Cybersäkerhetsscenarierna 2035 – ledningens sammanfattning

Förord

Cybersäkerhetsscenarierna 2035 beskriver fyra alternativa framtida världar där den accelererande tekniska utvecklingen, de ömsesidiga beroendena, storföretagens makt och hur väl regleringen lyckas formar framtidens cybermiljö på mycket olika sätt.

Syftet med scenarioarbetet är att erbjuda ett verktyg för att förstå alternativa utvecklingsvägar och deras konsekvenser för olika organisationer och aktörer. Arbetet speglar en ovanligt bred expertbild: över 200 experter från den offentliga och privata sektorn, den akademiska världen, internationella partnernätverk och det civila samhället har medverkat.

De mest kritiska riskerna kan uppstå när tekniskt beroende, svag hantering, urholkad identitet och integrationen mellan den fysiska och den digitala världen koncentreras och ackumuleras. Cybersäkerhetens framtid avgörs sannolikt i allt högre grad av hur beroenden, förtroende och makt är strukturerade. I alla scenarier blir AI, leveranskedjor, informationsmiljöns tillförlitlighet och den kritiska infrastrukturens uppkoppling avgörande frågor.

Cybersäkerhetsscenarierna stöder beredskap, beslutsfattande och strategisk diskussion i ett läge där säkerheten i framtidens digitala samhälle vilar på allt mer komplexa beroenden.

Cybersäkerhetsscenarierna 2035 är en del av genomförandet av Finlands cybersäkerhetsstrategi. Beredskap inför framtiden och den strategiska framsyn som anknyter till detta är också en av tyngdpunkterna i Transport- och kommunikationsverket Traficoms strategi.

Kirsi Karlamaa
Teknologi- och strategidirektör

TRAFICOM
Transport- och kommunikationsverket

Centrala iakttagelser

1. AI:s växande integration i samhället kan förändra cybersäkerhetens karaktär till en infrastrukturfråga. I centrum står data, beräkning, ledningsskikt och agentekosystem samt deras kopplingar till kritiska processer.

2. Informationsmiljöns tillförlitlighet står i centrum för cybersäkerheten i alla scenarier.

3. Framtidens hotaktörer kan till stor del vara desamma som idag. Deras inflytande beror på resurser och förmåga att agera i olika tekniska miljöer.

4. Koncentration eller splittring av tekniker kan skapa olika riskprofiler.

5. 6G, rymdteknik och kvantteknik kan förändra cybermiljöns struktur. De ökar både resiliensen och risken för systemiska störningar.

6. De största framtida riskerna kan uppstå när osäkerheter koncentreras och ackumuleras. De allvarligaste situationerna kan uppstå när autonomi, centraliserad infrastruktur, integrationen mellan den fysiska och den digitala världen, identitetens urholkning och bristande hantering flätas samman.

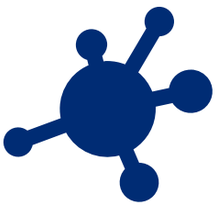
Fyra framtida världar

Fackelbäraren

I Fackelbäraren är världen fortfarande geopolitiskt spänd och leveranskedjorna har delvis regionaliserats. EU fungerar som fastställare av reglering och standarder för teknik och cybersäkerhet och bygger en ”tredje väg” mellan USA:s och Kinas modeller, med betoning på demokrati och integritetsskydd. Stark autentisering, EU-molnet och regleringsenliga datalösningar utgör miniminivån för säkerhet.

I detta scenario försöker man förhindra att informationsmiljön fragmenteras. Plattformarna avkrävs transparens och att skilja mellan syntetiskt och organiskt innehåll, och för medborgarna byggs miljöer med verifierad information bakom stark autentisering. Samtidigt är modellens baksida att vissa aktörer uppfattar detta som censur eller som en alltför styrande ”EU-verklighet”.

Den tekniska utvecklingen stannar inte upp, men införandet blir mer återhållsamt. Den överhettade hypen kring stora språkmodeller inom AI har avtagit. EU lyckas förbättra sin självförsörjning inom moln, AI, kvantteknik, 6G och rymdteknik. Detta undanröjer inte hoten, men gör dem mer hanterbara.



Fragmentering

I Fragmentering driver världen mot block, leveranskedjorna regionaliseras och EU förlorar sin förmåga att forma en gemensam linje för digitalisering och infrastruktur. Medlemsländerna delas upp i olika läger, storföretagen bromsar regleringen och den tekniska utvecklingen går framåt i ojämn takt. Resultatet är en lapptäcksliknande infrastruktur där interoperabilitet, hantering och förtroende försvagas.

I centrum för detta scenario står förtroendets kollaps. Det öppna internet blir en miljö mättad av syntetiskt innehåll, manipulation och bedrägerier, och människor och organisationer drar sig tillbaka till mer slutna lösningar. På olika plattformar uppstår olika sanningsgrunder, och den gemensamma kunskapsgrunden vittrar sönder. Samtidigt börjar medborgarna också aktivt motsätta sig systemen, till exempel genom motåtgärder som förgiftning av sensorer och smarta funktioner.

I denna värld har AI införts för snabbt och med alltför svag styrning. ”AI-katastrofer” har lett till läckor av känsliga uppgifter, manipulation och reverse engineering. Till följd av detta försvagas förtroendet för att lämna ut data och införandet bromsas upp. Teknik används visserligen, men mer försiktigt, snävare och med större misstro. Samtidigt fortsätter hotaktörer att utnyttja AI aggressivt.

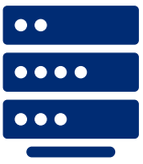
Trots misstron minskar beroendena inte, utan fördjupas. Teknikjättarna och de stora leverantörerna blir i praktiken de enda aktörerna som kan garantera digital kontinuitet, även om deras makt och legitimitet samtidigt urholkas.

Två maktsfärer

Två maktsfärer beskriver en värld där den globala digitala infrastrukturen har delats upp i två stormaktsledda block. USA försöker frigöra sig från leveranskedjor som är beroende av Kina. Kina är teknologiskt mycket starkt och EU blir säkerhetspolitiskt beroende av teknik och övervakning från USA. EU:s suveränitetsprojekt förblir ofullständiga, även om säkerhetsregleringen skärps.

I denna framtid går säkerhet före integritet. Övervakningen av den digitala infrastrukturen ökar, dataskyddet försvagas och stora tjänsteleverantörer får även övervakningsuppgifter. Informationsmiljön blir styrd, filtrerad och ideologiskt kontrollerad. I den interna och externa säkerhetens namn krymper också utrymmet för oliktänkande.

Teknikens logik är i denna värld kapprustningens logik. Autonoma angrepp och autonomt försvar förkortar responstiderna till ett minimum, funktioner som är kritiska för försörjningsberedskapen börjar vila på AI-styrning, och 6G, satellitbredband och kvantteknik kopplas till säkerhetsarkitekturen. Cybersäkerheten blir en del av det stormaktspolitiska maktspelet.



Dataimperier

I Dataimperier bygger den globala tillväxten på rörlighet, data och företagsledd teknisk integration. Stora teknikföretag lyckas hålla värdekedjorna stabila, dämpa protektionismen och bevara kopplingarna även till den världshandel som är beroende av Kina. Staterna delas i praktiken in i företagens intressesfärer, och EU:s roll förändras från en aktiv reglerare till kund.

Kärnan i detta scenario är maktförskjutning. Den offentliga regleringen håller inte jämna steg med den tekniska abstraktionsnivån och komplexiteten. Därför börjar dataimperierna fylla beslutsstrukturer, påverka politiken och erbjuda även förvaltningen sina egna AI-verktyg. Demokratins former består, men den praktiska styrningen flyttas i allt högre grad till företagsledda svarta lådor.

Medborgarnas vardag bygger i denna värld på slutna miljöer. Biometriska data fungerar som en port till bättre tjänster, det kritiska tänkandet försvagas och de verkligheter som människor upplever skingras beroende på inkomstnivå och vilket ekosystem de använder. Integritet blir en lyxprodukt: det bästa skyddet får man genom att betala, inte som en automatisk rättighet.

Cybersäkerhetens logik är selektiv. Dataimperierna skyddar sina egna datalager och betalningsförmögna kunder starkast, medan grundnivån för andra kan bli svag.