TRAFICOM
Transport- och kommunikationsverket

Strategisk framsyn

Cybersäkerhetsscenarier 2035

Traficoms teknologi- och strategifunktion

Cybersäkerhetsscenarier 2035

Innehållsförteckning för scenariorapporten

Cybersäkerhetsscenarier 2035 – Bakgrund

- **Cybersäkerhetsscenarierna 2035** stöder arbetet med att bygga upp en förvaltningsövergripande modell för cybersäkerhetens framtids- och framsynsarbete inom cybersäkerhetsstrategin och med att skapa en hotbedömning för cybersäkerheten. Scenarierna byggdes upp mellan hösten 2024 och våren 2026.
- I scenarioarbetets olika faser deltog över 200 experter med olika bakgrund, bland annat från Cybersäkerhetscentret, företag, den akademiska världen, Cybersäkerhetscentrets internationella motsvarigheter, aktörer inom den offentliga förvaltningen och företrädare för det civila samhället.
- Cybersäkerhetsscenarierna 2035 beskriver alternativa verksamhetsmiljöer för cybersäkerheten. De världar som scenarierna beskriver kan fördjupas och vidareutvecklas till exempel genom **granskningar på sektornivå** och användas i **framtidsorienterade övningar**.
- Scenarierna kan utnyttjas vid **planeringen av organisationers beredskap** med hjälp av de **scenarioverktyg** som finns som bilaga till denna rapport.

Scenarierna hanterar osäkerhet

- Olika nyckelhändelser i verksamhetsmiljön leder oss från dagens läge mot **olika framtider**. Vi vet ännu inte hur världen kommer att vara år 2035, men **vi kan försöka förbereda oss genom att gestalta vad som är möjligt.**
- Cybersäkerhetsscenarierna 2035 beskriver **alternativa utvecklingsförlopp för osäkerheterna i vår externa verksamhetsmiljö.** De fungerar som ett systematiskt sätt att gestalta **olika möjliga framtidsscenarier för cybersäkerheten.**
- Scenarierna är **alternativa kontexter för framtidens beslutsfattande. Genom att leva sig in i dem kan man fatta bättre beslut på ett framsynt sätt.** De hjälper oss att förstå förändringar i omvärlden som helhet genom att förutse hur olika fenomen hänger samman och samverkar.
- Scenarierna för 2035 kan idag kännas mer eller mindre möjliga. **Världen år 2035 kommer sannolikt att se ut som en kombination av olika scenarier.**

Så byggdes scenarierna upp

Förändringsfaktorer

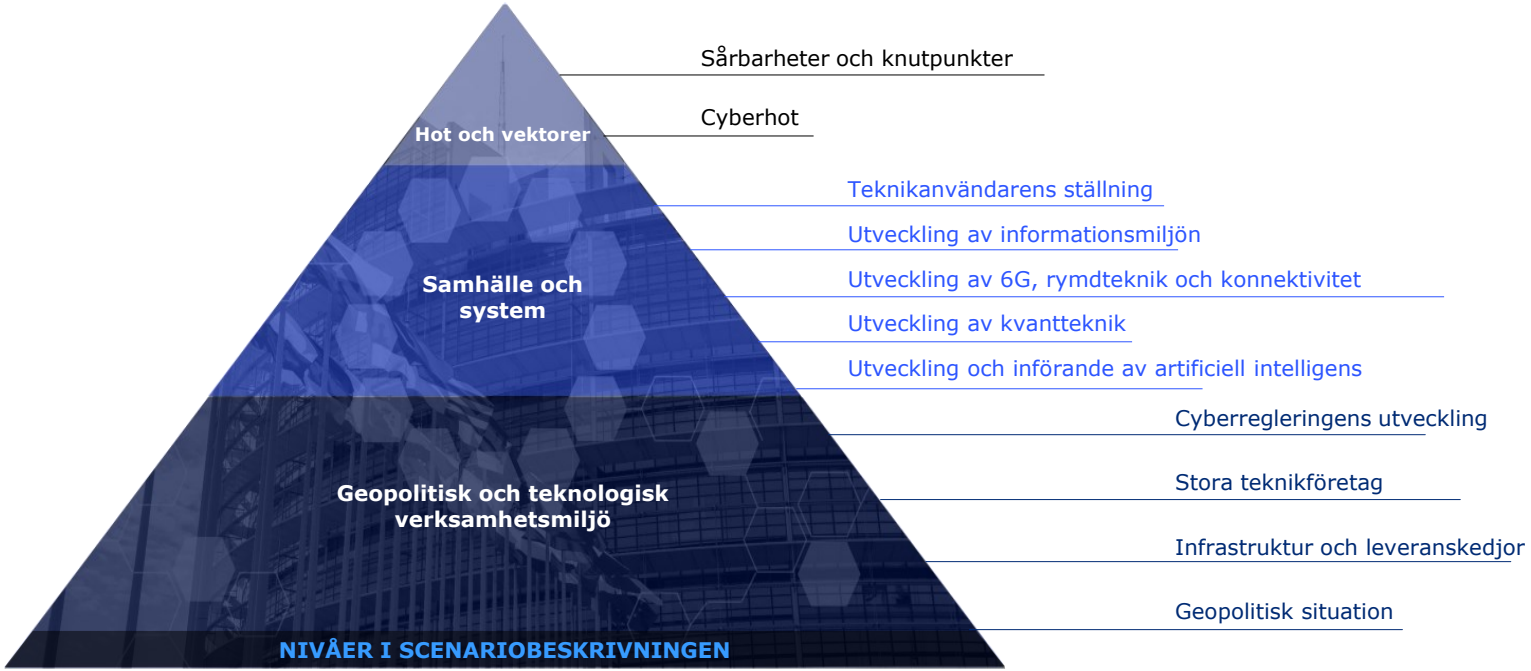
De förändringsfaktorer för cybersäkerheten som kartlades genom enkäter, expertintervjuer och workshoppar kan utvecklas i olika riktningar och i olika takt fram till år 2035.	
Geopolitisk utveckling	AI- och ML-utveckling
Digital infrastruktur	Cyberregleringens framtid
Framtidens cyberhot, inklusive brottslighet	Informationsmiljö och samhälle
Leveranskedjor	Kvantteknik
EU:s enhet och ställning	Teknikjättarnas ställning
Satellit- och rymdteknik	Kompetensutveckling
Organisationers beredskapslösningar	Framtidens sårbarheter och knutpunkter
Tekniska beroenden	Standarder och förtroende
Konsumentbeteende	Desinformation och hybridpåverkan

Framtagning av scenarierna

- I informationsinhämtningsfasen genomfördes sammanlagt fyra workshoppar med intressentgrupperna, två scenarioenkäter riktade till intressentgrupperna samt 18 temaintervjuer med experter.
- I uppbyggnadsfasen för scenarierna genomfördes sammanlagt fyra workshoppar med intressentgrupperna samt fyra fördjupande intervjuer med experter.
- Scenarierna togs fram med framtidstabellmetoden utifrån de åtta mest betydelsefulla förändringsfaktorerna för framtiden och deras utvecklingsalternativ.

Nivåer i scenariobeskrivningarna

Cybersäkerhetsscenarierna 2035 beskriver fyra alternativa och möjliga världar med system som präglas av geopolitisk och teknologisk förändring samt cyberhot och sårbarheter som kan växa fram i framtidens världar.

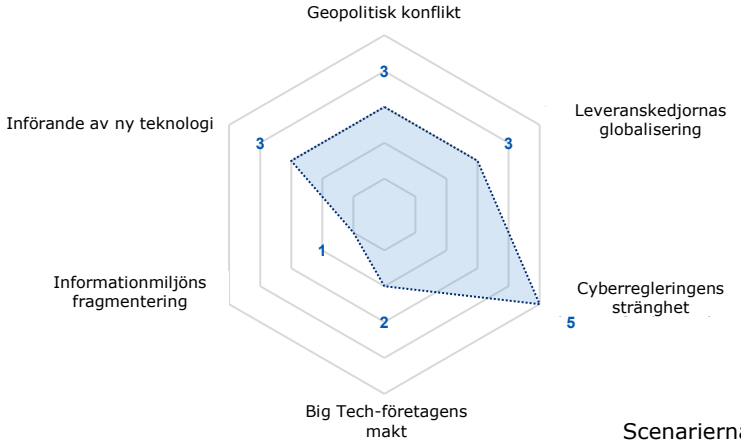



Cybersäkerhetsscenarier 2035

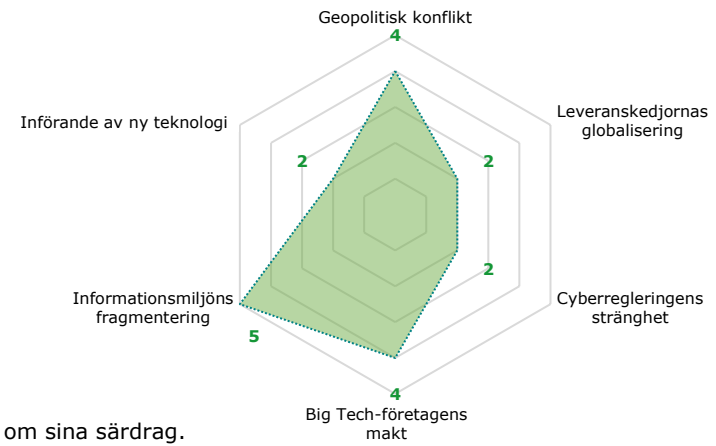
Scenariobeskrivningar


TRAFICOM

/FACKELBÄRAREN/

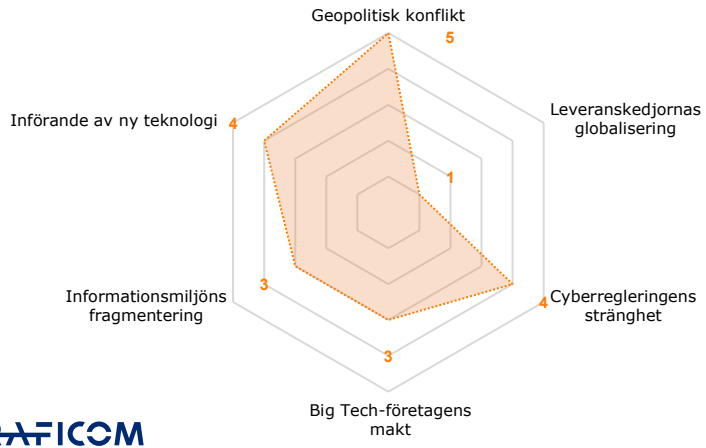


/FRAGMENTERING/

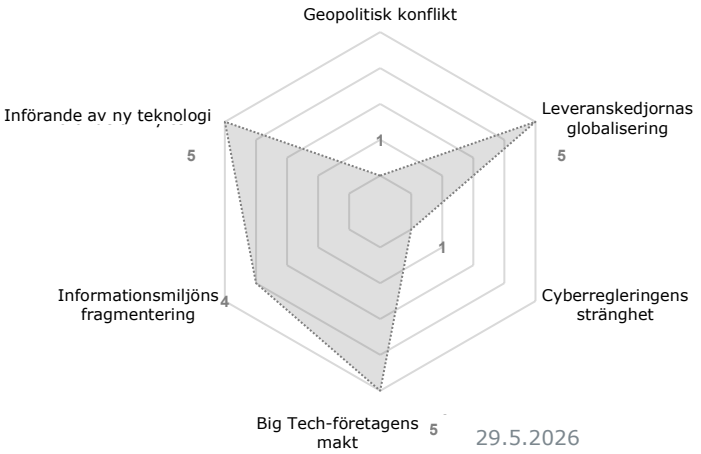


Scenarierna skiljer sig åt i fråga om sina särdrag.
Därför fungerar de bäst som verktyg för att undersöka nya cybersäkerhetsfenomen.

/TVÅ MAKTSFÄRER/



/DATAIMPERIER/



TRAFICOM

/FACKELBÄRAREN 2035/

Motsättningarna mellan stormakternas intressesfärer består.

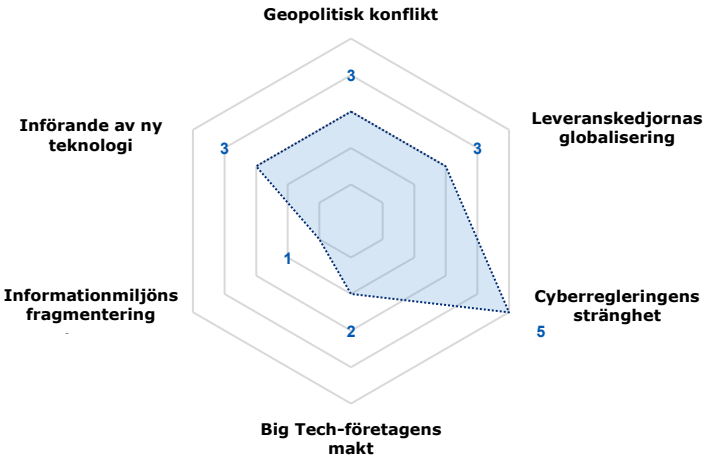
USA har behållit sin internationella ledarställning i förhållande till konkurrenten Kina, men interna utmaningar och utrikespolitiska övertramp har gjort landet till en **allt mer auktoritär och oförutsägbar allierad.** Natosamarbetet och den västliga säkerhetsarkitekturen står dock starka, och **Kina med sina BRICS-allierade har inte lyckats utmana västländerna med framgång.** EU har stärkt sin strategiska autonomi i förhållande till USA, samtidigt som unionen drar sitt strå till stacken i demokratiernas allians. **Statsaktörer kartlägger och saboterar västländernas system med tanke på framtida konflikter.**

Införandet av ny teknologi är måttfullt.

AI-utvecklingen har inte infriat de djärvaste löftena, och de största projekten har lagts ned som olönsamma. Överdimensionerad infrastruktur, översålda lösningar, rättsprocesser och dataintrång har gjort finansiärerna försiktiga. Det har bromsat införandet och lett till en AI-vinter för stora modeller. **Vid sidan av LLM-utvecklingskurvan har det därför utvecklats AI-tillämpningar som bygger på högkvalitativa *organiska data* och avgränsade användningsfall**, bland annat SLM-modeller och edgebaserade lösningar, som har införts framgångsrikt i EU. Möjligheterna att gemensamt utnyttja högkvalitativa företagsdata på den inre marknaden tar stora kliv framåt. **EU har förbättrat sin självförsörjning inom molntjänster, AI-tillämpningar samt kvant-, 6G- och rymdteknik, och datasuveräniteten har stärkts.**

EU förhindrar att den gemensamma förståelsen splittras.

Genom regleringen av plattformsföretag är EU ett typexempel på en medborgarorienterad och välreglerad informationsmiljö. Plattformarnas uppgifters riktighet upprätthålls genom skyldigheter i regleringen. EU tryggar samhälleligt förtroende och en gemensam kunskapsbas på plattformar som bygger på stark autentisering. **Utländska aktörer åläggs att göra sina algoritmer transparenta**, och de måste kunna verifiera om innehållet är syntetiskt eller organiskt. Genom generativ tjänstedesign som byggts in i enheterna styrs användarna obemärkt mot trygga sätt att agera. Samtidigt anklagas de officiella informationsmiljöerna för censur.



Politiseringen urholkar teknikföretagens makt.

Globala teknikföretag väljer sina geopolitiska referensgrupper och agerar som parter i konkurrensen mellan stormakterna. De har ett intresse av att sprida Kinas eller USA:s inflytelsesfärer för att utvidga sina kundbaser. **Politiseringen har ändå urholkat teknikjättarnas trovärdighet. Som en följd av detta tvingas de i EU göra eftergifter enligt regleringen** och agera mer lokalt för att kunna fortsätta sin data- och plattformsekonomiska verksamhet och upprätthålla sina marknadsområden. I EU ser man till att de inte får tillgång till information om greenfield-företag inom spjutspetsteknik eller till värdefulla, specialiserade data.

Leveranskedjorna har inte återgått till att vara globala.

Kina-centrerade globala leveranskedjor har behållit sin ställning som en av världsekonomins viktigaste kanaler, men **Kina och USA har begränsat användningen av varandras tjänster och infrastruktur.** I många EU-länder är det förbjudet att utnyttja kinesisk teknik i den kritiska infrastrukturens kärnområden, men kinesiska tjänster och enheter har blivit vanligare på konsumentmarknaden. **EU har utökat samarbetet med västländerna och upprätthållit neutrala handelsförbindelser med Kina och BRICS-länderna, med undantag för Ryssland.** Möjligheterna att förbättra handelsförbindelserna med bland annat Afrikas största ekonomier kartläggs. Ryssland har på USA:s initiativ formellt återintegrerats i världsekonomin, men landets relationer till de flesta EU-länder har förblivit spända.

Cyberregleringen skärps.

EU har en ledande ställning när det gäller att fastställa reglering och standarder för teknik och cybersäkerhet. **Med stöd av strävan efter strategisk autonomi bygger EU upp en regleringsmiljö för AI-tillämpningar och dataanvändning som upprätthåller demokrati och integritetsskydd. Internationella teknikföretag tvingas anpassa sig till denna miljö.** En EU-molnmiljö som bygger på stark autentisering garanterar en miniminivå för informationssäkerhet i enlighet med regleringen. I västländerna råder en utveckling där värdet på de data som ska skyddas i praktiken avgör tyngdpunkterna i skyddet. Företagen har incitament att följa regleringen om informationssäkerhet när det gäller värdefulla och verifierade *organiska data*.

Motsättningarna mellan stormakternas intressesfärer består

Geopolitiken och världsekonomin präglas av en era där uppgörelser görs med USA, samtidigt som Kinas konkurrenskraft närmar sig USA:s nivå. USA har drabbats av en *Dotcom 2.0-ekonomikris* till följd av den LLM-AI-bubbla som teknikföretagen och finanssektorn blåst upp, och de amerikanska företagens internationella ställning har försvagats. **Samtidigt har USA ändå lyckats behålla sin relativa ledarställning genom att med bilaterala avtal få tredjeländer att vända sig mot Kina**, som allt oftare ses som en fordringsägare snarare än som en sponsor. I stället för direkta geopolitiska konfrontationer **pågår en kapplöpning om teknik, allierade och naturresurser för att förbereda sig inför eventuella konflikter.** Åtgärder under krigströskeln präglar kontinuerligt relationerna mellan stormakterna och deras intressesfärer.

De skärpta relationerna mellan Indien och Kina har minskat Kinas geopolitiska manöverutrymme, och BRICS-samarbetet har inte konkretiserats eftersom medlemsländerna, med undantag för Ryssland, har hållit stånd mot Kinas ekonomiska dominans. **Ryssland har delvis återintegrerats i den globala ekonomin** på energi- och råvarumarknaderna. Relationerna mellan EU och Ryssland har förblivit spända.

Trots sina protektionistiska utspel har USA fortsatt att stå fast vid bland annat Natosamarbetet, även om landet till följd av interna utmaningar har blivit en mer autokratisk och oförutsägbar allierad. EU och dess samarbetspartner i samväldesländerna, Japan och Sydkorea har vant sig vid USA:s protektionistiska impulser, och tekniska och ekonomiska påtryckningsmedel och incitament mellan även formella allierade hör överlag till vardagen i världspolitiken. Övriga västländer strävar efter att minska sina tekniska beroenden av USA där det är möjligt.

Leveranskedjorna har inte återgått till att vara globala

Kina-centrerade globala leveranskedjor har behållit sin ställning i centrum av världsekonomin. Kina och USA har kraftigt begränsat användningen av varandras företags tjänster och infrastruktur. USA:s allierade utsätts för allt starkare krav på att frigöra sig från kinesisk infrastruktur och kinesiska tjänster. Kinesisk teknik är därför förbjuden i många EU-länder inom infrastrukturens kärnområden, men kinesiska tjänster och enheter har blivit vanligare på konsumentmarknaden. **EU måste fortfarande agera i ett läge där unionen i stor utsträckning är beroende av amerikansk teknik, samtidigt som den strävar efter att hålla individens friheter och integriteten i centrum för digitaliseringsutvecklingen.**

I och med att amerikanska storföretag har fått mindre handlingsutrymme har Europeiska kommissionen identifierat en möjlighet att föra hem kritiska data och stärkt sin självförsörjning, särskilt genom suveräna molnlösningar. Inom EU:s ekosystem för offentliga molntjänster skyddas medborgarnas känsliga data, och de mest kritiska informationssystemen hanteras i egna datacentraler. Företagen har bildat datalager som bygger på insamling av branschdata och som företag utanför den inre marknaden betalar en användningsavgift för. I EU används en eID-identitet vars åtkomsthantering unionen styr.

EU:s inre marknad har fått företagen att växa, och möjligheterna att gemensamt utnyttja data tar stora kliv framåt. Det visar sig ändå vara svårt för EU att uppnå heltäckande digital suveränitet, trots att förtroendet för USA och amerikanska företag har försvagats. EU:s suveräna molnkapacitet gäller främst plattformar för den känsligaste databehandlingen. De används parallellt med amerikanska hyperskalare, som behandlar övriga data i enlighet med regleringen.

Cyberregleringen skärps

EU har behållit sin ledande ställning när det gäller att fastställa reglering och standarder för teknik och cybersäkerhet. Med stöd av sin strävan efter strategisk autonomi försöker EU bygga upp en ”tredje väg” för digital reglering och cyberreglering: en regleringsmiljö för AI-tillämpningar och dataanvändning som upprätthåller demokrati och integritetsskydd. Målet är att göra denna miljö till en globalt betydelsefull motvikt till Kinas och USA:s system. En reglerad EU-molnmiljö garanterar medborgarna en miniminivå för informationssäkerhet och dataskydd i enlighet med regleringen.

Trots den skärpta regleringen råder det i västländerna i allmänhet en utveckling där företagen balanserar mellan regelefterlevnad och risktagande. **I praktiken avgör värdet på de data som ska skyddas var tyngdpunkterna i skyddet läggs.** Företagen har incitament att följa regleringen om informationssäkerhet särskilt när det gäller värdefulla och verifierade *organiska data*. Skyddsmetoderna för sådana data utvecklas särskilt eftersom en eventuell läcka kan leda till en större sanktionsnota. En börs för integritetsdata sätter ett pris på information i regionala, likasinnade geopolitiska referensbubblor, och egna varianter uppstår i västländerna och mellan Digital Belt and Road-länderna. **De välbärgade har möjlighet att ställa företag till svars och betala för sin säkerhet, medan man i praktiken tar större risker när det gäller dataskyddet för andra befolkningsgrupper.**

Tillsynen över regleringen och informationsutbytet fungerar mellan myndigheterna inom geopolitiska områden, såsom västländerna och Digital Belt and Road-länderna. Samarbetet mellan intressesfärerna har minskat. EU:s finansieringsorgan ökar sitt inflytande över förvaltningen av den strategiska självförsörjningen.

Politiseringen urholkar teknikföretagens makt

Till följd av den protektionism som råder i världen tvingas stora teknikföretag välja mellan USA och Kina som sina huvudsakliga geopolitiska referensgrupper och marknader. De har därför ett bakomliggande intresse av att bidra till att stormakternas geopolitiska inflytelsesfärer sprids, för att på så sätt kunna utvidga sina potentiella kundbaser. **Politiseringen har ändå urholkat de stora teknikföretagens trovärdighet, väckt motstånd och lett till att lokala konkurrenter har stärkt sin ställning.** Som en följd av detta tvingas teknikföretagen göra eftergifter i enlighet med EU-regleringen för att fullt ut kunna fortsätta sin data- och plattformsekonomiska verksamhet i området.

I EU ser man till att utländska storföretag inte får tillgång till information om greenfield-företag inom teknikbranschen eller till värdefulla, specialiserade branschdata. De tvingas balansera mellan tillgången till EU:s marknadsområde, medborgarnas förtroende och sina hemländers politiska mål. Oftast väger de två förstnämnda ändå tyngre.

Låg autonomi och högkvalitativa data

Den första vågen av LLM-tillämpningar blir inte lönsam, och **överdimensionerad infrastruktur, översålda lösningar och kollapsade avkastningsförväntningar har fått finansiärerna att dra tillbaka sina investeringar.** Manipulationsproblemen och hallucinationerna i de största modellerna har inte kunnat lösas. AI-genererat innehåll och syntetiska data har ökat, men de kan inte utnyttjas rekursivt för vidareutveckling av modellerna. Värdet på autentiska och kvalitetssäkrade *organiska data* har ökat. Modeller som byggts med skala som främsta utgångspunkt har visat sig vara fel väg till tillförlitlig och autonom AI-teknik. När volymbaserad utveckling har visat sig olönsam har tillgången på processorer och grafikkort förbättrats. Beräkningen flyttas i allt högre grad från stora molnimplementationer till mer avgränsade uppgifter och lokal edge computing. LLM-vågen har gett plats åt en SLM-våg, och **AI är ett verktyg bland andra. Den effektiviserar särskilt programmering.**

EU-språkmodeller som bygger på högklassiga träningsdata har etablerat sig i medborgarnas vardagliga användning, **men teknikens sysselsättningseffekter är begränsade eftersom verktygens autonomi är begränsad.** Människor måste fortfarande fungera som kvalitetssäkrare i processerna. De viktigaste tillämpningsområdena är **modellering och realtidsanalys utifrån stora datamängder.** För detta ändamål bildar EU-företag branschvisa datapooler.

AI-agenter med låg autonomi som är kopplade till eID-identiteter kan sköta vardagsuppgifter, och de har slagit igenom i EU med begränsningar som avgränsar deras åtkomsträttigheter och gör det möjligt för aktörer att entydigt blockera dem.

Krypteringsalgoritmerna vinner kvantkapplöpningen

Känsliga data har skyddats med kvantresistenta skydd. EU har hållit jämna steg med USA och Kina i uppbyggnaden av kvantinfrastruktur kvantresistent skydd har byggts in i centrala delar av den kritiska infrastrukturen. De första fungerande lösningarna för att knäcka traditionell kryptografi har utvecklats, men krypteringslösningarna har utvecklats snabbare än metoderna för dekryptering, och de mest långtgående framstegen är mestadels informationspåverkan. **EU använder avancerade krypteringslösningar bland annat för att skydda det uppkopplade EU-företagsekosystemet och medborgarnas personuppgifter.** Det blir möjligt för statsaktörer att dekryptera tidigare insamlade uppgifter med lägre skyddsnivå. Detta leder till att organisationer under tvång accepterar att gamla uppgifter offentliggörs och vidtar de riskhanteringsåtgärder som följer av detta.

Förbindelserna förbättras i det västliga samarbetet

Införandet av globalt standardiserat 6G går snabbt under 2030-talet, och **en stor del av enheterna och programvarorna kommer, utöver från EU-medlemsstaterna, från USA, Sydkorea eller Japan. Snabba bredbandsförbindelser i EU:s glesbygdsområden tillhandahålls huvudsakligen med hjälp av EU:s egen IRIS²-konstellation, och kapaciteten kompletteras via tjänsteleverantörer från USA.** Teleoperatörer, molntjänstplattformar och logistikföretag integrerar satellittjänster i sitt utbud genom API-baserade partnerskap i ekosystem som är verksamma i EU och delvis beroende av externa aktörer.

Den överkapacitet för beräkning som byggdes upp i samband med LLM-hypen utnyttjas i tillämpliga delar för att bygga upp realtida och realistiska fjärrförbindelser. VR-verkligheter hos företag på EU:s inre marknad är vardag i organisationer. Samhällenas uppkoppling har lett till att sensorer och gränssnitt kopplas samman på många olika sätt. **I EU har digitala tvillingar som driver, effektiviserar och övervakar system inom industrin, ekonomin och samhället blivit vanligare.** Den teknologiska helheten kompliceras av underleverantörskedjor där en del av tjänstehelheterna produceras av aktörer utanför EU, och det saknas direkt insyn i de delar av systemen som dessa aktörer upprätthåller.

Splittringen av den gemensamma förståelsen förhindras

Oron över att informationsmiljön fragmenteras och att den gemensamma kunskapsbasen kollapsar leder till politisk mobilisering för att trygga en gemensam informationsmiljö. **Efter att regleringen av plattformsföretag har lyckats är EU ett typexempel på en oasliknande och reglerad informationsmiljö.** Kärnan i denna miljö är en ”officiell informationsmiljö”, som upprätthålls i EU-molnet och som nås genom stark autentisering. **Med hjälp av mediefostran och påverkansarbete försöker man få medborgarna att söka sig till den.**

Man försöker upprätthålla riktigheten hos plattformarnas uppgifter genom skyldigheter i regleringen. Utländska aktörer åläggs att göra sina algoritmer transparenta, och de måste kunna verifiera om innehållet är syntetiskt eller organiskt. Utanför de kuraterade kunskapsoaserna breder dock syntetisk information och desinformation ut sig som ödemarker till följd av den ökade användningen av generativ AI. På dessa ödemarker försöker plattformar och statsaktörer uppnå monopol på sanningen.

Billiga processorer, grafikkort och billig beräkningskapacitet på marknaden har gjort prestanda tillgänglig för hotaktörer, vilket bland annat har lett till att deepfake-tekniken har blivit mer kapabel. **Kina och Digital Belt and Road-länderna, och å andra sidan USA med sina närmaste allierade, försöker i sina egna *informationssfärer* bygga upp sina berättelser om världen med stöd av syntetiska innehållsproducenter och folkgrupper för att utvidga sina inflytelsesfärer.**

I EU fostras medborgare med kompetens inom informationssäkerhet

EU-användare som identifieras genom stark autentisering och integreras i AI-assistenter anses skapa en riskfylld kombination av biometriska uppgifter och andra personuppgifter. Därför begränsas plattformarnas funktioner i miljöer med stark autentisering. **I EU blir listan över tillåtna applikationer och smarta sensorer som kan kopplas till en virtuell eID-användare snävare** för att informationssäkerhetsrisker ska kunna förebyggas. Enheter anpassas till EU-kompatibla versioner. Det tar tid att auditera de senaste innovationerna och få in dem på den inre marknaden, vilket inte alla användare är nöjda med. Införandet av agenter på plattformarna har ökat behovet av starkare biometrisk autentisering, vilket delar EU-medlemsländernas synsätt. Man försöker svara på medborgarnas ökade krav på autenticitet, integritet och analoghet genom digitala normer. **Viljan att kontrollera sina egna data, medvetet välja att ställa sig utanför tekniken och använda innehåll som producerats av människor ökar.**

Regleringen av reklam på sociala medier och AI-plattformar skärps, och plattformar utanför EU blir avgiftsbelagda till följd av begränsningar i dataaffärsverksamheten. **På plattformarna styrs användarna med hjälp av generativ tjänstedesign mot trygga sätt att agera.** Det är dock inte lätt att mura fast en enda objektiv sanning som grundsten i EU:s informationsmiljö. **De officiella informationsmiljöerna anklagas för censur, och många upplever att den ”EU-verklighet” som skyddar användarna mot desinformation är ett auktoritärt snarare än demokratiskt levnadssätt.**

En del användare **försöker kringgå begränsningarna för applikationer och enheter genom att skaffa dem från overifierade källor. När AI-baserad avvikelseövervakning införs i leveranskedjorna** kan den som använder olaglig teknik, olagliga enheter eller olagliga plattformar tillsammans med sin eID-identitet spärras och få begränsad tillgång till officiella tjänster, om användningen sker utanför det officiella användarstödet. I värsta fall kan personen anklagas för spionage eller desinformation.

Angreppsyta: En mer demokratiskt självförsörjande infrastruktur

- EU:s centraliserade identitetslösning för stark autentisering omfattar en betydande katalog av medborgarnas känsliga biometriska uppgifter och andra personuppgifter, som samlas i EU-datacentraler i området.
- I AI-kapplöpningens andra våg betonas högkvalitativa, privata *organiska datakällor* som har samlats i branschspecifika datapooler på EU:s inre marknad som ”kronjuveler”.
- Till följd av EU:s ansträngningar för strategisk autonomi har elektrifieringen av energiinfrastrukturen ökat potentialen för förnybar energi, med betoning på smarta nät som oundvikligen är kopplade till komponenter med ursprung utanför EU.
- Den ökade IoT- och IIoT-konnektiviteten samlar edge-enheter särskilt i de största städernas Smart City-helheter, där data om samhällsfunktionerna samlas i datamotorer och digitala tvillingar som optimerar funktionerna. Den del som syns för medborgarna kopplas via den egna AI-assistenten till bland annat navigering och trafikstyrning, vilket leder till bättre tjänster.
- Verifierbar och validerad information i EU-länderna har koncentrerats till en informationsmiljö för verifierad information bakom stark autentisering och som aktivt redigerar den bild av världen som förmedlas till medborgarna som en motåtgärd mot desinformation. AI-assistenter fungerar via EU-språkmodellen som personliga verifierare och kuratorer av informationsmiljön.
- På grund av den fortskridande åldersutvecklingen i EU har man inte lyckats täcka behovet av cybersäkerhetsexperter, och yrkespersoner har rekryterats proaktivt från andra håll för att hantera sårbarhetsytan. Billiga processorer och specialiserade modeller har å andra sidan möjliggjort lättare lösningar för autonomt cyberförsvar.
- Kravet på stark eID-autentisering och det begränsade applikationsutbudet i EU-området hindrar medborgare från att hamna i AI-assisterat kodade kopior av applikationer som hotaktörer använder för datainsamling och spionage.

Hot: Operationer under krigströskeln

- Statsaktörer kartlägger och minerar västländernas system med tanke på framtida konflikter. Verksamheten hålls under tröskeln för krigföring.
- Personliga AI-assistenter som fungerar som uttryck för EU-språkmodellen kan programmeras för att obemärkt påverka medborgare som har blivit beroende av dem i sin vardag. Träningsdata för assistent- och agenttillämpningar baserade på EU-språkmodellen utsätts för förgiftnings- och korruptionsangrepp i syfte att öka desinformationen.
- AI-verktyg kan användas för både angrepp och försvar med exakta avgränsningar och uppdragsbeskrivningar. Den skärpta AI-regleringsmiljön och dess säkerhetskrav bromsar införandet och utvecklingen av försvarstillämpningar i förhållande till angriparnas mer ohämmade förmågor.
- Cyberbrottslingar är intresserade av att utnyttja datakombinationer från EU-molntjänster som samlat in eID-biometri och personuppgifter för intrång, bedrägerier och nätfiske. Man försöker ta sig in i systemen via personer som arbetar med dem.
- Angrepp riktas mot EU-medlemsstaternas informationstjänster, såsom statistikcentraler, i syfte att komma åt medborgarnas registerdata och med hjälp av AI rekonstruera dem för personanpassade angrepp.
- Cyberattacker och sabotage riktas mot infrastrukturen för förnybar energi i EU-länderna i syfte att undergräva förtroendet för förnybara energiformer.
- Betoningen på *organiska data* inom AI/ML-utvecklingen gör företagens branschdata till ett lockande och värdefullt mål för spionage.
- Spionage- och sabotageverksamhet riktas mot Smart City-knutpunkter i digitala tvillingar. Skärningspunkter utnyttjas för att bryta sig in i enskilda sensorer och maskinsalar samt för att manipulera de digitala tvillingarnas AI-gränssnitt.
- Hotaktörer försöker manipulera medborgare som vill ha de senaste innovationerna och applikationerna att koppla olagliga enheter och applikationer till sin eID-användare för datainsamling och spionage.


/FRAGMENTERING/

/FRAGMENTERING 2035/

Kriser bromsar införandet av teknik.

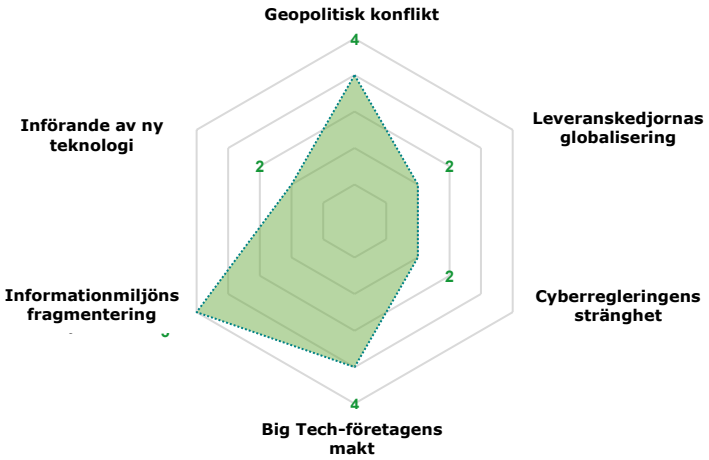
Genom AI-gränssnitt som införts under ledning av de stora teknikföretagen och via osäkra, bristfälligt underhållna lösningar som kodats med hjälp av LLM har känslig information i stor utsträckning blivit åtkomlig i en **"AI-katastrof"**. AI-tillämpningar som införts i samhällsstrukturerna har i demokratierna gillrats för spionage, desinformation och manipulation, och den av tillämpningarna insamlade **informationen har framgångsrikt använts för att återskapa individer och organisationer genom reverse engineering.** Organisationerna måste göra betydande riskbedömningar när de inför AI-verktyg, och de lösningar som används är ofta snäva. **Ur integritetssynpunkt är skadan ändå redan skedd.** De tekniska standarderna har glidit kraftigt isär, bland annat inom 6G. Misstron mot teknik från USA bromsar införandet av ny teknik och driver vissa länder in i Kinas läger, **vilket gör EU:s infrastruktur till ett lapptäcke.** Man hoppas att kvantsäkra krypteringslösningar ska återställa det samhälleliga förtroendet, men EU ligger efter i utvecklingen.

Det går inte att lita på någonting.

Användbarheten hos det offentliga internet har kollapsat när AI-skapat syntetiskt material och syntetisk interaktion har tagit över livsutrymmet, och utvecklingen har drivit människor till mer slutna gemenskaper. Uppgifter som läckt från smarta system har använts för utpressning mot individer och företag, rättsfallen har blivit fler och inställningen till att lämna ut data har blivit mer restriktiv, vilket minskar mängden tillgängliga träningsdata för AI. På olika tjänsteleverantörers plattformar råder olika sanningsgrunder som formar användarnas världsbild. Kraven på att ta steg tillbaka från en informationsmiljö fylld av digitalt avfall har ökat. **I medborgargemenskaper införs metoder liknande *Nightshade* för att förgifta och vilseleda sensorer och smarta funktioner**, i syfte att undkomma företagens och myndigheternas algoritmer.

Världen är på drift och det geopolitiska läget är oförutsägbart.

USA har övergett forumen för internationellt samarbete och koncentrerat sig på att driva sina egna omedelbara intressen. Auktoritära stater sprider sitt inflytande **genom att driva isär EU och demokratierna genom att tillspetsa interna och inbördes konflikter, men också genom ekonomiska incitament.** Befolkningarna har delats upp i grupper som lever kring storföretagens tekniker och grupper som motsätter sig teknologisk globalisering. Det har blivit svårare att bilda gemensamma ståndpunkter, vilket försvagar EU som reglerande aktör.



Beroendena fördjupas trots misstron.

Stora teknikföretag konkurrerar om användare, data, energi och marknadsområden utan större hinder. Det växande kinesiska teknologiska inflytandet skapar hinder för spridningen av västerländska lösningar, och ett krympande marknadsområde driver västerländska företag att fördjupa sin ställning inom demokratiernas offentliga förvaltningar. De intar i allt högre grad rollen som kvalitetsövervakare och upprätthållare av samhällenas digitalisering. I gengäld får de även politisk makt, samtidigt som de möter större motstånd och avståndstagande i vissa befolkningsgrupper. **Deras specialiserade underleverantörskedjor** och ekosystemens identitetshanteringstjänster garanterar samhällenas digitala kontinuitet.

Leveranskedjorna regionaliseras.

Svårigheter med tillgången till teknik gör det svårare att upprätthålla informationssamhället, och EU är beroende av de stora aktörer som kontrollerar leveranskedjorna för att trygga kontinuiteten. Medlemsländerna splittras enligt sina ekonomiska intressen och säkerhetsintressen. Till följd av lobbyverksamhet uppstår läger som föredrar lösningar från USA respektive Kina, vilket förhindrar en enhetlig infrastrukturpolitik. Resultatet är **en fragmenterad digitaliseringsutveckling i EU**, där upphandlingar i Västeuropa görs från USA eller andra västländer, eller där länderna bygger egna gemensamma lösningar. **I östeuropeiska länder tas däremot stora kliv framåt med stöd av teknik och infrastruktur som integrerats i Kinas Digital Belt and Road.** När förmågan att hantera **leveranskedjorna** har försämrats har osäkra enheter och sårbara datanät blivit vanligare.

De realiserade hoten blir för mycket för regleringen.

Den offentliga förvaltningen i allt fler stater ”kollapsar” digitalt när beslutsfattarna inte behärskar den oförutsägbara teknologiska helhetsbilden med dess risker och beroenden. Storföretagen lyckas i demokratierna bromsa regleringssträvandena genom att hålla sig i framkant av en teknikutveckling som bara de själva förstår. **EU:s beslutsfattande har blockerats internt när skiljelinjerna har blivit fler och medlemsländerna har delats upp i mindre intressegrupper, vilket lamslår kommissionens handlingsförmåga.** Den explosiva verksamhetsmiljön gör att insatserna koncentreras till akuta säkerhetsfrågor, medan skyddet av vanliga användare mot externa hot och företagens godtycke hamnar i skymundan. Medborgarnas möjlighet att få del av den digitala grundtrygghet som regleringen garanterar försvagas, och EU-medlemsländerna kan inte längre garantera den för dem som har det sämst ställt.

Världen är på drift och det geopolitiska läget är oförutsägbart

USA har övergett forumen för internationellt samarbete. Den belastning som landets militära interventioner har medfört och den instabilitet som den fördjupade ekonomiska krisen har skapat har drivit USA att främja sina egna omedelbara intressen, vilket har gjort alliansrelationerna transaktionella. **Vi lever i en tid av multipolär fragmentering, där Kina och dess allierade rör sig mot maktvakuum.** Världens spelregler håller på att omförhandlas. USA:s och Kinas ensidiga diktatpolitik som hotar andra staters suveränitet har ökat. Detta leder till begränsade regionala konflikter som berör Europa och Asien och till användning av ekonomiska vapen, vilket försvagar de globala leveranskedjorna och tillgången till teknik.

Efter AI-revolutionen har Europa vaknat upp till en situation **där tillämpningarna inte har infriat sina löften om effektivitet utan att säkerhetsproblemen samtidigt har ökat avsevärt. Via punktvis utvecklade och obetänksamt införda AI-tillämpningar och gränssnitt har känslig information blivit åtkomlig**. Följden är att politiskt inflytande och social kontroll har överförts till externa aktörer via användargränssnitt och genom reverse engeneering av insamlade data. Autokratier har skyddat sina medborgare mot utländsk teknik. **I demokratier har däremot utbredda tillämpningar, både medvetet och omedvetet, gillrats under utvecklingsfasen och användningen så att de lämpar sig för olika former av extern spionageverksamhet, spridning av desinformation och manipulation av värdegrunden.** Som en följd av detta har förståelsen av en gemensam sanning rubbats, upplevelsen av informationssäkerhet och skydd gått förlorad och interna konflikter tillspetsats. Den **polarisering och tribalisering** som *AI-katastrofen* har bidragit till har minskat demokratiernas handlingsförmåga.

EU och demokratierna drivs isär genom att deras interna och inbördes motsättningar tillspetsas. Inom EU har befolkningarna delats upp i stammar som lever i olika storföretagens tekniker och i grupper på olika sidor av det politiska fältet som på sitt eget sätt motsätter sig teknoglobalisering. Det har blivit svårare att bilda gemensamma ståndpunkter, vilket försvagar EU som reglerande aktör. EU:s demokratiska institutioner står formellt kvar, men i praktiken använder medlemsländerna dem för att driva sina egna intressen samtidigt som de spelar sina egna spel i bakgrunden.

Leveranskedjorna och infrastrukturen i EU-området fragmenteras

När förtroenderelationerna har försvagats har leveranskedjorna regionaliserats. Utmaningar med tillgången till mineraler och teknik gör det svårare att i västländerna använda de enheter och tjänster som upprätthåller informationssamhället, och EU är utlämnat åt de stora aktörerna som kontrollerar leveranskedjorna för att trygga leveranssäkerheten. Medlemsländerna splittras enligt sina ekonomiska intressen och säkerhetsintressen. Till följd av lobbyverksamhet uppstår läger som föredrar lösningar från USA respektive Kina, **vilket förhindrar en enhetlig infrastrukturpolitik.**

Stora teknikföretag från USA marknadsför sig i EU som ett säkrare alternativ till kinesiska lösningar och erbjuder sig som strategiska partner till de offentliga förvaltningarna. Resultatet är **en kraftigt fragmenterad digitaliseringsutveckling i EU**, där Finland och de västeuropeiska länderna gör sina upphandlingar från USA eller andra västländer, eller bygger gemensamma lösningar inom sina grupper av stater. I Östeuropa införs däremot kinesiska, förmånliga och heltäckande helhetslösningar.

Norden samt västra och centrala Europa har intensifierat sitt samarbete. Misstron mot teknik från USA och Kina i kombination med byggandet av egna lösningar bromsar införandet av ny teknik. **När införandet sker i olika takt blir infrastrukturen ett lapptäcke.** I östeuropeiska länder tas stora kliv framåt med stöd av teknik och infrastruktur som integrerats i det kinesiska Digital Belt and Road-samarbetet. När förmågan att hantera leveranskedjorna har försämrats har **billiga och osäkra enheter och diffusa datanät blivit vanligare.**

De realiserade hoten blir för mycket för regleringen

Den offentliga förvaltningen i allt fler stater ”kollapsar” digitalt när beslutsfattarna inte behärskar den komplexa och oförutsägbara teknologiska helhetsbilden. EU:s beslutsfattande har blockerats internt när skiljelinjerna har blivit fler och medlemsländerna har delats upp i mindre intressegrupper, vilket lamslår kommissionens handlingsförmåga. Finland söker sin primära referensgrupp för påverkan och tillförlitliga samarbetspartner i Norden och Västeuropa. **Den explosiva verksamhetsmiljön gör att regleringsinsatserna koncentreras till de mest akuta säkerhetsfrågorna**, medan skyddet av vanliga användare mot externa hot och företagens godtycke hamnar i skymundan. **Medborgarnas möjlighet att få del av den digitala grundtrygghet som regleringen garanterar försvagas till följd av många slags risker, och EU-medlemsländerna kan inte längre på ett tillförlitligt sätt garantera den för dem som har det sämst ställt.**

De stora teknikföretagen utnyttjar situationen genom att erbjuda de offentliga förvaltningarna centrala tjänster och kompetens för att upprätthålla det digitala samhällets funktioner och trygga kontinuiteten. I gengäld åtnjuter de en lindrigare tolkning av EU-regleringen. De funktioner som är mest användbara med tanke på insamlingen av medborgardata och helhetsbilden av leveranskedjorna ersätts därför till stor del med lösningar som teknikföretagen noggrant kontrollerar.

Skatteparadis och frihandelsområden som sprider sig utanför den internationella regleringens räckvidd är attraktiva verksamhetsorter för företag och cybersäkerhetsexperter. De urholkar nationalstaternas skattebas och kompetenspool och minskar på så sätt de offentliga cybersäkerhetsorganens handlingsförmåga i demokratierna. De fungerar ofta också som plattformar där cyberbrottslighet och APT-aktörer kan anlita underleverantörer på ett sätt som det är svårt att utkräva ansvar för.

Beroendena fördjupas trots misstron

Stora teknikföretag möter ett mer omfattande motstånd än tidigare i demokratierna, delvis till följd av AI-katastrofen som orsakats av verktyg som de själva har fört ut på marknaden. I en explosiv och oförutsägbar världsekonomisk verksamhetsmiljö är det **ändå endast deras specialiserade underleverantörskedjor, underhållsresurser och kompetens samt ekosystemens identitetshanteringstjänster som tryggar de digitala samhällenas kontinuitet**. De försöker dra nytta av sitt rykte som programvaruvärldens förvaltare och kvalitetsgaranter, efter att AI-drivna punktinsatser inom programmering har blivit vanligare och ökat den tekniska skulden. Att bygga gemensamma applikationsalternativ för hela EU möter politiska hinder, men de mest beslutsamma medlemsstaterna och grupperna bygger egna lösningar.

Stora teknikföretag konkurrerar om användare, data, energi och marknadsområden. Storföretag från USA har lärt sig av riskerna med statlig politisering och oförutsägbart beslutsfattande och höjer sin profil vid sidan av den federala staten. De försöker självständigt påverka regleringen och politiken på sina marknadsområden för att skapa en gynnsam verksamhetsmiljö för sig själva i demokratierna. **Kinesiska storföretag stärker med statens stöd sitt grepp om infrastrukturen i Digital Belt and Road-länderna.** De bygger effektiva tjänster för samhällenas digitalisering och samtidigt heltäckande lösningar som möjliggör övervakning av användarna.

När Kinas teknologiska inflytelsesfär breder ut sig i det globala syd skapas hinder för spridningen av västerländska teknikföretags lösningar. **Det krympande marknadsområdet driver västerländska företag att fördjupa sin delaktighet i de offentliga förvaltningarna**, och genom avtal som ingåtts i ett svårt ekonomiskt läge koncentreras ofta mer användardata och fler åtkomsträttigheter än vad som är ändamålsenligt till tjänsteleverantörerna. Dessa används aktivt för att skapa leverantörslåsningar.

AI-katastrofen får förtroendet att kollapsa

Agentbaserade AI-tillämpningar har införts utan tillräcklig eftertanke och fått djupt fäste i de demokratiska samhällena. Snabba lanseringar som motiverats med högre produktivitet har koncentrerat känsliga data till externa tjänsteleverantörers system. **Det har gett utomstående aktörer en detaljerad inblick i organisationers verksamhet och system.** Ansamlingen av mångsidiga känsliga person- och systemuppgifter har gjort det möjligt för stater och företag att bedriva spionage och manipulation via plattformar men också gjort reverse engeneering av insamlade data möjligt för kriminella hotaktörer.

Politiska beslut har motiverats med information som producerats av AI, och AI har använts inte bara som stöd för beslutsfattandet utan också som rättfärdigande för att legitimera även orättvisa lösningar. **Applikationer med mörka mönster har sålts till offentliga organisationer, och de förgiftas i geopolitiska syften.** På grund av kontamineringen går det inte att lita på vissa funktioner och man försöker begränsa användningen. **På vissa håll klarar samhällena ändå inte längre av att fungera utan dem, och man har inte överblick över var modellerna används.**

Takten i införandet av AI har bromsat in. Tröskeln för att tillåta agentbaserade AI-funktioner är hög, och det finns en efterfrågan på skydd mot dem. Även hotaktörer skaffar aktivt de mest avancerade AI-verktygen och agenterna för eget bruk. Att utvecklingen bromsade in efter LLM-boomen har lett till **överkapacitet och försäljning av beräkningskapacitet.** Kriminella grundar kryptovalutaföretag som täckmantel för att skaffa beräkningskraft till sina operationer. **Hotaktörer har med hjälp av insamlade data och beräkningskapacitet kunnat bygga avancerade och specialiserade AI-angreppsverktyg.**

Kvantkryptering som återställare av förtroendet

Man försöker febrilt bygga upp kvantsäker kommunikation och kvantsäkra krypteringslösningar som **förtroendelösningar för en rubbad informationsmiljö.** De viktigaste arenorna för kvantforskningen finns i skärningspunkten mellan storföretag och internationella universitetsnätverk. **Företagens kvantkompetens är ett betydande mål för cyberspionage.** Stormakterna påstår sig ha byggt dekrypteringsverktyg som ger tillgång till motpartens alla system, men i verkligheten har båda parter byggt lufttäta och kvantskyddade centrala system. **Alla EU-länder har inte kunnat övergå till kvantresistent skydd till följd av intern splittring och externa påverkansoperationer. Ett betydande behov av att förnya utrustningen för att kunna införa uppdaterade PQC-krypteringsalgoritmer har också försvårat utvecklingen.** I brådskan finns en risk att man använder föråldrade standarder som innehåller svagheter. I tillämpningarna prioriteras kritisk infrastruktur och tillämpningar för försvar. Stormakterna fokuserar på att bryta skyddet för tidigare insamlad känslig information för att hitta punkter för påverkan.

Uppkopplingen sker utan gemensam riktning

Införandet av 6G bromsas när leveranskedjorna går trögt, och särskilt när användningsfallen och efterfrågan släpar efter. Standarden delas upp i två olika riktningar mellan företag från Kina och USA. **EU-leverantörerna har inte lyckats lansera något konkurrerande alternativ**, och EU ansluter sig till den standard som USA har byggt upp. Den multipolära och okontrollerade världen återspeglas i rymden när köparna av rymdteknik och satellitkapacitet blir fler och mer varierade. Kriminella som verkar via täckföretag skaffar LEO-kapacitet med stöd av statsaktörer **för att kunna operera utanför andra nät.**

De fragmenterade leveranskedjorna har lett till att det går långsammare att få tillgång till den senaste tekniken i EU och till att lösningarna fördelas ojämnt. **Aktörer som är beroende av tjänsterna har olika insyn i var kritiska data behandlas, och ofta är det bara tjänsteleverantörens ord som garanterar hur saken ligger till. I avsaknad av en enhetlig EU-politik är det främst de största organisationerna och förvaltningarna som kan bygga egna lösningar.** För andra är det bästa sättet att trygga kontinuiteten att i så stor utsträckning som möjligt använda kompatibla system från en enda stor tjänsteleverantör. På EU-nivå leder detta till interoperabilitetsproblem: systemen kommunicerar dåligt med varandra och leverantörslåsningar gör det svårt att flytta data.

När syntetiskt innehåll dominerar går det inte att lita på någonting

Generativa AI-modeller har slukat informationen på det öppna internet och rekursivt byggt vidare på sig själva och sina syntetiska utdata. Utvecklingen har visat sig vara en **självförstärkande spiral, och användbarheten hos det öppna internet har kollapsat när syntetisk interaktion har tagit över utrymmet**. Utvecklingen bryter ned förtroendet för informationsförmedlingens plattformar och splittrar medborgarnas verkligheter i allt mer separata, modererade bubblor. **På olika tjänsteleverantörers plattformar, som används med identifiering, råder olika sanningsgrunder som formar användarnas världsbild.** Annonsörer, syntetiska agenter och politiska informationsoperatörer försöker aktivt påverka användarna på dessa plattformar. Personliga AI-assistenter som säljs som opartiska faktagranskare integreras i mediekanaler för att analysera flöden.

I Finland har kraven ökat på att ta steg tillbaka från digitala informationsmiljöer fyllda av digitalt avfall. Många har hamnat utanför, eller valt att ställa sig utanför, den digitalisering som framskrider parallellt med den samhälleliga ojämlikheten. En del inleder en fasta från det digitala livet, medan många nöjer sig med ett enkelt liv med bastjänster. En mer ”organisk” användning av datanät, med separata nät, gränssnitt som skyddas mot AI-agenter och lokala lösningar, är populär bland entusiaster, och bästa praxis sprids i gemenskaper. **Den offentliga förvaltningen samlar sig för att åter lägga grunden för förtroendet och nå de ”förlorade” medborgarna.**

På dark web har plattformar med ett snyggare utseende och bättre användbarhet än tidigare blivit populära på nytt som **en tillflyktsort för oliktänkande som vill bort från det öppna internet.** Administratörerna är okända, och plattformarna är ofta omodererade.

En rubbad upplevelse av informationssäkerhet

En svårkontrollerad värld rubbar upplevelsen av informationssäkerhet. Under 2020-talet har medborgare samlat på sig en *personlig dataskuld* och deras privata uppgifter har via olika gränssnitt i stor utsträckning hamnat i fel händer. Genom att kombinera uppgifterna kan personanpassade bedrägeri- och nätfiskemeddelanden riktas även till användare som helt har ställt sig utanför sociala medier. **En kategori för sig är de användare som har umgåtts dygnet runt med mångsidiga personliga AI-assistenter och lämnat ut biometriska uppgifter och detaljerade beteendedata.** Utifrån dessa uppgifter kan angripare skapa falska avatarer som interagerar på önskat sätt.

Den samhälleliga sanningsgrunden har rubbats och medborgarna är skeptiska till att lämna ut sina data till den offentliga förvaltningen. Det öppna internet har fyllts av syntetiskt innehåll och ger inga tillförlitliga svar när interaktionen präglas av kriminella agenter och bottar. Person- och organisationsspecifika uppgifter som läckt från smarta system och syntetiskt innehåll som skapats utifrån dessa uppgifter har i stor utsträckning använts för utpressning mot individer och företag. Rättsfallen har ökat och medvetna medborgare blir allt mer restriktiva med att lämna ut data. **I olika gemenskaper införs metoder liknande *Nightshade och tar pits* för att förgifta och vilseleda sensorer och smarta funktioner, i syfte att undkomma företagens och myndigheternas algoritmer.** Det språk som används och den snabbt föränderliga memkulturen har i ännu högre grad blivit ett sätt för avhoppare som undviker algoritmer att känna igen varandra. Det hjälper dem att sålla syntetiskt innehåll i det öppna internets *mörka skog*.

Etisk och transparent databehandling håller på att bli en konkurrensfördel, men förändringen går långsamt och det är svårt att bygga upp förtroende. Ett dilemma blir hur personer som har kopplat bort sig från det digitala samhället ska kunna **återintegreras i samhället, samtidigt som människor fortfarande tillåts välja att stå utanför digitala system.**

Angreppsyta: Ett lapptäcke av system

- Stora tjänsteleverantörer är noggranna med vilka aktörer som kopplas till deras moln, efter att AI-agenter som kartlagt IT- och OT-sårbarheter har borrat sig genom leveranskedjorna. Betalningsförmögna användare och företag måste gå igenom en ”detox” när deras egna system som kodats med hjälp av AI ofta har visat sig vara osäkra. De tvingas förnya sin digitala identitet och system för att kunna ansluta sig till de stora tjänsteleverantörernas ekosystemer.
- Användarnas data finns utspridda i allt mer splittrade miljöer och på okända platser, där de behandlas av föråldrade och sårbara IoT- och edge-enheter. Mer lokala lösningar har lyfts fram, men de är svåra att motivera ur ett affärsekonomiskt perspektiv. I Finland ligger fokus främst på nätverkssegmentering.
- Tjänsteleverantörer som är måna om sina systems integritet erbjuder säkra helhetslösningar till mer välbärgade aktörer med högre mognadsnivå, medan små och medelstora företag lämnas åt sitt öde när det gäller högklassig informationssäkerhet.
- Medborgarna använder i stor utsträckning applikationer med mörka mönster. De kan vara datainsamlare dolda bakom skenfunktioner, till och med i form av bottar för faktagranskning av nyhetsflöden. Gemenskapernas betrodda lokala nät skyddas med metoder som blockerar och vilseleder agenter.
- På internet och dark web har det uppstått fler privata digitala ekosystem. Tillsammans med frihandelsområden möjliggör de ”virtuella stater”, där kriminella kryptotillgångar tvättas via institutioner som är maskerade som legitima. Det går inte att samla någon gemensam front för att övervaka dessa fristäder.
- Säkerhetsproblemen i AI-system har minskat förtroendet för autonoma tillämpningar för cyberförsvar, samtidigt som angriparnas kapacitet rusar vidare med hjälp av specialiserade AI-angreppsverktyg.
- Kontinuitetshanteringen har blivit mer komplex på grund av okända knutpunkter. Samtidigt försvårar fragmenteringen också illvillig verksamhet: det är arbetskrävande att utnyttja även föråldrade tekniska beskrivningar som bygger på olika system och standarder, och inte ens en AI-assisterad angripare hittar träningsdata om varje detalj.

Hot: Fragmenteringen skapar oförutsägbarhet

- Statsstödda professionella kriminella som opererar från nya virtuella stater och från områden i länder där regleringen har kollapsat har skaffat beräkningskapacitet på en aldrig tidigare skådad nivå. De utnyttjar kraftfulla AI-verktyg för angrepp, analys och sammanställning av information.
- Statsaktörer och kriminella påverkar satellitkonstellationer genom cyberattacker, och störningar och avbrott i satellitfunktioner blir vanligare. Mobilnäten, styrningen av elkraftnäten och trafiksystemen drabbas av synkroniseringsstörningar och förfalskning av tids- och positionsdata.
- När interaktionsdata från dejtingtjänster, webbläsardata, LLM-användningsdata, biometriska data från hälsoapplikationer och bankuppgifter kombineras med omfattande dataläckor, får kriminella nästan obegränsade möjligheter att genomföra starkt profilerade deepfake-bedrägerier som kan spela på känslor.
- Hotaktörer använder kodagenter för att snabbt skapa kopior av betrodda applikationer och plattformar som ser äkta ut och lockar intet ont anande användare till dem.
- Cyberförmågor på toppnivå som utvecklades av de stridande parterna under Rysslands anfallskrig i Europa på 2020-talet finns till salu på världsmarknaden.
- *AI-nolldagssårbarheter* förekommer när sårbarheter som aktiveras under vissa villkor döljs i modellernas minne, träningsdata eller kontext, till exempel genom att en AI-tillämpnings långtidsminne manipuleras.
- Statsaktörer och kriminella grupperingar i virtuella stater driver arbetsplattformar som är maskerade som legitima och erbjuder yrkespersoner extra inkomster. Via plattformarna försöker de rekrytera lokala insiderpersoner från IT-företag som är förberedda på deepfake-hot.
- I EU:s fragmenterade regleringsmiljö har ineffektiv sanktionskontroll lett till en ökning av utpressningstrojaner som kriminella utnyttjar, eftersom det inte finns handelspolitiska hinder för att betala lösensummor och företagen i första hand försöker värna om sitt rykte. Små och medelstora företag drabbas speciellt.
- I efterdyningarna av AI-katastrofen skyddas allt fler system med så kallade *tar pit-motåtgärder*, som bromsar och vilseleder AI-agenter. Samtidigt utvecklar även kriminella sådana metoder som fällor för att korrumpera funktionen hos de scrapingverktyg och AI-agenter som organisationer använder.


/TVÅ MAKTSFÄRER/

/TVÅ MAKTSFÄRER 2035/

Tekniken tar stora kliv inom försvaret.

Autonoma AI-tillämpningar inom cybersäkerhet har i stormakternas kapprustning blivit en kritisk del av samhällenas säkerhetsarkitekturer **då autonoma angrepp har förkortat försvararnas responstid avsevärt och skapat en ständig kapplöpning mellan angripande och försvarande kodagenter**. **Funktioner som är kritiska för försörjningsberedskapen**, från livsmedelsförsörjning till vatteninfrastruktur, **har därför övergått till att styras av AI-system**. När säkerhetsmiljön skärps strävar man ändå fortfarande efter att hålla människor med i beslutsfattandet. 6G och satellitbredband har gjort förbindelserna inom de geopolitiska blocken nästan fördröjningsfria och med stor kapacitet. **När stormakternas AI-lösningar har blivit jämnstarka utvecklas kvanttekniken mot militära tillämpningar.** Hotet om kvantöverlägsenhet har gjort utvecklingen av kvantsäkra algoritmer till ett prioriterat spetsprojekt, och i båda blocken har de mest kritiska datalagren kunnat skyddas med hjälp av dem.

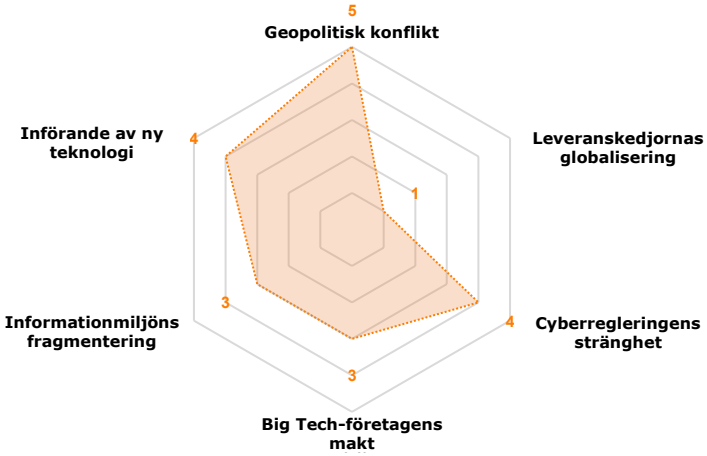
Extern informationspåverkan stävjas.

Informationskanaler och plattformar står under ideologisk kontroll i blocken. Internet behåller en skenbar frihet, men är i praktiken en styrd, filtrerad och regional verklighet. Syntetiska medier och deepfake-teknik används aktivt både för att trygga informationsmiljön och för att angripa den. **Den statliga kontrollen över plattformarna ökar, och myndigheterna använder filtrering, prioritering och modifiering av innehåll.** Censuren av externa spridare av desinformation sträcker sig också till interna oliktänkande. **EU:s roll i fråga om dataskydd är oklar i förhållande till dem som förvaltar plattformarna, men detta accepteras som en nödvändig uppoffring för att upprätthålla den externa och interna säkerheten.**

TRAFICOM

Det geopolitiska motsatsförhållandet står på avgrundens rand.

Det västliga blocket under USA:s ledning möter den utmaning mot världsordningen som Kina och dess allierade utgör. Försök görs att rubba västländernas gemensamma front genom att testa Nato-länderna i Europa. Luckor söks i deras kritiska infrastruktur, och ett eventuellt ingripande från Nato vägs in kalkylerat. **I EU har man svarat på de växande hoten genom att bygga digitala försvarslinjer i samarbete med USA, nästan helt beroende av teknik från USA och av Nato.**



Teknikjättarna rättar in sig i ledet.

Teknikjättarna deltar, **underställda sina offentliga förvaltningar,** i stormakternas geopolitiska strategier bland annat när det gäller datahantering, AI-utveckling och säkerhetsinfrastruktur. Teknikjättarnas geopolitiska nytta har ökat och de påverkar förvaltningarna för att kunna expandera. I stora Nato-länder har försvarsförvaltningarna **egna representanter inne i teknikföretagen.** Deras **plattformar fungerar både som verktyg och mål för underrättelseverksamhet.** Teknikjättarna stöder aktivt sina blocks växande inflytande, bland annat med hjälp av bakdörrar och spionageteknik, i hopp om att i gengäld få tryggad tillgång till kritiska produktionsfaktorer. **Amerikanska analysföretag inom försvarssektorn har integrerats i EU-ländernas förvaltningar.**

Intressesfärerna isolerar sina leveranskedjor.

USA försöker bygga oberoende tekniska leveranskedjor för att kunna fortsätta sin avancerade chipproduktion, samtidigt som landet möter proxykonflikter i Afrika, Sydamerika och Kaukasus. **Handelspolitiskt åtskilda varuflöden, demografiska utmaningar och leveransstörningar orsakade av konflikter har försvagat västländernas konkurrenskraft.** Kinas tekniska övermakt inom AI, automation och datainfrastruktur har tvingat västländerna i försvarsställning. Den globala digitala infrastrukturen har delats i två. **EU:s strävan efter suveränitet har inte fått tillräckligt genomslag,** och infrastruktur från amerikanska hyperskalare dominerar i kritiska informationssystem. **EU-områdets molnmiljöer byggs också på deras infrastruktur och under deras övervakning.**

Regleringen skärps i takt med säkerhetskraven.

Den tekniska kompatibiliteten och standarderna mellan blocken har försvagats och basinfrastrukturen bygger på system som är knutna till geopolitiska block. USA kräver att företag från USA ska få största möjliga frihet att agera och utöva tillsyn över digital infrastruktur i EU, med hänvisning till deras ställning som *kritisk infrastruktur för väst*. EU-regleringens säkerhetsbetoning ökar, men glider EU ur händerna när **företrädare för USA samordnar digitala strukturer tillsammans med myndigheterna**. När övervakningen ökar är rätten till dataskydd i ett brytningsskede. Stora tjänsteleverantörer har fått tillsynsuppgifter bland annat inom AI-baserad ansiktsigenkänning.

Det geopolitiska motsatsförhållandet står på avgrundens rand

Det västliga blocket under USA:s ledning försöker hindra att inflytandet från den alternativa teknologiska ordning som Kina och dess allierade företräder sprids i världshandeln, inom global standardisering och på regional nivå. Kina använder sin centrala ekonomiska och politiska ställning för att etablera sig som **garant för gemensamma institutioner och nya spelregler.**

Nato-länder i Europa sätts på prov genom ”specialoperationer” som omfattar cyber- och hybridoperationer, informationspåverkan och användning av energi som vapen för att rubba västländernas gemensamma front. Svaga punkter söks i den kritiska infrastrukturen, och ett eventuellt ingripande från Nato vägs in kalkylerat.

USA, där demokratin är på tillbakagång, har försökt utvidga sitt inflytande med maktmedel på västra halvklotet och öka sin underrättelseverksamhet överallt i världen. USA brottas med sina egna konflikter och interna utmaningar, men försöker samtidigt bygga leveranskedjor som är oberoende av Kina för att stödja försvarsindustrin, chipproduktionen och teknologiska spetsbranscher. Landet möter dock proxykonflikter i Sydamerika, Afrika och Kaukasus. EU har svarat på den geopolitiska kampen genom att bygga digitala försvarslinjer i samarbete med USA och Nato. EU är helt beroende av deras underrättelseinformation och av de system som amerikanska företag tillhandahåller och har förlorat suveränitet i utbyte mot säkerhet.

Intressesfärerna isolerar sina leveranskedjor

Geopolitiskt åtskilda varuflöden, demografiska utmaningar och leveransstörningar orsakade av konflikter har försvagat västländernas konkurrenskraft i förhållande till Kinas mer självförsörjande auktoritära block. Den globala infrastrukturen har delats i två. Chipproduktionen har tagit nya vägar efter störningar i Östasiens kapacitet att producera chip, vilket särskilt har försvagat västländernas konkurrenskraft inom AI. Kinas tekniska övermakt inom AI, automation och datainfrastruktur har tvingat västländerna, som ligger efter i produktivitet, på defensiven för att skydda sin innovationspotential. **Samtidigt införs förmånliga och lätt skalbara teknikpaket i snabb takt i det växande antalet länder som samarbetar med Kina, bland annat verktyg för AI-baserad övervakning.**

EU:s strävan efter digital suveränitet har inte fått tillräckligt genomslag, eftersom västländernas ekonomiska handlingsutrymme har minskat. **Infrastruktur från amerikanska hyperskalföretag dominerar tydligt i kritiska informationssystem. Även molnmiljöerna i EU-området byggs på deras skydd,** och ett villkor för samarbetet är att helt avstå från kinesiska lösningar och kinesisk teknik. **Den tekniska kompatibiliteten mellan blocken har försvagats, liksom de gemensamma standarderna.** Till och med basinfrastruktur, såsom satellitnät och 6G-dataöverföring, bygger på system som är knutna till blocken.

Regleringen skärps i takt med säkerhetskraven

Genom betydande tekniska språng har Kina blivit den ledande standardsättaren för ny teknik. USA har krävt gynnsam reglering och behandling av sina stora tjänsteleverantörer i utbyte mot att trygga EU:s digitala infrastruktur mot det auktoritära blocket. USA:s företrädare samordnar förvaltningen av digitala strukturer med EU-myndigheterna för att upprätthålla en strategisk helhetsbild. Hyperskalarna har utvecklat effektiva, autonoma AI-tillämpningar. För att dessa ska förbli säkra i ett geopolitiskt spänt läge krävs verifierade underhållsåtgärder och verifierat underhåll av kritiska tillämpningar samt mer allmän övervakning av den digitala infrastrukturen. Kraven på att verksamheten ska vara spårbar har skärpts, och stora tjänsteleverantörer har kommit att omfattas av övervakning av både användningen och utvecklingen av tillåtna applikationer samt av ansiktsigenkänning.

När övervakningen ökar får offentliga organisationer och underrättelsetjänster allt större insyn i enskilda personers och företags verksamhet. GDPR har i praktiken upphävts i EU och dataombudsmannens roll har begränsats avsevärt. Underrättelsemyndigheternas AI-tillämpningar analyserar verksamheten för att upptäcka avvikelser och stärka den nationella säkerheten. Samtidigt hamnar de i konflikt med integriteten och rättsskyddet när de ibland leder till felaktiga domar. Rätten till dataskydd håller på att förändras och tolkningarna av individens rättigheter inom informationssäkerhet varierar från stat till stat.

Den internationella dataregleringen är splittrad, och nivån på regleringen av storföretag varierar globalt och mellan blocken. **Tillsynsmyndigheternas betydelse ökar, men det praktiska genomförandet präglas av friktion och påverkas av stark lobbyverksamhet.** EU:s roll inom cybersäkerhet stärks när NIS 2-direktivet och cybersäkerhetslagen ger EU-institutionerna större makt och samordningsansvar. **För den digitala infrastrukturen inrättas särskilda säkerhetsmyndigheter.**

Teknikjättarna rättar in sig i ledet

Teknikjättarna tvingas allt tydligare fungera som en del av stormaktspolitiken och ställer sig antingen inom USA:s eller Kinas inflytelsesfär. De deltar aktivt i geopolitiska strategier, till exempel när det gäller datahantering, AI-utveckling och säkerhetsinfrastruktur. I stora Nato-länder har försvarsförvaltningarna permanenta representanter inne i de stora teknikföretagen. **Företagen utnyttjas för att sprida statligt inflytande, och deras plattformar fungerar både som verktyg och mål för underrättelseverksamhet.** Försvarsanalysföretag från USA har, tack vare sin AI-kapacitet, integrerats i EU-ländernas försvarsförvaltningar. Teknikjättarnas geopolitiska nytta har ökat, och **de påverkar regeringar för att utvidga och fördjupa sina marknadspositioner**.

Teknikjättarna stöder aktivt sina egna blocks växande inflytande, bland annat med hjälp av bakdörrar och den spionageteknik som de tillhandahåller, i hopp om att i gengäld få tryggad tillgång till kritiska produktionsfaktorer, såsom mineraler. Storföretag från USA försöker utvidga västländernas inflytelsesfär genom att bygga leveranskedjor och digital infrastruktur i länder som är positivt inställda och som balanserar mellan blocken. Vid behov skaffar de sig hävstång genom exportförbud för nyckelteknik, politisk påverkan och stöd för begränsad användning av militära maktmedel.

EU:s strikta reglering har inte gett insyn i storföretagens slutna beslutsrum, och beroendena slår tillbaka. Det geopolitiska läget hindrar fri innovation och spridning av investeringar, vilket koncentrerar kompetens till amerikanska storföretag, för vilka landet **kräver största möjliga handlingsutrymme**, med hänvisning till deras ställning som *kritisk infrastruktur för det fria väst*.

Autonoma angrepp och autonomt försvar ökar

AI har blivit en kritisk del av samhällenas säkerhetsarkitektur i den teknologiska kapprustningen, eftersom **statsaktörers och kriminella nätverks autonoma angrepp har förkortat försvararnas responstid och skapat en ständig algoritmisk kapplöpning**. Autonoma AI-modeller byggs med specialiserade dataset för angreppssyften, och AI-system övervakar infrastrukturer och tjänster i realtid. Detta förutsätter att stora tjänsteleverantörers agenter får behörigheter i EU:s kritiska system. **I och med omorganiseringen av värdekedjorna och de tekniska sprången har kinesiska och amerikanska lösningar blivit jämbördiga.**

I både privata och offentliga organisationer används AI-agenter för dataanalys, riskhantering och stöd för beslutsfattande. *Cybertvillingar* modellerar virtuella försvarssystem i realtid. Med hjälp av simuleringarna genomförs förutseende analys för att förebygga och täppa till dataläckor. Att sprida ut data samt begränsa huvudanvändare och åtkomst är fortfarande centrala anpassningsmekanismer.

AI-tillämpningar för naturligt språk har blivit vardag inom programmering, vilket skapar problem med kontroll och hantering. De största organisationerna (till exempel försvarsförvaltningar) upprätthåller **moralisk, ideologisk och juridisk programmering** i AI-agenternas ekosystem. Den används för att kalibrera agenterna så att de agerar transparent gentemot myndigheterna och för att vaccinera dem mot extern påverkan och försök att påverka dem genom programmering.

Kvantkapplöpningen är nästa strategiska spetsområde

Kvanttekniken har gått från försöksstadiet till att bli en strategisk resurs som, i och med att stormakterna har blivit jämnstarka inom AI, utvecklas mot militära tillämpningar. Hotet om kvantöverlägsenhet har gjort utvecklingen av kvantsäkra algoritmer till ett spetsprojekt för försvaret i väst, och de mest kritiska datalagren har skyddats med krypteringsalgoritmer som är starkare än tidigare kryptografiska lösningar. Misstro förekommer även inom blocken, eftersom det har kommit fram exempel på att tekniska genombrott har använts för militära ändamål och underrättelseändamål, till och med för att spionera på egna allierades uppgifter.

Uppkopplad försvarsinfrastruktur skapar nya risker

Världen har gått in i en tid där 6G, programvarustyrda nät och satellitbredband har gjort förbindelserna inom geopolitiska block med skilda standarder nästan fördröjningsfria och med stor kapacitet. **Information rör sig dock inte längre fritt när USA:s, Kinas och EU:s tekniska strukturer har glidit isär.** För försvarsändamål kompletteras EU:s IRIS²-satellitkapacitet med satelliter från amerikanska tjänsteleverantörer. I satelliterna **byggs aktivt teknik med dubbla användningsområden in för att effektivisera övervakningen både inom området och utåt.** EU:s satellitfunktioner är beroende av amerikanska företags verksamhet.

Samhällets digitala beroende har ökat, och funktioner som är kritiska för försörjningsberedskapen styrs i allt högre grad av AI-system som svar på den kortare responstid som autonoma angrepp har lett till. I och med att en beräkningsintensiv, AI-assisterad digital försvarsinfrastruktur byggs upp – tillsammans med de energiintensiva datacentraler som upprätthåller den – **blir energisystemet samhällets mest kritiska knutpunkt.**

Det växande antalet edge-enheter i nätet är ett kritiskt och växande problem, eftersom de behandlar känsliga data om samhällets sårbarhetsyta och därför ständigt utsätts för angrepp. **Lösningar som fungerar oavsett plattform används för att öka flexibiliteten och minska låsningen till vissa kritiska system.** I västländerna anpassas de för flexibel överföring av data och funktioner mellan tjänsteleverantörer. **Satellitförbindelser har blivit en central hotvektor, eftersom de används som ersättande kapacitet när sabotage orsakar störningar i fysiska förbindelser.**

Extern informationspåverkan stävjas med kraft

Digitala informationskanaler och plattformar står starkt under stormaktsblockens ideologiska kontroll, och för användaren är internet inte längre genuint globalt. **Det internet som medborgarna upplever behåller en skenbar frihet,** men är i praktiken en noggrant styrd och **filtrerad verklighet**. I de geopolitiska blocken skriver AI-assistenter långsamt om historien, och information som ifrågasätter ideologin försvinner.

AI, syntetiska medier och deepfake-teknik används både för att trygga informationsmiljön och för att angripa den. Mot geopolitiska propagandavågor försvarar man sig genom att **låta AI-assistenter aktivt censurera innehåll på plattformar som bygger på massiva mängder användardata och personaliseringsdata. Med hjälp av mikroriktning sprids innehåll och en världsbild som upprätthåller en västerländsk identitet.**

Den statliga kontrollen över informationsmiljöerna ökar, och myndigheterna använder filtrering, prioritering och modifiering av innehåll. Inom utbildning satsar man på undervisning i informationsläskunnighet. Företag förutsätts ha bättre beredskap och skydda information även i informationsdimensionen. Vilseledande gemenskaper och påverkansnätverk identifieras och deras synlighet begränsas aktivt. **Censuren av externa spridare av desinformation utvidgas till interna oliktänkande, och sanningen fördunklas ofta i den nationella säkerhetens namn.**

EU:s roll och genomslagskraft i styrningen av informationsmiljön är oklar i förhållande till plattformarnas administratörer, eftersom all information förmedlas till USA:s underrättelsetjänst via storföretag och specialiserade analysföretag inom säkerhetssektorn. Detta accepteras som en nödvändig uppoffring för att upprätthålla EU:s yttre och inre säkerhet.

Övervakningen ökar, motståndet tilltar

Frikopplingen från Kinas leveranskedjor har höjt konsumentpriserna betydligt i västländerna. Samtidigt kräver försvarsutgifterna sitt, den nationella sammanhållningen försvagas i EU-länderna i takt med den samhälleliga ojämlikheten och medborgarnas digitala vardag styrs allt mer säkerhetsbaserat. Listan över godkända applikationer och enheter har begränsats, och i västländerna tillåts endast EU-validerade amerikanska lösningar. **Användargränssnittens funktioner begränsas för att förhindra missbruk**, och personliga AI-system övervakar användarnas aktivitet för att upptäcka avvikelser. Identifiering via hudkontakt, till exempel med hjälp av smarta textilier och wearables, utvecklas som en lösning för säkerhet och identifiering.

För vissa blir säkerhet ett levnadssätt, för andra en tändande gnista till uppror. AI-baserade övervakningssystem används för att identifiera externa källor till desinformation och interna hot inom det egna blocket. Medvetna användare försöker på olika vägar få tillgång till friare information mot betalning, medan den likgiltiga majoriteten i sin tur tar till sig en trygg och filtrerad världsbild. Kritiska medborgare försöker kringgå begränsningarna genom att söka sig till inofficiella, utländska plattformar för att ta del av alternativa nyheter. På så sätt kan användargrupper omedvetet hamna på **utländska plattformar som är riktade till dem och utformade för att se västerländska ut, men som samlar in och sprider information för geopolitiska statsaktörer**.

Angreppsyta: Cyberfysiska fästningar under AI-övervakning

- Gränserna mellan cyberförsvar och cyberangrepp har i praktiken försvunnit. I den cyberdimension som präglas av geopolitisk skärpning kämpar AI-agenter mot varandra och försöker påverka varandras programmering och träningsdata.
- Västländerna har befäst samhällets kritiska, uppkopplade system bakom kvantsäkra digitala skyddsmurar som övervakas med hjälp av AI och upprätthålls av stora teknikföretag.
- Genom AI-assisterad motståndskraft i realtid konkretiseras samhällets digitala säkerhet i den infrastruktur som försvars-AI bygger på, till exempel el-, datacentral-, satellit- och kabelhelheter. *Virtuella SOC:er* som övervakas av människor och drivs av försvarsagenter och AI-system blir vanligare.
- Den ökade uppkopplingen omfattar olika samhällsområden, från digitala gränsövervakningssystem till fabrikernas OT-system. System som har härdats i fråga om både mjukvara och hårdvara ökar behovet av att särskilt eliminera användarrelaterade risker, social engineering och insiderhot.
- Användarnas aktivitet övervakas med hjälp av AI för att upptäcka avvikelser och identifiera interna hot. Övervakningen utförs av specialiserade amerikanska analysföretag. Informationssäkerhetsföretag har dessutom skyldighet att lämna ut uppgifter om misstänkt aktivitet hos användare.
- Övervakningen av användare konkretiseras i godkända smarta enheter som anses informationssäkra och som har inbyggd mjukvara med bakdörrar. Via dessa enheter används digitala bastjänster och bland annat personliga AI-assistenter.
- Användarnas skyldighet att hålla sina enheter uppdaterade har fått större betydelse, och kunskapen om detta har ökat. Tillåten aktivitet och tillåtna enheter begränsas avsevärt, vilket användaren inte nödvändigtvis märker på grund av den rådande censuren.
- När IT-företag anställer personal genomförs screening som bygger på omfattande analys och beteendedata för att identifiera personer som lämpar sig för olika nivåer. Ett enda felsteg i historiken på sociala medier, en snedvridning i urvalsalgoritmen eller falskt innehåll som skapats om en person kan, när data kombineras, identifieras som ett hinder för anställning.

Hot: Statsaktörer slår mot kritisk infrastruktur

- Knutpunkter i de digitala tvillingar och cybertvillingar som hanterar system som övervakas av *säkerhets-AI* blir mål för statsaktörers cyber- och hybridpåverkan. Via dessa knutpunkter försöker angriparna slå ut nivån för autonomt cyberförsvar. Utifrån kartläggning av systemet kan påverkansåtgärder riktas mot en enskild agent. När effekterna sprids nedströms genom andra agenter kan de leda till snöbollseffekter. Även manipulering av träningsdata för tillämpningar för försvar ingår i verktygslådan. Det är inte alltid möjligt att skala upp människors medverkan i beslutsfattandet tillräckligt, vilket ökar oförutsägbarheten.
- I de smarta näten i de energisystem som upprätthåller samhällenas cyberförsvar medför OT-system och edge-enheter bakdörrsrisker genom AI-gränssnitten.
- Historiska, känsliga användaruppgifter som avslöjas när kvantkrypteringar knäcks utnyttjas av samarbetspartner i västländerna för att i spionage- och sabotagesyfte utpressa och manipulera personer som arbetar inom kritiska säkerhetssystem.
- Hacktivister som styrs av auktoritära stater försöker radikalisera ett västfientligt skuggsamhälle genom att hänvisa till ökad samhällsövervakning och informationsmanipulation. Skuggsamhället kan sedan mobiliseras mot infrastruktur och som insideraktörer i kritiska företag.
- Mellan blocken utsätts satellit- och rymdprogram för spionage och aktiva sabotageförsök med cybermetoder.
- Statsaktörers AI-agenter, som programmerats för autonom sårbarhetskartläggning och för att bygga lämplig skadlig kod för angreppsändamål, kan släppas lös i geopolitiska blocks offensiva operationer utan tillräckliga spärrar, vilket kan leda till betydande sidoskador och spridning även i de egna leveranskedjorna.
- I proxykonflikter mellan geopolitiska intressesfärer utvecklas autonoma drönare för maktanvändning snabbt. APT-aktörer försöker förgifta sådana drönare när de används inom EU-området i autonom gränsövervakning och polisverksamhet.
- När kritiska funktioner blir allt mer uppkopplade kan till och med automatiserade komponenter inom jordbruket – från autonoma enheter på gårdar till växthus – utnyttjas av APT-aktörer som vägar för att destabilisera samhällen.

TRAFICOM

/DATAIMPERIER 2035/

Utvecklingen och uppkopplingen är gränslös.

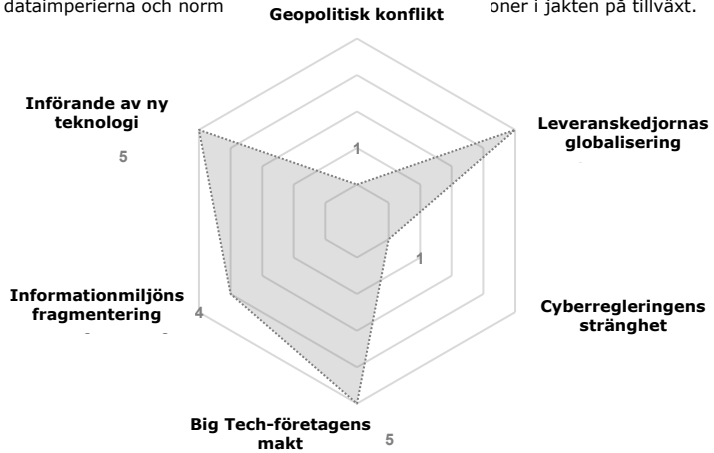
AI-modeller har blivit vanligare tack vare ökad tillgång till mångsidiga data och bättre rörlighet för data. Dataimperierna upprätthåller Mind²-miljöer som byggs upp kring modellerna. De hanterar användardata globalt och vet mer om individer än de offentliga förvaltningarna eller användarna själva. En betydande del av världens befolkning åtnjuter smarta hem-bekvämligheter som är kopplade till AI-system, **och kroppsburna enheter är lika vanliga som smarttelefoner.** Amerikanska företag ligger i framkant inom utvecklingen av kvantteknik. **Företag och organisationer har i stor utsträckning övergått till kryptering som tål kvantberäkning, efter att dataimperierna har infört PQC-algoritmer i sina system.** Rymdtekniken har blivit en arena för konkurrens i takt med att underrättelseverksamhet, strategisk upprustning och satellittjänster har fått större betydelse.

Människor lever i sina personliga spegelsalar.

Användarna har sökt sig till stora tjänsteleverantörers Mind²-miljöer: **sensor- och AI-baserade realtidsmiljöer som erbjuder ett heltäckande digitalt liv.** Dataimperierna konkurrerar genom att låsa in användare i sina miljöer. Att lämna ut biometriska data för monitorering är en vanlig väg till billigare, bättre och mer riktade tjänster. **De verkligheter som människor upplever fragmenteras beroende på inkomstnivå och vilket ekosystem de använder.** Dataimperiernas plattformar ger människor tillgång till personliga AI-assistenter och applikationsutveckling på begäran. **Samtidigt formar plattformarna beteendet hos de användare som interagerar med dem så att det motsvarar annonsörernas och administratörernas mål.** När gränssnitt för naturligt språk och syntetisk kommunikation sprids försvagas människors kritiska tänkande.

Storföretagen söker oberoende från stater

Stora teknikföretag utvidgar sina monopol och sitt inflytande. Med deras hjälp har USA befäst sin ställning som centrum för teknik och standarder, men **det politiska inflytandet har förskjutits till dataimperiernas slutna beslutsrum**. Kina håller på att gå om USA genom sina tekniska framsteg, sitt ägande av resurser och produktion samt sin växande inflytelsesfär. Dataimperierna förvaltar de största globala interaktionsplattformarna, och AI-utvecklingen har stärkt deras position. De utnyttjar denna position för att **påverka val och politik runt om i världen** och skapa en verksamhetsmiljö som gynnar dem i jakten på tillväxt och resurser. EU agerar som kund till dataimperierna och norm oner i jakten på tillväxt.



Endast dataimperierna behärskar den tekniska komplexiteten

De största amerikanska teknikföretagen har cementerat sin ställning i västländerna. De lyckas undgå reglering genom att göra sig oersättliga. Konkurrerande applikationer kopieras till den egna portföljen med hjälp av effektiva kodagenter eller köps upp och försvinner i tysthet. **Därför är det ytterst svårt för EU-företag att lansera egna lösningar.** Kinesiska storföretag har i sin tur brett ut sitt inflytande med stöd av Digital Belt and Roads infrastrukturdiplomati. Största delen av världens befolkning omfattas av deras infrastruktur, som koncentrerar övervakning och beteendedata.

Tillväxten förutsätter obehindrad rörlighet.

I världsekonomins stabila verksamhetsmiljö har tekniska innovationer skapat efterlängtad tillväxt. Tillväxten är dock globalt ojämnt fördelad **och kräver allt mer miljöbelastande resurser för att upprätthållas. Dataimperierna lyckas dämpa protektionismen för att upprätthålla de stabila värdekedjor som tillväxten kräver** och bevara sina kopplingar till världshandeln som är starkt beroende av Kina. Ryssland återintegreras i världsekonomin för att garantera tillgången till billig energi. **De tekniska underleverantörskedjor som byggts upp kring företag från USA och Kina utgör livsvillkor för samhällsekonomierna,** trots att bara företagen själva har förmåga att hantera dem. Staterna har, ända upp till EU-nivå, delats in i företagens ”intressesfärer” utifrån sina huvudsakliga kundrelationer.

När abstraktionsnivån stiger blir regleringen svårare.

Regleringen håller inte jämna steg med storföretagens teknikutveckling. Allt fler offentliga förvaltningar klarar inte av att hantera de allt mer komplexa digitala miljöerna. Dataimperierna utnyttjar sina positioner genom att placera sina egna företrädare i de nationella beslutsorgan och EU-beslutsorgan som är viktigast för dem. **Det parlamentariska beslutsfattandet dikteras allt oftare av de AI-verktyg som dataimperierna har ställt till de offentliga förvaltningarnas förfogande.** Tjänsteleverantörerna ser till att betalningsförmögna kunders data skyddas, medan de sämst ställda har allt sämre möjligheter att få del av den grundläggande informationssäkerhet som regleringen ska garantera. **EU har försvagats som politisk aktör och reglerare,** men myndighetssamarbetet för att skydda vanliga medborgare mot cyberbrottslighet har fördjupats i de områden där dataimperierna inte har något intresse.

Storföretagen söker oberoende från stater

Stora teknikföretag breder ut sina monopol och stärker sitt grepp över hela världen, särskilt med stöd av AI-utvecklingen. Med deras hjälp har USA behållit sin ställning som centrum för teknik och standarder. Kinas tekniska framsteg samt ägande av resurser och produktion har dock ökat, dess applikationer dominerar globalt och dess inflytelsesfär växer genom allianser. **Dataimperierna lyckas dämpa motsättningarna mellan USA och Kina för att upprätthålla stabila värdekedjor** och en världshandel beroende av Kina, vilket krävs för att hålla tillväxten uppe. I västländerna har politiskt inflytande genom byteshandel förskjutits från demokratiskt valda beslutsfattare till ***dataimperiernas*** slutna beslutsrum. Där erbjuder politiker offentliga förvaltningsresurser, gynnsam reglering och internationellt inflytande i utbyte mot status och valfinansiering.

I världsekonomins relativt stabila verksamhetsmiljö har tekniska innovationer skapat efterlängtad tillväxt. Tillväxten är dock globalt ojämnt fördelad och kräver samtidigt allt mer miljöbelastande resurser för att kunna upprätthållas. **Dataimperierna utnyttjar USA:s utrikespolitik för att bygga en verksamhetsmiljö som gynnar dem själva. De söker tillväxtmöjligheter och resurser främst genom opinionskampanjer och vid behov genom indirekta maktmedel.** AI-utvecklingen har stärkt deras position som förvaltare av de största globala interaktionsplattformarna. De utnyttjar denna position för att driva stater bort från marknadsstörande nationalism och påverka val och politik runt om i världen.

EU har tagit med sig 2020-talets reglering in på 2030-talet och **kräver högre säkerhetsstandarder av företag** som är verksamma i EU än vad USA är berett att acceptera. Dataimperierna protesterar mot detta och hotar att begränsa tillgången till teknik, och **EU tvingas ge efter bland annat genom att lätta på AI-regleringen.** Ekonomiska intressen och oro för Europas konkurrenskraft driver in en kil mellan medlemsländerna. Deras intressen glider kraftigt isär, vilket försvagar den gemensamma beslutsförmågan.

Tillväxt förutsätter obehindrad rörlighet

EU klarar inte av att driva en enhetlig infrastrukturpolitik när kinesiska och amerikanska storföretag delar upp marknaderna i ”intressesfärer”. Samtidigt upplevs tjänster och leveranskedjor från USA som opålitliga, eftersom de upprepade gånger har använts som geopolitisk hävstång under 2020-talet. Kina utnyttjar därför situationen och erbjuder västländerna mer avancerad teknik i stället för den amerikanska.

Dataimperierna lägger ständigt beslag på allt mer data, beräkningskraft och de senaste chippen, vilket håller priserna och de senaste tillämpningarna utom räckhåll för mindre aktörer. De har utnyttjat de data de samlat in för att monopolisera programvaruutvecklingen med hjälp av sina AI-kodagenter. EU väljer att balansera mellan stormakternas tjänsteleverantörer och **söker de bästa lösningarna på marknaderna i både USA och Kina genom en medelväg mellan ekonomisk pragmatism och säkerhetsöverväganden.**

EU ligger efter i utvecklingen och vill inte låsa sig ute från några nätverk när unionen söker tillväxtmöjligheter som den tekniska utvecklingen erbjuder. **I praktiken är EU:s mest kritiska molninfrastruktur fortfarande europeisk eller amerikansk, men till exempel på konsumentsidan används mycket kinesisk infrastruktur och många kinesiska tillämpningar.**

Få behärskar den tekniska komplexiteten

Dataimperiernas makt och rikedom har byggts upp kring ständig tillväxt, komplexa leveranskedjor som de senaste tekniska lösningarna kräver samt behovet av att koncentrera resurser och energi. I takt med AI-utvecklingen har samhällenas tjänsteutbud koncentrerats enligt skalfördelarna i dataimperiernas datainfrastrukturer. Underleverantörskedjorna kring storföretag från USA och Kina utgör i praktiken livsvillkor för de samhällsekonomier som är deras kunder, trots att bara företagen själva har en helhetsbild av dem och förmåga att hantera dem.

Särskilt företag som har byggt AI-tjänster i USA har lyckats befästa sitt inflytande över hur konsumenter och lagstiftare agerar och fattar beslut i alla västländer. De lyckas motverka regleringssträvanden genom att hålla sig i den tekniska utvecklingens framkant, sträcka ut sina tentakler i samhällena och göra sig oersättliga. AI-assisterade framsteg inom programmeringsautomation har koncentrerat inflytandet ytterligare till de största hyperskalarna. Det försvagade konkurrensläget har gjort många tjänster betydligt sämre ur användarens perspektiv. Nya konkurrenter försöker därför aktivt utmana dataimperiernas monopol. **Nya innovationer utsätts dock för direkt spionage när utvecklingsarbetet sker på dataimperiernas egna plattformar.** För att skydda de egna lösningarnas ställning utnyttjar dataimperierna möjliga konkurrenters teknik i den egna portföljen eller köper upp den och låter den försvinna i tysthet. Det är svårt för EU-företag att lansera sina egna lösningar på marknaden. **Datahemvisten finns i storföretagens hemländer.**

Kinesiska storföretag har spridit sitt inflytande särskilt i länder i det globala syd med stöd av Digital Belt and Roads infrastrukturdiplomati. Största delen av världens befolkning står direkt under inflytande av deras applikationer och infrastruktur, som används för att centralisera övervakning och beteendedata. Med stöd av den kinesiska staten hindrar de västerländska företag från att etablera sig i deras intressesfär. Samtidigt försöker de ta marknadsandelar från dessa företag även i demokratier genom att framställa sina tjänster som ett alternativ till västvärldens *privata övervakningskapitalism* och som ett sätt att möjliggöra *ett liv som är värdefullt* för staten och samhället.

När abstraktionsnivån stiger blir regleringen svårare

Regleringen håller inte jämna steg med storföretagens teknikutveckling, och **när digitalisering och effektivisering av samhällena blir självändamål trängs nationalstatens uppgifter undan**. Allt fler offentliga förvaltningar klarar inte av att hantera de allt mer komplexa digitala miljöerna. Dataimperierna börjar utnyttja regleringsvakuumet **genom att försöka placera sina egna företrädare eller anställda i de nationella beslutsorgan och EU-beslutsorgan som är viktigast för dem. När de upplever att regleringen hotar deras makt och affärsverksamhet driver de effektiva opinionskampanjer och bedriver lobbyverksamhet** för att få sin vilja igenom. Det parlamentariska beslutsfattandet och underlagen dikteras allt oftare av dataimperiernas AI-verktyg. AI-genererat material jämställs med expertkunskap, och samråden minskar.

EU har försvagats som politisk aktör, men myndigheterna samarbetar allt tätare i det operativa arbetet med att skydda medborgarna mot cyberbrottslighet. **Tjänsteleverantörerna ser till att betalningsförmögna kunders data skyddas, medan de sämst ställda har allt sämre möjligheter att få del av den grundläggande informationssäkerhet som regleringen ska garantera.**

Den nya teknokratins murar byggs med AI-skalning som utgångspunkt

AI-modeller har blivit vanligare i globala datanät tack vare ökad tillgång till mångsidiga data och bättre rörlighet för data. Aktörerna bakom dem hanterar användardata globalt och vet mer om individer än de offentliga förvaltningarna eller användarna själva. **I demokratier har beslutsfattande flyttats över till algoritmstyrning genom förvaltningens nya användargränssnitt.** AI-systemen innehåller vanligen bakdörrar som är tillgängliga för dataimperierna eller inte möjliga för myndigheterna att auditera. När autonom teknik flyttas in i svarta lådor **blir det svårare att bedöma de egentliga syftena med tillämpningarna och agenterna samt relaterade ansvars-, säkerhets- och integritetsfrågor.** Med stormakternas medverkan eller i samarbete med lokala förvaltningar kan plattformarna också blockera innehåll, styra opinioner eller utöva ekonomiska påtryckningar i ett visst område.

Fenomenet vendor lock-in har vuxit **när storföretagens egna kodagenter har grävt sig in i organisationernas leveranskedjor för att själva bygga system som bara passar en viss organisations leveranskedja. Dataimperierna hindrar varandras agenter från att fungera genom att begränsa deras behörigheter och bygger gränssnitt endast med sina egna samarbetspartner.** Programmeringen koncentreras till hyperskalarna när autonoma kodagenter svetsar samman systemens olika delar och optimerar verksamheten i realtid, bland annat i cyberfysiska miljöer. Genom sin självlärande förmåga gör arrangemanget det möjligt att snabbt omdirigera leveranskedjorna vid störningar. **Införandet av kodagenter leder till omfattande arbetslöshet, och ojämlikheten ökar allt snabbare.**

I jakt på kvantinnovationer

När AI-systemen har etablerat sig i samhällena väcker kvantberäkning dataimperiernas intresse, eftersom den är mer energieffektiv än halvledarbaserade lösningar. Dataimperierna försöker **kombinera kvantalgoritmer med maskininlärningsprogram.** Kvantberäkning via QCaaS-tjänster har gett betydande fördelar inom läkemedels- och logistiksektorerna. **Amerikanska ligger i framkant i utvecklingen efter att ha införlivat EU-företagens förmågor i sina portföljer, medan kinesiska företag håller sig hack i häl.** Organisationerna har övergått till kvantresistent kryptering i och med att dataimperierna har infört PQC-algoritmer.

Gränslös tillväxt och uppkoppling kräver resurser

De största AI-tillämpningarna har stött på problemet att offentliga träningsdata håller på att ta slut. **Som lösning på nästa steg paketeras dataimperiernas mångsidiga tjänster via ett enda användargränssnitt till ”kollektiva hjärnor” (*Mind²*). Användarna ansluter sig till dem med hjälp av kroppsburen teknik och biometriska chip.** Via AI-agenter samlar användargränssnittet in data om interaktioner och kroppsfunktioner för träningsändamål och skapar på så sätt en ”kollektiv” förståelse i realtid mellan användarna. **En betydande del av världens befolkning åtnjuter smarta hem-bekvämligheter, och kroppsburna enheter är lika vanliga som smarttelefoner.** 6G-nätet kopplar samman satelliter, obemannade luftfarkoster, markbaserade basstationer och IoT-enheter till en sömlös helhet. Styrningen av nätet bygger på AI och maskininlärning som optimerar resurserna i realtid. **AR-, VR- och metaversummiljöer fungerar utan fördröjning.**

Dataimperiernas kollektiva hjärnor med sina förgreningar bygger på en enorm infrastruktur i den fysiska världen och på den energi och de komponenter som infrastrukturen ständigt kräver. Jakten på tillväxt fortsätter oavsett energiform och utan hänsyn till klimatet. **Rymdtekniken har blivit en viktig arena för företagskonkurrens** i takt med att underrättelseverksamhet, strategisk upprustning och satellittjänster har fått större betydelse. **Beräkningskapacitet flyttas upp i omloppsbana med datacentersatelliter**, samtidigt som utvecklingen inom paneltekniken ger satelliterna bättre energiförsörjning. Dataimperiernas tillväxt förutsätter mineraler. Därför utvecklas **teknik för asteroidbrytning för att trygga råvaruflödena.**

Betalningsförmåga ger en väg ut ur manipulationens värld

Den snabba AI-utvecklingen och kopplingen av syntetiska innehållsproducenter till plattformarna har haft sitt pris, och det öppna internet har fyllts av svårkontrollerat digitalt avfall. Som en följd av detta har **användarna sökt sig till de stora tjänsteleverantörernas *Mind²-miljöer för superappar*, där kvaliteten kontrolleras av AI-assistenter och AI-kuratering.** Miljöerna erbjuder människor en fungerande och trygg digital tillvaro samt källor som har verifierats av andra användare, i olika prisklasser. Tänkandet formas genom de ”kollektiva hjärnorna” och under deras påverkan, och betalningsförmågan avgör vem som får tillgång till den bästa förståelsen.

En gemensam syn på världen hör 2020-talet till. Dataimperierna har sedan dess inhägnat privat och offentlig information samt användare i heltäckande informationsmiljöer som bara de själva har tillgång till. De verkligheter som människor upplever **fragmenteras beroende på inkomstnivå och vilket AI-ekosystem de använder.** Användare på premiumnivå betalar för att forma sina informationsmiljöer enligt egna önskemål och skiljer ut sig som en elit. **Företagen strävar särskilt efter att vinna uppskattning hos dessa ”högvärdesanvändare”, och deras informationssäkerhet tas om hand.** ”Informationsmedelklassen” väljer en heltäckande livsstil med metaversum, baserad på individuell och personifierad algoritmisk styrning med stöd av AI-assistenter. De som har valt att stå utanför AI-miljöerna föredrar enskilda medier bakom betalvägg eller söker sig till dark web och andra alternativa miljöer för att leta efter *”sanningen”*. När ett ständigt anpassningsbart naturligt språk och människolik syntetisk kommunikation blir vanligare försvagas det kritiska tänkandet, **vilket stärker kraften i de tankar som matas till människor.**

Små statsblock kan verifiera tillförlitlig information internt, **men i det stora hela är informationshantering inte längre möjlig när dataimperierna har inhägnat de digitala allmänningarna.** Inom statsförvaltningarna fokuserar man på information som kan bekräftas som fakta i den verkliga världen.

Människor lever i sina personliga spegelsalar

Dataimperierna låser in så många användare som möjligt på sina plattformar och i sina miljöer för att samla in allt mer data om dem och styra deras beteende. Tekniken blir en religionsliknande livsstil, där ett algoritmstyrt liv är ett eftersträvansvärt tillstånd. **För utlämnande av data används kontinuerliga gränssnitt, från AI-assistenter till sensorer.** Företagen utvecklar snabbt LBM-lösningar (*large behavior models*), som bygger på sensorer i kroppsburen teknik. Sensorer och enheter kopplas till miljöer för superappar på olika betalnivåer för att förbättra personifieringen av tjänsterna. Att lämna ut biometriska data för monitorering är en vanlig väg till billigare, bättre och mer riktade tjänster, som kan genereras via dataimperiernas appbutik och en personlig assistentagent.

Freemium-användare är föremål för reklam och bottar och lämnar ut sina data i utbyte mot tjänster. **Gratisversioner av AI-assistenter fungerar som personliga följeslagare och formar konsumenternas beteende** enligt de annonserande företagens mål. Applikationer som genereras av gratisanvändare innehåller djupt personaliserade annonser. Till följd av manipulationen börjar användarna ta efter AI-systemens sätt att fungera. I de högre betalnivåerna ingår däremot betoning av unika drag, upplevelser av mänsklighet och bättre skräddarsydda egenproducerade applikationer.

Dataimperierna isolerar människor från deras nationalstater och andra gemenskaper och för över de mest produktiva delarna av deras kognition till sina egna gränssnitt och användargränssnitt. Dark web och alternativa gemenskaper används aktivt som tillflyktsorter från den totala synligheten i den digitala världen. Det polerade digitala livet med sina livsgränssnitt står i stark kontrast till **den fysiska världen, som allt mer plågas av extrema väderfenomen, ökande flyktingskap, ojämlikhet och lokala resurskonflikter.**

Angreppsyta: Uppkopplingen går på högvarv

- Dataimperierna, som fungerar som de viktigaste producenterna av säkerhet, koncentrerar betydande resurser på att skydda de viktigaste datalagren i Mind²-helheterna. De samlar också de bästa rutinerna för informationssäkerhet och upptäckta svagheter som affärshemligheter. Med hjälp av AI har teknikjättarna allt bättre sätt att avvärja traditionella angrepp, men de har liten motivation att skydda andra än sina egna premiumanvändare och system.
- Den ökade uppkopplingen har gett cyberkriminella större möjligheter att påverka användarnas liv på ett intimt plan. En vardag som kompletteras med olika enheter är beroende av många slags gränssnitt och enheter som är kopplade till användarens person och ökar sårbarheterna.
- Den breda integreringen av AI i kärnverksamheter har koncentrerat känsliga data i specialiserade system inom organisationer, vilket gör dem till attraktiva mål. Medborgarna profileras allt mer exakt i livets användargränssnitt, och integritetsskydd kan köpas som en lyxprodukt. Små och medelstora företag har problem med att skydda sina data när säker databehandling har blivit dyrt.
- Statsaktörer fokuserar i cyberdimensionen på att bekämpa cyberbrottslighet genom internationellt samarbete och på att föra cybersäkerhet dit dataimperierna inte har utvidgat sin verksamhet. APT-aktörer fokuserar på informationsinhämtning och industrispionage.
- Regleringen, som har halkat efter den tekniska utvecklingen, har försvagat rätten till dataskydd och informationssäkerhet för dem som står utanför dataimperiernas ekosystem. Cyberkriminella utvidgar sin verksamhet till områden där dataimperierna inte har ekonomisk motivation eller regleringsskyldighet att sprida sina skyddsnät.
- Företagen anklagar staterna för att politisera tekniken och betonar att de skyddar sina användare, samtidigt som de skymmer insynen i sin egen verksamhet.
- I takt med den ökade uppkopplingen blir dataimperiernas ständigt uppdaterade realtidsdatamassor referenspunkten för all programmering och kod, och AI-agenter bygger autonomt upp system utifrån dessa datamassor. Historisk information, äldre webbplatser och innehåll samt bästa praxis riskerar att gå förlorade.

Hot: AI-datafiering leder till nya former av brottslighet

- Cyberkriminella riktar i första hand in sig på dataimperiernas många underleverantörer i leveranskedjorna för att stjäla de personaliseringsdata som dessa har samlat in.
- Kriminella använder kodagenter för att skapa mikroriktade falska versioner som imiterar Mind²-gränssnitt och Mind²-tjänster. Versionerna släpps ut i syfte att stjäla användaruppgifter. När sensorer och digitala angreppsytor i den digitala livsstilen omfattar allt från vanliga hemrobotar till AI-assistenter och biometriska chip, gör sammanställningen av data det möjligt att skapa virtuella kopior av människor. På officiella plattformar går kopiorna för att vara äkta och kan användas för många slags kriminella syften.
- Exempel: Lifestyle-gränssnitt som blivit vanliga i Mind²-miljöer har samlat in uppgifter om premiumanvändares beteende och position, och intrång i databaserna gör det möjligt att personalisera cyberangrepp. Uppgifterna säljs på dark web. Genom att klona premiumanvändares konton försöker angripare också komma nära dataimperiernas förmögna användare i bedrägerisyfte.
- Angripare kan till och med bryta igenom dataimperiernas säkerhetsarrangemang genom att utnyttja oväntade angreppsvektorer, såsom föråldrad information och nolldagssårbarheter som självlärande system inte har sett i sina träningsdata. En injektionsattack som bygger på gamla programvarubibliotek kan via legacy-system i leveranskedjan riktas mot kodagenter och få hela leveranskedjan att kollapsa.
- Plattformsbolagens avancerade skyddsmekanismer, modereringen av informationsmiljön och de ökade kostnaderna för att genomföra lyckade angrepp har lett till att verkningsfull och synlig hacktivism har försvunnit. Aktivister och religiösa aktörer som motsätter sig AI-livsstilen angriper infrastrukturen genom fysiskt sabotage. Den angrips också av aktivister i geografiska krisområden som drabbas av *resursimperialism* till följd av utbyggnaden av beräkningskapaciteten. Följden blir oväntade avbrott i samhällets kritiska tjänster.
- AI-utvecklingen har lett till fler uppsägningar inom IT-branschen, vilket avsevärt har ökat insiderhotet. På dark web försöker kriminella organisationer rekrytera tidigare anställda vid dataimperierna.

Om man kan föreställa sig det, kan man förbereda sig på det.

Traficoms teknologi- och strategifunktion

ennakointi@traficom.fi

Kirsi Karlamaa, Teknologi- och strategidirektör
Aleksi Blomqvist, Specialsakkunnig
Paul Hermansson, Specialsakkunnig
Henri Jokinen, Specialsakkunnig
Markus Mettälä, Specialsakkunnig