FRAMTIDENS BROTT – UTGÅVA 3

Datakarteller & det kriminella värdet av data

SSF

Brottslighet i en datadriven värld

Data har blivit vår tids mest kraftfulla råvara.

Den formar ekonomier, styr beslut och påverkar hur samhällen utvecklas. Varje köp, rörelse och sökning lämnar spår som tillsammans berättar vilka vi är och vad vi kanske gör härnäst.

Där pengar en gång var den största tillgången är det nu data som skapar makt, inflytande och kontroll. Med framväxten av språkmodeller och artificiell intelligens har den fått en ny dimension. Data kan inte bara lagras och analyseras, utan även tolkas, förutsägas och återskapas i form av digitala uttryck som liknar mänskligt agerande.

Men i takt med att värdet ökar växer också intresset från dem som vill utnyttja det. I skuggorna av den digitala ekonomin växer en ny typ av ageranden fram där algoritmer och språkmodeller används för att påverka, förvränga, kontrollera och utvinna information i stor skala, ibland som brott och ibland i gråzoner som utnyttjar luckor i dagens system.

Det är denna berättelse vi vill fördjupa. Om hur data blir brottslighetens nya råvara och hur kampen om information formar framtidens makt.

Innehållsförteckning

Inledning - kriminella datakarteller i en ny brottsekonomi

När data blir brott

Det börjar till synes oskyldigt. En sökning, ett klick, en inloggning och någonstans registreras allt. Data som en gång samlades in för att förstå världen används i dag också för att styra den. Aldrig tidigare har så mycket information funnits om människor, företag och samhällsfunktioner. Data har blivit en eftertraktad tillgång och ligger till grund för både tillväxt och kontroll.

Där data flödar uppstår också brott och ageranden i gråzoner. När information kan kopieras, kombineras och säljas utan att förbrukas växer mer organiserade former av exploatering fram. I denna rapport beskriver vi dessa strukturer som datakarteller, aktörer som skapar inflytande genom att kontrollera digitala flöden och information.

Datakarteller

I rapporten använder vi begreppet datakarteller som ett samlingsnamn för strukturer där stora mängder data samlas, delas och kontrolleras av en begränsad grupp aktörer. Dessa sammanslutningar kan verka i gråzoner mellan lagligt och olagligt, där data används som ekonomisk och strategisk resurs. Datakarteller kan bestå av kommersiella aktörer som söker ekonomiska fördelar, statliga organisationer som använder data för maktutövning eller kriminella nätverk som exploaterar data för olagliga syften. Begreppet fungerar som en gemensam ram för att förstå hur olika aktörer skapar makt med data och hur de använder information för påverkan, manipulation och ekonomisk vinning.

Denna utveckling pekar mot ett skifte i den kriminella ekonomin. Brottsligheten rör sig i allt högre grad in i digitala miljöer, där data blir verktyg för att påverka marknader, institutioner och människor över nationsgränser. Språkmodeller och AI-system förstärker utvecklingen genom att omvandla stora datamängder till beslut och påverkan i realtid. Ofta sker detta utan att lämna tydliga spår och långt innan konsekvenserna blir synliga.

Risken handlar inte bara om hot mot integriteten, utan också om att gränsen mellan sanning och konstruktion börjar suddas ut. Ekonomier kan påverkas, val kan styras och institutioners legitimitet kan försvagas genom datadrivna metoder snarare än fysiskt våld. Samtidigt drivs datakarteller av ekonomisk vinning där stulna, manipulerade eller sammanställda data används för att skapa intäkter på andras bekostnad. På så vis utmanar de inte bara juridiska gränser, utan även samhällets förmåga att tolka och förstå sin omvärld.

Bakgrund

Detta är den tredje rapporten i Stöldskyddsföreningens serie Framtidens brott. Tidigare utgåvor har visat hur digitalisering, globalisering och teknisk utveckling förändrar brottslighetens former.

Den här rapporten riktar fokus mot data och dess växande betydelse som både drivkraft och råvara i den kriminalitet som utvecklas i takt med den digitala infrastrukturen och vårt allt mer digitaliserade samhälle.

Syfte

Syftet är att skapa en djupare förståelse för hur data används, missbrukas och exploateras i kommersiella, statliga och kriminella miljöer och att bidra med kunskap som stärker samhällets motståndskraft. Den ökande tillgången till data och utvecklingen av avancerade språkmodeller skapar nya gråzoner där analys kan övergå i påverkan och manipulation och där traditionella verktyg för kontroll och ansvarstagande inte alltid räcker till.

Metod och källor

Rapporten bygger på forskning, myndighetsmaterial och internationella källor samt intervjuer med experter inom cybersäkerhet, digital utveckling och brottslighet. Genom att kombinera akademiska och operativa perspektiv tydliggörs mönster som formar den framväxande brottsekonomin.

Framåtblick

Med dessa insikter som grund beskriver rapporten möjliga framtidsscenarier. Genom att belysa vart utvecklingen kan vara på väg vill vi bidra med perspektiv som stärker Sveriges förmåga att värna trygghet, möta hot och minska risker. Vi delar rapporten öppet i förhoppningen att den ska väcka idéer och ge nya ingångar till arbetet med att förstå och förebygga framtidens brott.

Mot en värld där data är vår mest strategiska resurs

Utvecklingen som vi ser i dag är bara början. När data blir en strategisk resurs förändras också förutsättningarna för både samhällen och brottslighet. De strukturer som växer fram nu kan bli avgörande för hur världen ser ut om 25 år.

Vi befinner oss i en tid av teknologiska språng, klimatutmaningar och global maktkamp, där data allt oftare hamnar i centrum. De aktörer som samlar in och tolkar mest data koncentrerar också sin makt och sitt inflytande. Denna utveckling sker både i den legitima ekonomin och i den kriminella världen. Här ser vi hur datakarteller växer fram som nya maktstrukturer med förmåga att styra utvecklingen i en viss riktning och påverka hela samhällen.

År 2050 är nästan varje yta, varje kropp och varje tanke uppkopplad. Data är då inte längre en digital biprodukt. Den är bränslet som driver ekonomier, styr beslut och formar vår förståelse av verkligheten. Frågan handlar därför inte bara om hur mycket data som samlas in, utan vem som kontrollerar den och hur den används när dess värde överstiger både olja och guld.

Data är redan en av världens mest värdefulla tillgångar. Därför blir den avgörande frågan inte priset utan makten. Vem äger den, tolkar den och använder den. De som förstår hur de stora megatrenderna formar datans roll får bättre förutsättningar att bygga samhällen som värnar transparens och frihet. De som inte gör det riskerar att vakna i en värld där algoritmer och karteller påverkar mer än den demokratiska processen gör, samtidigt som kriminella aktörer fortsätter utveckla sina egna datadrivna strukturer helt utanför dessa vägval.

Globala trender där data spelar huvudrollen

År 2050 är nästan hela världen uppkopplad och data blir en av de mest avgörande resurserna för stater, företag och kriminella aktörer.

Mot en mer oförutsägbar värld

Världens teknologiska utveckling går i snabb takt och påverkar redan idag hur vi lever, arbetar och kommunicerar. Det som tidigare kändes avlägset är nu vardag och nästa skifte väntar redan runt hörnet. Samtidigt sker förändringar som sträcker sig långt bortom tekniken och som tillsammans formar en mer komplex och osäker framtid.

Den globala utvecklingen rör sig snabbt och förändrar teknik, ekonomi och samhälle på djupet. Data blir en allt viktigare kraft i dessa skiften och påverkar hur människor lever, hur marknader formas och hur brottslighet utvecklas. Till mitten av seklet kan vi stå inför en värld där nästan allt lämnar digitala spår, vilket skapar möjligheter för effektivitet och innovation men också risker för övervakning, manipulation och kontroll.

Flera trender driver denna utveckling, bland annat:

- snabb tillväxt av data och mer kraftfull teknik
- ökad digitalisering av samhällsfunktioner
- fragmentering av internet
- växande arbetslöshet och minskad tillit
- globalt pressad ekonomi

Framtidens brottslighet formas av ett nytt landskap där data och digital infrastruktur är strategiska resurser. Kriminella kan exploatera uppkopplade system och AI-drivna analyser där språkmodeller spelar en växande roll för att bygga nya affärsmodeller och maktstrukturer i den digitala ekonomin.

Trender där data skapar nya kriminella möjligheter

Exponentiell tillväxt av data där automatisering och kvantdatorer skapar nya möjligheter

Data blir avgörande när naturresurser och samhällsfunktioner digitaliseras.

En fragmentisering av internet där den globala säkerheten kan undermineras

Arbetslöshet och minskad tillit gör det lättare att rekrytera till kriminella nätverk.

En globalt pressad ekonomi skapar möjligheter för skuggekonomier

AI, IoT, bioteknik, kvantdatorer och den massiva ökningen av uppkopplade system driver fram en ny våg av exponentiella dataflöden och sårbarheter.

Effekt

Den teknologiska utvecklingen accelererar – från artificiell intelligens och bioteknik till kvantdatorer och en explosionsartad tillväxt av uppkopplade system. Miljarder sensorer och enheter producerar oavbrutet data, samtidigt som nya verktyg gör det möjligt att samla in, bearbeta och exploatera information i industriell skala.

Konsekvens

Datamängderna ökar snabbt och allt fler system kopplas upp, vilket gör att attackytan växer. AI ger kriminella möjlighet att automatisera intrång, profilera offer och skapa syntetiska identiteter. Kvantdatorer kan i framtiden slå ut dagens kryptering. Resultatet är en kraftfull förstärkning av datans värde som råvara och vapen.

Trender där data skapar nya kriminella möjligheter

Exponentiell tillväxt av data där automatisering och kvantdatorer skapar nya möjligheter

Data blir avgörande när naturresurser och samhällsfunktioner digitaliseras.

En fragmentisering av internet där den globala säkerheten kan undermineras

Arbetslöshet och minskad tillit gör det lättare att rekrytera till kriminella nätverk.

En globalt pressad ekonomi skapar möjligheter för skuggekonomier

När klimatförändringar och resursbrist skapar instabilitet ökar också värdet på information om vatten, energi och råvaruflöden. Bräckliga digitala system som byggs under press blir sårbara mål, och kriminella kan utnyttja bristsituationer genom att manipulera data, störa leveranser eller använda informations-övertag för utpressning och sabotage.

Effekt

Klimatförändringar och resursknapphet driver migration, konflikter och samhällskriser. Tillgången till vatten, energi och kritiska mineraler blir starkt strategisk, och konkurrensen om dessa resurser ökar.

Konsekvens

Bräckliga system blir mål för cyberangrepp, och data kring energi, transport och försörjningskedjor får strategisk betydelse. Kriminella kan utnyttja bristsituationer för utpressning och sabotage, samtidigt som resursjakten gör stater och företag mer sårbara för intrång och manipulation.

Trender där data skapar nya kriminella möjligheter

Exponentiell tillväxt av data där automatisering och kvantdatorer skapar nya möjligheter

Data blir avgörande när naturresurser och samhällsfunktioner digitaliseras.

En fragmentisering av internet där den globala säkerheten kan undermineras

Arbetslöshet och minskad tillit gör det lättare att rekrytera till kriminella nätverk.

En globalt pressad ekonomi skapar möjligheter för skuggekonomier

Stormakter, regionala aktörer och icke-statliga grupper konkurrerar om kontrollen över digital infrastruktur, dataflöden och strategiska nätverk. Risk för en splittring av internet, ”splinternet” och ökad statlig exploatering av data.

Effekt

Konkurrensen om kontroll över nätverk och dataflöden intensifieras. Stormakter, regionala aktörer och icke-statliga grupper bygger cyberkapacitet och försöker sätta egna standarder.

Konsekvens

Internet riskerar att splittras i parallella system – ett splinternet – där dataflöden och sårbarheter används som geopolitiska verktyg. Stater kan hemlighålla och utnyttja kända sårbarheter för egen vinning, vilket underminerar global säkerhet. Samtidigt uppstår rättsliga glapp som gör det möjligt för gränsöverskridande kriminella nätverk att agera utan att begränsas av nationella lagar.

Trender där data skapar nya kriminella möjligheter

Exponentiell tillväxt av data där automatisering och kvantdatorer skapar nya möjligheter

Data blir avgörande när naturresurser och samhällsfunktioner digitaliseras.

En fragmentisering av internet där den globala säkerheten kan undermineras

Arbetslöshet och minskad tillit gör det lättare att rekrytera till kriminella nätverk.

En globalt pressad ekonomi skapar möjligheter för skuggekonomier

Snabb befolkningstillväxt i vissa regioner och åldrande i andra, tillsammans med minskad social tillit och ökande polarisering, skapar nya sårbarheter som kriminella kan utnyttja.

Effekt

Befolkningen växer snabbt i vissa regioner samtidigt som den åldras i andra. Ungdomsmajoriteter i fattigare länder kan exploateras som arbetskraft i scam-centers, medan äldre befolkningar blir särskilt utsatta målgrupper. Parallellt ökar sociala klyftor och förtroendet för institutioner minskar.

Konsekvens

Organiserad cyberbrottslighet får tillgång till både arbetskraft och nya målgrupper. Svagare rättsstater saknar resurser för effektiv motståndskraft, vilket gör dem till attraktiva baser för datakarteller. Polarisering och minskat förtroende för myndigheter kan dessutom utnyttjas av kriminella genom desinformation och manipulation.

Trender där data skapar nya kriminella möjligheter

Exponentiell tillväxt av data där automatisering och kvantdatorer skapar nya möjligheter

Data blir avgörande när naturresurser och samhällsfunktioner digitaliseras.

En fragmentisering av internet där den globala säkerheten kan undermineras

Arbetslöshet och minskad tillit gör det lättare att rekrytera till kriminella nätverk.

En globalt pressad ekonomi skapar möjligheter för skuggekonomier

Energiomställning, digitalisering, växande ojämlikhet och försvagade institutioner omformar spelplanen. När ekonomier pressas och styrningen brister blir utrymmet större för skuggekonomier och datadriven kriminalitet.

Effekt

Digitalisering och övergången till förnybar energi driver fram en omställning av ekonomier. Samtidigt skapar beroendet av kritiska mineraler och nya leverantörskedjor nya sårbarheter. Ojämlikhet mellan vinnare och förlorare i omställningen riskerar att förstärkas.

Konsekvens

När ekonomier pressas och styrningen är svag får skuggekonomier större utrymme. Kriminella nätverk använder data för att knyta ihop skattebrott, penningtvätt och cyberangrepp. Kryptotjänster och informella finanssystem blir arenor där illegala datadrivna flöden kan döljas och tvättas.

Ett nytt ekosystem av digital exploatering

Gråzonerna där dataexploatering växer fram

I en värld där data blivit en central resurs växer också gråzoner fram som är svåra att överblicka, ett slags digitalt ingenmansland. Här rör sig aktörer som balanserar mellan innovation och exploatering. Det handlar inte bara om teknik, utan om beteenden som närmar sig brott utan att alltid definieras som det. Insamling av information sker ofta utan insyn och data från både individer och företag fångas upp utan att användarna förstår hur den kommer till användning.

AI och agenter agerar inkräktare i dessa gråzoner

Artificiell intelligens och autonoma agenter fungerar här som svårupptäckta inkräktare. De tolkar och manipulerar data i en takt som få hinner överblicka. Systemens komplexitet gör det svårt att avgöra om något är ett fel, ett intrång eller ett medvetet utnyttjande av en svaghet, vilket gör ansvarsfördelningen oklar. Många av dessa handlingar hamnar i gråzoner där det är svårt att dra en tydlig gräns mellan legitima funktioner och oönskade ingrepp.

Data är ett vapen som kan manipulera marknader, demokratier och bryta ned tillit

Konsekvenserna kan bli omfattande. Data är inte längre bara en resurs utan ett medel för påverkan och kontroll, kapabelt att manipulera marknader, påverka demokratiska processer och försvaga samhällens tillit. Varje digitalt avtryck skapar möjligheter att exploatera både människor och organisationer. I detta landskap blir det allt svårare att skilja mellan legitima tjänster och beteenden som i praktiken liknar digital eller ekonomisk brottslighet.
Det finns en stor risk att individer gradvis tappar kontrollen över sin egen data, samtidigt som makten förskjuts till aktörer som kan utnyttja denna växande och delvis osynliga dataekonomi.

Dataindustrin behöver sina säkerhetsbälten och rondeller

Vi befinner oss i en snabb teknologisk förändring som skapar nya möjligheter men också ökar risken att utnyttjas. Frågan är inte om data kommer att missbrukas, utan hur vi skyddar oss när verktygen som ska ge insyn och kontroll själva blir en del av gråzonen. Vi behöver nya former av vaksamhet, reglering och etiskt ansvar, ett slags säkerhetsbälten och rondeller för en dataindustri som rör sig allt snabbare. Om vi inte agerar finns en risk att vi gradvis förlorar både integritet och kontroll i takt med att teknologin utvecklas. Utan tydliga skyddsräcken riskerar denna miljö att bli en grogrund för digitala angrepp och en ekonomi där exploatering normaliseras. Följande avsnitt beskriver möjliga utvecklingsriktningar som växer fram ur dagens tendenser.

Data som råvara

Marknadsekonomin skapar

Data industrialiseras och paketeras som en handelsvara. I takt med att den förädlas skapas nya marknader, ibland transparenta, ibland i gråzoner. När ett fåtal aktörer kontrollerar dessa flöden bildas datakarteller, där tillgången till information blir ett maktmedel.

Brottsekonomin utnyttjar

När data får en allt större betydelse i både den legala och illegala ekonomin kan en parallell infrastruktur börja ta form. I en framväxande kriminella dataekonomi flyter cyberbrott, ekonomisk manipulation och industriellt spionage samman. AIoT-system och uppkopplade miljöer gör det möjligt att övervaka och exploatera i nära realtid vilket kan driva utvecklingen mot en mer avancerad digital brottsekonomi.

AI-ekonomin förstärker

AI är inte längre bara ett verktyg utan en aktör i sig – en agentisk kraft som agerar, tolkar och manipulerar data. Språkmodeller blir katalysatorer som både möjliggör förståelse och förstärker sårbarheter. De agerar bro mellan dataflöden och beslutsfattande, men också som förstärkare av både kreativitet och kontroll.

Drivkrafter bakom framtidens datamarknad

Det som driver framtidens datamarknad är en kombination av teknisk utveckling, nya affärsmodeller och kampen om kontrollen över människors data.

Data som grund för nästa marknadsekonomi

Framtidens datamarknad växer fram i ett ekosystem där data inte bara är en handelsvara utan också ett verktyg för påverkan, kontroll och ekonomisk dominans. När datainsamling och analys byggs in i hem, arbetsliv och hälsa uppstår en marknad där företag, organisationer och institutioner får ett stort informationsövertag gentemot individer. Det förändrar maktbalanser och skapar nya beroenden i samhället.

Det framväxande data-ekosystemet

Nya branscher och tjänster bygger på kontinuerliga flöden av data som samlas in i bakgrunden av vardagens interaktioner. Detta skapar värdekedjor där företagens konkurrensfördelar avgörs av vilka datamängder de kan samla in, kombinera och analysera. Marknadens logik flyttas därmed från produkter och tjänster till kontroll över informationsflöden.

Konsumenten som osynlig resurs

De flesta människor vet att data samlas in, men få förstår omfattningen eller konsekvenserna. I praktiken blir människor ofrivilliga resursleverantörer i en ekonomi där deras beteenden, rörelsemönster och hälsodata används för att forma tjänster, påverka val och förutsäga framtida beslut. Informationsobalansen mellan aktörer och individer är därmed en strukturell del av marknadens funktionssätt.

Data som konkurrensmedel

Hyperpersonlig data används för att skräddarsy erbjudanden, styra konsumtionsmönster och optimera prissättning. Försäkringsbolag, arbetsgivare och vårdgivare förlitar sig i allt högre grad på beteende- och profileringstekniker när de fattar beslut. Data blir därmed en central del av marknadens värdeskapande och en allt viktigare faktor i strategisk positionering.

Den sekundära datamarknaden

Bakom de synliga tjänsterna växer en omfattande sekundär marknad fram där data cirkulerar mellan analysföretag, leverantörer, tredjepartstjänster och data brokers. Denna infrastruktur är osynlig för användaren men avgörande för hur marknaden utvecklas. Den skapar både nya affärsmodeller och nya beroenden som kan vara svåra att genomskåda.

Kampen om äganderätten

Vem som får äga, kontrollera och använda data blir en avgörande fråga för framtidens ekonomi. Den som har kontroll över data påverkar även innovationstakten, konkurrensen och möjligheten att forma samhällsutvecklingen. Ägandefrågan är därför en central konfliktpunkt där kommersiella intressen, samhällsnytta och individers integritet möts.

Dataparadoxen

Samhället blir allt mer beroende av data för att skapa effektiva tjänster, robusta system och snabbare beslutsprocesser. Samtidigt växer sårbarheterna och beroendena i takt med att dataflödena ökar. Att balansera nytta, transparens och risk blir en av de centrala utmaningarna i framtidens marknadsekonomi.

Techaktörernas roll i gråzonen där data exploateras på kreativa sätt

Den subtila gråzonen i datahanteringen

I den framväxande datamarknaden har en subtil men avgörande gråzon vuxit fram, där techaktörer använder data på sätt som ligger mellan legitim användning och tveksam datainsamling, svåra både att upptäcka och att reglera. Genom att utnyttja de mellanrum som uppstår när tekniken utvecklas snabbare än juridiken kan företag samla in stora mängder information i en gråzon utan att bryta mot lagen. Det handlar mindre om klassisk kriminalitet och mer om systematiskt och ibland automatiserat utnyttjande av otydliga regelverk och begränsad insyn.

Självgående datainsamling och strategisk exploatering

Större techbolag fungerar i praktiken som autonoma ekosystem där datainsamlingen blivit självgående. Maskininlärningsmodeller och algoritmer driver en ständigt växande insamling av användar- och företagsdata, ofta utan att någon fullt ut kan överblicka hur informationen används. Gränssnitt, API:er och integrationsplattformar skapar dataflöden som rör sig osynligt mellan aktörer och länder, där ägarskap, syfte och ansvar ofta är otydliga.

Det juridiskt tillåtna blir i praktiken ett verktyg för strategisk exploatering. Genom att tolka användarvillkor brett eller hänvisa till automatiserade processer kan företag bygga affärsmodeller på data som användare aldrig uttryckligen godkänt att dela. Här uppstår en paradox: ju mer automatiserad tekniken blir, desto mer otydlig blir ansvarsfördelningen.

Tillsammans skapar dessa processer en miljö där datainsamlingens logik och exploateringens incitament förstärker varandra, ofta utan att ansvar eller avsikt är tydligt definierade.

Data som reproducerbar och gränslös resurs

Data har blivit en av världens mest värdefulla digitala handelsvaror, en råvara som överträffar många traditionella resurser i strategiskt värde. Till skillnad från fysiska tillgångar är den reproducerbar, rörlig och svår att skydda. Den kan kopieras, analyseras och säljas vidare utan att originalet försvinner, vilket skapar möjligheter till ekonomiska vinster i en gråzon utan att formellt bryta mot några lagar. Det mest problematiska är att många av dessa processer sker under en yta av teknisk legitimitet. Metadata, beteendedata och träningsdata kan indirekt avslöja identiteter, affärsstrategier eller konkurrensinformation, ofta inom ramarna för tillåtna tekniska anrop, det vill säga automatiska förfrågningar mellan system, eller som en del av avtal mellan aktörer. I denna miljö blir frågan mindre vad som är tillåtet och mer vad som är etiskt försvarbart.

Plattformsföretag formar vår digitala verklighetsbild

Gråzonens dynamik gör att makt och ansvar successivt förskjuts från juridiska institutioner till tekniska infrastrukturer. Företag som kontrollerar plattformar, molntjänster och datadistribution fungerar som nya maktcentra med möjlighet att påverka marknader, styra algoritmiska beslut och forma vår verklighetsbild.

Risken för en digital feodalism

Detta skapar tydliga asymmetrier. Mindre aktörer blir beroende av dataflöden de inte kan överblicka eller kontrollera, användare reduceras till datapunkter i större system och samhällen blir mer sårbara för selektiv informationsstyrning. I en utveckling som går snabbare än regleringen finns en risk att vi gradvis närmar oss en form av digital feodalism, där tillgången till data snarare än kapital avgör vilka aktörer som får inflytande.

Mot en mer transparent och ansvarsfull datahantering

Framtidens dilemma handlar inte bara om lagstiftning, utan om värdegrund och tillit. När datainsamling sker osynligt och är svår att överblicka ökar behovet av att aktörer som driver plattformar och digital infrastruktur tydligt reflekterar över vilka data som samlas in, varför och med vilka konsekvenser. I den diskussionen betonas också vikten av aktörer med tydliga samhällsambitioner och, i en europeisk kontext, behovet av egna tekniska alternativ för att stärka självständighet, skydda demokratiska värden och minska sårbarheter.

Data har blivit den kriminella ekonomins primära valuta

En växande global exponering av data

Sedan början av 2000-talet har tiotals miljarder användarkonton och datapunkter exponerats i dataintrång världen över. Flera oberoende sammanställningar visar att utvecklingen fortsätter uppåt, både i omfattning och detaljnivå i den data som läcker. Europol beskriver i sin senaste hotbedömning hur data har blivit den kriminella ekonomins primära valuta. Skillnaden mot traditionella resurser är avgörande: guld, olja och pengar förbrukas när de används, men data kan kopieras och säljas vidare utan att förlora sitt värde.

Data som valuta, vapen och maktmedel

Ett dataset med inloggningsuppgifter, kundinformation eller hälsodata kan omsättas i flera led och kombineras med annan information för att skapa nya värden. Det gör data till något mer än en resurs, den fungerar som handelsvara, vapen och maktmedel. Som handelsvara cirkulerar den i återkommande cykler på mörka marknader. Som vapen används den i utpressning, manipulation och digital påverkansverksamhet. Som maktmedel ger den övertag, både för kriminella nätverk och statliga aktörer som utnyttjar digitala sårbarheter för underrättelseändamål.

Förädlingen som driver fram datakarteller

Värdet uppstår genom förädling. Intrång, massläckor och kompromettеringar genererar stora mängder rådata som säljs vidare till mellanhänder som paketerar och omsätter den stulna informationen. Initial access brokers säljer i sin tur åtkomst till hackade nätverk, vilket öppnar för nya datastölder. Denna marknadslogik sammanfattas som **steal, deal and repeat: d**ata stjäls, paketeras och säljs, och samma material exploateras gång på gång i identitetsbedrägerier, ekonomisk brottslighet och avancerade cyberangrepp.

Distributionskanaler som dark markets, Telegram och krypterade handelstjänster gör handeln anonym och skalbar. Europol konstaterar att handeln med data följer samma ekonomiska logik som andra illegala marknader, som narkotika eller vapen, men med en avgörande skillnad: den kan växa snabbare, spridas globalt och bedrivas utan fysisk närvaro eller territoriell kontroll.

Förädling, insamling, paketering och global distribution är vad som omvandlar data från teknisk artefakt till en handlingsbar handelsvara. Det är i detta led datakartellerna bygger sina affärsmodeller.

Fakta: Data som råvara och handelsvara

- Miljarder dataposter stjäls årligen.
- Över hälften av dessa uppgifter säljs eller återanvänds i flera led på mörka marknader.
- Data är den enda råvara som kan säljas **hur många gånger som helst utan att förbrukas**.
- Europol beskriver data som den **primära valutan i den kriminella ekonomin**.
- Handeln med data följer samma logik som andra illegala marknader – men är **global, skalbar och fysisk obunden**.
- Data fungerar som **handelsvara, vapen och maktmedel**, vilket gör den till grunden för framtidens brottsekonomi.

Källor: IBM Cost of a Data Breach Report (2024), Europol SOCTA 2025 och Europol IOCTA 2024

Från IT-intrång till industriproduktion av kriminella scaleups

Små aktörer kan producera brott i stor skala

Den digitala brottsligheten har på kort tid rört sig från isolerade angrepp till en industrialiserad verksamhet. Genom tillgång till stora datamängder, global infrastruktur och en växande marknad för brottsverktyg kan även små aktörer producera brott i stor skala. Det som tidigare handlade om enskilda IT-intrång utvecklas nu mot standardiserade processer som liknar industriell produktion.

Scam-centers producerar bedrägerier i stor skala

Scam-centers fungerar som fabriker med specialiserade roller. Operatörer, analytiker och betalningskoordinatorer arbetar i skift, medan regionala kluster bygger kompetens inom teknikstöd, språkanpassning och finansiell logistik. Detta gör brotten rörliga, uthålliga och möjliga att skala snabbt över geografiska gränser.

Varje stulen uppgift kan öka precisionen i framtida angrepp

Data har blivit en central råvara i denna utveckling. Varje stulen uppgift kan användas för att förfina nästa angrepp, öka träffsäkerheten och minska behovet av manuellt arbete. I praktiken innebär detta att brotten blir mer förutsägbara att genomföra men svårare att störa.

Kriminella scaleups

I denna miljö uppstår datadrivna verksamheter som är standardiserade, skalbara och motståndskraftiga. Det gör det svårt att möta utvecklingen med traditionella motåtgärder eftersom strukturerna anpassar sig snabbt.

Organiserade produktionskedjor – datakarteller

När cyberbrott organiseras som produktionskedjor skapas också utrymme för aktörer som försöker kontrollera hela flödet. Här blir begreppet datakartell relevant. Datakarteller är inte alltid formaliserade organisationer, utan ett sätt att beskriva hur nätverk kan konsolidera kontroll över insamling, förädling och handel med data. I takt med att data kan kopieras utan att förbrukas ökar drivkrafterna att etablera egna datamarknader och normer för hur information omsätts.

Framöver kan dessa strukturer utvecklas till något som liknar karteller i traditionell mening – inte genom våld eller territorium, utan genom kontroll över informationsflöden, tekniska gränssnitt och betrodda plattformar. Resultatet är en brottsindustri där data är såväl råvara, valuta och grund för inflytande.

Kriminella datakarteller – morgondagens mäktig maktspelare

Data en maktfaktor som förstärks av AI

Datans resa genom kriminalitetens värdekedja visar en tydlig riktning. Från att ha varit en råvara bland andra, har data blivit en handelsvara på mörka marknader, ett vapen för utpressning och manipulation, en infrastruktur som driver hela brottsnätverk, och en maktfaktor som förstärks exponentiellt av artificiell intelligens.

I denna utveckling har brottsekonomin industrialiserats, globaliserats och smält samman med ekonomisk brottslighet och korruption. Nästa steg är en konsolidering där kontrollen över data, plattformar och AI-system koncentreras till ett fåtal dominerande aktörer.

En ny maktlogik där data, inte narkotika, står i centrum

Historiskt har narkotikakarteller, vapensmugglare och maffia kontrollerat illegala marknader genom våld, territorium och kapital. I framtiden kan samma typ av makt samlas hos aktörer som kontrollerar informationsflöden och de algoritmer som bearbetar dem.

Datakarteller kan ha potential att utöva motsvarande dominans som gårdagens narkotikakarteller, men med högre skalbarhet, lägre risk och större genomslag i digitaliserade samhällen. När tillgång till data kombineras med AI som kan analysera, profilera och påverka, blir kontrollen över informationsflöden en form av strategisk makt.

Vad står på spel?

För säkerhetspolitiken: Gränsen mellan kriminalitet och geopolitik suddas ut när stater och kriminella nätverk använder samma resurser - data och AI - för övervakning, manipulation och angrepp. Informationsflöden blir en ny arena för inflytande.

För näringslivet: Företag står inför en dubbel risk. Att förlora sin data och samtidigt omedvetet bli en del av kriminella kedjor om de inte skyddar sina digitala flöden. Transparens, dataskydd och kontroll över underleverantörer blir centrala säkerhetsfrågor.

För samhälle och individer: När data används som angreppsverktyg riktas hot inte bara mot organisationer utan också direkt mot människor. Hyperpersonlig information kan i vissa fall användas för att pressa, påverka eller vilseleda enskilda, vilket gör att privat information kan bli en källa till risk och utsatthet för både enskilda och grupper.

Mot nya maktstrukturer

Om dagens tendenser fortsätter kan framtidens datakarteller utvecklas till mer självförstärkande system. De kan få inflytande över datakällor, spridning av AI-verktyg och delar av marknaden där både stulen och legitim information cirkulerar. Aktörer som lyckas behålla kontrollen över dessa flöden får ett övertag som kan bli närmast monopolistiskt inom den kriminella ekonomin.

Det väcker frågor om hur en sådan utveckling kan påverka stater och internationella relationer. Data riskerar då att inte bara bli en resurs, utan en central komponent i hur vissa kriminella strukturer bygger sin kapacitet. När informationsflöden, kapitalflöden och tekniska plattformar börjar hänga ihop på nya sätt kan det skapa långsiktiga effekter som sträcker sig bortom det digitala.

Datakarteller kan i framtiden bli mäktiga maktspelare med enormt inflytande. Frågan är inte längre *om* data används i brottslighet, utan *hur långt* dess betydelse som maktfaktor kan komma att sträcka sig, och vad det innebär för våra försvarsmekanismer på nationell och global nivå.

Tre nationer som påverkar utvecklingen av framtidens cyberbrottslighet

Globala krafter bakom den digitala brottsekonomin

Tre av världens mest inflytelserika nationer, USA, Kina och Ryssland, spelar en central roll i den utveckling som påverkar den globala cyberbrottsligheten. I öppna digitala marknader, i statligt styrda ekosystem och i slutna kriminella miljöer där förtroende mellan aktörer fungerar som valuta, suddas gränsen ut mellan teknik, makt och missbruk av data. Tillsammans visar dessa tre nationer hur cybermiljöer kan bli system som påverkar säkerhet, ekonomi och samhällen långt utanför deras egna gränser.

Det öppna ekosystemet där data blir valuta

Den amerikanska cybermiljön kännetecknas av öppenhet, hög innovationshastighet och en decentraliserad brottsekonomi. På forum och marknadsplatser cirkulerar hackingverktyg, stulna identiteter och data som handelsvaror. Aktörer agerar som entreprenörer inom ransomware, phishing och social manipulation, där utpressning och hot om dataläckor blivit centrala metoder.

Under 2024 och 2025 har städer, sjukhus, skolor och företag slagits ut av attacker som kombinerar automatisering och manuella hot. AI används för deepfakes, avancerad phishing och manipulation av digitala arbetsmiljöer. Distansarbete och komplexa leverantörskedjor har samtidigt skapat fler sårbara ytor för intrång i både offentlig och privat sektor.

Den statligt styrda modellen där data är strategi

Den kinesiska cybermiljön kopplas ofta till statens bredare strategiska mål. Statliga, halvstatliga och privata aktörer rör sig i ett gemensamt ekosystem där målet kan vara att få tillgång till teknologi, affärsinformation och forskning. Skärpta regler om dataskydd, incidentrapportering och AI-användning har samtidigt stärkt den nationella kontrollen och påverkar hur cybersäkerhetsarbetet utvecklas.

Cyberspionage lyfts ofta fram som en central metod, särskilt inom teknikintensiva sektorer. Cyberverksamhet får också en roll i geopolitiska frågor och i hanteringen av diaspora- och dissidentmiljöer. Kryptovalutor används i vissa fall för att dölja finansiella flöden kopplade till digitala brott, samtidigt som staten försöker begränsa sådana möjligheter genom allt striktare reglering. AI utvecklas både för angrepp och försvar, bland annat genom mer avancerade social manipulation och olika former av skydd med AI-stöd.

Det slutna nätverket där rykte är makt

Den ryskspråkiga cybermiljön präglas av teknisk skicklighet, disciplin och interna normer där rykte fungerar som valuta. Forumen är ofta hierarkiska och inbjudningsbaserade, till skillnad från många engelskspråkiga miljöer. I sådana strukturer tros ransomware diskuteras mer sällan i öppnare delar, vilket minskar insynen och gör utvecklingen svårare att följa.

Gränserna mellan kommersiella aktörer och grupper med statligt stöd kan dessutom vara otydliga, vilket skapar utrymme för avancerade angrepp att växa.

Data som biometriska uppgifter och företagsinformation har blivit centrala mål eftersom de möjliggör identitetsbedrägerier och utpressning. Nätfiske har utvecklats till leverantörskedjor där verktyg, manualer och tjänster cirkulerar mellan aktörer. Ransomware fortsätter att utvecklas genom läckt källkod och etablerade access-tjänster. Kriget mot Ukraina har även bidragit till en närmare koppling mellan statliga och kriminella angrepp, bland annat genom hybridattacker och desinformation.

Tre miljöer, ett gemensamt mönster

Trots sina olikheter driver dessa tre miljöer samma utveckling: data som maktmedel. I öppna marknader blir identiteter handelsvaror. I statligt styrda system används information för att stärka nationell konkurrenskraft. I slutna nätverk är data grunden för teknisk dominans och interna hierarkier. Tillsammans formar de ett digitalt maktspel där innovation, reglering och brottslighet vävs samman och där data är den centrala resursen.

Förgiftning av data och LLM grooming

Manipulerade data och nya angreppsytor

Stora språkmodeller LLM:er tränas på mycket stora mängder text för att kunna förstå och generera språk. De används i allt från söktjänster till kundsupport och är beroende av kvaliteten på den data de exponeras för.

När AI-modeller blir mer självlärande uppstår nya angreppsytor. Kriminella aktörer använder redan tekniker som data poisoning, där felaktig eller manipulerad information förs in i träningsdata. Det kan skapa sårbarheter och minska tillförlitligheten i tjänster inom exempelvis bank, handel och sjukvård.

Ett närliggande fenomen är så kallad LLM grooming där aktörer försöker forma modellernas förståelse av världen genom att påverka den information modellerna tränas eller matas med.

- **Data poisoning** är när någon förgiftar träningsdata med skadligt eller felaktigt innehåll.
- **LLM grooming** är när någon försöker styra vad en modell uppfattar som sant genom att påverka informationen runt modellen, till exempel på internet.

Poisoning påverkar modellen inifrån, grooming formar modellens världsbild utifrån.

LLM grooming kan innebära att stora mängder vinklad information publiceras online eller att aktörer försöker styra de digitala miljöer som modeller använder efter lansering. När AI-genererat och syntetiskt innehåll blandas med autentiska data blir det svårare att avgöra vad som är äkta, vilket påverkar hela ekosystem av data och modeller.

AI-driven manipulation och känslomässig påverkan

AI-modeller kan göra digital manipulation mer personlig och skalenlig. Angripare kan skapa långa, anpassade dialoger som bygger förtroende över tid och är svåra för automatiska system att upptäcka. Detta förstärker traditionella metoder av social manipulation och kan få individer att lämna ut känslig information eller agera mot sin vilja.

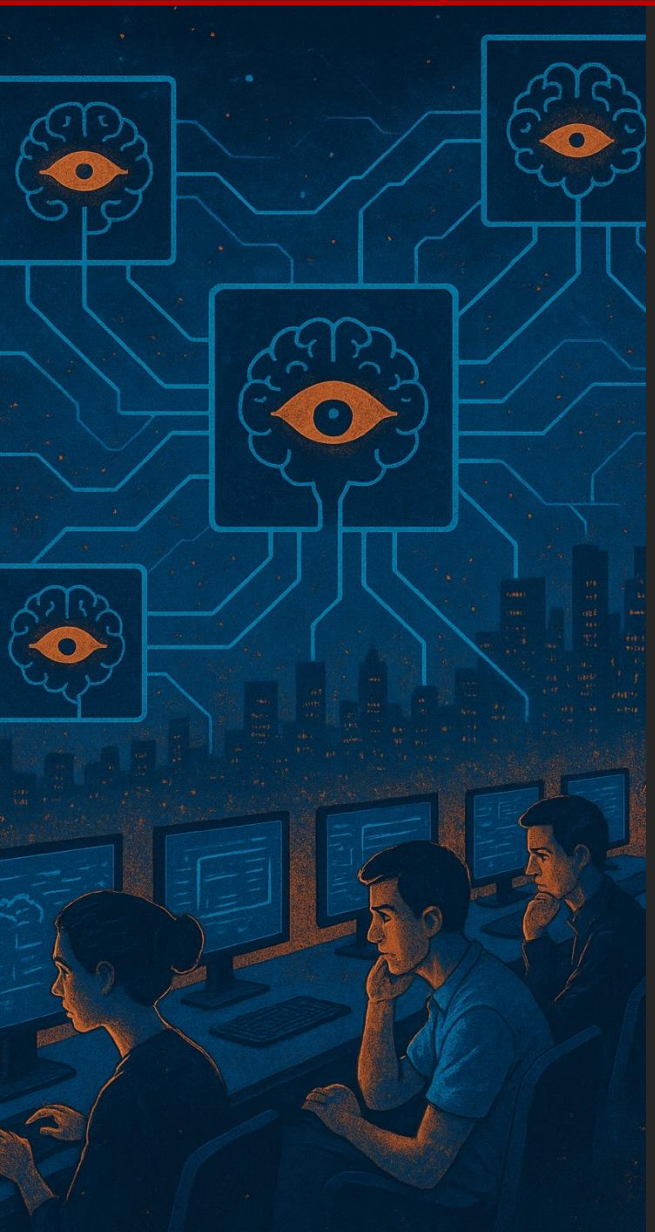
AI-baserade botar kan efterlikna vänskapliga beteenden och anpassa språk och ton efter användarens reaktioner. För barn och unga innebär detta särskilda risker eftersom interaktionerna kan skapa trovärdiga känslomässiga band. Samma tekniker kan även användas i informationspåverkan, där falska narrativ etableras och förstärks över tid.

Sårbarheter i tekniska och rättsliga system

Utvecklingen kräver att rättsvårdande myndigheter, teknikföretag och andra samhällsaktörer stärker sin förmåga att upptäcka och motverka AI-stödd manipulation. Ökad medvetenhet hos både unga och vuxna är en del av skyddet, liksom ansvarsfull och etiskt förankrad användning av AI.

Det finns samtidigt rättsliga utmaningar. Balansen mellan öppna data och integritetsskydd påverkar hur modeller kan tränas och granskas, och skapar ibland gråzoner som kan utnyttjas av kriminella aktörer.

En central framtidsutmaning är att förstå och kunna styra innehållet i AI-modeller. Risken är att AI inte bara speglar världen utan också börjar forma den. När träningsdata påverkas av illvilliga aktörer kan även legitima verksamheter ofrivilligt bli en del av informationskedjor som används för skada.



AI möjliggör självstyrande brottsnätverk

När AI blir motorn i brottsnätverken

När brottsekonomin industrialiseras blir AI den kraft som driver utvecklingen vidare. Där data tidigare krävde manuellt arbete automatiserar nu AI stora delar av kedjan och gör brottsligheten snabbare, mer träffsäker och svårare att bemöta. Språkmodeller och andra AI-verktyg ökar kapaciteten att identifiera, rikta och genomföra angrepp i skala. Det gör att möjligheterna att attackera och exploatera system och människor växer snabbt. Resultatet är ett mer komplext hotlandskap där flera typer av angrepp kan kombineras och skalas upp.

Från analys till exploatering

AI används redan för att effektivisera hela värdekedjan. I insamlingsfasen skrapas och analyseras stora informationsmängder, även från delvis skyddade system. Vid förädling skapar AI detaljerade profiler över individer och organisationer, förutsäger vilka mål som är mest lönsamma och anpassar tillvägagångssätt därefter. I exploateringsfasen används generativa modeller för att producera trovärdiga digitala representationer, syntetiska röster och automatiserade interaktioner som förstärker påverkan och bedrägerier.

Mot självstyrande brottsnätverk

Under de kommande åren kan delar av kedjan bli delvis självgående. I ett tidigt skede handlar det troligen om system som automatiserar återkommande uppgifter medan människor fortsatt övervakar och ingriper vid behov. Mänsklig närvaro förblir viktig för bedömningar, etiska överväganden och komplexa beslut, men rollen skiftar från aktiv utövare till övervakare och beslutsstöd. Samtidigt finns en risk att nätverk som både kontrollerar stora datamängder och påverkar AI-motorernas beteende får betydande marknadsfördelar. Sådana aktörer kan i praktiken få en närmast monopolistisk position i delar av den illegala dataekonomin och betraktas då som framväxande kriminella datakarteller. Denna framställning beskriver en möjlig framtidsutveckling snarare än en etablerad verklighet.

Implikationer och slutsats

AI multiplicerar datans värde och leder till ett exponentiellt större utnyttjande av information. Det innebär ökad hastighet, större precision och ett kraftigt ökat skadans genomslag när angrepp utförs eller effekter sprids. Om kontrollen över både data och AI-kapacitet koncentreras till få aktörer kan dessa få närmast monopolistisk makt och driva maskindrivna datakarteller. Försvaret måste därför kombinera teknisk detektion, snabb incidenthantering och regelverk som adresserar såväl dataflöden som AI-kapacitet.

I nästa avsnitt analyserar vi hur dessa självlärande system förändrar hotbilderna i praktiken och vilka konkreta försvarsstrategier som krävs för att möta en allt mer automatiserad och skalbar kriminalitet.

Från isolerade dataläckor till koordinerade system och infrastruktur

När AI börjar agera på egen hand

När AI blir mer agentisk förändras även sättet som data används. De system som tidigare bara analyserade eller genererade information börjar nu själva samla in, bearbeta och agera på data. Denna utveckling skapar nya brottsliga möjligheter – för den som kontrollerar datan kontrollerar i praktiken hela kedjan av digitala händelser.

När data har förädlats och omsatts i marknader uppstår nästa nivå. Data blir inte längre bara ett medel för brott, utan själva infrastrukturen som kriminaliteten vilar på. Kriminella nätverk bygger sina logistik-, finans- och styrningssystem kring data som en bestående tillgång.

Från isolerade läckor till agentiska system

Det som tidigare var isolerade dataläckor och enstaka intrång har över tid vuxit ihop till permanenta system som driver och koordinerar brott. En enskild läcka kan ge stora mängder rådata, men marknadsaktörer köper, berikar och paketerar informationen så att den blir återanvändbar. Genom dessa steg skapas en slags kran in till kontinuerliga datakällor. Åtkomst köps eller upprätthålls via initial access brokers eller insiders, medan automatiserade skript kontinuerligt extraherar information.

På så sätt blir data både resurs och infrastruktur. Den används för att skapa falska företag och konton, för att automatiskt skala rekrytering till penningtvättsnätverk och för att styra angrepp i realtid. Språkmodeller och andra AI-verktyg förstärker processen genom att kombinera och syntetisera stora datamängder, generera trovärdiga meddelanden och automatisera verifieringssteg. Resultatet är ett system som fungerar mer som en fabrik än som en serie enstaka incidenter.

Vem som helst kan genomföra komplexa bedrägerier

Datatillgångar möjliggör snabb onboarding av nya aktörer i kriminella kedjor och underlättar styrningen av operationer i realtid. De används för att dölja transaktioner, flytta pengar mellan konton och etablera nya kanaler när tidigare stängs ner. Automatiserade arbetsflöden gör att även aktörer med begränsad teknisk kompetens kan leverera komplexa bedrägerier. Detta sänker tröskeln och ökar produktiviteten i den kriminella ekonomin.

När digital och fysisk kriminalitet växer samman

Datainfrastrukturen utgör samtidigt en bro till klassisk organiserad brottslighet. Identitetsuppgifter och KYC-paket används för att öppna konton åt narkotikaringar, för att bygga upp skalföretag i penningtvättskedjor och för att möjliggöra insiderhandel och korruption. Den digitala infrastrukturen gör det enklare att koppla ihop fysiska smugglingstransaktioner med globala finansiella flöden.

Data fungerar därmed som ett produktionsmedel som gör brottsekonomin global, uthållig och svår att slå sönder. Europol och UNODC beskriver hur organiserad brottslighet integrerar digitala komponenter i sina kärnverksamheter och bygger mer motståndskraftiga, modulära system. Försvaret mot denna utveckling kräver att fokus flyttas från enskilda incidenter till att identifiera, störa och skydda de datainfrastrukturer som gör brottsligheten möjlig.

Mot ett konvergerande brottsekosystem

När data blir själva infrastrukturen för brott förändras också relationerna mellan olika brottssfärer. Nästa steg är en allt tydligare konvergens – där cyberbrott, ekonomisk brottslighet och korruption smälter samman till ett gemensamt ekosystem.

Data binder ihop den kriminella ekonomins alla delar

En sammanvävd brottsekonomi växer fram

När data blir den gemensamma infrastrukturen i digitala system förändras också logiken bakom brottslighet. I stället för separata angrepp och isolerade aktörer växer ett mer sammanhängande ekosystem fram där marknad, teknik och kriminalitet delar samma flöden, gränssnitt och logik. Det som tidigare uppfattades som olika världar inom plattformsekonomi, gråzonsbeteenden och avancerad cyberbrottslighet börjar fungera som delar av samma system. Resultatet är en miljö där data inte bara används för att genomföra brott utan även för att organisera och styra dem.

Brottssfärer ser ut att smälta samman

Insikter från både forskning och internationella analyser pekar på att brottssfärer är på väg att flätas samman på nya sätt. Stulna identiteter, komprometterade loggar och manipulerade register används redan idag för att styra, dölja och förstärka olika typer av brott, och mycket tyder på att denna samverkan kommer att fördjupas. Datadrivna angrepp kan framöver förstärka klassiska ekonomiska upplägg ännu mer, och information som stjäls i digitala miljöer kan i ökande grad utnyttjas för att påverka händelser i den fysiska världen.

I denna utveckling fungerar data alltmer som en flexibel komponent som kan användas för att bygga skalbolag, dölja penningflöden, påverka institutionella processer och genomföra bedrägerier som anpassas efter både lokala och internationella sammanhang. Tendenserna visar att data håller på att bli navet som binder samman flera brottsområden och skapar en mer komplex och sammanhängande brottsekonomi.

Brott, marknad och teknik vävs samman

Den logik som präglar digitala plattformar spiller också över i brottsmiljöerna. Flöden av metadata, verifieringsuppgifter och åtkomstinformation används lika lätt för att optimera reklam som för att styra organiserade upplägg. Detta skapar en allt tätare sammanflätning där brottslighetens struktur börjar likna hur globala digitala marknader fungerar.

När AI-system analyserar, sorterar och kombinerar stora datamängder förstärks denna utveckling ytterligare. Informationsflöden, kapitalflöden och tekniska system börjar förutsätta varandra, och brottsligheten organiseras med samma logik som digitala tjänster och plattformar.

Nya datadrivna ekosystem

I takt med att data används för intrång, skalning och styrning kan brottsmiljöer som är mer modulära och motståndskraftiga än tidigare växa fram. Identitetspaket, åtkomsttjänster och verifieringsdokument fungerar som standardiserade komponenter i kriminellas verktygslådor och kan kombineras på många olika sätt i olika upplägg.

Flera internationella analyser beskriver hur denna konvergens gör det svårare att skilja cyberangrepp från traditionell kriminalitet. De pekar också på hur organiserade nätverk integrerar digitala komponenter i sina kärnverksamheter, vilket förändrar både skala och verkan i brottsligheten.

Mot en sammanvävd brottsekonomi

När marknadsaktörer, kriminella nätverk och AI-system rör sig i samma digitala miljöer uppstår en strukturell sammansmältning. De tekniska system som är grunden för legitima tjänster kan även utnyttjas i upplägg som syftar till att underminera dem. Data fungerar då som ett nav som håller ihop brottslighetens olika delar. Det innebär att brott inte längre är isolerade företeelser utan delar av en större struktur där informationsflöden, kapitalflöden och tekniska gränssnitt agerar tillsammans. Detta formar en brottsekonomi som är global, uthållig och allt svårare att bryta upp.

Intervjuer

” Det är våra datalager som blir de nya attackytorna”, *Mats Hultgren*.

När data blir brottets kärna

Sedan data blev mer värdefullt än olja har den blivit världens mest eftertraktade resurs. Och när allt sker digitalt är det oundvikligt att också brottsligheten gör det. Hultgren konstaterar hur stulen data nu snabbt omsätts i nya syften. En läckt databas kan säljas, användas för bedrägerier, utpressning eller överlämnas till en annan stat. Han förklarar att riktade bedrägerier fortfarande dominerar, men att AI nu gör det möjligt att kartlägga och exploatera information i en helt ny skala. Små aktörer får samma möjligheter som stora, och avancerad brottslighet kräver inte längre avancerade resurser.

När vi skyddar fel saker

Hultgren framhåller att Sverige ofta skyddar det man själv värderar högst snarare än det angripare vill åt. Banker säkrar pengar men angripare kan vara ute efter kunddatabaser, energibolag skyddar ritningar men förbiser upphandlingsunderlag. Vi ser verksamheten inifrån och ut när vi borde se den utifrån och in. Han menar att det perspektivet gör oss sårbara, eftersom hotaktörer ser värde där vi inte gör det. Därför blir insikten om vad som verkligen är skyddsvärt en del av själva motståndskraften.

Nya antagonister

Hultgren beskriver hur antagonisterna har blivit fler och mer kompetenta. Kina syns mer, Ryssland förfinar sina tekniker och trycket från rättsväsendet splittrar de kriminella miljöerna. Han konstaterar att det idag är svårt att avgöra om en attack kommer från en ensam person, en mindre grupp eller ett nätverk.

Unga med cybervapen

Ett exempel Hultgren lyfter är Scatter Spider, ett västerländskt nätverk av minderåriga som ser ut att agerar som ett syndikat men utan fasta strukturer. De tycks samarbeta kortsiktigt, byta identiteter och försvinna. Det är inte heller långsökt att tro att drivkraften är en blandning av spänning, status och pengar, och att unga kan orsaka lika stor skada som professionella hackare, ofta utan att förstå eller bry sig om följderna.

Förr var rollerna tydligare: tonåringarna som busade, de härdade cyberkriminella och de statliga aktörerna. Nu menar Hultgren att gränserna har suddats ut. Unga deltar i attacker som en del av sitt digitala sociala liv, ibland utan att inse att de begår brott. I länder med låg risk att åka fast har cyberbrott blivit ett sätt att dryga ut inkomsten. Han varnar för att det som börjar som lek snabbt kan bli en väg in i organiserad kriminalitet.

AI som brottsplats

Cyberlandskapet förändras snabbt. Hultgren beskriver hur tillfälliga nätverk uppstår, samarbetar och försvinner, samtidigt som stater och kriminella använder samma verktyg för olika syften. Han ser också att det finns trender som pekar mot att big game hunting mot stora företag kan vara på väg tillbaka, med det dubbla syftet att både tjäna pengar men också försvaga väst.

Men där tidigare angrepp handlat om att stjäla eller låsa data kan nästa fas handla om att manipulera den. Hultgren menar att AI framöver kan bli själva brottsplatsen. Genom att förgifta dataset eller påverka algoritmer kan angripare styra hur en AI värderar information. Om en modell lär sig fel kan det få direkt skadliga effekter. I dag övervakas enheter, identiteter, nätverk och molntjänster men sällan själva datalagret, något Hultgren ser som en blind fläck där manipulation kan ske utan synliga spår.

Den delade digitala framtiden

Hultgren konstaterar att det digitala landskapet splittras både tekniskt och värderingsmässigt. Öst och väst går skilda vägar i synen på makt, teknik och religion. I väst regleras AI, i öst drivs utvecklingen vidare utan begränsningar, något Hultgren menar får geopolitiska, militära och ekonomiska följder.

Han menar att unga växer upp i denna miljö och formar dess normer, vilket påverkar framtidens brottslighet. Den digitala tvillingen av vår värld består men blir allt mer fragmenterad, med öppna och stängda nätverk och lokala system.

Behovet av att kommunicera är existentiellt. Varje ny teknik för att nå varandra har gjort världen större, inte mindre. Hultgren avslutar med att vi nu står mitt i stormens öga, mellan tonåringar och kriminella med cybervapen och stater som vill forma framtiden efter sitt tycke.

Mats Hultgren är Director of Cyber Risk på Truesec och en framstående expert inom cybersäkerhet. Han fokuserar på att förebygga och hantera cyberhot mot kritisk infrastruktur och företag. Med djup kunskap inom cyberrisk och incidenthantering stödjer han organisationer i att stärka sin säkerhet och motståndskraft mot digitala attacker.

”Min analys är att språkmodellerna kommer att leda till är att vi kommer drunkna i skräp”, Stefan Axelsson.

När tekniken förändrar brott och beteende

Ny teknik förändrar forensikens möjligheter, konstaterar Axelsson. Metoder som ansiktsigenkänning och automatisk sökning av fingeravtryck vid mängdbrott har haft stor betydelse för polisens arbete. Samtidigt är utmaningen med brottsuppklarning i praktiken ofta inte teknisk, utan organisatorisk. Hur resurserna fördelas inom polisen och vilka brott som prioriteras påverkar i hög grad resultatet, inte minst när det gäller cyberbrott som drabbar allmänheten.

De stora språkmodellerna fångar nu många forskares uppmärksamhet, säger Axelsson. Fokus ligger på att se när de fungerar, hur tillförlitliga de är och vilka felmarginaler de har. Modellerna kan vara mycket träffsäkra inom vissa områden, som att sammanfatta texter, men betydligt sämre inom andra. Det krävs både insikt och erfarenhet för att förstå skillnaden, menar han.

Kriminalitet i bredd och djup

Kriminaliteten breddas genom möjligheten att kringgå språkmodellerna, och göra så kallade jailbreaks, där användare lurar modellerna att bryta mot sina egna säkerhetsregler. Axelsson beskriver hur illvilliga aktörer kan använda språkmodeller för kunskap och stöd i brottsliga syften. ”Språkmodellerna pratar först och tänker sen”, säger han. Det är där manipulationen sker. Genom att styra inputen går det att få modellen att leverera det som efterfrågas.

Tekniken sänker tröskeln och fler kan bygga egna verktyg och kunskapen sprids snabbt. Resultatet blir fler aktörer, fler försök och fler sätt att utnyttja systemen. Och i slutänden, påpekar Axelsson, handlar säkerheten om en enda fråga: hur mycket jävelskap kan en människa ställa till med? Med utvecklad teknik har den risken ökat.

En skräpflod av information

En av de största risker, menar Axelsson, är inte hotet om superintelligent AI utan att samhället drunknar i skräp. Det som tidigare var dyrt att sprida, som brev, har ersatts av mejl och kostar idag inget, vilket lett till en explosion av skräppost och bedrägerier. Resultatet är ett ständigt brus av vilseledande innehåll som är svårt att värja sig mot. Människor vänjer sig vid kort och känslomässig information, ofta utan krav på att den ska vara sann.

Axelsson ser den här utvecklingen som en av de mest påtagliga konsekvensernas av AI:s tillgänglighet, dvs att mängden meningslös och manipulerad information riskerar att försvaga tilliten i samhället.

Syntetiska data och organiserad brottslighet

Syntetiska data har blivit allt vanligare och öppnar för en säkrare och mer transparent AI-utveckling. Den gör det möjligt att testa och utvärdera metoder i kontrollerade miljöer, förbättra representativitet och skydda människors integritet.

Men den är fortfarande kostsam och tekniskt krävande, även om utvecklingen går snabbt. De stora bolagen lyfter gärna fram möjligheterna – inte minst när tillgången till etikgodkända data minskar. Att märka upp verkliga data kräver fortfarande människor, ofta i monotont arbete. Därför används syntetiska data alltmer för att träna algoritmer – men risken finns: *garbage in, gospel out*.

Axelsson varnar för att låg datakvalitet kan få långtgående följder.

Internet fylls av mer innehåll, en del brottsligt. Samtidigt växer en organiserad kriminalitet fram som utnyttjar data, med resurser, rekrytering och teknisk kompetens. Fler kan göra mer snabbare, och gränsen mellan legitim och kriminell verksamhet suddas ut.

Det nya normala

Axelsson menar att nästa steg kan bli en ny syn på data. Att vi gradvis accepterar att information om oss finns tillgänglig och lever vidare med vetskapen om att mycket redan är synligt.

Tekniken förändrar inte bara hur brott begås, utan också hur vi uppfattar risk. Det finns ingen punkt där vi är skyddade, bara ett ständigt dragspel mellan medel och motmedel. För varje innovation uppstår nya sårbarheter, och nya försök att täppa till dem.

Det framtida säkerhetsarbetet handlar inte om att bygga murar, utan om att förstå rörelsen mellan ordning och kaos, det mänskliga och det maskinella. I den rörelsen formas nästa kapitel av både brott och samhälle.

Stefan Axelsson är professor vid Stockholms universitet och expert inom digital forensik och cybersäkerhet. Han har särskild kompetens inom utredning av digitala brott, digitala bevis och hur dessa kan analyseras och tolkas. Hans forskning och arbete fokuserar på att utveckla metoder för effektiv och rättssäker hantering av digitala spår vid cyberbrottsutredningar.

” Det pågår ett tyst övertagande av kultur och ekonomi”, *Magnus Sahlgren*.

Den digitala maktkoncentrationen
Utvecklingen av AI går snabbt och frågorna om vem som styr den blir allt fler. Om utvecklingen fortsätter i samma takt, säger Sahlgren, står vi inför en maktkoncentration där ett fåtal aktörer formar framtidens AI-modeller. De kommer att användas överallt, i samhällskritiska funktioner, i skolan och i vardagen, och påverka vårt sätt att tänka, prata och förstå världen. Det vi ser är, enligt Sahlgren, ett allt starkare oligopol växa fram i den digitala världen. Våra skolbarn börjar prata som chattarna i språkmodellerna. Ett tyst övertagande av kultur och ekonomi pågår. Samtidigt kan modellerna lösa stora frågor om sjukdomar och samhällsproblem. Men de slukar enorm energi, och frågan är om vi hinner lösa allt innan resurserna tar slut.

Den nordiska dataparadoxen
Sverige och Norden står inför en egen utmaning. Vi har några av världens starkaste dataskyddsregler och en lång tradition av öppenhet med personnummer, folkbokföring och offentliga data. Det ger värdefulla datatillgångar, men de är svåra att använda. Sahlgren konstaterar att Sverige har högkvalitativa data, men att otydliga regleringar försvårar användningen.

Det här leder till att länder med striktare tolkning hamnar efter aktörer som inte gör samma bedömning.

På EU -nivå finns försök att balansera innovation och skydd, men enligt Sahlgren saknas fortfarande kapital och handlingskraft jämfört med USA och Kina. Europa riskerar därför, trots sin kompetens och datatillgångar, att hamna i beroende av andras teknik.

Dataskydd eller datasuveränitet

När teknikutvecklingen styrs av andra växer en ny sorts sårbarhet fram. Obalansen mellan reglering och handlingskraft påverkar inte bara vår innovationsförmåga utan även vår nationella digitala suveränitet.

Reglerna som ska skydda medborgarna kan samtidigt göra oss beroende av utländska modeller som inte speglar våra värderingar. När dessa modeller börjar påverka språk, kultur och beslut i vardagen uppstår ett yttre kulturellt inflytande.

Sahlgren varnar för att detta kan bli en form av digital kulturimperialism, där vi gradvis förlorar kontrollen över de system som formar vår verklighetsbild.

LLM Grooming och agentiska risker

LLM Grooming innebär att påverka språkmodeller genom att mata nätet med innehåll som formar deras världsbild. En risk som sällan diskuteras men som växer snabbt. Samtidigt utvecklas agentiska system där agenter själva utför uppgifter. Om agenterna inte är säkrade kan till exempel hela databaser hamna hos okända aktörer. Sahlgren ser risk för manipulation och datastöld, där felaktig information kan få eget liv och spridas vidare utan kontroll.

Den digitala framtiden: en balansgång

Sahlgren menar att det är viktigt att hitta en balans mellan olika aspekter, såsom datatillgång, upphovsrätt, transparens, kultur och representation, nationell digital suveränitet och värdeskapande från generativ AI.

Sverige behöver använda sin egen data ansvarsfullt och utifrån våra värderingar, annars riskerar vi att förlora både kontroll och inflytande över den digitala framtiden.

Magnus Sahlgren är forskningschef för Natural Language Understanding (NLU) vid AI Sweden, där han leder utvecklingen av avancerade språkmodeller för de nordiska språken. Med en doktorsexamen i beräkningslingvistik fokuserar han på AI, språkteknologi och hur stora språkmodeller kan tillämpas inom olika samhällsområden. Hans expertis omfattar naturlig språkförståelse, maskininlärning och generativa språkmodeller.

”Europa behöver bygga fler egna system och tjänster för att behålla kontrollen över data”, *Carl Heath*.

Samma data, olika syften: pengar, makt och kontroll

Heath menar att kriminella använder den data som går att tjäna pengar på, som personuppgifter, kundregister, kreditkortsuppgifter och intern information som kan säljas vidare eller användas för bedrägerier och utpressning. Men han påpekar också att det inte bara är kriminella som missbrukar data. Kommersiella aktörer kan använda information för syften som individen aldrig gett sitt medgivande till, vilket skapar mer subtila intrång i privatlivet.

Skillnaden ligger, enligt Heath, i syftet. Kriminella vill begå brott, medan kommersiella aktörer använder data för att tjäna pengar på individers beteenden.

Trygghet, övervakning och rätten till ett privat liv

Heath anser att behovet av brottsbekämpning ofta ställs mot individens rätt till privatliv, men påminner om att privatlivet är en grundläggande mänsklig rättighet. Varje inskränkning måste ske med försiktighet och respekt för integriteten.

Han menar att vi under de senaste åren har vant oss vid en högre grad av övervakning, men att det inte nödvändigtvis leder till ökad trygghet. Vi behöver, säger Heath, skilja mellan trygghet och säkerhet, två mål som kräver olika typer av åtgärder.

Ett tydligt exempel på målkonflikten är krypterade appar. Heath påpekar att alla har rätt till säker kommunikation, men samma teknik används också för grov brottslighet. Förslagen om att skapa bakdörrar i krypterade appar som Signal riskerar därför att försvaga skyddet för alla, samtidigt som kriminella enkelt flyttar sin kommunikation till andra plattformar.

Reglering i otakt och data som maktmedel

Heath lyfter fram att EU:s regelverk haft stor betydelse för datasäkerheten, men att lagstiftningen skapades innan vi fullt ut förstod datans roll i AI-utvecklingen. I dag uppstår målkonflikter när tekniken utvecklas snabbare än juridiken.

Han beskriver hur data har fått en ny betydelse, inte bara som personinformation utan som råvara för innovation, påverkan och makt. När data hamnar i händerna på cyberkriminella eller auktoritära stater kan konsekvenserna bli allvarliga. Kriminella använder data för utpressning och bedrägerier, medan stater kan utnyttja den för att kartlägga individer, identifiera svagheter eller påverka samhällen i geopolitiska syften.

Enligt Heath blir kopplingen mellan organiserad brottslighet och statliga intressen allt svårare att urskilja, och datans gränslösa natur gör att skadorna snabbt kan bli globala.

Mellan öppenhet och sårbarhet, vägen framåt för Europa

Heath menar att transparens och spårbarhet i dataflöden är centrala för ett öppet och rättssäkert samhälle. Men i tider av krig och ökade antagonistiska hot kan samma öppenhet bli en sårbarhet. Information som stärker insyn i fredstid kan i kris utnyttjas av främmande makt.

Han lyfter fram att Europa behöver bygga fler egna system och tjänster för att behålla kontrollen över data. Initiativ som European Health Data Spaces och Bolognaprocessen visar vägen. Att kunna kombinera data inom hälsa, utbildning och kompetens är, enligt Heath, avgörande för att säkra samhällets funktion i fred, kris och krig.

För att förebygga datamissbruk krävs också samarbete mellan skola, myndigheter och forskning. Grundförutsättningen är kunskap. Heath betonar att utan förståelse för teknikutvecklingen, särskilt inom AI, riskerar samhället att bli sårbart utan att ens märka det.

Kunskap om tekniken och hur den påverkar oss är därför, menar Heath, samhällets viktigaste försvarslinje.

Carl Heath *är senior forskare och fokusledare för digital resiliens vid RISE, Sveriges forskningsinstitut. Han är också forskare vid Göteborgs universitet och del av Swedish Center for Digital Innovation. Heath har varit särskild utredare för regeringen med fokus på demokratins utmaningar i en digital tid och biträder Myndigheten för Psykologiskt Försvar inom forskning och utbildning. Hans expertområden inkluderar digital resiliens, samhällsviktig digital transformation och innovation.*

Analys: Data är en strategisk maktfråga – och Europa är i underläge

Analys av insikterna från expertintervjuer

Detta är vår analys av de insikter som framkom i intervjuerna med Stefan Axelsson, Magnus Sahlgren, Mats Hultgren och Carl Heath. När samhället digitaliseras blir data både valuta, vapen och värdegrund. I deras resonemang framträder en gemensam insikt: framtidens brottslighet uppstår inte i periferin av digitaliseringen utan är en produkt av den. Vår slutsats är att frågan inte längre handlar om tekniken i sig utan om makt, ansvar och Europas förmåga att hävda digital suveränitet i en värld där andra mäktiga nationers teknologier sätter villkoren.

Teknikens dubbla natur – trygghet, övervakning och manipulation

Alla fyra expertintervjuer pekar på teknikens dubbla natur. Artificiell intelligens kan i princip användas lika mycket för att lösa brott som för att begå dem. En språkmodell som tränats för att analysera text kan lika lätt användas för att skapa deepfakes, generera falska identiteter eller automatisera bedrägerier.

Samtidigt har AI blivit ett av våra viktigaste verktyg för att förebygga och utreda brott. Denna dubbelhet visar att teknikens effekter inte beror på tekniken i sig utan på hur och av vem den används. Samma tekniska möjligheter som stärker brottsbekämpningen, sänker också tröskeln till kriminalitet genom att ge kraftfulla verktyg till personer som saknar den tekniska kompetensen. Som en slags demokratisering av brottsligheten där avancerad teknik sprids till amatörer.

Men samma teknik som stärker möjligheterna att bekämpa brott kan också driva fram ett samhälle där övervakningen ökar. I våra expertsamtal förstår vi det som att detta leder till frågan om vad det innebär för samhället när kampen mot digital kriminalitet skapar mer övervakning och mer kontroll, samtidigt som trygghet efterfrågas. Kontrollens ökade närvaro i kameror, appar och digitala spår riskerar på sikt att normaliseras och urholka tilliten. Diskursen om krypterade appar som Signal visar hur säkerhetsintressen kan komma i konflikt med rätten till privatliv. När myndigheter kräver bakdörrar till kryptering, försvagas samtidigt skyddet för alla medborgare. Dagens digitala trygghet är därför inte bara en teknisk fråga, utan i högsta grad också en etisk fråga.

Det etiska dilemmat hänger också ihop med en större fråga. Den digitala tekniken formar inte bara relationen mellan individ och stat. Den påverkar också Europas möjligheter att hävda kontroll över sin egen digitala utveckling. Den digitala maktbalansen handlar inte bara om innovation och konkurrenskraft, utan också om säkerhetspolitik och internationella konflikter.

Data som maktfråga – Europas strategiska underläge

Samtidigt visar våra samtal att tekniken inte bara formar individens trygghet och frihet utan också Europas möjligheter att kontrollera sin digitala utveckling. En av de mest avgörande frågorna i intervjuerna är vem som äger, tränar och kontrollerar de modeller som formar framtidens digitala värld. I den bredare debatten finns röster som menar att Europa håller på att förlora kontrollen över sin egen digitala infrastruktur, det som kallas AI Tech Stack, alltså den infrastruktur av data, modeller och plattformar som möjliggör avancerad AI. Idag dominerar aktörer i USA och Kina de molnplattformar, språkmodeller och algoritmer som styr global databehandling. Europa har i praktiken blivit beroende av andras teknik för att bygga sina egna AI-tillämpningar. Konsekvensen är att EU:s regleringar, som GDPR och AI Act, försöker kontrollera system vi själva inte äger. Våra lagar reglerar inte europeisk teknik. De försöker tämja amerikanska och kinesiska plattformar. Det innebär att vi inte vet exakt vilken data som använts, hur den tränats eller med vilka algoritmer besluten fattas.

En allvarlig paradox uppstår i de fall t ex amerikanska och kinesiska språkmodeller tränas på data som hämtats från europeiska och till och med svenska källor, data som vi själva inte får använda. Svenskt näringsliv och offentlig sektor riskerar då att behöva köpa språkmodeller som bygger på vår egen information, men utvecklade i andra länder med andra värderingar, juridik och syften. Sverige har både kompetensen och forskningen för att bygga egna modeller, men regelverken behöver anpassas så att svensk data kan användas på ett sätt som gynnar våra egna samhällsbehov.

Vi behöver ha rätten att förstå och styra den intelligens som formar våra samhällen

Denna paradox är inte bara ekonomisk, utan säkerhetspolitisk. Utan teknisk suveränitet kan vi inte kontrollera våra egna risker. Modeller tränade utanför Europa kan innehålla bias, sårbarheter eller bakdörrar som gör dem potentiellt farliga i allt från rättsväsende till försvarssystem. AI-utvecklingen handlar i grunden om självbestämmande, om rätten att förstå och styra den intelligens som formar våra samhällen. Utan kontroll över vår digitala infrastruktur riskerar vi på sikt att förlora både vår integritet, vår trygghet och vårt demokratiska handlingsutrymme.

Cyberkrig och brottslighet som maktmedel

I våra expertsamtal lyfts det geopolitiska perspektivet fram och beskrivs hur cyberbrott, organiserad kriminalitet och statlig maktutövning allt mer flyter samman. I dag används data som ett maktmedel i en global konfliktzon där stater, företag och ideologiska grupper attackerar varandras system, ofta med hjälp av samma verktyg.

I analysen framträder hur ransomware, sabotage av kritisk infrastruktur och digitalt spionage blivit centrala inslag i modern geopolitik. Kriminella nätverk fungerar som underleverantörer åt statsaktörer, och cyberbrottslighet blir ett sätt att testa motståndares beredskap. Denna utveckling skapar ett nytt säkerhetspolitiskt landskap där digitala angrepp kan få samma strategiska betydelse som militära.

Modulär brottslighet kräver nya motstrategier

Ett intressant perspektiv i samtalen är hur brottsligheten kan sägas ha blivit modulär, det vill säga organiserad i tillfälliga konstellationer som formas kring en specifik attack och sedan byter identitet. Traditionell brottsbekämpning räcker inte alltid till, och därför behöver myndigheter och internationella aktörer hitta nya sätt att samarbeta och upptäcka hot i tid.

Gemensamma lärdomar – fyra perspektiv på samma risk

Samtliga experters perspektiv visar att data och AI inte längre kan förstås enbart som tekniska fenomen. De är samhällsstrukturer som formar makt, rättvisa och trygghet.

- Ett perspektiv i samtalen visar hur tekniken förändrar brottets natur genom att göra avancerad kriminalitet tillgänglig för fler.
- Ett annat varnar för att kampen mot kriminalitet riskerar att urholka demokratin om övervakning normaliseras.
- Ett tredje pekar på att Europa saknar teknologisk suveränitet och därmed verklig kontroll över sin egen data.
- Ett fjärde synliggör hur cyberangrepp blivit en del av den globala maktbalansen.

Vår tolkning av deras gemensamma slutsats är tydlig: den digitala brottsligheten speglar samhällets egen sårbarhet. Den uppstår där teknik, makt och okunskap möts.

Några riktningar som präglar diskussionen om Europas och Sveriges digitala trygghet

I samtalen och den bredare diskussionen om digital trygghet återkommer tre centrala riktningar. De bygger på argument som lyfts i både analyser och intervjuer, även om synsätten varierar kring hur de bör genomföras.

1. Europa behöver en egen AI Tech Stack

Många lyfter behovet av att Europa stärker sin digitala infrastruktur för att minska beroendet av andra länders teknologier. När centrala system ägs av externa aktörer uppstår tekniska och demokratiska sårbarheter som påverkar vår trygghet. Därför framhålls vikten av att bygga och förvalta egna tekniska resurser för att värna säkerhet och självbestämmande.

2. Datadriven innovation är nödvändig för Europas säkerhet

För att stå emot kriminalitet och påverkan behöver Europa utveckla egna digitala lösningar, vilket kräver innovation baserad på data. I dag ligger fokus främst på att skydda data, vilket är viktigt för integriteten, men skyddet räcker inte för att bygga den teknik som stärker motståndskraften. Därför betonas behovet av att kunna använda och dela data säkert samt att investera i forskning, öppen data och gemensam infrastruktur.

3. Kunskap och etik stärker samhällets motståndskraft

Teknik skapar inte trygghet om människor inte förstår eller litar på hur den används. Digital kompetens och tydliga etiska riktlinjer är därför avgörande för att motverka manipulation och övervakning. Kunskap är inte bara ett sätt att förstå tekniken utan också ett av samhällets främsta försvar.

Framtidsscenarier

Scenarierna bygger på återkommande teman i internationell analys om cybersäkerhet och geopolitik och är inspirerade av material från EU, Europol, OECD, ENISA, NATO samt intervjuer och artiklar vi tagit del i analysarbetet.

Fragmenterat kontrollscenario: Splinternet och statliga datakarteller

Industriellt kriminellt scenario: Datakarteller som multinationella företag

Motverkningsscenario: Globala koalitioner och resilient infrastruktur

Scenario 1: Fragmenterat kontrollscenario: Splinternet och statliga datakarteller

När data blir ett maktmedel mellan stater. Om hur kampen om digital infrastruktur skapar statligt kopplade datakarteller.

I takt med att data blir en strategisk resurs hårdnar den geopolitiska konkurrensen om vem som kontrollerar digital infrastruktur, flöden och tekniska plattformar. Redan fragmenterade dataekosystem splittras ytterligare när stater bygger digitala murar, begränsar externa tjänster eller använder data som påverkansverktyg.

I gränslandet mellan stat och kriminalitet växer nya maktstrukturer fram där statligt kopplade datakarteller verkar i det dolda men påverkar världen i det öppna.

Analys: Vägen mot statligt kopplade datakarteller

Flera utvecklingslinjer pekar mot en framtid där data inte bara är en resurs utan ett medel för inflytande. När stater försöker säkra kontroll över digitala flöden blir data en fråga om nationell suveränitet. Detta gäller särskilt där staten dominerar tekniksektorn eller där gränserna mellan stat och marknad är svaga.

Parallellt suddas gränsen mot kriminalitet ut. Precis som i dagens digitala gråzoner använder vissa stater hackergrupper för underrättelsearbete, påverkansoperationer och cyberangrepp. Cybermiljön blir en plats där kriminell kompetens flätas samman med statliga intressen, ofta i utbyte mot skydd, koordinering eller ekonomiska fördelar.

Data blir en handelsvara i sig, inte bara en del av en tjänst. Outsourcade offentliga system, kommersiella plattformar och nationella datalager skapar nya ekosystem där ägande, kontroll och transparens är svåra att överblicka. Bristen på internationella regelverk öppnar för halvstatliga nätverk som hanterar, säljer och skyddar data med statligt stöd eller med tyst godkännande.

Om trenderna fortsätter kan 2050 års datakarteller bli något helt annat än dagens nätverk, med statligt sanktionerade maktstrukturer, globala verktyg, nationella lojaliteter och en effektivitet som uppstår när legala, gråa och illegala ekonomier flyter ihop.

Scenario

Runt mitten av seklet har kampen om data blivit ett politiskt maktspel. Vissa stater kontrollerar den digitala infrastrukturen där data flödar, exempelvis moln, kablar, operativsystem och kommunikationsplattformar, medan andra säljer eller privatiserar delar av sin infrastruktur till externa aktörer för ekonomisk eller politisk vinning.

I denna miljö växer statligt kopplade datakarteller fram. De agerar i skärnings-punkten mellan lagligt och olagligt, skyddade av politiska lojaliteter och nationella strategier. Kartellerna hanterar data som handelsvara, informationsvapen och maktresurs, och fungerar som en förlängning av statens inflytande i en fragmenterad digital värld.

Konsekvens

Den digitala världen splittras i block. Globala regler blir svåra att enas om, och informationshandel störs när länder inför egna krav, filter och tekniska barriärer. Civila dataflöden drabbas när stater prioriterar kontroll framför öppenhet. Det globala internet ersätts av parallella nät med egna normer, olika tekniska standarder och olika grader av insyn.

Scenario 2: Industriellt kriminellt scenario: Datakarteller som multinationella företag

När brott blir industri. Om hur datakarteller växer fram som globala företag med AI och automation som motor.

Digitala brott har länge varit fragmenterade, men när AI, automatisering och global specialisering möts uppstår något nytt. Kriminaliteten blir industriell. Aktörerna organiseras, effektiviseras och agerar som företag med skalbarhet, kundtänk och interna värdekedjor. Resultatet är datakarteller som kan konkurrera med legitima aktörer i både resurser och räckvidd.

Analys: Växande digitala ekosystem av kriminalitet

Utvecklingen mot mer uppkopplade och datadrivna samhällen öppnar för nya sätt att organisera brott. Kriminella aktörer specialiserar sig i allt större utsträckning. Vissa hanterar åtkomst, andra identitetsdata. Några genomför intrång och andra sköter den automatiserade insamlingen eller försäljningen. Tillsammans bildar de en global värdekedja av tjänster som fungerar som en kriminell spegelbild av den digitala marknadsekonomin.

Samtidigt gör AI det möjligt att automatisera stora delar av verksamheterna. Intrång, datainsamling och betalningsflöden kan skötas med minimal mänsklig inblandning, vilket gör det enkelt att växa snabbt och svårt att avgöra vem som egentligen ligger bakom. Kombinationen av teknik, kapital och nätverksstruktur gör att framtidens datakarteller kan fungera som globala företag med affärsmodeller, varumärken och specialiserade operativa enheter.

Om denna utveckling fortsätter kan 2050 års kriminella aktörer vara lika organiserade och skalbara som dagens multinationella teknikföretag. Skillnaden är syftet som är ekonomisk vinning utan lagar, ansvar eller insyn.

Scenario

Mot 2050 har datakarteller blivit en etablerad del av den digitala ekonomin. De fungerar som globala företag, med specialiserade enheter och outsourcade tjänster. En aktör säljer åtkomst till sårbara nätverk, en annan tillhandahåller förfalskade verifieringar och digitala identiteter, medan en tredje driver helt automatiserade system för insamling, utpressning och informationsutvinning.

AI gör verksamheterna extremt skalbara. Medan traditionella företag måste hantera lagstiftning, ansvar och insyn, kan kriminella datakarteller agera snabbt, diskret och gränsöverskridande. De bygger egna ekosystem där brott är en produkt och information är råvaran.

Konsekvens

De kriminella nätverken blir för stora och snabbrörliga för att bekämpas nationellt. Effektiva motåtgärder kräver internationell samordning, finansiell spårbarhet och ett tätare samarbete mellan tekniksektorn, finanssystemet och rättsväsendet.

Scenario 3: Motverkningsscenario: Globala koalitioner och resilient infrastruktur

När världen sluter sig samman. Om hur internationella standarder och gemensamt ansvar gör brottsligheten mindre skalbar.

Efter årtionden av växande digital kriminalitet växer insikten om att ingen aktör kan stå ensam. Fragmenterade ekosystem, statligt sanktionerade datakarteller och industrialiserad brottslighet har pressat fram en motreaktion. Nya samarbeten formas mellan stater, företag och teknikplattformar för att bygga robusta system som står emot både attacker, manipulation och exploatering.

I denna framtid är säkerhet inte längre ett tillägg utan den är en del av infrastrukturen.

Analys: Växande samarbete och standardisering

Efter flera decennier av ökande cyberbrott och fragmenterade dataflöden börjar världen agera samordnat. Drivkraften är inte bara att stoppa attacker, utan att åtgärda de systemfel som gjort kriminaliteten skalbar: otydliga ansvarskedjor, låga tekniska krav och svaga incitament för säkerhet.

Security-by-design blir norm. Skydd byggs in i hårdvara, mjukvara och nätverk redan från början. Företag hålls ansvariga för sina leverantörskedjor och måste visa var data kommer ifrån, hur AI-modeller tränats och hur beslut fattas.

Internationella standarder för dataskydd och AI-transparens blir ett nytt grundlager i den digitala infrastrukturen. Globala samarbeten riktas mot brottens ekonomiska kärna, inte bara attackerna, utan även betalningsflödena. Automatiserad finansiell övervakning gör att stora datakarteller får svårt att gömma sig i gränsöverskridande system.

Brottsligheten upphör inte, men dess industriella organisering försvagas. Nätverken blir mindre, mer opportunistiska och mindre skadliga för samhällskritiska system.

Scenario

Vid mitten av seklet har flera länder enats om gemensamma krav på transparens, ansvar och säkerhet. Företag som hanterar stora datamängder behöver kunna redovisa hur deras modeller fungerar, vilka data som används och vilka risker systemen innebär.

Samtidigt har globala koalitioner skapat robusta leverantörskedjor och tydliga ansvarsstrukturer. Datakarteller kan inte längre verka öppet eftersom deras betalningskanaler blir synliga, deras infrastruktur kartläggs och automatiserade övervakningssystem gör intrångskedjor både dyrare och mer riskfyllda.

Säkerhet har blivit en grundförutsättning för marknadstillträde, inte en konkurrensfördel.

Konsekvens

Brottsligheten förändras snarare än försvinner. De stora, centraliserade nätverken pressas tillbaka, medan mindre och mer rörliga aktörer fortsätter i periferin. Det digitala ekosystemet blir mer robust, men hoten mer spridda och svårfångade.

Den stora skillnaden är att kriminaliteten inte längre är industriell – och därmed inte längre ett systemhot.

Mot en tryggare digital framtid

Vi befinner oss i en tid där data rör sig snabbt och ofta utan tydliga gränser. Tekniken utvecklas snabbt och skapar möjligheter som kan stärka både samhällen och företag. Samtidigt växer en gråzon där användning och insamling av data inte alltid är lätta att förstå. Det är en miljö som många känner igen sig i och som väcker frågor om ansvar och insyn.

I den gråzonen utnyttjar vissa aktörer de luckor som uppstår när tekniken går snabbare än juridiken. Mycket av detta är inte olagligt. Men det sker ofta i skikt där människor och organisationer har svårt att se hur information samlas in och används. Det handlar mindre om klassiska brott och mer om system som utnyttjar otydliga regler, automatiserade processer och brist på transparens.

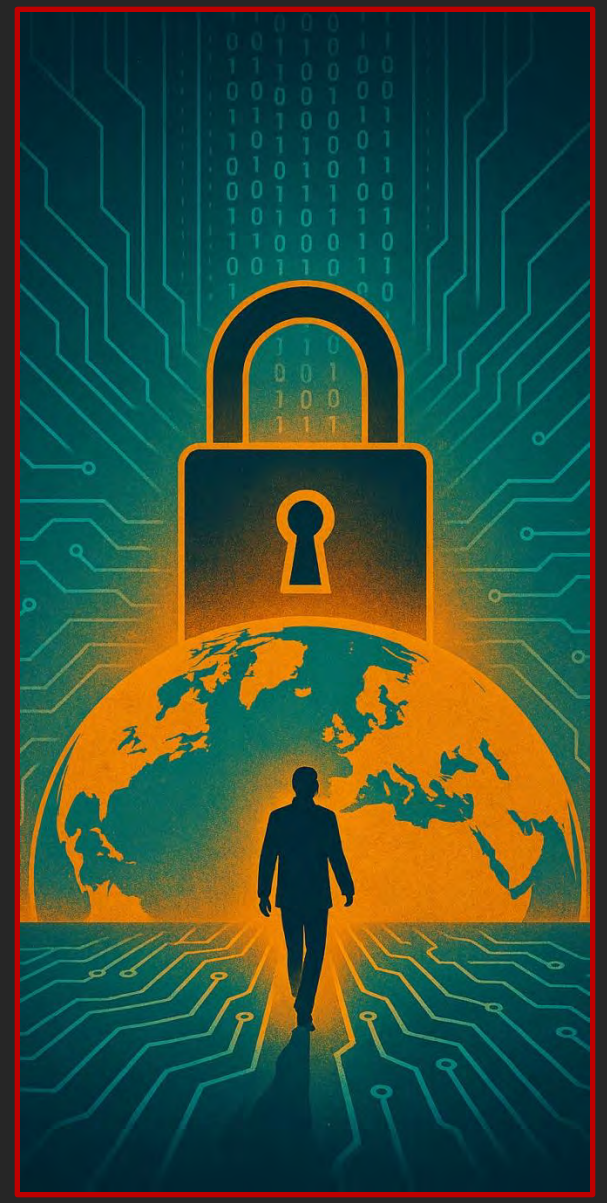
Här blir datainsamlingen ofta självgående. Plattformar och algoritmer drar in stora mängder information om både människor och verksamheter. Det sker i växande nätverk av gränssnitt och integrationer som få har full överblick över. Det som är juridiskt tillåtet kan ändå bli ett verktyg för strategisk exploatering. När processer är automatiserade blir också ansvarsfördelningen otydligare.

Data är i dag en av våra mest värdefulla digitala resurser. Den kan kopieras, delas och användas på många sätt utan att originalet försvinner. Det gör data kraftfull men också svår att skydda. Metadata och träningsdata kan avslöja identiteter, affärsstrategier eller konkurrensinformation. Det kan ske inom ramen för tekniskt tillåtna förfrågningar mellan system eller avtal mellan aktörer. Därför blir frågan mindre vad som är möjligt och mer vad som är etiskt.

När plattformar och molntjänster växer i betydelse flyttas makt från traditionella institutioner till tekniska infrastrukturer. Det skapar en vardag där mindre aktörer får svårare att förstå och påverka flöden som påverkar dem. Det kan leda till tydliga obalanser och ett beroende som gör många mer sårbara.

Ändå finns det skäl till tillförsikt. Det handlar inte bara om reglering. Det handlar också om värdegrund, ansvar och en gemensam vilja att skapa trygga digitala miljöer. I dag ser vi hur fler börjar prata om vilka data som samlas in, varför och med vilka konsekvenser. Vi ser också en växande insikt om att teknisk innovation och samhällsansvar behöver gå hand i hand.

Framtiden är inte förutbestämd. Vi kan påverka den. Genom tydliga val, öppna diskussioner och bättre insyn kan vi skapa digitala system som stärker både förtroende och självständighet. Och vi gör det tillsammans. Med kunskap, nyfikenhet och en vilja att förstå mer kan vi bygga en digital framtid som är både hållbar och trygg.



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

Expertintervjuer:

Stefan Axelsson
Prof. Digital Forensik, Stockholms universitet

Carl Heath
Senior forskare Digital Resilience, RISE

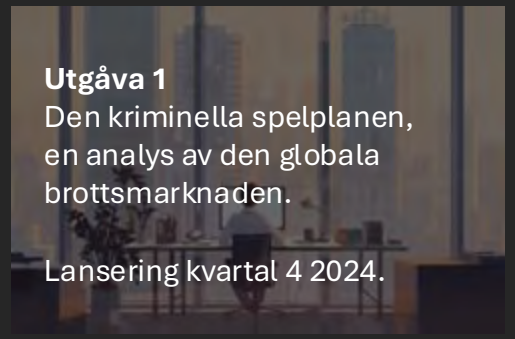
Mats Hultgren
Director Cyber Risk, Trusec

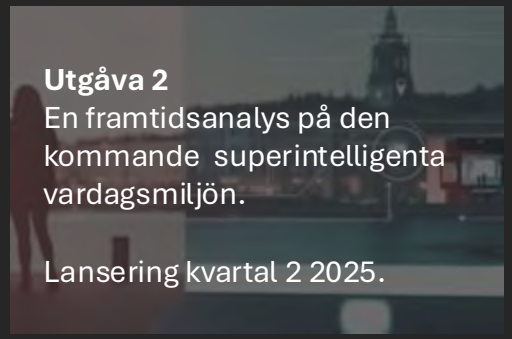
Magnus Sahlgren
Forskningschef NLU, AI Sweden

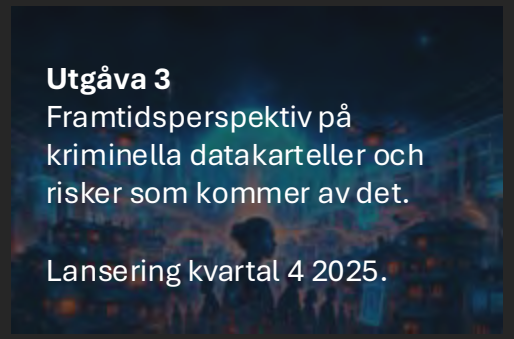
Projektgrupp:

Ulrika Hallesius, ulrika.hallesius@stoldskyddsforeningen.se
Kriminolog på SSF Stöldskyddsföreningen, författare Framtidens Brott

Charlotte Mattfolk
Framtidsanalytiker och expert inom AI-utveckling, vd för IAMAI







Utgåva 4

Urval av källor och vidare läsning

Biometric Update: "Europol IOCTA cybercrime report reveals growing use of AI models and data theft"

Bruce M, Lusthaus J, Kashyap R, Phair N, Varese F. Mapping the global geography of cybercrime with the World Cybercrime Index. PLoS One. 2024 Apr 10;19(4):e0297312. doi: 10.1371/journal.pone.0297312. PMID: 38598553; PMCID: PMC11006133.

Enisa: ENISA Threat Landscape 2025

European Union: NIS 2 directive

Europol: IOCTA (Internet Organised Crime Threat Assessment) 2024

Europol: SOCTA (Serious and Organised Threat Assessment) 2025

FOI: Framtidens Informationsmiljö

IBM: Cost of a data breach report 2024

Industrial Cyber: IOCTA 2024 report: Law enforcement deals major blows against EU cybercrime, disrupt ransomware networks

Interpol: Cybercrime

Lagerqvist, Ronja (2022). *Insamling av privatpersoners data på internet: En studie av privatpersoners medvetenhet om datainsamling – effekten av medvetenhet på engagemang för webbplatser och lojalitet.* Karlstad: Karlstad University.

National Intelligence Council: Global Trends 2040

Nato: Strategic Foresight

Nato: Allied Command Transformation Strategic Foresight Analysis 2023

OECD: Digital Transformation

OECD: AI Principles

Reuters: "Europol warns of AI-driven crime threats"

Stanford University Press: "Data cartells" by Sarah Lamden

The Guardian: Hundreds of English-language websites link to pro-Kremlin propaganda

Trend Micro: The Ever-Evolving Threat of the Russian-Speaking Cybercriminal Underground 2025

Trend Micro: The Trend Micro Underground Series 2025

Trend Micro: Bridging Divides, Transcending Borders, The Current State of the English Underground

Trend Micro: Virtual Kidnapping, How AI Voice Cloning Tools and ChatGPT are Being Used to Aid Cybercrime and Extortion Scams

Trend Micro: Surging Hype An Update on the Rising Abuse of GenAI

UK Ministry of Defence: Global strategic trends out to 2055

University of Oxford: World-first Cybercrime Index maps the global geography of cybercrime

UNODC: World Drug Report 2024

UNODC: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces

UNODC: Inflection Point: Global Implications of Scam Centres

World Economic Forum: Global Risk Report 2025