Civila tekniktrender med relevans för cyberförsvar – sammanfattning

Projektet Omvärldsanalys av koncept och teknik för cyberförsvar kartlägger civil kunskap för cyberförsvaret. Detta memo sammanfattar rapporten *Civila tekniktrender med relevans för cyberförsvar – Explorativ analys av trender 2026* (FOI-R--5956--SE).

NIO TEKNIKTRENDER har valts ut baserat på spaningar från några analysföretag. Memoförfattarna har bedömt trenderna utifrån relevansen för Försvarsmakten och särskilt cyberförsvaret. Trenderna är även relevanta för cybersäkerhetsarbete. Utifrån trenderna besvaras följande frågor:

1. Vilka trender beskrivna av analysföretag är relevanta för cyberförsvaret?
2. Vad rekommenderas cyberförsvaret göra för att hantera trenderna?

De flesta av trenderna rör artificiell intelligens (AI) och främst stora språkmodeller i exempelvis chattbottar. Trenderna rör även moln och kryptering. Nedan förklaras varje trend kort, följt av rekommendationer till cyberförsvaret.

Multiagenta system

Enskilda specialiserade AI-agenter har börjat koordineras för att tillsammans utföra arbetsflöden med flera steg och nå mer komplexa mål. Rekommendationer:

R1. Analysera hur multiagenta system kan koordineras utan att kontrollen av agenterna övergår till motståndare.

R2. Analysera hur ett AI-baserat cyberförsvar skulle se ut organisatoriskt när det kompletteras av multiagenta system.

Tillgång till AI-modeller och AI-beräkningskapacitet

Allt mer AI införs vilket kraftigt ökar behovet av beräkningskapacitet. De stora kraven på beräkningskapacitet gör i sin tur att få aktörer kan bygga egna AI-modeller som kan mäta sig med de bästa. Detta ger en utmaning med att få lämplig tillgång till AI-modeller. Rekommendationer:

R3. Analysera för vad det är lämpligt att använda molnbaserade AI-modeller kontra lokala modeller, exempelvis vilken verksamhet som har kortvariga krav på konfidentialitet.

R4. Träna på att upptäcka och känna igen skyddsräcken i AI-modeller och där de ger användarna vilseledande svar.

Molntjänsters utmaningar

Den säkerhetspolitiska utvecklingen ökar behoven av bättre kontroll över data och tjänster, vilket ställer krav på molntjänsterna. Den ökade kontrollen kan delvis hanteras med tekniska lösningar som kryptering, delvis genom att skapa redundans med andra molntjänster eller helt migrera till suveräna eller lokala molnlösningar. Rekommendationer:

R5. Analysera för vilka användningsområden som externa moln kan användas genom konfidentiell databehandling eller annan teknik.

R6. Följ utvecklingen av EU:s Cloud Sovereignty Framework [1], Natos införskaffande av Google Cloud Air-Gapped [2] samt liknande initiativ.

AI-baserad mjukvaruutveckling

Organisationer ser produktivitetsfördelar och lägre kostnader med att utveckla mjukvara med hjälp av AI.
Rekommendationer:

R7. Träna på att hitta sårbarheter i kod skriven med AI-baserad mjukvaruutveckling, med tanke på de särdrag som präglar AI-kod.

R8. Analysera hur kodgranskningskompetens ska upprätthållas på sikt om kodskrivning inte längre prioriteras hos universitet och företag.

R9. Analysera vilka operativa, stödjande och ledande rollers uppgifter som kan försvinna eller flyttas med anledning av AI samt vilka nya roller som kan tillkomma.

AI för cyberförsvar

AI missbrukas allt mer av angripare, vilket också ökar intresset av proaktivt AI-försvar. Rekommendationer:

R10. Skapa förtrogenhet med Nist IR 8596 [3] om försvar och angrepp med och mot AI.

R11. Analysera hur rätt nivå av tillit till AI ska uppnås och vilka typer av fel som AI kommer göra i vilka försvarssituationer.

R12. Analysera vilka försvarsuppgifter som är mest lämpade för AI och vilket behov av specialisering som finns för dessa uppgifter.

FOI Memo: 9333
Forskningsområde: Cyberförsvar och cybersäkerhet
Godkänd av: Foteini Papiri

Digitalt ursprung

Organisationer står inför ökade risker med kodmanipulation och AI-driven desinformation, vilket skapar behov av bättre verifiering hos tredjepartsmjukvara och AI-genererat innehåll. Rekommendationer:

R13. Träna på att motstå AI-baserad social manipulation.
R14. Följ utvecklingen av märkning av AI-genererat innehåll, exempelvis hur arbete fortlöper med EU:s Code of Practice on Marking and Labelling of AI-generated content [4].

Postkvantkryptering

Organisationer har lagt mer fokus på att planera för byten av kryptoalgoritmer, för att motstå de nya angrepp som skulle realiseras med kvantdatorer när dessa når tillräcklig kapacitet. Rekommendationer:

R15. Analysera Nists [5] och NCSC:s [6] vägledningar och notera svåra moment, särskilt i kombination med erfarenheter från tidigare övergångar mellan kryptosystem.

Säkerhet för stora språkmodeller

Nya säkerhetsmekanismer införs för stora språkmodeller som svar på de nya säkerhetsproblem som uppstår när AI-modellerna blir allt mer kraftfulla. Rekommendationer:

R16. Identifiera hur exponering och behörigheter påverkar lämpliga användningsområden för språkmodeller.
R17. Skapa förtrogenhet med angrepp och skydd i Mitre Atlas [7] och i Owasps taxonomi [8].
R18. Testa olika sätt att kringgå stora språkmodellers säkerhetsmekanismer.

Fysisk AI

Organisationer försöker överföra fördelar med rent digital AI till AI som mer interagerar med den fysiska omgivningen, i smarta byggnader, robotar etc. Rekommendationer:

R19. Analysera skillnader mellan försvar av fysisk AI och försvar av traditionella cyberfysiska system.
R20. Analysera varianter av promptinjektion för fysisk AI.
R21. Öva på CEMA (cyber och telekrig) för AI-drönare.

Avslutande ord

De flesta av trenderna rör AI, vilket stämmer väl med den generella omvärldsutvecklingen. De enorma summor som läggs på AI gör det rimligt att dessa trender fortsätter de närmaste åren. De mest populära AI-teknikerna har dock inneboende begränsningar med hallucinationer och svårigheter att skapa en modell av världen. Trenden om moln handlar om något som är relativt moget tekniskt sett, men där utmaningarna handlar om vem som ska ha kontroll över data. Därtill finns trenden om att proaktivt gå över till krypteringsalgoritmer som är säkra mot kvantdatorer, trots att kraftfulla kvantdatorer ännu inte finns.

Försvarsmakten har sedan tidigare strategier som rör trenderna. Förhoppningsvis kan realiseringarna av strategierna stödjas av de rekommendationer som ges här. Dessa rekommendationer rör tre behov:

- Skydda och försvara AI-baserade system eller att nyttja AI för att skydda och försvara.
- Ändra i organisatoriska roller, pga. införandet av AI.
- Uppnå suveränitet utan att gå miste om de positiva effekter som utlovas av AI och andra trender. ■

Författare: Henrik Karlzén och John Ziegenbein.

Referenser

[1] EU, ”Cloud Sovereignty Framework”, v.1.2.1, 2025. https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en
[2] Google, ”Nato and Google Cloud sign multi-million dollar deal for AI-enabled sovereign cloud”, 24 nov 2025. https://www.googlecloudpresscorner.com/2025-11-24-NATO-and-Google-Cloud-Sign-Multi-Million-Dollar-Deal-for-AI-Enabled-Sovereign-Cloud
[3] K. Megas m.fl., ”Cybersecurity Framework Profile for Artificial Intelligence (Cyber AI Profile)”, NIST IR 8596 (Initial preliminary draft). doi:10.6028/NIST.IR.8596.iprd, 2025.
[4] Europeiska kommissionen, ”Second Draft - Code of practice on transparency of AI-generated content”, 2026. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-second-draft-code-practice-marking-and-labelling-ai-generated-content
[5] Nist, ”Transition to Post-Quantum”, NIST Internal Report 8547. doi: 10.6028/NIST.IR.8547.ipd, 2024.
[6] NCSC, ”Nationella rekommendationer för övergången till kvantsäker kryptografi”, 2026.
[7] The MITRE Corporation, ”MITRE ATLAS”, https://atlas.mitre.org [Använd 30 juni 2026.]
[8] Owasp Foundation, ”OWASP Top 10 for LLM Applications 2025”, 2025. https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-v2025.pdf

FOI Memo: 9333
Forskningsområde: Cyberförsvar och cybersäkerhet
Godkänd av: Foteini Papiri