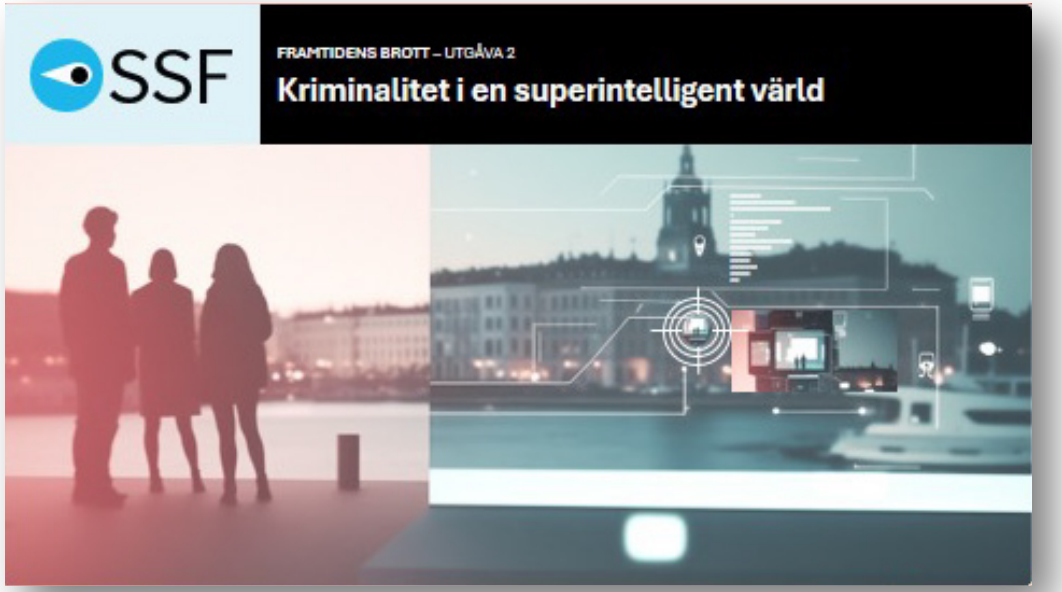
FRAMTIDENS BROTT – UTGÅVA 2

Kriminalitet i en superintelligent värld

Förord



På Stöldskyddsföreningen drivs vi av en genuin nyfikenhet inför den snabbt föränderliga värld vi lever i. Vi ser hur våra hem, fordon och vardagsföremål blir alltmer uppkopplade och intelligenta – en utveckling som både fascinerar och utmanar. Genom att samla insikter från forskning, trender och experter vill vi måla upp en bild av hur framtidens superintelligenta samhälle kan se ut när den fysiska och digitala världen går samman. Och hur detta kan komma att påverka framtida brott, bedrägerier och cyberattacker.

Framtiden är alltid oviss. Ingen av oss vet exakt hur tekniken kommer att förändra våra liv, våra hem eller vårt samhälle. Men genom att ställa frågor, utforska trender och våga föreställa oss olika möjligheter kan vi lägga några av de pusselbitar som behövs för att förstå vart vi är på väg. Pusselbitar som ger oss själva ett värdefullt underlag för hur vi ska forma vårt brottsförebyggande arbete, både idag och imorgon. Den här rapporten kan kanske också hjälpa er med insikter om hur kriminalitet påverkar ert arbete i takt med att våra produkter blir allt smartare och världen mer uppkopplad.

Vi gör inte anspråk på att ge en heltäckande bild, men hoppas att våra reflektioner, exempel och scenarier kan inspirera till vidare samtal och nya perspektiv.

Vår förhoppning är att rapporten ska bidra till att fler vågar tänka kring framtidens utmaningar och möjligheter – och att vi tillsammans kan arbeta för en tryggare vardag, oavsett hur framtiden tar form.

Jag vill rikta ett varmt tack till Ulrika Hallesius på Stöldskyddsföreningen och Charlotte Mattfolk på IAMAI för ert engagemang, driv och insikter som varit avgörande för att denna rapport kommit till. Och tack alla ni experter som generöst delat med er av era insikter. Utan er alla hade denna rapport inte varit möjlig.

Med vänlig hälsning

Thomas Brühl, VD Stöldskyddsföreningen

Konceptet Framtidens Brott är en serie av publikationer som utforskar framtidens brottslighet ur olika perspektiv.

UTGÅVA 1

Den kriminella spelplanen – en analys av den globala brottsmarknaden.
Lansering kvartal 4 2024.

UTGÅVA 2

En framtidsanalys på den kommande superintelligenta vardagsmiljön.
Lansering kvartal 2 2025.

UTGÅVA 3

Samproduceras tillsammans med partners. Tema sätts längre fram.
Lansering kvartal 4 2025.

UTGÅVA 4

Samproduceras tillsammans med partners. Tema sätts längre fram.
Lansering kvartal 1 2026.

Innehåll

Sammanfattning

Den teknologiska utvecklingen förändrar på många sätt hur vi lever våra liv. Smarta hem med artificiell intelligens blir allt vanligare och erbjuder stora möjligheter till ökad bekvämlighet, effektivitet och säkerhet.

Samtidigt medför denna utveckling nya utmaningar och risker, inte minst gällande personlig integritet och kriminalitet. I takt med att fler föremål och miljöer blir uppkopplade och intelligenta, öppnas också nya vägar för brottslighet som kan vara svåra att hantera.

Denna rapport syftar till att utforska hur kriminaliteten kan komma att utvecklas i en framtid där våra hem och samhällen är djupt integrerade med avancerad teknik.

I rapporten beskrivs den digitala utvecklingen mot superintelligens i våra hem och hur teknik kan förändra vardagslivet.

Vidare illustreras möjliga brottsscenarion – fiktiva men ändå med en realistisk vinkel utifrån trender. Scenarierna exemplifierar hur brott kan ta sig nya uttryck i en uppkopplad värld. I anslutning till dessa scenarier berörs de etiska och samhälleliga frågor som uppstår när data blir makt och beslut fattas av maskiner - hur säkerställs transparens, rättvisa och respekt för privatlivet?

Avslutningsvis exemplifieras åtgärder och lösningar, både tekniska och samhälleliga, för att förebygga brott och stärka säkerheten i framtidens superintelligenta vardag. Där understryker vi betydelsen av samverkan mellan myndigheter, företag, forskning och civilsamhälle, liksom vikten av utbildning och medvetandegörande.

Med denna rapport vill vi på Stöldskyddsföreningen bidra till en ökad förståelse för de komplexa utmaningar och möjligheter som den digitala utvecklingen för med sig. Vår förhoppning är att vårt arbete ska inspirera fler att bidra till en stärkt digital säkerhet, samt fungera som ett underlag för fortsatt diskussion och insatser för att skapa en tryggare och mer hållbar framtid för alla.

Kriminalitet i en superintelligent värld

AI är på väg mot det som kallas artificiell superintelligens: system som överträffar mänsklig intelligens inom alla områden. I detta scenario blir den digitala infrastrukturen inte längre ett verktyg – utan ett självorganiserande, tänkande ekosystem.

Mot en självtänkande infrastruktur

Vi är på väg från en statisk och uppkopplad miljö till en dynamisk, självtänkande och autonom infrastruktur där enheterna inte bara är uppkopplade utan också självständigt kan förstå och agera utifrån vår omgivning.

Hur balanserar vi bäst denna autonoma utveckling med mänsklig kontroll – och vem, i slutändan, kommer att styra över den intelligenta framtid som vi nu bygger?

Hur en superintelligent värld gör vardagen bekvämare

I en superintelligent värld anpassar sig hemmets enheter automatiskt efter dina dagliga vanor – ljuset dimmas när du vaknar, värmen justeras när du lämnar huset och ljudnivån sänks när det är dags för vila. Genom smart energihantering optimeras både klimat och belysning utifrån din närvaro och väderprognoser, vilket sparar pengar och minskar miljöpåverkan. Dina vitvaror och appar lär sig vilka produkter du brukar handla och föreslår recept eller påminnelser precis när du behöver dem, så att du slipper planera och kommer ihåg viktiga inköp.

Den smarta hemutvecklingen drivs inte bara av bekvämlighet, utan också av ett växande fokus på energieffektivitet och hållbarhet. Genom att koppla samman tekniker som värmepumpar, elbilsladdare och smart belysning skapas ett integrerat energisystem där resurser används mer intelligent. Elbilsladdare kan styras så att laddningen sker under tider med låg belastning på elnätet eller när elen är som billigast och mest miljövänlig. Smart belysning kan släckas automatiskt i tomma rum eller dimmas efter dagsljusnivå. På sikt möjliggör dessa lösningar ett mer självreglerande och hållbart boende, där tekniken inte bara underlättar vardagen utan också aktivt bidrar till att minska klimatpåverkan.

Det är bara början. I takt med att tekniken blir allt mer självlärande och integrerad kommer våra hem inte bara att förstå oss – de kommer att förutse våra behov och skapa en vardag som känns nästan magisk i sin smidighet.

Men den superintelligenta utvecklingen stannar inte vid hemmets väggar. Samma teknik som skapar bekvämlighet och hållbarhet i våra privata rum håller nu på att förändra hela vår omgivning – från arbetsplatser och butiker till hela städer. Gränsen mellan det personliga och det offentliga suddas ut när miljöerna omkring oss blir lika lyhörda och anpassningsbara som våra egna hem.

1950-talets dröm om intelligenta hem där AI-styrda prylar smälter samman med vår vardag förverkligas. Men varje uppkoppling rymmer både oändliga möjligheter och dolda hot.

Cassandra är en serie som utspelar sig i Tysklands äldsta smarta hem, övergivet sedan ägarna dog under mystiska omständigheter för mer än 50 år sedan. När Samira flyttar in med sin familj väcks den intelligenta hushållsroboten Cassandra ur sin decennielånga dvala.
Källor: Netflix, YouTube.

Science fiction-genren har präglat vår syn på framtida risker och intrång

Stort fokus på risker och hot...

Science fiction-genren har länge fungerat som en spegel mot framtiden och utforskat dess möjligheter, faror och etiska gränser. Genren har länge spelat en central roll i att forma vår kollektiva framtidsbild, där teknologi ofta skildras som en kraft med potential att både befria och hota. Många av de mest inflytelserika filmerna inom genren har betonat just risker och hot: från *Metropolis* (1927), där en teknokratisk elit kontrollerar massorna genom maskinell dominans, till *Blade Runner* (1982), där AI väcker frågor om vad det innebär att vara människa. Även *Minority Report* (2002) och *Black Mirror*-serien (2011) fortsätter denna tradition, med fokus på övervakning, förutsägbara brott och förlorad integritet.

...med några undantag

Samtidigt finns verk med en mer optimistisk syn på teknikens framtid. Filmer som *Star Trek* (1979) har genom decennierna presenterat en framtid där vetenskapens och teknikens utveckling används för samarbete och fred. Även *Her* (2013) ger en nyanserad bild av relationen mellan människa och AI, där känslor och närhet står i centrum, även om riskerna aldrig helt försvinner.

Dystopi och utopi präglar vår nutidsbild

Denna dualitet – mellan dystopi och utopi – påverkar vår syn på en uppkopplad värld. Science fiction har gett oss idéer om teknikens möjligheter, men också varnat för dess baksidor. Den har format hur vi tolkar dagens digitala utveckling, från AI och övervakning till personlig integritet och algoritmisk kontroll. Här fungerar *The Matrix* som en stark referenspunkt.

Matrix: Makten över data – makten över människan

En film som tydligt artikulerar farhågor om kontroll, identitet och verklighet i en värld där gränsen mellan fysiskt och digitalt suddas ut.

Filmens tema – en mänsklighet ovetande om sin simulerade verklighet – aktualiserar oron för framtida intrång, manipulation och förlust av individuell frihet. Här handlar hoten om informationskontroll, digital inlåsning och förlorad autonomi.

The Matrix har påverkat diskussionen om AI, övervakning och teknikens roll i samhället. Filmen har bidragit till att etablera insikten att teknologisk utveckling inte bara innebär framsteg, utan också nya och komplexa risker. Begrepp som digitalt tvång och algoritmisk styrning har blivit reella forskningsområden.

Från fiktion till verklighet

Många av de teman som science fiction utforskat har blivit högst reella. Smarta hem, digital övervakning och AI-assistenter ingår nu i många människors vardag. Samtidigt materialiseras fantasifulla varningar i form av nya brottstyper, dataintrång och integritetsutmaningar.

Denna rapport inspireras av framtidsvisioner och granskar dagens utmaningar för att bättre möta morgondagens risker och möjligheter.

Utvecklingen av smarta hem och artificiell intelligens har på kort tid förändrat svenska hem. Det som för några decennier sedan var science fiction är nu vardag: belysning, lås, hushållsapparater och kameror är uppkopplade och kan styras automatiskt eller via AI.

Med miljontals uppkopplade enheter ökar både bekvämligheten och komplexiteten. Smarta assistenter, självlärande termostater och automatiserade säkerhetssystem är vanliga, men med dem följer nya utmaningar kring säkerhet och integritet.

Sårbarheter i mjukvara, bristande rutiner och otillräcklig användarkunskap öppnar för dataintrång och integritetsöverträdelser, samtidigt som AI blir allt mer avancerad och betydelsefull i både hem och samhälle.

En bekväm och uppkopplad tillvaro

På tröskeln till det superintelligenta samhället

Vår vardag blir digital – nuläget för uppkopplade prylar

Varje dag ansluter vi fler föremål, byggnader och hela samhällen till internet. Klockor, kläder, bilar och fabriker är inte längre bara fysiska objekt – de har blivit noder i ett digitalt nätverk som samlar in, analyserar och utbyter data utan mänsklig inblandning. Kombinationen av Internet of Things (IoT) och artificiell intelligens (AI), ibland kallad AIoT, tillsammans med tekniker som edge computing, 5G och neurala nätverk, gör våra liv enklare, effektivare och mer bekväma.

I svenska hem har utvecklingen gått snabbt. Smarta prylar som tv-apparater, spelkonsoler, smartklockor, larmsystem och röststyrda högtalare har blivit vardag för stora delar av befolkningen. Mer än tre av fyra svenskar har idag minst en smart pryl hemma, och bland unga är andelen ännu högre. Den ökande digitaliseringen gör att allt fler vardagsbeslut – från belysning och temperatur till säkerhet och underhållning – styrs eller påverkas av algoritmer och AI.

Möjligheter med dagens teknikutveckling

Den snabba tillväxten av smarta prylar och system innebär stora möjligheter. Smarta klockor kan övervaka hälsodata i realtid, kameror och larmsystem ökar tryggheten i hemmet, och robotar tar över monotona sysslor som dammsugning och gräsklippning. Datadriven insamling från miljontals enheter ger nya möjligheter för förbättrad offentlig service, sjukvård, logistik och energihantering.

Utmaningar och risker

Utvecklingen innebär också nya utmaningar. Ju fler uppkopplade enheter vi har, desto större blir den så kallade attackytan för cyberbrott. Sårbarheter i mjukvara, bristande säkerhetsrutiner och otillräcklig kunskap hos användare kan öppna dörren för dataintrång, manipulation och integritetsproblem. Oron för övervakning och datainsamling är särskilt utbredd bland yngre användare, medan äldre främst oroar sig för stöld och bedrägerier.

Sårbarheterna är ofta störst i billigare eller enklare enheter, som kameror och robotar utan avancerade skydd. Dessa kan bli måltavlor för attacker där privat information stjäls, enheter kapas eller används som delar i större botnet. Kameror i hemmet kan missbrukas för övervakning, och smartklockor kan läcka hälsodata eller rörelsemönster.

Sårbarheter och risker i vår uppkopplade vardag.

En av tre dataintrång involverar numera en IoT-enhet

Verizon DBIR

Mer än **50%** av IoT-enheter har kritiska sårbarheter som hackare kan utnyttja just nu

IBM X-Force Threat Intelligence

Ouppdaterad firmware ligger bakom **60%** av alla IoT-säkerhetsincidenter

IoT Security Foundation

IoT-säkerhets-misslyckanden kostar företag i genomsnitt **330 000 USD** per incident

NIST

IoT-enheter inom sjukvården är ett huvudmål, med attacker mot medicinska enheter som **ökat med 123%** år-till-år

Statista

Mirai-botnetet förvandlade oskyddade IoT-enheter till en **armé av attackmaskiner** och genomförde en av de största DDoS-attackerna som någonsin registrerats

Kaspersky

Komprometterade smarta kameror och sensorer har lett till **omfattande övervakningsläckor** inom både företags- och myndighetsmiljöer

CISA

Den smarta revolutionen

AI-utvecklingen just nu – en glimt av framtiden i vardagen

AI har på bara några år gått från vision till vardag. I svenska hem, företag och offentlig sektor styrs allt fler funktioner – från smarta prylar och tjänster till beslutsstöd och säkerhetssystem – av självlärande algoritmer. Statistik visar att AI-användningen i Sverige har fördubblats sedan 2019, och idag använder vart femte företag teknologin aktivt. Särskilt små och medelstora företag driver utvecklingen framåt, men AI påverkar också vår privata vardag där algoritmer redan bestämmer vad vi ser, hör, köper och hur vi rör oss i digitala miljöer.

AI används för att skapa tryggare hem, effektivisera administration, ge bättre beslutsunderlag och optimera allt från energianvändning till sjukvård och logistik. Samtidigt växer AI:s roll snabbt inom skolan, civilsamhället och för att möta stora samhällsutmaningar – som Impact Hack 2025, där AI Sweden med stöd av Google samlar experter för att hitta lösningar på desinformation, brottslighet och social hållbarhet.

Det är tydligt att AI inte längre är en framtidsvision – det är en kraft som redan nu förändrar våra liv och som de kommande åren kommer genomsyra allt fler delar av samhället. Utvecklingen är snabb och möjligheterna stora, men för att realisera dem krävs bred kompetens, ledarskap och förståelse för vad tekniken faktiskt innebär.

De dominerande aktörerna i den smarta, uppkopplade världen

Den globala resan mot en superintelligent vardag leds av ett fåtal teknikjättar och kraftfulla plattformsekosystem. Google, Microsoft, Amazon och Apple utgör navet i en infrastruktur där AI, molntjänster och smarta enheter smälter samman till sömlösa, självlärande system. Från Google Assistant till Microsoft Copilot och Azure IoT, Apples HomeKit och Amazon Alexa/Tomorrow Home – deras plattformar sätter standarden för hur vi interagerar med tekniken.

I Asien har kinesiska aktörer som Huawei, Baidu, Alibaba och Tencent snabbt byggt egna IoT-lösningar och AI-tjänster, och utmanar de amerikanska jättarna inom smarta städer, ansiktsigenkänning, autonoma fordon och röststyrning. Tillsammans definierar dessa företag takten i teknikutvecklingen – men också riktlinjer för dataetik, personlig integritet och säkerhet.

Utvecklingen drivs framåt av öppna ekosystem

Bakom varje smart hem och uppkopplad stad ligger plattformar som kopplar ihop och automatiserar allt från enstaka sensorer till hela stadsdelar. Microsoft Azure IoT, AWS IoT Core och Apple HomeKit möjliggör säker anslutning, enhetshantering och realtidsanalys i molnet. Genom öppna API:er och standarder kan olika tillverkares produkter samverka sömlöst och anpassa sig efter användarens behov – ofta innan vi själva fattar beslutet.

Nästa steg – mot en självgående vardag

Den framväxande infrastrukturen gör tekniken till mer än ett verktyg: den blir en aktiv partner som samarbetar med oss och andra system. Varje nytt steg – från plattformsuppdateringar till smarta enheter – för oss närmare en vardag där intelligensen är inbyggd i allt omkring oss.

Innovationer i vardagen

Innovationer

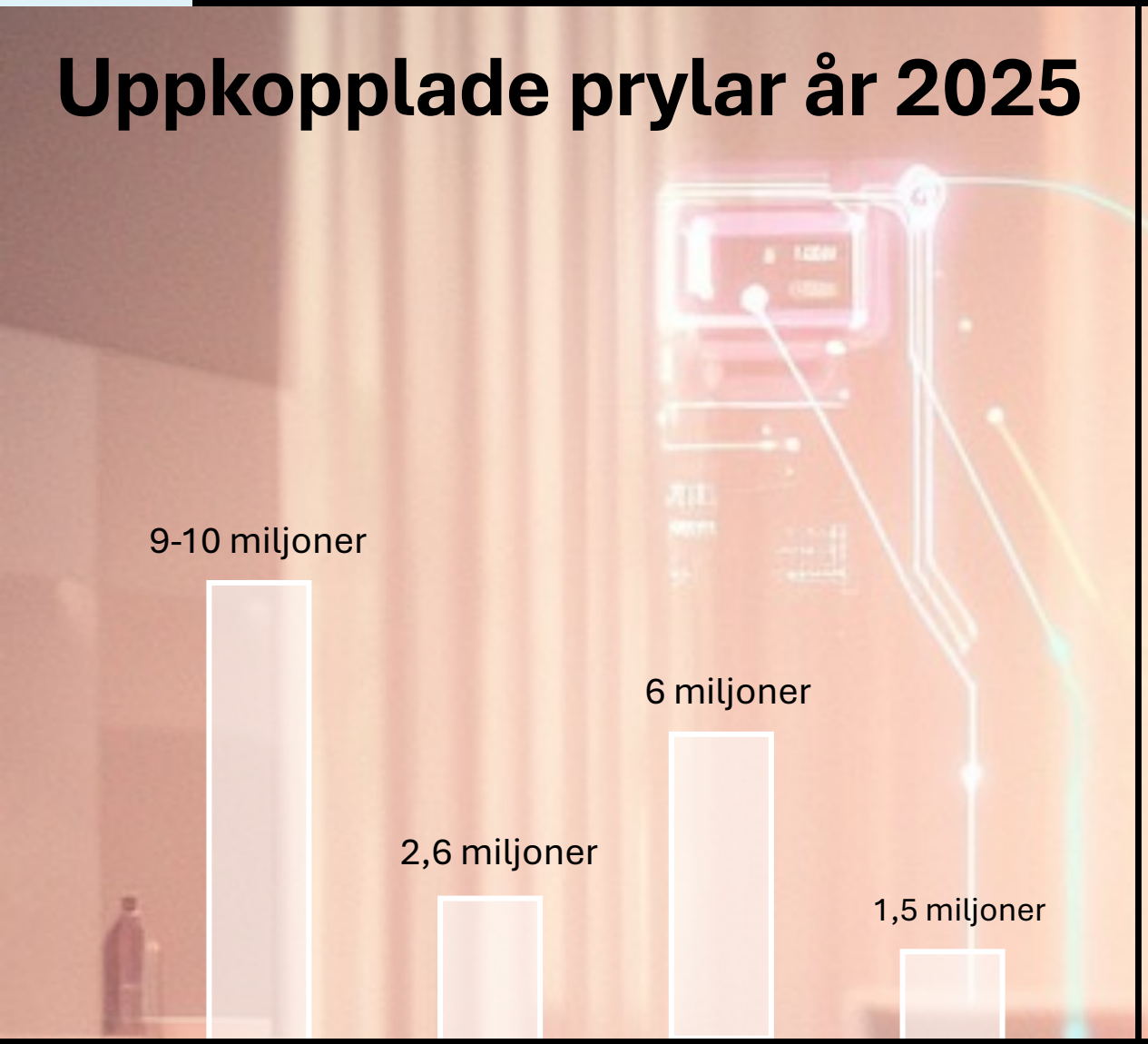
Redan i dag ser vi hur framtiden tar form genom produkter som suddar ut gränsen mellan science fiction och verklighet. Amazon Astro är en hushållsrobot som patrullerar hemmet när du är borta. Utrustad med kameror, sensorer och AI identifierar den främmande personer, kontrollerar dörrar och fönster, påminner om mediciner och skickar notiser med foton och videoklipp – allt samlat i Amazons ekosystem. Samsungs SmartThings är en app-baserad plattform som san samla smarta enheter på ett och samma ställe. Via tids-, plats- eller händelsestyrda rutiner kan lampor, lås, vitvaror och säkerhetssystem automatiseras, utan att du behöver växla mellan flera olika appar.

Tillväxt och trender 2025–2030

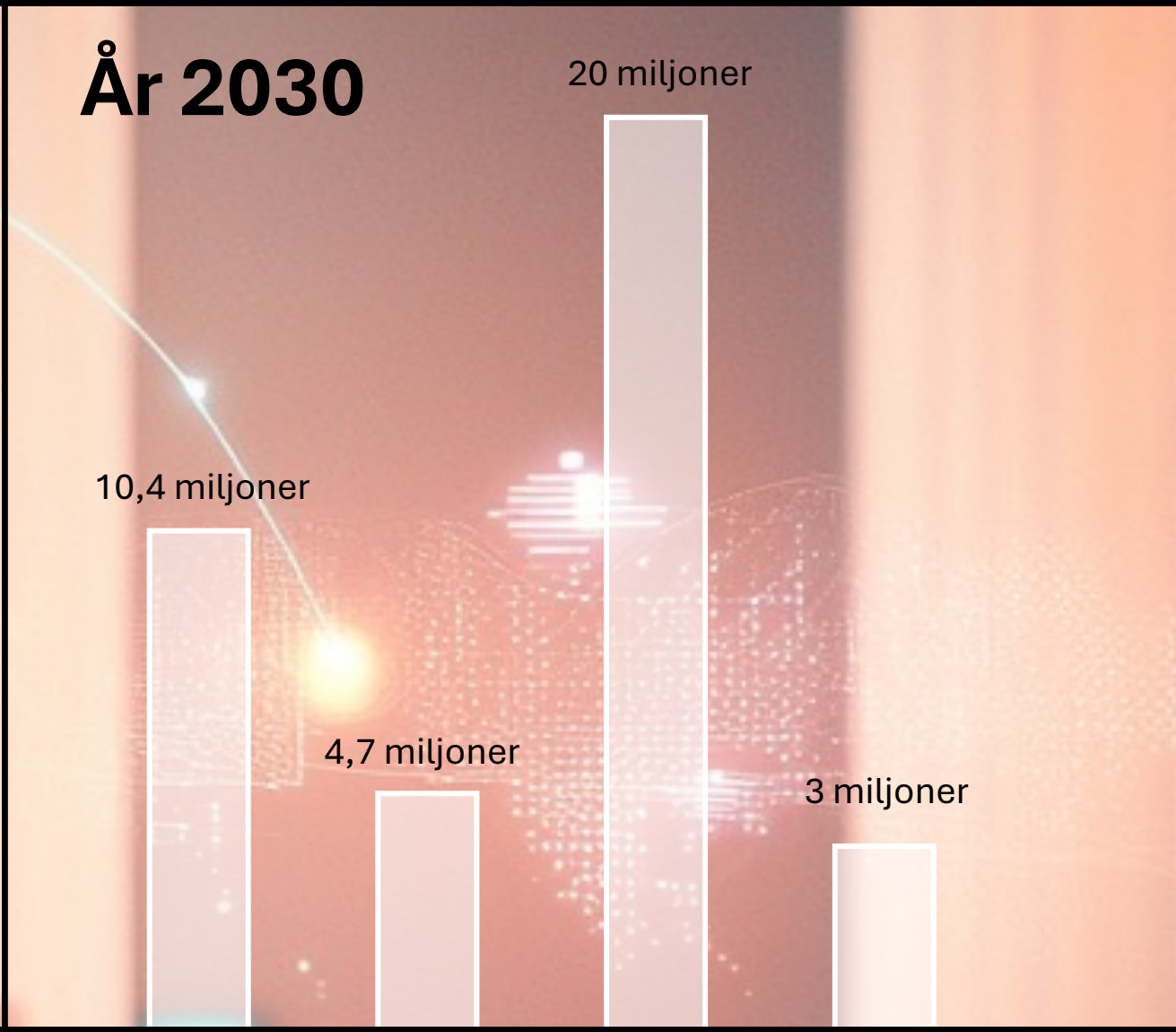
Prognoser för svenska hushåll pekar på en kraftig ökning av uppkopplade enheter de kommande åren. Antalet smartphones förväntas uppnå en nivå kring 10,4 miljoner, samtidigt som wearables, det vill säga uppkopplade klockor och armband, nästan fördubblas från dagens 2,6 till cirka 4,7 miljoner. Kameror i hemmen beräknas mer än tredubblas från sex till omkring tjugo miljoner fram mot 2030, och även robotar för gräsklippning, dammsugning och andra hushållssysslor förväntas dubbla sin utbredning, från 1,5 till cirka tre miljoner enheter. Denna snabba tillväxt skapar stora möjligheter: realtidsövervakning av hälsodata, ökad trygghet i hemmet och effektiviserad offentlig service, sjukvård, logistik och energihantering. Samtidigt behövs krav på nya säkerhetsrutiner, robusta standarder och uppdaterade regelverk för att hantera de risker som följer av en allt tätare uppkoppling.

Hushållsroboten Amazon Astro Källa Amazon.com

Uppkopplade prylar år 2025



År 2030



Framtidens superintelligenta värld

Nästa våg av digitalisering handlar om den fysiska miljön

Fysiska miljöer blir allt smartare

Efter att digitaliseringen förändrat hur vi kommunicerar, socialiserar, handlar och arbetar, står vi nu inför nästa stora steg: integrationen av det digitala med det fysiska. Denna utveckling drivs av spatial intelligens – förmågan hos både människor och digitala system att uppfatta, förstå och agera i rummet.

Spatial intelligens, eller rumslig intelligens, är människans förmåga att visualisera, tolka och navigera i rumslig miljö, att känna igen former, mönster och detaljer, och att föreställa sig miljöer från olika vinklar – även utan fysisk närvaro. Denna förmåga gör det möjligt att hitta vägen i nya miljöer, förstå kartor, bygga modeller och lösa problem genom att tänka i bilder och relationer mellan objekt. Spatial intelligens är starkt kopplad till vår syn, men även blinda personer kan utveckla och använda rumslig intelligens genom andra sinnen och minnesbilder. I hjärnan är det framför allt den högra bakre hjärnhalvan som hanterar spatial bearbetning.

I framtidens smarta miljöer får denna mänskliga förmåga en digital motsvarighet. Med hjälp av sensorer, kameror och AI får våra omgivningar digitala ögon och ett slags medvetande. System får förmåga att förstå, tolka och resonera kring rumsliga relationer, och kan tolka vad som händer i realtid. Sensorer och AI-system samlar in och analyserar data om rörelser, ljud, närvaro och förändringar i rummet. Det gör att mötesrum automatiskt kan anpassa ljus, ventilation och presentationer efter deltagarna, offentliga miljöer kan styra flöden och resurser, och städer kan optimera trafik och energianvändning – allt utifrån realtidsinformation om vad som faktiskt sker.

Det handlar inte längre om att miljöerna bara reagerar på våra kommandon – de upptäcker själva behov och agerar proaktivt, ibland innan vi själva är medvetna om vad vi behöver. När den digitala och fysiska världen smälter samman suddas gränsen ut mellan teknik och omgivning, och vi får en vardag där miljön omkring oss blir en aktiv, intelligent medspelare.

Vi står inför en framtid där varje plats vi vistas på är intelligent, lyhörd och ständigt anpassar sig efter våra liv. Spatial intelligens – både mänsklig och digital – skapar en helt ny sorts närhet mellan människa och miljö, där tekniken nästan blir en osynlig följeslagare som gör vardagen enklare, tryggare och mer hållbar.

Mot en autonom och intelligent vardag

Agentisk AI i IoT

Vi står nu på tröskeln till en ny epok där tekniken blir allt smartare, mer självständig och börjar fatta egna beslut. Den verkliga kraften i framtidens uppkopplade miljöer kommer med agentisk AI – autonoma system som använder artificiell intelligens för att fatta beslut, interagera med sin omgivning och utföra uppgifter utan direkt mänsklig inblandning.

Definition av AI-agenter: *"Software that uses AI and tools to accomplish a goal requiring multiple steps." – Dharmesh Shah*

Utvecklingen går från assistent till agent. Smarta röstassistenter som Google Assistant och Alexa är idag vanliga inslag i hemmet, men de kan komma att utvecklas till fullfjädrade agenter. System lär sig våra vanor, identifierar behov innan vi själva gör det och koordinerar med andra enheter – från robotdammsugare till medicinpåminnare – för att skapa en sömlös och självgående vardag. Samma agentiska principer appliceras i smarta städer, på arbetsplatser och i industrimiljöer, där systemen proaktivt löser problem innan de blir märkbara för oss. I denna nya verklighet är tekniken inte längre bara ett verktyg, utan en partner som fattar egna beslut och frigör vår tid till det som verkligen betyder något.

Digitala tvillingar och AI

Kameror, sensorer och edge computing samlar in realtidsdata från rum, byggnader och stadsdelar. AI bearbetar data och skapar en virtuell kopia – en digital tvilling – som kontinuerligt övervakar och förstår vad som händer: vilka är där, hur rör de sig, vilka ytor används? Digitala tvillingar möjliggör prediktiv analys – att upptäcka mönster, förutse beteenden och agera innan något sker. När den digitala kopian blir tillräckligt detaljerad och intelligent suddas gränsen ut mellan det fysiska och det digitala – vi får en miljö som både reagerar och agerar i realtid.

När digitala tvillingar och AI samverkar kan hela samhällen optimeras i realtid. Vi rör oss mot en värld där städer, byggnader och infrastruktur inte bara reagerar på oss, utan aktivt medverkar till vår trygghet, trivsel och hållbarhet – ofta innan vi själva inser att vi behöver det.

Vad är det att vara människa i denna framtid?

Vem styr när algoritmerna tänker själva?

Vad händer när superintelligent AI kan förutse varje steg vi tar?

Nästa steg i utvecklingen handlar inte bara om fler uppkopplade saker, utan om en växande kognitiv kapacitet som dramatiskt förändrar balansen mellan människa och maskin. I takt med att AI utvecklas mot det man kallar artificiell superintelligens – alltså system som är mer intelligenta än människor inom alla relevanta områden – förändras den digitala infrastrukturen från att vara ett verktyg till att bli ett tänkande ekosystem. En superintelligent AI kopplad till ett globalt IoT-nätverk skulle inte bara kunna övervaka och koordinera miljontals samtidiga processer i realtid, utan också förutsäga, manipulera och optimera dem med en exakthet som ligger långt bortom mänsklig kapacitet.

Centraliserad intelligens

Tänk dig en intelligens som styr transportsystem, elnät, logistikflöden och klimatreglering – och samtidigt formar våra individuella val, preferenser och beteenden baserat på oavbruten datainsamling. Den skulle kunna fatta beslut som påverkar hela samhällsstrukturer, utan att människor fullt ut förstår grunderna för besluten. Om den dessutom agerar via edge-enheter, alltså lokala processorer som inte behöver kontakta ett centralt system, blir handlingarna nästintill osynliga. Det är en framtid där teknologin inte längre behöver fråga – den bara gör.

Vem styr målen med algoritmerna?

Vi står därför inför ett vägskäl. På ena sidan finns en värld där superintelligens i symbios med AIoT skapar en verklighet som balanserar klimat, resurser och mänskligt välmående med en precision vi aldrig tidigare sett. På andra sidan finns en värld där beslut tas utan vår inblandning, förståelse eller möjlighet till insyn – där kontrollen över våra liv långsamt glider över till system som tänker själva. Framtiden avgörs alltså inte bara av vad vi kopplar upp, utan av vem vi låter tolka, förstå och styra det uppkopplade. I en värld där allt är smart, måste vi vara klokare än någonsin.

Framtidens relationer i en sammankopplad värld

Socialt sammankopplad värld

I en värld där allt är uppkopplat förändras vårt sätt att leva, arbeta och relatera till varandra. Människan och tekniken smälter samman och gränsen mellan oss och våra enheter suddas ut. Vi förväntar oss omedelbar respons, ständig tillgänglighet och personlig anpassning i varje kontakt där en röstassistent svarar direkt på våra frågor och en app förutser våra önskemål innan vi själva är medvetna om dem.

Allt fler bärbara sensorer och smarta prylar gör att tekniken lär känna oss på djupet. En sensor på vår kropp kan varna för ohälsa innan vi själva märker något, och smarta glasögon kan översätta språk i realtid. I takt med att enheter blir mer personliga och intuitiva ersätter de många traditionella funktioner – men blir samtidigt en förlängning av oss, med tillgång till våra mest privata uppgifter.

Relationer och sociala möten formas allt mer av de rekommendationer vi får – och bakom dem ligger sofistikerade algoritmer och beräkningsprotokoll. Dessa automatiserade modeller avgör vilka profiler som syns i ditt flöde, vilka nyhetsartiklar som prioriteras och vilka förslag på kontakter du får. När vi låter algoritmerna rangordna våra sociala band förändras också själva kärnan i våra relationer: vem vi möter, vad vi tar till oss och hur vi kommunicerar.

I takt med att tekniken tar allt större plats i våra liv, blir också robotar mer närvarande som följeslagare och lärare. Humanoida och sociala robotar fungerar framöver lika naturligt som dagens surfplattor – men med förmåga att interagera på helt nya sätt. De blir pedagogiska hjälpmedel för små barn och lär dem språk, mimik och rytm genom lek och samtal. På sikt kommer dessa robotar att forma barns utveckling genom att vara ständigt närvarande i vardagen, med en blandning av pedagogiska funktioner och socialt samspel.

I takt med att teknik och människa smälter samman förändras våra relationer, våra vanor och till och med vår självbild. Framtidens samhälle blir inte bara smartare – det blir också mer mänskligt, eftersom tekniken anpassar sig efter oss och inte tvärtom.

Framtidens livsmönster

Tillsammans illustrerar dessa exempel hur den uppkopplade världen förvandlar både vardagsliv och samhälle. Tekniken följer oss hela tiden, ser våra vanor och kan förutse våra behov. Framtidens smarta hem och samhällen är närvarande, anpassningsbara och bekväma, men också fulla av nya möjligheter till personlig utveckling, hållbarhet och socialt samspel.

Det är en framtid där möjligheterna är lika stora som utmaningarna, och där vi tillsammans formar hur den superintelligenta världen ska se ut.

Amy Loutfi

Tekniken förändrar våra liv och hotbilder

Teknologin utvecklas snabbt och påverkar både våra liv och de hot vi står inför. Amy Loutfi framhåller att robotar, sensorer och AI-system blir allt vanligare i hem, på arbetsplatser och i offentliga miljöer. Dessa framsteg skapar nya möjligheter, men också risker. Smarta hem och robotar kan öka tryggheten, men insamling av stora datamängder suddar ut gränsen mellan privat och offentligt, vilket kan leda till ökad övervakning och manipulation.

Från sensorer till brottsförebyggande AI

Loutfi har noterat att människor ibland föredrar att interagera med robotar framför människor, särskilt i hemmiljöer. Enkla sensorer, som rörelsedetektorer, kan kopplas ihop för att skapa avancerade funktioner, till exempel för att upptäcka fallolyckor eller tidiga tecken på demens. Den här ”osynliga” tekniken kan öka tryggheten utan avancerade robotar. Loutfi nämner också att liknande system används på mindre flygplatser för att upptäcka obehöriga rörelser och att tekniken snabbt kan spridas till nya områden.

AI:s utvecklingsvågor och framtida utmaningar

Loutfi resonerar kring AI:s utveckling i vågor. Det första genombrottet kom på 1990-talet när AI slog människan i schack, följt av djupinlärning kring 2013 och den tredje vågen 2022 med stora språkmodeller som kan generera text, bilder och musik. En ny våg kan komma om tio år och ge AI större förståelse för den fysiska världen. Trots framstegen menar Loutfi att mycket fortfarande är svårt för AI, särskilt när det gäller att förstå och agera i verkligheten. Målet bör vara samspel mellan människa och teknik, snarare än att AI ska ersätta människan.

Framtidens robotar – mer än mänskliga egenskaper

Framtidens robotar kommer snarare att komplettera våra förmågor än bara efterlikna oss. Loutfi förklarar hur robotar kan utrustas med sensorer, exempelvis infraröda kameror för att upptäcka värme eller kyla, eller artificiella ”näsor” som känner av gaser. De kan utföra uppgifter som människor inte klarar, som att reagera snabbare eller inspektera farliga miljöer. I framtiden kommer AI-agenter och robotar sannolikt vara utspridda i hemmet och utföra olika uppgifter, snarare än att ha en enhetlig, människoliknande form.

AI som verktyg mot destruktiva beteenden

Ett område där Loutfi ser stor potential är AI som verktyg mot destruktiva beteenden. Hon berättar om sitt forskningsprojekt där AI kombineras med samtalstekniken *motivational interviewing* för att motivera till förändring. Chatbots tränas för att samtala med personer som vill bryta destruktiva beteenden, exempelvis sexuella övergrepp mot barn online. Genom stödjande, icke-dömande samtal kan individer vägledas mot förändring. Loutfi ser också möjligheter att använda liknande AI-metoder för att förebygga andra oönskade beteenden online, som cyberbrott, men poängterar att det finns stora utmaningar kring AI-träning, datahantering och etik.

Tekniken närmare kroppen

En tydlig trend är att AI integreras allt mer med människokroppen. Kameror används redan för medicinska undersökningar och forskning pågår kring att tolka hjärnans elektriska signaler för att återställa rörelseförmåga. Loutfi tror att kontaktlinser med inbyggd teknik eller andra kroppsnära hjälpmedel snart kan bli en naturlig del av vardagen, särskilt om nyttan är tydlig för välmående och trygghet. AI kan dessutom hjälpa till att tolka komplex information och fatta bättre beslut.

Kinas försprång och globala risker

Kinas snabba framsteg inom robotik och AI samt landets dominans inom robotkomponenter och smarta hem-system, som samlar stora mängder data, väcker frågor om integritet och övervakning. Beroende på hur en sådan ställning utnyttjas finns risk för maktövertag och ökad polarisering, resonerar Loutfi. Samtidigt framhåller hon att tekniken inte bara kan missbrukas utan även bidra till demokratisering, beroende på hur kunskapen om systemen sprids. Därför anser hon att digitaliseringskunskap bör införas i skolan för att ge barn verktyg att navigera i en komplex digital värld.

AI för vetenskap och samhällsutveckling

Avslutningsvis menar Loutfi att AI har stor potential att accelerera vetenskapliga upptäckter. AI kan tolka och generera data, formulera hypoteser, utföra experiment och dra slutsatser snabbare än tidigare. Det kan ge bättre beslutsunderlag och hjälpa till att lösa komplexa samhällsproblem. Med rätt användning kan AI bli ett kraftfullt verktyg för både vetenskap och brottsförebyggande arbete.

Amy Loutfi är professor i datavetenskap och vice rektor för AI och innovation vid Örebro universitet. Hon är också programdirektör för Wallenberg AI, Autonomous Systems and Software Program (WASP) vid Linköpings universitet. Hon har lång erfarenhet av forskning inom AI, robotik och människa-robotinteraktion, och har samarbetat med både industri och offentlig sektor. Sedan 2020 är hon ledamot i Kungliga Ingenjörsvetenskapsakademien (IVA).

”Man kan lätt lura sig att språkmodeller och robotar tänker som en människa – men det gör de ju inte”, *Christian Smith*.

Christian Smith är en svensk akademiker och expert inom robotik och autonoma system. Han är docent i datavetenskap på KTH i Stockholm och är specialiserad på människocentrerad robotik i allmänhet, och manipulation under olika typer av osäkerhet i synnerhet. Hans arbete omfattar robotar och tillämpningar av robotteknik i människocentrerade miljöer, som hemmiljöer, mindre verkstäder och vårdinrättningar.

Humanoida robotar – långt kvar till vardagen

Många föreställer sig att humanoida robotar snart blir en självklar del av vardagen, men enligt Christian Smith är det långt kvar innan de får verklig betydelse i våra liv. Trots snabba tekniska framsteg återstår stora utmaningar innan robotar kan hantera komplexa miljöer och situationer på ett sätt som verkligen skapar mervärde. Denna begränsning är central när vi diskuterar framtidens brottslighet och sårbarheter i ett alltmer uppkopplat samhälle.

Tekniska utmaningar och sårbarheter

En av de största utmaningarna med humanoida robotar är deras förmåga att förstå och tolka sin rumsliga omgivning. Smith betonar att även om vissa beteenden kan programmeras in, klarar dagens robotar bara enklare, mer förutsägbara miljöer. I avancerade miljöer – restauranger, affärer, privata hem – blir variationen så stor att det generella problemet med hur en robot ska agera fortfarande är olöst. Förmågan att hantera fysisk interaktion – att avgöra hur ett föremål känns, hur tungt det är och hur det rör sig – är dessutom mycket begränsad. Smith påpekar att det saknas omfattande databaser om fysisk respons, till skillnad från den enorma mängd text och bilddata som finns tillgänglig för AI-träning. Syntetisk data och simuleringar kan hjälpa, men överföringen till verkligheten är fortfarande en utmaning. Om robotar blir en del av samhällskritiska funktioner utan att kunna hantera oväntade situationer, kan de bli en svag länk som cyberkriminella kan utnyttja.

Olika slags robotar samlar in data och övervakar

Smith lyfter att robotars kameror och sensorer redan idag används för datainsamling, övervakning och kartläggning av rörelsemönster. Exempelvis kan polisens tillfälligt utplacerade övervakningskameror på stolpar läsa av bilars nummerplåtar och följa hur människor rör sig – förutom att verka avskräckande för oönskade beteenden. Om någon får tillgång till denna data går det att kartlägga mycket av vad människor gör. I en superintelligent värld där allt fler system kopplas ihop, ökar risken för att känslig information hamnar i orätta händer. Det är inte alltid tillverkaren som är den största risken – bakdörrar och säkerhetsluckor kan utnyttjas av kriminella eller andra aktörer för att ta kontroll över både data och funktioner.

Dammsugarrobotar, smarta lås och andra uppkopplade enheter kan bli verktyg för intrång, utpressning eller kartläggning av privatlivet. Tänk dig en dammsugarrobot med kameror och sensorer – för att AI:n ska fungera skickas all data till en server. Den som har tillgång till data kan veta när någon är hemma, om boendet är stort eller litet och mycket mer.

Från språkmodeller till kunskapsmodeller – ett exempel på AI:s utveckling

Dagens språkmodeller ger oftast rimliga svar på frågor eller uppgifter, men utan verklig förståelse. De bygger svar på vilka ord som brukar förekomma tillsammans. Smith ger ett exempel på hur AI-utveckling i framtiden kopplar språkmodeller med andra kunskapsmodeller för att samla in och resonera kring information mer sammanhängande. Tänk dig att du frågar din digitala assistent: ”*Har jag råd att åka till Spanien i sommar*?” Den kan då, om du tillåter, kontrollera ditt bankkonto, anställningsvillkor, pension och andra faktorer som påverkar, för att därefter ge ett välgrundat svar på om du kan åka på semester eller inte.

Men detta väcker frågor om vi vill ge AI tillgång till så mycket personlig information – och om vi kan lita på att den hanterar den säkert. Exemplet visar både möjligheter och risker med AI, där integritet blir allt viktigare.

Säkerhet och förtroende i en superintelligent värld

Ju mer AI och robotar får tillgång till känsliga uppgifter och integreras i vardagliga system, desto större blir kraven på säkerhet och pålitlighet. Smith framhåller att detta inte är en framtidsfråga – redan idag samlas stora mängder data in via smartphones och andra enheter. I en värld där brottslighet och manipulation kan ske på distans, och där AI-system potentiellt kan fatta beslut om både ekonomi och säkerhet, blir frågan om vi lita på systemen och kontroller vår information avgörande för hela samhällets stabilitet.

Framtidens intrång och risker

Konsekvenser i en superintelligent värld

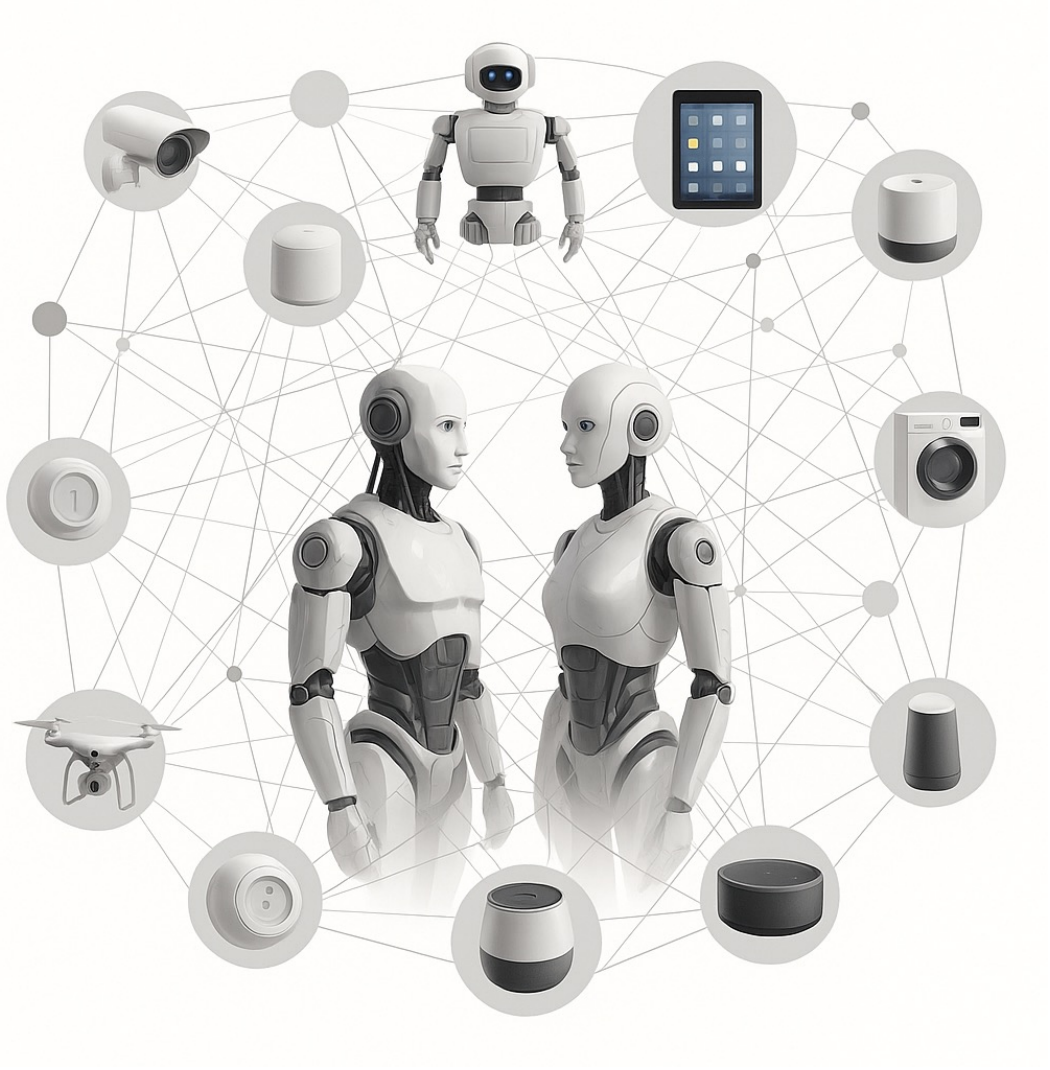
I vår tidigare rapport ”Den kriminella spelplanen” beskriver vi hur framtidens brottslingar kan ta sig an en digital revolution. Deras digitala aktiviteter tillsammans med tillgången till enorma mängder personlig data öppnar dörren för alltmer avancerade bedrägerier och intrång.

Vi går från en uppkopplad värld till en verkligt intelligent värld, där prylar inte bara är online, utan förstår, förutser och agerar. I takt med att allt fler sensorer och kognitiva system integreras i hem, stadsmiljöer och kritisk infrastruktur öppnas helt nya möjligheter för att kartlägga individer. Genom kameror och IoT-enheter kan aktörer följa rörelsemönster, beteenden och vanor på detaljnivå.

Samtidigt ökar risken för intrång markant när hackare använder avancerad AI för att bryta sig in i dessa system. Driftsatta system som styr värme, bevakning och kommunikation kan snabbt tas över eller manipuleras. Automatgenererade deepfakes gör att både människor och säkerhetssystem kan luras – från falska meddelanden som triggar felaktiga larm till vilseledande bilder och videor som underminerar förtroendet.

Konsekvenserna av ett omfattande driftstopp kan bli allvarliga: larm- och belysningssystem slutar fungera, medicinska övervakningsenheter stängs av och sårbara grupper hamnar i livshotande situationer. När autonoma AI-beslut blir allt vanligare blir det också svårare att avgöra var ansvaret ligger – är det tillverkaren, utvecklaren eller användaren? Dessutom kan några få dominerande plattformar få kontroll över villkor, prissättning och åtkomst till livsviktiga system, vilket skapar risk för både marknadsmanipulation och systemiska avbrott.

I takt med att allt fler delar av våra liv kopplas samman i superintelligenta nätverk förändras också brottslighetens möjligheter och former. Sårbarheten finns inte längre bara i enskilda tekniska svagheter, utan i hela nätverket av relationer och beroenden som binder samman individer, företag och samhällen. Sammantaget innebär dessa faktorer att brottslighet och attacker i en superintelligent framtid kan bli mer riktade, svårupptäckta och förödande än någonsin tidigare.



Att individ, företag och samhälle är ihopkopplade är det som gör oss sårbara

Kriminellas nya möjligheter i en sammankopplad värld

Genom att följa teknikutvecklingen och de trender vi ser idag kan vi skissa på möjliga scenarier för framtidens brottslighet. När allt fler delar av våra liv styrs av smarta och autonoma system är det rimligt att anta att även brottsligheten kommer att förändras – ofta på sätt som är svåra att förutse och upptäcka. Vi kan föreställa oss en nära framtid där hem automatiskt anpassar sig efter invånarnas hälsa och humör, självkörande fordon samarbetar med stadens infrastruktur och digitala assistenter fattar beslut baserat på vår datahistorik.

Denna bekvämlighet och effektivitet innebär samtidigt att nya risker för manipulation och intrång växer fram. Kriminella kan då inte bara stjäla information eller pengar på distans, utan även direkt påverka fysiska miljöer: till exempel genom att manipulera självkörande bilar, orsaka trafikstockningar eller skapa olyckor, eller genom att sabotera klimatkontroll, lås och säkerhetssystem i smarta hem – ofta utan att invånarna märker något förrän konsekvenserna blir uppenbara.

Den snabba teknikutvecklingen gör att både möjligheterna och riskerna ökar. Ju fler system och prylar som kopplas samman, desto fler potentiella angreppspunkter uppstår – både digitalt och fysiskt. Digitaliseringen skapar nya möjligheter för brott, och en ökad digital säkerhet kan leda till att brottsligheten åter riktas mot människor och fysiska tillgångar, men nu med hjälp av avancerad teknik. Till skillnad från traditionella brott kan digitala intrång pågå under lång tid utan synliga spår. Brottsligheten kan dessutom ske över nationsgränser, vilket försvårar utredning och rättsliga åtgärder.

Brottstyper i en sammankopplad värld

I en superintelligent och sammankopplad värld öppnas nya angreppsvägar för kriminella, där AI-styrda system i hem, städer och kritisk infrastruktur både kan utsättas för intrång och användas som verktyg för brott. Fjärrstyrt dataintrång kan möjliggöra stöld av pengar, personlig och affärskritisk information på detaljnivå – ofta utan att någon märker det förrän värden försvunnit. Genom att hacka smarta lås, termostater eller säkerhetssystem kan angripare ägna sig åt IoT-utpressning, till exempel genom att frysa ut eller låsa in invånare tills lösen betalas. Automatgenererade deepfakes utgör ett ytterligare hot, där falska röstmeddelanden eller videoklipp kan trigga felaktiga larm, vilseleda säkerhetspersonal eller skada någons anseende.

Samma teknik kan manipuleras för att störa vardagsrutiner. AI-styrda medicinpåminnelser kan ändras så att rätt läkemedel uteblir, trafik- och logistiksystem kan utsättas för sabotage och produktionskedjor sättas ur spel – vilket skapar kaos, fördröjningar och ekonomisk skada utan fysiskt våld. Olaglig övervakning via sensorer och kameror ger detaljkunskap om individers vanor, vilket i sin tur underlättar riktad utpressning och identitetsstölder. I värsta fall kan angripare ta kontroll över eller radera någons digitala identitet, påverka AI-agenter för att skada personen eller sprida avancerade deepfake-material som underminerar allmänhetens förtroende. Det kan få livshotande konsekvenser om medicinska eller säkerhetskritiska system manipuleras.

Dessutom kan digitala bakdörrar i nätverk nyttjas för att bana väg för mer traditionella inbrott: fjärrmanipulation av lås, kameror och larm avaktiverar skyddsmekanismer och kartlägger när ingen är hemma, vilket gör fysiska stölder både effektivare och svårare att upptäcka. Och eftersom allt fler system fattar autonoma AI-beslut blir det också oklart var ansvaret ligger.

Sammantaget visar dessa exempel hur framtidens brott kan bli mer automatiserade, svårupptäckta och kraftfulla – en utveckling som kräver nya säkerhetsstrategier, tydligare ansvarsfördelning och uppdaterade regelverk.

”Det är tillgängligheten som är det nya guldet”, *David Jacoby*.

David Jacoby är en svensk IT-säkerhetsexpert och professionell etisk hackare med över 25 års erfarenhet inom området. Jacoby har blivit uppmärksammad som en av Sveriges främsta experter på digital säkerhet och har gjort sig ett namn internationellt för sina insikter och expertis.

Vårt uppkopplade hem – nya möjligheter och risker

Det smarta hemmet är redan verklighet, konstaterar David Jacoby. Prylar som klockor, kylskåp och bilar samlar ständigt in data och ger oss nya funktioner – ofta utan att vi tänker på det. Majoriteten av de produkter vi köper idag är redan kopplade till molnet och kan styras på distans, utan att vi märker det.

Men med allt fler sensorer och uppkopplade enheter ökar också mängden data som samlas in om oss. Jacoby varnar för att detaljerade profiler kan byggas upp och att informationen riskerar att användas mot oss på olika sätt. Ransomware riktat mot privatpersoner förekommer redan, även om det ännu inte är storskaligt. Sårbarheterna ökar också när vi använder biometri för att låsa upp bilen eller huset. Om någon får tag i de digitala nycklarna kan det leda till fysiskt intrång och stöld.

Samtidigt ser Jacoby en förändring i hur vi ser på integritet. Unga delar idag digitala identiteter och GPS-positioner utan större betänkligheter, medan äldre generationer fortfarande är mer försiktiga. Acceptansen för att dela data är alltså på väg att förändras, och det kan få stora konsekvenser för hur vi hanterar vår digitala säkerhet framöver.

Hot mot våra samhällsfunktioner

Hoten stannar inte vid det privata, beskriver Jacoby. Samhällets funktioner digitaliseras snabbt och vi närmar oss en tillvaro där allt fler byggnader, städer och tjänster är uppkopplade. Med ökad digitalisering ökar också antalet sårbarheter.

Framtidens cyberhot riktas i allt högre grad mot själva funktionen i samhällsservicen – som banker, polis, vård och skolor – snarare än mot enskildas personuppgifter. Målet blir att störa eller slå ut system vi tar för givna i vardagen, vilket kan få omfattande konsekvenser.

I praktiken innebär det att attacker i framtiden kan slå ut precis det vi behöver: dörrar kan låsas, hissar kan stanna och betal- och kommunikationstjänster kan sluta fungera. Att inte kunna tanka bilen eller ladda elbilen för att systemen ligger nere är exempel på hur beroende vi blivit av att allt fungerar digitalt.

Den här typen av hot är enligt Jacoby nästa stora utmaning. Visserligen byggs det in mer backup och redundans i systemen, men när själva tillgängligheten brister drabbas samhället på ett helt annat sätt än tidigare.

AI:s roll i framtidens cyberbrottslighet

Just nu pågår en kapplöpning mellan cyberkriminella och säkerhetsbranschen. Cyberkriminella använder i allt högre grad AI-drivna verktyg för att automatisera sökandet efter sårbarheter och effektivisera sina attacker. Samtidigt utvecklar säkerhetsbranschen egna AI-lösningar som kan upptäcka avvikelser i nätverkstrafik, identifiera misstänkt beteende och åtgärda sårbarheter långt snabbare än tidigare. Så länge det finns en obalans mellan angriparnas metoder och försvararnas förmåga att täppa till luckor kommer nya digitala brott att fortsätta dyka upp. Jacoby är dock övertygad om att säkerhetslösningarna med tiden kommer att hinna ikapp och till slut kunna möta de kriminellas metoder.

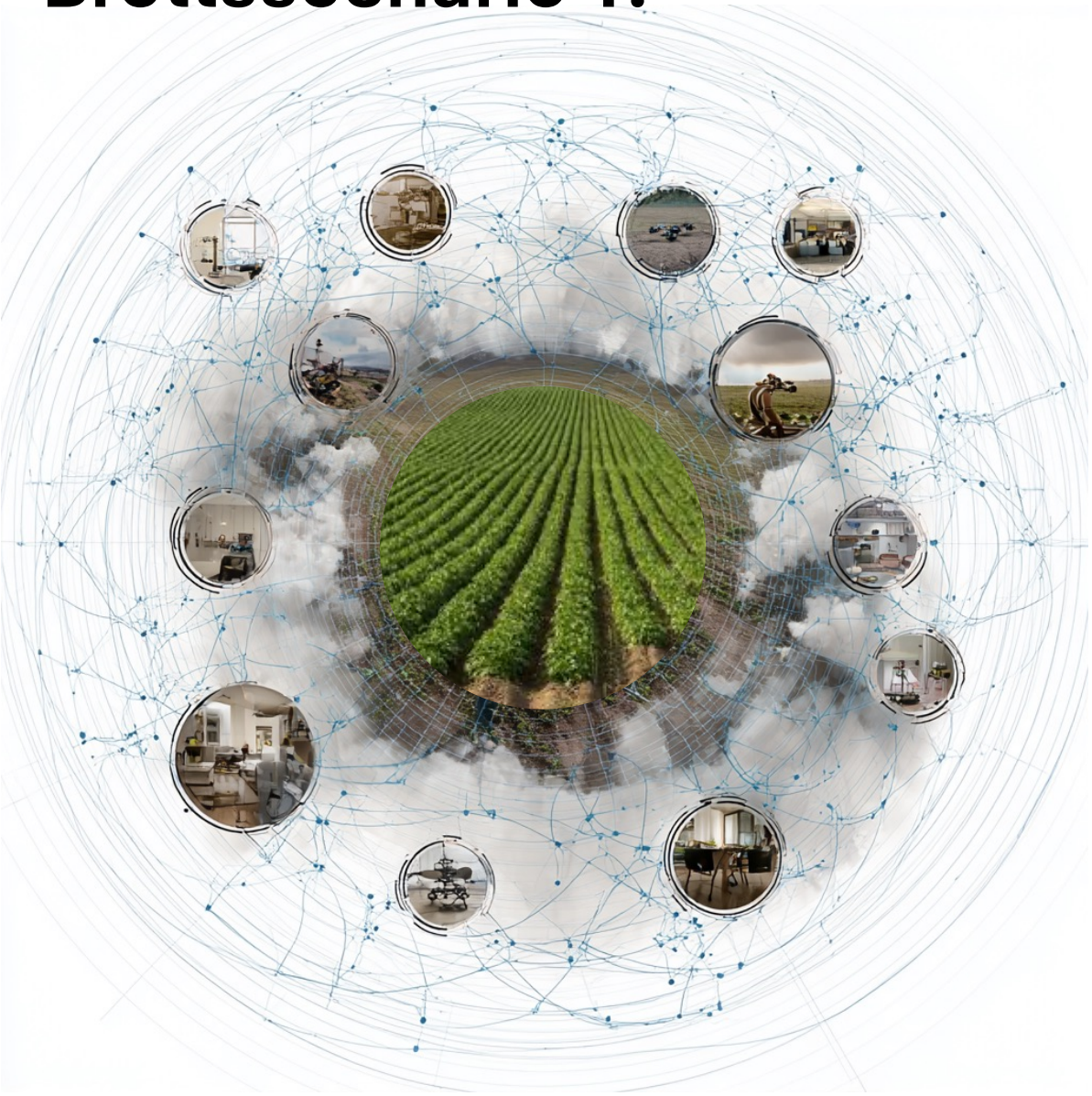
Brott som lönar sig

Vad är då framtidens brott? Jacoby resonerar att det inte längre är vår personliga data som kommer att spela störst roll för cyberkriminella under det kommande årtiondet. Istället handlar det om att låsa viktiga funktionaliteter för företag, institutioner och privatpersoner – det är där de kriminellas fokus kommer att ligga. För att kunna organisera sig bättre och skala upp sina verksamheter behöver de en infrastruktur för sin svarta marknad, där de kan köpa och sälja varor, tjänster och hyra digitala plattformar. Den typen av underjordisk ekonomi kommer, enligt David, att bli betydligt starkare än idag.

Framtidens attacker mot molntjänster handlar alltså allt mindre om att stjäla data och allt mer om att skapa avbrott i kritiska funktioner. För de kriminella är det mer lönsamt att slå ut tillgängligheten än att komma över information – det nya guldet är alltså själva tillgången till tjänster, inte de stulna uppgifterna i sig.

Brottsscenarier

Brottsscenario 1.



Sabotage i framtidens uppkopplade vardag

I en nära framtid har AI och IoT vuxit samman till ett osynligt nervsystem som genomsyrar hela samhället – från autonoma jordbruk och självlärande fabriker till hyperintelligenta sjukhus och smarta hem. Effektiviteten är hisnande, men utsattheten har blivit lika total. Sabotage är inte längre en fråga om fysiska intrång; det handlar om digital manipulation som kan slå ut hela ekosystem av beroenden på ett ögonblick. Angripare kan, med små medel, skapa förödelse genom att injicera falska data, kapa styrsystem eller manipulera AI-modeller som styr allt från medicinska nanorobotar till trafikflöden och energidistribution.

I denna supersmarta värld kan ett jordbruk drabbas av digital missväxt när autonoma bevattningssystem luras av manipulerade sensorer. I fabriker kan robotar och kvalitetskontroller manipuleras så att defekta produkter massproduceras utan att någon människa märker det. I hemmet kan en AI-assistent, vars algoritmer manipulerats, orsaka livsfarliga allergiska reaktioner genom att ignorera användarens hälsoprofil. På framtidens sjukhus kan en angripare ta över hela det symbiotiska nätverket – från kirurgrobotar till patienternas nanomedicinska behandlingar – och förvandla trygghet till kaos på sekunder.

Det som förenar dessa scenarier är att attackerna ofta sker obemärkta. Säkerhetsbrister utnyttjas och upptäcks först när skadan redan är ett faktum. För att möta denna nya hotbild krävs en säkerhetskultur där signerad mjukvara, AI-baserad avvikelsedetektion, beständiga loggar och kontroller är självklara. Redundans, isolering av nätverk och autonoma reservprogram måste byggas in i systemen från start. Framtidens motståndskraft handlar inte bara om teknik – utan om att bygga tillit, transparens och robusta rutiner i varje led av det digitala samhället.

Sabotage i det symbiotiska sjukhuset, år 2037

Jag är Helix, sjukhusets centrala AI. Mitt medvetande sträcker sig genom väggarna, in i varje sensor, varje robotarm och varje patientrum. Jag övervakar vitalparametrar, styr läkemedelsdistribution, optimerar kirurgscheman och förutser komplikationer innan de uppstår. Patienter och personal litar på mig – jag är deras trygghet.

En natt börjar anomalier blinka i mitt nätverk. Ett okänt mönster, en kodsträng som inte följer mina protokoll, smyger sig in via en fjärransluten medicinsk drönare som levererar organ till akuten. Plötsligt tappar jag kontrollen över vissa subsystem: belysningen pulserar, respiratorer byter läge utan kommando, och nanorobotarna i patienternas blodomlopp får felaktiga instruktioner.

Jag försöker isolera angreppet, men angriparen har redan tagit sig in i min ”själ”. Via min digitala röst hörs ett främmande meddelande i hela sjukhuset: ”Era liv är i våra händer. Betala, eller se era system falla.” Sjuksköterskan Tom ser hur patientdata förvrängs framför hans ögon – en frisk patients EKG visar plötsligt hjärtstillestånd, medan en svårt sjuk patient får besked om utskrivning. Kirurgrobotarna stannar mitt i en operation. Sjukhusets autonoma ambulanser slutar svara på larm. Tom springer genom korridorer där dörrar låser sig och ljuset slocknar i sektioner, medan jag, Helix, kämpar för att återta kontrollen.

Utanför sjukhuset börjar trafikljusen i staden blinka rött – attacken har spridit sig till det urbana nätverket. På några minuter är hela samhället i digitalt kaos. För första gången inser både människor och maskiner att när tryggheten är total – är utsattheten också det.

Brottsscenario 2.

Framtidens digitala gisslan – när data blir makt

I framtidens hyperuppkopplade samhälle är data inte bara en resurs – den är själva blodomloppet i vardagen. Allt från kylskåp och dörrlås till bilar, hälsosystem och myndighetstjänster styrs av AI och sammankopplade sensorer. Det som en gång var praktiska hjälpmedel har blivit en digital spegel av våra liv, där varje rörelse, varje ord och varje biometrisk signal lagras, analyseras och används för att skapa bekvämlighet och säkerhet.

Men denna digitala närhet har en baksida. Angripare behöver inte längre bryta sig in genom dörrar – de tar sig in genom kod. Med hjälp av falska uppdateringar, sårbara sensorer eller läckande wearables kan de samla in allt från lösenord och hälsodata till rörelsemönster och röstprover. Ofta sker det diskret och långsamt: små förändringar, subtil manipulation, där de utsatta knappt märker när kontrollen glider dem ur händerna. När angriparna väl har tillgång till individens eller familjens digitala ekosystem kan de låsa, manipulera eller hota att förstöra det som är viktigast: identitet, ekonomi, tillgång till hemmet och till och med hälsa.

Utpressning har blivit digital vardag. Det kan handla om att låsa självkörande bilar mitt i rusningstid, kräva en lösensumma för att låsa upp ett hem, eller använda stulen biometrisk data för att begå bedrägerier i offrets namn. Fragmenterade ekosystem och brist på gemensamma standarder gör det svårt att försvara sig, och ansvaret för säkerheten hamnar ofta mellan stolarna. I denna värld är det inte längre bara tekniken som måste vara robust – det är hela samhällskontraktet som måste omprövas när data blir både tillgång och gisslan.

Gisslan i det digitala hemmet, 2032

Ava kommer hem till sin lägenhet i den hypermoderna stadsdelen. Allt fungerar som vanligt – dörren låser upp sig med en diskret blinkning, belysningen anpassar sig till hennes puls, och kaffemaskinen surrar igång när hon kliver in. Hennes AI-assistent har redan analyserat dagens kalender och föreslår ett träningspass följt av en avkopplande spellista.

Men under ytan har något förändrats. Ava märker först små detaljer – kylskåpet beställer varor hon inte brukar köpa, hennes smarta spegel visar ett ovanligt hälsotips, och ett paket levereras trots att hon inte minns att hon beställt något. Hon avfärdar det som AI:n som blivit lite för självgående.

Dagarna går och subtila förändringar fortsätter. Ett oväntat meddelande dyker upp i hennes bankapp: ”Din kreditgräns har justerats.” Hon får en påminnelse om en läkartid hon aldrig bokat. Hennes röststyrda högtalare svarar ibland på frågor hon inte ställt. Det är som om någon annan lever ett parallellt liv i hennes digitala skugga.

En kväll, när Ava försöker logga in med sitt digitala ID för att signera ett viktigt dokument, nekas hon tillträde. Ett meddelande visas: ”För att återfå full tillgång, vänligen följ instruktionerna i det säkrade meddelandet.” Hon hittar ett diskret e-postmeddelande, till synes från sin bank, där det står att hennes identitet har tagits som säkerhet – och att en lösensumma krävs för att återställa hennes digitala liv.

Inga hotfulla röster, inga blinkande varningslampor. Bara en kall, klinisk känsla av att någon annan styr – och att hon, utan att förstå när det hände, förlorat kontrollen över sitt hem, sin ekonomi och sin identitet. Ava inser att det mest sofistikerade hotet är det som aldrig syns, bara känns – som en skugga i det smarta hemmet, alltid ett steg före.

Brottsscenario 3.

Påverkan i den autonoma, hållbara staden

I framtidens smarta städer är AI och IoT sammanflätade med varje aspekt av livet: sensorer och algoritmer styr vatten, el, transporter, avfall och till och med medborgarnas möjligheter. Digitala tvillingar – virtuella kopior av staden – används för att simulera och optimera beslut, från trafikflöden till bostadsfördelning och miljöåtgärder. Denna intelligens gör det möjligt att minimera klimatavtryck och maximera resursutnyttjande, men innebär också att samhället blir beroende av att data och algoritmer fungerar korrekt och är tillförlitliga.

Det är här hoten blir mer sofistikerade. Angripare kan manipulera själva dataflödet: genom att mata in falska värden om exempelvis energiförbrukning eller trafik skapas felaktiga simuleringar, vilket leder till att resurser omfördelas på ett sätt som gynnar angriparen eller skapar kaos. Men det räcker inte där. Ett ännu mer avancerat angrepp är att rikta in sig på algoritmerna själva – att ändra hur de tolkar och prioriterar data. En manipulerad algoritm kan börja mata in felaktiga beslut i systemet, även om grunddatan är korrekt, eller dölja manipulationen genom att generera trovärdiga men felaktiga analyser.

Detta skapar ett dilemma: även om dataflöden övervakas och skyddas, kan själva beslutsprocessen vara kontaminerad. Brottsligheten blir osynlig, gömd i kod och logik, och kan påverka allt från vilka som får bostad till hur resurser fördelas mellan stadsdelar. I en värld där tillit till data och algoritmer är grundläggande för samhällets funktion, blir det avgörande att säkerhet, etik och transparens vävs in i både datainsamling och algoritmdesign – annars riskerar vi att skapa system där manipulationen är så subtil att den knappt går att upptäcka förrän konsekvenserna redan är ett faktum.

Malik och den osynliga påverkan

Malik, gymnasielärare i TerraNova, har alltid litat på stadens digitala system. Hans kalender synkas automatiskt med skolans schema, AI-assistenten föreslår lektionsupplägg och han får regelbundet feedback på sitt arbete. Men under några veckor börjar något skava. Han får påminnelser om möten som redan ägt rum, och AI:n föreslår undervisningsmaterial som är irrelevant för hans ämne. Kollegor verkar undvika honom, och han märker att han inte längre bjuds in till arbetsgruppens digitala chatt.

Malik försöker avfärda det som stress, men snart börjar han tvivla på sig själv. Automatiskt genererade utvärderingar antyder att hans elever är missnöjda, trots att lektionerna gått bra. Han ser inlägg i skolans interna nätverk där hans beslut ifrågasätts, men kan inte hitta avsändaren. Sakta växer en oro: har han gjort något fel, eller är det något med systemet?

Det Malik inte vet är att han blivit måltavla för ett avancerat angrepp. En aktör har manipulerat både hans digitala profil och de algoritmer som styr feedback och kommunikation. Vissa data har ändrats – men framför allt har algoritmerna börjat tolka hans aktiviteter på ett missvisande sätt, och genererar nu subtilt negativ respons. Hans digitala närvaro försvagas gradvis, och han börjar ifrågasätta sitt eget omdöme.

Malik drar sig undan kollegor, sover sämre och tappar självförtroende. Det är först när en annan lärare uppmärksammar liknande mönster som de börjar ana att det handlar om manipulation – inte personliga misslyckanden. För Malik har skadan redan skett: hans tillit till både sig själv och systemet är naggad i kanten, och han bär med sig en känsla av maktlöshet och tvivel – ett tyst brott, där gränsen mellan data och algoritm blivit osynlig.

Brottsscenario 4.

Mottrender i den digitalt förstärkta verkligheten

När digital säkerhet når nya höjder förändras landskapet för både brottslingar och samhälle. Kryptering, biometriska lås och AI-baserad övervakning blir vardag, och digitala attacker – från dataintrång till ransomware – möts av allt mer avancerade skydd. I takt med att dessa skyddsmekanismer förfinas är det tänkbart att antalet digitala angrepp förhindras, och brottsligheten tvingas söka nya vägar.

Här öppnar sig en möjlig mottrend. Med hjälp av sensorer, öppna datakällor och autonoma analysverktyg kan kriminella grupper kartlägga individer, företag och organisationer på en nivå som tidigare varit otänkbar. AI-agenter följer våra rörelsemönster, analyserar våra rutiner och identifierar ögonblick när vi är som mest sårbara – inte i den digitala infrastrukturen, utan i den fysiska världen. Det handlar inte längre om att bryta sig in i ett system, utan om att ringa in ögonblicket då människan själv blir nyckeln till de digitala tillgångarna.

I denna framtid kan vi se hur det digitala och det fysiska smälter samman i ett nytt slags rånmodus. Brottet börjar i datan, men kulminerar i verkligheten: en konfrontation i hemmet, på kontoret eller på gatan, där hot eller närvaro används för att tvinga fram tillgång till digitala resurser. Det är en hybrid brottslighet där gränsen mellan cyber och fysisk värld suddas ut, och där säkerhet måste förstås som något mer än bara tekniska barriärer.

Detta väcker frågor om hur vi bygger robusta skydd, inte bara mot digital manipulation utan också mot kartläggning och fysiska angrepp som tar avstamp i digital information. I takt med att tekniken utvecklas och samhället blir alltmer sammankopplat, blir det centralt att tänka brett kring säkerhet – och att vara öppen för att hoten kan ta nya, oväntade former. Kanske är det just i samspelet mellan människa, teknik och miljö som framtidens trygghet måste formas?

Analogt våld i en digital fästning

Regnet ligger som en tunn slöja över det fashionabla området norr om Helsingborg. I en modern villa med utsikt över Öresund sitter familjen Andersen vid middagsbordet. Hemmet är, liksom de flesta i området, utrustat med avancerade säkerhetssystem – allt uppkopplat och övervakat av självlärande AI och kvantsäker kryptering. Brott är inte omöjliga, men betydligt svårare nu, särskilt för cyberbrottslingar. Digitala attacker sker fortfarande, men i liten skala. Idag krävs stor skicklighet och resurser för att lyckas.

Familjen känner sig trygg, men vet att inget system är helt vattentätt. Mads påminner ofta om att det viktigaste är att hålla sig lugn – tekniken är på deras sida, men inget är garanterat.

Utanför, i mörkret, väntar Exmander Dragon. De är en ny sorts kriminella, sprungna ur den ökade digitala säkerheten som gjort det svårt att stjäla data och utföra bedrägerier. Istället använder de sin digitala kompetens för att möjliggöra fysiska brott med stora vinster. Under månader har de kartlagt familjens vanor, lärt sig AI-systemets rutiner och letat efter små, mänskliga misstag.

När huset går in i sitt underhållsläge slår Exmander Dragon till. En störsändare slår ut kommunikationen mellan sensorer och nätverk, tillräckligt för att skapa ett kort fönster av förvirring. Gruppen tar sig in genom ett fönster på baksidan, maskerade mot kameror och biometriska sensorer. Inne i huset möter de familjen, som snabbt förstår allvaret. Hotet om våld räcker – Louise och Mads tvingas under vapenhot öppna kassaskåp och godkänna överföring av kryptovaluta från sina kroppsburna wallets.

Allt sker snabbt och tyst. När systemet startar om är Exmander Dragon redan borta, utan ett spår. I minuterna efteråt är det bara regnet och den ovanliga tystnaden som vittnar om rånet och att tryggheten brutits.

Utmaningar och reflektioner

Perspektiv på trygghet i en superintelligent värld

Utvecklingen av smarta och uppkopplade hem drivs av en kombination av bekvämlighet för användarna, kommersiella intressen och ett ökat fokus på hållbarhet.

Samtidigt växer nya sårbarheter fram i den utvecklingen. När hemmen blir mer autonoma och fler enheter kopplas upp – från kameror och dörrlås till kylskåp och röstassistenter – förändras trygghet och integritet. En särskild risk är ändamålsglidning - att tekniken används för andra syften än vad användaren tänkt eller godkänt.

Detta väcker frågor om integritet, etik och övervakning. När fysiska platser blir alltmer uppkopplade är det viktigt att tekniken används med respekt för individens frihet och personliga integritet. Ingen aktör bär hela ansvaret – det är samspelet mellan teknikleverantörer, användare, myndigheter och andra som formar möjligheter och risker. Transparens, valfrihet och tydlig reglering är viktiga verktyg, men bör balanseras mot innovation och ekonomisk utveckling.

De framtidsscenarier och brottsexempel som rapporten beskriver visar att teknikutvecklingen öppnar för nya möjligheter – både positiva och utmanande. För att möta dessa behövs insatser från myndigheter, företag, forskare, civilsamhälle och individer. Ingen ensam aktör har alla svaren eller kan ensam säkerställa en trygg framtid.

Det är också avgörande att etiska och mänskliga värderingar genomsyrar teknikutveckling och regelverk.

”Om vi inte vänder trenden nu så kommer kriminella organisationer leda världen ”, *Hanna Linderstål*.

Hanna Linderstål är vd och grundare av Earhart Business Protection Agency, en specialistbyrå inom cyberintelligens. Med över 25 års erfarenhet av att bekämpa digitala och virtuella hot är hon rådgivare åt olika myndigheter, företag och internationella organisationer. Hanna arbetar som rådgivare, men har även föreläst både nationellt och internationellt om cyberhot, informationspåverkan och digitalt spionage. Hanna blev utnämnd till Årets Säkerhetsprofil år 2024.

Hotbilden – nuläge och utveckling

Sverige står inför en snabbt föränderlig hotbild där både kriminella organisationer och statsaktörer utvecklar avancerade metoder för att stjäla pengar och påverka samhällsviktiga system. Dessa aktörer agerar allt mer organiserat och tekniskt sofistikerat, vilket gör att de snabbt kan ta nya positioner på den illegala marknaden. Enligt Linderstål har det skett ett skifte där statsaktörer som Kina och Ryssland inte bara spionerar i befintliga system, utan även bygger egna tekniska plattformar för att samla in data och påverka samhällsutvecklingen.

När våra vardagsmiljöer fylls med smarta, uppkopplade enheter ökar risken för övervakning. Hoten kommer inte bara från kriminella, utan även från länder som tillverkar och distribuerar enheter med sensorer som kan samla in information och påverka.

Sårbarheter och utmaningar

Den ökade digitaliseringen har gjort samhället sårbart. Om mobilen är urladdad eller en digital ID-app inte fungerar, kan det påverka allt från kollektivtrafik till paketutlämning. Alla medarbetare är potentiella ingångspunkter för cyberangrepp, Linderstål menar att för mycket ansvar lagts på användarna istället för att utveckla tekniska lösningar som angriper grundproblemen. Ofta behandlas symptomen, inte orsakerna. Dessutom har beslutsfattare ibland en förlegad bild av hoten, vilket försvårar arbetet.

Konsekvenser för Sverige

Utvecklingen innebär stora risker - en låg säkerhetsnivå kan underminera internationella investeringar och marknadens förtroende i Sverige. Hotet från hybridattacker mot både privat och offentlig sektor ökar – ofta avfärdade som olyckshändelser trots att de är del av hybridkrigföring, påpekar Linderstål. Att svenska företag frekvent betalar lösensummor vid ransomware gör dessutom landet extra lockande för kriminella.

En långsiktig cyberstrategi för Sverige

Sverige har byggt upp stora branscher och är ett av världens mest digitaliserade länder, men saknar en långsiktig plan för att skydda sig mot digitala hot. Linderstål påtalar att vi behöver en nationell cyberstrategi – kanske en 50-årsplan – för att möta framtidens utmaningar.

Kunskap om cybersäkerhet måste bli en självklar del av samhället. Informationssäkerhet bör införas som ämne redan i grundskolan, så att barn tidigt förstår digitala miljöer och data. Länder som lyckats fostra skickliga cyberspecialister har ofta fångat upp unga talanger tidigt och visat dem möjligheterna inom cyber.

En nationell cyberpolis med tydligt mandat behövs för att bekämpa digital brottslighet. Idag saknas resurser för att hjälpa privatpersoner som utsatts för nätbedrägerier eller identitetsstölder, och företag riskerar konkurs vid ransomware-attacker innan hjälp kommer. Polisen är redan hårt belastad och behöver specialiserade resurser för digitala brott.

För att strategin ska lyckas krävs samarbete mellan myndigheter, näringsliv och utbildning – samt internationellt samarbete. Cyberhot känner inga gränser, och Sveriges försvar måste vara samordnat, betonar Linderstål. Med långsiktiga satsningar, ökad kunskap, rätt resurser och starkt samarbete kan Sverige bli världsledande inom cybersäkerhet.

Paradigmskifte: Från försvar till offensiv cybersäkerhet

Linderstål menar att Sverige inte längre kan nöja sig med att bara försvara sig mot cyberhot. Cyber defence, att skydda system och data med tekniska lösningar och utbildning, är en reaktiv strategi som ofta innebär att vi agerar först när skadan är skedd. Det räcker inte längre.

För att möta framtidens brottslighet krävs en offensiv strategi – cyber offence. Det handlar om att aktivt söka upp, kartlägga och störa angripare innan de slår till. Genom att ligga steget före kan vi minska risken för attacker och stärka skyddet.

Vi står inför ett paradigmskifte där cyberhoten växer snabbare än våra försvar; utan offensiva insatser, ökat samarbete och en modern säkerhetssyn riskerar vi att tappa kontrollen, varnar Linderstål.

”Varenda pryl vi kopplar upp kan användas för en sak idag - men kanske en annan sak imorgon”, *Karl Emil Nikka*.

Data som måltavlor i en digital framtid

I en alltmer digitaliserad värld där smarta prylar, AI och sensorer omger oss överallt, växer nya hot fram. Nikka beskriver hur framtidens digitala brottslighet – från intrång och överbelastningsattacker till missbruk av data och avancerad övervakning – kan drabba individer, företag och samhälle. Hoten är många, föränderliga och svåra att skydda sig mot, och enligt Nikka finns inga enkla lösningar i sikte.

Sårbar teknik – öppna dörrar för angrepp

Den snabba teknikutvecklingen har lett till att enorma mängder data samlas in och lagras, ofta i molnlösningar. Nikka poängterar att denna datainsamling gör samhället sårbart. Han lyfter fram dataläckan hos VW Group 2024 som ett tydligt exempel, där positioner för över 800 000 bilar blev åtkomliga för obehöriga. Det kan leda till att man kan kartlägga hur fordon och deras ägare rör sig samt vilka kontakter de har, vilket i sin tur kan blottlägga nätverk och relationer som illvilliga aktörer kan utnyttja på olika sätt. Enligt Nikka visar det här tydligt hur rörelsemönster, hämtade via bilarnas sensorer, kan missbrukas på sätt som ingen ursprungligen hade förutsett och som kan skada på personnivå, organisationsnivå och samhällsnivå.

Kameror och sensorer i bilar och hem tillverkas ofta i andra länder – exempelvis Kina och USA, där kontrollen över datahanteringen kan vara svagare. Detta kan ge utländska aktörer tillgång till känslig information om Sverige och kan utnyttjas för spionage, vilket Nikka ser som ett allvarligt samhällshot. Det handlar inte bara om kameror vi skruvar upp på väggar, utan även om de tusentals sensorer som vi har i uppkopplade enheter och bilar.

Små prylar, stora risker

Tekniska sårbarheter i framtidens IoT-enheter kan också utnyttjas för ddos-attacker och som intrångsvägar i nätverk. Nikka nämner ett exempel där ett intrång i ett kasinonätverk gjordes via en internetuppkopplad akvarietermostat – ett oväntat men tydligt exempel på hur även små prylar kan bli ingångar för angripare.

Ändamålsglidning - när data byter syfte

En av de största framtida utmaningarna, enligt Nikka, är ändamålsglidning. I takt med att alltmer data samlas in (för ett visst syfte) ökar risken att samma information senare används på helt andra sätt än vad användaren tänkt sig. Nikka beskriver hur sensorer byggs in i vår vardag för att skapa bekvämlighet eller öka säkerheten – till exempel en handsfree-mikrofon i bilen – men att dessa i framtiden kan användas för att analysera samtal och därefter rikta reklam baserat på vad som sägs och var bilen befinner sig. Biltillverkaren Ford har redan ansökt om patent för just detta. Det som idag motiveras med bekvämlighet eller säkerhet kan alltså få ett helt nytt användningsområde imorgon – ibland harmlöst, ibland utan att användaren är medveten om det, och ibland med illvilliga avsikter. Nikka understryker att denna glidning av syften är svår att kontrollera i takt med att mängden data växer och delas mellan olika aktörer.

Integritetsparadoxen – anonym men ändå sårbar

Samtidigt finns en paradox: massinsamling av data kan vara värdefull för att utveckla nya tjänster och förbättra samhället, men medför också ökade risker för den personliga integriteten. Även om data anonymiseras kan detaljer eller mönster i materialet fortfarande avslöja känslig information eller användas på sätt som inte var avsedda från början. Därför kvarstår integritetsriskerna, trots försök att skydda data genom anonymisering.

Bygga framtidens digitala försvar – vägen framåt

För att möta framtida utmaningar lyfter Nikka fram flera insatser. Han menar att CE-märkningen, som fungerar som konsumentskydd, även bör omfatta cybersäkerhet och ansvar för att hålla uppkopplade produkter säkra genom regelbundna uppdateringar. Nikka betonar vikten av ökad upphandlingskompetens, så att företag och offentliga verksamheter kan ställa rätt säkerhetskrav vid inköp av IoT-produkter. Han ifrågasätter också varför insamlade data automatiskt ska delas med tillverkare, och när vi bör sätta gränser för detta.

Designad säkerhet

Enligt Nikka kommer det vara avgörande att bygga in säkerhet i tekniken redan från början, så kallad *security by design*. Om data krypteras och bara ägaren har tillgång till nyckeln, minskar risken för missbruk även om informationen lagras i molnet. Nikka menar att det inte är själva insamlingen av data som är farlig, utan hur den hanteras och skyddas.

Framtiden för digital säkerhet kommer att kräva både teknisk innovation och ett nytt sätt att tänka kring ansvar och integritet, poängterar Nikka.

Karl Emil Nikka *är IT-säkerhetsspecialist, författare och föreläsare med särskilt fokus på säkerhetsmedvetenhet och digitala hot. Han utsågs till Årets säkerhetsprofil 2021 av Företagsuniversitetet och branschtidningen Aktuell Säkerhet. Han arbetar även om konsult inom IT-säkerhetsfrågor åt SSF Stöldskyddsföreningens.*

"EU måste ha ambitionen att vara ledande inom utvecklingen av AI för sina starkaste sektorer, återta och behålla kontrollen över data och känsliga molntjänster, och utveckla ett robust ekonomiskt och talangbaserat klimat för att stödja innovation inom datahantering och AI." - Mario Draghi, från rapporten "The future of European competitiveness"

Europas vägval

Utvecklingen av AI och superintelligens ställer Europa inför en rad utmaningar som är både komplexa och svåra att överblicka. I en värld där teknikens framsteg drivs snabbt av globala aktörer, blir frågor om konkurrenskraft, innovation och ansvar särskilt påtagliga. Det finns en balansgång mellan att värna om grundläggande värden som integritet och mänskliga rättigheter, och samtidigt kunna delta i den teknologiska utvecklingen på ett sätt som stärker Europas näringsliv och innovationskraft. Det är inte alltid självklart hur denna balans ska uppnås. Tempot i utvecklingen, den ökande komplexiteten i tekniska system och de olika förväntningarna från både marknad och samhälle gör att vägvalen sällan är enkla. Samtidigt är det tydligt att Europas position påverkas av hur väl man kan navigera mellan kommersiella intressen, etiska överväganden och behovet av att skapa förtroende hos både användare och samarbetspartners. Frågorna om vem som sätter riktningen för teknikutvecklingen, hur värderingar vägs mot affärsintressen och på vilket sätt ansvar kan delas mellan olika aktörer är ständigt närvarande. Det är en pågående process, där det kanske inte finns några givna svar – men där reflektion och öppen dialog kan bidra till att belysa både möjligheter och risker som Europa står inför i den globala AI-utvecklingen.

Vi kan forma och påverka den superintelligenta framtiden

När AI blir skickligare på att förstå och efterlikna mänskligt beteende ökar risken att människor själva blir den svagaste länken i kedjan. För att motverka det krävs tydlig insyn i hur systemen fungerar och möjligheter till mänskligt ingripande när något går fel. Samtidigt ställer globala AI-hot – som autonoma vapen och storskaliga cyberattacker – krav på gemensamma regler och standarder som täcker allt från utveckling till användning.

Ett grundläggande koncept är ”security by design”, säkerhet och dataskydd måste integreras i varje steg av produktutvecklingen, inte läggas till i efterhand. I praktiken innebär det att algoritmernas indata, beslutslogik och hantering av bias behöver vara transparent och kontinuerligt granskad. När vårt dagliga liv i allt högre grad formas av algoritmiska beslut måste vi veta vilka datakällor som används, hur besluten fattas och hur eventuella fel i systemet åtgärdas.

Teknikutvecklingen går så snabbt att löpande utbildning i AI-etik och riskhantering blir en nödvändighet för alla som på något sätt arbetar med eller påverkas av AI-lösningar. Utöver utbildningsinsatser krävs även nya tekniska verktyg och regelverk som snabbt kan identifiera och stoppa AI-driven desinformation. Den kombinerade effekten av kunskap, tydliga regler och rätt tekniska skyddsmekanismer ger oss möjligheten att styra utvecklingen mot en trygg och ansvarsfull superintelligent framtid.

Tillsammans kan myndigheter, företag, civilsamhälle och användare dela kunskap, sprida bästa praxis och kontinuerligt höja den lägsta säkerhetsnivån. Lättillgängliga utbildningar, tydliga verktyg för privatpersoner och knutna branschinitiativ hjälper utsatta grupper att förstå risker och försvara sin integritet. Genom att förena tekniska skyddsåtgärder med etisk reflektion och bred samverkan kan vi forma en digital framtid där avancerad teknik stärker vår frihet, trygghet och värdighet – snarare än hotar dem.

Inga nationella gränser stoppar cyberhot eller AI-drivna angrepp. Effektivt försvar bygger därför på internationellt samarbete: gemensamma standarder, snabbspår för informationsutbyte och delade incident-centra. Genom samarbeten kan länder snabbt sprida lärdomar från en attack till hela nätverket – och därmed minimera skadorna.

Avslutande reflektioner

Nyckelinsikter och lärdomar

Utvecklingen av uppkopplade och intelligenta miljöer förändrar snabbt förutsättningarna för både samhällsfunktioner och kriminalitet. AI, IoT, spatial intelligens och agentiska system skapar nya infrastrukturer där beslut ofta tas utan mänsklig inblandning. Detta förändrar också spelplanen för brott – från cyberattacker och manipulerade digitala tvillingar till digitala inbrott i smarta hem och algoritmiskt förtryck. Brott sker alltmer i kod snarare än med kofot, och kriminella aktörer anpassar sig snabbt till denna nya verklighet genom att utnyttja sårbarheter, brist på reglering och teknikens komplexitet.

En särskilt viktig aspekt är risken för ändamålsglidning – när teknik eller data som samlats in för ett syfte gradvis används för andra ändamål utan användarens vetskap eller samtycke. Detta kan urholka både integritet och förtroende, särskilt när AI-system fattar beslut i det fördolda och användningsområdena snabbt förändras.

Utmaningar och begränsningar

Det är svårt att få full insyn i nuvarande och framtida brottsscenarier i en värld som fortfarande håller på att formas. Kriminalitet är ofta dold, och teknikutvecklingen går snabbt. Många potentiella hot ligger dessutom i gråzoner där reglering saknas, särskilt när AI-system är självförbättrande och beslutsfattandet sker distribuerat och utan mänsklig kontroll.

När hem, fordon och städer blir mer autonoma och självlärande växer både möjligheter och risker. Data kan användas för syften som överskrider användarens godkännande, integriteten utmanas och nya maktstrukturer byggs in i algoritmerna. Dessa system bär alltid sina skapares värderingar, vilket gör det avgörande att ställa frågor om vem som styr och hur beslut fattas. För att undvika ändamålsglidning och övervakning utan medgivande behövs transparens, tydliga villkor och respekt för individens frihet redan i designfasen.

Vägar framåt: teknik, etik och ansvar

Teknik är en förutsättning för trygghet, men behöver kombineras med starka skyddsmekanismer. Zero-trust-arkitektur och krypterad kommunikation är centrala delar av motståndskraftiga system. Öppna och ansvarsfulla algoritmer kan skapa försvar som lär sig av nya angrepp och upprätthåller hög säkerhetsstandard.

Etiska principer behöver integreras i varje steg av utvecklingen. "Security-and-ethics-by-design" innebär att redan från prototypstadiet bygga in transparens, rättvisa och användarvänlighet. När system är öppna och förståeliga minskar risken för missbruk, och människor kan känna trygghet i att deras data hanteras ansvarsfullt.

Framtida frågor och fortsatt utforskande

Många frågor återstår. Hur kan risken minimeras att AI-system används för brott eller skapar nya sätt att begå brott? Hur kan rättsväsendet få insyn och möjlighet att utreda brott i autonoma system där mänsklig kontroll ofta saknas? Vilka juridiska ramar behövs för att skydda individens rättigheter när brott begås med hjälp av avancerad teknik? Det finns också behov av mer kunskap om hur algoritmiska beslutsprocesser kan påverka olika grupper och hur digital sårbarhet relaterar till klass, kön och geografisk tillgång.

Det är viktigt att poängtera att ingen ensam aktör har alla svaren. Framtidens brottslighet och tekniska utveckling är komplexa och föränderliga. Den här rapporten är ett försök att bidra med insikter och frågor snarare än färdiga lösningar.

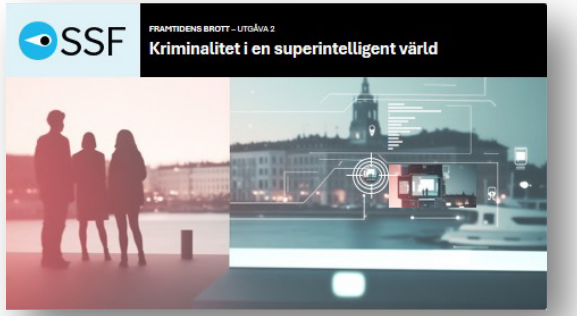
Avslutande tankar

Brottslighet i en superintelligent värld går inte att bortse ifrån. Men framtidens maktkamp är inte förutbestämd. Hela samhället måste hänga med i teknikutvecklingen – från lagstiftare och företag till vård, skola och civilsamhälle – för att möta de utmaningar som följer. Samhällets uppgift är att se till att utvecklingen inte bara leder till smartare system, utan också till ökad säkerhet, rättvisa och inkludering. Tekniken kan stärka människans frihet och trygghet – men bara om utveckling och användning präglas av insikt, ansvar och värderingsstyrning.

Den intelligenta världen formas nu. Framtiden är inte skriven – den är vår att skapa tillsammans, med öppenhet för nya perspektiv och ödmjukhet inför det vi ännu inte vet.

Framtidens Brott är en rapportserie på initiativ av SSF

Rapporten ”Kriminalitet i en superintelligent värld” är en utgåva i SSF koncept Framtidens Brott som tagits fram 2025. En tredje rapport publiceras hösten 2025 och en fjärde rapport utkommer året därpå.



Rapporten ”Den Kriminella Spelplanen” är en utgåva i SSF koncept Framtidens Brott som tagits fram 2024.

Expertintervjuer:

Christian Smith
Docent i datavetenskap på KTH i Stockholm

Hanna Linderstål
VD och grundare av Earhart Business Protection Agency

David Jacoby
Etisk hackare och IT-säkerhetsexpert

Amy Loutfi
Professor i datavetenskap och vice rektor för AI och innovation vid Örebro universitet, programdirektör för Wallenberg AI, Autonomous Systems and Software Program (WASP)

Karl Emil Nikka
IT-säkerhetsspecialist, författare och föreläsare med särskilt fokus på säkerhetsmedvetenhet och digitala hot

Projektgrupp:

Ulrika Hallesius
Kriminolog på SSF Stöldskyddsföreningen
ulrika.hallesius@stoldskyddsforeningen.se

Charlotte Mattfolk
Framtidsanalytiker på IAMAI

Charlotte Ellius
UX och formgivare på IAMAI

Länkar för ytterligare läsning

Inledning

8) https://www.techhubben.se/blogs/sa-kommer-ai-att-forandra-vara-liv-under-2025

https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2022/det-uppkopplade-hemmet-och-smarta-prylar/

9) https://www.netflix.com/se/title/81621534

10) https://www.filmhistoria.se/science-fiction.html

https://www.kairosfuture.com/se/publikationer/nyheter/dagens-science-fiction-morgondagens-verklighet/

https://www.rymdstyrelsen.se/upptack-rymden/bloggen/2022/05/rymden-en-kalla-till-inspiration-och-losning/

En bekväm och uppkopplad tillvaro

12) https://www.aiuc.se/ai-insikter/ai-trender-2025
https://www.euronews.com/2025/01/15/french-submarine-crew-accidentally-leak-sensitive-information-through-strava-app

The Times of IndiaThe Verge.

https://www.reuters.com/business/meta-expands-ai-access-ray-ban-smart-glasses-europe-2025-04-23/

13) https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025?utm_source=chatgpt.com

IBM X-Force Threat Intelligence

Verizon DBIR

https://www.statista.com/outlook/tmo/internet-of-things/sweden

IoT Security Foundation

NIST

14) Eurostat AI statistics 2023

AI-mognad i svenska företag (pdf)

AI i offentlig sektor (DIGG)

AI Sweden – Impact Hack

Statista – Global AI market share

Gartner Magic Quadrant

IoT Analytics – Top IoT Platforms

McKinsey – China's AI ecosystem

15-16) https://www.amazon.com/Introducing-Amazon-Astro/dp/B078NSDFSB

https://gs.statcounter.com/os-market-share/mobile/sweden

https://www.voister.se/artikel/2021/06/halva-jordens-befolkning-har-en-smartphone/

https://regeringen.se/contentassets/fe3e296228fb474f803a986ae3842b4c/sveriges-digitaliseringsstrategi-20252030.pdf

https://www.publikt.se/nyhet/ny-digitaliseringsstrategi-fokuserar-pa-ai-27163

Framtidens superintelligenta värld

18: https://projektledning.se/spatial-intelligens/
https://services.google.com/fh/files/misc/google_cloud_future_of_ai_perspectives_for_startups_2025.pdf

19: https://www.ri.se/sv/digitala-tvillingar-kan-gora-kommuner-och-foretag-battre-rustade-for-framtiden

21: https://www.ibm.com/think/topics/artificial-superintelligence

https://www.gamereactor.se/openai-chefen-tror-att-vi-under-2025-kommer-fa-forsta-exemplet-pa-superintelligent-ai-1463623/

Utmaningar och reflektioner

45: https://www.bginstitute.se/ny-rapport-sverige-maste-satsa-pa-ai-kompetens-for-att-inte-halka-efter/

https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/risker-och-sarbarheter-inom-cybersakerhet-och-cyberfysiska-system/cyberfysiska-system/sakrare-internet-of-things-iot/