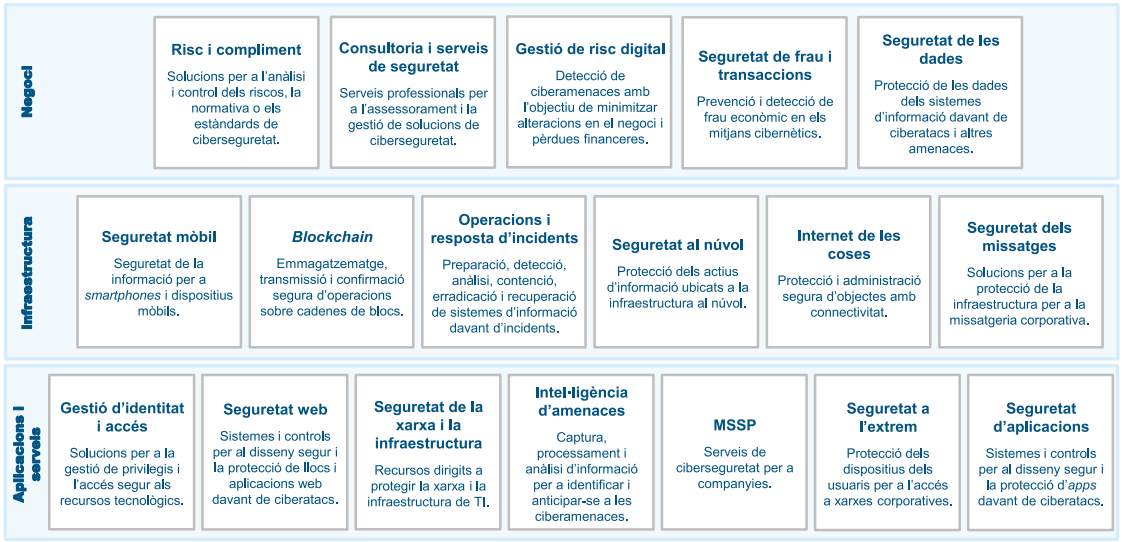

Font: ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic

## 2.23. Importance of cybersecurity for industry




Font: ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic

## 2.24. Cybersecurity: Activity areas and Technologies

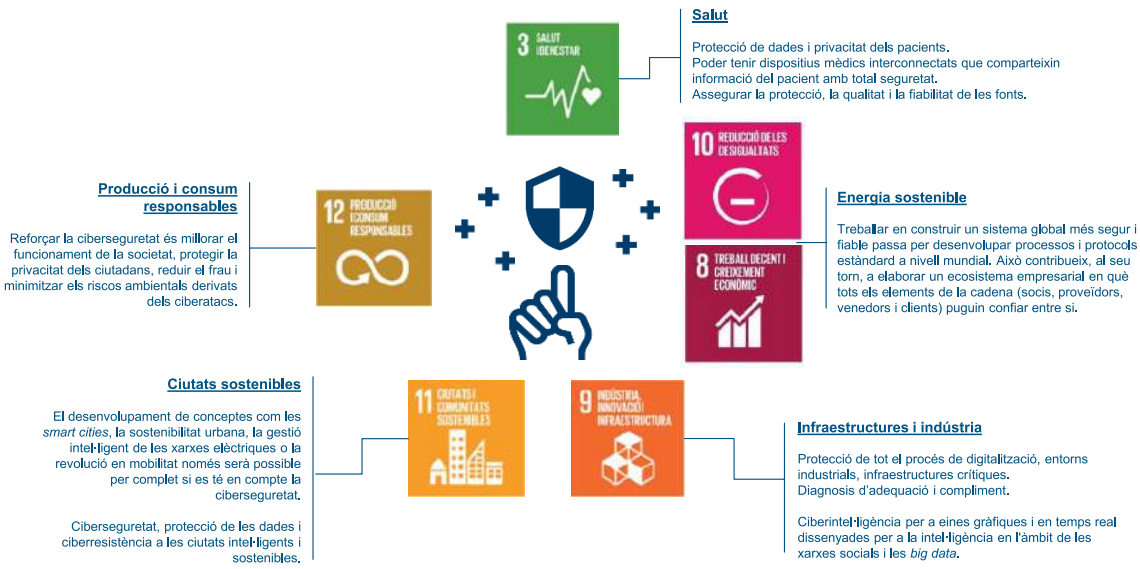



Font: ACCIO i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic

## 2.25. Cybersecurity ecosystem in Catalonia (2019)


Font: ACCIÓ i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic

## 2.26. Cybersecurity and sustainable development goals



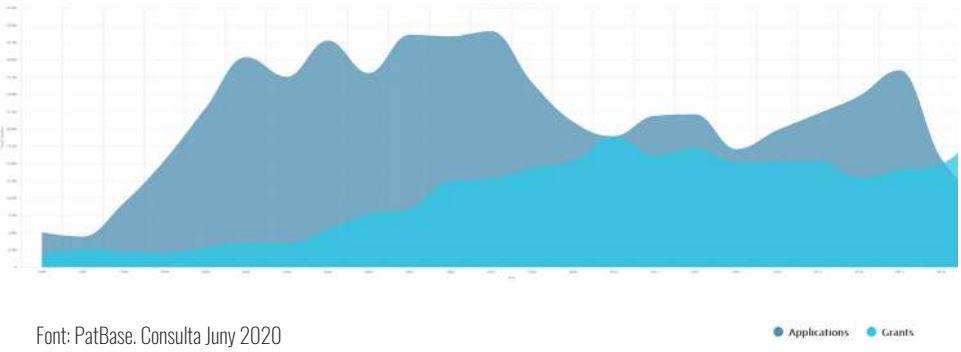

Font: ACCIÓ i CESICAT (2019) La ciberseguretat a Catalunya: informe tecnològic

# 3
# Anàlisi de patents

## 3.1. Evolució patents sol·licitades i concedides

L'anàlisi de patents sol·licitades i concedides en l'àmbit de Ciberseguretat permet apreciar una **tendència de creixement**, amb un increment molt significatiu el 2007 i un segon pic a finals de 2017 (aquest volum significatiu probablement es manté encara, però no es reflecteix en el gràfic per la demora de 18 mesos entre les sol·licituds de patents i la seva publicació).

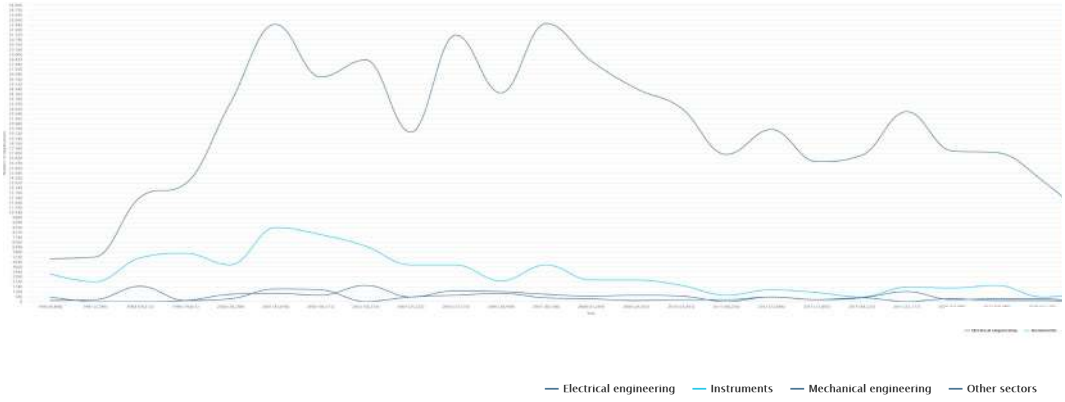
L'anàlisi també il·lustra que la proporció de patents sol·licitades que finalment foren **concedides** fou del **55%**.




Font: PatBase. Consulta Juny 2020

## 3.2. Sector tecnològic de les patents sol·licitades

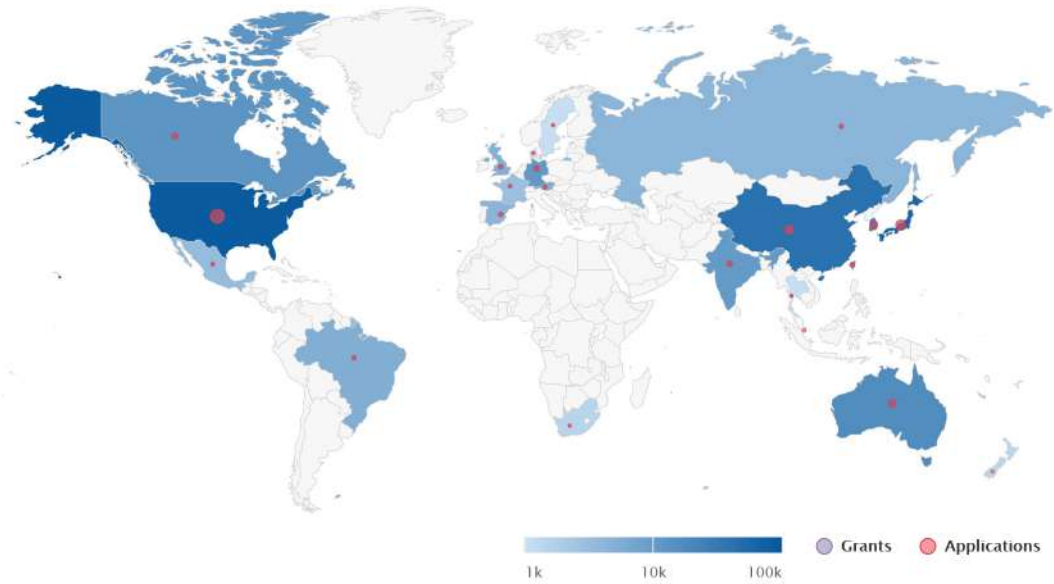
En les dues darreres dècades, les tecnologies més actives en patents sol·licitades en la indústria de la ciberseguretat pertanyen sobretot als camps següents: **enginyeria elèctrica, instruments, enginyeria mecànica i altres** sectors.




Font: PatBase. Consulta Juny 2020

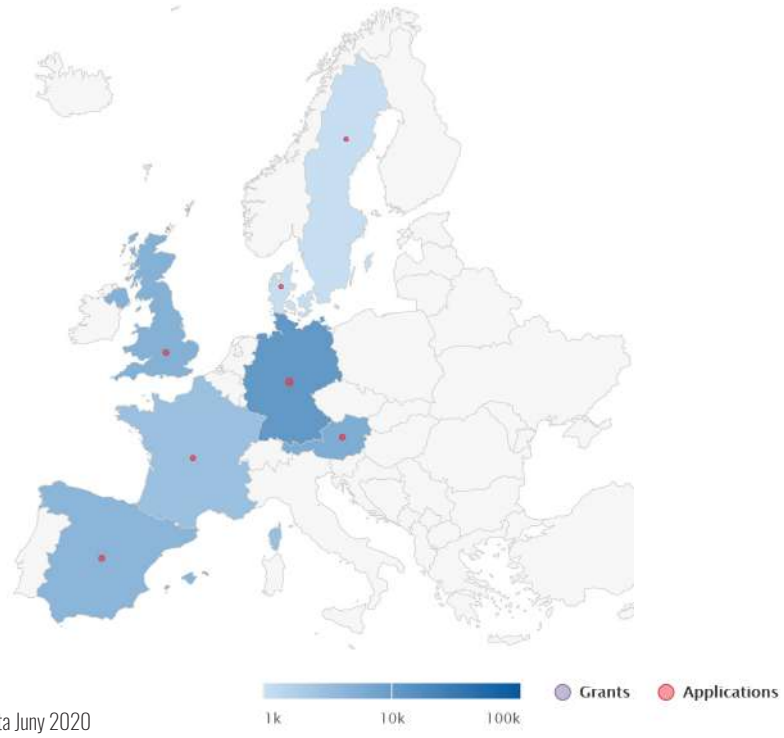
## 3.3. Localització territorial de patents

A **nivell global**, sobre aquest tòpic, les oficines regionals que els darrers 25 anys han encapçalat la demanda de sol·licituds de patents són les dels **Estats Units** i la **Xina**, seguides de les d'Austràlia, la Unió Europea i Brasil.




Font: PatBase. Consulta Juny 2020

Dins de la **Unió Europea**, els països amb més sol·licituds de patents són, tal com es mostra al següent mapa, **Alemanya, Anglaterra, Espanya i França.**

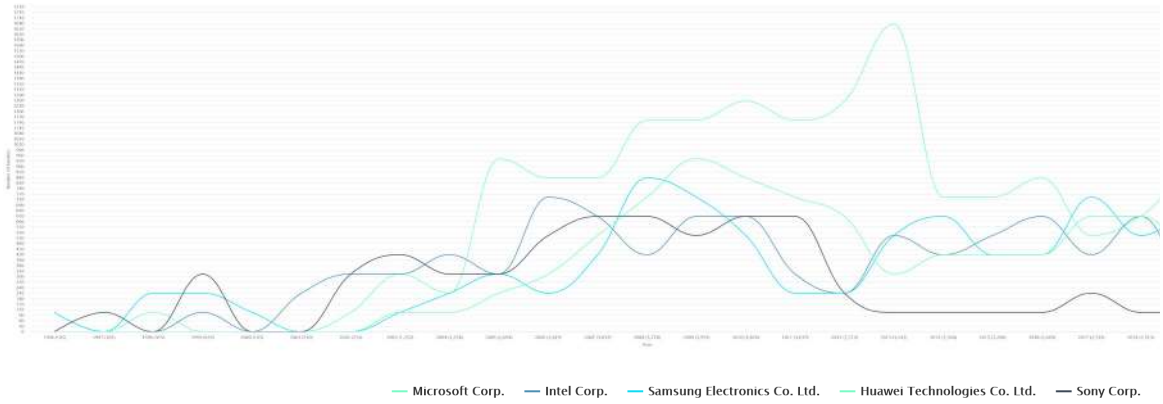



Font: PatBase. Consulta Juny 2020

## 3.4. Sol·licitants de patents més actius

En el següent gràfic s'explicita, des de 1996, quines són les organitzacions més actives en sol·licitants de patents, així com els períodes temporals en els que s'han concentrat aquestes sol·licituds.

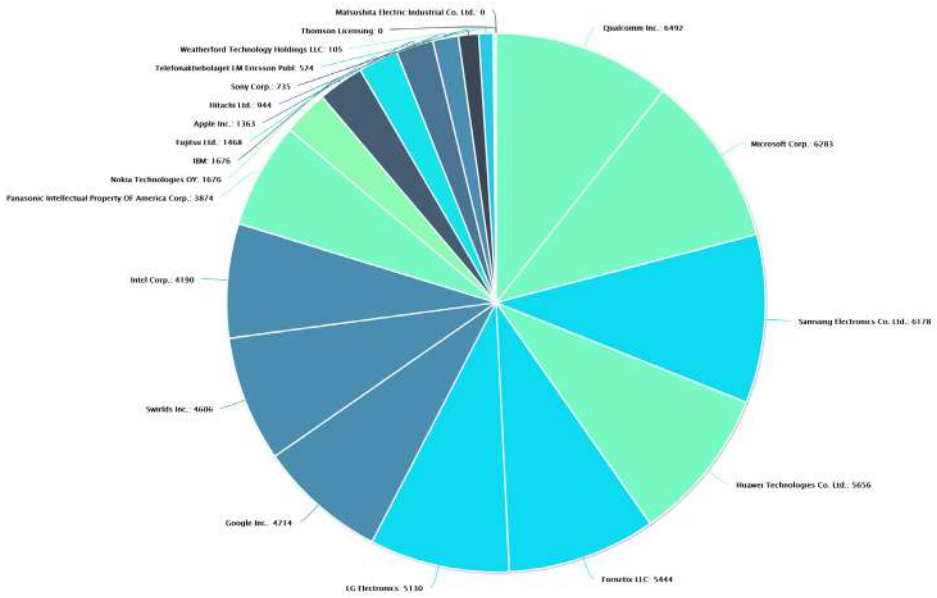
Destaquen, entre d'altres, les cinc següents: **Microsoft** Corp, **Intel** Corp, **Samsung** Electronics Co, **Huawei** Technologies Co i **Sony** Corp.




Font: PatBase. Consulta Juny 2020

## 3.5. Altres sol·licitants de patents actius

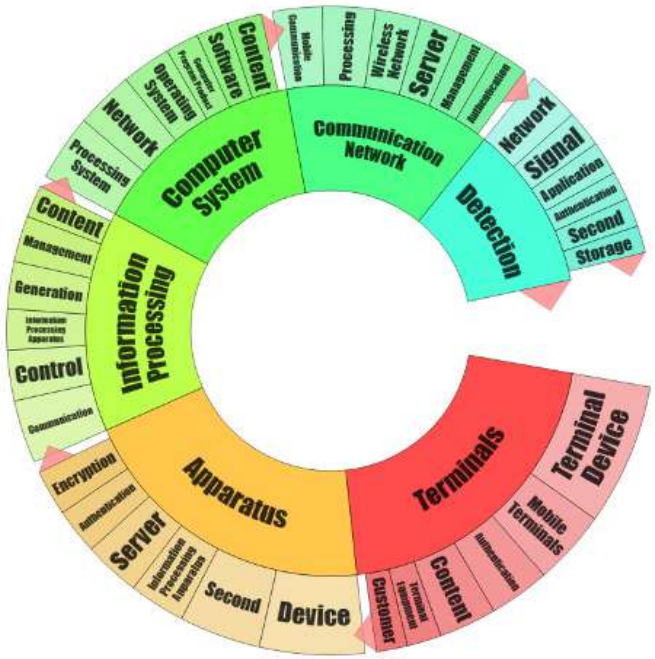
A continuació es mostren les 20 **entitats** (empreses, institucions o persones) sol·licitants de patents, especificant el **volum d'operacions** tramitades per cadascuna. Destaquen, entre d'altres, **Google**, **LG** Electronics, Swirlds Inc, Fornetix LLC, Samsung Electronics, Qualcomm Inc i Microsoft Corp.




Font: PatBase. Consulta Juny 2020

## 3.6. Paraules clau atribuïdes a les patents en aquest camp

Les principals paraules clau atribuïdes a les sol·licituds de patents en el camp d'estudi són les següents: **aparells, terminals, detecció, processament d'informació, xarxa de comunicació i sistema informàtic.**




Font: PatBase. Consulta Juny 2020

## 3.7. ANNEX METODOLÒGIC

La informació aportada en el capítol "Anàlisi de patents" es refereix a l'estudi realitzat sobre una mostra de **554.944 sol·licituds de patents** en l'àmbit de ciberseguretat.

**155.820**
Família de patents

Nombre total de famílies en aquest conjunt de resultats

**96.276**
Família de patents concedides

Nombre total de famílies amb publicacions concedides en aquest conjunt de resultats

**554.944**
Sol·licituds

Aplicacions en aquest resultat

**786.319**
Publicacions

Publicacions en aquest resultat

Font: PatBase. Consulta Juny 2020

## Principis sobre l'àmbit

- En aquest informe, la **ciberseguretat** ha estat definida com el "conjunt de tecnologies, processos i pràctiques desenvolupades per protegir tots els sistemes connectats a internet i les dades contra qualsevol atac digital, així com la pràctica per garantir la integritat, confidencialitat i disponibilitat de la informació".
- La seguretat de la informació al ciberespai ha esdevingut extremadament crucial, i les **innovacions de productes de programari** requereixen una protecció adequada de patents.
- Els **agents de patents** desenvolupen estratègies de protecció a través de patents per a actius d'innovació relacionats amb la ciberseguretat: invencions relacionades amb ordinador, programari, intel·ligència artificial i aprenentatge automàtic, incloses les patents de processos i productes.
- La **redacció de patents és una tasca extremadament complexa**. El contingut de les sol·licituds inclou una descripció completa del millor mode d'implementació del programari innovador, descrit mitjançant figures que il·lustren diagrames de flux i arquitectura del sistemes. Especialment la redacció de reivindicacions de patents per a invencions relacionades amb software, requereix una comprensió detallada de les novetats que cal reclamar.
- A més a més cal remarcar que, a Europa, els programes d'ordinador o **algoritmes**, per se, són excloïbles de patentabilitat. Sí que són patentables, però, d'invencions que apliquen algoritmes per a la **resolució** de problemes tècnics.

## Consideracions metodològiques de l'anàlisi de patents

- La font d'aquesta anàlisi és **PatBase**.
- La consulta fou realitzada el juny de **2020**.
- Aquest estudi s'ha centrat en l'activitat de patents **mundial** els últims vint-i-cinc anys, posant un especial èmfasi a **Europa**.
- El criteri pel que s'ha fet la cerca i generat la mostra ha estat del **màxim abast** en el camp. S'han utilitzat tant **paraules clau**, com **codis de patents** definitoris de l'àmbit.
- Respecte a paraules clau, per delimitar la mostra de l'àmbit "ciberseguretat" s'ha considerat la inclusió, entre d'altres, de les següents:

  - Sistemes d'informació
  - Processament d'informació
  - Sistemes informàtics.

## Codis de patents per obtenir la mostra

- És sabut que les bases de dades de patents estan ordenades mitjançant diversos **sistemes internacionals de classificació**, essent els més utilitzats l'*International Patent Classification* (**IPC**) i *Cooperative Patent Classification* (**CPC**) per a camps més específics.
- Per a l'obtenció de la mostra d'aquest informe únicament s'ha considerat la inclusió d'índexs **IPC**. Són, específicament, els següents:

- H04L63/00
  Network architectures or network communication protocols for network security (cryptographic mechanisms or cryptographic arrangements for secret or secure communication H04L9/00; network architectures or network communication protocols for wireless network security H04W12/00; security arrangements for protecting computers or computer systems against unauthorised activity G06F21/00)

- G06F21/00
  Security arrangements for protecting computers, components thereof, programs or data against unauthorised activity

- H04W12/00
  Security arrangements, e.g. access security or fraud detection; Authentication, e.g. verifying user identity or authorisation; Protecting privacy or anonymity; Protecting confidentiality; Key management; Integrity; Mobile application security; Using identity modules; Secure pairing of devices; Context aware security; Lawful interception

- H04L67/00
  Network-specific arrangements or communication protocols supporting networked applications (message switching systems H04L51/00; network management protocols H04L41/00; routing or path finding of packets in data switching networks H04L45/00; protocols for real-time multimedia communication H04L65/00; information retrieval G06F16/00; services or facilities specially adapted for wireless communication networks H04W4/00; network structures or processes for video distribution between server and client or between remote clients H04N21/00; exchange systems providing special services or facilities to subscribers involving telephonic communications H04M3/42; distributed information systems G06F9/00, G06F17/00; lower layer network functionalities which support application layer provisions H04L12/00)

- H04L9/00
  Cryptographic mechanisms or cryptographic arrangements for secret or secure communication (network architectures or network communication protocols for network security H04L63/00 or for wireless network security H04W12/00; security arrangements for protecting computers or computer systems against unauthorized activity G06F21/00)

- G06Q20/00
  Payment architectures, schemes or protocols (apparatus for performing or posting payment transactions G07F7/08, G07F19/00; electronic cash registers G07G1/12)

- G06F16/00
  Information retrieval; Database structures therefor; File system structures therefor

- H04L12/00
  Data switching networks (interconnection of, or transfer of information or other signals between, memories, input/output devices or central processing units G06F13/00)

- H04W8/00
  Network data management

- H04L41/00
  Arrangements for maintenance or administration or management of packet switching networks.

# hubb30.

## UNA ALIANÇA PER PROMOURE LA INNOVACIÓ DEL TERRITORI B30

www.hubb30.cat

Una iniciativa de:

CSIC IRTA UAB Parc de Recerca UAB

UAB Universitat Autònoma de Barcelona

eurecat Centre Tecnològic de Catalunya

Associació Àmbit B30

UPC UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

ALBA

esadecreapolis

CONSELL COMARCAL DEL VALLÈS OCCIDENTAL

Generalitat de Catalunya ACCIÓ

SCE SANT CUGAT EMPRESARIAL

CERDANYOLA EMPRESARIAL

UPC UPIC UNIÓ DE POLÍGONS INDUSTRIALS DE CATALUNYA Cambra

cecot

Projecte cofinançat per:

Generalitat de Catalunya
Departament d'Empresa i Coneixement
Secretaria d'Universitats i Recerca

Unió Europea
Fons Europeu
de Desenvolupament Regional