

Framtidens informationsmiljö och icke-statliga aktörer

Lisa Bergsten och Sofia Olsson

2050. Klockan slår 07:00 och ett hologram dyker upp på pucken som står på nattduksbordet. En kvinna med vänligt men obestämt utseende återger nyhetsrubrikerna: ”Fortsatta störningar efter måndagens cyberangrepp. Biometrisk data stulen. Snart kommer värmen.” Du tar på dig glasögonen som ligger på fönsterbrädet ovanför sängen. På glasen projiceras ett meddelande från din kollega. Suck. Han vabbar – igen. Med ögat styr du till ikonen för att svara och pratar sedan rakt ut i luften. Hologram-kvinnan har nu fått sällskap av en gäst. När du talat klart tittar du förstrött mot pucken och tänker på att i din ungdom fanns det något som kallades TV. Du saknar den ibland.

Under de senaste årtiondena har den teknologiska utvecklingen accelererat. 2024 har den smarta telefonen existerat i snart 30 år, sociala medier är sedan ett par decennier en del av vardagen, och på ett år har AI-baserade tjänster som ChatGPT bidragit till att förändra den digitala informationsmiljön. Den snabba utvecklingen gör det än svårare att utforska framtiden. Nya kommunikationssätt kan uppstå och kombinationer av teknologier och verktyg som inte går att föreställa sig kan 2050 vara lika självklara som den smarta telefonen är idag.

Parallellt med den teknologiska utvecklingen spår ett antal framtidsspanande rapporter att olika icke-statliga aktörer på diverse sätt kommer att spela en roll i

framtidens kriser och väpnade konflikter, liksom i gråzonen mellan fred och konflikt.¹ Det inkluderar allt från privata företag och våldsbejakande grupper till civilsamhällesorganisationer och individer.

I detta memo presenteras fyra scenarier som målar upp möjliga framtider för den digitala informationsmiljön 2050, med fokus på icke-statliga aktörer. Syftet är att genom scenarierna kunna resonera om vad utvecklingen skulle kunna innebära för Försvarsmaktens framtida operationsmiljö. Studien har gjorts inom projektet *Stöd till långsiktiga omvärldsanalyser*, vars övergripande syfte är att bidra till Försvarsmaktens långsiktiga utblick, Perspektivstudien.

De fyra scenarierna är medvetet utformade för att utforska långtgående förändringar. Ett delsyfte med memot är att väcka tankar och tjäna som diskussionsunderlag – memot innehåller inga svar på vad framtiden faktiskt kommer att innebära. De framtagna scenarierna ska ses som exempel på eller illustrationer av möjliga utvecklingar.² Memot bidrar till en större samling av FOI-publikationer som utforskar framtiden och dess implikationer för Försvarsmakten, som med fördel kan läsas parallellt.³

Härnäst följer en kort beskrivning av studiens process, och forskningsfrågorna och viktiga definitioner. Därefter listas scenariernas kullkastare. Utgångspunkter ges i avsnittet därefter, på vilket scenarierna följer. Memot avslutas med en diskussion om den framtida operationsmiljön och slutord.

1 Se US National Intelligence Council. *Global Trends 2040 – A More Contested World*. 2021; Nato Allied Command Transformation (ACT). *Strategic Foresight Analysis 2023*. Norfolk, Virginia, 2023, s.54; kommande Ministry of Defence UK, Development, Concepts and Doctrine Centre (DCDC). *Global Strategic Trends 2024*, s.4. Sjunde upplagan. 2024. Gråzonen förstås generellt som utrymmet på konfliktskalan mellan krig och fred eller en situation som är präglad av osäkerhet. För övergripande beskrivning av gråzon samt scenarier för gråzonslägen i krig och fred, se Daniel K Jonsson, Camilla Eriksson, Jenny Ingemarsdotter, Niklas H Rossbach och Christoffer Wedebrand. *Gråzonslägen i krig och fred*. FOI-R--5447--SE. Stockholm: Totalförsvarets forskningsinstitut, 2023.

2 Andy Hines och Peter Bishop. *Thinking about the future: Guidelines for strategic foresight*. Houston: Hinesight, 2015, s.131ff.

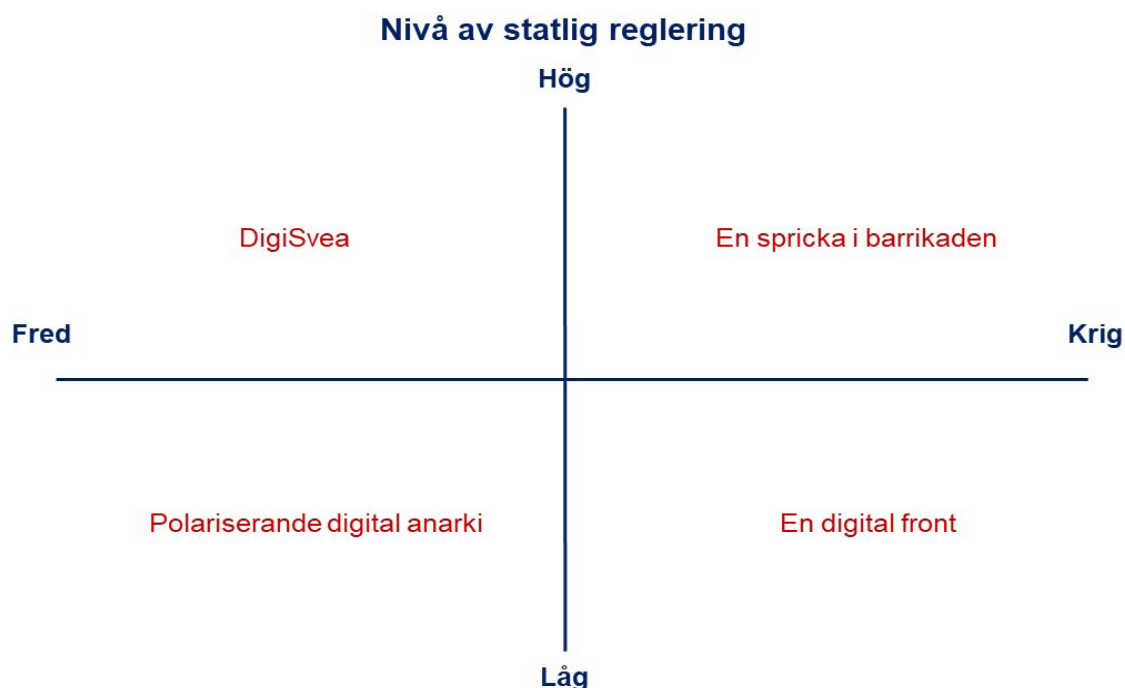
3 Se Malin Karlsson, Andreas Johlander, John Welsh och Jonatan Westman. *Svensk säkerhetspolitik och Försvarsmaktens operationsmiljö i rymddomänen 2050 – ett första utforskande steg*. FOI-R--5638--SE. Stockholm: Totalförsvarets forskningsinstitut, 2024; Lisa Bergsten, Malin Karlsson och Henrik Persson. *Ryssland som militär motståndare 2050 – fyra möjliga utvecklingsvägar*. FOI-R--5635--SE. Stockholm: Totalförsvarets forskningsinstitut, 2024.

Studiens process

Scenarierna har skapats genom en kombination av tillvägagångssätt, som bygger på kreativa tankegångar, ledda av intuition och implicit kunskap.⁴ Processen har bestått av tre steg: 1) trendinsamling, 2) trendbearbetning och 3) scenarioframtagning. Det första steget, trendinsamling, utgjordes av en litteraturöversikt av framtidsstudier, och åtta intervjuer. Intervjuerna genomfördes under våren 2024 med experter på FOI liksom med ett antal experter knutna till primärt USA-baserade tankesmedjor; Brookings Institute, Council of Foreign Relations, RAND och RAND Europe. De intervjuade har företrätt olika områden såsom våldsbejakande extremism, radikalisering och terrorism, framtida teknologi, strategisk kommunikation, underrättelseverksamhet samt informationskrigföring. Intervjuerna följde en intervjumall men var semistrukturerad, det vill säga att intervjuaren delvis följdes upp med nya frågor.⁵ En kortare intervju hölls även med experter på the Digital Forensic Research Lab (DFR-Lab) vid Atlantic Council.

I det andra steget bearbetades de insamlade trenderna genom metoden *Driver mapping*.⁶ Metoden användes för att sortera de cirka 60 insamlade trenderna i två kategorier: kritiska osäkerheter och bakgrundstrender. Kritiska osäkerheter är trender som har en hög påverkan på framtidens informationsmiljö och vars konsekvenser är omgärdade av osäkerhet. Bakgrundstrender är trender som identifierades att ha hög påverkan på framtidens informationsmiljö men vars konsekvenser anses relativt "förutsägbara". Dessa återfinns i avsnittet Utgångspunkter. Trender som inte ansågs ha en betydande påverkan på informationsmiljön sorterades bort. Därtill bearbetades vissa av trenderna genom enskilda samtal med FOI-medarbetare inom specifika expertområden som kvantteknik och AI.

I det tredje steget, scenarioframtagningen, valdes två kritiska osäkerheter som bedömdes kunna generera mest varierande scenarion ur: 1) nivån av statlig reglering och 2) om Sverige befinner sig i krig eller fred. Krig definieras här som att Sverige befinner sig i en militär



Figur 1. Axes of uncertainty. Scenariokors som användes för att visualisera scenarierna. Scenariologiken utgörs av axlarna krig – fred och nivå av statlig reglering, hög – låg.

4 Hannah Kosow och Robert Gaßner. *Methods of Future and Scenario Analysis: Overview, Assessment, and Selection Criteria*. Bonn: Deutsches Institut für Entwicklungspolitik, 2008, s.62-64.

5 Intervjumallen bygger på ramverket sju frågor. Se Government Office for Science. *The Futures Toolkit – Tools for Futures Thinking and Foresight Across UK Government*. Upplaga 1.0, 2017, s.29-32.

6 Se Government Office for Science. *The Futures Toolkit – Tools for Futures Thinking and Foresight Across UK Government*, 2017, s.42-56 för en detaljerad beskrivning av metoden. Samma metod med annat namn är *The Global Business Network Method* (GBN). Mer information om tillämpning, se Malin Karlsson och Lovisa Mickelson. *Idéer till Försvarsmaktens arbete med scenarier inom Perspektivstudien*. FOI Memo 8193. Stockholm: Totalförsvarets forskningsinstitut, 2023.

konflikt, antingen på ett allierat lands territorium eller på eget. Fred är avsaknaden av sådan konflikt. Nivån av statlig reglering delades upp i hög respektive låg.

Metoden *Axes of uncertainty*⁷ användes, och de två utvalda kritiska osäkerheter korsades för att skapa scenariologiken (se figur 1). Resterande kritiska osäkerheter placerades in i de fyra rutorerna, och har utforskats i scenarierna. Det genomfördes delvis under en workshop med FOI-medarbetare. De kritiska osäkerheter som inte varit förenliga med den framtagna scenariologiken eller bakgrundstrenderna har identifierats som kullkastare och redogörs i nästa avsnitt.

För att uppnå syftet har studien haft en utforskande ansats för att ta fram scenarier som speglar flera möjliga och varierande utvecklingsvägar. Sannolikheten i att respektive scenario skulle inträffa har inte värderats, men samtliga scenarier har bedömts rimliga.⁸ Studien har utgått från en västerländsk kontext, vilket speglas i litteraturinhämtningen och de genomförda samtalen och intervjuerna, där samtliga mer eller mindre agerar i en västerländsk kontext.

Datainhämtning och författande av memot har genomförts mellan februari 2024 och juni 2024. Det har således funnits tidsekonomiska begränsningar, i synnerhet avseende djupare resonemang kring icke-statliga aktörers motiv och bakomliggande drivkrafter. En fördjupning skulle sannolikt ha gett mer omfattande och komplexa scenarier.

Forskningsfrågor och definitioner:

Studiens tre centrala frågeställningar är:

1. **Hur kan den digitala informationsmiljön se ut 2050?**
2. **Vilken roll spelar icke-statliga aktörer i den?**
3. **Hur kan detta påverka Försvarsmaktens framtida operationsmiljö?**

Dessa frågeställningar innefattar tre för studien centrala begrepp: informationsmiljö, icke-statliga aktörer och operationsmiljö.

Informationsmiljö beskrivs som en gränslös miljö, som möjliggör utbyte av data och information men som är styrd av tekniska, geografiska och kontextuella faktorer.⁹ Studien utgår från Natos definition av informationsmiljö: ”en miljö bestående av informationen självt, individerna, organisationerna och systemen som tar emot, behandlar och framför informationen samt den kognitiva, virtuella och fysiska rymd i vilka detta sker”.¹⁰ Den kognitiva, virtuella och fysiska dimensionen inkluderas i studien men huvudfokus ligger på de två förstnämnda dimensionerna.¹¹ Studien behandlar primärt den digitala informationsmiljön.

Även om informationsmiljön inte är något som går att stiga in i eller ut ifrån – det är inte ett faktiskt rum – används i memot beskrivningar som kan tolkas som att informationsmiljön är något fristående, autonomt. Det är för att kunna beskriva och resonera om något som är gränslöst och ständigt närvarande men som inte alltid går att fysiskt ta på.

I denna studie ses icke-statliga aktörer som ett paraplybegrepp, och inkluderar alla entiteter som inte är statliga. Det innefattar väpnade grupper, våldsbejakande extremister och kriminella grupperingar, liksom civilsamhället, löst sammansatta nätverk, idéburna- eller religiösa organisationer och företag.¹² Även inflytelserika individer inkluderas. Givet att det handlar om aktörer har de agens. Det innebär inte att en aktör måste agera, däremot att den har förmåga att agera. I scenarierna beskrivs antagonistiska, icke-antagonistiska eller neutrala aktörer. Neutrala och välvilligt inställda icke-statliga aktörer benämns båda som icke-antagonistiska.

7 Se Government Office for Science. *The Futures Toolkit – Tools for Futures Thinking and Foresight Across UK Government*, 2017, s.42-56, för en detaljerad beskrivning av metoden.

8 Peter Schwartz. *The Art of the Long View – Planning for the Future in an Uncertain World*. New York: Crown Business, 1996, s.xiii-xv; Henrik Persson. *Framtidsforskning - en kartläggning*. FOI Memo 7802. Stockholm: Totalförsvarets forskningsinstitut, 2022.

9 För en genomgång av informationsmiljön, se Per-Erik Nilsson, Sofia Olsson och Ivar Ekman. *Den nya informationsmiljöns topografi – Teknik, människa och strategi i osäkerhetens tidevarv*. FOI-R--5342--SE. Stockholm: Totalförsvarets forskningsinstitut, 2022.

10 Författarnas översättning. I original: ”An environment comprised of the information itself, the individuals, organizations and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs”. Nato Standardization Office. *AJP-10 Allied Joint Doctrine for Strategic Communications*. Bryssel, 2023, s.7.

11 Kognition i relation till informationsmiljön syftar här på ”de processer genom vilka sinnesintryck omvandlas, reduceras, utvecklas, lagras, återkallas och används”. Det handlar bland annat om uppmärksamhet, perception och beslutsfattande samt om hur information eller innehåll påverkar människors medvetna eller omedvetna agerande. Per-Erik Nilsson, Sofia Olsson och Ivar Ekman. *Den nya informationsmiljöns topografi – Teknik, människa och strategi i osäkerhetens tidevarv*, 2022, s.11. Den virtuella dimensionen avser plattformar och mjukvara som möjliggör att kommunicera, producera och ta del av innehåll i informationsmiljön, liksom ”cyberpersonas” vilket ska förstås som virtuella manifestationer av personer, som en sociala medie-profil. Den sociala handlar om människor, enskilt och i grupp, som är i informationsmiljön. Det berör också psykologiska, kulturella, ekonomiska och politiska aspekter. Se Nato Standardization Office, *AJP-10 Allied Joint Doctrine for Strategic Communications*, 2023, s.8.

12 Andrew Clapham. Non-state Actors. I *Post-Conflict Peacebuilding: A Lexicon*. Vincent Chetail (red), 200–212. New York: Oxford University Press, 2009. Definitionen skiljer sig exempelvis från hur begreppet vanligen används inom freds- och konfliktforskningen där det ofta enbart handlar om väpnade grupper bortom statens kontroll. Se även Agata Kleczkowska. *States vs. Non-State Actors – A Public International Law Perspective*. Hybrid CoE Strategic Analysis 20. Helsingfors: The European Centre of Excellence for Countering Hybrid Threats, 2020.

Denna breda och generella definition används för att inkludera så många aktörer som möjligt i scenarierna. En smalare definition, som exempelvis enbart inkluderar icke-statliga väpnade grupper, skulle gett ett betydligt snävare utfallsrum och inte inkludera den variation av aktörer som Försvarsmakten behöver förhålla sig till i framtiden.

Operationsmiljö beskrivs i Försvarsmaktens militärstrategiska doktrin som ett sammanhängande system bestående av tre delar: den fysiska miljön, aktörer och informationsmiljön.¹³ Samtliga diskuteras i avsnittet om Försvarsmaktens framtida operationsmiljö.

KULLKASTARE

I tabell 1 listas de identifierade kullkastarna. En kullkastare är en kritisk osäkerhet, en händelse eller en process som förändrar förutsättningar, och således den framtida utvecklingen, på ett drastiskt och betydande sätt.¹⁴ Kullkastarna är alltså inte förenliga med

de framtagna scenarierna, utan kan generera andra möjliga utvecklingsvägar.

UTGÅNGSPUNKTER

Följande avsnitt beskriver grundläggande utgångspunkter och är en sammanfattning av de insamlade bakgrundstrenderna. Avsnittet är en bakgrundsbeskrivning för de fyra framtagna scenarierna.

Det teknikpräglade samhället

2050 beräknas två tredjedelar av världens befolkning bo i städer,¹⁶ i Sverige potentiellt 93% av befolkningen.¹⁷ Vissa kommer vara så kallade ”smarta” städer där informations- och kommunikationsteknologi används för att lösa diverse urbana utmaningar. Med hjälp av optiska och andra sensorer kombinerat med AI kan trafikflöden optimeras, luftkvaliteten förbättras och energiförbrukningen effektiviseras för att minska klimatavtryck.¹⁸ Samtidigt

Tabell 1. Kullkastare.

Kullkastare	Beskrivning
Den okända teknologiska revolutionen	Nästa teknologiska revolution utbryter till följd av en teknikutveckling som idag inte går att förutspå, möjligen på grund av dubbel-användning, dual-use, av en teknik eller blandade teknologier. Implikationerna för informationsmiljön går inte att förutse.
Diktaturen Sverige	Sverige utvecklas till en diktatur med begränsad frihet och repressalier. Informationsmiljön påverkas med betydande kontroll över dess innehåll. Handlingsutrymmet i informationsmiljön begränsas för icke-statliga aktörer och individer.
En återgång till det analoga	En majoritet av samhället förkastar den digitala informationsmiljöns plattformar och kommunicerar istället mer ”analogt”. Den digitala informationsmiljön kan bli en plats för tjänster istället för kommunikation.
Generell AI	Utvecklas generell AI från teori till praktik, skulle det ha omvälvande men svårbedömda implikationer på samhället och informationsmiljön. Teoretiskt skulle generell AI inte bara replikera mänskligt agerande utan holistiskt förstå kontexten och appliceringen av dess handlingar. ¹⁵
Massförstörelse av data	En händelse inträffar som leder till fullkomlig destruktion av data. Effekten blir att delar av, eller hela, samhället återgår till ett för-digitalt stadie under en längre period.
Ransonering av energi	Bristande tillgång på el och energi leder till att samhället tvingas prioritera. Det skulle kunna innebära införande av ”ransoneringskort” för att spara energi, även för den digitala informationsmiljön och tjänster som tillhandahållits genom den.

13 Försvarsmakten. *Militärstrategisk doktrin*. Stockholm, 2022.

14 Pär Gustafsson. *Metod för framtida motståndarbeskrivning: Tillämpning på rysk militär förmåga 2045*. FOI-R--5095--SE, Stockholm: Totalförsvarets forskningsinstitut, 2021, s.21.

15 Det är osannolikt att artificiell generell intelligens kommer att ske de kommande 20 åren, om någonsin. Nato Science and Technology Organization. *Science & Technology Trends 2023-2024. Across the Physical, Biological, and Information Domains. Volume 1: Overview*. Bryssel: Nato Headquarters, 2023, s.32.

16 Alex Baeumler, Olivia D’Aoust, Annie Gapihan, Soraya Goga, Carina Lakovits, Paula Restrepo Cavadid, Gayatri Singh och Horacio Terraza. *Demographic Trends and Urbanization*. Washington, DC: Världsbanken, 2021, s.9-13; kommande Ministry of Defence UK, Development, Concepts and Doctrine Centre (DCDC). *Global Strategic Trends 2024*, s.4. 2024.

17 Världsbanken. DataBank. Population estimates and projections: Sweden. *Världsbanken*. 2024. <https://databank.worldbank.org/reports.aspx?source=population-estimates-and-projections&preview=on> (hämtad 2024-07-11).

18 Filipe Moura och Joao de Abreu e Silva. Smart Cities: Definitions, Evolution of the Concept, and Examples of Initiatives. I *Industry, Innovation and Infrastructure. Encyclopedia of the UN Sustainable Development Goals*. Walter Leal Filho, Anabela Marisa Azul, Luciana Brandli, Amanda Lange Salvia och Tony Wall (red), 1-9. Springer Charm, 2019.

ökar möjligheten att övervaka människor, fordon och infrastruktur. Stater, i synnerhet auktoritära men även demokratiska, kan komma att utnyttja denna möjlighet i olika syften innan 2050.¹⁹ Stora städer är maktcentrum och kan eftersträva större autonomi från staten. Urbaniseringen har potential att öka spänningar mellan stad och landsbygd.²⁰ I hög- och medelinkomstländer förändras demografin när fler lever längre och färre barn föds. Det kommer ha en påverkan på samhället, inklusive ekonomin, när konkurrens mellan satsningar på välfärd och exempelvis försvar blir påtagligare. Kommersiella aktörer kan ta över fler uppgifter som traditionellt ansetts som statens ansvar.²¹ Allt detta kan bidra till en ökning av sårbarheter i samhället.

Möjligheten att vara uppkopplad till internet kommer i stort vara universell och en essentiell del av livet 2050.²² En del stater kan försöka kontrollera segment av internet genom att begränsa tillgången.²³ I vissa fall tar extrema rörelser till långtgående metoder för att få och upprätthålla intresse, exempelvis genom uppseendeväckande våldsdåd.²⁴

Ett antal kommersiella aktörer kommer att äga förutsättningsskapande infrastruktur (inklusive tillverkning av kritiska komponenter) såsom IT-infrastruktur.²⁵ Givet internets roll i vardagen 2050, blir det högst relevant vem som möjliggör för människor att vara uppkopplade. I vissa fall kan det röra sig om multinationella företag, i andra om enskilda individer, vilka kan påverka statliga liksom icke-statliga aktörer genom att styra tillgången till dessa förutsättningsskapande förmågor och på andra sätt påverka internationella relationer och statsangelägenheter.²⁶ Den kommersiella sektorn kommer driva innovation,

forskning och utveckling, särskilt i demokratiska länder. Det berör en rad sektor som har betydelse även för militär verksamhet, såsom logistik, telekommunikation och rymd.²⁷ Rymden ökar i betydelse för civilt såväl som militärt bruk och mot 2050 kommer privata företag att vara nyckelaktörer, mycket på grund av minskade ekonomiska kostnader.²⁸

Det teknikpräglade samhället innebär fler sårbarheter avseende exempelvis kritisk infrastruktur.²⁹ För att stärka cyberförsvaret samverkar och samarbetar likasinnade stater och icke-statliga aktörer. Flera länder utvecklar frivilliga cyberförsvarsförmågor.³⁰ Cyberlegosoldater, det vill säga cyberexperter och hackare vars tjänster kan köpas, förekommer. Kriminella grupper nyttjas av antagonistiska aktörer för att via ombud begå cyberangrepp. Det är alltså svårt att med säkerhet attribuera dem.

Utvecklingen inom AI fortgår, men takten är osäker. Innan 2050 kan utkomsten av debatter om etisk användning av AI ha påverkat informationsmiljön. Det innefattar frågor om vem och hur beslut understödda av AI-analys tas men även huruvida normer, regler och gruppers inställning till integritet och data påverkar realiseringen av AI-förmågor.³¹ Utvecklingen inom många av de för informationsmiljön relevanta områdena håller så hög takt att reglering och lagstiftning inte kan hålla jämna steg. Det är en betydande utmaning givet komplexiteten i att exempelvis attribuera cyberangrepp eller påverkansförsök liksom reglering av potentiellt skadliga dubbla användningsområden av teknik och teknologi.³²

2050 är fler objekt smarta, uppkopplade till ett sakernas internet (IoT, *Internet of Things*) och "alltings internet" (IoE,

19 US National Intelligence Council. *Global trends 2040 – A More Contested World*. 2021, s.65.

20 Nato Allied Command Transformation (ACT). *Strategic Foresight Analysis 2023*. 2023, s.54.

21 Ibid, s.47.

22 Kommande Ministry of Defence UK, Development, Concepts and Doctrine Centre (DCDC). *Global Strategic Trends 2024*, s.4. 2024.

23 Nato Allied Command Transformation (ACT). *Strategic Foresight Analysis 2023*, s.48-52, 56.

24 Ministry of Defence UK, Development, Concepts and Doctrine Centre (DCDC). *Future Operating Environment 2035*. First edition. Strategic Trends Programme. 2014, s.12.

25 US National Intelligence Council. *Global trends 2040 – A More Contested World*, 2021, s.54, 82, 93.

26 Nato Allied Command Transformation (ACT). *Strategic Foresight Analysis 2023*, s.53. Ett samtida exempel är Elon Musk genom sitt ägandeskap av den satellitbaserade internettjänsten Starlink, liksom sociala medie-plattformen X.

27 Ibid, s.20, 51.

28 Sandra Lindström och Kristofer Hallgren. "Rymden" i *Militärteknik 2045. Ett underlag till Försvarsmaktens perspektivstudie*. Redaktörer Göran Kindvall och Anna Lindbreg. 2020., FOI-R--4985—SE. Stockholm: Totalförsvarets forskningsinstitut, 2020, s.101-104

29 Nato Allied Command Transformation (ACT). *Strategic Foresight Analysis 2023*, 2023, s.37.

30 Ett samtida exempel är cyberenheten inom Estlands hemvärn, skapad 2011. Republiken Estland, Försvarsministeriet. Government formed Cyber Defence Unit under the Defence League. *Försvarsministeriet*. 20 januari 2011. <https://kaitseministeerium.ee/en/news/government-formed-cyber-defence-unit-defence-league> (hämtad 2024-06-19).

31 Det råder mer eller mindre konsensus om att AI kommer påverka nästan alla aspekter av livet, inklusive arbetslivet. Nya jobb kommer skapas och andra slås ut. De länder som ligger i framkant avseende utbildning och omskolning av arbetskraft tros klara omställningen bäst. US National Intelligence Council. *Global trends 2040 – A More Contested World*, 2021, s.57-59.

32 Nato Allied Command Transformation (ACT). *Strategic Foresight Analysis 2023*, 2023, s.38, 63.

Internet of Everything).³³ Globalt varierar hastighet och bandbredd, vissa samhällen använder nya generationer av trådlös telekommunikation som möjliggör bättre dataöverföringshastighet och minskad fördröjning. Teknik för förstärkt-, virtuell- och förlängd verklighet liksom exempelvis interaktiv hologramvideo kan nyttjas till fullo. Den virtuella verkligheten kan upplevas lika påtaglig som den fysiska verkligheten och inkorporeras i flera delar av vardagen.³⁴ Digitala assistenter, smartare än en normalbegåvad människa, kan påverka produktiviteten hos både statliga och icke-statliga aktörer, liksom vara typiska inslag i gemene mans vardag – från att utgöra ett extra ”minne” och påminna om kalenderhändelser, till att omförhandla bolån, sköta dejtingprofiler eller scanna shoppingsidor efter födelsedagspresenter. Språkbarriärer har upplösts tack vare AI-stödd simultanöversättning. Populära listettor, tv-serier och storfiler kan helt eller delvis vara skapade av AI. En del kommer ha kärleks- och vänskapsrelationer med AI:s som kommer uppfattas som mänskliga även om de inte kan anta fysisk form.³⁵

Informationsmiljöns karaktär

Trenderna antyder att framtidens informationsmiljö är en kaotisk och omstridd miljö 2050. Innehåll genererat av användare, verkliga eller inte, kommer att skapa en tätare och mer multifacetterad miljö. Dagens trender avseende exempelvis förekomsten av manipulerade bilder, vilseledande information och riktat innehåll kan utvecklas än mer i framtiden. 2050 har den digitala informationsmiljön varit en del av vardagen i flera decennier. Ett antal tekniker och verktyg för att bedöma innehålls äkthet, ursprung och syfte kommer sannolikt att ha sjösatts, testas och förkastats.

Om någon av metoderna kommer vara framgångsrik är osäkert.³⁶

Bedömningen är att den explosionsartade ökningen av AI-genererat innehåll fortgår, åtminstone under en tid. Allt fler aktörer – statliga, icke-statliga och individer – skapar med hjälp av AI trovärdigt och engagerande innehåll, som falska profiler, med några få klick och försök till informationsmanipulation fortgår och ökar. Nya tillvägagångssätt, exempelvis att manipulera biometrisk data för att imitera individer, kan skapa nya utmaningar för samhället och fler möjligheter för antagonistiska aktörer och kriminella som nyttjar AI för att begå brott.³⁷

Med hjälp av AI skapas botnätverk med trovärdig och långtgående internethistoria – ett konto får en manipulerad närvaro på sociala medier där det framstår som att kontot är äkta.³⁸ Utvecklingen innebär att produktionskostnader för att skapa trovärdigt innehåll är väldigt låga 2050. Antagonistiska aktörer som terroristorganisationer kan därför skapa digital propaganda och bedriva påverkanskampanjer utan större ansträngning, vare sig i arbetsinsats eller i ekonomisk kostnad. Minskade kostnader och ökad tillgänglighet dämpar samtidigt asymmetrin mellan statliga och icke-statliga aktörer.³⁹

Den digitala informationsmiljön präglas av de sociala medieplattformar som är populära 2050, liksom av andra typer av kommunikationsförmågor. Eftersom förmågan att övervaka den digitala informationsmiljön kan öka, söker vissa mer oreglerade digitala tillhåll, motsvarande samtidens *dark web*.⁴⁰ En effekt kan bli större fragmentering av informationsmiljön.⁴¹

Informationsmiljön består även av information och innehåll skapat av redaktionell och annan

33 Sakernas internet, IoT, är förenklat saker, system och tjänster som kommunicerar med varandra genom att vara sammankopplade och uppkopplade. Det handlar ofta om vardagssaker som hushållsapparater och lampor, men kan även nyttjas på samhällsnivå inom exempelvis renhållning och smarta städer. Alltings internet, IoE, kan beskrivas som en effekt av IoT. IoT Sverige. IoT – så funkar det. *IoT Sverige*. N.d. <https://iotsverige.se/om-oss/iot-sa-funkar-det> (hämtad 2024-07-09); Hello Future. Industri 4.0, internet of things, tredje vågen – vi reder ut den digitaliserade industrins begrepp. *Hello Future*. 2018. <https://hellofuture.se/aktuellt/industri40-smartindustri-begrepp/> (hämtad 2024-07-09).

34 Nato Allied Command Transformation (ACT). *Strategic Foresight Analysis 2023*, 2023, s.56.

35 Andrew R. Chow. AI-Human Romances Are Flourishing – And This Is Just the Beginning. *Time*. 23 februari 2023. <https://time.com/6257790/ai-chatbots-love/> (hämtad 2024-07-11).

36 Under intervjuer har tekniker som blockkedjor och vattenstämplar nämnts, båda befästa med stor osäkerhet.

37 Nato Science and Technology. *Science & Technology Trends 2023-2024*, 2023, s.26.

38 Detta förekommer redan. Botnätverk aktiveras för att förstärka särskilda budskap. I vissa fall går det att identifiera att samma nätverk använts tidigare. Ett exempel är botnätverk som publicerade innehåll till stöd från Brexit och som tidigare använts för att publicera innehåll till stöd för Palestina. Se Arild Bergh. *Social Network Centric Warfare – Understanding Influence Operations in Social Media*. FFI-rapport 19/01194, Oslo: Forsvarets forskningsinstitut, 2019, s.16.

39 Nato Allied Command Transformation (ACT). *Strategic Foresight Analysis 2023*, 2023, s.41.

40 *Dark web* är en gömd eller ”mörk” del av internet, som inte går att nå via det synliga, indexerade, internet (eller *surface web*). Det krävs speciell mjukvara, som exempelvis TOR, för att nå *dark web*. Kaspersky. What is the Deep and Dark Web?. *Kaspersky*. 2024. <https://www.kaspersky.com/resource-center/threats/deep-web> (hämtad 2024-07-09).

41 Nato Allied Command Transformation (ACT). *Strategic Foresight Analysis 2023*, 2023, s.41.

media. Nyhetscykeln kan 2050 vara intensivare och lättillgängligare, med rapportering i text, ljud, video eller liveströmmat genom individers linser alla tider på dygnet. Interaktion i informationsmiljön sker via ”bärbar teknik” (*wearable tech*), utöver den handhållna mobila enheten. Glasögon, linser, klockor och smycken är några exempel.⁴² Teknik för virtuell-, förstärkt-, eller förlängd verklighet⁴³ kan vara integrerad i både bärbar och icke-bärbar teknik. En stor andel av dessa sätt att interagera med informationsmiljön kan vara möjliga att ta av sig; många människor vill fortfarande ha känslan av att kunna ”välja” att inte vara uppkopplade, även om implantatbaserade lösningar finns och föredras av vissa.⁴⁴ Nya metoder för att interagera i informationsmiljön påverkar vilken typ av innehåll som produceras eftersom det anpassas till hur användarna tar det till sig, exempelvis genom hologram.

Fler individer interagerar med informationsmiljön och dess omfattande innehåll 2050, vilket gör det än viktigare för aktörer att förfina redan idag existerande metoder för att nå ”rätt” individ i ”rätt” ögonblick. Med hjälp av data från såväl kläder med inbyggda sensorer, handhållna enheter och andra digitalt registrerade vanor och känslolägen, skräddarsys och målgruppsanpassas innehåll för att slå an rätt ton hos den tilltänkta målgruppen – ner på individnivå genom än mer avancerad så kallad *microtargeting*.⁴⁵ Denna metod kan användas såväl kommersiellt som i mer sinistra syften, som individanpassade påverkanskampanjer.

Ett brett utbud av innehåll i informationsmiljön skapar stora möjligheter för individer att själva välja ut delar av olika idéströmningar och ideologier och på så sätt skapa en subjektiv förklaring för livets problem och tillkortakommanden. Det kan leda till en ökad individualiserad radikaliserings, att nya grupper eller löst sammansatta nätverk uppstår kring nya frågor, och med medlemmar som traditionellt inte uppfattats vara i farozonen för radikaliserings.⁴⁶

SCENARIER: MÖJLIGA UTVECKLINGSVÄGAR

Nedan presenteras fyra scenarier om informationsmiljön och icke-statliga aktörer 2050.

Scenario 1: DigiSvea – innovationsnavet

- Hög nivå av statlig reglering
- Fredstid
- Sverige tekniskt och innovativt framstående
- Statlig superapp DigiSvea – med ID-kontroll
- Fredliga liksom våldsbejakande aktörer organiserar sig främst *offline*

I det svenska samhället finns en hög nivå av statlig reglering av informationsmiljön, och det råder fred.

Sverige befinner sig 2050 i ett gott ekonomiskt läge. Sällsynta jordartsmetaller och andra fyndigheter i kombination med en lyckad grön omställning har banat väg för välbefindandet. Traditionen av stark ingenjörskonst har omhändertagits och den utbredda digitaliseringen av samhället som inleddes under 2000-talet har burit frukt. Svenska företag som skapar digitala tjänster och verktyg som bygger på stora AI-modeller (vilka kräver mycket energi för att underhålla och upprätthålla) såsom avancerade AI-assistenter, bärbar teknik och automatiserade hushållsnära tjänster är framgångsrika både nationellt och internationellt.

Under de föregående decennierna var tonen i sociala medier hård, polarisering och radikaliserings drevs av anonyma konton och falska profiler. Barn och unga mår allt sämre psykiskt och befolkningens fysiska hälsa tog skada. De stora sociala medie-jättarnas regleringar ansågs inte bra nog för att stävja utvecklingen. Trots att förslag om begränsningar av skärmtid för barn och unga lades redan under 2020-talet, blev det lag först 2040 och gällde då även vuxna.

I samband med detta togs beslutet att införa ID-kontroll på den digitala informationsmiljöns primära plattformar, vilket inte godtogs av flera stora aktörer. De lämnade landet, vilket motiverade framväxten av *DigiSvea*, den statligt ägda superappen. Samtidigt förbjöds vissa plattformar och företag från att verka i Sverige, plattformar som uppfattades som särskilt skadliga för barn och för att vara förtäckta påverkansoperationer från främmande makt. Långsamt har den folkliga mentala hälsan, liksom den fysiska, förbättrats. Som en konsekvens av den mer kontrollerade informationsmiljön engagerar sig människor mer i civilsamhället, som blomstrar.

42 2024 lanserade exempelvis Meta Wayfarer, ett samarbete mellan Meta och glasögonstillverkaren Ray-Ban. RAY-BAN META WAYFARER. *Ray-Ban*. 2024. <https://www.ray-ban.com/sweden/electronics/RW4006ray-ban%20%7C%20meta%20wayfarer-svart/8056597982788> (hämtad 2024-04-19).

43 Ibland används de engelska begreppen, *virtual*, *augmented* och *extended*, förkortat VR, AR respektive XR.

44 Intervju. Senior forskare vid RAND Europe, Washington DC, 12 mars 2024.

45 Microtargeting används primärt i marknadsföringssyften och handlar förenklat om att analysera datapunkter för att identifiera preferenser och intressen hos individer eller grupper med liknande karaktärsdrag. Mot 2050 kan det utvecklas än mer tack vare bland annat fler sensorer som ger mer specifik data. Gavin Wright. Definition microtargeting. *TechTarget*. 2023. <https://www.techtarget.com/searchcio/definition/microtargeting> (hämtad 2024-07-09).

46 Intervju. Expert vid Council of Foreign Relations, Online, 22 mars 2024.

Majoriteten av medborgarna använder *DigiSvea* som sin primära källa till kommunikation. Myndighetspost, chattfunktioner, betalningstjänster samt motsvarande sociala medier finns i applikationen. Den har blivit en nödvändig del av samhället, och individers vardag. Det går inte att vara anonym och ID-kontroll görs för att kunna skapa och upprätthålla ett konto i *DigiSvea*. Medborgarna har accepterat detta efter en utdragen debatt där den personliga integriteten ställts i kontrast till skydd och säkerhet.

Trots kontrollen över informationsmiljön, och att det i många fall inte längre går att vara anonym, finns det vissa plattformar som står utanför den. Dessa är ”hemmasnickrade”, skapade av öppen källkod som de tidigare dominerande jättarna var tvungna att uppgå i samband med en större regleringsvåg inom EU på 2030-talet. Spel faller utanför kontrollen, även om skärmtidsbegränsningar även gäller för dem. I spelen skapas världar som i stort är obegränsade och för vissa sammanfaller de med verkligheten genom teknik för virtuell-, förstärkt- och förlängd verklighet. Antagonistiska aktörer har svårt att bedriva storskaliga påverkanskampanjer via digitala kommunikationsplattformar, men lokala kampanjer förekommer.

För individer och icke-statliga aktörer som av diverse anledningar vill verka bortom statens kontroll blir dessa plattformar och spelvärldar samlingspunkter. Det gäller även grupper som värjer sig emot de stora ingreppen i yttrandefriheten som begränsningarna av informationsmiljön har inneburit. Eftersom plattformarna inte är särskilt välkända blir också användandet av dem geografiskt begränsat vilket försvårar rekrytering och mobilisering till rörelserna. För att nå ut och få uppmärksamhet nyttjar allt fler gator och torg. Många av dem är fredliga, men en del grupper använder våld och sabotage. Dessa gruppers kommunikation sker primärt utanför den digitala informationsmiljön och ofta bortom de urbana stadskärnorna där sensorer och kameror gör det svårt att undgå övervakning.

Scenario 2: En spricka i barriaden

- Hög nivå av statlig reglering
- Krig i Sveriges närområde, råder höjd beredskap
- Geografiskt begränsad informationsmiljö
- Acceptans för regleringar börjar svikta
- Betydande påverkansförsök mot vissa grupper

I det svenska samhället finns en hög nivå av statlig reglering av informationsmiljön. Sverige är involverad i ett krig i närområdet, både genom Natomedlemskapet och genom starka historiska bilaterala relationer till det invaderade landet.

Sedan invasionen inleddes råder höjd beredskap. Lagar som skyddar enskilda medborgares rätt till

åsikt- och yttrandefrihet, dataskydd och personlig integritet begränsas eller ”pausas”. Staten har markant ökat kontrollen av den svenska digitala informationsmiljön för att förhindra informationspåverkan av främmande makt och antagonistiska icke-statliga aktörer. Det talas om en digital barriad för att skydda Sverige. För att vara aktiv på de stora plattformarna krävs identifiering. Informationsmiljön är geografiskt begränsad, endast vissa sidor fungerar på svenska internet, även det ett försök att minska möjligheten för antagonistiska aktörer att bedriva påverkansoperationer mot Sverige. Övervakning av informationsmiljön sker med hjälp av AI. I de statliga kanalerna, som lättast går att nå, sprids samstämmiga narrativ som syftar till att stärka och upprätthålla försvarsvilja och motståndskraft.

En rad regleringar som ger staten tillgång till data som finns i privat ägo har införts – regleringarna baseras på geografi och eftersom många dataservrar befinner sig på svensk mark, hjälper Sverige allierade genom att ta kontroll över dem och delge information. Många företag delar frivilligt med sig, men vissa vägrar och då nyttjas lagstiftning som möjliggör för statliga aktörer att ta kontroll över dem. Det gäller även inom andra sektorer av samhället, exempelvis har viss infrastruktur införlivats i det gemensamma cyberförsvaret.

Sedan invasionen inleddes har det funnits en förståelse hos invånarna att reglering och begränsningar av yttrandefriheten har varit nödvändig. Men allt eftersom tiden går minskar acceptansen. Fler söker information bortom statens kanaler. Med hjälp av en blandning av ny och gammal teknik kommer invånare åt information utanför den geografiskt begränsade informationsmiljön. Genom dessa sprickor i barriaden försöker inhemska och externa aktörer att påverka den svenska befolkningen, med narrativ som anspelar på historiska händelser och svenska förluster, liksom att den svenska staten är förtryckande genom sina begränsningar av informationsmiljön. Försvarsmakten attackeras också, i syfte att försöka underminera de svenska insatserna i det invaderade landet. Bland annat sprids manipulerade videoklipp på svenska soldater som begår övergrepp på civila.

Delar av den svenska befolkningen tilltalas av narrativen och börjar organisera sig runt dem. Veckovis sker demonstrationer mot Sveriges inblandning i kriget. Protester hörs även i andra allierade länder. Samtidigt är solidariteten med det invaderade landet stor i Sverige, och mot- och stödprotester sker. Eftersom den angripande aktören har en stark statskyrka som nyttjas för politiska ändamål, är religiösa grupper av olika religiösa tillhörigheter särskilda måltavlor för påverkansoperationer. Flera av dem har börjat sprida och förstärka den angripande aktörens propaganda. Det fungerar relativt väl, eftersom

många i samhället söker efter något som kan förklara omvärldsläget och händelserna som utspelar sig utanför deras fönster.

Scenario 3: Polariserande digital anarki

- Låg nivå av statlig reglering
- Fredstid
- Motreaktion mot tidigare inskränkande reglering
- Fristad för antagonistiska icke-statliga aktörer – ansträngda diplomatiska relationer
- Många söker efter svar på stora frågor i informationsmiljön

Den statliga regleringen av informationsmiljön är låg och det råder fred.

Efter flera år av inskränkningar av den personliga integriteten och yttrandefriheten i form av övervakning, ID-kontroller i informationsmiljön och andra sätt att kontrollera enskilda medborgares förehavanden, kom en kraftig motreaktion. Flera av de inskränkande lagarna avskaffades, vilket sågs som en framgång för demokratin.

Sveriges nu fragmentariska kontroll av den digitala informationsmiljön har lett till att landet utvecklats till en fristad för icke-statliga aktörers aktiviteter i informationsmiljön och en digital hubb. Det inkluderar både kriminella och antagonistiska icke-statliga aktörer, vilka kan agera från Sverige till en lägre kostnad än från andra länder. Dessa genomför digital mobilisering, organisering och träning av likasinnade som befinner sig i och utanför landet. Det har förekommit att taktisk styrning av våldbejakande extremistgrupper som genomför dåd i andra europeiska länder har utgått från Sverige. Men det gäller inte bara antagonistiska aktörer – aktörer som kämpar för mänskliga rättigheter använder också Sverige som utgångspunkt för digital mobilisering och global opinionsbildning.

Utvecklingen har lett till att diplomatiska relationer med andra länderna är ansträngda, både inom och utom EU. Unionen har dock lite att sätta emot – nationell rätt har stärkts efter att nationalistiska krafter dominerat under flera år. Denna en gång starka institution har tappat i inflytande och samarbete sker nu enbart i grundfrågor som ekonomi och handel.

Tack vare AI-revolutionen arbetar allt fler i Sverige färre timmar. Den digitala informationsmiljöns innehåll är mer närvarande genom utbredd användning av förstärkt- och virtuell verklighet. Allt fler tillbringar mer tid i informationsmiljön, inte minst för underhållning. Eftersom omvärlden känns mer osäker med klimatförändringar och storpolitiska spänningar, söker många efter distraktioner från vardagen. En parallell trend är att individer lämnar informationsmiljön till förmån för fysiskt mellanmänniskt utbyte. Viljan att

träffa människor fysiskt har lett till att fler engagerar sig i föreningar. Urbaniseringen har bidragit till utvecklingen. Samtidigt är det en ekonomisk fråga, och de välbeställda har möjligheten att koppla ner och *outsourca* sin digitala närvaro. Det personliga mötet har blivit en statusvara, vilket flera företag hörsammat.

Den digitala informationsmiljön har återgått till att vara som under internets tidiga år, med fler nischade plattformar som komplement till de stora jättarna, vilka fortfarande är verksamma i Sverige men inte är särskilt populära. Alla som vill kan skapa en egen plattform, sitt egna innehåll och direkt sända ut det genom sitt val av teknik. Många plattformar är lokala, för enskilda skolor, företag, organisationer och föreningar. En stor del av befolkningen tar endast in information och nyheter via sin ”filterbubbla”. En del radikaliserar, inte minst när svaren som ges i ”filterbubblan” adresserar personliga problem eller omvärldsutvecklingen. Bidragande är också att samma idéer och narrativ återkommer och står oemotsagda i dessa bubblor. Det finns exempel på hur radikaliseringen tar sig uttryck i våld – särskilt uppmärksammas unga kvinnor och flickor som är aktiva inom våldsbejakande klimatrörelser.

Scenario 4: En digital front

- Låg nivå av statlig reglering
- Krig på svenskt territorium
- Stark försvarsvilja och motståndskraft
- Frivillig information- och cyberarmé
- Sårbar digital informationsmiljö

I det svenska samhället finns en låg nivå av statlig reglering av informationsmiljön och det pågår ett krig på svenskt territorium.

Kriget är starkt präglad av cyber- och informationsdimensionen av konflikten. Informationsmiljön är kaotisk, med mycket vilseledande innehåll och frekventa cyberangrepp. Regeringen har öppnat för att låta flera svenska rörelser och individer stötta arbetet med att försvara landet på det digitala slagfältet. En rad företag har ställt om sin verksamhet för att stötta Sveriges befolkning i stort, myndigheter i allmänhet och Försvarsmakten i synnerhet. Kriget har öppnat möjligheterna för innovation och utvecklingen inom många områden går snabbt. Staten åtnjuter högt förtroende hos medborgarna och det råder en stark motståndanda.

Kodningskompetensen hos den vanlige medborgaren har ökat de senaste decennierna eftersom det har varit ett obligatoriskt ämne i grundskolan. Det finns således en god kompetens hos Sveriges befolkning att bidra och hjälpa till att hantera digitala hot, framförallt när flera AI-tjänster inte längre kan försörjas på

grund av angrepp på infrastruktur för elförsörjning. Privatpersoner, företag och försvarsföreningar utvecklar gemensamt förmågor, såsom drönare, och bildar en frivillig informations- och cyberarmé som stöttar Försvarsmakten och staten.

Att skydda civilbefolkningen, samhällskritisk infrastruktur och säkra kommunikation till medborgarna står högst upp på agendan och enar den svenska befolkningen. Kriget är mycket närvarande i vardagen, och dominerar informationsmiljön. Tack vare ny teknik kommer slagfältet nära. För att hålla försvarsviljan och motståndskraften intakt har det gjorts stora satsningar på sport, kultur och andra typer av underhållning. Dessa satsningar genomförs av såväl public service som av privata aktörer.

Den frivilliga informations- och cyberarmén är en del av totalförsvaret, och arbetar nära både staten och redaktionell media för att delge information om krigets utveckling till befolkningen. I stort följs regeringens officiella linje och narrativ, men andra perspektiv finns i omlopp.

Eftersom den frivilliga informations- och cyberarmén främst koncentrerar sig på att skydda fysiska civila mål och statliga informationskanaler, lämnas mycket av den övriga digitala informationsmiljön öppen för yttre påverkan. Desinformation och vilseledande innehåll sprids relativt fritt i den digitala informationsmiljön från alla olika håll, inklusive länder som Sverige har uppfattat som allierade eller neutrala. Internationella digitala rörelser bidrar och arbetar med att motverka desinformationen och försöker spåra varifrån den kommer. Det är alltjämt svårt att fastslå avsändaren, men det framstår som att antagonistiska rörelser inom och utanför landet försöker påverka befolkningens uthållighet och försvarsvilja, liksom undergräva förtroendet för staten.

Cyberkriminella nyttjar den kaotiska informationsmiljön till att begå brott, men agerar även ombud för främmande makt. Andra icke-statliga aktörer, bland annat terrororganisationer, tar tillvara på tillfället för att rekrytera. Även om den svenska befolkningen generellt har god källkritik efter att ha spenderat dryga två decennier i en informationsmiljön full av desinformation, finns en minoritet som är mottaglig för påverkansförsöken. Det gäller framförallt de grupper som har fått, eller upplever sig ha fått, det markant sämre sedan kriget inleddes.

FÖRSVARSMAKTENS FRAMTIDA OPERATIONSMLJÖ

Nedan beskrivs faktorer och möjliga effekter för Försvarsmaktens framtida operationsmiljö till följd av utvecklingen inom informationsmiljön och icke-statliga aktörers agerande i den. Analysen utgår från Försvarsmaktens definition av operationsmiljön och berör samtliga nivåer i konfliktskalan. Den berör den militärstrategiska nivån primärt. Analysen ska inte ses som heltäckande utan lyfter ett antal centrala aspekter att beakta mot 2050.

Som avsnittet Utgångspunkter och scenarierna visar påverkar samhällsutvecklingen i stort informationsmiljön, och i förlängningen operationsmiljön. Samhällets och Försvarsmaktens beroende av ett antal digitala tjänster, plattformar och infrastruktur är ett exempel. Ägandeförhållanden och geografi kommer att spela en roll, vilket framgår i vissa scenarier, som *En spricka i barrikaden* och *DigiSvea – Innovationsnavet*.

Motståndaren, statlig eller icke-statlig, kommer med stor säkerhet fortsätta att nyttja informationsmiljön för angrepp med olika syften. Eftersom motståndaren nyttjar hela samhällets sårbarheter, nu och 2050, kommer samverkan inom Försvarsmakten, mellan Försvarsmakten och övriga totalförsvaret samt med Nato att vara viktig även i ett längre tidsperspektiv. Ett exempel är inom strategisk kommunikation, som förutsätter att aktörer följer samma strategiska narrativ.⁴⁷ Det gäller inte bara under krig och konflikt – att sätta bilden och att avskräcka via kommunikation sker redan i fredstid.⁴⁸ Även inom lägesbildsproduktion krävs samverkan med andra. Försvarsmakten varken kan eller ska vara överallt, i synnerhet i fredstid och i gråzonen mellan fred och krig. Mycket av detta är självklart idag, men kommer vara än viktigare mot 2050, när samhället och slagfältet kan vara än mer digitaliserat.

I ett par scenarier, exempelvis *Polariserande digital anarki*, återfinns en fragmenterad informationsmiljö. En sådan utveckling kan innebära en rad utmaningar, exempelvis fler plattformar att ha kännedom om och nå ut via. I händelse av krig och ett fragmenterat slagfält spelar geografiska faktorer in, områden som ockuperas eller ligger nära landsgränser kan finnas i en annorlunda och mer svårpenetrerad informationsmiljö. En mer kaotisk och innehållstung informationsmiljö innebär även mer brus att både nå ut igenom och att analysera för att genomföra rätt aktiviteter.

47 Ett samtida exempel är Ukrainas strategiska kommunikation och "one-voice-policy". Se Ivar Ekman och Per-Erik Nilsson. *Ukraine's Information Front. Strategic Communication during Russia's Full-Scale Invasion of Ukraine*. FOI-R--5451--SE. Stockholm: Totalförsvarets forskningsinstitut, 2023.

48 Nato Allied Command Transformation (ACT). *Strategic Foresight Analysis 2023*, 2023, s.38.

Sverige, som medlem av Nato och andra internationella organisationer, kan även 2050 delta i insatser utanför landets gränser. Även här måste informationsmiljön beaktas – vad är Sverige-bilden i det mottagande landet? Vilka narrativ skulle kunna undergräva förtroendet för Sverige och Försvarsmakten hos lokalbefolkningen? För att genomföra aktiviteter krävs vad som kan jämföras med terränganalys i informationsmiljön. Det handlar både om vilka plattformar som dominerar, och om vilka populärkulturella och samhälleliga strömningar som formar innehållet i informationsmiljön.⁴⁹ Risken är annars att den sökta effekten uteblir.

Idag som 2050 kan civila, medvetet eller omedvetet, sätta bilden av ett krig eller en militär verksamhet genom livesändningar via glasögon eller linser, och 2050 kan trovärdigt AI-genererat innehåll nyttjas för att skapa en falsk berättelse om en händelse, exemplifierat i *En spricka i barrikaden*. Att ha egendokumenterat material att använda för att försöka rätta felaktigheter kommer vara viktigt – även om det inte garanterar att alla tror på äktheten. Att kunna visa autentiskt material kan bidra till trovärdighet och tillit, förutsatt att Försvarsmakten upprätthåller en hög nivå av trovärdighet hos den svenska befolkningen innan konflikten börjar.

2050 är troligen imitationer i informationsmiljön vanligare, vilket även kan drabba Försvarsmakten. Bedragare kan imitera centrala personer för att förvirra, vilseleda eller påverka stridsviljan. I en framtid där video, bild och ljud enkelt manipuleras, blir personkännedom viktigt. Den behöver byggas över tid, för att underlätta att upptäcka när något avviker från normalbilden.⁵⁰

På samma sätt som civila, och antagonister, kan nyttja bärbar teknik (liksom virtuell eller förstärkt verklighet) kan Försvarsmaktens soldater göra detsamma, i såväl skarp insats som övning och träning. Det innefattar anpassning till den bärbara teknikens förutsättningar, såsom produktion av nya former av innehåll. Det innebär både möjligheter och utmaningar – det kan bidra till förmågeutveckling men kräver också medvetenhet och analys av hur även det kan nyttjas av antagonister.

Som visas i alla scenarierna kommer Försvarsmakten behöva förhålla sig till olika aktörer. Kommersiella aktörer som tillhandahåller tjänster och infrastruktur eller möjliga nya frivilligorganisationer, likt i *En digital front* och *En spricka i barrikaden*. Löst sammansatta nätverk av ”informationskrigare” som stödjer Sverige i händelse av krig kan uppstå.⁵¹ Analyser från OSINT-nätverk⁵² skulle kunna nyttjas i lägesbildaarbete men även avslöja sådant som Försvarsmakten vill hemlighålla. Mer civilt agerande i informationsmiljön under krig och konflikt kommer aktualisera frågor om deras status, det vill säga om de kan anses legitima mål. Det rör inte minst hur motståndaren ser på dem. Motståndaren följer inte samma regler och lagar som Sverige och Försvarsmakten och kan ha större acceptans för att använda verkansmedel som den svenska försvarsmakten varken kan eller vill nyttja, liksom mot mål som inte anses legitima. Uppfinningsrikedomen hos en motståndare med få etiska och moraliska spärrar ska heller inte underskattas.

SLUTORD: FRAMTIDA OSÄKERHETER OCH IMPLIKATIONER

En osäkerhetsfaktor relevant för framtidens operationsmiljö är kognitiv krigföring. Begreppet saknar en fastslagen definition och det pågår såväl militär konceptutveckling som akademisk debatt om vad det faktiskt innehåller. I korthet berör kognitiv krigföring människans kognition, eller hjärna, som slagfält. Det handlar om nanoteknik, bioteknik, informationsteknik och kognitionsvetenskap som används i subversiva syften för att påverka människor, även via informationsmiljön. Vad konsekvenserna för informationsmiljön och operationsmiljön i stort kan bli är i nuläget osäkert. Då det potentiellt innefattar dubbel-användning av vetenskapliga och tekniska framsteg för att skapa förmågor, betyder det dock att icke-statliga aktörer kan spela en roll för utvecklingen av såväl medel som motmedel.⁵³

En annan osäkerhetsfaktor är hur det transparenta, eller genomskinliga, slagfältet kommer att påverka och påverkas av informationsmiljön.⁵⁴ Möjligen blir

49 Det kan ses som en fördjupad IEA (*Information environment assessment*) och TAA (*Target Audience Analysis*). AJP-10 *Allied Joint Doctrine for Strategic Communications*. Bryssel, 2023.

50 Under de senaste åren har fejkade video och samtal med högprofilerade personer avslöjats – ofta för att de har agerat på ett avvikande sätt. Ett exempel är ett robotsamtal som påstods vara den amerikanska presidenten Biden som uppmanade personer att inte gå och rösta, vilket inte rimmade med hans vanliga budskap. Vittoria Elliot och Makena Kelly. The Biden Deepfake Robotcall Is Only The Beginning. *Wired*. 23 januari 2024. <https://www.wired.com/story/biden-robotcall-deepfake-danger/> (hämtad 2024-07-12).

51 Samtida exempel är Nafo och IT-Army Ukraine, vilka bekämpar rysk desinformation respektive ryska cyberangrepp.

52 OSINT står för *Open Source INTElligence*, det vill säga underrättelse inhämtat från öppna källor.

53 Se vidare Per-Erik Nilsson. Kognitiv krigföring. En utforskande och övergripande introduktion till ett esoteriskt begrepp och koncept. FOI-D-1308--SE. Stockholm: Totalförsvarets forskningsinstitut, 2024.

54 Det transparenta, eller genomskinliga, slagfältet syftar på att utvecklingen av fler och mer kvalificerade sensorer tillsammans med sambands- och informationssystem, gör att det blir betydligt svårare att inte synas. Jan Henningsson. *Natomedlemskapets konsekvenser för markdomänen – Ett diskussionsunderlag inför fortsatt förmågeutveckling*. FOI Memo 8520. Stockholm: Totalförsvarets forskningsinstitut, 2024.

vilsledning⁵⁵ som metod och informationsmiljön som dess skådeplats än vanligare, liksom ”informationskriget” i stort. Om både Försvarsmakten och motståndaren ständigt kan ses och se, blir kampen på andra arenor – som informationsmiljön – än viktigare. För att skydda informationsmiljön och hålla operationsmiljön säker från påverkansförsök, krävs kontinuerlig analys av samtliga dimensioner; den kognitiva (politiska, kulturell, ekonomiska, psykologiska aspekter), den virtuella (mjukvaran och sociala nätverken) och den fysiska (ägendeskap av hårdvara och geografi). Det krävs också förståelse för egna sårbarheter – kognitivt och kommunikativt – för att dämpa konsekvenser av angrepp, oavsett dess natur.

Det krävs även skydd, ett holistiskt sådant för att värna sinnet likväl som uppkopplad teknik. Påverkansförsök mot militär personal kan ske när som och bli än mer potentia mot 2050. Detta kan vara särskilt kraftfullt i ett scenario som i *Polariserande digital anarki*.

I slutänden handlar det om människor. Hur är hon, människan som arbetar i Försvarsmakten 2050? Redan idag diskuteras hur allt fler har svårt att upprätthålla koncentrationen eftersom det ständigt finns något som pockar på uppmärksamhet – och när den smarta telefonen inte ligger bredvid oss är vi smärtsamt medvetna om dess frånvaro.⁵⁶ Det debatteras om vi får ett sämre minne eftersom telefonen kan ge svar på ett par sekunder. Därtill

kommer effekter på den fysiska och psykiska hälsan. De långtgående konsekvenserna av vårt kollektiva beroende av smarta telefoner och andra tjänster vi idag och imorgon tar för självklara, är inte fastslagna. Vad effekterna blir för operationsmiljön är därför svårbedömt, men att människan påverkas är de flesta överens om. Det kommer att ha inverkan även på Försvarsmakten och potentiellt på Försvarsmaktens grunduppgifter – att försvara Sverige och vår territoriella integritet i samtliga arenor och dimensioner, samt våra allierade.

2050. Du slår sig ned vid köksbordet för att äta frukost. Samtidigt lyssnar du på kvinnan som projiceras på dina glasögon. Med den transparenta skärmen ser du kaffekoppen samtidigt som kvinnan är som en skugga, ständigt närvarande. Du funderar över samtalet du hade med din kollega dagen före – vad måste du hinna med före helgen? Du tar en tugga när hologramkvinnan stelnar till och bilden skakas om. Du hinner tänka ”äh nej, de har kapat sändningen igen” innan otäcka scener från bränderna som härjar i Centraleuropa dyker upp på glasen. Du förnimmer doften av bränd hud när kameran sveper över eldhärjade kroppar, träd och bebyggelse. Du sliter av dig glasögonen samtidigt som en textrad – AGERA NU! – dyker upp. Det är tredje gången den senaste månaden det händer dig. ■

INTERVJUER OCH SAMTAL

Forskare vid FOI
Forskningsledare vid FOI
Senior forskare vid RAND Europe
Expert vid Brookings Institute
Experter vid DFRLab, Atlantic Council
Expert vid Council of Foreign Relations
Förste forskare vid FOI
Senior forskare vid RAND
Förste forskare vid FOI
Forskare vid RAND
Forskare vid FOI

Stockholm	27 februari 2024
Stockholm	5 mars 2024
Washington DC	12 mars 2024
Washington DC	14 mars 2024
Online	14 mars 2024
Online	22 mars 2024
Stockholm	25 mars 2024
Online	8 april 2024
Stockholm	8 april 2024
Online	17 april 2024
Stockholm	28 maj 2024

Lisa Bergsten är biträdande analytiker vid FOI:s enhet Strategi och policy.

Sofia Olsson är analytiker vid FOI:s enhet Informationsmiljö och påverkan.

55 I Försvarsmaktens Doktrin för gemensamma operationer nämns överraskning som en av flera principer. Det handlar om att agera på ett för motståndaren oväntat och oförutsägbart sätt, exempelvis genom vilsledning. Försvarsmakten. *Doktrin för gemensamma operationer*. Stockholm: Försvarsmakten, 2020, s.128.

56 Se exempelvis Jeanette Skowronek, Andreas Seifert och Sven Lindberg. The mere presence of a smartphone reduces basal attentional performance. *Scientific Reports*, 13, 9363, Nature. 2023.