Vilse i lasagnen?

En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur

Jenny Ingemarsdotter, Daniel Eidenskog,
Vidar Hedtjärn Swaling

FOI-R--4814--SE

Januari 2020

FOI

Jenny Ingemarsdotter, Daniel Eidenskog, Vidar Hedtjärn Swaling

Vilse i lasagnen?

En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur

Titel	**Vilse i lasagnen?– En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur**
Title	Lost in the Lasagna?– A Journey Into the Multi-Layered Problem Structure of Swedish Digitalisation
Rapportnr	FOI-R--4814--SE
Månad	Januari
Utgivningsår	2020
Antal sidor	125
ISSN	1650-1942
Kund	Justitiedepartementet
Forskningsområde	Krisberedskap och civilt försvar
FoT-område	Inget FoT-område
Projektnr	A1190807
Godkänd av	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Bild: Daniel Eidenskog, FOI

Sammanfattning

Sverige och svensk förvaltning genomgår enligt många utredningar och analyser en digital transformation. Digitaliseringen av offentlig sektor antas medföra stora potentiella vinster i form av exempelvis effektiviseringar, kostnadsbesparingar och bättre service. Samtidigt är det ingen självklarhet att digitalisering ger dessa fördelar då det finns många fallgropar längs vägen. Misslyckad digitalisering kan också leda till högre kostnader, onödig administration och inte minst ökade sårbarheter.

Denna rapport utforskar digitaliseringens problem och sårbarheter snarare än dess möjligheter. Några exempel som tas upp är ökat beroende av digital infrastruktur, bristande samordning och riskhantering och en större exponering av skyddsvärda tillgångar. Med utgångspunkt i digitaliseringens komplexitet och några av de förändringsparadigm som digitaliseringen medför sammanfattas de huvudsakliga problem som Sverige måste hantera för att möjliggöra en ändamålsenlig digitalisering inom offentlig förvaltning.

De flesta av dessa problemområden är inte tekniska i sin natur utan handlar om utmaningar på samhällsnivå, såsom samordning av infrastruktur, kompetensförsörjning och hur transparensen kan upprätthållas i automatiserade beslut.

Nyckelord: digitalisering, data, AI, IoT, infrastruktur, automatisering, risker, sårbarheter, hot

Summary

As commonly described in national strategy and policy documents, Sweden is undergoing a digital transformation. From the point of view of the public administration system, the potential of this transformation is declared to be huge, whether in terms of greater efficacy, reduced costs or in terms of better services to the citizens. However, there is no guarantee that digitization will actually bring about these improvements as there are many pitfalls on the way. In fact, failed digitization projects can lead to increased costs, more administration and new security risks.

This report explores potential vulnerabilities and problems related to the digital transformation, focusing particularly on society's increasing dependencies on digital infrastructures and services, and the related challenge of coordinating and addressing risk assessments. It is argued that the rapid deployment of new digital technologies give rise not only to new layers of complexity but also to new types of vulnerabilities and threats.

The main point of the analysis is that the challenges of digitization are often not technical in nature but exists on a societal level, where issues of coordination, expectations, security and ethics must be addressed.

Keywords: digitization, data, automation, AI, IoT, threats, vulnerability, risk

Innehåll

1 Inledning

Digitalisering presenteras ofta som en stor möjlighet – för Sverige, för befolkningen, företagen, staten, landstingen och kommunerna. Kort sagt, digitalisering ses som ett tåg som inte får missas. Detta tåg är samtidigt beroende av en fungerande digital infrastruktur och en genomtänkt riskhantering. Den infrastrukturmodell som växt fram i Sverige har av Kungl. Ingenjörsvetenskapsakademien (IVA) liknats vid en lasagne där aktörerna verkar horisontellt snarare än i stuprör.[1] Lite förenklat behöver inte varje aktör bygga ett eget stuprör där denne själv äger all nödvändig infrastruktur och alla tjänster utan kan fokusera på sin specialitet, i sitt eget ”lager”. I denna modell innehåller det översta lagret tjänsterna, mellanlagren kommunikationsöverföringen och de undre lagren olika slags infrastruktur. Användningen av denna lasagnemodell har visat sig ha många fördelar (i termer av exempelvis innovationsmöjligheter) men som IVA påpekar rymmer den i praktiken också svagheter som bland annat handlar om hur risker hanteras och bristande samordning ur ett samhällsperspektiv.

Problematiken känns igen från krisberedskapssystemet i stort där frågan om samordning mellan och inom olika samhällssektorer har varit föremål för många analyser.[2] I ett risk- och sårbarhetsperspektiv tillför den ökande digitaliseringen nya dimensioner som dock inte bara beror på att sektorer digitaliseras var för sig, utan också på att digitala system numera i praktiken utgör en tvärgående infrastruktur som all annan infrastruktur är beroende av. Frågan är hur robust och hur sammanhängande denna digitala infrastruktur är.

Denna rapport fokuserar på digitaliseringens risker och problem snarare än på dess möjligheter. Titeln har inspirerats av IVA:s lasagnemodell för digital infrastruktur, men precis som i det klassiska barnprogrammet från 1975, *Vilse i pannkakan*, utforskas även en större värld utanför lasagnen, som rymmer såväl hotbilder som inslag av surrealism. Att fenomen som *artificiell intelligens, big data* och *Internet of Things (IoT)* redan nu samspelar i formandet av nya affärsmodeller, relationer, samhällsstrukturer och etiska förhållningssätt står klart.[3] Mot den bakgrunden utforskas i rapporten såväl förändringsparadigm och problem som behovet av nya riskhanteringsstrategier.

Studien är genomförd av Totalförsvarets forskningsinstitut (FOI) inom ramen för anslaget Säkerhets- och försvarspolitisk forskning och analys (SOFFA). Projektet har bedrivits under 2019 på uppdrag av Regeringskansliet utifrån den övergripande inriktningen att belysa området digitala sårbarheter.

[1] IVA, 2019.
[2] Se t.ex. MSB, 2009; Denward m.fl. 2017.
[3] Innebörden av dessa begrepp kommer att förklaras och exemplifieras i rapportens kommande kapitel.

1.1 Syfte och frågeställningar

Digitalisering, det digitala samhället, den smarta staden, Industri 4.0 – begreppen som vill beskriva vår tids teknikskiften flödar. Då och då ställs frågan om den nya tekniken också medför nya hotbilder. Syftet med denna rapport är dock inte att lista olika typer av hot och cyberattacker – sådana sammanställningar finns redan.[4] Avsikten är istället att undersöka ett antal grundläggande men ändå komplexa frågor som handlar om varför digitalisering sker och, framför allt, om vilka sårbarheter och risker som den digitala teknikutvecklingen medför. De frågor som har väglett studien har formulerats enligt följande:

- Vad innebär det att ”digitalisera”? Vilka är drivkrafterna att digitalisera?
- Varför och hur uppstår risker och sårbarheter när processer digitaliseras?
- Vilka förändringsparadigm, eller trender, kan vi urskilja som formar dagens och morgondagens utveckling och användning av digital teknik?
- Hur ser digitaliseringens problem ut i en svensk kontext?
- Vilka strategier finns eller kan utvecklas för att mildra digitaliseringens sårbarheter?

1.2 Teoretiska utgångspunkter, metod och material

Som framgår av ovanstående frågeställningar betraktas i denna rapport vare sig digitaliseringen eller dess sårbarheter ur ett rent tekniskt perspektiv. Vår utgångspunkt är istället att framväxten av tekniska system är beroende av många aktörer, intressen, målkonflikter, praktiker, processer, normer och ideal.[5] Denna ansats har utvecklats teoretiskt inom den akademiska inriktning som kallas *Science and Technology Studies* (STS). Sheila Jasanoff, professor i vetenskaps- och teknikstudier vid Harvard Kennedy School, har beskrivit STS som ett fält som riktar särskild uppmärksamhet på ”hur tekniska och sociala osäkerheter hanteras, och på vad som går förlorat eller blir förenklat i ansträngningen att producera trovärdiga berättelser”.[6] Av särskilt intresse, menar Jasanoff, är ”sådana beslut som åsidosätter tvivel och deklarerar att ett tekniskt system kommer att fungera

[4] Se t.ex. World Economic Forum, 2019; Verizon 2018; OWASP, 2018.

[5] Felt, Fouché, Miller & Smith-Doerr, 2017. Studier av teknikutveckling utifrån denna bredare ansats har formats utifrån en kritik av tidigare forsknings smalare fokus på framgångsrika pionjärer och ”heroiska aktörer”. Se Summerton, 1998, s. 34.

[6] Jasanoff, 2016, s. 26. ”STS analysis demands, in particular, close attention to the ways in which technical and social uncertainties are resolved, and to what gets lost or simplified in the effort to produce believable accounts of the world.”

tillräckligt säkert och effektivt."[7] Hur osäkerheter (och tvivel) hanteras är av särskilt intresse också för denna studie som syftar till att belysa digitala sårbarheter.

Även om tekniken i sig inte står i fokus för rapporten, så är det samtidigt viktigt att förstå vad olika teknologier innebär, både för att kunna bedöma vad som står på spel (och inte), och för att undvika missuppfattningar om vilka lösningar som kan vara gångbara. Av denna anledning har vi valt att vid behov infoga kortare beskrivningar av olika tekniska begrepp och fenomen liksom exempel på desamma.

Studiens frågeställningar har undersökts dels genom läsning av relevant litteratur[8] (akademisk forskning, myndighetsdokument och rapporter), dels genom ett mindre antal intervjuer. Syftet med intervjuerna, som har genomförts med representanter för Myndigheten för samhällsskydd och beredskap (MSB), Internetstiftelsen[9] och Netnod,[10] har varit att täcka upp perspektiv som textläsningen inte har fångat in liksom att uppnå en fördjupad förståelse av samband och sammanhang som ofta är mycket komplexa. Urvalet av litteratur liksom intervjuade organisationer har gjorts utifrån en önskan att fånga in analyser som kombinerar ett brett samhällsperspektiv med kunskap om den digitala teknikens utveckling och konsekvenser.

1.3 Rapportens struktur

Denna rapport innehåller många perspektiv, problemområden och exempel som ofta är överlappande och på olika sätt sammanhängande. Det finns en poäng med att belysa frågor från flera perspektiv, särskilt teknikutveckling tenderar att präglas av en dubbelhet där samma drivkrafter som skapar värden också kan skapa sårbarheter.[11] Samma skyddsvärde kan dessutom belysas ur flera hotperspektiv. I korthet introduceras i rapporten användningen och innebörden av vissa nyckeltermer, med fokus på digitaliseringsbegreppet i kapitel 2 och fokus på begreppen risker, sårbarheter och hot i kapitel 3. I kapitel 4 analyseras ett antal breda tekniktrender, eller förändringsparadigm, som idag formar den digitala arenan, medan kapitel 5 fokuserar på problemområden i en svensk kontext.

[7] Ibid. "Of particular interest to STS are the decisions that sideline doubt and declare that a technological system will function safely and effectively enough."
[8] Längre citat på engelska har översatts av rapportförfattarna om inget annat sägs.
[9] Internetstiftelsen ansvarar för internets svenska toppdomän .se och sköter drift och administration av toppdomänen .nu. Stiftelsen arbetar även för att främja forskning, utbildning och undervisning med inriktning på internet.
[10] Netnod Internet Exchange i Sverige AB, som ägs av den icke-vinstdrivande TU-stiftelsen (Stiftelsen för Telematikens utveckling), driver de centrala knutpunkterna i Sveriges del av internet.
[11] Ransbotham, Fichman, Gopal & Gupta, 2016.

Rapporten innehåller även avslutningsvis i kapitel 6 exempel på säkerhets-strategier.

Nedan beskrivs närmare var studiens olika frågeställningar återfinns i rapportens disposition.

I kapitel 2 analyseras frågeställningarna *vad det innebär det att ”digitalisera”* och *vilka drivkrafterna är att digitalisera*. I detta kapitel presenteras ett antal bredare perspektiv på digitalisering med fokus på digitaliseringsbegreppets innebörd och användning i en svensk kontext. Kapitlet avslutas med en beskrivning av framstegstänkandets arv liksom utvecklingen av feministiska perspektiv på digital teknikutveckling.

Kapitel 3 beslyser frågan om *varför och hur risker och sårbarheter uppstår när processer digitaliseras*. Här beskrivs vad komplexitet innebär med fokus på digitala sårbarheter och risker. Att digital teknik och dess användande skapar komplexitet betraktas här mer som ett faktum än något som i sig går att åtgärda. Komplexitet beskrivs dock inte som enbart en teknisk fråga utan som resultatet av ett samspel mellan teknik, kultur och samhälle.

Kapitel 4 beskriver *vilka förändringsparadigm, eller trender, som vi kan urskilja som formar dagens och morgondagens utveckling och användning av digital teknik*. I detta kapitel görs en analys av digitala tekniktrender och relaterade risker och sårbarheter. Analysen presenteras i form av tre typer av förändringsparadigm, nämligen *cyber/fysiskt, människa/maskin* och *data/individ*. Utgångspunkten är här att fenomen som tidigare har varit åtskilda alltmer har börjat överlappa varandra eller sammansmälta, samt att dessa trender tillsammans driver och skapar nya digitala sårbarheter.

I kapitel 5 analyseras frågan om hur *digitaliseringens problem ser ut i en svensk kontext*. Vissa av dessa kan kopplas till de förändringsparadigm som beskrivits i föregående kapitel, medan andra snarare har sina rötter i förhållanden som råder i Sverige. Med stöd av genomförda intervjuer samt aktuella rapporter och litteratur identifieras här nio problemområden som påverkar eller kan få konsekvenser för utvecklingen och användningen av digital teknik i Sverige.

I kapitel 6 ges exempel på *strategier för att mildra digitaliseringens sårbarheter*. I detta kapitel beskrivs principer för säkerhetsarbete inom områden som relaterar både till de problem som beskrevs i kapitel 5 och till de förändringsparadigm som beskrevs kapitel 4. Kapitlet är på inget sätt heltäckande när det gäller möjliga åtgärder och säkerhetsstrategier utan syftar till att lyfta intressanta principer, exempel och vägar framåt. Dessa exempel kan sammantagna ses som en skiss till en framtidsinriktad säkerhetskarta som kan förfinas i vidare studier.

Rapporten avslutas med några sammanfattande reflektioner över studiens resultat (kapitel 7).

2 Perspektiv på digitalisering

> … utvecklingen har gått med en sådan hastighet, att vi hava svårt att följa med, trots att vi vistas mitt i brännpunkten.[12]

Att utvecklingen går snabbt har varit en sanning under hela den industriella epoken.[13] Citatet ovan kommer från *Bonniers Veckotidning* år 1926 och handlar om ”samhällets automobilisering” (där brännpunkten syftar på Stockholm). Trots att massbilismen enligt historieskrivningen inträffar i Sverige först under 1950-talet[14] upplevdes alltså bilismen redan under 1920-talet som en väldig kraft som var i färd med att stöpa om samhället i grunden – både tid och rum krympte när platser blev tillgängliga som aldrig förr genom explosionsmotorns drivkraft och automobilens bekvämlighet.[15] Men samtidigt som automobilismen av många sågs som en progressiv kraft som slutgiltigt skulle slunga Sverige in i moderniteten och knyta samman landet och dess befolkning, luftades också farhågor. Trafikstockningar, buller, föroreningar, trafikolyckor och så alla dessa damer bakom ratten – var bilkörning verkligen förenligt med kvinnligheten?[16]

Vår tids digitalisering jämförs inte sällan med bilismens barndom.[17] Liknelsen handlar kanske framför allt om hastighet och en teknisk utveckling som tycks skena, men också om behovet av kontroll och famlandet efter regler. Så länge bilarna var få och långsamma spelade det inte så stor roll vilken sida av vägen man körde på, men redan på 1920-talet hade det blivit tydligt att fungerande regler var en fråga om liv och död. Idag diskuteras om även digitaliseringen har nått en punkt där liv står på spel – här handlar det inte bara om skräckscenarier om självkörande bilar som löper amok utan kanske snarare farhågan om att sjukhus, larmsystem eller annan grundläggande infrastruktur skulle kunna slås ut genom t.ex. hacker-attacker.

Automobilism-metaforen är på många sätt belysande, även om den kanske inte riktigt håller fullt ut. Till skillnad från bilismens initiala regelutmaningar är det exempelvis inte självklart att staten på något enkelt sätt kan lagstifta (eller utlysa en folkomröstning) för att avgöra hur digitaliseringens spelregler ska se ut. Digitaliseringens globala och gränsöverskridande karaktär påverkar alla samhällssektorer men begränsar samtidigt enskilda staters makt i förhållande exempelvis till globalt verkande företag. Icke desto mindre har det offentliga

[12] ”Krönika som denna vecka handlar om samhällets automobilisering”, *Bonniers Veckotidning*, 31 oktober 1926, s. 13.
[13] Löfgren, 2000; Berman, 2001 [1982].
[14] Se t.ex. Lundin, 2014.
[15] Om 1920-talets debatter om automobilismen, se Ingemarsdotter, 2019, s. 141-188.
[16] Ibid.
[17] Se t.ex. Per Runesson, ”Du sköna digitala värld – vad behöver vi kunna om dig?”, den 29 december 2015. Hämtad 2019-12-04 från https://www.lth.se/digitalth/news/article/du-skoena-digitala-vaerld-vad-behoever-vi-kunn/.

fortfarande ett ansvar eftersom enskilda företag inte nödvändigtvis tar ansvar för helheten eller konsekvenser som uppstår i andra eller tredje ledet. Alternativet är att den enskilda individen, konsumenten, eleven eller patienten ytterst får betala priset när något går snett.

Hur var det då med kvinnorna bakom ratten? Om någonstans är det väl ändå där liknelsen mellan automobiliseringen och digitaliseringen haltar mest? Förvisso har mycket hänt sedan 1920-talet vad gäller samhällets inställning till kvinnliga bilförare (och teknikentreprenörer). Samtidigt finns också mönster som kan kännas igen. För den som betänker könsfördelningen på de mest omtalade AI-konferenserna, eller skapandet av mediala hjälteberättelser kring den manliga IT-entreprenören, står det klart att det fortfarande finns genuspräglade strukturer som påverkar attityder och villkor på informations- och kommunikationsteknikområdet (IKT).[18] I många fall bildas därför fortfarande parallella kvinnoföreningar som syftar till att stötta kvinnors möjligheter i manligt dominerade branscher.[19] Vi återkommer i slutet av detta kapitel till automobiliseringens metafor och teknikhistoriens bredare debattlinjer. Dessförinnan går vi igenom vad som idag brukar menas med digitalisering. Kapitel 2 adresserar därmed frågeställningarna *vad digitalisering innebär* och *vilka drivkrafterna är att digitalisera*.

2.1 Vad är digitalisering?

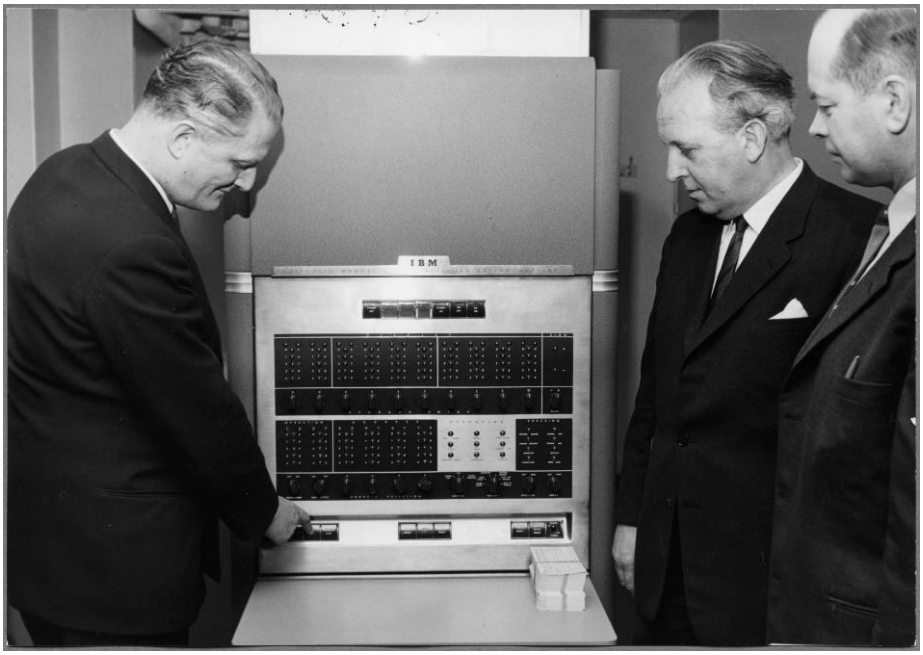
Begreppet digitalisering har blivit ett ledord för många aktörer som vill lyfta fram innovation, utveckling, framtid, förändring och kanske rentav en pågående revolution: ”Digitaliseringen innebär en mycket snabb och genomgripande samhällsförändring, en fjärde industriell revolution.”[20] Innebörden av denna revolution brukar beskrivas i termer av djupgående förändringar som påverkar individer såväl som strukturer. I ett av sina betänkanden konstaterade den statliga Digitaliseringskommissionen att digitaliseringen innebär ”en strukturomvandling där information, kommunikation och interaktion sker på nya sätt, där varor och tjänster produceras och distribueras på nya sätt och där analys av stora mängder data kommer att påverka vår kunskap och förståelse.” [21]

[18] På engelska förkortat ICT, Information and Communications Technology. Om genus och teknikutveckling med fokus på ICT, se Ahuja, 2002; Hill, Corbett & St. Rose, 2010; Felt m.fl. (2017). Om stereotypa bilder av entreprenörer, se t.ex. även Lianne Taylor, ”How gender stereotypes are still undermining the capability of female entrepreneurs”, World Economic Forum, 26 maj 2017. Hämtad 2019-12-04 från https://www.weforum.org/agenda/2017/05/why-female-entrepreneurs-are-cursed-with-male-only-business-attributes.

[19] Se t.ex. *Women in AI* (https://www.womeninai.co/), *Women in Science* (http://womeninscience.se/), *Womengineer* (http://womengineer.org/), *Women in data science and AI - Hub* (https://www.turing.ac.uk/about-us/equality-diversity-and-inclusion/women-data-science-and-ai).

[20] IVA, 2019, s. 7. Uttrycket fjärde industriella revolutionen härstammar från Schwab, 2016.

[21] SOU 2015:28, s. 97.



Figur 2.1. IBM 650, kallad första generationens dator, invigs 1958 av Generaldirektören för SJ, Erik Upmark.[22] Fotograf: Walther Seved. Ingår i samling Järnvägsmuseets foton.

I vid mening syftar alltså digitalisering på processer som förändrar eller skapar något nytt genom användning och integrering av digital teknik. En förutsättning för att digitalisera är att information finns tillgänglig i digitalt format. Arbetet med att överföra befintliga (t.ex. pappersbaserade) system till digitala motsvarigheter kallas ibland *digitisering*.[23] Digitaliseringskommissionen har istället kallat detta ”informationsdigitalisering” vilket avser en process där analog information transformeras till digital information som sedan blir strukturerad, sökbar och tillgänglig genom digitala kanaler och verktyg.[24] Inget av dessa begrepp (*digitisering*, *informationsdigitalisering*) har blivit särskilt etablerat, men nämns här eftersom de pekar på att digitalisering kräver en slags basal datoriseringsfas där information blir digitalt tillgänglig.

Att byta lagringsmedium kan vara en tidskrävande process som dock inte i sig nödvändigtvis medför några omvälvande förändringar av själva verksamheten. Ett exempel på skillnaden mellan digitisering och digitalisering är musiktjänsten Spotify som har skapat en ny modell för hur vi lyssnar på musik. Till skillnad från

[22] Bilderna i denna rapport utgörs av foton från datoriseringens historia i Sverige. Med detta urval vill vi påminna om att digital teknik, som brukar framställas med en mycket futuristisk estetik, också har historiska rötter.
[23] Ekholm, Jebari & Markovic, 2018, s. 6.
[24] SOU 2015:28, s.17.

övergången från vinylskiva till CD-skiva, som kan betraktas som en digitiseringsfas, utgör skiftet från skivor till streaming ett exempel på digitalisering. Den nya tjänsten byggde inte bara på streamingtekniken (en teknik som fanns även innan Spotify), utan också på en annorlunda affärsmodell: Genom att upprätta avtal med ett stort antal innehavare av musikrättigheter skapades en attraktiv tjänst som samtidigt förändrande musikindustrins villkor.[25]

Den nya myndigheten för digital förvaltning (DIGG), inrättad i september 2018, beskriver hur förväntningarna har ökat även på offentlig sektor att digitalisera innovativt, dvs. att göra mer än att ersätta blanketter på papper med PDF.[26] Man betonar att arbete med digitalisering idag inriktas ”på att helt stöpa om hur det offentliga interagerar med privatpersoner och företag”.[27] I enlighet med denna transformativa målbild tenderar digitalisering generellt att beskrivas i termer av något *nytt*, t.ex. nya sätt att arbeta, konsumera, undervisa, kommunicera eller ge service.[28] Detta understryks också av DIGG som beskriver sig själv som ”en ny myndighet, skapad för att tänka nytt, hantera nya utmaningar och se nya möjligheter.”[29]

Mer konkret kan det nya innebära att nya/andra kunskaper efterfrågas, att personalsammansättningen blir annorlunda eller att rutiner ändras. Visioner om smarta, digitaliserade lösningar genererar dock inte alltid lyckade förändringsprocesser. För många i Stockholm räcker det med att säga ”skolplattformen”, som är ett system som ska hantera kommunikation och information mellan skola och föräldrar/elever. Bristerna i plattformen (som rapporterats handla om såväl säkerhet som användarvänlighet) har inte bara skapat stor frustration hos föräldrar, elever och lärare utan har också kostat betydligt mer än planerat.[30]

De lyckade exemplen blir mindre omskrivna, vilket kan ha att göra med att de snabbt blir en del av en ny och självklar vardag. Ett exempel är Skatteverkets införande av e-deklaration vilket inte bara var en teknisk förändring – för att skapa en välfungerande digital deklarationstjänst krävdes också hantering av en rad frågor relaterade till säkerhet, juridik och regelverk. En viktig faktor i

[25] Ekholm, Jebari & Markovic, 2018, s. 22.
[26] ”Den digitala förvaltningen”, Myndigheten för digital förvaltning. Hämtad 2019-12-04 från https://www.digg.se/digitalisering-av-offentlig-sektor/den-digitala-forvaltningen.
[27] Ibid.
[28] Ekholm, Jebari & Markovic, 2018, s. 22.
[29] ”Om oss”, Myndigheten för digital förvaltning. Hämtad 2019-12-04 från https://www.digg.se/om-oss.
[30] ”Försenade IT-tjänster kan leda till miljonkostnader för skolor i Stockholm”, *Dagens nyheter*, 8 oktober 2019. Hämtad 2019-12-04 från https://www.dn.se/sthlm/forsenade-it-tjanster-kan-leda-till-miljonkostnader-for-skolor-i-stockholm/; ”Stockholm panikstänger skolplattform – ’Chockerande att säkerheten är så dålig’”, *Ny Teknik*, 21 augusti 2019. Hämtad 2019-12-03 från https://www.nyteknik.se/sakerhet/stockholm-panikstanger-skolplattform-chockerande-att-sakerheten-ar-sa-dalig-6968823.

Skatteverkets arbete anses ha varit ett tydligt verksamhetsansvar och en sammanhängande förändringsprocess.[31]

Ett annat exempel är den så kallade *Trelleborgsmodellen* som syftar på det förändringsarbete som Trelleborgs kommun har genomfört kring hur man arbetar med arbetslivsfrågor. Som en del i denna modell digitaliserades och automatiserades besluten om försörjningsstöd under våren 2017. Digitaliseringen visade sig vara lyckad i många avseenden, till exempel resulterade den i ökad upplevd professionalism, ökad effektivitet och förbättrad service till medborgarna.[32] Samtidigt fanns en viss kritik mot systemet då transparensen i hur besluten tas upplevdes som sämre då besluten automatiserats.[33] Trelleborgs-modellen har fått stor uppmärksamhet runt om i Sverige och många kommuner har diskuterat att införa den. Detta har dock inte alltid gått smärtfritt, som i exempelvis Kungsbacka där 12 av 16 socialsekreterare valde att säga upp sig, delvis på grund av hur digitaliseringen skulle genomföras.[34] En viktig aspekt i detta fall är att digitaliseringen endast är en liten del i ett större förändringsarbete. Det här är också något som påtalas i den utvärdering av projektet som Trelleborgs kommun har låtit genomföra:

> Digitaliseringen sker alltså som en logisk följd av ett avancerat organisatoriskt effektiviseringsarbete, inte tvärtom. Trelleborgsmodellen kan därför beskrivas som en ypperlig metod för att skapa en kapacitet för att digitalisera delar av verksamheten, snarare än att vara ett resultat av att ha digitaliserat ett arbetsmoment.[35]

Återigen betonas alltså vikten av att börja med målet med verksamhets-förändringen, och att inte låta digitalisering vara ett mål i sig.

2.2 Drivkrafter – välfärdsperspektivet

Vilka är då drivkrafterna bakom digitaliseringssatsningarna? Ur det offentligas perspektiv finns flera uttalade mål med att digitalisera verksamheter, vare sig det handlar om olika slags tjänster, administration eller omsorg. Potentialen att effektivisera förs ofta fram, liksom den närliggande förhoppningen om kostnads-besparingar, men också möjligheten att uppnå ökad kvalitet.[36] Särskilt artificiell

[31] Netnod, intervju, 2019-09-23.
[32] Ranerup & Henriksen, 2019.
[33] Ibid.
[34] ”12 av 16 socialsekreterare säger upp sig i protest”, *SVT Nyheter Halland*, 17 januari 2018, hämtad 2019-12-03 från https://www.svt.se/nyheter/lokalt/halland/robot-tar-over-i-kungsbacka; ”Succémodellen i Trelleborg möter motstånd: ’Man kopierar’”, *Arbetsvärlden*, 12 januari 2018, hämtad 2019-12-03 från https://www.arbetsvarlden.se/succemodellen-i-trelleborg-moter-motstand-man-kopierar/.
[35] Rakar, 2018.
[36] Se t.ex. Digitaliseringskommissionens temarapporter sammanfattade i SOU 2016:85 samt slutbetänkandet SOU 2016:89. För kommunala och regionala perspektiv, se SKL, 2018a och

intelligens (AI) har de senaste åren diskuterats i flera rapporter som lyfter fram teknikens potential att avlasta, utveckla eller förstärka olika typer av mänskliga förmågor och arbetsuppgifter i offentlig sektor.[37] Även robotisering diskuteras som ett alternativ för att avlasta delar av omsorgen.[38] I det följande beskrivs argumenten för att digitalisering kan leda till effektiviseringar, ökad kvalitet och/eller kostnadsbesparingar, samt även hur ett antal relaterade antaganden har problematiserats. Att förstå denna typ av nyttoargument (och kritiken av dem) kan vara relevant i en bredare kontext av hur risker och sårbarheter uppstår, eftersom styrkan i drivkrafterna kan påverka hur osäkerheter bedöms i förhållande till potentiella vinster.

2.2.1 Effektiviseringsargumentet

Begreppet effektivisering förekommer i många policynära digitaliseringsanalyser. Digitaliseringsrådet menar att den svenska förvaltningen ”behöver moderniseras och effektiviseras” och drar vidare slutsatsen att offentlig sektor behöver kunna ”svara upp mot växande krav på både ökad effektivitet i verksamheterna, informationssäkerhet och på ökad servicegrad och digitala tjänster från medborgarna”.[39] Regeringens delmål *digital ledning* pekar på vikten av att ”verksamheter effektiviseras, utvecklas och får högre kvalitet genom styrning, mätning och uppföljning.”[40]

Idén att digitalisering kommer att öka effektiviteten i offentlig sektor bygger i många fall på antagandet att olika typer av uppgifter, ofta av administrativ art, går att automatisera.[41] Analyser av tillgänglig statistik indikerar dock att de administrativa uppgifterna under de senaste två decennierna har ökat snabbare än vad de har kunnat automatiseras.[42] Ekholm, Jebari och Markovic, som har studerat kommunsektorn, menar att den ökande administrationen i kommunerna kan härledas till nya arbetsuppgifter men också till nya statliga krav på dokumentation

Ekholm, Jebari & Markovic, 2018. För regeringens digitaliseringspolitik, se https://www.regeringen.se/regeringens-politik/digitaliseringspolitik/.

[37] Se t.ex. Andersson, Lindsjö & Hagberg, 2018; SKL, 2017; Vinnova, 2018.

[38] Som påpekas i Vinnovas (2018, s.28) rapport *Artificiell intelligens i svenskt näringsliv och samhälle: Analys av utveckling och potential* finns dock fortfarande stora utmaningar för robottekniken att reproducera basala motoriska funktioner.

[39] Digitaliseringsrådet, 2018b, s. 49.

[40] Regeringskansliet, 2017a, s. 6.

[41] Konsekvenserna av automatisering i ett arbetsmarknadsperspektiv är omdebatterad, särskilt vad gäller risken för ökad arbetslöshet om vissa jobb kan automatiseras helt. I sin översikt över ett antal internationellt uppmärksammade rapporter på temat automatisering konstaterar Sveriges kommuner och landsting (SKL) dock att det snarare handlar om att delar av yrken och specifika uppgifter kan komma att automatiseras. Dessutom medför utvecklingen också att nya yrkeskategorier tillkommer, som t.ex. jobb för att bygga och underhålla digital teknik. SKL, 2018a, s. 12.

[42] Ekholm, Jebari & Markovic, 2018, s. 7; Hall, 2007.

eller lokalt initierade uppföljningar.[43] Trenden i detta sammanhang är att allt mindre andel av personalens tid spenderas tillsammans med eleven, vårdtagaren, klienten osv.[44] Även om digitalisering ofta anförs som ett sätt att vända denna utveckling, uttrycks också en oro för att det kan bli tvärtom: Som Sveriges kommuner och regioner (SKR)[45] skriver finns en tendens att digitaliseringsprojekt, tvärtemot intentionen, skapar mer, snarare än mindre, administration:

> Digitaliseringen har hittills ofta drivits i kombination med en styrningskultur med många mål, regler och krav på återrapportering. De investeringar som gjorts i digital teknik har därför inte alltid bidragit till den förväntade produktivitetsökningen utan snarare till ökad administration och minskande tid för värdeskapande arbete.[46]

Att administrationen ökar tycks alltså stå klart, men frågan är också vilken typ av administration som ökar. Som Ekholm, Jebari och Markovic skriver är det ”intressant att notera att den typ av administratörer som hjälper mikrosystemets utförare tvärtom minskar i antal, t.ex. läkarsekreterare.”[47] Vad gäller den typ av administration som däremot har ökat i omfång beskriver Forssell och Ivarsson Westerberg i artikeln *Granskningens (glömda) kostnader* uppkomsten av flera nya administrativa yrken, som t.ex. ekonomer, controllers, informatörer, HR-personal, strateger, upphandlare och kommunikatörer. Istället för en administrativ personal där de flesta hade relativt låg utbildning menar Forsell och Westerberg att utvecklingen har gått mot en administrativ professionalisering (överbyggnad) där de administrativa experternas uppgifter handlar om utveckling och införande av nya former av styrning och kontroll i organisationerna, vilket också får administrativa konsekvenser för kärnverksamheten:

> Ett viktigt resultat av dessa managementbyråkraters arbete är att de policies de utarbetar skapar administrativt arbete för andra, längre ned i den organisatoriska hierarkin. […] Under både arbetet med att installera ett system och därefter i det kontinuerliga driftsarbetet kan en mängd personer dras in i arbetet, och ofta gäller det personer som är sysselsatta direkt i kärnverksamheten, alltså den verksamhet som organisationen i fråga formellt är skapad att syssla med. Det betyder att yrkesgrupper som lärare, läkare, sjuksköterskor, poliser, domare och ingenjörer dras in detta administrativa arbete. Denna förändring har vi kallat amatörisering av det administrativa arbetet, och inom många områden är detta mycket påtagligt.[48]

I ett automatiseringsperspektiv väcker denna utveckling därmed frågor om vad som avses när ”administrationen” ska automatiseras, dvs. vilken nivå i organisationen och vilka uppgifter som avses. I de fall där införandet av olika typer av digitala system har orsakat onödig administration för kärnverksamhetens utförare finns förstås effektiviseringsmöjligheter. Ett exempel på ”arkaiskt” system som

[43] Ekholm, Jebari & Markovic, 2018, s. 7.
[44] Ibid.
[45] Sveriges kommuner och regioner (SKR) hette tidigare Sveriges kommuner och landsting (SKL).
[46] SKL, 2019, s. 64.
[47] Ekholm, Jebari & Markovic, 2018, s. 28.
[48] Forssell & Westerberg, 2016, s. 28–29.

ges av Ekholm, Jebari och Markovic är arbetsscheman som görs i Excel som varje medarbetare sedan måste mata in i ett annat system, som dessutom har väntetider på att logga in på flera minuter: ”Den typen av små ineffektiviteter i stora organisationer blir snart till heltidstjänster i tidsspillan.”[49]

Figur 2.2. Persondator. IBM lanserade sin första PC (Personal Computer) 1981. Modellen hette 5150 och blev en stor succé. Ingår i samling Tekniska museets saker.
Fotograf: Ellinor Algin/Tekniska museet.

Automatisering brukar dock inte bara presenteras i termer av behov utan också i termer av nya möjligheter. Bland annat Vinnova har i en rapport om artificiell intelligens (AI) betonat att utvecklingen av nya affärsmodeller, varor, tjänster och systemlösningar inom såväl näringsliv som offentlig sektor rymmer en stor potential för såväl värdeskapande som ökad effektivitet.[50] I AI-sammanhanget tar Vinnova även upp ett antal utmaningar och risker, bland annat risken att omogna AI-lösningar baseras på felaktiga data och algoritmer liksom säkerhetsrisker som kan uppstå genom medvetet skadlig dataanvändning och datamanipulering.[51] Sammantaget förmedlas dock i många rapporter att potentialen till (bland annat) ökad effektivitet, oavsett om det gäller AI eller digitalisering i allmänhet, väger tyngre än riskerna. Begreppet effektivitet tenderar att i dessa sammanhang stå listat

[49] Ekholm, Jebari & Markovic, 2018. s. 64.
[50] Vinnova, 2018, s. 8, 9. Se även Andersson, Lindsjö & Hagberg, 2018 för konkreta exempel.
[51] Vinnova, 2018, s. 8.

sida vid sida med begrepp som kvalitet och värdeskapande, men det finns ändå anledning att titta närmare på kvalitetsargumentet i separat ordning.

2.2.2 Kvalitetsargumentet

Kvalitetsargumentet kan syfta på en önskan att förbättra den offentliga förvaltningens service inom en rad områden, som t.ex. myndigheters kommunikation med invånarna eller olika typer av ärendehantering.[52] Det kan också handla om helt nya tillämpningar, som exempelvis individanpassade lösningar inom skolan eller omsorgen. Den senare typen av tillämpningar beskrivs ibland i termer av ökad *precision*, där myndigheter genom att exempelvis dela data skulle kunna bli bättre på att anpassa lösningar efter olika individers (t.ex. elevers eller vårdtagares) behov och förutsättningar.[53] Som har påpekats finns dock ett antal hinder för att realisera denna typ av tillämpningar vilka bland annat har att göra med restriktioner i myndigheters möjlighet att dela data med varandra.[54] Detta blir ett problem eftersom data många gånger skapas på en plats medan dess värde uppstår någon annanstans.[55]

I vilken grad digitalisering kan öka kvaliteten i välfärden, eller svara på olika typer av samhälleliga utmaningar, är en fråga som naturligtvis inte är begränsad till juridiska eller tekniska aspekter. Avgörande är samtidigt hur samhällets utmaningar ser ut och vad som menas med begrepp som kvalitet och effektivitet. Ett vanligt förekommande argument för en ökad digitalisering av välfärdssektorn utgår, som beskrevs i föregående avsnitt, från idén att mer automatisering kommer att kunna frigöra personal att arbeta med sina kärnuppgifter snarare än rutinartad administration.[56]

För att förstå i vilken grad digitaliseringssatsningar kan komma att frigöra mer så kallad värdeskapande (icke-administrativ) tid behöver man samtidigt begrunda administrationens motivation och innehåll. Den administration som syftar till att mäta och kontrollera resultat i det offentliga har av filosofen Jonna Bornemark i en kritisk ansats beskrivits i termer av ”förpappringens dubbla verkligheter”: å ena

[52] ESV, 2018; SKL 2018b.
[53] Ekholm, Jebari & Markovic, 2018, s. 32.
[54] Ibid., s. 8. I Digitaliseringsrådets (2019a, s. 18) rapport *Data som strategisk resurs* noteras att Statskontoret lyfter fram främst tre hinder för de offentliga aktörerna att tillgängliggöra öppna data: resursbrist, att verksamhetssystem som gör det enkelt att tillgängliggöra informationen saknas och svårigheter att identifiera den relevanta informationen samt att få myndigheter, kommuner och landsting att se arbetet med att främja vidareutnyttjande som en del av sitt uppdrag. Myndigheten för digital förvaltning har ett regeringsuppdrag att undersöka hur den offentliga förvaltningens förmåga att tillgängliggöra öppna data kan ökas, se https://www.digg.se/utveckling--innovation/oppna-data-och-datadriven-innovation/regeringsuppdrag-oppna-data-datadriven-innovation-och-ai.
[55] Digitaliseringsrådet, 2019a, s. 43.
[56] SKL, 2018a.

sidan en vardagsrealitet för personal och brukare, och å den andra en pappers-exercis av kvalitetsredovisningar, resultatrapporter med mera[57]:

> Långsamt har syftet med verksamheterna förskjutits, från att till exempel inom äldreomsorgen handla om att vårda de äldre till att vårda register och checklistor genom att följa manualer. Det har blivit viktigare att fokusera på vad det står i papprena än att fokusera på de äldre. Det här är en till synes oskyldig glidning, alla papper är ju där för att det ska bli så bra som möjligt för den äldre. Säkerställa att de får den omsorg de ska ha och inte vara utsatta för personalens godtycke. Men det är en glidning som i längden får ödesdigra konsekvenser. Kvalitetsarbetet tar plats i papprena, inte i verkligheten. Och det gör att någon utanför verksamheten ska säkerställa kvaliteten, inte de som är på plats, de ska bara lyda order. På så sätt har vi skapat ett system som ger allt mindre plats för ett professionellt omdöme.[58]

Kvaliteten i vård och omsorg har förstås varit föremål för debatt och kritik även i ett längre historiskt perspektiv; i Sverige under hela välfärdsstatens uppbyggnad.[59] De reformer som har genomförts under årens lopp har som regel tillkommit, som Bornemark också noterar, just i syfte att åstadkomma förbättringar. Men oavsett om det var bättre eller sämre förr är det alltid viktigt att betrakta teknikutveckling i en bredare kontext, särskilt om den framförs som lösningen på många problem. Digitalisering har å ena sidan en uppenbar potential att automatisera processer som innebär rutinartade överflyttningar av data, men har å den andra sidan den lika uppenbara begränsningen att vara beroende av information som är kvantifierbar och mätbar. Risken finns därmed, som även Ekholm, Jebari och Markovic har tagit upp, att sådant som ”tyst kunskap” och mänskligt omdöme oavsiktligt faller bort när verksamhetens olika delar ska kategoriseras, sorteras och digitiseras.[60] Att i förväg definiera vad kvalitet är låter sig alltså inte enkelt göras, och är kanske inte heller alltid, utifrån Bornemarks resonemang om professionellt omdöme, eftersträvansvärt.

I sin granskning av digitalisering i offentlig sektor har Ekonomistyrningsverket dragit slutsatsen att digitaliseringsprojekt ”behöver i långt större utsträckning ske med användaren i fokus för att skapa tjänster och processer som ger ökad användar- och samhällsnytta.” Med användaren avser ESV i sin undersökning i första hand medborgaren, men samma argument torde gälla för personalen som är användare av systemen i sin yrkesroll. [61]

Digitalisering behöver dock inte nödvändigtvis syfta på stora och komplexa verksamhetsförändringar. Inom vården finns många exempel på smalare tillämpningar av exempelvis AI som fokuserar på specifika problem (som t.ex. skiktröntgenanalys).[62] Tillämpningarna bygger i allmänhet på tillgång till stora mängder medicinsk data, självlärande algoritmer och olika typer av avancerad

[57] Bornemark, 2018, s. 53.
[58] Bornemark, 2019.
[59] Hirdman m.fl., 2012, s. 273-284.
[60] Ekholm, Jebari & Markovic, 2018, s. 19.
[61] ESV, 2018, s. 6.
[62] Danielsson, 2017.

bildanalys.[63] För den enskilde kan denna typ av innovationer i vården, som alltså har potential att tidigt identifiera eller till och med förebygga hälsoproblem, göra stor skillnad i termer av hälsa och livskvalitet. Även SKR påpekar att digitaliseringen, rätt hanterad, kan bidra på olika sätt till bättre resultat och kvalitet i välfärden. Några exempel som listas av SKR är monitorering av personer med kroniska sjukdomar, diagnosmetoder för cancer och depression, användning av artificiell intelligens för att tidigt upptäcka läs- och skrivsvårigheter hos barn samt uppkopplade fastigheter som sänker driftkostnader och minskar miljöpåverkan.[64]

Samtidigt som kvalitetsargumentet alltså kan kritiseras baserat på historiska erfarenheter av offentlig förvaltnings administrationskultur (”förpappringen”), finns många goda exempel på konkreta innovationer som pekar i en annan riktning. Lite förenklat skulle man kunna säga att digitaliseringens framgångspotential i grunden beror på i vilken grad metoderna (t.ex. automatisering) kommer att leda fram till målen (t.ex. ökad kvalitet). Uppgiften att koppla samman dessa tycks vara icke-trivial.

2.2.3 Kostnadsbesparingsargumentet

Möjligheten att automatisera olika processer kan också handla om förhoppningar om ökad kostnadseffektivitet och besparingar.[65] Som framgår av de ekonomiska prognoser som görs av Sveriges kommuner och regioner (SKR) står Sverige idag inför en betydande demografisk utmaning som kommer att sätta (ytterligare) press på många kommuners ekonomi.[66] I samhällsdebatten hörs ofta argumentet att ökad digitalisering kommer att vara en del av lösningen på denna utmaning.[67] Många utredningar och rapporter argumenterar för att en digitaliserad välfärdssektor, som arbetar med större precision och tydligare fokus på personalens kärnuppgifter, kan skapa större kostnadseffektivitet.[68] Forskning om kostnader för implementering av nya tekniska system visar dock att det kan dröja länge innan ny teknik ger avkastning i termer av ökad produktivitet och/eller minskade kostnader.[69] Vad

[63] Modlitba, 2018, s. 16.
[64] SKL, 2019, s. 64.
[65] SOU 2015:28, 294; SOU 2016:85, s. 50, Andersson, Lindsjö & Hagberg, 2018, s. 24.
[66] SKR (tidigare SKL) konstaterar att befolkningen i Sverige ökar snabbt vilket innebär ”krav på kommuner och landsting att tillhandahålla ett ökande utbud av sjukvård, skola, äldreomsorg, bostäder, kollektivtrafik, individ- och familjeomsorg, vatten, vägar med mera – det som ibland brukar benämnas välfärd. Alla verksamheter påverkas, tittar vi framåt ökar antalet unga och äldre kraftigt. Antal invånare som är 80 år eller äldre beräknas öka med cirka 230 000 de kommande 10 åren (2017–2027) vilket motsvarar en ökning på 44 procent. Antalet barn i skolåldern beräknas öka med cirka 240 000, vilket motsvarar 11 procent.” SKL, 2019, s. 5.
[67] Se t.ex. Anders Wahlberg m.fl., ”Ska vi klara framtidens välfärd måste vi digitalisera”, debattartikel publicerad i *Dagens Samhälle*, den 7 februari 2019. Hämtad 2019-12-16 från https://www.dagenssamhalle.se/debatt/ska-vi-klara-framtidens-valfard-maste-vi-digitalisera-25889.
[68] Ekholm, Jebari & Markovic, 2018, s. 23; Digitaliseringsrådet 2019b.
[69] Polák, 2017; Ekholm, Jebari & Markovic, 2018, s. 23.

gäller digitalisering av komplexa verksamheter kan i själva verket kostnaden vara avsevärd, menar Ekholm, Jebari och Markovic, som påpekar att införandet av ny teknologi och nya arbetssätt ofta innebär en lång process där många olika mål och behov ska beaktas samtidigt.[70] Därtill kommer, som SKR påminner om, de långsiktiga förvaltningskostnaderna.[71]

Mot bakgrund av detta konstaterar Ekholm, Jebari och Markovic att digitalisering dessvärre har låg potential att vara kostnadsbesparande på kort sikt, men menar samtidigt att potentialen för att tackla välfärdens problem är stor på längre sikt (i rapporten talas om 50 års sikt).[72] Denna potential hänförs, som vi har sett ovan, till användandet av digitala verktyg som kan skapa ökad precision och effektivare samhällsplanering och förvaltning, men också om helt nya tillämpningar och sätt att arbeta. Nya arbetssätt, som t.ex. bygger på nya tekniska möjligheter att samla in stora mängder data, kan dock även föra med sig nya risker och sårbarheter. I betänkandet av digitaliseringsrättsutredningen 2018 konstaterades att den politiska inriktningen i Sverige är att den offentliga förvaltningen ska leda vägen när det gäller den digitala omvandlingen och att ny teknik gärna ska tas i bruk tidigt.[73] Som betänkandet påpekade sätter detta mål samtidigt ljuset på att det kommer att finnas ”ett växande behov av ett stabilt informationssäkerhetsarbete som ett fundament i myndigheternas informationshantering”.[74] Det är inte orimligt att anta att ett växande behov av informationssäkerhetsarbete också kommer att generera kostnader (vilket dock tenderar att utgöra ett frånvarande perspektiv i kostnads-besparingssammanhang).

Om kostnadsbesparingar utgör den dominerande drivkraften för att digitalisera finns en uppenbar risk att andra motiv och värden i praktiken hamnar i skymundan. Exempelvis konstaterar ESV att offentlig sektors drivkraft att effektivisera inte i första hand tycks handla om att öka den externa effektiviteten, dvs. att förbättra medborgarservicen, utan om att uppnå interna effektiviseringar i besparingssyfte: ”En hel del tyder på att det är kostnadsbesparingar snarare än medborgarfokus som driver utvecklingen.”[75]

Det finns alltså en risk att sådant som på kort sikt ses som kostnadsdrivande, som t.ex. säkerhetsaspekter, åsidosätts när nya digitaliseringsprojekt ska sjösättas. Ur ett risk- och sårbarhetsperspektiv kan därmed kostnadsbesparingsargumentet innebära en risk, om säkerhetsarbetet därmed prioriteras ned.

[70] Ekholm, Jebari & Markovic, 2018, s. 22.
[71] SKL, 2019, s. 64.
[72] Ekholm, Jebari & Markovic, 2018, s. 23.
[73] SOU 2018:25, s. 140.
[74] Ibid. ESV konstaterar när det gäller den offentliga sektorns arbete med informationssäkerhet att ”i stort sett alla” har påbörjat en diskussion eller ett arbete inom sina respektive organisationer, men konstaterar samtidigt att det bara är 36 procent inom statlig sektor och 15 procent inom kommun-sektorn som uppger att de har implementerat en modell för arbetet. ESV, 2018, s. 44.
[75] ESV, 2018, s. 59.

2.3 Svenska digitaliseringsstrategier

Sverige har tagit fram en rad strategier för att tillvarata digitaliseringens möjligheter. Det övergripande målet i Sveriges nuvarande digitaliseringsstrategi, *För ett hållbart digitaliserat Sverige*, beslutad av regeringen i maj 2017, är ”att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.”[76] För att nå detta mål har fem delmål satts upp, benämnda digital kompetens, digital trygghet, digital innovation, digital ledning och digital infrastruktur, som formulerats enligt följande:[77]

- D-kompetens: i Sverige ska alla kunna utveckla och använda sin digitala kompetens.
- D-trygghet: i Sverige ska det finnas de bästa förutsättningarna för alla att på ett säkert sätt ta del av, ta ansvar för samt ha tillit till det digitala samhället.
- D-innovation: i Sverige ska det finnas de bästa förutsättningarna för att digitalt drivna innovationer ska utvecklas, spridas och användas.
- D-ledning: i Sverige ska relevant, målmedveten och rättssäker effektivisering och kvalitetsutveckling ske genom digitalisering.
- D-infrastruktur: hela Sverige bör ha tillgång till infrastruktur som medger snabbt bredband och stabila mobila tjänster och som stöder digitalisering.

Som stöd i arbetet med att förverkliga dessa mål inrättade regeringen i mars 2017 Digitaliseringsrådet som fortlöpande bevakar områden av relevans för digitaliseringspolitiken.[78] Den övergripande digitaliseringsstrategin är dock inte den enda strategin av relevans för digitaliseringsfrågor.

I Digitaliseringsrådets nyligen utkomna rapport *En lägesbild av digital ledning* ges en översikt av närliggande strategidokument som också har bäring på digitaliseringsfrågorna.[79] Här listas *Informations- och cybersäkerhetsstrategin, Demokratistrategin, Smart industri – en ny industrialiseringsstrategi för Sverige, Strategin för skolans digitalisering, Regeringens strategi för standardisering, Bredbandsstrategin, Vision e-hälsa 2025* (inte formellt en strategi), *Nationell inriktning för artificiell intelligens* (inte formellt en strategi) samt *Med medborgaren i centrum: Regeringens strategi för en digitalt samverkande statsförvaltning*. Som nämnts ovan har en ny myndighet inrättas, Myndigheten för digital förvaltning (DIGG), som ska stödja digitaliseringen av offentlig sektor.

[76] Regeringskansliet, 2017a.
[77] Citerade från Regeringskansliet, 2017b.
[78] ”Vårt uppdrag”, Digitaliseringsrådet. Hämtad 2019-12-04 från https://digitaliseringsradet.se/vi-aer-digitaliseringsraadet/vaart-uppdrag/.
[79] Digitaliseringsrådet, 2019b.

Digitaliseringsrådet konstaterar att det ser ut ungefär på samma sätt i andra undersökta länder, ”det vill säga det finns en digitaliseringsstrategi men även ett antal andra strategier som berör specifika aspekter av digitaliseringen och ofta på liknande områden som i Sverige.”[80] Sverige anses placera sig bra i internationella digitaliseringsindex samtidigt som en oro uttrycks att utvecklingen tycks gå snabbare i andra länder.[81]

Nationella strategier har även formulerats för att hantera olika typer av it-relaterade risker och sårbarheter.[82] Regeringen planerar även att inrätta ett nytt nationellt cybersäkerhetscenter vars huvudsyfte blir att ”stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige och minska sårbarheter”.[83]

MSB:s övergripande arbete med att stödja och samordna arbetet med samhällets informationssäkerhet inriktas på strategisk nivå av den nationella informations- och cybersäkerhetsstrategin, som listar sex strategiska prioriteringar:[84]

- Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet.
- Öka säkerheten i nätverk, produkter och system.
- Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter.
- Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet.
- Öka kunskapen och främja kompetensutvecklingen.
- Stärka det internationella samarbetet.

Förutom MSB finns en rad statliga aktörer som har olika roller för det nationella arbetet med informations- och cybersäkerhet, bland annat Post- och telestyrelsen (PTS), Försvarsmakten, Försvarets radioanstalt (FRA), Polismyndigheten och Säkerhetspolisen.[85] Myndigheternas arbete samordnas genom SAMFI, dvs samverkansgruppen för informationssäkerhet. I en nyligen utkommen rapport gav SAMFI 77 förslag på olika åtgärder som kan stärka Sveriges arbete med informations- och cybersäkerhet.[86] Dessa förslag konkretiserar behov och

[80] Ibid., s. 17.
[81] ESV 2018:31, s. 8. Se även SOU 2016:89, s. 69. I EU:s digitaliseringsrapport *Indexet för digital ekonomi och digitalt samhälle (Desi) 2019 års landsrapport Sverige* framgår att ”Sverige ligger fortfarande efter andra EU-länder när det gäller öppna data (22:a plats).” (s. 12). Samtidigt framgår också att Sverige ligger på andra plats av de 28 EU-medlemsstaterna vad gäller helheten. Hämtad 2019-12-04 från https://ec.europa.eu/digital-single-market/en/scoreboard/sweden.
[82] SFS 2008:1002.
[83] ”Regeringen inleder arbetet med att inrätta nationellt cybersäkerhetscenter”, Regeringskansliet, pressmeddelande, 27 september 2019. Hämtad 2019-12-04 från https://www.regeringen.se/pressmeddelanden/2019/09/regeringen-inleder-arbetet-med-att-inratta-nationellt-cybersakerhetscenter/.
[84] Regeringskansliet, 2016.
[85] För en beskrivning av dessa aktörers roller, se SOU 2015:23.
[86] MSB, 2019, s. 9.

rekommendationer som identifierats på en mer övergripande nivå i den nationella informations- och cybersäkerhetsstrategin.

Sammantaget finns alltså en rad inriktande dokument och initiativ som alla signalerar vikten av att digitalisering sker i Sverige.

Digitaliseringsstrategier i backspegeln

Dagens digitaliseringsstrategier föregås av en rad kommissioner och utredningar under 1980- och 90-talen som har behandlat frågor om ADB (automatisk databehandling) och sedermera it.[87] Bland annat inrättade den så kallade IT-kommissionen ett ”observatorium för IT-infrastrukturfrågor” i slutet av 1990-talet i syfte att skapa ett forum för diskussioner och rekommendationer kring frågor rörande den grundläggande infrastrukturen för it.[88]

IT-kommissionens arvtagare Digitaliseringskommissionen, som bildades av regeringen i juni 2012, fick till uppgift ”att verka för att det it-politiska målet uppnås och att regeringens ambitioner inom området fullföljs” (dir. 2012:61).[89] Digitaliseringskommissionen har utkommit med en rad delbetänkanden på temat Sveriges digitala agenda.[90] Kommissionen arbete sammanfattades med slutbetänkandet *För digitalisering i tiden* (SOU 2016:89).[91]

De rapporter som publicerats av Digitaliseringskommissionen och andra aktörer visar tydligt hur analyserna har vidgats från ett teknik- och infrastrukturfokus till mycket breda samhällsperspektiv som vill betrakta digitaliseringen som en transformerande kraft som påverkar individer och samhället på alla nivåer. Man kan också tydligt se en begreppsvandring vad gäller terminologin, från *ADB* till *IT* till dagens *digitalisering*.

[87] Barck-Holst, 2005.

[88] Kommissionens arbete sammanfattades i rapporten *Framtidssäker IT-infrastruktur för Sverige* med förslag om hur regeringens mål om tillgång till ”en väl utbyggd bredbandig digital infrastruktur” skulle kunna förverkligas.” SOU 1999:134.

[89] ”Digitaliseringskommissionen - en kommission för den digitala agendan”, Näringsdepartementet, Dir 2012:61. Hämtad 2019-12-04 från https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2012/06/dir.-201261/.

[90] Digitaliseringskommissionen har utkommit med följande publikationer: *En digital agenda i människans tjänst – Sveriges digitala ekosystem, dess aktörer och drivkrafter* (SOU 2013:31); *En digital agenda i människans tjänst – en ljusnande framtid kan bli vår* (SOU 2014:13); *Gör Sverige i framtiden – digital kompetens* (SOU 2015:28); *Om Sverige i framtiden – en antologi om digitaliseringens möjligheter* (SOU 2015:65); *Digitaliseringens transformerande kraft – vägval för framtiden* (SOU 2015:91) samt *Digitaliseringens effekter på individ och samhälle – fyra temarapporter* (SOU 2016:85). Kommissionens arbete avslutades i och med slutbetänkandet *För digitalisering i tiden* (SOU 2016:89).

[91] SOU 2016:89.

Det kan slutligen noteras att det finns en grupp av relativt nybildade myndigheter som fokuserar på digitaliseringens möjligheter, t.ex. ur ett effektiviserings-perspektiv, och en annan grupp som ska fokusera på olika typer av risker och sårbarheter. I takt med ökad digitalisering torde samverkan mellan dessa grupper att få betydelse för utvecklingen i sin helhet.

2.4 Debattlinjer

Vi avslutar detta kapitel med att vidga blicken och beskriva några återkommande teman i talet om digital teknik och digitalisering. Historiskt sett har ny teknik betraktats både som ett löfte och ett hot. Digital teknik beskrivs ofta som en löftesrik vision av framtiden. Samtidigt är ord som ”död” och ”haveri” inte helt ovanliga, t.ex. i termer av ”butiksdöden” eller farhågor om bokens död, eller om misslyckade försök att digitalisera vården eller skolan.[92] Den resulterande debatten hamnar ofta i en retorik som pendlar mellan utopi och dystopi.[93] I populärkulturens mörkaste framtidsbilder beskrivs ett dystert samhälle styrt av iskalla algoritmer och mördar-drönare.[94] I de mest positiva förutsägelserna kommer den nya smarta tekniken, som t.ex. AI, att lösa vår tids stora samhällsutmaningar, inklusive klimatkrisen, och dessutom skapa helt nya oanade tillämpningar som vi knappt ens kan föreställa oss idag.[95]

Liknande pendelrörelser mellan optimism och pessimism har funnits bland forskare och debattörer som har lagt ett genusperspektiv på teknikutvecklingen: medan somliga har sett Internet som en arena för total frigörelse från gamla (inte minst biologiska) kategoriseringar, har andra tyckt sig se hur patriarkala strukturer reproduceras i it-branschernas mansdominerade styrelserum och kanske till och med i de nya algoritmernas sorteringsmekanismer. I det följande beskrivs dessa debattlinjer närmare, framstegstron och dess kritiker, liksom de genushistoriska skiftningarna mellan optimism och pessimism.

2.4.1 Framstegsperspektivet

I Sverige ackompanjerades det statliga välfärdsbygget tidigt av en framtids-orienterad teknikoptimism.[96] Att vara ett *modernt* land innebar redan under början 1900-talet att se framåt, att använda rationella, vetenskapliga metoder i samhälls-planeringen, att samla statistik för främjandet av folkhälsan liksom att omfamna

[92] Se t.ex. ”Butiksdöd väntar när digitala handeln växer”, *Svenska dagbladet*, 14 maj 2018; ”Sju år kvar – sen dör pappers-boken”, *Sundsvalls Tidning*, den 7 februari, 2013; ”Haveri i digitaliseringen av vården”, *Svenska dagbladet*, debattartikel Mårten Blix m.fl., 2 december 2018.
[93] Wormbs, 2018.
[94] Qvarsell, 2015, s. 144-163.
[95] Om AI i populärkulturen, se även Royal Society, 2018.
[96] Om teknikoptimismen i Sverige under efterkrigstiden, se Skovdahl, 1998, s. 145-165.

och utveckla ny teknik.[97] Efterkrigstidens expansiva välfärdssatsningar och stora industriprojekt förstärkte ytterligare den svenska självbilden av att vara en modern nation i framkant.[98] Måttstocken på framgång låg ofta i jämförelser med andra länder, inte minst i sammanhanget av den ökande mekaniseringen och motoriseringen. År 1969 konstaterades exempelvis att Sverige hade blivit Europas mest motoriserade land.[99]

Sverige har alltså länge präglats av en teknikoptimism som ofta kombinerats med en slags kapplöpningsretorik. I ett idéhistoriskt perspektiv kan det svenska modernitetsprojektet beskrivas som präglat av framstegstanken, det vill säga en tro på teknikens utveckling och samhällets ständiga framåtskridande mot ökat välstånd.[100] Denna tradition är tydlig även i dagens visioner om samhällets digitalisering. Som vi har sett är målet i den svenska digitaliseringsstrategin att Sverige ”ska vara bäst i världen på att använda digitaliseringens möjligheter”.[101] På Digitaliseringsrådets hemsida kan man följa hur det går:

> Sverige ligger i framkant vad gäller den digitala utvecklingen. Sveriges befolkning beskrivs i internationella index som digitalt mogen. Det finns däremot områden och trender som behöver hanteras om utvecklingen ska bestå.[102]

Samtidigt som det ofta sägs att Sverige ligger i framkant uttrycks i debatten också en oro för att Sverige ska ”halka efter”, åtminstone i relation till hur snabbt utvecklingen sker i andra länder.[103] Under rubriken *Sveriges digitalisering* beskriver Digitaliseringsrådet den kommande utvecklingen som något av en ödesfråga: ”Men om Sverige ska bli bäst i världen på att ta tillvara digitaliseringens möjligheter behövs nyfikenhet, intresse och vilja. Det är inte längre en IT-fråga utan en bred utvecklingsfråga för att stärka samhällets chanser.”[104] Viljan att bli bäst åtföljs i detta fall av viss oro för hur detta ska gå till – ett ”men” åtföljd av en uppfordran om samhällelig uppslutning. Vetenskapshistorikern Nina Wormbs har beskrivit vår tids digitaliseringsretorik i termer av ett digitalt imperativ, dvs. en

[97] Hirdman, Lundberg & Björkman, 2012.
[98] Schön, 2017.
[99] Siösteen, 1969, s. 24.
[100] Runeby, 1998.
[101] Regeringskansliet, 2017a.
[102] Digitaliseringsrådet, 2019.
[103] Se t.ex. ESV 2018:31, s. 8: ”Vi vet däremot att vi halkar efter i jämförelse med andra länder. Inte för att vi blir sämre utan för att andra länder utvecklas i snabbare takt än Sverige”. Ett par typiska rubriker: ”Sverige bäst på digitalisering? Nej, sanningen är snarare det motsatta.” (Joakim Arstad Djurberg, *Computer Sweden*, 25 november 2016, hämtad från https://computersweden.idg.se/2.2683/1.670187/sverige-efter-digitalisering); ”Sverige halkar efter – nu måste vi snabba på digitaliseringen” (Sofia Mirjamsdotter, *Sundsvalls Tidning*, 19 mars 2018, hämtad från https://www.st.nu/artikel/sofia-mirjamsdotter-sverige-halkar-efter-nu-maste-vi-snabba-pa-digitaliseringen).
[104] ”Sveriges digitalisering”, Digitaliseringsrådet. Hämtad 2019-12-04 från https://digitaliseringsradet.se/sveriges-digitalisering/.

uppmaning som inte är förhandlingsbar (människor förväntas *vilja* dessa förändringar).[105] Även mediehistorikern Pelle Snickars har uppmärksammat hur talet om internet snabbt utvecklades till en slags allomfattande och normativ agenda som alla behövde anpassa sig till.[106]

Konsekvensen av att använda en retorik där ordet digitalisering i praktiken fungerar som en synonym för det nya, moderna, smarta, effektiva och framtida kan bli, menar Wormbs, att satsningarna inte behöver motiveras, tekniken blir ett mål i sig, snarare ett medel för att uppnå något annat.[107] Det digitala imperativet är dock inte ett fenomen unikt för Sverige – tilltron till innovativa tillämpningar av digital teknik är globalt spridd och har beskrivits som ”en hörnsten i modernt regeringsarbete inom alla områden av service, omsorg och kontroll”.[108] I synnerhet inom området AI har antalet nationella strategier och policydokument exploderat de senaste åren.[109] Inte sällan är målen i dessa strategier formulerade i termer av att bli bäst eller först – inte i termer av vad som ska uppnås. Detta gäller även för Sveriges inriktning för AI vilken upprepar att ”Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter och i internationell jämförelse ligger Sverige i absolut framkant.”[110] Ett annat exempel är regeringens och SKR:s *Vision e-hälsa 2025* som slår fast att Sverige år 2025 ska vara ”bäst i världen på att använda digitaliseringens och e-hälsans möjligheter”.[111]

Samtidigt hörs också kritik mot det som uppfattas som ett alltför okritiskt anammande av ny digital teknik. På AI-området är debatten livlig vad gäller såväl etiska som säkerhetsmässiga konsekvenser av datainsamling och algoritmer som inte är transparenta eller möjliga att påverka för konsumenter (vilket vi återkommer till i kapitel 4). En närliggande debatt handlar om hur nätets rekommendationsalgoritmer (exempelvis på plattformar som Facebook) bidrar till att skapa filterbubblor där de egna åsikterna ständigt bekräftas och förstärks. Frågeställningarna kan också handla om samhällets sårbarheter i mer fysisk bemärkelse – vad händer i händelse av en kris, exempelvis ett längre strömavbrott, om allt har digitaliserats utan reservrutiner?[112]

Ibland väcks till och med frågan om hur innovativa digitaliseringsprojekt egentligen är. I Danmark har en tankesmedja med namnet Analogiseringsstyrelsen skapats med syfte att väcka debatt om vad man kallar ”en huvudlös och oövervägd

[105] Wormbs, 2010.
[106] Snickars, 2014.
[107] Wormbs, 2010, s. 148-149.
[108] Prins, Broeders & Griffioen, 2012, s. 273: ”Innovative use of new technologies is rapidly becoming a cornerstone of modern government policy in every area of service, care and control”.
[109] Cussins Newman, 2019.
[110] Regeringskansliet, 2018a, s. 4.
[111] Regeringskansliet och SKL, 2016, s. 9.
[112] ”Vad händer i samhället när it-systemen rämnar?”, *Computer Sweden*, 1 maj 2017. Hämtad 2019-12-04 från https://computersweden.idg.se/2.2683/1.681417/it-system-sverige-haveri.

tvångsdigitalisering av det offentliga."[113] Utgångspunkten är inte teknikfientlighet eller nostalgi, betonar man, utan en kritik mot "digitalismen" som man menar innebär att digitalisering alltid är svaret, oavsett frågan.[114]

Figur 2.3. Interiör från Siemens datacentral i Stockholm, årtal okänt. Fotograf: okänd/Tekniska museet. Ingår i Tekniska museets samlingar.

Kritiken av den uppfordrande retoriken negerar förstås inte möjligheten att digitalisering faktiskt rymmer stora utvecklingsmöjligheter för olika verksamheter – alltifrån innovationer inom hälso- och sjukvården till nya sätt att kommunicera eller konsumera. Samtidigt kan det medföra risker om tekniksatsningar stressas igenom utan hänsyn till grundläggande frågeställningar som kan röra själva syftet med satsningen eller frågor om etik och säkerhet. Här finns en historisk parallell till automobilismen, särskilt så som den utvecklades i Sverige under 1960 och 1970-talen då inte bara Stockholm utan i praktiken hela det svenska samhället byggdes om för att passa bilåkandet. Då var det bilismen som formulerades som

[113] Anders Colding-Jørgensen, "Mandag Morgen: Digitalismen er død", Analogiseringsstyrelsen, blogginlägg. Hämtad 2019-12-04 från https://analogist.dk/digitalismen-er-doed/. " en hovedløs og uovervejet *tvangsdigitalisering* af det offentlige".

[114] Se även Merete Mazerella, "De luddigas revansch i en teknologisk värld", *Svenska dagbladet*, 9 augusti 2019, s. 26.

ett imperativ, som en transformerande kraft och en symbol för utveckling, innovation och modernitet.

2.4.2 Feministiska perspektiv

Debatter om den digitala teknikutvecklingens relation till etik och mänskliga rättigheter har på senare tid föranletts bland annat av risken för partiskhet (bias) och diskriminering i olika slags algoritmbaserade beslutsprocesser. Ett uppmärksammat exempel är Amazons rekryteringsalgoritm som visade sig sortera bort kvinnor då systemet tränats på data som visade sig vara partisk.[115] Genus och mångfaldsfrågor har fått mycket uppmärksamhet i AI-sammanhang, inte minst på grund av incidenter som i fallet med Amazon. Men frågeställningarna handlar inte bara om tekniskt bristfälliga algoritmer. Många debattörer har uppmärksammat att den grupp som utvecklar och tar beslut om ny teknik är väldigt homogen – ungefär nio av tio Silicon Valley-chefer är män, och av deras anställda programmerare har ungefär 3% afroamerikanskt ursprung.[116] Som författaren Ellen Broad (bland andra) har påpekat är digital teknik inte ”neutral”: Algoritmer designas av människor i en social kontext, vilket innebär att ett antal större och mindre beslut fattas under utvecklingens gång. Om chefer och utvecklare befinner sig inom en snäv sfär av erfarenheter, intressen och värderingar finns en uppenbar sannolikhet att de frågor som ställs och de beslut som fattas också präglas av kulturen i denna sfär.[117] En större mångfald och jämställdare fördelning bland chefer och programmerare skapar utrymme för fler erfarenheter och intressen att mötas, vilket har visat sig vara bra för resultaten påpekar Broad.[118]

Sett i ett längre tidsperspektiv har feministisk forskning om genus och teknik tenderat att växla mellan optimism och pessimism.[119] Internets frigörande potential var något som många tog fasta på under 1990-talet då ett vanligt argument handlade om att den kroppsliga basen för könsskillnader hade blivit irrelevant i cyberrymdens virtuella världar.[120] Sadie Plant argumenterade exempelvis 1998 i boken *Zeros and Ones: Digital Women + The New Technoculture* för att digitala tekniker kommer att sudda ut gränserna mellan inte bara människa och maskin utan också mellan män och kvinnor i och med att Internet öppnat upp för var och en att experimentera med nya/alternativa identiteter. [121] Denna optimism, ibland benämnd feministisk teknofori[122], har sedermera kritiserats för att bortse från att

[115] ”Amazon scraps secret AI recruiting tool that showed bias against women”, *Reuters*, 10 oktober 2018.
[116] Susskind, 2018, s. 8. Se även Boman, 2018, s. 9.
[117] Empiriska studier har visat att marginaliseringen av kvinnor i tekniksammanhang påverkar design, innehåll och användning av tekniken (Wajcman, 2007, s. 293).
[118] Broad, 2018, s. 130.
[119] Wyatt, 2008, s. 112; Wajcman 2007.
[120] Wajcman, 2007, 291.
[121] Plant, 1998; Wajcman, 2007, s. 291; Wyatt, 2008, s. 119.
[122] Wyatt, 2008, s. 119.

virtuella världar trots allt är villkorade och präglade av den materiella världen.[123] Som Judy Wajcman konstaterade tio år efter Plants bok hade inte minst realiteten i it-branscherna förändras mindre än vad många trott, och kvinnor var fortfarande tydligt underrepresenterade i design- och utvecklingssammanhang.[124]

Även idag bryts optimism mot pessimism i debatten om den digitala teknikens framtid. Å den ena sidan beskrivs hur mobilkommunikation och sociala medier har möjliggjort att tidigare osynliggjorda grupper nu kan göra sig hörda, kommunicera och bilda intressegrupper på ett sätt som är historiskt unikt.[125] Å den andra sidan tycks skepticismen samtidigt växa vad gäller den digitala teknikens frigörande potential. Diskriminerande algoritmer, spridandet på sociala medier av hatretorik liksom förekomsten av kränkande *deep fake*-filmer (som vi återkommer till i kapitel 4) har tagits upp som ett växande hot mot såväl tilliten i samhället som mänskliga rättigheter. I Sverige har flera debattörer lyft risken för att utvecklingen inom AI – tvärtemot löften om neutralitet – faktiskt har en potential att motverka jämställdhet om systemen lär sig att reproducera könsstereotypa föreställningar om kvinnor och män.[126] I dessa sammanhang påminner många också om bristen på mångfald i teknikbranscherna: Enligt en kartläggning gjord av *World Economic Forum* är bara cirka 22% av världens AI-specialister är kvinnor.[127] I Sverige är andelen kvinnor som jobbar i IT-branschen cirka 20% och andelen som läser tekniska utbildningar 35%.[128]

Orsakerna till dessa mönster är flera och komplexa, där såväl kommersiella faktorer (t.ex. att reklam för datorer historiskt sett riktats till pojkar) som organisatorisk diskriminering har påverkat könsfördelningen i teknikbranscher.[129] Fortfarande är många populärkulturella berättelser om teknik liksom representationer av ingenjörer och vetenskapsmän präglade av könsstereotyper.[130] För att få fler kvinnor att söka it-relaterade utbildningar och jobb initieras ofta olika typer av program, på såväl lokal och nationell nivå som på EU-nivå. Problemet

[123] Wajcman, 2007, s. 292.
[124] Ibid., s. 295.
[125] Broad, 2018, s. 120.
[126] Se t.ex. Tone Marie Wahlström och Dilan Kaya, ”Utan kvinnliga utvecklare riskerar AI att motarbeta jämställdhet”, *Computer Sweden*, debattartikel, 6 mars 2019, hämtad 2019-12-03 från https://computersweden.idg.se/2.2683/1.715694/artificiell-intelligens-jamstalldhet; Malpuri Groth, ”Debatt: 100 år med kvinnlig rösträtt – nu behöver vi kämpa för jämställd AI”, *Dagens Industri*, debattartikel, 24 maj 2019. Hämtad 2019-12-03 från https://digital.di.se/artikel/debatt-100-ar-med-kvinnlig-rostratt-nu-behover-vi-kampa-for-jamstalld-ai.
[127] “The Global Gender Gap Report 2018”, World Economic Forum, 2018, s. viii. Hämtad 2019-12-04 från http://reports.weforum.org/global-gender-gap-report-2018/.
[128] ”Yrkesregistret med yrkesstatistik 2017”, Statistiska Centralbyrån, 7 mars 2019. Hämtad 2019-12-03 från https://www.scb.se/contentassets/1fe7f957920f4eaf97bddcc0270553f2/am0208_2017a01_sm_am33sm1901.pdf.
[129] Broad, 2018, s. 121; Ahuja, 2002; Hill, Corbett & St. Rose, 2010.
[130] Royal Society, 2018, s. 15.

med sådana program, menar somliga feministiska forskare, är att de lokaliserar problemet hos flickor och kvinnor och inte i hur arbete organiseras eller hur utbildning och träning genomförs.[131] Istället för att enbart fokusera på de som är frånvarande (som t.ex. kvinnor) menar t.ex. Wajcman att en djupare förståelse kräver att blicken också riktas på de praktiker som tycks leda fram till denna frånvaro.[132]

För att inte falla in i förenklade optimism- eller pessimismspår har feministisk forskning sedan 1990-talet bland annat hämtat inspiration från den forsknings-inriktning som kallas STS (Science and Technology Studies), som utgår från att samhälle och teknik formar varandra i ett ständigt föränderligt samspel mellan teknikanvändning, människor, organisationer och kulturella betydelser. Detta innebär, menar Wajcman med flera, att teknik och genus inte kan ses som fixerade poler av maktförhållanden. Istället betonas sådant som föränderlighet och motsägelser, och att teknik kan vara både en källa till och en konsekvens av genus-relationer.[133]

*

Som detta kapitel visat är debatterna om digitalisering och digital teknik livaktiga och berör många områden. Detta har sin grund i att digitala innovationer på många sätt redan har förändrat vår vardag. Att smarttelefoner idag kan användas för vägbeskrivningar, restaurangtips, bankärenden, shopping och som ett sätt att hitta information om i princip vad som helst i hela världen är ett exempel på en teknisk utveckling som hade varit svår att förutse för ett par decennier sedan. Lika svårt är det att idag förutse hur den tekniska utvecklingen kommer att ha förändrat vår vardag tjugo år framåt i tiden. Poängen med att belysa olika typer av debatter, farhågor och förhoppningar är att visa att det finns många fler perspektiv på digitalisering än de rent tekniska. Särskilt när det gäller frågeställningar om nya risker och sårbarheter står det klart att sådana sällan är begränsade till tekniken i sig utan existerar i ett fält av frågor om varför, vad, hur och för vem.

[131] Wyatt, 2008, 120.
[132] Wajcman, 2007, s. 295.
[133] Ibid., s. 293.

3 Digitala sårbarheter – begrepp och typer

> Code is the stuff nightmares, as well as dreams, are made of.[134]

I det förra kapitlet introducerades digitaliseringsbegreppet utifrån såväl nutida debattlinjer som historiska perspektiv. Detta kapitel introducerar innebörden av sårbarhet och risk i ett digitaliseringsperspektiv, dels ur ett begreppsanvändnings-perspektiv (3.1), dels ur ett bredare samhällsperspektiv där sårbarheter kan härledas till olika slags komplexitet (3.2.) liksom till strukturella och organisatoriska faktorer (3.3).

Att it-system är komplexa, sårbara och utsatta för olika typer av angrepp är ingen nyhet. Konsekvenserna av beroenden mellan olika system har varit föremål för många studier inom ramen för svensk krisberedskap.[135] Samtidigt har de senaste årens digitaliseringssatsningar rest frågor om vi nu står inför nya, eller än mer komplexa, typer av sårbarheter. Till att börja med kan man fråga sig om de begrepp vi är vana vid att använda i risk- och sårbarhetssammanhang, såsom ”system” och ”beroenden”, idag är tillräckliga för att beskriva utvecklingen. I sammanhanget av ett framväxande sakernas internet (Internet of Things) används i den engelskspråkiga litteraturen ofta begreppen ”ubiquitous and pervasive” (ungefär ”överallt och inuti allt”).[136] Som konstateras i en artikel på detta tema genomsyrar digital teknik numera nästintill varje aspekt av individuell, organisatorisk, social och ekonomisk aktivitet. Ett resultat av denna allnärvaro (*ubiquity*) är att nya sårbarheter skapas som vi ännu inte till fullo förstår.[137]

Samtidigt är inte allt okänd mark – det finns trots allt koncept och modeller att ta stöd av vid analyser av de risker och sårbarheter som kan uppstå som följd av ny digital teknik. Till att börja med introduceras därför innebörden av begreppen sårbarheter, hot och risker med exempel från det digitala teknikområdet.

3.1 Sårbarheter, hot och risker

Alla system – såväl tekniska som organisatoriska – har någon form av skyddsvärda tillgångar i sig. Det kan vara personers liv och hälsa, information, pengar, fysiska resurser och mycket annat som är skyddsvärt. I Sveriges nationella säkerhetsstrategi formuleras denna bredd av skyddsvärden i termer av ett antal

[134] Mackenzie & Vurdubakis, 2011, s. 9.
[135] Se t.ex. MSB, 2009.
[136] Ransbotham, Fichman, Gopal & Gupta, 2016.
[137] Ibid.

nationella intressen. Dessa inbegriper såväl målet att ”säkra försörjning och skydd av samhällsviktiga funktioner” som ”att upprätthålla grundläggande värden: demokrati, rättsstat, mänskliga fri- och rättigheter”.[138] Mot bakgrund av att digital teknik anses påverka alla delar av samhället följer därmed också ett behov av att studera uppkomsten av nya typer av risker och hot som kan drabba hela spektrumet av skyddsvärden.

Det skyddsvärda med informationsobjekt brukar beskrivas med termerna konfidentialitet,[139] riktighet och tillgänglighet, vanligtvis förkortade CIA efter motsvarande ord på engelska.[140] *Konfidentialitet* innebär att informationen behöver skyddas så att obehöriga inte kan ta del av den. *Riktighet* betyder att informationen inte får förvanskas eller manipuleras. *Tillgänglighet* avser att informationen ska vara åtkomlig för den som behöver den vid den tidpunkt när den behövs.

Med skyddsvärda tillgångar följer även risker för att något av dessa skyddsvärden åsidosätts, exempelvis genom att ett hot effektueras via en sårbarhet i systemet. Det finns många olika definitioner av termerna sårbarhet, hot och risk. Med utgångspunkt i den internationella standarden ISO 27000, som beskriver en vokabulär för området informationssäkerhet och it-säkerhet, går det att beskriva dem på följande sätt.[141]

- En *sårbarhet*[142] är en svaghet i ett system eller en organisation som kan leda till att en skyddsvärd tillgång[143] utsätts för skada som följd av ett hot.
- Ett *hot*[144] utgör en bakomliggande orsak till en händelse som (via en sårbarhet) föranleder skada.
- En *risk*[145] beskriver hur osäkerheter kopplade till hoten påverkar systemet eller organisation och dess målsättningar, ofta i form av de uppskattade skadekostnader som associeras med hoten. I dessa fall beskrivs en risk som kombinationen av sannolikheten för att hotet

[138] Regeringskansliet, 2017c.
[139] Ofta används ordet *sekretess* i stället för konfidentialitet. Sekretess har dock en juridisk betydelse i Offentlighets- och sekretesslagen (2009:400) och därmed en delvis annan innebörd än konfidentialitet.
[140] Eng. *confidentiality, integrity* och *availability*.
[141] ”Information technology – Security techniques – Information security management systems – Overview and vocabulary”, ISO/IEC 27000:2016, International Organization for Standardization, 2016.
[142] Definition av *vulnerability*: ”weakness of an asset or control that can be exploited by one or more threats”. Ibid., s. 14.
[143] ISO/IEC 27000:2016 saknar intressant nog definition av termen ”asset” trots att den används på många ställen i standarden.
[144] Definition av *threat*: ”potential cause of an unwanted incident, which may result in harm to a system or organization”. Ibid., s.13.
[145] Definition av *risk*: ”effect of uncertainty on objectives”. Ibid., s. 10.

verkställs och den konsekvens som i så fall följer av den oönskade händelsen.

I FOI-rapporten *Civilt försvar i gråzon* (2019) lyftes även begreppet hotbild som definierades som en aktörs *tolkning* av någonting som ett hot.[146] Att någonting tolkas som ett hot är inte liktydigt med att detta faktiskt är ett hot, och omvänt kan ett faktiskt hot föreligga utan att någon har uppfattat en hotbild.[147] Detta perspektiv på hot och hotbilder, med betoning på tolkningar och osäkerheter, är kanske särskilt relevant på cyberarenan som just karaktäriseras av en ständig möjlighet att hot kan komma att förverkligas, i form av t.ex. cyberattacker.

Hoten mot systemet eller organisationen kan vara antagonistiska eller icke-antagonistiska. Ett antagonistiskt hot innebär att någon hotagent försöker orsaka skada genom att nyttja någon sårbarhet. För att ett antagonistiskt hot ska kunna realiseras måste angriparen nyttja en så kallad attackvektor, det vill säga en väg in till systemet, mot en sårbarhet i systemet som på något sätt exponerats mot omvärlden. Ett icke-antagonistiskt hot innebär att det antingen saknas hotagent helt eller att agenten inte har någon avsikt att orsaka skada. Ett exempel på ett antagonistiskt hot är de bedragare som ringer upp äldre personer med avsikt att lura till sig pengar. Ytterligare ett exempel på ett antagonistiskt hot är utpressningsförsök mot offentliga organisationer, som i fallet där 120 franska sjukhus drabbades av utpressningsvirus (så kallat *ransomware*).[148]

Icke-antagonistiska hot uppstår på grund av sådant som misstag, olyckor och naturkatastrofer. Bränder, översvämningar och kablar som skadas vid grävarbeten är några exempel på icke-antagonistiska hot. En sådan händelse är det omfattande regnväder som drabbade Köpenhamn den 2 juli 2011, där regn motsvarande två månaders normalnederbörd föll under ett par timmar. Webbhotellet Surftown hade vid tillfället sitt primära datacenter i Köpenhamns hamn, där de stora regnmängderna ledde till att källaren – med datacentrets elcentral – översvämmades.[149] Följden blev ett omfattande driftavbrott och det tog över en vecka att återställa funktionen, då placerad i ett nytt datacenter på annan plats.[150]

Det finns även något som går att se som en hybrid mellan antagonistiska och icke-antagonistiska hot, nämligen de händelser som leder till sekundärskador (eng. *collateral damage*) som följd av olika angrepp. Ett exempel på detta är angreppet

[146] Jonsson, Ingemarsdotter, Johansson, Rossbach, Wedebrand, Eriksson, 2019, s. 65
[147] Ibid.
[148] Jarvis Wagner, "120 hospitals in France affected by massive ransomware attack: Health systems are down", *Information Security Newspaper*, 14 august 2019. Hämtad 2019-12-04 från https://www.securitynewspaper.com/2019/08/14/120-hospitals-in-france-affected-by-massive-ransomware-attack-health-systems-are-down/.
[149] Kresten Bach Søndergaard, "På väg ut ur vattenmassorna", Surftown blogg, 4 juli 2011. Hämtad 2019-12-04 från https://blogg.surftown.se/6/.
[150] Kresten Bach Søndergaard, "Återställning avklarad – uppdaterad", Surftown blogg, 10 juli 2011. Hämtad 2019-12-04 från https://blogg.surftown.se/aterstallning-avklarad/.

med den skadliga koden *Notpetya* i juni 2017, där angriparna modifierade en uppdatering av ett ukrainskt skatteprogram så att den skadliga koden följde med. Angreppet var sannolikt inte riktat mot enstaka organisationer, utan tycks ha haft en målgrupp i form av företag i allmänhet i Ukraina.[151] Notpetya var aggressivt och spred sig snabbt inom de drabbade organisationerna, däribland det danska rederiet Maersk som fraktar stora mängder med containrar över hela världen. Stora delar av Maersks datorsystem slogs ut helt och företaget förlorade tillgången till all information om fraktoperationerna under flera dagar.[152] Maersk var inte något direkt mål med drabbades ändå mycket hårt av angreppet.

Hotbilden mot it-system är hög, oavsett om det ligger några aktiva, riktade hot mot systemen eller inte. Den allmänna hotbilden mot systemen blir hög bland annat genom den stora spridning som många cyberangrepp får. I många fall är angriparna inte intresserade av något specifikt system, utan siktar snarare på en stor bredd i angreppen för att få den önskade effekten. Detta är vanligt för exempelvis utpressningsvirus, där det kan vara betydligt mer lönsamt att få många drabbade att betala en liten summa för att komma åt sina data snarare än att sikta på ett stort belopp från en enskild drabbad individ eller organisation. Allmänna hot av detta slag är svåra att värja sig mot då det alltid finns en risk att angreppen nyttjar en nyupptäckt sårbarhet eller något som är känt men ännu inte åtgärdats i it-systemen.

Asymmetrin mellan angripare och försvarare reflekteras även i Försvarsberedningens rapport *Motståndskraft* från 2017:

> Det pågår ständigt intrångsförsök mot internetanslutna system. Sårbarheter måste hanteras på både hård- och mjukvarusidan. Den som ansvarar för ett it-system måste utgå från att intrång och attacker kan lyckas, trots att en stor mängd faktiskt avvärjs.[153]

Hotbilden inom it-området beskrivs närmare av World Economic Forum som genomför en årlig undersökning över de största riskerna som världen står inför.[154] I rapporten för 2019 ligger cyberangrepp på femte plats när det gäller sannolikhet och sjunde plats när det gäller konsekvens.[155] Detta innebär att de som har svarat på undersökningen bedömer att riskerna kring cyberangrepp nästan ligger i paritet med risker kopplade till extrema väderhändelser eller risken att mänskligheten misslyckas med att hantera klimatförändringarna.

För att ett hot ska kunna förverkligas måste det finnas någon form av sårbarheter. Dessa sårbarheter kan förekomma på många olika nivåer i ett system eller i en organisation, från de lägsta tekniska nivåerna till den övergripande processnivån.

[151] Greenberg, 2018.
[152] Ibid.
[153] Försvarsberedningen, 2017, s. 116.
[154] Undersökningen bygger på svar från knappt 1000 personer som benämns som beslutsfattare inom offentlig sektor, privat sektor, akademin och civilsamhället. Mer information om undersökningen går att hitta på https://www.weforum.org/reports/the-global-risks-report-2019.
[155] World Economic Forum, 2019.

På den lägsta nivån kan det vara ett enkelt programmeringsfel i ett it-system som gör att en angripare kan ta kontroll över it-systemet. Ett exempel på en sådan sårbarhet är Heartbleed, där mjukvaran OpenSSL inte kontrollerade mottagen data på rätt sätt. Effekten av detta blev att en angripare med nätverksanslutning till systemet (exempelvis via internet) i vissa fall kunde läsa ut känslig data ur systemet.[156]

På den högsta nivån kan brister i en process potentiellt ge långtgående konsekvenser. Ett sådant exempel är när Transportstyrelsen lade ut driften av stora delar av sina it-system till ett privat bolag med verksamhet utanför Sveriges gränser. I systemen fanns ett antal olika register, bland annat vägtrafikregistret som inkluderar information om exempelvis fordon och körkort.[157] Utläggningen av it-driften gjordes efter interna beslut om avsteg från tvingande lagstiftning kring bland annat säkerhetsskydd och sekretess.[158] Detta exempel utgör en sårbarhet som inte är teknisk i sig då det inte finns några direkta problem i de tekniska systemen. Sårbarheten har i stället uppkommit i kölvattnet av digitaliseringen genom att systemen har hanterats felaktigt sett utifrån gällande lagstiftning. Mellan dessa två extremer – Heartbleed och Transportstyrelsens utläggning av it-drift – finns många andra exempel på sårbarheter i både processer och it-system, såväl inom offentlig förvaltning som privat verksamhet.

Sårbarheterna kan även vara tekniska men bygga på sådana tekniska beroenden att det är svårt för en organisation eller verksamhet att se kopplingen innan det är för sent. I oktober 2016 skedde en omfattande överbelastningsattack mot namnuppslagningstjänsten DNS hos det amerikanska företaget Dyn. På grund av angreppet gick det inte att nå ett stort antal webbplatser på internet under ett antal timmar. Förutom ett antal kommersiella aktörer, exempelvis Netflix och Amazon, så drabbades även samhällsviktiga svenska webbplatser såsom regeringen.se och krisinformation.se.[159] I detta fall var det en extern aktör som träffades av det direkta angreppet medan de olika webbplatserna endast drabbades indirekt – men effekten blev i praktiken att de aktuella webbplatserna blev helt oåtkomliga samtidigt som de ansvariga för respektive webbplats inte kunde göra mycket mer än att vänta.

Digitaliseringen har alltså en omfattande påverkan på både privata och offentliga verksamheter som i praktiken ofta är sammanvävda. Hur digitaliseringen påverkar Sverige tas upp i Försvarsberedningens rapport *Värnkraft* från 2019 som bland

[156] "The Heartbleed Bug", Heartbleed, 2014. Hämtad 2019-12-04 från http://heartbleed.com/
[157] Regeringskansliet, 2018b.
[158] Ibid.
[159] "Hacked Cameras, DVRs Powered Today's Massive Internet Outage.", *Krebs On Security*, 21 oktober 2016. Hämtad 2019-12-04 från https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/. Se även "Så sänktes Twitter och Regeringen.se i attacken", *Sveriges Radio*, 24 okt. 2016. Hämtad 2019-12-04 från https://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=6547041.

annat beskriver hur förutsättningarna för samhällsviktig infrastruktur har förändrats:

> Olika typer av industriella informations- och styrsystem är centrala för exempelvis energi- och vattenförsörjning, transporter, sjukvård, industri och livsmedelsförsörjning. Många av dessa system sträcker sig såväl tekniskt som organisatoriskt över nationsgränser. De är uppbyggda av och handhas av personal från olika delar av världen, och utveckling av systemen sker i en mängd olika länder. Datavolymer och bearbetningsförmågor i elektroniska kommunikationsnät, it-system och styrsystem ökar kontinuerligt, inte minst inom samhällsviktiga verksamheter. Sammantaget innebär denna utveckling att möjligheterna till antagonistisk påverkan genom cyberattacker och andra former av intrång blir mångfalt fler samtidigt som risken för andra allvarliga it-incidenter i form av rena olyckor också ökar. Hot blir svårare att upptäcka, riskerna blir mer svårbedömda och beroenden blir svårare att överblicka.[160]

I och med digitaliseringen blir även den digitala kommunikationsinfrastrukturen allt viktigare. När verksamheterna förlitar sig på digitala system följer ofta att de även måste förlita sig på digitala kommunikationer. Infrastrukturen är dock något som verksamheterna sällan styr över själv, utan denna köps in från externa aktörer. När de digitala kommunikationsvägarna blir essentiella för olika verksamheters operativa förmåga följer även ökade sårbarheter i verksamheterna till följd av detta beroende. Som Försvarsberedningen skriver i rapporten *Motståndskraft* från 2017 har internet ”gått från att vara viktig infrastruktur till att bli infrastrukturen för all annan infrastruktur.”[161]

Digitaliseringen innebär alltså att verksamheter förändras och att allt större del av verksamheternas funktion blir beroende av att it-system och kommunikationsnät fungerar. Därmed tillför digitalisering lätt sårbarheter då den nya, tekniska lösningen ofta för med sig såväl tekniska som organisatoriska sårbarheter. Av denna anledning krävs att både it-systemen och de sammanhang som de används i är väl fungerande för att den digitaliserade verksamheten ska fungera bra. Med professor emeritus i informatik Göran Goldkuhls ord: ”Digitala resurser kan aldrig bli bättre än sina externa förutsättningar”.[162]

3.2 Komplexitet som sårbarhet

Komplexitet behöver inte nödvändigtvis innebära sårbarheter – internet kan exempelvis beskrivas som komplext med dess miljoner servrar och datorer men just tack vare det stora antalet noder fallerar inte hela systemet om en nod blockeras. Komplexitet i meningen decentralisering och heterogenitet kan alltså innebära viss robusthet. Men i detta avsnitt fokuserar vi på komplexitet ur ett

[160] Försvarsberedningen, 2019, s. 29.
[161] Försvarsberedningen, 2017, s. 44.
[162] Göran Goldkuhl, ”Förändring och digitalisering – Varför är det så svårt?”, Linköpings Universitet, filmad presentation, 15 oktober 2019. Hämtad 2019-12-03 från https://liu.se/artikel/strimman---inspelade-forelasningar.

sårbarhetsperspektiv, och frågar oss vad det är, närmare bestämt, som skapar eller fördjupar den typ av sårbarheter som beskrevs i föregående avsnitt. Varför blir den totala systembilden så komplex?

Till att börja med karaktäriseras tekniken i sig – datorerna – av en hög grad av teknisk komplexitet, som dessutom har ökat över tid.[163] Redan 1965 skrev Gordon E. Moore, en av grundarna till Intel, en artikel där han förutspådde att det maximala antalet transistorer som får plats på en integrerad krets skulle öka exponentiellt.[164] *Moores lag*, som detta kommit att kallas, har inneburit en fördubbling ungefär vartannat år. Dagens processorer är extremt komplexa, exempelvis rymmer Qualcomm Centriq 2400 cirka 18 miljarder transistorer i en och samma krets.[165] Antalet transistorer per krets har sedan den integrerade processorns introduktion för snart 50 år ökat med ungefär 10 miljoner gånger.[166]

Mjukvaran har gått en liknande väg, där den alltmer kraftfulla hårdvaran har gett möjlighet att implementera allt fler funktioner och finesser (en vanlig kontorsdator har i storleksordningen 100 miljoner rader källkod). Komplexiteten hos såväl hårdvara som mjukvara innebär att det blir omöjligt för slutkunden att inspektera och testa systemet för att se till att det är fritt från brister och sårbarheter. Ta därtill med den komplexa leveranskedjan för it-systemen och deras komponenter så blir det uppenbart att systemen innehåller brister, åtminstone sådana som har tillkommit oavsiktligt.[167]

Utgående från komplexiteten i en enskild dator går det att vidga resonemanget till it-system bestående av sammankopplade datorer eller sammankopplade system av datorer. Även om datorerna till stor del består av liknande hårdvara och mjukvara så finns det i många fall variationer mellan dem, exempelvis olika delar i hårdvaran och olika versioner av mjukvara. Interaktion mellan olika datorsystem och kommunikation över otillförlitliga kanaler (såsom internet) lägger till ytterligare komplexitet. Dessutom interagerar system ofta med användare av olika bakgrund, med olika kompetens, med olika drivkrafter och med olika värderingar. Detta ger ytterligare en dimension av komplexitet i den totala systembilden.

Att digitalisering medför ökad komplexitet innebär ett faktum snarare än ett problem som kan åtgärdas. I sin analys av det ”digitala risksamhället” skriver Deborah Lupton att denna insikt har skapat en djup ambivalens i förhållande till

[163] Detta avsnitt bygger på FOI-rapporten *Säkra leveranskedjor för IT-system* (Eidenskog, Bildsten & Endres, 2019) som beskrivit den digitala teknikutvecklingen i större detalj.
[164] Moore, 1965.
[165] “Qualcomm Datacenter Technologies Announces Commercial Shipment of Qualcomm Centriq 2400 – The World’s First 10nm Server Processor and Highest Performance Arm-based Server Processor Family Ever Designed.”, Qualcomm, pressmeddelande, 8 november 2017. Hämtad 2019-09-09 från https://www.qualcomm.com/news/releases/2017/11/08/qualcomm-datacenter-technologies-announces-commercial-shipment-qualcomm.
[166] Eidenskog, Bildsten & Endres, 2019.
[167] Ibid.

den digitala utvecklingen: Å den ena sidan tycks den digitala tekniken utlova nya lösningar på svåra problem, men å den andra sidan tycks vårt vardagliga liv kunna raseras mycket snabbt just på grund av vårt djupa beroende av de digitala lösningarna.[168]

Fler exempel på digitaliseringens inneboende motsägelser ges i artikeln ”Ubiquitous IT and Digital Vulnerabilities” skriven av Ransbotham, Fichman, Gopal och Gupta (2016) som bland annat tar upp konsekvenserna av den digitala teknikens minskade kostnader.[169] Den positiva sidan handlar om att individer eller uppstartsföretag kan prova idéer som tidigare skulle ha krävt betydligt större investeringar och resurser. Den mörkare sidan är att även individer med illasinnade motiv har tillgång till de billiga digitala verktygen. Exempelvis sprids kunskap om säkerhetsluckor snabbt bland hackers, medan andra utnyttjar möjligheten att sätta igång storskaliga cyberattacker som inte är riktade mot något särskilt system men som kan drabba många.[170]

Ett annat exempel som tas upp av Ransbotham, Fichman, Gopal och Gupta handlar om den digitala teknikens möjliggörande av såväl ökad synlighet som osynlighet.[171] Den ökande synligheten handlar om de spår som människor eller organisationer lämnar efter sig genom att använda mobiltelefoner, browsers och sociala medier, men det kan också handla om fysiska ting som genom den ökande användningen av inbäddade sensorer och trådlös uppkoppling har blivit alltmer synliga. Som artikelförfattarna påpekar finns flera fördelar med detta: såväl organisationer som produkter kan tjäna oss bättre om de vet mer om oss, samtidigt som vi kan göra mer informerade val. Smarta saker kan göra mycket som ”dumma” saker inte kan. Den negativa sidan är att den ökade synligheten kan spåra och avslöja en hel del information som vi skulle föredra att hålla för oss själva, och som vi ofta har en rätt att hålla för oss själva. Detsamma gäller för företag och organisationer.

Samma dubbelhet finns i det parallella exemplet om ökad *osynlighet*. Paradoxalt nog möjliggör ju digital teknik också stor potential att hålla sig osynlig eller dold. Den negativa sidan av detta handlar om risken för säkerhetsintrång, påhittade identiteter, bedrägerier, falska konton, olaglig handel, nätmobbning och falska recensioner. Listan kan göras lång på problem som bottnar i möjligheten att hålla sin egen identitet eller agenda dold på den digitala arenan. Samtidigt utgör möjligheten att vara privat eller anonym en motvikt till de problem som den ökade synligheten medför i termer av ökad exponering och oönskad spårning. Det är dock denna typ av dubbelheter och paradoxer som gör det så komplext att hantera sårbarheterna: ”Denna dialektiska motsättning, där samma mekanismer som

[168] Lupton, 2016.
[169] Ransbotham, Fichman, Gopal & Gupta, 2016.
[170] Ibid., s. 4.
[171] Ibid.

skapar värde även förstärker sårbarheter, är kruxet; det är detta som gör det så utmanande att mildra sårbarheterna".[172]

3.3 Strukturella sårbarheter

De sårbarheter som beskrevs i föregående avsnitt har en teknisk grund men uppstår framför allt i praktikerna – hur tekniken används och tillämpas. Bortom användarperspektivet finns också en än större samhällelig kontext där själva organiserandet av den digitala teknikens utveckling påverkar hur sårbarheter uppstår eller hanteras. Det kan handla om hur den digitala infrastrukturen byggs ut, om samordningsbehov mellan olika aktörer eller om hur incitamenten ser ut för att arbeta med säkerhet. Som beskrevs i föregående kapitel kan även själva drivkrafterna att digitalisera innebära risker, om exempelvis en övertro på digitaliseringens möjligheter till kostnadsbesparingar eller effektivitetsökningar leder till att risker och problem inte beaktas i tillräckligt hög grad.

I den svenska kontexten har Kungl. Ingenjörsvetenskapsakademien (IVA) uppmärksammat flera av dessa faktorer. Digitaliseringens strukturella förutsättningar beskrivs av IVA i termer av "lasagnemodellen".[173] I korthet innebär denna att drift och kontroll av Sveriges digitala infrastruktur har gått från en stuprörsmodell där en aktör kontrollerar alla nivåer för sin tjänst till en situation där olika aktörer samverkar i olika lager – en lasagne. Specialiserade aktörer verkar och konkurrerar alltså på en och samma nivå (lager). Exempelvis säkerställer kommunikationsoperatörer transmission och överföring av data medan andra aktörer (företag, myndigheter och andra) erbjuder olika typer av tjänster som webbåtkomst, e-post och appar.[174]

Denna struktur, som har sina rötter i 1980-talets avregleringar, har visat sig ha flera fördelar menar IVA. Enskilda aktörer behöver t.ex. inte själva förfoga över alla lager vilket är kostnadseffektivt och leder till ökad konkurrenskraft. Dessutom skapas utbytbarhet i systemet genom att gemensamma standarder garanteras.[175] Den lasagneliknande marknadsstruktur som växt fram över tid verkar dock i praktiken inte vara så sammanhängande och välfungerande som aktörerna skulle önska. Som IVA påpekar fungerar marknaderna dåligt på flera olika sätt:

[172] Ibid., s. 2.
[173] IVA, 2019, s. 20-25.
[174] På ett sätt som påminner om lasagnemodellen beskrivs i Norges digitaliseringsstrategi *Digital 21* (2018), hur digitaliseringens tvärgående karaktär kräver att kompetenser och förmågor också utvecklas på tvärs: "Det betyr at vi må tenke annerledes om organisering. Vi må bygge kompetanse på tvers – vi må utvikle teknologier som fungerer på tvers – vi må utvikle bedrifter som opererer på tvers – vi må utvikle regelverk på tvers – og vi må sørge for at forvaltningen også kan operere på tvers." Se Digital21, 2018, s. 1.
[175] IVA, 2019, 24.

Infrastrukturens utbyggnad lider av bristande styrning och planering, beställarkompetensen är alltför låg och riskhanteringen är bristfällig. Detta får en rad konkreta konsekvenser, bland annat har det visat sig vara svårt att hitta affärsmodeller som säkerställer det politiska målet att 95 procent av alla svenska hushåll ska ha fiberanslutning år 2020. Ur ett samhällsperspektiv blir bristen på helhetssyn särskilt problematisk när det gäller just infrastrukturens utbyggnad:

> Bristen på samordning kan därför leda till onödiga kostnader eller lösningar som inte är de bästa tekniskt och systemmässigt sett ur ett samhällsperspektiv. Detta kan bli problem eftersom det är många aktörer – privata och offentliga – som i sina enskilda verksamheter driver, underhåller och investerar i infrastrukturen.[176]

Den låga beställarkompetensen vid upphandlingar är också problematisk, menar IVA, då det idag är avgörande att ordentliga konsekvensanalyser görs för den egna verksamheten. En potentiellt sett mycket allvarlig brist handlar om systemets riskhantering. Som IVA konstaterar klarar marknadsaktörerna visserligen av händelser som väntas inträffa relativt ofta, men för händelser som beräknas inträffa mer sällan krävs åtgärder och ett ansvarstagande från staten.[177] Bristen på samordning och helhetssyn gör dock att inte heller riskhanteringen blir optimal ur ett samhällsperspektiv.

Liknande slutsatser dras även i andra rapporter som har studerat digitaliseringens strukturella förutsättningar i Sverige. Exempelvis har OECD rekommenderat Sverige att öka robustheten i fibernätverk liksom att stärka samordningen av nationella, regionala och lokala digitaliseringsstrategier.[178]

Sammanfattningsvis reser dessa analyser av svenska förhållanden ett antal frågetecken: Hur kan specialiseringens fördelar bevaras samtidigt som det säkerställs att den digitala infrastrukturen byggs ut på ett sammanhängande sätt? Hur hantera risker och sårbarheter som är nya, som kan uppstå på längre sikt eller som är kända men beräknas uppstå mer sällan? Dessa frågor kan också kompletteras med ett ansvarsperspektiv. I vissa fall är det bara staten som har möjlighet att ta ett övergripande ansvarstagande för risker och sårbarheter i ett samhällsperspektiv. Samtidigt krävs samverkan och samordning med privata aktörer som driver och utvecklar infrastrukturen och tjänsterna. Även om dessa frågor är komplexa saknas det inte förslag om åtgärder och vägar framåt vilket vi återkommer till i kapitel 6.

3.4 Sårbarheter i sammanfattning

Exemplet med den mycket aggressiva Notpetya-attacken ger en illustration av den hotpotential som idag föreligger på den digitala arenan liksom vilka medel som är tillgängliga för cyberkrigföring. Som exemplet visar kan denna typ av angrepp slå

[176] Ibid.
[177] Ibid., s. 25.
[178] OECD, 2018.

brett, hårt och oförutsägbart. I kombination med att många företag och myndigheter använder samma system och tjänsteleverantörer kan konsekvenserna av cyberangrepp bli mycket stora. I Sverige finns dessutom, som beskrevs i föregående kapitel, starka drivkrafter att öka digitaliseringstakten. Detta innebär att lämpliga motåtgärder och säkerhetsstrategier blir nödvändiga för att inte öka sårbarheterna i samhället.

Som detta kapitel har visat kan digitala sårbarheter finnas på olika nivåer i samhället. Sårbarheter på *teknisk nivå* kan syfta på felaktig kod eller olika slags luckor i säkerhetsskydden som möjliggör att cyberangrepp kan effektueras. Sårbarheter på *användarnivå* och *ledningsnivå* kan uppstå genom oavsiktliga användarmisstag eller genom att regler och rutiner som syftar till skydd av system och tillgångar inte efterföljs. Dessa typer av sårbarheter handlar framför allt om hur systemen hanteras av människor. Samtidigt finns alltid ett samspel mellan teknik och teknikanvändning. Som visades i avsnitt 3.2 rymmer datorer en hög grad av komplexitet som i kombination med en komplex omgivning (olika användare, olika normer och kulturer, olika organisationer osv.) skapar ytterligare dimensioner av komplexitet i den totala systembilden. Detta förhållande, dvs. digitaliseringens inneboende komplexitet, utgör i sig en sårbarhet eftersom det ofta är svårt att förutse exakt var och hur problem kan uppstå.

Slutligen finns sårbarheter även på en *strukturell nivå* som handlar om hur organiseringen av den digitala teknikutvecklingen sker. Mot bakgrund av den stora mängd aktörer som verkar för att driva, förvalta och utveckla digital infrastruktur och digitala tjänster finns ett behov av att delarna utvecklas på ett sådant sätt att det gynnar systemet i helhet. Detta gäller inte minst hantering av risker och sårbarheter i ett samhällsperspektiv. Som beskrevs i avsnitt 3.3. finns en risk att en bristande samordning av digitaliseringens utbyggnad kan skapa eller förvärra olika typer av sårbarheter genom att infrastrukturen inte blir tillräckligt robust eller genom att säkerhetsskyddet blir bristfälligt.

4 Digitala förändringsparadigm

> Tekniska förbättringar och metodologiska framsteg rapporteras i en takt, som gör det svårt att hålla sig á jour med utvecklingen, och redan skymtar nästa datamaskingeneration, som torde komma att födas under 1960-talet och kännetecknas av ytterligare radikala framsteg.[179]

I det förra kapitlet introducerades innebörden av begreppen risker, sårbarheter och hot i det digitala perspektivet. I detta kapitel behandlas frågan om *vilka förändringsparadigm, eller trender, som formar utvecklingen och användningen av digital teknik*. I ett tekniskt och kommersiellt innovationsperspektiv finns naturligtvis oräkneliga trender som driver utvecklingen, men här har vi velat fokusera på övergripande tendenser som ökar komplexiteten och svårigheten i att bedöma risker och sårbarheter. Vi har valt att strukturera analysen utifrån vår observation att fenomen som förr var åtskilda har börjat överlappa varandra allt mer. Detta beskriver vi genom tre begreppspar, eller *förändringsparadigm* som vi valt att kalla dem:

- cyber/fysiskt – saker kopplas upp
- människa/maskin – datorer blir intelligenta
- data/individ – data driver samhället

Dessa begreppspar utgör, menar vi, tre typer av förändringsparadigm som tillsammans skapar såväl nya möjligheter som nya sårbarheter. I det första fallet beskrivs hur uppdelningen i cyber och fysiskt tidigare fungerade som en underförstådd kategorisk skillnad – cyberhot ansågs i första hand riktas mot information och data, inte mot fysiska ting som bilar och fabriker. I och med utvecklingen mot en alltmer uppkopplad värld, där även samhällskritisk verksamhet riskerar att bli exponerad mot internet, kommer denna distinktion att bli allt svårare att upprätthålla.

Begreppsparet människa/maskin fokuserar på utvecklingen av artificiell intelligens. Visserligen är det (ännu) inget problem att skilja på människor och robotar, men när det handlar om beslutsprocesser där algoritmer avgör vissa delsteg och människor andra delsteg kan det bli problem att förstå var ansvaret ytterst ligger eller hur ett visst beslut eller en viss händelseutveckling ska förklaras. Detta begreppspar kan förstås handla om mycket mer än så, som t.ex. frågor om autonoma robotsystem eller om olika typer av människa-maskin-interaktion. Utan att fördjupa oss alltför mycket i specifika forskningsfält presenteras i detta avsnitt ett antal bredare principiella frågeställningar som påverkar den sammantagna riskbilden.

[179] SOU 1962: 32, s. 27.

Begreppsparet data/individ handlar om konsekvenserna av att allt mer data, exempelvis gällande individers hälsa, vanor och intressen, blir tillgängliga för sammanställningar och analys. Som förändringsparadigm betraktat syftar detta avsnitt till att belysa innebörden av det datadrivna samhället och de nya analysmöjligheterna riktade mot den enskilda individen.

4.1 Cyber/fysiskt – saker kopplas upp

Det kommunicerande kylskåpet är ett så vanligt förekommande exempel på vad Internet of Things (IoT) är att det kanske rentav har blivit själva sinnebilden av IoT, eller *sakernas internet* som är den svenska benämningen. Andra tillämpningar som ofta lyfts fram handlar om självkörande bilar och hjälpmedel inom vården. Mindre känt är kanske att begreppet ”cyberfysiska system” i industrisammanhang istället brukar syfta på *industriella informations- och styrsystem*, förkortat ICS från engelskans Industrial Control Systems.[180] Termen cyberfysiska system definieras sällan men brukar åsyfta något som överskrider gränsen mellan cyberrymden och den fysiska världen,[181] eller kopplar samman den digitala världen med den analoga.[182] Därmed kan termen också användas om IoT som syftar på fysiska ting som via uppkoppling utnyttjar de fördelar som ”smarta algoritmer” och stora mängder data kan ge.

På grund av oklarheterna kring begreppet cyberfysiska system kommer vi här att behandla IoT och ICS var för sig. Vi beskriver drivkrafterna bakom utvecklingen liksom vilka risker och sårbarheter som denna medför. Avslutningsvis kommer vi att föra en diskussion om vad digitalisering innebär för den cyberfysiska domänen som helhet.

4.1.1 Internet of Things (IoT)

Även om IoT inte finns entydigt definierat är utgångspunkten enkel – IoT syftar på fysiska enheter och apparater (eng. *devices*) som är kopplade till internet. Dessa enheter kan bestå av små anordningar med en egen trådlös transmissionskanal men mer karaktäristiskt är att systemen åtminstone till viss del är inbyggda (eng. *embedded*) och styr eller övervakar något i sin omgivning. En definition som inkluderar även denna aspekt kommer från USA:s departement för inrikes säkerhet (Department of Homeland Security) som beskriver IoT som ”fysiskt mätande,

[180] Ibland även IACS, *Industrial Automation and Control Systems*.

[181] I standarden ISO/IEC 27032 *Information technology, Security techniques – Guidelines for cybersecurity* definieras inte “cyberfysiska system”, men väl ”cyberspace” som ”a complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.”

[182] Holm, 2017.

avläsande eller påverkande system och enheter som via interoperabla protokoll, ofta implementerade i inbyggd elektronik, sammankopplas med informationsnätverk”.[183]

Samtidigt som IoT i flera avseenden är ett nytt fenomen påpekar många att det inte är teknologin i sig som är ny utan förutsättningarna att tillämpa den som förändrats med exempelvis snabbare nätverk, bättre sensorer och billigare hårdvara. Utvecklingen mot allt fler uppkopplade enheter manifesteras inom mobiltelefonin med smartare plattformar, inom trådlös kommunikation med utvecklingen av 5G och inom datakommunikation med IPv6 (Internet Protocol version 6) som tillåter varje enskild sak att ha en unik IP-adress. Enligt International Data Corporation (IDC) sker utvecklingen främst inom konsumentelektronik och sensorer (bland annat inom industriproduktion och sjukvård) och man bedömer att Sverige är det EU-land som kommer att stå för den största procentuella tillväxten inom IoT.[184]

4.1.1.1 Betydelse och tendenser

Som beskrivits i FOI-rapporten *NCS3 Förstudie – Bortom sakernas internet* (2018) handlar mycket av IoT-diskussionen om privatkonsumtion och saker som i första hand är smarta ur ett individperspektiv.[185] Det kan dock vara svårt att i förväg få en bild av hur en teknik faktiskt kommer att användas och till vad. Möjligheterna att utbyta information med omgivningen kommer att öka, liksom möjligheten att styra saker omkring oss utifrån vilka vi är och vad vi vill, men exakt hur, vilka saker, och i vilket syfte är svårt att sia om. Drivkrafter kan handla om upplevda effektiviserings- och rationaliseringsbehov, men även den sociala aspekten är viktig – vi konsumerar inte bara produkter och tjänster för att vinna praktiska eller ekonomiska fördelar, utan också för att få status eller för att vi har vissa personliga preferenser. En ”pryl” kan stärka vår känsla av social tillhörighet.

Diskussionen om IoT handlar också om att effektivisera samhället och industrin på olika sätt.[186] Bland annat långsiktig planering avseende klimatförändringar och en åldrande befolkning utgör viktiga drivkrafter för innovation. Inom industrin finns samtidigt ett naturligt incitament att effektivisera för att maximera kapacitet och vinst. Trenden mot ökad digitalisering, som berör såväl affärs- som produktdimensionen, är således stark inom industrin. Begreppet Industri 4.0 gör gällande att vi nu är inne i den fjärde industriella revolutionen efter ångmaskinen, elektriciteten och elektroniken.[187] Digitaliseringsvisionerna handlar bland annat om att nå självorganiserande fabriker som gör kundanpassade produkter i små serier till konkurrenskraftiga priser.

[183] Förf. översättn. Se Kamrani, Wedlin & Rodhe, 2016, s. 7.
[184] Swaling & Andersson, 2018, s. 14–16.
[185] Ibid., s. 16.
[186] Ibid., s. 16-17.
[187] Schwab, 2016.

Sammantaget finns alltså flera faktorer som driver på utbyggnaden av IoT - konsumenter som önskar köpa smarta saker och tjänster, företag som vill sälja dessa saker och tjänster, industrier som vill effektivisera sin produktion och offentliga aktörer som vill effektivisera sin verksamhet. Ett exempel på det sistnämnda är satsningar på att utveckla den ”smarta staden” som innebär att många funktioner och ting kopplas upp mot ett centralt system, allt från trafiksensorer till soptunnor och lås. Denna typ av upp- och sammankoppling skapar samtidigt många potentiella vägar in vilket gör att en angripare potentiellt kan slå ut många funktioner samtidigt. Detta leder in på frågan om vilka risker och sårbarheter IoT-utvecklingen medför.

4.1.1.2 Risker och sårbarheter

När en angripare lyckas göra intrång i en IoT-enhet kan denne sedan försöka ta sig vidare in i andra enheter kopplade till nätverket. Där kan angriparen få ytterligare tillgång till uppgifter, manipulera data och införa skadlig kod. En och samma attack kan alltså drabba flera av elementen i den så kallade CIA-triaden, dvs. potentiellt både sekretess, riktighet och tillgänglighet. Samtidigt finns flera samverkande faktorer som gör traditionella it-säkerhetslösningar otillräckliga - den starka exponeringen, kommunikationen över flera olika protokoll, svaga (ofta fabriksinställda) lösenord samt att enheterna i många fall aldrig stängs av.[188]

Som beskrevs i kapitel 3 beror risken för att ett antagonistiskt hot ska realiseras i ett tekniskt system dels på attackvektorn (det sätt på vilket systemet angrips), dels på systemets inneboende sårbarheter och brister, men även på hur systemet är exponerat. I synnerhet exponeringen men även teknologins heterogenitet och designförutsättningar är viktiga faktorer i IoT-sammanhang. Vad detta innebär preciseras nedan:

- *Mångfald och heterogenitet*: Antalet uppkopplade IoT-enheter är redan stort och bedömningen är att tillväxttakten kommer att vara hög under de närmaste åren. Jämfört med dagens datornätverk förväntas också IoT bli långt mer heterogent ifråga om tillverkare, mjukvaruplattformar och kommunikationsprotokoll. Eftersom det finns en stor variation av uppgifter som en enhet kan ha uppstår också många olika typer av datainnehåll och dataformat. Detta innebär utmaningar vad gäller såväl kompatibilitet som att upprätthålla den systemförståelse som krävs för att hålla systemet säkert.[189]

- *Designförutsättningar*: IoT-enheter är ofta batteridrivna och tillgången på energi därmed en starkt begränsande faktor. Generellt sett har de också

[188] Schneier, 2017.
[189] Kamrani, Wedlin & Rodhe, 2016, s. 8.

liten processorkraft och minne jämfört med konventionella nätverksenheter. Dessa begränsningar gör att det kan bli svårt att tillämpa tillräckligt bra säkerhets- och anonymiseringslösningar.[190] I mobilt internet används säkerhetsprotokoll som är näst intill omöjliga att använda i de resursbegränsade IoT-noderna. IoT-noder kommunicerar därför generellt via långsammare och mindre säkra trådlösa media.[191] Dessutom tillverkas enheterna ofta av mindre företag som inte har samma resurser att lägga på kvalitetssäkring som större företag, t.ex. att felsöka mjukvara innan den släpps ut på marknaden.[192]

- *Exponering*: Servrar och arbetsstationer är ofta skyddade rent fysiskt (i ett serverrum, en kontorsbyggnad eller liknande) medan persondatorer och mobila enheter skyddas i ägarens närvaro. I ett IoT-nätverk kan däremot de ingående komponenterna finnas på obevakade och svårskyddade platser.[193] Det påpekas ofta att IoT förväntas bli ”ubiquitous and pervasive” (ungefär ”överallt och inuti allt”).[194] Uppkopplade enheter kommer att bäras av oss och integreras i världen omkring oss. De kommer att samla in data och kommunicera och interagera med andra enheter utan vårt tillstånd och ibland utan att vi är medvetna om det.[195] Informationen kan bland annat röra var människor befinner sig geografiskt, deras hälsotillstånd och deras levnadsvanor. Eftersom det många gånger saknas säkerhetsfunktionalitet i IoT kan en antagonist relativt enkelt extrahera och avslöja människors personliga data.[196]

4.1.2 Industriella informations- och styrsystem (ICS)

Industriella informations- och styrsystem (ICS) omfattar flera typer av system för styrning, kontroll och processövervakning. Sådana system är vanligt förekommande inom kritisk infrastruktur såsom el, drivmedel, VA, transport och livsmedelsförsörjning, men också inom industrisektorer som olja-gas, kemisk industri, och fordonstillverkning.[197] I MSB:s *Vägledning till ökad säkerhet i industriella*

[190] Ibid., s. 9. I allmänhet finns bara utrymme att använda enkla algoritmer för att uppnå bättre säkerhet eftersom beräkningskraft och energiförbrukning behöver balanseras mot varandra.
[191] Jing, Vasilakos, Wan, Lu & Qui, 2014.
[192] Schneier, 2017.
[193] Ibid.
[194] Ransbotham, Fichman, Gopal & Gupta, 2016.
[195] Kamrani, Wedlin & Rodhe, 2016, s. 9.
[196] Jing, Vasilakos, Wan, Lu & Qui, 2014. Något som bidrar till exponeringen är att individer ofta använder samma inloggningsuppgifter för alla ändamål, samt att fabriksinställda lösenord ofta är kända eller enkla att knäcka och sällan ändras av användaren. Stafford, 2016.
[197] Andra vanliga, mer eller mindre överlappande benämningar är processkontrollsystem, processautomation, process-it, tekniska it-system, anläggnings-it, distribuerade kontrollsystem och inbyggda realtidssystem (RTE). Ibland finns det också branschspecifika lösningar eller benämningar. Swaling & Sonnek, 2016, s. 18-19.

informations- och styrsystem omfattar ICS all automatisering som kontrolleras eller stöds med hjälp av informationsteknik.[198]

Industriella informations- och styrsystem är designade för att uppfylla högt ställda krav på tillförlitlighet. Systemen har traditionellt varit separerade från omgivande nätverk, med patentskyddad maskinvara och kommunikationsprotokoll för enkel felsökning, men inte med de förutsättningar för säker kommunikation som krävs i dagens it-system.[199] Nätverksbaserade tekniker gjorde sitt intåg inom ICS-design under sent 90-tal. ICS designas och implementeras numera med standardiserade datorer (t.ex. olika pc-plattformar), operativsystem, nätverk och protokoll, vilket gör att de alltmer liknar rena it-system. Ofta kopplas de samman med verksamhetens administrativa it-system för att samla in processdata och möjliggöra fjärranslutning, allt i syfte att optimera processen och öka effektiviteten.[200]

Vad är ICS?

Industriella informations- och styrsystem (ICS) kan förenklat delas in i process, kontrollcenter, och kommunikation. Därtill kommer i allmänhet en kontorsdel, dvs. en administrativ nivå som kan ha kopplingar till övriga delar.[201]

Processen innefattar de teknologier som övervakar och styr fysiska maskiner. Exempel på sådana teknologier är Remote Terminal Units (RTU), Programmable Logical Controllers (PLC), Intelligent Electronic Devices (IED) och dataundercentraler (DUC). Dessa datorer har i regel specialskrivna uppgifter, är robusta mot väder och är väl testade gällande vanliga programvarufel. De är dock oftast inte härdade mot it-attacker.

Kontrollcentret involverar centraliserad loggning, övervakning och styrning av processen. Oftast innebär detta en kombination av datalagring, dataprocessande och mänsklig övervakning. Typiskt nyttjas vanliga commercial-off-the-shelf (COTS) produkter såsom Microsoft Windows och Linux Red Hat för detta ändamål. Supervisory Control and Data Aquisition (SCADA) är en vanlig benämning för system som används inom kontrollcentret. SCADA används typiskt i system för vattendistribution samt övervakning av rör- och transportledningar inom olja-gas, elkraftnät och järnvägsnät.

Kommunikationen omfattar teknologier som nyttjas för att slussa data, dvs. fältbussar, routrar, switchar och modem.

[198] MSB, 2014.
[199] Ibid.
[200] Ibid.
[201] För en mer detaljerad beskrivning av ICS, se Swaling & Sonnek, 2016.

4.1.2.1 Betydelse och tendenser

Att styrsystemsvärlden närmar sig it-världen beror i grunden på att allt större krav ställs på sänkta kostnader och ökad funktionalitet, exempelvis gällande övervakning och styrning. Därmed har specialisering och isolering ersatts med generalisering och sammankoppling.[202] Tendensen är också att färre kundspecifika lösningar används och att systemen istället bygger på färdiga produkter. Detta har inte bara medfört ett allt starkare leverantörsoligopol utan också att kunskapen idag är ytligare om hur systemen fungerar.

Situationen kan liknas vid ett slags digitaliseringsspiral där effektivisering (med allt vad det innebär av möjligheter till fjärranslutning och fjärrstyrning, insamling av stora datamängder, etc.) driver på integrationen mellan industriella informations- och styrsystem och it. När tekniken exponeras mot internet skapas sårbarheter vilket i sin tur kräver nya systemlösningar och mer integration, som öppnar för nya sårbarheter. Detta är en ny situation för ICS-säkerhetsarbetet, men också för it-säkerhetsarbetet då hoten riktas mot fysiska processer istället för information.[203]

Figur 4.1. ”Elektronisk computer för numerisk styrning av en industriprocess (Toledo).” Fotograf: okänd/Tekniska museet. Årtal: okänt. Ingår i samlingen Tekniska museets arkiv.

[202] Holm, 2017, s. 9.

[203] Ross Anderson, “Internet of Things Problems – Computerphile”, videofilmad intervju, 17 maj 2017. Hämtad 2019-10-21 från https://www.youtube.com/watch?v=PLiE0Nr8VOE.

Genom att de administrativa systemen ofta har kopplingar mot internet öppnas en möjlighet att komma åt styrsystemen och i värsta fall störa eller slå ut processen. I särskilt kritisk verksamhet är man fortsatt noga med att isolera ICS från internet.[204] Samtidigt kan det i praktiken vara svårt att skilja ICS från it eftersom de ofta är starkt integrerade.[205] En drivkraft kan också vara så enkel som att något görs för att det går: De senaste åren har exempelvis inneburit en explosionsartad ökning av antalet ICS-enheter som är förberedda för trådlös kommunikation, dvs. med en direkt anslutningsmöjlighet till publika nätverk. Även om denna i utgångsläget inte *används*, så finns den där.[206] Vilka risker det kan innebära diskuteras i nästa avsnitt.

4.1.2.2 Risker och sårbarheter

Samtidigt som det finns lösningar för att hantera säkerhetsproblem i typiska it-system, så måste särskild försiktighet iakttas när dessa introduceras i ICS-miljö. ICS är t.ex. ofta realtidssystem som inte tolererar oplanerade avbrott. Ofta kan de inte startas och stoppas utan att produktionen påverkas. De höga kraven på tillgänglighet, tillförlitlighet och underhållsmöjlighet innebär att typiska it-strategier som t.ex. återstart inte är acceptabla.[207] Att ett system inte är uppkopplat mot internet utgör dock ingen garanti för säkerheten. Om det finns en anslutningsmöjlighet kan det räcka att någon (t.ex. en servicetekniker) ansluter en laptop eller ett USB-minne, eller glömmer att koppla ur en tillfällig anslutning, för att skadan ska vara skedd. Stuxnet är ett exempel på att fysisk separation, genom exempelvis luftgap, inte alltid ger relevant skydd.[208]

En särskild aspekt inom industriella informations- och styrsystem handlar om att den ICS-utrustning som används inom svensk industri är gammal.[209] Åldern i sig ses dock inte som ett problem – i många fall uppges att man har väl fungerande utrustning kvar från 80-talet och så länge reservdelar finns tillgängliga kan utbyten, underhåll och reparationer ske vid planerade revisioner och i många fall under drift. Fysiskt åldrande[210] får därmed sällan effekter i form av produktionsbortfall, haverier, personskador eller dylikt.[211] Däremot kan mötet mellan gammal

[204] Se t.ex. Josef Nylén, ”Efter larm om cyberhot: ’Går inte att fjärrstyra Forsmark’”, Uppsala Nya Tidning, hämtad 2020-01-14 från https://www.unt.se/nyheter/osthammar/efter-larm-om-cyberhot-gar-inte-att-fjarrstyra-forsmark-4825556.aspx.
[205] Swaling & Sonnek, 2016, s. 18-19.
[206] Valassi & Karresand, 2019.
[207] Swaling & Sonnek 2017, s. 18-19.
[208] Här spreds skadlig kod bl.a. genom USB-minnen som lämnats på en parkeringsplats och plockades upp av personal på anläggningen.
[209] I Swaling, Andersson & Mork, 2016 uppgav en aktör inom VA-sektorn att styrsystemsparken utgörs av cirka 10–15 procent ”väldigt gamla” system (25–30 år och äldre) och ca 70 procent ”medelålders” system (cirka 20 år).
[210] Typiska exempel på fysiskt åldrande är termisk påverkan på instrumentering, kablage och elektroniska delar såsom integrerade kretsar och I/O-kort.
[211] Swaling, Andersson & Mork, 2016.

och ny teknik skapa sårbarheter. Det finns många andra orsaker till att ny teknik införs, exempelvis ändrade anläggningsförutsättningar, otillräcklig funktionalitet, ändringar i säkerhetskriterier och myndighetskrav samt utfasning av obsolet utrustning, så kallat *teknologiskt åldrande*.

Digitaliseringen är ett exempel på en utveckling som i första hand medför teknologiskt åldrande med vidhängande behov av storskaliga utbyten.[212] I FOI-studien *Gammal är inte äldst* från 2016 ges exempel på vilka problem detta kan medföra:

- **Kompatibilitetsproblem**: Samfunktion mellan olika system blir mer komplicerad när gammal och ny teknik möts. Det är inte ovanligt att uppdateringar och uppgraderingar av vissa systemdelar ger kaskadeffekter i form av byten i andra delar av systemet (som i sig inte behöver bytas).[213] Kompabilitetsproblem kan också uppstå med system från olika leverantörer.[214] De kan fungera på olika sätt, i vissa fall via leverantörsspecifika protokoll eller gränssnitt. Mixen av gammalt och nytt, olika leverantörer, standarder och protokoll, kan göra systemet instabilt, men det kan också bli omöjligt att få supportgarantier för kombinationerna.[215]

- **Leverantörsberoende**: Moderna it- och mjukvarukomponenter har en relativt kort supporthorisont. I regel erbjuder leverantörerna heller inte garantier eller supportavtal för att köra gamla styrsystem på nya operativsystem vilket medför att även styrsystemen byts ut i snabbare takt.[216] I takt med att komponenter byts ut mot digitala, mjukvarubaserade motsvarigheter ändras betingelserna för systemens livscykler. Det handlar dels om att mjukvaruleverantörer uppdaterar med kortare intervaller, dels om att operatörerna själva i allt mindre grad har kompetens om, eller tillgång till, den underliggande tekniken, och därmed i mindre utsträckning själva kan göra modifieringar, säkerhetsuppdateringar och liknande. Systemen kan i värsta fall bli ”svarta lådor” som ingen vet hur de fungerar.[217]

[212] Ibid.

[213] T.ex. kan ny utrustning medföra högre hastigheter i kommunikationskanalerna vilket leder till att andra komponenter måste uppgraderas eller bytas ut. Andra exempel som ges är när de introducerade komponenterna kommunicerar med modernare protokoll, när 64- bitarsteknik ska ersätta delar av system som körs i 32-bitar, eller med I/O-kort som inte är kompatibla med ny mjukvara. I andra fall beskrivs hur den nya mjukvarubaserade tekniken inte hänger med i de gamla, snabbare, hårdvarubaserade lösningarna, exempelvis i ställverk. Ibid., s. 29.

[214] I ett exempel från processindustrin är ca 10 procent av anläggningen från Siemens och 90 procent från ABB vilket uppges räcka för att skapa bekymmer. Ibid., s. 29.

[215] Ibid.

[216] Generellt överlever komponenter längre närmast processen (decennier) och kortare längst ifrån den (några år). Som en av de intervjuade kommenterade i nämnda FOI-studie: ”Ju längre från Microsoft man kommer, desto längre kan grejerna sitta.” Swaling, Andersson & Mork, 2016, s. 31.

[217] Ibid.

- **Kompetensbrist** tas ofta upp som en viktig utmaning kopplat till systemförvaltning och underhåll. Nyutexaminerade ICS-ingenjörer lär sig hellre, och arbetar hellre med, nya system än system som är gamla eller på utgående. Vissa system uppges redan vara så gamla att endast en handfull personer i Sverige kan ge support på dem.[218] Samtidigt har de äldre ingenjörerna små möjligheter att ta till sig allt det nya. Detta kompetensglapp gör att operatörerna riskerar att bli beroende av externa resurser (såsom konsulter), oavsett om det handlar om ny eller gammal teknik.[219]

- **Feltillstånd**, dvs. sätt som en komponent kan gå sönder eller felfungera, upplevs som mer komplexa i ny utrustning än i äldre utrustning. Vid val av utrustning försöker man ofta minimera onödiga funktioner för att minska antalet potentiella feltillstånd.[220]

Sammantaget innebär detta att styrsystemsmiljön har blivit både mer komplex och mer exponerad samtidigt som det har uppstått olika typer av kompetensbrist. Till denna bild kan läggas att upphandlingskrav, för de aktörer som omfattas av sådana, upplevs som en försvårande omständighet när det gäller möjligheterna att få till en enhetlig styrsystemstruktur. Upphandlingskraven kan innebära att supportkvalitet, supporttillgång och systemkompabilitet i praktiken inte kan avgöra vilken leverantör som väljs. Man kan inte heller åberopa supportstöd eller kompatibilitetsskäl för att välja samma leverantör varje gång man ska införskaffa nya komponenter, vilket leder till att man i slutändan riskerar att sitta med ett svåröverskådligt lapptäcke av delar med varierande grad av kompatibilitet.[221]

4.1.3 Den uppkopplade världen

Det finns mycket som förenar utvecklingen inom ICS och IoT och som kan ses som uttryck för digitaliseringen av cyberfysiska system generellt. Men det finns också väsentliga skillnader.

ICS-säkerhet handlar i första hand om att skydda processen, dvs. säkerhet i klassisk *safety*-bemärkelse (funktionell säkerhet). Systemen kopplas i vissa fall upp av effektiviseringsskäl, men när de inte gör det kan det ändå finnas dolda eller latenta exponeringar mot yttervärlden genom att kopplingar finns till it-domänen, eller att utrustningen är förberedd för uppkoppling ifall det skulle behövas senare. Precis som att it och ICS alltmer smälter samman kan man givetvis tänka sig att det successivt, mer eller mindre avsiktligt, introduceras IoT-enheter i ICS-utrustning. Det har även visats hur oönskade funktioner på ett svårkontrollerbart

[218] System som nämns är bl.a. ABB-systemen AC 110 och AC 450. Ibid., s. 29.
[219] Ibid.
[220] Swaling & Sonnek, 2016, s. 38–39.
[221] Ibid.

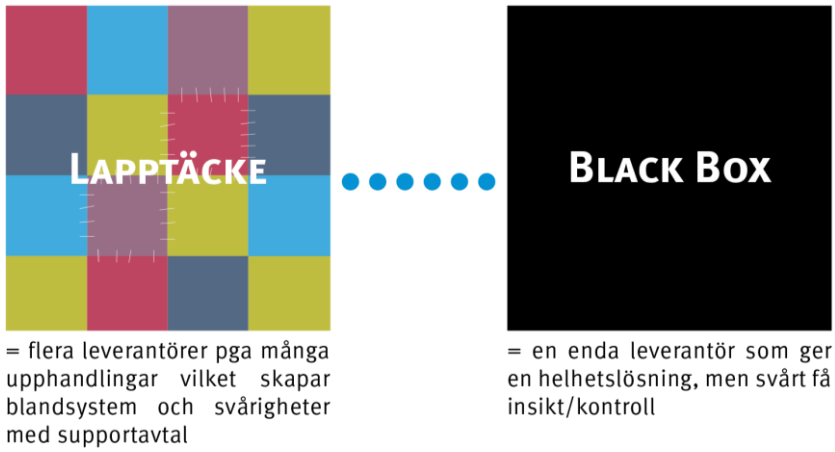
sätt smyger sig in i utrustning långt bak i leverantörskedjan.[222] Syftet kan ha antagonistiska motiv, men det kan också handla om att säkerhetsperspektivet får stå tillbaka för en vilja att vara först (eller en rädsla för att bli sist) med det nya i kombination med effektiv marknadsföring, lobbying etc. I dessa fall kan funktionerna vara fullt synliga och transparenta, men likväl svåra eller omöjliga att välja bort när de väl är på plats.

Sårbarheter kan öppna sig för den enskilda anläggningen, men de kan också få betydelse på samhällsnivå om många aktörer har samma underleverantörer samt ett större inslag av standardiserad mjukvara. Det kan röra sig om latenta fel med bäring på tillgänglighet och riktighet, men leverantörsberoendet och kopplingen till it gör också att det finns ett större inslag av kritiska data och därmed ett informationssäkerhetsproblem.

När det gäller IoT är uppkopplingen förutsatt och det är snarare mängden uppkopplade saker, vad som kopplas upp och hur detta görs som kan ha kritiska implikationer. Således kan man tänka sig att en stor mängd uppkopplade låsfunktioner i en stad sammantaget utgör en samhällsviktig funktion, medan en enstaka uppkopplad dörr inte nödvändigtvis är lika kritisk (såvida den inte öppnar upp till en kritisk produktionsanläggning). Utvecklingen inom big data och artificiell intelligens kan dessutom innebära att kritisk kunskap uppstår om ett stort antal enheter eller användare, och därmed finns också risken för oönskade händelser (både antagonistiska och icke-antagonistiska). Om kritisk utrustning är uppkopplad och om uppkopplingen är säker eller inte påverkar också riskbilden.

Jämfört med dagens datornätverk förväntas IoT bli långt mer heterogent ifråga om tillverkare, mjukvaruplattformar och kommunikationsprotokoll. När det gäller ICS finns denna tendens också, på grund av det ökande it-inslaget, men mot denna tendens står den starkare trenden att ett fåtal aktörer (som t.ex. ABB, Siemens, Honeywell och Emerson) tar över marknaden i vad som kan ses som ett leverantörsoligopol.[223] ICS-området var tidigare diversifierat, men stabilt och kontrollerat i kraft av skräddarsydda lösningar, en djup kunskap hos de enskilda aktörerna och en tydlig, *safety*-orienterad, riskbild. Med uppkopplingen tenderar lösningarna att antingen bli svarta lådor med begränsad insyn för operatören, eller lapptäcken där en aktör med överblick saknas, vilket illustreras i figur 4.2.

[222] Eidenskog, Bildsten & Endres, 2019.
[223] Swaling, Andersson & Mork, 2016.



Figur 4.2. Lapptäcke vs Black box.

På IoT-området syns inte denna utveckling lika tydligt, troligen för att området är så pass omoget. När tekniken har mognat och vi får en konvergens ifråga om tillämpningar och riskbild kan det hända att vi också ser en tydligare koncentration av aktörer. En sådan koncentration kan i sig utgöra en sårbarhet, i synnerhet om många samhällsviktiga verksamheter förlitar sig på en och samma tjänsteleverantör. Den så kallade Tieto-incidenten 2012 innebar att datalagringen slutade att fungera på ett stort antal servrar vilket orsakade stora driftstörningar hos ett stort antal myndigheter och företag under olika lång tid, vissa under några dagar och andra i flera veckor.[224] På myndighetsnivå kan det samtidigt vara svårt att ha tillsynsansvaret för en verksamhet med en komplex beroende- och sårbarhetsstruktur orsakad av en tjänsteleverantörsstruktur som inkluderar alltifrån lapptäcken till svarta lådor.

Att ett system är cyberfysiskt innebär att det överskrider gränsen mellan analogt och digitalt. Men var det ena börjar och det andra slutar är inte tydligt när i princip vad som helst kan kopplas upp och när uppkopplingen flyttas från it-system, till molnet och vidare ut i en okänd cyberrymd. Tingen som vi känner dem, var börjar och slutar de? Vad är en pryl i framtiden? Vad är närmare bestämt cyber, och vad är fysiskt när dessa världar börjar förutsätta varandra?

[224] MSB, 2012.

4.2 Människa/maskin – datorer blir intelligenta

Fokus i detta avsnitt är på utvecklingen inom artificiell intelligens (AI) som kan sägas ha en rad transformativa egenskaper. Med transformativ menas här en teknologis potential att förändra samhällen och människors levnadssätt, ofta på oförutsedda sätt.[225] I ett sårbarhetsperspektiv uppstår flera frågor: Hur hantera oförutsedda konsekvenser relaterade till AI? Vem har kontrollen och vad innebär egentligen kontroll? Vad kan illvillig användning av AI innebära?

Begreppsmässigt fungerar AI idag närmast som ett samlingsnamn för en rad olika fenomen.[226] Som matematikern Olle Häggström påpekar finns möjligen också en tendens att olika aktörer överanvänder denna typ av trendiga begrepp i syfte att vinna finansiering eller rikta uppmärksamheten mot en ny produkt eller tjänst.[227] Stora förhoppningar har även uttryckts inom offentlig sektor gällande AI:s potential att avhjälpa välfärdens utmaningar genom olika typer av automatisering och effektiviseringar (se kapitel 2). Samtidigt hörs också kritiska röster som snarare ser AI-utvecklingen som ett hot mot grundläggande värden som mänskliga rättigheter, jämställdhet, demokrati och samhällets säkerhet.

Som så ofta i framtidsinriktade teknikdebatter är det lätt att argumenten faller in i fåror av stark optimism eller mörk pessimism. Med utgångspunkt snarare i att samspelet mellan teknik och samhälle är komplex, beskrivs i detta avsnitt AI-utvecklingens drivkrafter liksom risker och sårbarheter.

Det kan inledningsvis även noteras att vad som avses med AI historiskt sett har förändrats – kreativa uppgifter som tidigare bedömts som omöjliga för en dator att utföra har i många fall visat sig vara möjliga. Samtidigt är tendensen att AI-baserade applikationer som används i vardagen ganska snabbt tappar sin aura av magi – och därmed sin status av att vara AI. Gränsen för vad AI är flyttas alltså hela tiden framåt.[228]

[225] Cussins Newman, 2019, s. 11.
[226] Broad, 2018, s. xix, Cussins Newman, 2019, s.11.
[227] Häggström, 2019, s. 14-19.
[228] Bostrom, 2016, 14.

Vad är AI?

Artificiell intelligens är, som många konstaterat, notoriskt svårt att definiera.[229] Detta beror bland annat på det finns många olika uppfattningar om vad *intelligens* är. Forskarna Stuart Russel och Peter Norvig har beskrivit hur definitioner av AI tenderar att variera enligt två nyckeldimensioner: på den ena axeln syftar intelligens antingen på tankeprocesser eller på beteenden, på den andra syftar intelligens antingen på mänsklig intelligens eller på en slags idealföreställning av intelligens.[230]

Själva begreppet artificiell intelligens myntades i samband med det så kallade sommarprojektet i Darthmouth 1956 då en grupp forskare formulerade övertygelsen att datorer kan läras att lösa problem som man tänker sig att bara människor kan lösa.[231] Sedan dess har över 70 olika definitioner på artificiell intelligens föreslagits.[232]

En definition av AI som ofta citeras idag är att "artificiell intelligens handlar om att göra maskiner intelligenta, och intelligens är den kvalitet som möjliggör att något kan fungera på meningsfulla sätt och med framsynthet i förhållande till sin miljö.[233] Artificiell intelligens kan också beskrivas i termer av sin nytta där vanliga tillämpningsområden handlar om optimering, sökningar/ rekommendationer och diagnoser/prediktion.[234] Stora framsteg har också gjorts inom området mönsterigenkänning där tillämpningar kan handla om ansiktsigenkänning och översättning mellan olika språk.[235]

Kritik finns också mot att överhuvudtaget använda begreppet intelligens om datorer. Den svenske filosofen Hans Ruin menar att bilden av intelligens som bara abstrakt symbolhantering, utan koppling till kropp och livssammanhang, är alltför snäv.[236] Frågan är också, menar Ruin – och påminner här om vad filosofen Martin Heidegger tog upp redan 1953 i skriften *Teknikens väsen* – vad tron på maskinell intelligens gör med människans självförståelse. Om vår förståelse av teknik leder till en teknisk förståelse av oss själva riskerar vi kanske också att lättare avsäga oss ansvar och omdömesförmåga.[237]

[229] Ibid.
[230] Russell & Norvig, 1995.
[231] Bostrom, 2014, s. 6-8.
[232] Cussins Newman, 2019, s. 11.
[233] Formulerat av Nilsson, 2010, citerat i Renda, 2019.
[234] Renda, 2019. Exempel på tillämpningar är optimering av logistikkedjor, diagnosticering av sjukdomar, eller skräddarsydda rekommendationer till slutanvändare.
[235] Cussins Newman, 2019, s. 8.
[236] Ruin, 2018.
[237] Ibid.

4.2.1 Betydelse och tendenser

Två faktorer brukar anges som en förklaring till de senaste årens snabba utveckling inom AI, dels den ökade tillgången till datorkraft och dels den ökade tillgången till stora datamängder.[238] I kombination har dessa faktorer möjliggjort att den metod som kallas maskininlärning fått stora framgångar. Maskininlärning innebär i korthet att systemet löser en uppgift genom att ”tränas” på stora dataset istället för att följa hårdkodade regler.[239] Särskilt användningen av så kallade djupa neuronnät har varit framgångsrik inom områden som språköversättning, datorseende, talsyntes och rekommendationssystem.[240] Denna typ av maskininlärning, så kallad *deep learning*, använder sig av många processande lager som sammantaget utvinner information från data.[241] I detta sammanhang förekommer även begreppet algoritm; i dess mest basala mening är en algoritm helt enkelt kod (ett program) designat i enlighet med vissa logiska samband.[242] En algoritm kan syfta på allt ifrån en enkel statistisk formel till ett avancerat sök- och rekommendationssystem.

De AI-baserade system som finns idag räknas alla till vad som brukar kallas ”smal AI” som klarar av att lösa väldefinierade smala uppgifter (som att spela schack eller framföra ett fordon). Förhoppningar (och farhågor) finns dock om att AI-system i framtiden kommer att klara av att hantera mer generella problem. Steget från olika typer av prediktiva eller mönsterigenkännande beräkningar, baserade på stora datamängder, till kontextberoende bedömningar är dock fortfarande långt: dagens AI-system förlitar sig i grunden på kvantitativa analyser men har svårare att göra kvalitativa analyser som kräver en förståelse av kultur och sammanhang.[243]

En tillämpning som ofta lyfts fram som ett område med stor potential handlar om AI-assisterat beslutsstöd. Vad gäller förmågan att fatta beslut är det välkänt att människor tycks vara ohjälpligt dåliga på att fatta rationella och objektiva beslut – de är inte bara fördomsfulla och känslosamma utan är dessutom lättpåverkade av

[238] Cussins Newman, 2019, s.11; Andersson, Gustavi & Karasalo, 2019, s. 75.
[239] Royal Society, 2017, s. 19.
[240] Nilsson, Luotsinen, Schubert & Svenmarck, 2017.
[241] Cussins Newman, 2019, s.11. En mer precis beskrivning är att djupa neuronnät består av ett system med ett stort antal seriekopplade lager av parallellkopplade neuroner, där ett neuron är en enkel beräkningsenhet (en funktion som processar in- och utsignaler). Se Nilsson, Luotsinen, Schubert & Svenmarck., 2017, s. 3.
[242] Broad, 2018, s. xviii.
[243] Amerikanska DARPA (The Defense Advanced Research Projects Agency) skiljer i detta sammanhang på tre nivåer, eller ”vågor” av AI: Den första vågen beskrivs i termer av manuell kunskap som syftar på system som kan lösa avgränsade problem och beskriva ett resultat. Den andra vågen handlar om statistiskt lärande vilket inbegriper neurala nät med förmåga att lära och göra prediktioner. Dessa system har dock fortfarande inte någon förmåga att förstå de kontexter inom vilka de agerar. Den tredje vågen, som ännu inte inträffat, kallar DARPA för kontextuell anpassningsförmåga. Antagandet är här att denna typ av system ska kunna utvecklas med en kontextuell modell av sig själva och världen, vilket skulle ge dem förmåga att resonera och göra abstraktioner. Se Cussins Newman, 2019, s. 9.

faktorer som maskiner inte påverkas av som t.ex. hunger och trötthet.[244] Men, som vi återkommer till i avsnitt 4.3., kan inte heller data eller algoritmer betraktas som helt neutrala.[245] Data kan t.ex. utgöra ett snedvridet urval samtidigt som algoritmerna som ska användas för beslutsstödet har utvecklats och designats av just människor. Förslag som syftar till att minska risken för partiskhet (eng. *bias*) i AI-baserade beslutsstödsystem handlar ofta om att främja en öppenhet och transparens för hur algoritmer designats och data samlats in.[246]

Figur 4.3. Datacentral IKEA, Älmhult, 1971. Fotograf: okänd/Järnvägsmuseet. Ingår i samling: Järnvägsmuseets foton.

Enligt vissa bedömare ligger den största nyttan med AI i dagsläget i *kombinationen* av maskinella och mänskliga styrkor, där den artificiella intelligensen används för att hitta mönster, medan människan står för kreativ analys och högre beslutsfattande. Ett exempel är läkarens stöd av AI för medicinsk diagnos, där AI-systemets styrka är dess möjlighet att utföra statistiska analyser av stora mängder bilder i kombination med andra medicinska data, medan läkarens styrka utgörs av

[244] Kahneman, 2013.

[245] Fall med upptäckt av algoritmer som genererat snedfördelning och partiskhet i resultaten (*bias*) har väckt en debatt om användning av AI för prediktiva och beslutande funktioner. Se t.ex. O'Neil, 2017; Catherine Tucker, "Algorithmic Bias or Fairness: The Importance of the Economic Context", The Ethical Machine, Shorenstein Center, 13 november 2018. Hämtad 2019-12-03 från https://ai.shorensteincenter.org/ideas/2018/11/12/algorithmic-bias-or-fairness-the-importance-of-the-economic-context.

[246] Broad, 2018.

erfarenhet och förståelse för det unika sammanhang som varje patient representerar.[247]

AI-tillämpningar kan existera i virtuella miljöer såväl som inbäddade i fysiska objekt.[248] Att fungera med framsynthet i förhållande till sin miljö, som en av definitionerna av AI formulerar det, kräver framför allt någon grad av självständighet i systemet.[249] Men vad som exakt menas med självständiga, eller autonoma, system är dock ofta oklart. Mer eller mindre autonoma system finns i många produkter idag – en vanlig bil består av flera funktioner som i någon mån är autonoma, som t.ex. bromssystem, adaptiv fartkontroll och självparkeringssystem. Bilar körs fortfarande av människor men en rad funktioner kan alltså assistera föraren eller till och med ta över kontrollen för en kortare stund. En grundläggande fråga blir därmed när vi egentligen anser att ett system är autonomt (eller semi-autonomt). [250]

För att reda ut vad som menas med autonoma system skiljer Paul Scharre i boken *Army of None* (2018) på tre dimensioner av autonomitet. För det första vilken typ av uppgift maskinen utför, för det andra vilken roll människan har i systemet, och för det tredje vilken grad av komplexitet som ligger bakom maskinens beslutsfattande.[251] Den första dimensionen är betydelsefull eftersom inte alla uppgifter har samma tyngd och risk. En termostat är ett autonomt system som ges kontroll över temperaturreglering medan *Terminator*-filmens Skynet gavs kontroll över kärnvapenkoderna.

Den andra dimensionen, enligt Scharres indelning, handlar om vilken möjlighet till kontroll människan har i systemet. En beslutsloop kan förenklat sett sägas bestå av momenten *observera*, *orientera*, *besluta* och *agera*.[252] Scharre beskriver i detta sammanhang hur människan kan vara i loopen, ovanpå loopen eller utanför loopen.[253] I det första fallet krävs ett mänskligt beslut innan maskinen kan agera, i det andra fallet övervakar människan processen och kan avbryta om så skulle behövas, medan människan i det tredje fallet inte har möjlighet att ingripa i tid. I detta senare fall är systemet alltså helt fristående från mänsklig inblandning, förutom vad gäller de ingående parametrar som systemet fått i designstadiet.

[247] Modlitba, 2018, s. 21
[248] Renda, 2019, s. 4
[249] Nilsson, 2010.
[250] Scharre, 2018, s. 27.
[251] Ibid.
[252] I militära sammanhang används den så kallade OODA-loopen för att beskriva ett beslutsförlopp i termer av *Observe, Orient, Decide* och *Act* (Scharre, 2018, s. 23). Gustavi, Karlholm, Oskarsson, Beran m.fl. (2019) beskriver hur området artificiell intelligens kan delas upp i delområden som väl matchar OODA-loopens komponenter: *Observe:* Sensordatabehandling, perception och informationsinhämtning, *Orient:* Kunskapsrepresentation, omvärldsuppfattning, *Decide:* Planering, problemlösning, slutledning, *Act:* Styrning.
[253] Scharre, 2018, s. 29-30.

Den tredje dimensionen handlar om intelligens och vilken komplexitet i sin omgivning som maskinen klarar av att hantera. En enkel mekanisk termostat som ställts in med en önskvärd temperatur har två val: att aktivera värmesystemet om temperaturen har blivit för låg eller aktivera kylsystemet om temperaturen har blivit för hög. En självkörande bil har många fler parametrar att ta hänsyn till. Eftersom det inte är möjligt att programmera i förväg exakt hur en bil ska agera under en färd måste den ges flexibilitet att själv bestämma när den exempelvis ska bromsa, köra vidare, svänga eller byta fil. Som Scharre påpekar är den högre komplexiteten i autonoma system ett tveeggat svärd. I praktiken kommer komplexa system att upplevas som svarta lådor vars handlande inte nödvändigtvis kan förutses. Om maskinerna beter sig på ett oväntat sätt finns därför en risk för obehagliga överraskningar ur användarnas perspektiv. Frågan är vilka möjligheter till kontroll som finns eller borde byggas in – och om blandningen av mänskliga och maskinella beslut i sig kan medföra risker.

I grunden väcker tanken på självständigt agerande maskiner eller system frågor om när mänsklig intervention är önskvärd och i så fall hur sådana människa-maskin-system ska utformas.

4.2.2 Risker och sårbarheter

Användning av AI kan både minska, öka och skapa nya sårbarheter. Stora förhoppningar finns om att olika typer av automatiserade AI-baserade verktyg skulle kunna minska de sårbarheter som oundvikligen finns i komplexa it-system. System som utvecklats under lång tid kan i många fall liknas vid ”spretiga vidunder”, sammansatta av en mängd olika delsystem vars underhåll ofta är eftersatta.[254] Som en konsekvens tenderar därför många system att vara mer eller mindre osäkra. I kombination med brist på personal med rätt kompetens finns därför en stor lockelse att undersöka möjligheterna att använda olika slags AI-verktyg i syfte att öka säkerheten (ett exempel är automatiserad sökning efter sårbarheter i mjukvaran).[255] Men möjligheten att använda AI för identifiering av sårbarheter i mjukvaran kan också användas för att lätta på arbetsbördan för de som planerar intrång och attacker.[256] Det finns därför incitament till en accelererande kapplöpning, eftersom AI kan användas för både försvar och attack.

På temat försvar och attack har mycket uppmärksamhet även riktats mot utvecklingen av mer eller mindre autonoma vapensystem.[257] Risken att en accelererande kapprustning kommer att skapa allt mer avancerade och dödliga autonoma vapensystem har väckt en internationell debatt som mynnat ut i krav på ett internationellt förbud eller reglering av så kallade LAWS (Lethal Autonomous

[254] Brundage m.fl., 2018, s. 31.
[255] Ibid., s. 33.
[256] Ibid.
[257] Scharre, 2018, s. 75.

Weapon Systems).[258] Debatten om denna typ av vapensystem, som har såväl folkrättsliga som etiska och militära dimensioner, förs i många forum, bland annat i FN:s nedrustningskommission för konventionella vapen.[259]

Bortom den oroväckande tanken på en accelererande utveckling mot dödliga autonoma vapensystem finns ett antal andra oklarheter relaterade till frågan om mänsklig kontroll över AI-system.

4.2.2.1 ”Datorn säger nej” – kontrollproblemet

”Datorn säger nej”-frasen har kommit att beteckna en stelbent attityd hos stora organisationer eller företag som, baserat på felaktig eller bristfälligt lagrad information, nekar kunder service.[260] På senare tid har farhågor väckts gällande algoritmer som används för att exempelvis göra kreditvärderingar eller sålla bland sökande till en tjänst eller till en utbildning. Å ena sidan har AI-system visat sig effektiva för hantering av denna typ av stora mängder rutinartade beslut. Å andra sidan kan ett beslut som är rutinartat på systemnivå uppfattas som livsavgörande på individnivå. Ur ett etiskt perspektiv kan därför frågan uppstå om vilken acceptans som finns för beslut som avgörs av en algoritm som man inte förstår eller kanske misstänker baseras på skeva premisser.[261]

Möjligheterna för offentlig sektor att tillämpa innovativ digital teknik, som AI, inom områden som service, omsorg och kontroll har väckt stora förhoppningar om effektiviseringar och förbättrad kvalitet, men har också rest frågor om hur denna tekniska utveckling påverkar individens kontroll i förhållande till den statliga kontrollen.[262] Frågan om individens möjlighet att navigera i stora byråkratiska system är förstås inte ny. Stephen Cave, chef för Leverhulme Centre for the Future of Intelligence (CFI), påminner om den vision Franz Kafka formulerade kring 1915 i sin roman *Processen*, en parodisk berättelse om en likgiltig byråkratisk statsapparat där beslut fattas med stora konsekvenser för en människas framtidsutsikter utan att denne själv har möjlighet att påverka.[263] I Kafkas

[258] Hagström, 2016.

[259] Som påpekas av Gustavi, Karlholm, Oskarsson, Beran m.fl. (2019) finns ingen vedertagen definition av LAWS, och det kan vara oklart om termen inkluderar system som redan finns eller om det handlar om möjliga framtida system. Målsökande robotar utvecklades redan under andra världskriget, men utvecklingen av AI har sedan dess gett möjlighet till ett mer komplext autonomt uppträdande (Ibid.)

[260] Denna catch phrase har sitt ursprung i den brittiska humorserien *Little Britain* där en banktjänsteman (sedermera hotellreceptionist) bemöter kunder genom att knappa in deras ärende i datorn för att sedan leverera svaret att datorn säger nej (”computer says no”), oavsett kundens fråga “Computer says no”, *Wikipedia*. Hämtad 2019-12-03 från https://en.wikipedia.org/wiki/Computer_says_no.

[261] Lupton, 2016, s. 5.

[262] Prins, Broeders & Griffioen, 2012, s. 273.

[263] Stephen Cave, “To save us from a Kafkaesque future, we must democratise AI”, *The Guardian*, debattartikel, 4 januari 2019.

berättelse är systemet komplext och ogenomträngligt; det sorterar människor i vinnare och förlorare, men sorteringens kriterier förblir oklara; de som utvärderas vet inte vilka data systemet har samlat om dem, eller med vilken data de jämförs. Ingen verkar heller vilja ta ansvar för systemets beslut, den som tillfrågas hänvisar enbart till sin kugge i systemet.

Hundra år senare, menar Cave, har vi datoriserade system som beskrivs på liknande sätt av dess kritiker – system som kan få stora konsekvenser för den enskilda individen men som ändå är otransparenta och svåra att ställa till svars.[264] Med detta vidgade historiska perspektiv belyser Cave ett annorlunda perspektiv på intelligens som inte tar sin utgångspunkt i jämförelser med mänsklig intelligens utan med en slags byråkratisk systemintelligens som har sina rötter i 1900-talets byråkratier:

> Med andra ord, intelligens i artificiell intelligens är inte intelligensen hos en människa – inte den hos en kompositör, en vårdgivare eller doktor – det är systemintelligensen hos en byråkrati, hos maskinen som processar stora mängder data om människors liv för att sedan kategorisera dem, sätta dem i fack, ta beslut om dem och placera dem där de passar in. AI:s problem liknar den kafkaeska statens eftersom de är en produkt av dem. Josef K skulle omedelbart känna igen ”datorn säger nej”-kulturen i vår tid.[265]

Detta perspektiv på intelligens som byråkratisk kontroll påminner om Jonna Bornemarks resonemang om samhällets fixering vid mätbarhet (se kapitel 2). Samtidigt finns stora möjligheter med AI inom en rad olika områden som ger utrymme för just det som ofta efterfrågas, nämligen mer tid för omsorg och möten mellan människor. Ett exempel är den så kallade Trelleborgsmodellen där införandet av AI-stöd för rutinartade beslut om försörjningsstöd frigjorde tid för personalen att träffa sina klienter.[266] Ur ett demokratiperspektiv diskuteras samtidigt fortsatt om det är rimligt att algoritmer som påverkar många människor ofta är affärshemligheter som inte medger möjligheter till transparens och insyn.[267]

I den populärvetenskapliga litteraturen om AI brukar kontrollproblemet handla om mänskligheten kontroll över sin framtid i vidare mening.[268] De exempel som diskuterats i detta avsnitt har alla handlat om så kallad smal AI, dvs. program som

---

[264] Ibid.

[265] Cave, 2019: “In other words, the ‘intelligence’ in ‘artificial intelligence’ is not the intelligence of the human individual – not that of the composer, the care worker or the doctor – it is the systemic intelligence of the bureaucracy, of the machine that processes vast amounts of data about people’s lives, then categorises them, pigeonholes them, makes decisions about them, and puts them in their place. The problems of AI resemble those of the Kafkaesque state because they are a product of it. Josef K would immediately recognise the ‘computer says no’ culture of our time.”

[266] Ranerup & Henriksen, 2019.

[267] “Digitala utanförskapet: Minister ifrågasätter techbolagens affärshemligheter”, *Dagens Nyheter*, 26 augusti 2019. Hämtad 2019-12-03 från https://www.dn.se/ekonomi/digitala-utanforskapet-minister-ifragasatter-techbolagens-affarshemligheter. Se även Susskind, 2018, s. 150.

[268] Bostrom, 2014; Tegmark, 2017.

syftar till att lösa vissa väldefinierade uppgifter. På sikt förutspås dock en utveckling mot generell AI (*artificial general intelligence*, eller AGI) som likt en människa kan ta sig an en mängd olika typer av problem och uppgifter. Farhågan i detta sammanhang handlar om att en sådan generell AI skulle kunna utveckla en superintelligens vars mål och agerande inte säkert kan förutses eller nödvändigtvis sammanfalla med mänsklig etik och värderingar.

För att undvika globala katastrofala händelseutvecklingar har många debattörer rekommenderat mer forskning kring den så kallade *alignment*-problematiken, det vill säga frågan hur man kan säkerställa att agerandet hos generella AI-system inte kommer att hota mänsklighetens existens.[269] Detta utgör det yttersta kontrollproblemet vilket också har varit föremål för många böcker, filmer och tv-serier.[270] Filosofen Hans Ruin menar dock i detta sammanhang att det stora intresset för superintelligens riskerar att överskugga de mer vardagliga problem som redan finns här och nu, frågor som t.ex. rör arbetslivets påverkan, politisk kontroll eller hur den mänskliga självförståelsen påverkas av AI-utvecklingen: ”Snarare än över ’superintelligens’ borde vi kanske oroa oss över den ’superdumhet’ som hotar när människan inte längre anser sig behöva tänka för att hon tror att hennes verktyg gör det åt henne.”[271]

4.2.2.2 Oförutsedda konsekvenser

En risk inom all teknikutveckling handlar om oförutsedda eller oavsiktliga konsekvenser. Ett välkänt exempel från den digitala sfären är den så kallade *flash crash*-incidenten som inträffade år 2010 på den amerikanska börsen då en triljon dollar raderades från marknaden genom ett olyckligt samspel mellan säljalgoritmer och tradingprogramvara.[272] Raset kunde återställas, delvis tack vare en automatiserad stoppfunktion, men händelsen illustrerar hur svårt det kan vara att förutse hur algoritmer – måhända enkla var för sig – kommer att samverka under specifika omständigheter.

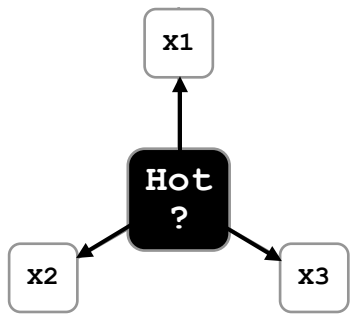
De senaste åren har utvecklingen inom AI möjliggjort fler och än mer avancerade varianter av automatisering i en rad olika branscher. Den höga graden av komplexitet kan samtidigt medföra svårigheter för människor att förstå, kontrollera eller verifiera hur systemen har kommit fram till sina resultat. System som bygger på t.ex. maskininlärning har kallats ”svarta lådor” av denna anledning. Den så kallade black box-problematiken rymmer såväl säkerhetsmässiga som

[269] Ibid.
[270] För exempel, se “Artificial Intelligence in fiction”, Wikipedia. Hämtad 2019-12-18 från https://en.wikipedia.org/wiki/Artificial_intelligence_in_fiction.
[271] Ruin, 2018.
[272] Bostrom, 2014, s. 20-21. Se även Felix Salmon & John Stokes, “Algorithms Take Control of Wall Street,” *Wired*, 27 december 2010. Hämtad 2019-12-03 från https://www.wired.com/2010/12/ff-ai-flashtrading/.

etiska dimensioner: inom branscher med höga säkerhetskrav (som t.ex. flygplanstillverkning) måste varje komponent eller delsteg kunna isoleras och kontrolleras på ett verifierbart sätt, medan beslut inom vården eller i militära sammanhang som handlar om liv och död måste kunna förklaras och härledas. Oöverblickbara black box-system uppfyller inget av dessa krav. Forskning pågår i detta sammanhang som syftar till att skapa transparens i AI-system och hitta sätt att integrera metoder för att återskapa beslutsvägar och begripliggöra resultat.[273]

En aspekt som brukar tas upp i detta sammanhang är också AI:s potential för *dual use*, dvs. dubbla användningsområden. Produkter som ursprungligen tagits fram för ett visst syfte kan flyttas över till andra användningsområden. Ett exempel är ansiktsigenkänning som skulle kunna användas för att identifiera eftersökta terrorister lika väl som politiska dissidenter. Ytterligare ett exempel handlar om förhoppningen att AI-verktyg ska kunna stärka säkerheten i komplexa it-system som nämnts ovan, men denna typ av utveckling stimulerar sannolikt också mer sofistikerade attacker.[274] Hur balansen i denna kapplöpning kommer att falla ut är svårt att förutse.

Hotperspektivet i detta avsnitt har sammanfattningsvis utgått från systemet i sig som hot, dvs. risken att en AI-tillämpning skapar oklarheter kring exempelvis beslutsfattande eller att möjligheten till kontroll och förutsägbarhet (figur 4.4). I nästa avsnitt byter vi perspektiv och beskriver hot som uppfattas komma utifrån och riktas mot det system som vi vill skydda (figur 4.5).



Figur 4.4. Hot *inifrån* systemet: I detta fall uppfattas hotet komma från själva systemet, som kan uppfattas som en black box som antas oavsiktligt kunna rubba viktiga principer och säkerhetsaspekter (X1-X3), som t.ex. tydligt ansvarstagande, rättvist beslutsfattande och möjligheten till kontroll och förutsägbarhet. Jämför figur 4.5.

[273] Gustavi, Karlholm, Oskarsson, Beran m.fl., 2019, s. 10.
[274] Ibid., s. 12.

4.2.2.3 Illvillig användning

Illvillig användning av artificiell intelligens kan potentiellt föra med sig allvarliga konsekvenser för en rad olika skyddsvärden.[275] Genom att skaffa sig tillgång till data, algoritmer och tränade modeller kan en angripare relativt enkelt manipulera exempelvis mönsterigenkänningsfunktioner som därmed kommer att ge felaktiga resultat. Ett bildigenkänningssystem kan på detta sätt fås att tro att en bild på en skåpbil (fordon) föreställer en Siberian husky (hund) genom att insignalen till systemets neuronnät manipuleras.[276]

Användning av AI kan också möjliggöra att sofistikerade attacker kan utföras på en större skala än tidigare. I rapporten *The Malicious Use of Artificial Intelligence* beskrivs bland annat hur automatiserade *spear phishing*-system kan användas för att skräddarsy tweets baserat på användares intressen, vilket i sin tur kan genera en stor mängd klicks på en illvillig länk.[277] AI-baserade språkgenereringstekniker kan också användas för att rikta budskap mot grupper av människor som använder ett visst språkbruk. Med andra ord möjliggör AI attacker som är storskaliga men ändå personliga (*customized*).[278] Rapportförfattarna beskriver i sin slutsats att AI förändrar hoten på tre olika sätt:[279]

- Genom att existerande hot *förstärks*: I och med att kostnaden sjunker för att utföra storskaliga, avancerade angrepp (som tidigare krävde mänsklig expertis och arbete) blir gruppen av möjliga angripare också större.
- Genom att *nya* hot uppstår: AI kan användas på nya sätt som människor inte skulle ha kunnat tillämpa, och kan också användas för att överlista försvararens system.
- Genom att *karaktären* på hoten ändras: Angrepp med hjälp av AI kan bli effektivare, mer precisa, svårare att härleda. Angreppen kan också bli bättre på att utnyttja sårbarheter i andra AI-system.

Samspelet mellan dessa hot och utvecklingen på andra områden, som t.ex. ett växande IoT, skapar också nya sårbarheter – AI-understödda attacker i den cyberfysiska miljön skulle kunna orsaka stor skada på infrastruktur och andra samhällsfunktioner.[280] Utvecklingen av autonoma robotar och drönare som potentiellt kan användas för att attackera människor eller materiella mål utgör ett annat exempel på hot som egentligen uppfyller alla tre ovan beskrivna förändringsfaktorer: angrepp från luften är inget nytt fenomen i sig, men kan med billiga drönare bli möjliga att utföra av i princip vem som helst (förstärkning); hotet är samtidigt nytt eftersom drönare kan konfigureras på nya sätt, t.ex. genom

[275] Brundage, Avin, Clark, Toner m.fl., 2018, 53.
[276] Nilsson, Luotsinen, Schubert & Svenmarck., 2017.
[277] Brundage, Avin, Clark, Toner m.fl., 2018, s. 33.
[278] Ibid.
[279] Ibid., s. 5.
[280] Ibid. s. 40.

att sättas samman i svärmar eller skickas in i utrymmen där andra farkoster tidigare inte nått, och karaktären av hotet ändras när precisionen av angreppet ökar samtidigt som angriparen kan hålla sig gömd.[281]

Sammantaget gör möjligheten till illvillig användning av AI att hotbilden blir mer komplex liksom att spektrumet av skyddsvärden som kan drabbas utökas i jämförelse med vad traditionell krisberedskap brukar fokusera på: Illvillig användning av AI är inte bara ett hot mot fysiska tillgångar (som kritisk infrastruktur) utan även mot demokratiska värden och nationell säkerhet. I detta sammanhang kan särskilt nämnas samspelet mellan automatisering och AI: genom användning av bots och botnets kan algoritmer manipuleras till att göra felaktiga prediktioner eller rekommendationer (Facebook har uppskattat att plattformen är ”infekterad” av cirka 60 miljoner bots).[282] Användningen av bots i det amerikanska presidentvalet 2016 visar tydligt att det finns en marknad för teknik som kan förstärka och sprida negativ eller falsk information.

Även fenomenet *deep fake* har fått ökande uppmärksamhet den senaste tiden.[283] I korthet handlar deep fake om möjligheten att manipulera ljud och video på sätt som gör att aktörer ser ut att säga och göra saker som de inte har gjort. Med hjälp av avancerade maskininlärningsmetoder, baserade på *deep learning*, blir resultaten idag så bra att det kan vara nästintill omöjligt att skilja på autentiskt och fabricerat material.[284]

Implikationerna av deep fake är potentiellt ett allvarligt hot mot såväl enskilda individer som demokratiska processer och tilliten i samhället i stort menar författarna till rapporten *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*:

> Idéernas marknadsplats lider redan av ett sanningsförfall i takt med att våra nätmiljöer interagerar på förgiftande sätt med våra kognitiva tendenser att vara partiska. Deep fakes kommer att förstärka detta problem avsevärt. Individer och företag kommer att möta nya former av utnyttjande, skrämseltaktiker och personligt sabotage. Även riskerna för vår demokrati och vår nationella säkerhet är djupgående.[285]

---

[281] Regleringar på detta område har införts de senaste åren både i USA och i EU: USA:s Federal Aviation Administration (FAA) införde ett regelverk för drönare i augusti 2016 och i juni 2019 antog den europeiska flygsäkerhetsbyrån regler för civila drönare som kommer att börja gälla inom EU från juni 2020. MSB, 2018a, s. 65-66. För information om EU:s regelverk för drönare, se ”EU wide rules on drones published”, EASA, pressmeddelande, 11 juni 2019, hämtad 2019-12-03 från https://www.easa.europa.eu/newsroom-and-events/press-releases/eu-wide-rules-drones-published.

[282] Chesney & Citron, 2018, s. 12. En bot (ordet kommer från ordet robot) är enkelt uttryckt ett automatiserat program som körs på internet.

[283] Marcus Jerräng, ”Deepfakes är det läskigaste på nätet just nu – och ett tydligt exempel på riskerna med AI”, *ComputerSweden*, 31 januari 2018. Hämtad 2019-12-12 från https://computersweden.idg.se/2.2683/1.696965/deepfakes-riskerna-med-ai.

[284] Ajder, Patrini, Cavalli & Cullen, 2019.

[285] Chesney & Citron, 2018, s. 1: “The marketplace of ideas already suffers from truth decay as our networked information environment interacts in toxic ways with our cognitive biases. Deep fakes

Ett möjligt scenario är att en video med en politiker dyker upp dagen före ett val där denne säger något upprörande eller skandalöst.[286] Risken är här att den politiska kandidaten ifråga liksom den demokratiska processen hinner ta stor skada innan videons falskhet hinner avslöjas. Paradoxalt nog uppstår en annan typ av risk ju högre allmänhetens medvetenhet blir om deep fakes – genom att utnyttja människors skepsis kan även äkta inspelningar avfärdas om de inblandade påstår att de har blivit utsatta för fabricering.[287] Deep fakes skulle alltså kunna göra det enklare att undgå ansvar för sådant som faktiskt har hänt. Denna lögnarens fördel (”liar’s dividend”) kan i längden utgöra ett hot mot tilliten i samhället och demokratiska processer.[288]

Det dominerande användningsområdet hitintills för fabricerat videomaterial har dock inte varit politiskt utan pornografiskt, vilket påminner om att det finns en tydlig genusdimension på deep fakes. Typiskt handlar det om att kända skådespelerskors ansikten klipps in pornografiska filmer som sedan görs tillgängliga via olika typer av siter på internet. Rapporten *The State of Deepfakes*, som kartlagt hur deep fakes används och sprids, visar att detta har blivit ett etablerat fenomen på internet med många miljoner visningar för de filmer som innehåller kända skådespelerskor.[289] Juristen Danielle Citron har i detta sammanhang betonat allvaret i att deepfake-teknik relativt enkelt kan förvandlas till ett vapen mot kvinnor som är skrämmande, kränkande och förnedrande och som kan leda till en känsla av otrygghet.[290] Ironiskt nog har alltså en teknik utvecklats under samma tidsperiod som me too-rörelsen (som riktade ljuset mot sexuella övergepp) som utgör en ny attackvektor riktad främst mot kvinnor.

Med sin kapacitet att skapa falska digitala identiteter utgör deep fakes och fabricerat material även ett växande cybersäkerhetsproblem.[291] Under 2019 upptäcktes exempelvis visuella anomalier i profilfotot på två olika Linkedin-konton som visade sig vara påhittade identiteter (med syntetiskt genererade foton).

---

will exacerbate this problem significantly. Individuals and businesses will face novel forms of exploitation, intimidation, and personal sabotage. The risks to our democracy and to national security are profound as well.”

[286] Ibid., s. 3.

[287] Ibid, s. 28.

[288] Ibid., s. 4. Se även Jennifer Finney Boylan, “Will Deep-Fake Technology Destroy Democracy?”, *The New York Times*, debattartikel, 17 oktober 2018. Hämtad 2019-12-03 från https://www.nytimes.com/2018/10/17/opinion/deep-fake-technology-democracy.html.

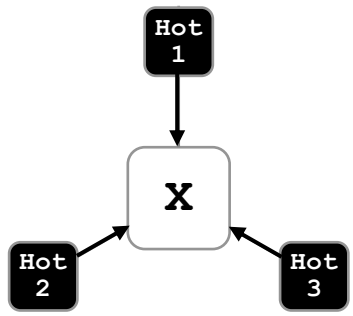
[289] Ajder, Patrini, Cavalli & Cullen., 2019, s. 7. Diskussioner och inlägg på online-forum visar också att det finns ett intresse bland användare som vill producera denna typ av filmer föreställande före detta flickvänner. Chesney & Citron, 2018, s. 17.

[290] Danielle Citron citerad i Ajder, Patrini, Cavalli & Cullen, 2019, s. 6: “Deepfake technology is being weaponized against women by inserting their faces into porn. It is terrifying, embarrassing, demeaning, and silencing. Deepfake sex videos say to individuals that their bodies are not their own and can make it difficult to stay online, get or keep a job, and feel safe.” Se även Chesney & Citron, 2018, s. 18.

[291] Ajder, Patrini, Cavalli & Cullen., 2019, s. 13.

Det ena kontot försökte samla information relaterad till företaget Tesla, det andra försökte få kontakt med amerikanska regeringstjänstemän (båda kontona togs bort från Linkedin). Att olika slags manipulering (*social engineering*) används för åtkomst av information, vare sig det handlar om affärshemligheter eller spionerі, är förstås ingen nyhet. Det nya är att deep fakes och syntetiskt genererade bilder kan förstärka, eller skapa nya, metoder för att uppnå dessa mål.[292]

De exempel som anförts i detta avsnitt utgör långt ifrån en heltäckande beskrivning av möjlig illvillig användning av AI. En slutsats som kan dras är dock att AI ser ut att möjliggöra attacker som både är mer storskaliga och sofistikerade (skräddarsydda) samt att gränserna håller på att suddas ut inte bara mellan människa och maskin utan också mellan äkta och falskt.



Figur 4.5. Hot *mot* systemet: Perspektivet i detta fall handlar om hot som kommer utifrån mot något skyddsvärt (X), t.ex. någon typ av digital infrastruktur eller samhällsfunktion, som vi vill skydda. Hotverktygen (1-3) kan handla om storskaliga automatiserade attacker, riktade attacker eller manipulation. Jämför figur 4.4.

4.3 Data/individ – data driver samhället

Analys av aggregerade datakällor med stora datamängder, så kallad *big data*, har växt till ett stort teknikområde på senare år. Analysföretaget Gartner definierar big data som ”informationstillgångar med stor volym, stort informationsflöde och/eller stor variation som kräver kostnadseffektiva och innovativa sätt att bearbeta informationen för att möjliggöra förbättrad insikt, beslutsfattande och processautomation”.[293]

Big data är ett område med stor potential för att kunna hitta nya sätt att ta fram och analysera information inom alla upptänkliga områden. Big data-analyser kan

[292] Ibid.
[293] “Big Data”, Gartner Glossary. Hämtad 2019-07-10 från https://www.gartner.com/it-glossary/big-data/.

användas för att stödja forskning, underlätta sjukdomsdiagnoser, spåra epidemier, hitta efterlysta personer, minska trafikstockningar och otaliga andra ändamål. Som med alla större tekniska innovationer följer även ett antal problem som måste hanteras för att tekniken ska ge maximal nytta utan att utsätta vare sig samhället eller enskilda individer för oacceptabla risker. Detta avsnitt diskuterar några övergripande risker med big data.

4.3.1 Betydelse och tendenser

Data har blivit en vara som säljs och köps på en global marknad, där datamäklare (eng. *data brokers*) är företag som specialiserat sig på att köpa, aggregera och sälja vidare data. Aggregeringen tillför värde i processen genom att ytterligare information går att extrahera ur den aggregerade datamängden jämfört med indatamängderna var för sig. Ett exempel på en datamäklare är amerikanska Acxiom, som år 2018 sade sig ha omfattande data om 700 miljoner konsumenter runt hela världen.[294] Enligt amerikansk lagstiftning behövs i dagsläget inte samtycke för att behandla så kallad icke-känslig data (Acxiom 2018), vilket innebär att företagen fritt kan behandla stora mängder personlig data utan att informera berörda personer eller att de får godkänna behandlingen.[295]

Två stora användningsområden för konsumentdata är marknadsföring och riskbedömningar.[296] Riktade marknadsföringskampanjer är mer kostnadseffektiva än bredare kampanjer, vilket är en stark drivkraft för massanalyser av konsumentdata. Med allt mer riktad marknadsföring följer risken att mindre nogräknade företag kan rikta reklam för tveksamma produkter och tjänster till avgränsade men sårbara konsumentgrupper, exempelvis i form av dyra krediter riktade till äldre personer med spelmissbruk.[297]

Privatpersoner delar med sig av personlig data till många olika företag då det ofta är ett villkor för att använda företagens produkter och tjänster. Delningen kan ske genom uttrycklig interaktion, som på sociala medier, och genom tyst datainsamling i samband med exempelvis webbsurfning, mobilapplikationer, aktivitetsklockor, uppkopplade bilar och andra IoT-enheter. Stora företag som interagerar med slutanvändare – såsom Amazon, Google och Facebook – har tillgång till mycket omfattande datamängder som täcker en stor del av befolkningen i Sverige. Möjligheterna att dra intressanta slutsatser vid dataanalyser ökar med mängden data som finns tillgänglig. Även relativt små mängder information från sociala medier kan räcka för att kunna dra slutsatser om användaren när det gäller sådant

[294] ”2018 Annual Report”, Acxiom. Hämtad 2019-08-22 från http://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_ACXM_2018.pdf
[295] Ibid.
[296] Christl, 2017.
[297] Favaretto, De Clercq & Elger, 2019.

som politiska och religiösa övertygelser, etniskt ursprung, personlighetsdrag och sexuell läggning.[298]

Även myndigheter och andra aktörer inom den offentliga förvaltningen har tillgång till enorma mängder data om landets medborgare, företag, geografi, väder och mycket mer. För medborgare finns det exempelvis data om födelsedatum, inkomst, bostadsadress, släktskap, anställningar, utdömda straff, bidrag, studielån, skulder och fastighetsinnehav. Diskussioner om samkörning av olika register brukar dyka upp i debatter om exempelvis bidragsfusk, då det är normalt sett inte är tillåtet att göra samkörning inom offentlig förvaltning av integritetsskäl.[299] Inom det privata näringslivet är olika typer av samkörning, det vill säga mer omfattande och avancerad aggregering av datamängder, ett stort och växande affärsområde. Problemet med samkörning – som alltså gränsar till teknikerna inom big data – är att det potentiellt går att missbruka den sammantagna informationsmängd som uppstår när olika register aggregeras.

När flera datakällor kopplas samman kan det ge möjligheter som inte är uppenbara sett till respektive källa. Som en forskargrupp har visat kan en kombination av data ur olika mängder användas för att positionera en mobiltelefon utan användning av telefonens inbyggda positioneringsfunktioner.[300] Genom att kombinera exempelvis kartdata och väderdata från internet med telefonens tidzon, lufttryck och accelerometerdata kan de lokalisera telefonen med god noggrannhet efter att den har förflyttat sig en kortare sträcka. Detta exempel visar hur kreativ analys i kombination med nya sätt att lägga samman data kan ge information som till synes inte finns i datamängden. Om stora mängder data av många olika typer kombineras blir potentialen för analyser och slutsatser enorm.

4.3.2 Risker och sårbarheter

Riskbedömningar av olika slag utgör beslutsunderlag när konsumenter exempelvis tar lån, tecknar försäkringar, hyr lägenhet och söker arbete. Riskbedömningarna kan därför påverka enskilda konsumenter stort, till exempel om ett lån nekas eller godkänns på felaktiga premisser. Med allt större datamängder tillgängliga för dem som genomför riskbedömningarna följer möjligheten att ta fram bättre beslutsunderlag men även faran att underlagen väger in irrelevanta faktorer eller diskriminerande värderingar. Det finns alltså risker med denna typ av riskbedömningar då det inte är säkert att data förbättrar våra beslut:

[298] Kosinski, Stillwell & Graepel, 2013.
[299] SOU 2017:39.
[300] Mosenia, Dai, Mittal & Jha, 2018.

> Data präglas av rörighet och komplexitet. Data kan vara ofullständig, partisk, bedräglig. Den kan vara föråldrad. Den kan utgöra en dålig representation av det som vi faktiskt vill mäta. Data kan vara ett dokument över det förflutna utan att vara en förutsägelse av framtiden.[301]

Samtidigt finns en risk att den information som kommer ut från ett datorsystem, i form av exempelvis underlag och beslut, ändå ses som sanningen då det är en maskin som producerat informationen.[302] Argumentet är att människors uppfattning färgas av erfarenheter, känslor och värderingar medan algoritmer maskinellt bearbetar data och därmed ofta ses som ofelbara i sina slutsatser. Men då även algoritmer och datamängder kan vara behäftade med olika brister, inklusive explicita eller implicita värderingar, finns det risk för att slutsatserna påverkas av dem.[303]

För en utomstående kan det vara mycket svårt att få insyn i algoritmer som används för analys av big data. Algoritmerna är ofta mycket komplexa och är därmed svåranalyserade. De utgör dessutom i regel affärshemligheter, varför externa parter inte får ta del av och undersöka algoritmerna. Alla algoritmer tas fram med ett syfte och det finns risk för att olika typer av värderingar byggs in i dem. Det kan vara såväl explicita som dolda värderingar från exempelvis beställare och utvecklare, men även värderingar eller avvikelser som följer med algoritmens eventuella träningsdata.[304] Dessutom baseras resultaten från många algoritmer på egenskaper på gruppnivå, snarare än individnivå, samtidigt som gruppindelningen kan vara implicit och oklar.[305]

Hur data samlas in kan få stor påverkan på hur väl besluten speglar verkliga förhållanden. Ett illustrerande exempel är *Boston Street Bump App*, en mobilapplikation som lanserades 2011 och som använde sensorer i användarnas smarta mobiltelefoner för att detektera och rapportera hål i Bostons gator. Det blev snabbt tydligt att data som rapporterades från mobilapplikationen var snedvriden då oproportionerligt många rapporter gällde områden med rikare och yngre befolkning, där användningen av smarta mobiltelefoner var betydligt högre än i andra delar av staden.[306]

Fallet med Boston Street Bump App illustrerar hur orättvisor kan uppstå som effekt av den *digitala klyftan*, det vill säga skillnaden mellan personer som har tillgång till och intresse av att använda it och de som inte har det. I detta fall reagerade myndigheten bakom applikationen snabbt, men fallet visar tydligt hur

[301] Broad, 2018, xiii. ”But data doesn’t always improve our decisions. Data is messy and complicated. It can be incomplete, biased, fraudulent. It can be out of date. It can be a poor proxy for the thing we’re actually trying to measure. It can be a record of the past without being a prophecy of the future.”
[302] Favaretto, De Clerq & Elger, 2019.
[303] Ibid.
[304] Vedder & Naudts, 2017.
[305] McGregor, Murray & Ng, 2019; Favaretto, De Clerq & Elger, 2019.
[306] Gent, 2016.

bristande dataunderlag riskerar att leda till felaktiga, orättvisa eller diskriminerande beslut. I andra lägen, där bristerna i insamlad data inte är uppenbara eller där många olika källor aggregeras, finns en märkbar risk att det leder till beslut med motsvarande brister. Sådana fall kan leda till att såväl nya orättvisor uppkommer som att befintliga strukturer befästs i samhället. Automatiserad analys kan också leda till att nya grupper, som inte är sammansatta på uppenbara sätt, utsätts för orättvisor eller diskriminering.[307]

Som McGregor, Murray och Ng (2019) betonar måste utdata från algoritmer i form av beslut eller beslutsunderlag användas med försiktighet när det gäller frågor som kan påverka exempelvis individens rätt till frihet (såsom beslut inom rättsväsendet) eller skydd mot diskriminering (såsom riskbedömningar där etniskt ursprung indirekt vägs in). De konstaterar att algoritmer blir allt mer sofistikerade och att transparensen sjunker, vilket försvårar spårbarhet och bedömningar av om algoritmernas resultat är förenliga med de mänskliga rättigheterna.[308]

[307] Favaretto, De Clerq & Elger, 2019.
[308] McGregor, Murray & Ng, 2019.

5 Digitaliseringens problem – den svenska kontexten

> Vi här i socknen vill inte vara sist. Vi är istället före på många områden. Vi är pionjärer.[309]

I föregående kapitel beskrevs tre förändringsparadigm som karaktäriserar den digitala utvecklingen – cyber/fysiskt, människa/maskin och data/individ. I detta kapitel återvänder vi till den svenska kontexten och undersöker ett antal problemområden som uppstått i digitaliseringens svallvågor. Som vi ska se har dessa områden ofta en direkt koppling till förändringsparadigmen, men i vissa fall tycks även inhemska traditioner, attityder och vägval spela en roll för vilka problem och sårbarheter som förstärks just i den svenska kontexten.

Baserat på såväl aktuell litteratur som genomförda intervjuer fördjupar vi i detta kapitel nio problemområden som vi benämner som följer: *(o)takten*, *kompetensen*, *infrastrukturen*, *exponeringen*, *asymmetrierna*, *tilliten*, *styrningen och samordningen*, *förväntningarna* samt *Plan B*.

5.1 (O)takten

Går digitaliseringen för snabbt i Sverige? Eller kanske för långsamt? Svaret på dessa frågor beror på vilket perspektiv som anläggs. De strategier och visioner som betonar digitaliseringens möjligheter varnar framför allt för att utvecklingen i Sverige verkar gå långsammare jämfört med andra länder.[310] Samtidigt noteras också att det ibland tycks gå för fort när verksamheter ska digitaliseras, exempelvis genom att säkerhetsfrågorna förs in alltför sent i processen.[311] Detta kan resultera i att digitaliseringssatsningar hamnar i ett gasa/bromsa-mönster när problem väl måste hanteras.[312]

Ett grundläggande problem tycks handla om underskattningar av den tid som krävs för att skapa säkra och användarvänliga system, vilket medför, som det uttrycks i en av våra intervjuer, att det ”slarvas med grunden”. [313] Detta kan få allvarliga följdverkningar: dels att tjänster skapas som motverkar sitt syfte (genom att de

[309] Ivar Lo-Johansson (1951), *Analfabeten: en berättelse från min ungdom*, Stockholm: Bonnier. Publicerad som e-bok 2013 av Albert Bonniers förlag.
[310] Se t.ex. Digitaliseringsrådet, 2018b, s. 48; ESV 2018:31, s. 8.
[311] Internetstiftelsen, intervju, 2019-09-02; MSB, intervju, 2019-09-27.
[312] MSB, intervju, 2019-09-27.
[313] Internetstiftelsen, intervju, 2019-09-02.

skapar ökade kostnader, ineffektivitet och frustration snarare än nytta), dels att sårbarheter och säkerhetsbrister byggs in i de nya systemen.[314]

En forcerad digitalisering av offentlig sektor med huvudfokus på förenklingar och service snarare än korrekthet och säkerhet riskerar också, som Delegationen för korrekta utbetalningar från välfärdssystemen nyligen konstaterat, att leda till större felaktiga utbetalningar från välfärdssystemen (se även avsnitt 5.7).[315]

Samtidigt som signalen från strategidokumenten är att myndigheterna ska vara drivande vad gäller digitalisering tycks det alltså finnas ett gap mellan behovet av säkerhet och förutsättningarna att bedriva säkerhetsarbete.[316]

5.2 Kompetensen

En god kunskaps- och kompetensförsörjning brukar lyftas fram som en nyckelfaktor i it-sammanhang. I Sverige har dock olika typer av kompetensbrister påtalats på detta område, som inte enbart handlar om brist på ingenjörskompetens. Även vikten av humanistisk och samhällsvetenskaplig forskning har diskuterats på senare tid, särskilt i AI-sammanhang. Ytterligare en typ av kompetensfråga handlar om de ökande kraven på beställarkompetens i offentlig sektor. Bristerna inom dessa tre kompetensområden beskrivs närmare nedan:

- *Humanistisk och samhällsvetenskaplig kompetens:* Behovet av mer humanistisk och samhällsvetenskaplig kompetens inom AI brukar motiveras med att de nya tillämpningarna berör hela samhället inom en rad domäner, inklusive de politiska, sociala, juridiska och ekonomiska.[317] Digitaliseringsrådet skriver i lägesrapporten *Digital kompetens* att Sverige behöver ta sig an utmaningen kring AI utifrån andra aspekter än enbart tekniska och rekommenderar därför särskilda satsningar på forskning inom hållbar AI. [318]

[314] Ett uppmärksammat exempel i Stockholm är den så kallade skolplattformen som orsakat ett stort missnöje bland föräldrar, personal och elever. Kritiken har dock inte enbart handlat om dålig användarvänlighet utan även om säkerhetsbrister som gjorde det möjligt för obehöriga att komma åt personuppgifter och annan känslig information om både elever och lärare (”Stockholm panikstänger skolplattform – ’Chockerande att säkerheten är så dålig’”, *Ny Teknik*, 21 augusti 2019. Hämtad 2019-12-03 från https://www.nyteknik.se/sakerhet/stockholm-panikstanger-skolplattform-chockerande-att-sakerheten-ar-sa-dalig-6968823; ”Omfattande kritik mot Skolplattformen”, SVT Nyheter, 22 augusti 2019. Hämtad 2019-12-03 från https://www.svt.se/nyheter/lokalt/stockholm/omfattande-kritik-mot-skolplattformen.).

[315] SOU 2019:59, s. 22.

[316] IVA, 2019.

[317] Emma Byrne, ”From ethics to accountability, this is how AI will suck less in 2019”, *Wired*, 27 december 2018. Hämtad 2019-12-03 från https://www.wired.co.uk/article/artificial-intelligence-2019-predictions; Stefan Larsson, ”Breddad AI-forskning kan vägleda politikerna”, *Svenska Dagbladet*, debattartikel, 17 oktober 2018. Hämtad 2019-12-03 från https://www.svd.se/breddad-ai-forskning-kan-vagleda-politikerna.

[318] Digitaliseringsrådet, 2018b, s. 33.

- *Ingenjörs- och specialistkompetens*: Samtidigt som mer bredd efterfrågas tycks Sverige även ha en utmaning vad gäller de tekniska kärnkompetenserna.[319] Visserligen har Sverige i en internationell jämförelse en hög andel specialister på området informations- och kommunikationsteknik, men efterfrågan är betydligt större än utbudet, och ingenjörsbristen förväntas öka de närmaste åren.[320] Mot bakgrund av dessa trender, samt att regeringen har utpekat digital kompetens som en strategisk fråga för Sverige, rekommenderar Digitaliseringsrådet att antalet utbildningsinsatser och examinerade inom informations- och kommunikationsteknik utökas.[321] Det bedöms även råda en allt större brist på specialistkompetens för att bedöma och hantera risker. IVA konstaterar att antalet specialister på detta område är få och minskar jämfört med behovet.[322]

- *Beställarkompetens:* En tredje typ av kompetensbrist som många lyfter fram handlar om det offentligas upphandlingar av olika typer av it-system. Utan tydliga krav på säkerhetsnivåer eller krav på efterföljande kontroller riskerar redan själva upphandlingsprocessen att lägga en alltför låg ribba på säkerhetsarbetet.[323] Som framkommit i våra intervjuer är det viktigt att högre ledningsnivåer förstår att en godtagbar säkerhetsnivå måste upprätthållas genom hela kedjan av leverantörer och underleverantörer.[324] Även IVA noterar i detta sammanhang att en samlad hög beställarkompetens är avgörande för förmågan att vid upphandlingar göra konsekvensanalyser för den egna verksamheten: ”Man måste förstå vilka drifts- och säkerhetsnivåer som verkligen ligger bakom leverantörens löfte om lösningar som en ’fungerande infrastruktur’ eller ’bra molntjänst’”.[325]

Digitaliseringsrådet menar även att det är alarmerande att så få kvinnor jobbar inom it-området eftersom bristen på arbetskraft inte skulle vara lika stor ”om även kvinnor betraktade det som intressant att jobba som it-specialist.”[326] Formuleringen är ett exempel på det som noterades i kapitel 2, att skulden generellt brukar läggas på de frånvarande i it-sammanhang istället för att undersöka orsakerna till frånvaron (se kapitel 2.4.2.).

[319] IVA, 2019, s. 31.
[320] Vinnova, 2018, IVA, 2019, s. 32.
[321] Digitaliseringsrådet, 2018b, s. 32.
[322] IVA, 2019, s. 28.
[323] Tidigare avdelades exempelvis resurser för att åka ut och ”provskjuta” brandväggar, som en av våra intervjupersoner beskriver det, men denna typ av kontroll förekommer sällan idag. Internetstiftelsen, intervju, 2019-09-02.
[324] Netnod, intervju, 2019-09-23; Internetstiftelsen, intervju, 2019-09-02.
[325] IVA, 2019.
[326] Digitaliseringsrådet, 2018b, s. 87.

5.3 Infrastrukturen

Enligt IVA:s rapport *Digitalisering för ökad konkurrenskraft* (2019) finns idag ett gap mellan infrastrukturens kapacitet och de digitala tjänsternas faktiska behov av kapacitet. Hos viktiga beslutsfattare såväl som i samhället i stort saknas dock kunskap om att detta gap existerar.[327] Detta är allvarligt menar IVA, som gör liknelsen med fungerande vatten- och avloppssystem: Skillnaden är att för VA-system finns en omfattande kontroll av kvalitet och driftsäkerhet men någon motsvarande samlad planering finns inte för den digitala infrastrukturen.[328] Det innebär, som IVA konstaterar, en mycket stor riskaggregering när vi antar att många funktioner helt enkelt ”bara ska fungera”.[329] En bakgrund till dessa förhållanden tycks bland annat handla om bristande samordning av infrastruktur-utbyggnaden. Pilotprojektet Särimner, som syftade till att undersöka möjligheterna att bygga en robust internetinfrastruktur, konstaterade i sin slutrapport att:

> Dagens svenska IT-infrastruktur har framförallt byggts ut där det funnits affärsmässiga skäl som talat för detta, och bristande koordinering har medfört att det finns för få mötesplatser för fiber, vilket i sin tur leder till bristande redundans. Några få operatörer har etablerat redundanta vägar, men långt ifrån i den utsträckning samhället behöver.[330]

Problemet med otillräcklig infrastruktur tas även upp i rapporten *Förbjuden framtid?* som tagits fram av Institutet för framtidsstudier.[331] Rapporten poängterar att olika typer av data, som t.ex. text, ljud, bild, video och sensordata, kräver väldigt olika kapacitet i hårdvara liksom att teknisk infrastruktur (nätverk, routrar och fiber) för hanteringen av alla dessa datatyper är otillräcklig. Kommunerna har hittills nästan enbart hanterat text, vilket inte kräver särskilt stora resurser. Inte heller ljudfiler eller bilder tar idag särskilt stor plats. Men datamängderna växer. Att zooma in en bild på ett hudprov för att kunna se förändringar i cellkärnor kräver ”ohyggliga datamängder”, och sjukhus som går över till digitaliserad patologi måste därför bygga ut servrar och nätverk.[332] Strömmande video från kameror som övervakar sopförbränningsanläggningar, sovande vårdtagare på äldreboenden och den allmänna ordningen på torget, är andra exempel på tekniska lösningar som kräver nätkapacitet och lagringsutrymme.

Infrastrukturperspektivet lyfts också i de intervjuer vi har genomfört.[333] Vid sidan av säkerhetsfrågorna, som ofta är svåra att motivera ekonomiskt, tycks det som att även erforderliga investeringar i den helt nödvändiga infrastrukturen har kommit

[327] IVA, 2019, s. 7.
[328] Ibid, s. 23
[329] Ibid.
[330] Vetenskapsrådet, 2018, s. 2.
[331] Ekholm, Jebari & Markovic, 2018.
[332] Ibid., s. 19.
[333] Internetstiftelsen, intervju, 2019-09-02; Netnod, intervju, 2019-09-23; MSB, intervju, 2019-09-27.

på skam. Det ansvar, mandat och perspektiv som krävs för att bygga grunden tycks i många fall ha saknats, och avsaknaden på infrastruktur tycks i många fall vara en fullt utvecklad flaskhals. Ett exempel kan hämtas från hälso- och sjukvården där digitalisering ofta framförs som en lösning på i synnerhet glesbygdens utmaningar med stora avstånd och brist på personal. Mot denna bakgrund installerades ny digital teknik på Hälsocentralen i Funäsdalen som skulle möjliggöra läkarundersökningar på distans. Men som Östersunds-Posten kunde rapportera i september 2019 kunde inte den nya tekniken användas eftersom brist på fiberuppkoppling gjorde att överföringen mellan parterna inte fungerade. Sedan dess har tekniken inte haft någon annan funktion än att den har stått och tagit plats.[334]

Figur 5.1. IBM-maskinerna anländer till Skogsbrukets datacentrals nybyggda lokaler på Södra Allén, Sundsvall. Årtal:1963. Fotograf: Norrlandsbild/Ragge Ellefsson. Ingår i samling: Sundsvalls museum.

[334] ”Tekniska problem för vård på distans”, *Östersunds-Posten*, 30 sept. 2019.

5.4 Styrningen och samordningen

Flera rapporter och utredningar har identifierat behovet i Sverige av att stärka samordningen och styrningen i digitaliseringssammanhang, särskilt när det gäller utbyggnad av infrastruktur och samordning av informationssäkerhetsarbetet.[335] Mot bakgrund av mängden offentliga aktörer är uppgiften icke-trivial. Som Digitaliseringsrådet konstaterar:

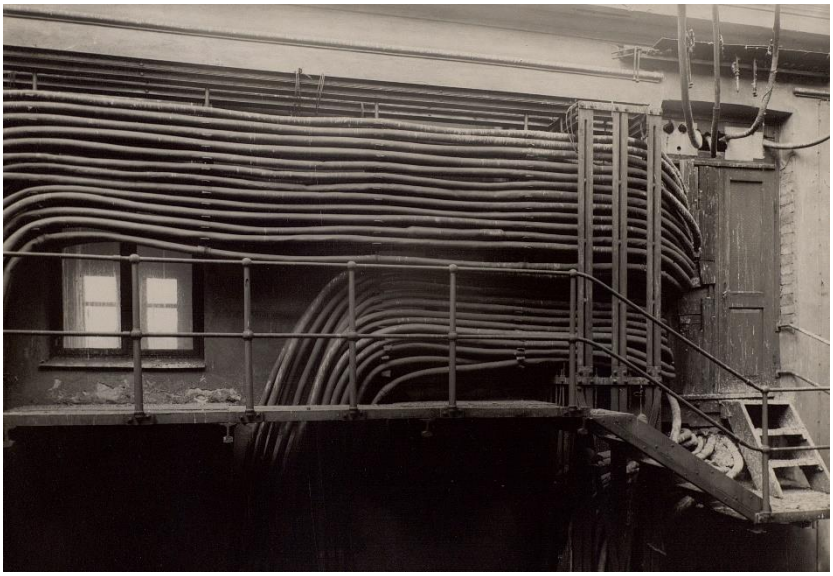
> Sverige består av 290 kommuner, 21 länsstyrelser, 20 landsting/regioner, fler än 200 statliga förvaltningsmyndigheter, 37 lärosäten, 80 domstolar samt 40 helägda statliga bolag. Det är en omfattande förvaltning som kompliceras av stora skillnader mellan verksamheterna vad gäller storlek, geografi, uppdrag, finansiella resurser och kompetens. Alla ska dock med i den digitala transformationen.[336]

Dessutom tillkommer alla de privata företag som på något sätt driver och förvaltar samhällets infrastruktur. Som IVA påpekar har Sverige en avreglerad marknad med olika skikt av infrastrukturproducenter, operatörer och tjänsteutvecklare, som å ena sidan har många fördelar men som å andra sidan lider av bristande helhetssyn och samordning:

> Sverige är mycket nära en situation där alla vitala samhällsfunktioner kräver en välfungerande digital infrastruktur. Denna förutsätts fungera minst lika säkert som vattenledningar och elnät. Men för dessa typer av infrastruktur finns regler och planer för drift och utbyggnad. Motsvarande systematik finns inte för de digitala. Ansvaret ligger istället på många händer. Samordningen brister på både statlig och kommunal nivå. [337]

Grundläggande infrastruktur för digital kommunikation i Sverige är enligt IVA ett av de viktigaste områdena att styra och samordna (se även föregående avsnitt). Den svenska digitala infrastrukturen är, menar IVA, uppbyggd enligt en lasagnemodell (se kapitel 3) med olika lager av verksamheter, men styrning och samordning är inte fullt ut anpassade till detta. Modellen förutsätter att statliga myndigheter och kommuner både investerar och utövar tillsyn, samtidigt som privata aktörer är ansvariga för vitala delar av infrastrukturen. Syftet med samordning och styrning är att se till att både befintliga och nya delar av infrastrukturen har tillräcklig robusthet och kapacitet. Styrningen och samordningen av digitaliseringsfrågorna inom regeringskansliet är, menar IVA, dock svag och otillräcklig.[338]

[335] IVA, 2019, s. 49-50; Vetenskapsrådet, 2018; ESV 2018:31.
[336] Digitaliseringsrådet, 2018b, s. 48.
[337] Tuula Teeri, Jan Nygren, Karl Bergman, Patrik Fältström & Pia Sandvik, ”Akut brist på kunskap hotar viktig digitalisering”, *Ny Teknik*, debattartikel, 3 maj 2018. Hämtad 2019-12-03 från https://www.nyteknik.se/opinion/akut-brist-pa-kunskap-hotar-viktig-digitalisering-6912528.
[338] IVA, 2019, s. 49-50.



Figur 5.2. Skeppsbron 2. Kabelintag till överkopplingen. Telefonstationen Skeppsbron 2 "Centralen" var i drift till år 1929, då den automatiserades och flyttades till Jakobsbergsgatan 24. Fotograf: okänd. Ingår i samling: Tekniska museets arkiv.

Sett ur ett informationssäkerhetsperspektiv noterade utredningen *Reboot – omstart för den digitala förvaltningen* 2017 risken för att de informationssäkerhetskrav som utfärdas i praktiken fördröjs eller aldrig blir utförda på grund av oklara ansvarsförhållanden.[339] Utredningen påpekade att det finns en risk för ökad fragmentering av kravställningar när fler aktörer utan samordning utfärdar regler på området, något som kan leda till att ”samma typ av information riskerar att få helt olika skydd beroende på var i förvaltningssystemet som den hanteras.”[340]

Bristen på styrning och samordning har också identifieras som ett problem i ett datadelningsperspektiv. Ekonomistyrningsverket (ESV) har understrukit vikten av att fler förvaltningsgemensamma tjänster och strukturer skapas men att (bland annat) bristande tillgång till gemensamma grunddata utgör ett hinder för detta.[341] ESV konstaterar att runt hälften av de offentliga aktörerna fortfarande hämtar uppgifter direkt från privatpersoner eller företag trots att uppgifterna redan finns hos en annan offentlig aktör. Som jämförelse noteras att i Estland får endast en offentlig aktör lagra grunddata – medan andra aktörer hämtar information från

[339] SOU 2017:114, s. 164.
[340] Ibid.
[341] ESV 2018:31, 53. Myndigheten för digital förvaltning har ett regeringsuppdrag att undersöka hur den offentliga förvaltningens förmåga att tillgängliggöra öppna data kan ökas, se https://www.digg.se/utveckling--innovation/oppna-data-och-datadriven-innovation/regeringsuppdrag-oppna-data-datadriven-innovation-och-ai.

denna när de behöver tillgång till data i sin verksamhet. En sådan lösning begränsar kravet på den enskilde att lämna in samma uppgifter till olika offentliga aktörer. ESV drar slutsatsen att arbete behöver göras i Sverige för att skapa ökad interoperabilitet och en modern lagstiftning som tillåter en effektivare informationsförsörjning.[342]

Styrnings- och samordningsaspekter tas också upp i våra intervjuer. Det betonas att det är viktigt att ledningsnivåerna förstår vad digitalisering innebär och inte minst vad som krävs för att tillgodose säkerheten. Att säkerställa kvalitet i upphandlingar liksom att genomföra strukturomvandlingar är ytterst ledningens ansvar och inte en enskild it-avdelnings.[343]

5.5 Exponeringen

En sårbarhet som brukar lyftas när det gäller Internet of Things handlar om exponeringen, dvs. att tekniken blottas för angrepp och intrång. Många nya tekniker bär på olika typer av barnsjukdomar som i sig innebär sårbarheter. Därför är det viktigt att ny teknik testas i skyddade miljöer och introduceras med försiktighet och i lagom takt. För att åstadkomma en kontrollerad och strukturerad utbyggnad av ett nytt system, eller en ny teknik, krävs någon form av genomtänkt agenda. Tekniska standarder kan fylla denna funktion och tillämpas ofta just med det syftet. Ett dilemma är att det kan finnas olika incitament att bygga ut eller exploatera teknik, och att alla incitament inte innebär att tekniken blir säker när den väl är på plats. Om teknik byggs ut i stor skala, med många latenta fel eller sårbarheter kan samhället nå en punkt där det är svårt att backa. Utvecklingen av IoT bedöms dessutom bli explosionsartad vilket betyder att denna punkt kan nås överraskande fort.

Om tekniken, och därmed dess sårbarheter, sprids okontrollerat kan problem uppstå. I bästa fall åtgärdas sårbarheterna längs vägen, men om utvecklingen är snabb kan detta vara svårt (särskilt om sårbarheterna är okända). Ett sådant exempel skulle kunna vara slarvigt genomförda satsningar på ”smarta städer” som inte har tagit hänsyn till riskerna med att koppla upp och ihop många olika typer

[342] ESV 2018, 7, 54. I Ekholm, Jebari & Markovic, 2018 sägs titeln på rapporten (”Förbjuden framtid?”) komma sig av ”det faktum att vi idag inte får använda data för att hantera sammansatta komplexa samhällsproblem med metoder som involverar informationsöverföring över sekretessgränser.” (s. 8). Se även ”Hinder för att använda myndigheternas öppna data”, Statskontoret, 2018:6. Hämtat 2019-12-03 från http://www.statskontoret.se/publicerat/publikationer/2018/hinder-for-att-anvanda-myndigheternas-oppna-data/.

[343] Netnod, intervju, 2019-09-23.

av sensorer och funktioner.[344] Denna typ av digitala tjänster möjliggör potentiellt effektiviseringar men också att många funktioner kan slås ut samtidigt.

Hur skulle då sårbarheter kunna uppstå mer konkret genom ökad exponering? Vi ser här åtminstone två potentiella problem. För det första finns det exempel på att produkter förses med uppkopplingsmöjligheter utan någon specifik anledning, utan helt enkelt för att det går. Detta ger utrymme för tekniken att användas som om den inte vore uppkopplingsbar, t.ex. i en säkerhetskritisk tillämpning eller miljö, men sedan kanske ändå kopplas upp. Än mer problematiskt blir det om uppkopplingsmöjligheten är okänd. Kanske har den införts långt bak i leverantörskedjan med små möjligheter till spårbarhet? I detta fall är risken att de tekniska installationerna, särskilt om de är mångfaldigade, blir en (i värsta fall dold) hävstång för angrepp mot t.ex. kritisk infrastruktur.

För det andra finns en risk att digital teknik kopplas till sårbar infrastruktur på ett problematiskt sätt. Ett exempel kan hämtas från energisektorn och den begynnande utvecklingen av framtidens ”smarta elnät” vars höga prestanda bland annat kräver synkroniserad, exakt tid.[345] GPS-satelliter kan ge sådan stabil tid eftersom de har atomur ombord, men GPS-signaler är också lätta att störa ut. Än så länge är kraven i elnäten relativt sett låga, men i framtiden kan detta komma att ändras. Om GPS då kommer att användas som enda tidskälla har en ny sårbarhet introducerats i en samhällskritisk funktion. Risken är, omvänt mot föregående exempel, att infrastrukturen blir en hävstång för attacker mot tekniska installationer.

I bägge fallen riskerar inlåsningen att underblåsas av mer eller mindre teknik-offensiva kampanjer, där målet är viktigare än vägen dit, t.ex. att föreställningen om Stockholm som världens smartaste stad inte åtföljs av en idé om hur den blir säker i motsvarande grad. Om en teknik ska byggas ut för att tillgodose framtidens krav så måste infrastrukturen, och den redundans som krävs, stärkas i motsvarande takt och omfattning. För detta krävs någon form av medveten agenda eller policy, till exempel med stöd i någon teknisk standard. Alternativet är organisk utbyggnad vilket inte ger några säkerhetsgarantier.[346]

[344] När SVT under våren 2019 undersökte 22 svenska digitaliseringsprojekt kopplat till idén om den smarta staden framkom att inget av projekten hade en egen säkerhetsbudget. Även om allt säkerhetsarbete inte speglas i budget betonar kritiker att hoten och riskerna är så pass omfattande att de inte kan analyseras planlöst eller som en eftertanke. Emil Hellerud, ”Städerna blir smartare – experter varnar för säkerhetsbrister”, *SVT Nyheter*, 1 april 2019. Hämtat 2019-12-03 från https://www.svt.se/nyheter/lokalt/stockholm/stockholm-vill-bli-smart-stad-men-saknar-budget-for-it-sakerheten.

[345] Se Swaling, 2015.

[346] Ett annat exempel är hur säkerhetskritiska eller potentiellt säkerhetskritiska funktioner har börjat kopplas upp mot olicensierade band, som inte kräver någon speciell tillåtelse men inte heller någon garanti för att kommunikationen kommer att fungera. Detta kan tolkas som att bristen på infrastruktur har ett samband otillbörlig exponering. Swaling, Wiklundh & Fors, 2017, s. 10.

5.6 Asymmetrierna

På den digitala arenan finns många typer av asymmetrier, såsom skeva maktförhållanden eller glapp mellan förväntningar och verklighet. En sådan allvarlig obalans är det ökande beroendet av allt färre tjänsteproducenter.[347] Två exempel utgörs av Swish och Bankid som på relativt kort tid nått en mycket hög användningsgrad i Sverige. Om dessa skulle sluta att fungera skulle konsekvenserna bli omedelbara och omfattande – ett viktigt betalningsmedel skulle förloras om Swish inte är tillgängligt och det skulle vara svårt att sköta bankaffärer och myndighetskontakter om Bankid inte fungerar.[348] Andra exempel är produkter och tjänster med många användare, såsom operativsystem, molntjänster och sökverktyg. När många är beroende av funktion och säkerhet i en enda produkt eller tjänst kan en sårbarhet där orsaka stora konsekvenser om den nyttjas med ont uppsåt (eller på annat sätt utsätts för oväntade händelser).

Digitalisering driver ofta fram nya asymmetrier, t.ex. genom att distribuerade icke-digitala system ersätts med centraliserade digitala system, vilket innebär att det lätt uppstår felkritiska systemdelar.[349] Ett sådant exempel är fallet med larmnumret 911 i USA, där ett enkelt programmeringsfel ledde till att numret inte gick att nå i sju delstater under sex timmar i april 2014. Felet gjorde att 6000 samtal till larmnumret inte kom fram.[350] Denna typ av felkritiska systemdelar och de följdeffekter som de kan ge när något går fel måste alltid tas i beaktande när en kritisk verksamhet digitaliseras. Det kan vara mycket svårt för verksamheten att förstå hur systemen är uppbyggda och vilka beroenden som finns, speciellt om de upphandlas från en extern part. En förstärkande faktor kan vara att en enskild leverantör står för funktioner hos många verksamheter, till exempel inom många olika kommuner.

[347] MSB, intervju 2019-09-27; Internetstiftelsen, intervju, 2019-09-02.

[348] IVA, 2019, s. 28

[349] En felkritisk systemdel (eng. *single point of failure*) är en svag länk i systemet som måste fungera för att systemet som helhet eller kritiska funktioner i systemet ska fungera. Om ett system är beroende av en enda punkt för sin funktion kan konsekvenserna bli stora om denna slås ut. I många fall är dock inte diversifiering möjlig när det gäller val av systemkomponenter. Detta är extra tydligt för operativsystem, såsom Microsoft Windows eller Apple MacOS, då många applikationsprogram endast finns tillgängliga för ett operativsystem. Angripare som nyttjar kritiska säkerhetsbrister i systemen kan orsaka stora skador på kort tid. Bristen på diversifiering är ett globalt problem som påverkar svenska verksamheter i stor utsträckning.

[350] Bishr Tabbaa, "Busy Signal: Behind CenturyLink's 911 Service Outage of 2014", *The Startup, Medium*, 22 april 2019. Hämtat 2019-11-03 från https://medium.com/swlh/the-counter-overflowth-behind-centurylinks-911-service-outage-of-2014-58eb30ca6252.

Figur 5.3. Datasal. Fotograf: okänd/ Järnvägsmuseet. Fotografering 1975 - 1985 (1985). Ingår i samling: Järnvägsmuseets foton.

En övergripande typ av asymmetri är den mellan de stora teknikbolagen och i princip alla andra, inklusive enskilda stater. Idag är det ett fåtal stora teknikbolag som tillsammans har stor makt över det som sker på internet. De så kallade *big five* eller *GAFAM* – det vill säga *Google*, *Amazon*, *Facebook*, *Apple* och *Microsoft* – står för en signifikant del av den informationshantering, näthandel och teknik som används idag. I Kina finns det ytterligare tre företag – *Baidu*, *Alibaba* och *Tencent* – som har liknande dominans inom sina branscher i den delen av världen. Så som marknaden fungerar är denna oligopolsituation ett faktum som såväl politiker som verksamheter måste förhålla sig till och hantera.

Med de stora informationsbolagen följer en asymmetri även mellan individen och företagen.[351] Individen blir i många avseenden beroende av företagen för att kunna få tillgång till information, men som användare har de liten möjlighet att påverka vilken information som företagen samlar in från dem. Slutligen kan asymmetrier även uppstå mellan individen och staten. Den så kallade *digitala klyftan*, det vill säga skillnaden mellan de som förstår och kan använda digitala system och de som inte har den förmågan, har tidigare bestått mestadels i tillgång till datorer och internetuppkoppling samt hur dessa ska användas. På senare tid har dock forskningen visat att digitalisering av offentliga tjänster riskerar att lägga till ytterligare lager på denna klyfta. En viktig funktion som handläggarna har haft i samband med personliga möten eller telefonkontakt är att hjälpa medborgarna med

[351] Lupton, 2016, s. 4.

information för att navigera den offentliga förvaltningen, exempelvis när det gäller vilka rättigheter de har och vem de ska kontakta. En effekt av digitaliseringen är att medborgaren till viss del blir sin egen handläggare då de måste veta vilka myndigheter de ska kontakta och hur de ska hitta de digitala tjänsterna för att göra detta.[352]

5.7 Tilliten

I februari år 2019 uppdagades att 2,7 miljoner inspelade samtal till Vårdguiden (1177) under flera år hade legat helt öppet på en oskyddad webbserver.[353] Den så kallade 1177-skandalen är ett av många exempel på uppmärksammade incidenter i digitala sammanhang med berättelser om system som har slutat fungera, om system som inte fungerar som de ska, eller om känslig data som läckt. Frågan är hur denna typ av skandaler i längden påverkar allmänhetens förtroende för digital teknik. I ett scenario med ett större sammanbrott i samhällets funktionalitet, exempelvis inom sjukvården eller elförsörjningen, skulle det kunna bli svårt att återupprätta detta förtroende. En konsekvens på sikt skulle kunna bli en backlash för Sveriges ambitioner vad gäller digital utveckling.[354]

Tillit kan också avse medborgarnas förtroende för välfärdssystemen i ett bredare perspektiv. I den kartläggning som *Delegationen för korrekta utbetalningar från välfärdssystemen* har genomfört framkommer att de felaktiga utbetalningarna totalt uppskattas till cirka 5,5 procent av de totala utgifterna (exklusive ålderspensionssystemet), vilket motsvarar 18 miljarder kronor årligen.[355] Delegationens kartläggning visar också att potentialen är stor för att minska felaktiga utbetalningar med hjälp av digitalisering och AI. Samtidigt beskrivs hur myndigheterna inte tar tillvara denna potential: ”Mycket talar för att dagens satsningar på digitalisering och AI istället riskerar att leda till större felaktiga utbetalningar från välfärdssystemen.” [356] Delegationen konstaterar vidare att perspektivet korrekta utbetalningar inte lyfts inom regeringens styrning inom digitaliseringsområdet

[352] Lindgren, Madsen, Hofmann & Melin, 2019.
[353] “2,7 miljoner inspelade samtal till 1177 Vårdguiden helt oskyddade på internet”, *Computer Sweden*, 18 februari 2019. Hämtad 2019-12-03 från https://computersweden.idg.se/2.2683/1.714787/inspelade-samtal-1177-vardguiden-oskyddade-internet. Händelsen fick stor uppmärksamhet då stränga krav gäller för uppgifter som rör individers hälsa. Sedan avslöjandet har Datainspektionen inlett tre separata granskningar av 1177 Vårdguiden. ”Datainspektionen inleder tre nya granskningar kring 1177 Vårdguiden”, Datainspektionen, 28 juni 2019. Hämtad 2019-12-03 från https://www.datainspektionen.se/nyheter/datainspektionen-inleder-tre-nya-granskningar-kring-1177-vardguiden/.
[354] Internetstiftelsen, intervju, 2019-09-02.
[355] SOU 2019:59, s. 19.
[356] Ibid., s. 22-23.

samt att korrekta utbetalningar är ”lågt prioriterat i myndigheternas digitaliserings-arbete i förhållande till service och effektivisering av de egna processerna”.[357]

Det går inte att utesluta att denna typ av prioriteringar på sikt kan komma att påverka medborgarnas inställning till digitalisering. Sveriges kommuner och regioner (SKR) genomför sedan några år tillbaka en årlig undersökning över invånarnas inställning till digital service inom välfärden. I undersökningen från 2018 ingick för första gången en frisvarsfråga om vad respondenterna anser som viktigt när samhällsservicen blir allt mer digital. De två områden som förekom mest frekvent bland svaren var *säkerhet och integritet* samt *att personlig kontakt inte glöms bort*.[358]

5.8 Förväntningarna

Ett av de problem som återkommer i såväl litteratur som intervjuer är skillnaden mellan förväntningar och verklighet. Här finns en koppling till kompetens-problemet: När beställarkompetensen brister finns en överhängande risk att verksamheten inte förstår vilken servicenivå som beställts och vad den innebär. När digitala system ersätter manuella rutiner, exempelvis när äldrevården inför digitala system för att upptäcka om någon vårdtagare ramlat, så krävs teknik och infrastruktur som matchar ambitionerna. Om ambitionerna överstiger tillgänglig teknik och infrastruktur riskerar digitaliseringsprojekten att fallera. Det kan innebära att systemet aldrig kan driftsättas men det kan även innebära att systemet blir ineffektivt, opålitligt, dyrt eller arbetskrävande; effekter som dessutom riskerar att leda till svikna förväntningar.

Förväntningar kan också handla om missförstånd gällande vad digital teknik kan åstadkomma. Som Agneta Gulz, professor i kognitionsvetenskap, har observerat är det inte ovanligt med felställda förväntningar när det gäller digitaliseringen av skolan.[359] Gulz tar i detta sammanhang upp motiv som handlar om att digitalisering skulle spara pengar eller öka likvärdigheten:

> Inte minst är det naivt att tro att digitaliseringen ökar likvärdigheten. Det som styr är fortfarande elevernas bakgrund och om de har föräldrar som stöttar och följer upp skolarbetet. I Sverige finns tyvärr en kanske alltför stark tilltro till tekniken, som kommer ur vår tradition och historia med många starka uppfinningar.[360]

Den forskargrupp som Gulz tillhör, *Educational Technology Group*, är tvärveten-skaplig och består av flera svenska lärosäten och även en forskargrupp vid

[357] Ibid.
[358] Malin Annergård, ”Invånarnas inställning till digital service i välfärden”, Sveriges Kommuner och Regioner, 27 november 2019. Hämtad 2019-12-03 från https://skr.se/naringslivarbetedigitalisering/digitalisering/sammanhallendigitalservice/invanarnasinstallningdigitalservice.16155.html.
[359] ”Teknik ger inte billigare skola”, *Pedagogiska magasinet*, nr 4, 20 november 2019.
[360] Ibid.

Stanford.[361] Forskarna är inte kritiska till den digitala tekniken i sig – tvärtom ser man intressanta möjligheter med digitala läromedel som bygger in pedagogernas kunnande och känner av vad den enskilda eleven behöver. Dit är det dock långt kvar, menar Gulz.[362]

Glappet mellan förväntningar och realitet kan även vara en faktor i ett mer grundläggande infrastrukturperspektiv. Drivkrafterna för aktörerna på den öppna marknaden – som i många avseenden styr hur it-systemen och infrastrukturen ser ut – är ofta effektivitet och låga kostnader, snarare än säkerhet på samhällsnivå och genomtänkt systemfunktion för offentlig verksamhet. Dessa faktorer leder till en signifikant risk att alldeles för lite tankekraft läggs på tillförlitlighet på den högre systemnivån, där även systemets kontext i en bred mening tas med inkluderande kommunikationer, elförsörjning, kompetens, användare och samhällseffekter. Samtidigt förväntar sig sannolikt systemens användare, dvs. medborgarna, att de grundläggande samhällsfunktionerna helt enkelt ska fungera. Om brister finns i samordningen av den digitala infrastrukturen finns alltså en risk att medborgarnas förväntningar på densamma inte kommer att mötas.

5.9 Plan B?

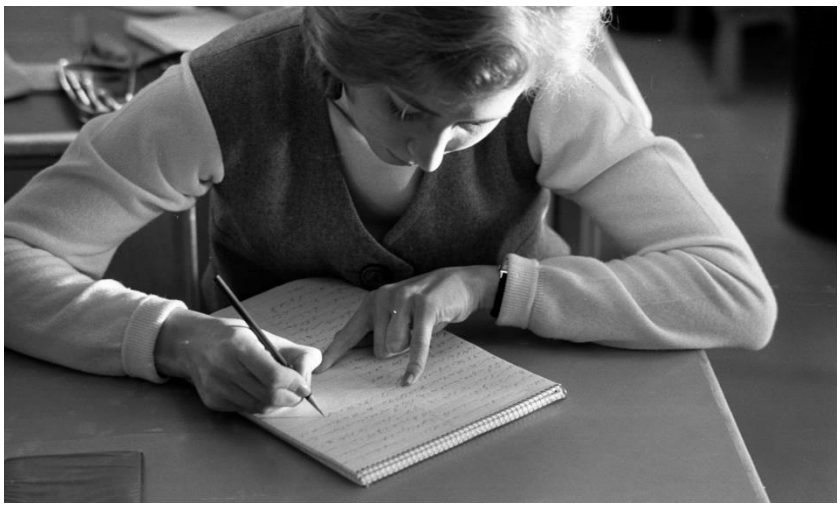
För den som vill vara i framkant kan det också behövas perspektiv på vad det innebär att stå allra längst ut på kanten. Vad händer om något går riktigt fel – om systemen av någon anledning slutar fungera? Vilka backup-system finns, vilka reservplaner kan sättas igång, vilka alternativ finns att tillgå?

Väldigt få it-system byggs idag för riktigt hög driftsäkerhet och tillgänglighet då detta är kraftigt kostnadsdrivande. Det här gäller speciellt när it-systemen är distribuerade över flera platser och därmed kräver en kommunikationsinfrastruktur. De generella kraven på tillgänglighet i bredbandsnät och mobilnät är generellt sett låg, där exempelvis Post- och telestyrelsens föreskrifter tillåter driftavbrott på 12–18 timmar för utrustning med färre än 2000 aktiva anslutningar.[363] I en undersökning som Bredbandsforum har genomfört angående digitala trygghetslarm poängterade operatörerna att kravställningen på tillgänglighet och redundans ibland har varit orimligt hög vid upphandlingar.[364] Vissa operatörer avrådde från att ansluta trygghetslarm och liknande tjänster via deras nät då de inte

[361] Om Educational Technology Group, se https://www.lucs.lu.se/etg/.
[362] Gulz framför också förslag på hur inköp och val av digitala läromedel skulle kunna styras mot en högre kvalitet, och föreslår en checklista bestående av ett antal frågor att ställa inför ett nytt digitalt läromedel, där fråga nummer ett handlar om huruvida produkten är systematiskt utvärderad av personer som inte har kommersiella intressen av den. För checklistan, se https://pedagogiskamagasinet.se/vagen-mot-en-digital-skola/.
[363] PTSFS 2015:2.
[364] Bredbandsforum, 2019.

kan garantera tillgängligheten.[365] Det här visar vikten av att rätt kunskap finns i beställar- och användarled angående vad tekniken och leverantörerna kan utlova, exempelvis i form av servicenivåavtal.

Att samhället i stort blir mer och mer beroende av datorer noterades med oro redan på 1970-talet, bland annat i totalförsvarssammanhang och sedermera i utredningar om ADB och samhällets sårbarhet.[366] På 1980-talet diskuterades om myndigheterna behövde ha en ”utlistningsberedskap”, dvs att de i händelse av krigshot skulle skriva ut viktiga dokument och register på papper för säkerhets skull.[367] Just papper har setts som en grundläggande plan B i beredskaps-sammanhang, i form av viktiga pärmar, blanketter, kuponger, informations-broschyrer osv. I MSB:s beredskapsbroschyr, *Om krisen eller kriget kommer* (2018) rekommenderas Sveriges invånare att ha kontanter hemma, en papperslista med viktiga telefonnummer liksom utskrifter på papper av exempelvis försäkringsbrev och bankuppgifter.



Figur 5.4. Stenografi 14 januari 1967. Fotograf: Örebrokuriren/Örebro läns museum. Ingår i samling: Örebro kuriren, Örebro läns museum.

Kontanter har länge setts som det viktigaste reservsystemet om de digitala betalmedlen inte längre skulle fungera. Nu pågår arbete med att utreda en digital krona, en e-krona, som eventuellt ska kunna fungera off-line.[368] Men en viktig princip i riskhantering är att plan B ska vara olik plan A, så kallad diversifiering.

[365] Ibid.
[366] SOU 1979: 93; SOU 1986: 12.
[367] Barck-Holst, 2005, s. 33.
[368] Sveriges Riksbank, 2018.

Om alltså vår tidigare plan B, dvs. kontanterna, nu ska bli digitala, kan man fråga sig om det även behövs en plan C, om betalningssystemen trots allt fallerar. Svenska folket är i en klass för sig när det gäller att rata kontanter som betalmedel.[369] Men är Sverige verkligen moget för en e-krona?

En skillnad idag jämfört med it-erans barndomsår på 1980- och 90-talen är att mycket skapas digitalt från första början. Ofta finns ingen analog back-up (inget papper). Beroendet blir därmed totalt till det nya systemet. Idag är också frågan om vem som har kunskap om systemet, eller processerna. Är det handläggarna (som inte längre utför de automatiserade processerna), utvecklarna som har implementerat processerna (men som knappast jobbar på myndigheten), någon annan eller ingen alls? Vad händer när automationen går sönder och man behöver arbeta manuellt under en period? Ett närliggande perspektiv handlar om hur medborgarna ska hantera sina ärenden, som t.ex. att hämta ut medicin, få sin pension eller få kontakt med myndigheter.

Även om mycket av den digitala infrastrukturen och tjänsterna drivs av privata aktörer kan det digitala samhällets plan B inte axlas av enskilda privata aktörer; här krävs ett samlat grepp och ett statligt helhetsansvar.

[369] Sveriges Riksbank, 2019.

6 Strategier för att minska risker och sårbarheter

> Datoriseringen ger möjlighet till nya och effektiva metoder att med små medel skapa förvirring och kaos i samhället.[370]

Om problemen med digital teknik tycks oräkneliga så finns som tur är lika många analyser som försöker lösa dem. I detta kapitel finns egentligen bara utrymme att skumma på ytan av de många förslag, strategier och idéer som fokuserar på olika sätt att minska riskerna och sårbarheterna med digital teknik. Till att börja med ger vi exempel på förslag i den svenska kontexten med koppling till de nio problem som beskrevs i föregående kapitel. Därefter ges ett antal strategiexempel för IoT-säkerhet (som relaterar till vårt ovan beskrivna område *cyber/fysiskt*), AI-säkerhet (som relaterar till området *människa/maskin*) samt dataskydd (som relaterar till området *data/individ*).

6.1 Nio problem, många lösningar?

För en enskild aktör kan det vara svårt att skaffa sig en överblick över mängden potentiella sårbarheter, hotbilder och kritiska beroenden. Därför blir det än viktigare att det finns tydliga strukturer för säkerhetsarbetet och visioner som förmedlar att det viktigaste kanske inte alltid är att vara ”bäst i världen”[371], som dagens svenska strategier på digitaliseringsområdet deklarerar, utan att skapa ändamålsenliga lösningar som både är användarvänliga och säkra. En sådan attitydförändring skulle möjligen kunna mildra problemet med den ryckighet i svenska digitaliseringssatsningar som beskrevs i avsnitt 5.1, där ett vanligt problem tycks vara en underskattning av den tid som kvalitets- och säkerhets-analyser kräver.

Som forskning inom fältet STS (Science and Technology Studies) har belyst är teknik och samhälle i ständig förändring och formar varandra.[372] Detta innebär också att de problem som uppstår i digitaliseringens kölvatten aldrig kan bli helt färdiglösta. Arbetet för att stärka säkerheten måste istället vara en ständigt pågående process. Kvaliteten i denna process kan höjas om de rätta kunskaps- och kompetensmässiga förutsättningarna finns. Som beskrevs i avsnitt 5.2. diskuteras flera typer av kompetensbrister i Sverige. Rekommendationerna som framkommit handlar både om att stödja humanistisk och samhällsvetenskaplig forskning och om att öka antalet utbildningsinsatser och examinerade inom informations- och

[370] Sekretariatet för säkerhetspolitik och långsiktsplanering inom totalförsvaret (1976), *Svensk samhällsutveckling: Datorerna*, Försvarsdepartementet.
[371] Regeringskansliet, 2017a.
[372] Jasanoff, 2016; Felt, Fouché, Miller & Smith-Doerr, 2017.

kommunikationsteknik.[373] Att även tilldela resurser för att höja beställarkompetensen inom offentlig sektor har framförts som viktigt.[374]

En trend internationellt är satsningar på tvärvetenskapliga centrumbildningar och nätverk: Ett framgångsrikt sådant exempel är universitetet i Montreal i Kanada som har etablerat ett världsledande AI-centrum som för samman forskare från olika fält i syfte att integrera sociala konsekvenser av tekniken i projekten.[375] Flera nya initiativ finns också i Storbritannien som syftar till att föra samman forskare från olika discipliner.[376] Det finns även exempel på särskilda forskningssatsningar i Sverige, såsom det fleråriga forskningsprogrammet *Wallenberg AI, Autonomous Systems and Software Program* (WASP) där ett spår fokuserar på humanistisk och samhällsvetenskaplig forskning.[377]

När det gäller bristerna inom digital infrastruktur, som beskrevs i avsnitt 5.3, har IVA rekommenderat en effektivare politisk samordning och att statens verktygslåda används på ett mer offensivt sätt (till exempel genom användning av regleringsbrev, ägardirektiv, föreskrifter, regler och lagar).[378] Just styrnings- och samordningsperspektivet, som beskrevs i avsnitt 5.4. återkommer i många strategiförslag. I Digitaliseringsrådets rapport *En lägesbild av digital ledning* efterlyses framför allt en större tydlighet vad gäller genomförandet av regeringens digitala strategi:

> Det är också nödvändigt att regeringen tydligt står bakom visionen. I detta avseende har även Digitaliseringsrådet och DIGG uppgifter att fylla men det saknas mandat och resurser gentemot respektive sakområde. Flera andra länder har tydligare mål vilket också gör att uppföljningen blir enklare.[379]

Digitaliseringsrådet tar upp Storbritannien som ett land som arbetar aktivt med att underlätta för offentliga organisationer att utvecklas digitalt, bland annat genom den så kallade ”Digital Service Standard” med 18 kriterier som hjälper staten att ta fram bra digitala tjänster (alla tjänster som används av allmänheten måste följa denna standard). Ett annat exempel är den norska digitaliseringsstrategin Digital

[373] Digitaliseringsrådet, 2018b, s. 32.
[374] Internetstiftelsen, intervju, 2019-09-02.
[375] ”Artificial intelligence”, Université de Montreal. Hämtad 2019-12-03 från https://www.umontreal.ca/en/artificialintelligence/.
[376] Exempelvis *Future of Humanity Institute* vid universitetet i Oxford och *Ada Lovelace Institute*. I USA finns sedan 2016 AI Now Institute som studerar sociala konsekvenser av AI.
[377] “WASP - Humanities and Society”, Wallenberg AI, Autonomous Systems and Software Program. Initiativet löper under åren 2019–2028. Hämtat 2019-12-03 från https://wasp-sweden.org/research/wasp-hs/. Som Andersson, Gustavi och Karasalo (2019, s. 79) noterar utgör forskningsprogrammet WASP den enskilt största AI-satsningen i Sverige, men man konstaterar också att WASP är ett privat initiativ, finansierat av Knut och Alice Wallenbergs Stiftelse, som inte kan förväntas täcka svenska statens intressen och som bör ses som ett komplement till statliga satsningar.
[378] IVA, 2019, s. 25.
[379] Digitaliseringsrådet, 2019, s. 14.

21, som anger ett antal praktiska rekommendationer för säkerhetsarbetet: bland annat att små och mellanstora organisationer ges bättre verktyg för säkerhetsarbetet (t.ex. i form av checklistor för att kunna göra en ”enkel hälsokontroll” av den digitala säkerheten); att informationsöverföring mellan privata och offentliga aktörer om it-incidenter stärks i syfte att samhället ska bli bättre på att avvärja angrepp; att en minimistandard för cybersäkerhet tas fram som ska gälla för leveranser till det offentliga.[380]

I Sverige ansvarar den nya myndigheten för digital förvaltning, DIGG, för *vägledning för webbutveckling* som är de officiella riktlinjerna för arbete med webbplatser i offentlig sektor, men som Digitaliseringsrådet påpekar är den svenska vägledningen just riktlinjer som främst har fokus på utvecklingsarbete och tillgänglighetsaspekter.[381]

När det gäller frågan om exponering, som beskrevs i avsnitt 5.5, som handlar om att allt fler saker och processer kopplas upp, riskerar Sverige att bli särskilt sårbart genom de många satsningarna på ”smarta” lösningar, exempelvis ”smarta städer”, som innebär att många funktioner kopplas upp mot en central enhet. Som visats i tidigare FOI-studier finns många förslag på hur säkerheten kan förbättras på IoT-området.[382] Ett av dessa exempel beskrivs närmare i avsnitt 6.2

Frågan om asymmetrier, som vi beskrev i avsnitt 5.6, är komplex eftersom den har att göra med globala strukturer och marknadsförhållanden som har skapat en trend mot allt färre tjänsteleverantörer som allt fler är beroende av. IVA har i detta sammanhang föreslagit en kartläggning av konsekvenserna av dagens monokulturer i syfte att minska risken med ”single point of failure”.[383] I sammanhanget asymmetrier tog vi även upp risken för att en digital klyfta skapas mellan de i samhället som har kapacitet och möjlighet att använda sig av den digitala tekniken och de som inte har detta. Det saknas dock inte aktörer och traditioner som kan motverka en sådan negativ utveckling. Särskilt biblioteken kan få, och har redan, en viktig roll när det gäller att tillgängliggöra digitaliseringens nya verktyg och förhållningssätt. Som beskrivs i den nationella biblioteksstrategin:

> Biblioteken ska spela en stor roll för att överbrygga de digitala klyftorna och fortsätta det framgångsrika arbete som pågår, inte minst i samverkan med folkbildningen. De som inte har tillgång på annat vis ska få tillgång till datorer och annan digital utrustning på biblioteken. På så sätt ska biblioteken ses som samhällets väg till allas möjlighet att bli del i det digitala samhället.[384]

När det gäller frågan om tillit och förväntningar, som beskrevs i avsnitt 5.7 och 5.8 handlar detta återigen mer om kultur och attityder än teknik. Här handlar det

[380] Digital21, 2018, s. 82.
[381] Digitaliseringsrådet, 2019, s. 24.
[382] Se t.ex. Swaling & Johansson, 2018.
[383] IVA, 2019, s., 29.
[384] Fichtelius, Persson & Enarson, 2019, s. 12.

kanske inte om att hitta lösningar och svar utan mer om att ändra sättet att ställa frågor. Istället för att börja med målet att digitalisera kan det vara rimligt att ställa frågor om vad verksamheten vill uppnå och hur digitaliseringen kan stödja detta.

En av de kanske svåraste frågorna som denna rapport har ställt beskrevs i avsnitt 5.9, *Plan B?* Frågan handlar om vilken eventuell back-up-plan samhället bör, vill eller kan ha för den händelse att en allvarlig samhällsstörning inträffar där strömförsörjningen slås ut och de digitala lösningarna inte längre är tillgängliga. Ytterst handlar detta om vilken risk vi är villiga att acceptera liksom vilka kostnader för redundans vi är redo att bära. Ju högre risk vi accepterar, desto färre reservsystem och alternativa rutiner kommer vi att ha på plats, och desto större kommer också standardsänkningen att bli i händelse av en kris.

En sammanställning som denna av problem och utmaningar förmedlar möjligen en dyster utblick över det digitala risklandskapet. Men som påpekas i Verizons årliga undersökning *Data Breach Investigations Report* finns ingen anledning att gå och gömma sig. Bättre är att acceptera att även om det inte finns något sådant som total säkerhet, så finns trots allt möjligheten att agera proaktivt för att skydda det man värderar. [385] Med utgångspunkt i detta avslutas kapitlet med tre fördjupande exempel på strategier inom IoT, AI och dataskydd.

6.2 Strategier för IoT-säkerhet

Trenden att koppla upp ett stort antal objekt mot nätet och med varandra har identifierats som en säkerhetsrisk i forskning och litteratur. Som beskrevs i kapitel 4.1 är den inbyggda säkerheten ofta låg, med svaga lösenordsskydd och ogenomtänkta sammankopplingar mellan icke-skyddsvärda och skyddsvärda objekt eller funktioner. Denna problematik har även börjat uppmärksammas på nationsnivå, där ett exempel är de grundläggande principer för IoT-säkerhet som tagits fram av USA:s departement för inrikes säkerhet, U.S. Department of Homeland Security (DHS). DHS kriterier har analyserats och bearbetats i en FOI-rapport som också har legat till grund för publikationer om IoT-säkerhet som MSB har givit ut.[386]

Principerna är riktade till utvecklare, tillverkare, tjänsteleverantörer och aktörer med ett övergripande säkerhetsansvar inom samhällsviktig verksamhet, industri och statlig styrning.

[385] Verizon, 2018, s. 4.
[386] Swaling Hedtjärn & Johansson, 2018. Se även MSB, 2018b.

För att organisera sitt sätt att tänka kring IoT-säkerhet föreslår DHS att aktörerna ska

1. verka för säkerhetsuppdateringar och sårbarhetshantering
2. bygga in säkerhet redan i designfasen (s.k. ”security by design”)
3. ansluta enheter genomtänkt och med försiktighet
4. bygga på beprövad praxis
5. prioritera säkerhetsåtgärder utifrån potentiell påverkan
6. verka för transparens inom IoT.

Det finns väsentligen två sätt att eliminera risker – antingen genom att minska sannolikheten för en händelse genom *förebyggande riskhantering*, eller att mildra konsekvenserna genom *konsekvenslindrande riskhantering*. Hur harmonierar DHS principer med dessa strategier? I det följande beskrivs olika typer av åtgärder kopplat till dessa 6 principer.

Principen om att *verka för säkerhetsuppdateringar och sårbarhetshantering* (1) harmonierar med en strategi för förebyggande riskhantering. Denna måste i sin tur fokusera antingen på attackvektorerna som utnyttjar sårbarheterna, eller på sårbarheterna i sig. I bägge dessa fall är *begränsad access* en nyckelparameter. Det kan noteras att många attacker förutsätter någon form av informationsinhämtning eller sekretessöverträdelse. Angrepp mot riktighet och tillgänglighet sker många gånger i ett andra steg, med effekter i samhällsviktiga funktioner som tänkbar följd. Många angrepp skulle därmed kunna förhindras om själva informationsinhämtningen eller intrånget förhindrades. Sårbarheter i IoT-enheter som det tydligt går att göra något åt är svaga lösenord och fysisk exponering.

Även principerna om att *bygga in säkerhet i designfasen* (2) och *ansluta enheter genomtänkt och med försiktighet* (3) är väsentligen av förebyggande karaktär. Lösenord bör vara säkra som standard, och om nödvändigt kunna ändras till något enklare och eventuellt mindre säkert, inte tvärtom. På motsvarande sätt ska en enhet inte levereras med några andra uppkopplingar än de som är nödvändiga för dess grundläggande funktion och syfte. Inte minst inom industriella tillämpningar gäller att enheter inte ska vara uppkopplade i onödan.

När det gäller konsekvenslindrande åtgärder så handlar dessa mycket om traditionell it- och ICS-säkerhet eftersom den stora risken med IoT-enheter är att de kan utnyttjas för att ta sig in i it- och ICS-system. En vettig strategi torde därmed vara att stärka det ordinära it- och ICS-säkerhetsarbetet i samhällsviktig verksamhet för att begränsa konsekvenserna *om* ett intrång lyckas. Principerna om att *bygga på beprövad praxis* (4) och att *prioritera säkerhetsåtgärder utifrån potentiell påverkan* (5) harmonierar med en sådan strategi. Rent konkret kan de konsekvenslindrande åtgärderna handla om att öka robustheten genom att redundans byggs in och genom robust hantering av feltillstånd i viktig utrustning, dvs. att det finns felsäkra reservrutiner för viktiga funktioner.

Principen om att *verka för transparens inom IoT* (6) kan tolkas i termer av att syftet med att en enhet är uppkopplad tydligt ska kommuniceras till användarna. Det kan också betyda att information om händelser och sårbarheter ska kunna delas av många utan att detta äventyrar grundläggande kommersiella incitament. Några av de förslag som DHS ger handlar om att bygga upp certifieringsmöjligheter, regelverk och standarder samt att stärka möjligheterna att ställa aktörer till svars för IoT-händelser. Det gäller att skapa incitament så att ”säkerhet lönar sig”. Genom att se säkerhet som ett attribut hos nätverksuppkopplade enheter har det hävdats att både tillverkare, leverantörer och tjänsteleverantörer ges en möjlighet till marknadsdifferentiering. Här finns säkerligen utrymme för flera tekniska certifieringar.

6.3 Strategier för AI-säkerhet och automatiserat beslutsfattande

Som beskrevs i kapitel 4.2 har utvecklingen inom AI (där begreppet förstås i vid mening) bäring på såväl infrastruktur och nationell säkerhet som demokrati och mänskliga rättigheter. Detta innebär att det finns många olika dimensioner av AI-säkerhet. Andersson, Gustavi och Karasalo (2019) konstaterar att säkerhet kopplat till AI idag är ett växande forskningsområde som studerar frågor som exempelvis berör *transparens* (hur intelligenta system kan designas som samtidigt är transparenta); *väldefinierade mål* (hur man kan säkerställa att det mål som sätts för ett intelligent system verkligen leder till önskat resultat utan allvarliga bieffekter); *robusthet och stabilitet* (hur man kan säkerställa att oväntade förändringar i systemets förutsättningar inte leder till allvarliga negativa effekter) och *hantering av sårbarheter* (hur man kan skapa och träna system för att minimera risken för felbedömningar på grund av avsiktlig manipulation).[387]

Ett område som fått relativt stor uppmärksamhet de senaste åren berör automatiserat beslutsfattande (och relaterade transparensfrågor). I svensk offentlig förvaltning har frågan om automatiserat beslutsfattande i stor skala varit aktuell sedan åtminstone 2004, då försöken med trängselskatt i Stockholm började planeras.[388] Lagen som infördes för dessa försök inkluderade en skrivning om att besluten tas genom automatiserad behandling. Numera är automatiserade beslut uttryckligen generellt tillåtna inom offentlig förvaltning, sedan en ändring av Förvaltningslagen trädde i kraft den 1 juli 2018.[389] Förändringen innebär att automatiserade beslut kan användas utan speciella undantag eller tillägg i andra författningar.[390] Lagen gör ingen skillnad på automatiserade och manuella beslut, utan dessa omfattas av samma skyldigheter och ansvarsförhållanden som icke-

[387] Andersson, Gustavi & Karasalo, 2019, s. 78.
[388] Prop 2003/04:145.
[389] SFS 2017:900.
[390] Prop. 2016/17:180.

automatiserade beslut. Exempelvis ska besluten dokumenteras enligt samma principer som om de hade tagits av en mänsklig handläggare.[391]

AlgorithmWatch[392] och Bertelsmann Stiftung[393] har tillsammans tagit fram rapporten *Automating Society*, där de undersöker läget kring automatiserat beslutsfattande i EU:s medlemsländer.[394] Rapporten noterar att automatisering av beslut kan vara fantastiskt, men att det även kan innebära negativa konsekvenser som exempelvis att beslut fattas på diskriminerande grunder. De trycker på att system för automatiserade beslut inte kan ses som enbart tekniska system, utan att de måste ses i ett socioteknisk sammanhang som även inkluderar beslutsmodeller, algoritmer, indata samt den politiska och ekonomiska omgivning som systemet verkar i. Utifrån resultaten som presenteras i *Automating Society* presenteras följande rekommendationer, riktade brett till politiker, intresseorganisationer och företag inom EU.[395]

- Fokusera diskussionen på de aspekter som är politiskt relevanta.
- Avgränsa debatten kring AI till den utveckling som pågår eller ligger nära i tiden.
- Överväg automatiserade beslutssystem som en helhet, inte bara som en teknik.
- Utbilda medborgarna så de har möjlighet att anpassa sig till de nya utmaningar som tekniken för med sig.
- Se till att offentlig förvaltning har den kompetens som krävs för att anpassa sig.
- Stärk civilsamhällets engagemang i frågor kring automatiserat beslutsfattande.
- Se till att lämpliga tillsynsmyndigheter finns och att de har rätt kompetens.
- Minska skillnaderna mellan medlemsländer.
- Ta fram de regelverk som behövs utöver dataskydd.
- Inkludera ett brett spann av intressenter och intresseorganisationer, inklusive medborgarrättsorganisationer, när kriterier utvecklas för vad som är bra designprocesser och tillsyn.

En ännu mer övergripande diskussion i AI-sammanhang handlar om huruvida mer reglering och kontroll är en god eller dålig idé. Vilken ståndpunkt som intas beror

[391] Ibid.
[392] AlgorithmWatch är en icke vinstdrivande organisation med syftet att undersöka och belysa algoritmbaserade beslutsprocesser som har inflytande på samhället, se https://algorithmwatch.org/en/what-we-do/.
[393] Bertelsmann Stiftung är en politiskt obunden stiftelse som grundades av Reinhard Mohn, ägaren till Bertelsmann AG. Stiftelsens syfte är att verka för allmänhetens bästa (eng. *common good*) och att alla ska kunna delta i samhället, se https://www.bertelsmann-stiftung.de/en/.
[394] Speilkramp, 2019.
[395] Ibid.

på hur olika aktörer bedömer riskerna och sannolikheten att olika hot ska realiseras. Här finns en bred skala där somliga lutar åt att stora överdrifter vidhäftar AI-debatten, medan andra manar till försiktighet med tanke på de värden som står på spel. Historiskt är det inte ovanligt att regleringar införts inom nya teknikområden utifrån försiktighetsprincipen: forskning om mänskligt DNA och utveckling av biologiska vapen utgör exempel på områden som tidigt reglerades.[396] De senaste åren har sett en stor produktion av policys och riktlinjer för utveckling och tillämpning av AI-system, dokument som har tagits fram av såväl företag som enskilda länder och organisationer.[397] Fokus i dessa sammanhang tenderar att vara på tillväxt och etik snarare än traditionella säkerhetsfrågor. Regleringar av digital teknik via lagstiftning är än så länge relativt ovanligt, med undantag av frågor som gäller skydd av data och/eller personlig integritet.[398]

Ett argument *för* mer reglering är att AI är ett typiskt teknikområde med *dual use*-karaktär, vilket innebär att godvilliga tillämpningar lika väl kan omstöpas till illvilliga sådana.[399] Det antas även finnas ett behov av att dämpa starka kommersiella drivkrafter som inte har säkerhet eller de större samhällsperspektiven som främsta fokus.[400] Det har i detta sammanhang påpekats att det stora intresset hos globala företag att ta fram policys om etik kan ha att göra med en önskan om att undvika tvingande regleringar och lagstiftning.[401] Samtidigt finns också exempel på företagsledare som tvärtom betonat vikten av regleringar. Till exempel sade Elon Musk, en av grundarna till OpenAI,[402] i juli 2017 att "AI utgör det ovanliga fallet där vi behöver vara proaktiva vad gäller reglering, snarare än reaktiva".[403]

Argumenten *mot* reglering handlar bland annat om att lagstiftarna, på grund av sin bristfälliga förståelse för tekniken, riskerar att överreglera (eller reglerera fel saker) vilket skulle kunna lägga en blöt filt över ett teknikområde som på många sätt skulle kunna gynna mänskligheten. En problematik i detta sammanhang handlar om teknikutvecklingens hastighet – ny lagstiftning kan vara obsolet redan när den träder i kraft. Om lagstiftningsinstrumentet ska användas måste den alltså vara principiell nog för att vara relevant utan att för den skull bli för luddig och därmed verkningslös.[404]

Frågan om regleringsbehov handlar i grunden om bedömning av risk. I EU-kommissionens utkast till Ethics Guidelines (2018) drogs slutsatsen att "På det

[396] Yudkowsky, 2008.
[397] Se kartläggning i Cussins Newman, 2019.
[398] Ett exempel är EU:s nyligen implementerade GDPR-lagstiftning.
[399] Brundage, Avin, Clark, Toner m.fl., 2018, s. 16.
[400] Broad, 2018, s. 140.
[401] Men som påpekas i Broad, 2018, s. 140: "You cannot have ethics without justice."
[402] OpenAI är ett Kalifornien-baserat företag som vill främja utvecklingen av god AI. Se https://openai.com/about/.
[403] Elon Musk, citerad i Cussins Newman, 2019, s. 34: "AI is a rare case where we need to be proactive about regulation instead of reactive."
[404] Wahlgren, 2018.

hela taget överväger AI-utvecklingens möjligheter dess risker…”.[405] Detta uttalande har kritiserats av matematikern Olle Häggström som menar att dokumentet saknar en systematisk analys av just riskerna och därmed utgör ett exempel på hur vågskålen med risker tenderar att bagatelliseras i politisk mainstreamretorik. Särskilt problematiskt blir detta, menar Häggström, i sammanhanget av autonoma vapen och anför som exempel en debatt under en konferens år 2017 då kognitionsvetaren Steven Pinker framhöll att det skulle krävas ”en galning” för att konstruera något så hemskt som ”en svärm av robotinsekter avsedd att attackera enskilda människor baserat på ansiktsigenkänning”.[406] Enligt Pinker finns det idag inte längre utrymme för sådana enstaka galningar då ju alla betydande ingenjörsprojekt numera genomförs i stora samarbeten. Men som Häggström påpekar ignorerar denna optimism helt den inre logiken i kapprustningar och ”förbiser att minst lika hemska vapen har utvecklats i över 70 års tid – inte av ensamma galningar, utan just i stora samarbetsprojekt (varav Manhattanprojektet är det mest kända).”[407]

Något som kan konstateras är att AI-system, precis som annan teknik, är behäftade med en uppsättning möjliga fel, brister och sårbarheter som måste hanteras. Det kan också antas att detta förhållande blir viktigare att beakta ju mer kontroll som lämnas över till tekniken där utvecklingen av generell (superintelligent) AI i förlängningen kan innebära mycket stora risker om inte kontrollproblematiken hanteras. En komplicerande faktor i detta sammanhang är, som Häggström påpekar, den kapplöpningsmentalitet som allmänt råder inom AI-området och som är vanligt förekommande även i den svenska AI-diskursen. Faran här ligger i att säkerhetsfrågorna kommer som en eftertanke när de istället skulle behöva integreras i utvecklingsarbetet på ett tidigt stadium, såväl vad gäller de mer vardagliga tillämpningarna som forskningen om generell AI.[408]

Vad gäller framtagandet av strategier för att hantera risker och sårbarheter relaterade till AI kommer det att finnas behov av att dela upp och konkretisera dessa på olika teknikområden och domäner. Det är exempelvis skillnad mellan att utforma strategier för att hantera deep fakes eller för att hantera illvillig användning av drönare. Inom varje område finns dessutom en hel verktygslåda av motåtgärder. För att ta exemplet med deep fakes beskrivs i rapporten *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* (2018) såväl

[405] Häggström, 2019, s. 14-19. Se även ”Draft Ethics guidelines for trustworthy AI”, Europeiska kommissionen, AI HLEG, 18 december 2018, hämtad 2019-12-03 från https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai. Denna formulering finns dock inte med i den slutliga versionen av riktlinjerna: ”Ethics guidelines for trustworthy AI”, Europeiska kommissionen, 8 april 2018, hämtad 2019-12-03 från https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
[406] Häggström, 2019, s. 17.
[407] Ibid.
[408] Ibid., s. 18-19.

tekniska och juridiska som kommersiella lösningar på problemet med manipulerade eller falska film- och ljudinspelningar.[409] Ett exempel på försök med ny lagstiftning är initiativet att inrätta ett slags partiellt förbud som pågår just nu i Kalifornien där en lag har tillkommit som gör det olagligt att distribuera manipulerade videor som har som syfte att misskreditera en politisk kandidat och lura väljare 60 dagar före ett val.[410]

I sin kartläggning av nationella AI-strategier noterar Jessica Cussins Newman slutligen att många regeringar betonar vikten av privat-offentliga partnerskap. Samtidigt, påpekar Cussins Newman, har policymakare i detta sammanhang ”ett unikt ansvar för att skydda allmänhetens intressen, ett ansvar som är än tyngre i tider av stor teknisk förändring.”[411] Andersson, Gustavi och Karasalo (2019), som skrivit om AI i en svensk totalförsvarskontext, betonar att även om Sverige i grunden har goda förutsättningar att ta sig an de utmaningar som AI-utvecklingen medför så är det riskabelt att i för hög grad förlita sig på att industrin och privata forskningsinitiativ ska ta ansvar för frågor av nationellt intresse. Särskilt viktigt blir det i detta sammanhang, menar Andersson, Gustavi och Karasalo, att säkerställa kompetensförsörjningen – för att inte Sveriges nationella säkerhet ska bli helt beroende av utländsk expertis behöver en inhemsk kompetens inom avancerad databehandling byggas upp och bibehållas.[412]

6.4 Strategier för dataskydd

Dataskydd innebär att insamling, hantering och behandling av data kopplad till individer ska göras på ett säkert sätt. Dessutom ska eventuella beslut kopplas till att sådana data tas på ett rättssäkert sätt. Principerna för dataskydd utgår från etiska hänsyn till individen och dennes rättigheter. Förenta Nationernas generalförsamling noterar 2018 att den snabba tekniska utvecklingen innebär en ökad risk för att företag, stater och individer bryter mot de mänskliga rättigheterna genom exempelvis ökad övervakning eller insamling av data.[413]

---

[409] Chesney & Citron, 2018. Som rapportförfattarna påpekar är inte alla deepfakes illvilliga – experiment med filmteknik kan tänkas tillämpas inom konst, vetenskap, utbildning och nöjesindustrin (ett exempel på det senare är Stars Wars-filmen *The Last Jedi* där en scen med prinsessan Leia tillkom efter Carrie Fischers död, genom deep learning-teknik). Ibid., s. 15.

[410] Lagtexten kan läsas här: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730. Enskilda medborgare ska också kunna stämma den som skapar en video där de placeras utan samtycke. https://computersweden.idg.se/2.2683/1.724587/kalifornien-politiska-deepfakes.

[411] Cussins Newman, 2019, s. 4: ”Policymakers have the unique primary responsibility to protect the public interest, and this responsibility carries even greater weight during periods of significant technological transformation.”

[412] Andersson, Gustavi & Karasalo, 2019, s. 80.

[413] “The right to privacy in the digital age”, United Nations General Assembly, A/C.3/73/L.49/Rev.1, 14 november 2018. Hämtad 2019-12-03 från https://undocs.org/pdf?symbol=en/A/C.3/73/L.49/Rev.1.

FN utarbetade riktlinjer för insamling och behandling av data redan år 1990. Dessa riktlinjer antogs som resolution av FN:s generalförsamling, vilket innebär att samtliga medlemsländer uppmanas att arbeta in riktlinjerna i sina respektive lagstiftningar.[414] Riktlinjerna består av sex grundprinciper för datahanteringen: *laglighet och rättvisa, precision, ändamålsenlighet, åtkomst till information om egna personen, icke-diskriminering* samt *att data ska skyddas mot säkerhetshot*.[415] Därtill finns fyra principer som rör lagstiftningens utformning och som berör möjligheten att göra undantag från grundprinciperna, att det ska finnas övervakning och sanktionsmöjligheter, hur reglering av gränsöverskridande dataflöden ska utformas samt inom vilka områden som riktlinjerna ska appliceras.[416]

FN:s riktlinjer ligger på en hög nivå vilket gör att det kan vara svårt att se exakt hur dessa ska appliceras för olika fall. *EU:s byrå för grundläggande rättigheter*[417] (FRA) ger ut handböcker och råd inom bland annat dataskyddsområdet. I deras rapport om läget kring de grundläggande rättigheterna år 2019 tar de upp att senare tids utveckling inom AI och big data har lett till många initiativ som fokuserar på att maximera de ekonomiska fördelarna med tekniken.[418] De säger att endast *ett rättighetsbaserat förhållningssätt* kan garantera en hög skyddsnivå mot de faror som tekniken för med sig.[419] Därmed bör EU:s medlemsstater utgå ifrån de grundläggande rättigheterna när de tar fram nationella strategier kring AI och big data och att arbetet ska inkludera experter från alla relevanta områden. De noterar även att etik kan komplettera ett rättighetsbaserat förhållningssätt, men inte ersätta det.[420]

EU:s stadga om de grundläggande rättigheterna fastslår följande grundprinciper för dataskydd.[421]

- Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

[414] "General Assembly – Forty-fifth Session: 45/95. Guidelines for the regulation of computerized personal data files", FN:s generalförsamling, 14 december 1990. Hämtad 2019-13-03 från https://undocs.org/A/RES/45/95.
[415] "Guidelines for the Regulation of Computerized Personal Data Files", Office of the United Nations High Commissioner for Human Rights, 1990. Hämtad 2019-12-03 från https://www.refworld.org/pdfid/3ddcafaac.pdf.
[416] Ibid.
[417] FN:s term *mänskliga rättigheter* och EU:s term *grundläggande rättigheter* avser båda individens rättigheter.
[418] "Fundamental Rights Report", European Union Agency for Fundamental Rights, juni 2019, s.166. Hämtad 2019-11-20 från https://fra.europa.eu/en/publication/2019/fundamental-rights-2019.
[419] Ibid., s. 166.
[420] Ibid.
[421] "Europeiska unionens stadga om de grundläggande rättigheterna", EU 2012/C 326/02. Hämtad från https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:C2012/326/02&from=HR.

- Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem.
- En oberoende myndighet ska kontrollera att dessa regler efterlevs. (EU 2012/C 326/02, artikel 1).[422]

Sedan maj 2018 gäller EU:s dataskyddförordning GDPR[423] i samtliga medlemsländer inom EU. GDPR utgår från de grundläggande rättigheterna och förtydligar dessa genom ett antal principer för behandling av personuppgifter. Bland annat anges att uppgifterna om den registrerade ska samlas in för *särskilda, uttryckligt angivna och berättigade ändamål* och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.[424] Principerna innebär i praktiken att systemen ska utgå från att den personliga integriteten ska bevaras och att all insamling och behandling av personuppgifter ska minimeras till de fall där den är nödvändig eller berättigad. Lagen föreskriver även ansvarsskyldighet där exempelvis ett företag som bryter mot GDPR kan påföras kännbara sanktionsavgifter – maximalt belopp är det högre beloppet av antingen 20 miljoner euro eller 4 % av företagets globala årsomsättning.[425] Denna möjlighet har nyttjats av CNIL, den franska motsvarigheten till Datainspektionen, som i januari 2019 beslutade att påföra Google en sanktionsavgift på 50 miljoner euro för att de har brutit mot GDPR.[426]

Som forskaren och debattören Wolfie Christl påpekar är individens *medgivande* och dennes *valmöjlighet att avstå* datainsamling nödvändiga förutsättningar för att hantera de mest brådskande problemen med påträngande datainsamling.[427] Medgivande och valmöjlighet kan dock ge en illusion av valfrihet, då priset för att

[422] Ett specifikt rättsfall som EU:s byrå för grundläggande rättigheter tar upp är EU-domstolens utslag angående lagring av trafikdata hos teleoperatörer. Efter att EU-domstolen annullerade EU-direktivet om datalagring år 2014 blev följden att vissa EU-länder justerade de egna lagarna inom området så att de följde domstolens utslag, medan andra EU-länder fortfarande behöll lagstiftning motsvarande det ogiltiga EU-direktivet. I ett uppmärksammat fall från 2016 slog EU-domstolen fast att nationell lag inte får föreskriva datalagring som står i strid med de grundläggande rättigheterna eller med EU-lagar. Dom av den 21 december 2016, Tele2 mot Watson, C-203/15 och C-698/15, ECLI:EU:C:2016:970. Hämtad från https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX%3A62015CJ0203. Byrån för grundläggande rättigheter anser att medlemsländerna måste se till att de nationella lagarna är i linje med EU-domstolens utslag och att de måste ta hänsyn till proportionalitet. FRA, 2019, s. 165.

[423] General Data Protection Regulation.

[424] "Europaparlamentets och rådets förordning (EU) 2016/679", EU 2016/679, artikel 5. Hämtad från https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=celex%3A32016R0679.

[425] Ibid, artikel 83.

[426] "Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC", Commission Nationale de l'Informatique et des Libertés (CNIL). Hämtad 2019-12-04 från https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf.

[427] Christl, 2017.

avstå är att individen inte kan nyttja en tjänst som exempelvis är ekonomiskt fördelaktig.[428] Brist på valmöjligheter blir extra tydlig i de fall där individen står i beroendeställning gentemot den som samlar in personuppgifter. I augusti 2019 utfärdade Datainspektionen sin första sanktionsavgift enligt GDPR till en gymnasieskola som på försök testade automatiserad, kamerabaserad ansiktsigenkänning för att registrera elevernas närvaro.[429] Beslutet motiverades delvis med att eleverna befann sig i beroendeställning mot skolan och att samtycke därför inte kan utgöra en laglig grund för personuppgiftsbehandlingen.[430] Dessutom är de biometriska data som samlades in att betrakta som känsliga personuppgifter.[431]

Ett specifikt område där potentiellt mycket känslig information samlas in om individer i utsatta positioner är medicinsk forskning. The Belmont Report från USA:s hälso- och socialdepartement fastställde tre grundläggande etiska principer för att skydda mänskliga forskningssubjekt: *respekt för individen*, *godhet* (eng. *beneficence*) och *rättvisa*. En aspekt som lyfts fram är vikten av att skydda personer med begränsad möjlighet till eget bestämmande.[432]

Den Europeiska läkemedelsmyndigheten (EMA) har bildat en arbetsgrupp tillsammans med Heads of Medicines Agencies (HMA) för att undersöka big data-området. Avsikten med arbetsgruppen är att ta fram rekommendationer och riktlinjer för hur regelverk kan utformas kring big data, för att tekniken ska kunna ge bättre förståelse av sjukdomar, mediciner och effektiviteten hos medicinska produkter. De slutliga rekommendationerna från arbetsgruppen är inte publicerade när denna rapport skrivs, men däremot finns delresultat i form av nio nyckelområden med tillhörande preliminära rekommendationer. Bland dessa kan nämnas att *standardisera till några få dataformat*, *förbättra bedömning och dokumentation av datakvalitet*, *öka datadelningen inom hälso- och sjukvård*, *uppmuntra sammanlänkning av data* samt *utveckla ramverk för att möjliggöra nya analysmetoder*.[433]

Policyer på hög nivå, exempelvis baserade på de grundläggande rättigheterna, måste kompletteras med rekommendationer och riktlinjer på en betydligt mer

[428] Ibid.
[429] ”Tillsyn enligt EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever” , DI-2019-2221, Datainspektionen.
[430] Ibid.
[431] Ibid.
[432] Ryan, Brady, Cooke, Height, Jonsen, King, Lebacqz, Louisell, Seldin, Stellar & Turtle, 1979.
[433] “HMA-EMA Joint Big Data Taskforce: Summary report”, Heads of Medicines Agencies (HMA) och European Medicines Agency (EMA), 13 februari 2019. Hämtad 2019-12-04 från https://www.ema.europa.eu/en/documents/minutes/hma/ema-joint-task-force-big-data-summary-report_en.pdf.

tekniknära nivå. ENISA[434] har genomfört en studie där de fokuserat på informationssäkerheten vid insamling och hantering av stora datamängder. Rapporten tar upp fem rekommendationer till de organisationer som arbetar med big data:[435]

- Beslutsfattare bör fokusera på att ge riktlinjer för säker användning av big data i kritiska sektorer.
- Företag bör följa relevanta säkerhetsstandarder när de utvecklar produkter inom big data.
- Myndigheter med sektorsansvar bör uppmuntra företagen att använda säkra protokoll och autentiseringsmekanismer i deras produkter.
- Standardiseringsorgan bör anpassa existerande säkerhetsstandarder eller skapa nya säkerhetsstandarder för big data-området.
- Företag bör investera mer i att förbättrad personalens kunskap kring teknisk säkerhethet för big data, exempelvis genom utbildningar och certifieringar.

För att motverka att medborgarna i allt större utsträckning måste bli sina egna handläggare som följd av digitalisering krävs en betydande samordning av olika myndigheters verksamheter och system. Samtidigt finns hinder för offentliga verksamheter då det i de flesta fall inte är tillåtet att dela information mellan dem. En proaktiv samordning kan exempelvis innebära att ingången till olika myndigheters tjänster blir gemensam och att medborgarna får möjlighet att mata in sina data *en* gång oavsett antalet inblandade myndigheter.

Ett svenskt exempel på gemensam ingång är Verksamt.se, en webbplats för Bolagsverket, Skatteverket, Tillväxtverket och Arbetsförmedlingen.[436] Webbplatsen innehåller dock bara ett mindre antal egna tjänster för användarna. Övriga tjänster återfinns på webbplatserna som tillhör respektive myndighet, vilket innebär att användaren blir vidareskickad dit för att utföra sina ärenden. Estland har kommit längre genom sin portaltjänst Eesti.ee, där medborgare kan hitta många digitala tjänster inom exempelvis hälsa- och sjukvård, fordonsregister, medborgarskap, utbildning, familjefrågor och företagande.[437] Riksrevisionens granskning *Enklare att starta företag* visar att denna typ av samverkansplattform inte är oproblematisk i Sverige, med exempelvis olika prioriteringar hos de inblandade parterna, komplicerade finansieringsfrågor och rättsliga hinder att utbyta information mellan aktörer.[438] För att ge bättre förutsättningar för digitaliseringen av offentlig förvaltning rekommenderar Riksrevisionen att Regeringen ska

> … fortsatt vidta åtgärder för att underlätta digital samverkan mellan myndigheterna. Fokus bör läggas på […] till exempel rättsliga förutsättningar för digitala tjänster, mål- och

[434] Europeiska unionens cybersäkerhetsbyrå (European Union Agency for Cybersecurity).
[435] Naydenov, Liveri, Dupre, Chalvatzi & Skouloudi, 2015.
[436] https://www.verksamt.se/.
[437] https://www.eesti.ee/en/.
[438] RIR 2019:14.

> prioriteringskonflikter vid digital samverkan samt finansieringsutmaningar vid utveckling och drift av förvaltningsgemensamma digitala tjänster.[439]

Den etiska utgångspunkten och de mänskliga rättigheterna genomsyrar flera arbeten med principer för att skydda individen när det gäller data. Några grundprinciper som omnämns är *rättvisa*, *transparens* och *ansvarsskyldighet*.[440] Databehandling ska ske rättvist för individen, på ett rättssäkert sätt utan diskriminering eller annan negativ särbehandling. För att säkerställa att databehandlingen är rättvis så krävs transparens, det vill säga insyn, i verksamheterna och hur de hanterar data. I fall där rättvisan eller transparensen inte upprätthålls måste det finnas sanktionsmöjligheter för att utkräva ansvarsskyldighet från ansvariga.

[439] Ibid.
[440] Vedder & Naudts, 2017.

7 Avslutande reflektioner

Begreppet digitalisering har kommit att stå i centrum för många framtidsinriktade diskussioner och dokument i den svenska offentligheten. Digitalisering har presenterats både som ett nödvändigt sätt att möta den ekonomiska och demografiska utmaning som många kommuner står inför, och som vägen in i en helt ny verklighet, karaktäriserad med ord och uttryck som Industri 4.0, den smarta staden, AI och IoT etc. Enligt Sveriges digitala strategi ska landet bli ”bäst i världen” på att tillvarata digitaliseringens möjligheter.[441] Samtidigt tycker sig olika aktörer se tecken på att Sverige håller på att halka efter relativt andra länders framsteg på digitaliseringsområdet.[442] Sammantaget tycks dessa förhållanden ha skapat en känsla av det är *bråttom*. Som vi har visat i denna rapport innebär det dock risker med att ha för bråttom. Förutom risken att ogenomtänkta satsningar riskerar att skapa frustration snarare än användarvänlighet finns också en risk att otillräckliga säkerhetsanalyser gör att sårbarheter byggs in eller negligeras. Sådana projekt hamnar lätt i ett gasa/bromsa-mönster när problem till slut uppstår som måste hanteras.

Digitalisering handlar i grunden, som påpekats i våra intervjuer, om processer som förändrar eller skapar nya värden. Tack vare nya digitala teknologier och it-verktyg har det helt enkelt blivit möjligt att göra saker på annat sätt. Om och hur denna förändring sker är dock inte avhängigt verktygen: Istället krävs en helhetssyn på den verksamhetsförändring som digitaliseringen innebär – varför, hur och för vem sker digitaliseringen? Vilka risker och sårbarheter måste hanteras? Inte minst finns anledning att återvända till frågan om varför. Vanligt förekommande argument i den politiska retoriken är att digitalisering kan spara pengar och effektivisera välfärden. Men dessa motiveringar har ifrågasatts – att digitalisera kan åtminstone initialt vara mycket kostsamt, och frågan om ökad effektivitet beror på om digitaliseringen i praktiken leder till ökad administration för personalen och därmed mindre tid för värdeskapande arbete.[443] En tredje vanlig motivering handlar om att digitaliseringen kan skapa större jämlikhet och rättvisa. Även detta har ifrågasatts, bland annat mot bakgrund av att de data som samlas in i sig aldrig är neutrala – data utgör alltid ett urval som kan vara bristfälligt på olika sätt, eller i värsta fall spegla diskriminerande strukturer i samhället.

Den kritik som exemplifierats ovan handlar inte om att vara emot digitalisering utan om att den tycks göras på fel sätt och ibland av fel orsaker. För den som försöker ta sig an mängden av rapporter på detta område är det dock svårt att få en helhetsbild av digitaliseringens problem. Många rapporter fokuserar på en viss pusselbit, eller ett visst perspektiv (som förvisso kan vara brett, som det vanligt

[441] Regeringskansliet, 2017a; Regeringskansliet, 2017b.
[442] Se t.ex. Digitaliseringsrådet, 2018b, s. 48; ESV 2018:31, s. 8.
[443] SKL, 2019, s. 64.

förekommande tillväxtperspektivet). I denna studie har vi velat ta oss an ett antal grundläggande frågeställningar som har bäring på digitalisering i ett risk- och sårbarhetsperspektiv: Vad innebär det att ”digitalisera”? Vilka är drivkrafterna att digitalisera? Varför och hur uppstår risker och sårbarheter när processer digitaliseras? Vilka förändringsparadigm, eller trender, kan vi urskilja som formar dagens och morgondagens utveckling och användning av digital teknik? Hur ser digitaliseringens problem ut i en svensk kontext? Vilka strategier finns eller kan utvecklas för att mildra digitaliseringens sårbarheter?

Några grundläggande aspekter som beskrevs i kapitel 3 handlade om innebörden av risker, sårbarheter och hot i ett digitaliseringsperspektiv. Här beskrevs också den digitala teknikens inneboende komplexitet liksom samhällets komplexa marknadsstruktur. IVA har i detta sammanhang beskrivit hur samhället tidigare fungerade enligt en stuprörsmodell där en enskild aktör hade kontroll över hela kedjan av infrastruktur.[444] Sedan 1980-talet har istället en avreglerad, horisontell struktur vuxit fram med många konkurrerande aktörer i varje skikt. Denna modell, som IVA liknat vid en lasagne, har skapat fördelar men också en stor samordningskomplexitet.

I kapitel 4 analyserades tre typer av förändringsparadigm med utgångspunkt i begreppsparen *cyber/fysiskt*, *människa/maskin* och *data/individ*. Med dessa tre begreppspar ville vi belysa något mer än tekniktrender. Förändringsparadigmen signalerar framför allt att ytterligare lager av komplexitet tillkommer när gränserna mellan kategorier som tidigare har varit tydligt åtskilda blir alltmer suddiga eller oklara. I det första fallet beskrevs hur utvecklingen mot en alltmer uppkopplad värld, där även samhällskritisk verksamhet riskerar att bli exponerad mot internet, har gjort uppdelningen i cyber och fysiskt alltmer problematisk i ett hot- och riskperspektiv. I det andra fallet, på temat människa/maskin, diskuterades konsekvenserna av en ökad användning av artificiell intelligens i samband med exempelvis automatiserade beslutsprocesser, där risker för oklarheter kan uppstå när det gäller att förstå var ansvaret ytterst ligger eller hur ett visst beslut eller en viss händelseutveckling ska förklaras. Även riskerna med illvillig användning av AI diskuterades inom ramen för detta förändringsparadigm.

I det tredje fallet, på temat data/individ, analyserades konsekvenserna av att allt mer data, exempelvis gällande individers hälsa, vanor och intressen, blir tillgängliga för sammanställningar och analys. Sammantaget belystes hur dessa förändringsparadigm skapar nya sårbarheter samtidigt som de ibland också förstärker eller ändrar karaktären på gamla hot i en redan komplex miljö.

Digitaliseringens problem i den svenska kontexten relaterar på olika sätt till förändringsparadigmen, men har ofta sina rötter i förhållanden som råder i Sverige. I kapitel 5 presenterade vi en analys av nio identifierade problemområden varav

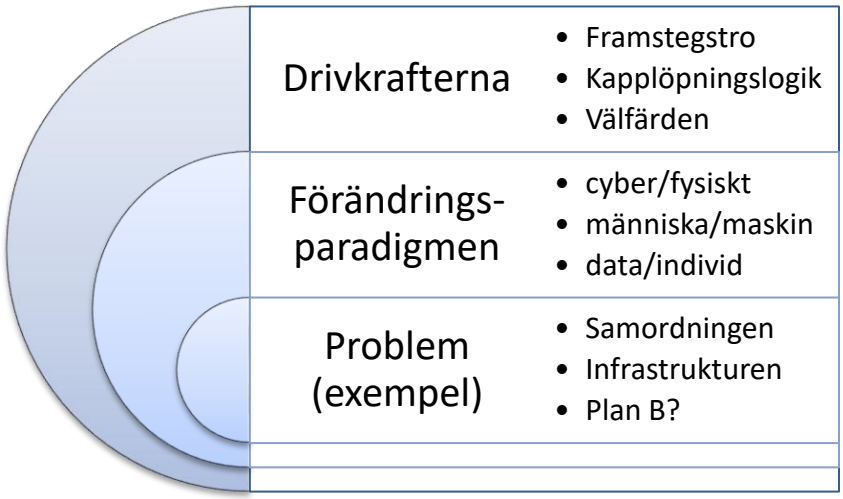
[444] IVA, 2019.

fyra kan hänföras till digitaliseringens praktiska genomförande i Sverige: *(O)takten* syftade bland annat på den ryckighet som uppstår när konsekvens- och säkerhetsanalyserna brister i digitaliseringsprojekt; under rubriken *kompetens-problemet* beskrevs bland annat hur en låg beställarkompetens kan bli en riskfaktor när otillräckliga krav ställs på säkerhet och robusthet; *infrastrukturen* handlade om hur otillräckliga investeringar i nödvändig digital infrastruktur kan leda till osäkra system liksom ett gap mellan faktisk kapacitet och ambitioner; *styrningen och samordningen* handlade om en problematik nära relaterad till infra-strukturproblemet – vem tar ansvar för att lasagnen hänger ihop? Om alltfler samhällsfunktioner kräver en välfungerande digital infrastruktur krävs också ett tydligt samordningsansvar för denna, liksom en plan för hantering av risker som enskilda privata aktörer inte kan förväntas ta ansvar för. På detta område finns dock i Sverige betydande oklarheter som detta avsnitt visade.

Att bristen på samordning och helhetssyn gör att riskhanteringen inte blir optimal ur ett samhällsperspektiv illustrerades vidare under problemen *exponering* och *asymmetrier* som i grunden handlar om konsekvenser av förändringsparadigmen. Exponeringsproblemet handlar om de sårbarheter som skapas genom att olika verksamheter, i värsta fall samhällskritiska sådana, blottas för angrepp genom att många objekt kopplas upp eller ges uppkopplingsmöjligheter (som bäddar för misstag längre fram). Asymmetriproblemet handlar egentligen om flera typer av asymmetrier, bland annat om det ökande beroendet av allt färre tjänsteproducenter och om den relaterade sårbarheten att system ofta är beroende av en enda punkt för sin funktion. Konsekvenserna kan därmed bli stora om denna felkritiska systemdel slås ut (*single point of failure*). Men asymmetrier kan också handla om alltmer skeva maktförhållanden mellan individer och företag, där utvecklingen inom AI bland annat har skapat nya möjligheter att analysera och sortera människor med hjälp av algoritmer som ses som affärshemligheter. Asymmetrier kan också uppstå mellan individer och staten, där komplexa digitaliserade byråkratier riskerar att skapa en klyfta mellan de som har kapacitet och möjlighet att använda sig av de digitala möjligheterna och de som inte har detta.

Under rubrikerna *tilliten* och *förväntningarna* beskrevs ett problematiskt glapp mellan ambitioner och realitet. När förväntningarna överstiger tillgänglig teknik och infrastruktur riskerar digitaliseringsprojekten helt enkelt att fallera. Miss-lyckade digitaliseringsprojekt kan sedan skada tilltron till digitaliseringens möjligheter vilket skulle kunna slå över i en tillbakagång för offentliga satsningar på digitalisering. Risken med detta är att digitaliseringens potential att faktiskt förbättra samhällsservice och skapa tillväxt förspills eller fördröjs. Under rubriken *Plan B?* lyfte vi till slut frågan om det digitala samhällets behov av reservplaner och alternativ i den händelse att något går riktigt fel – om systemen av någon anledning slutar fungera, eller, för att låna titeln på MSB:s beredskapsbroschyr, *om krisen eller kriget kommer*. Även här krävs en helhetsblick på förutsättningarna att skapa robusthet.

De överlappande sambanden mellan drivkrafter att digitalisera, förändringsparadigm och problemområden illustreras i figur 7.1.



Figur 7.1. Illustration av överlappande faktorer som skapar sårbarheter. En typ av sårbarhet grundläggs redan genom drivkrafterna att digitalisera som i Sverige präglas dels av ett kapplöpningsfärgat framstegstänkande, dels vilja att effektivisera och hantera välfärdens utmaningar. Ingen av dessa drivkrafter har säkerhet och robusthet som huvudfokus. Samtidigt skapar teknikens förändringsparadigm nya risker och sårbarheter. Konsekvenserna av dessa förhållanden blir ett antal problem som bland annat handlar om bristande samordning av, liksom robusthet i, den digitala infrastrukturen.

I denna studie har fokus varit på att förstå problemen snarare än att hitta lösningarna. Men vi samlade även avslutningsvis några exempel på strategier för att minska riskerna och sårbarheterna, kopplade såväl till de nio problemen som till förändringsparadigmen. Vad dessa strategiexempel visar är att lösningar sällan är rent tekniska utan handlar om varför och hur den nya tekniken utvecklas och tillämpas liksom även om förmåga att bedöma risker och ställa krav. Ur ett svenskt perspektiv blir det avgörande att skapa förståelse för hur den digitala teknikens förändringsparadigm samspelar med de förutsättningar som råder i Sverige. Om denna orienteringsförmåga utvecklas minskar risken att gå vilse i lasagnen.

Referenser

Intervjuförteckning

Internetstiftelsen. Intervju 2019-09-02.

Netnod. Intervju 2019-09-23.

Myndigheten för samhällsskydd och beredskap (MSB). Intervju 2019-09-27.

Bildkällor

Figur 2.1, s. 13. IBM 650, kallad första generationens dator, invigs 1958 av Generaldirektören för SJ, Erik Upmark. Fotograf: Walther Seved. Ingår i samling Järnvägsmuseets foton. DigitaltMuseum ID 021018177936.

Licens: Fritt från kända upphovsrättsliga restriktioner – Public Domain Mark (PDM)

Figur 2.2, s. 18. Persondator. IBM lanserade sin första PC (Personal Computer) 1981. Modellen hette 5150 och blev en stor succé. Ingår i samling Tekniska museets saker. Fotograf: Ellinor Algin/Tekniska museet. DigitaltMuseum ID 021026360749.

Licens: Erkännande (CC BY):
https://creativecommons.org/licenses/by/4.0/legalcode.sv

Figur 2.3, s. 29. Interiör från Siemens datacentral i Stockholm, årtal okänt. Fotograf: okänd/Tekniska museet. Ingår i Tekniska museets samlingar. DigitaltMuseum ID 021016300504.

Licens: Fritt från kända upphovsrättsliga restriktioner – Public Domain Mark (PDM)

Figur 4.1, s. 51. ”Elektronisk computer för numerisk styrning av en industriprocess (Toledo).” Fotograf: okänd/Tekniska museet. Årtal: okänt. Ingår i samlingen Tekniska museets arkiv. DigitaltMuseum ID 021016300519.

Licens: Fritt från kända upphovsrättsliga restriktioner – Public Domain Mark (PDM)

Figur 4.3, s. 60. Datacentral IKEA, Älmhult, 1971. Fotograf: okänd/ Järnvägsmuseet. Ingår i samling: Järnvägsmuseets foton. DigitaltMuseum ID: 021018076293.

Licens: Erkännande-DelaLika (CC BY-SA):
https://creativecommons.org/licenses/by-sa/4.0/legalcode.sv

Figur 5.1, s. 79. IBM-maskinerna anländer till Skogsbrukets datacentrals nybyggda lokaler på Södra Allén, Sundsvall. Fotograf: Norrlandsbild/Ragge Ellefsson. Ingår i samling: Sundsvalls museum.

Figur 5.2, s. 81. Skeppsbron 2. Kabelintag till överkopplingen. Telefonstationen Skeppsbron 2 "Centralen" var i drift till år 1929, då den automatiserades och flyttades till Jakobsbergsgatan 24. Fotograf: okänd. Ingår i samling: Tekniska museets arkiv. DigitaltMuseum ID: 021018294215.

Figur 5.3, s. 85. Datasal. Fotograf: okänd/ Järnvägsmuseet. Fotografering 1975 - 1985 (1985). Ingår i samlingen Järnvägsmuseets foton. DigitaltMuseum ID: 021018188334.

Figur 5.4, s. 89. Stenografi 14 januari 1967. Fotograf: Örebrokuriren/Örebro läns museum. Ingår i samling: Örebro kuriren, Örebro läns museum. DigitaltMuseum ID: 021016194193

Litteratur

Ajder, Henry, Giorgio Patrini, Francesco Cavalli & Laurence Cullen (2019, september), *The State of Deepfakes: Landscape, Threats, and Impact*, Deeptrace, https://deeptracelabs.com/mapping-the-deepfake-landscape/, hämtad 2019-12-05.

Ahuja, M. K. (2002), "Women in the Information Technology profession: A Literature Review, Synthesis and Research Agenda", *European Journal of Information Systems*, 11(1), 20-34, https://doi.org/10.1057/palgrave.ejis.3000417.

Andersson, Caroline, Göran Lindsjö & Rebecca Hagberg (2018), *Artificiell intelligens i offentlig sektor: Hur realiserar vi potentialen?*, Governo, https://governo.se/case/vinnova/, hämtad 2019-12-05.

Andersson, Christer, Tove Gustavi och Maja Karasalo (2019), "Artificiell intelligens – möjligheter och utmaningar för Sveriges nationella säkerhet" i

Niklas H. Rossbach, Josefin Öhrn-Lundin, Daniel K. Jonsson, Anna Sundberg, Sofia Olsson, Jakob Gustafsson och Camilla Trané (red.), *Strategisk utblick 8: Totalförsvarets tillväxt – utmaningar och möjligheter*, FOI-R--4773--SE, Stockholm: Totalförsvarets forskningsinstitut, s. 75-81.

Annergård. Malin (2019), *Invånarnas inställning till digital service i välfärden*, Sveriges Kommuner och Regioner, https://skr.se/naringslivarbetedigitalisering/digitalisering/sammanhallendigitalservice/invanarnasinstallningdigitalservice.16155.html, hämtad 2019-11-03.

Barck-Holst, Svante (2005), *Nationellt säkerhetsarbete inom samhällsviktig infrastruktur*, FOI-R--1553--SE, Stockholm: Totalförsvarets forskningsinstitut.

Berman, Marshall (2001 [1982]), *Allt som är fast förflyktigas: modernism och modernitet*, Lund: Arkiv.

Boman, Magnus (2019) ”Vad är AI?” i Eva Regårdh & Sofie Pehrsson (red.), *Livet med AI*, Stockholm: Stiftelsen för strategisk forskning.

Bornemark, Jonna (2018). *Det omätbaras renässans – en uppgörelse med pedanternas världsherravälde*, Stockholm: Volante.

Bornemark, Jonna (2019), ”Högtidstal”, framfört vid riksmötets öppnande den 10 september 2019, https://www.svenskakyrkan.se/stockholmsdomkyrkoforsamling/gudstjanst-i-samband-med-riksmotets-oppnande_20190910, hämtad 2019-12-05.

Bostrom, Nick (2014), *Superintelligence: Paths, Dangers, Strategies*, Oxford: Oxford University Press.

Bredbandsforum, 2019. *Infrastruktur för digitalisering*. Dnr 19-7842, hämtad 2019-12-16 från https://bredbandsforum.se/media/1252/2019-infrastruktur-foer-digitalisering-slutrapport.pdf.

Broad, Ellen (2018), *Made by Humans: The AI Condition*, Melbourne: Melbourne University Press.

Brundage, Miles, Shahar Avin, Jack Clark, Helen Toner m.fl. (2018), *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, Future of Humanity Institute m.fl., https://maliciousaireport.com/, hämtad 2019-12-05.

Cave, Stephen (2019), “To save us from a Kafkaesque future, we must democratise AI”, *The Guardian*, debattartikel, 4 januari 2019. Hämtad 2019-12-03 från https://amp.theguardian.com/commentisfree/2019/jan/04/future-democratise-ai-artificial-intelligence-power.

Chesney, Bobby & Danielle Citron (2018), ”Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security”, California Law Review, under utgivning, https://dx.doi.org/10.2139/ssrn.3213954.

Christl, Wolfie (2017), “Corporate Surveillance in Everyday Life – How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions”, Cracked Labs, https://crackedlabs.org/en/corporate-surveillance, hämtad 2019-08-22.

Cussins Newman, Jessica (2019), *Towards AI Security: Global Aspirations for A More Resilient Future*, UC Berkeley, Center for Long-Term Cybersecurity, https://cltc.berkeley.edu/towardaisecurity/, hämtad 2019-12-05.

Danielsson, Ola (2017, februari), ”Smart, smartare, doktor AI”, *Medicinsk Vetenskap*, nr 1, s. 24–28, https://nyheter.ki.se/arkiv-tidskriften-medicinsk-vetenskap, hämtad 2019-12-05. Texten har även publicerats på https://ki.se/forskning/nyfiken-pa-artificiell-intelligens-sa-kan-ai-losa-vara-halsoproblem.

Denward, Carl, Per Larsson & Ann-Sofie Stenérus Dover (2017), *Sektorsansvar: Ansvarssystem eller semantik?*, FOI-R--4542--SE, Stockholm: Totalförsvarets forskningsinstitut.

Digital21 (2018), *Digitale grep for norsk verdiskaping*, Digital21, https://digital21.no/, hämtad 2019-12-05.

Digitaliseringsrådet (2018a), *En lägesbild av digital trygghet*, Dnr: 18-3238, Stockholm: Digitaliseringsrådet, https://digitaliseringsradet.se/sveriges-digitalisering/digital-trygghet/, hämtad 2019-12-05.

Digitaliseringsrådet (2018b), *En lägesbild av digital kompetens*, Dnr: 18-5698, Stockholm: Digitaliseringsrådet, https://digitaliseringsradet.se/sveriges-digitalisering/digital-kompetens/, hämtad 2019-12-05.

Digitaliseringsrådet (2019a), *Data som strategisk resurs*, Dnr: 19-3731, Stockholm: Digitaliseringsrådet, https://digitaliseringsradet.se/aktuellt/foerdjupningsomraaden-2019/data-som-strategisk-resurs/, hämtad 2019-12-05.

Digitaliseringsrådet (2019b), *En lägesbild av digital ledning*, Dnr: 19-5942, Stockholm: Digitaliseringsrådet, https://digitaliseringsradet.se/sveriges-digitalisering/digital-ledning/, hämtad 2019-12-05.

Eidenskog, Daniel, Caroline Bildsten & Bodo Endres (2019), *Säkra cyberleveranskedjor*, FOI-R--4851--SE, Stockholm: Totalförsvarets forskningsinstitut.

Ekholm, Anders, Karim Jebari och Drasko Markovic (red.) (2018), *Förbjuden framtid? Den digitala kommunen*, Institutet för Framtidsstudier, https://www.iffs.se/publikationer/ovrigt/forbjuden-framtid/, hämtad 2019-12-05.

ESV 2018:31, *Digitalisering av det offentliga Sverige – En uppföljning*, Ekonomistyrningsverket, 15 mars 2018, https://www.esv.se/publicerat/publikationer/2018/digitaliseringen-av-det-offentliga-sverige--en-uppfoljning/, hämtad 2019-12-05.

Favaretto, Maddalena, Eva De Clercq, & Bernice Simone Elger (2019), ”Big Data and discrimination: perils, promises and solutions. A systematic review”, *Journal of Big Data*, 6(1). https://doi.org/10.1186/s40537-019-0177-4.

Felt, Ulrike, Rayvon Fouché, Clark Miller & Laurel Smith-Doerr (red.) (2017), *The Handbook of Science and Technology Studies* [Fourth Edition], Cambridge, MA: The MIT Press.

Fichtelius, Erik, Christina Persson & Eva Enarson (2019), *Demokratins skattkammare: Förslag till en nationell bibliotheksstrategi*, Dnr: 6.7-2015-1181, Kungliga biblioteket, http://libris.kb.se/bib/8j4tcb5g69kl2544, hämtad 2019-12-05.

Forssell, Anders & Anders Ivarsson Westerberg (2016), ”Granskningens (glömda) kostnader”, *Statsvetenskaplig tidskrift*, nr 1, https://journals.lub.lu.se/st/article/view/15954, hämtad 2019-12-05.

Försvarsberedningen (2017), *Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021-2025*, Ds 2017:66, Försvarsdepartementet, Regeringskansliet.

Försvarsberedningen (2019), *Värnkraft. Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021-2025*, Ds 2019:8, Försvarsdepartementet, Regeringskansliet.

Geist, Edward och Andrew J. Lohn, (2018), *How Might Artificial Intelligence Affect the Risk of Nuclear War?*, Rand Corporation, https://www.rand.org/pubs/perspectives/PE296.html, hämtad 2019-12-05.

Gent, Edd (2016), “Big Data’s Dark Side”. *Engineering & Technology*, 11(9), 32–35. https://doi.org/10.1049/et.2016.0901.

Greenberg, Andy (2018), “The Untold Story of NotPetya, the Most Devastating Cyberattack in History”, *Wired*, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, hämtad 2019-12-05.

Goldkuhl, Göran (2019), ”Förändring och digitalisering – Varför är det så svårt?”, filmad presentation, Linköpings universitet,

https://liu.se/artikel/strimman---inspelade-forelasningar, hämtad 2019-12-05.

Gustavi, Tove, J. Karlholm, D. Oskarsson, T. Beran m.fl. (2019), *Försvarsnära tillämpningar av artificiell intelligens*, Stockholm: Totalförsvarets forskningsinstitut, FOI-R--4707--SE.

Hagström, Martin (2016), *Autonom våldsutövning – hot eller möjligheter*, FOI MEMO 5676, Stockholm: Totalförsvarets forskningsinstitut.

Halford, Susan & Savage, Mike (2010), "Reconceptualizing digital social inequality", *Information, Communication & Society*, 13(7), 937-955, https://doi.org/10.1080/1369118X.2010.499956.

Hall, Patrik (2007), "Byråkratisering som konsekvens av företagisering inom offentlig förvaltning?", *Statsvetenskaplig tidskrift*, 109(2).

Hill, Catherine, Christianne Corbett & Andresse St. Rose (2010), "Why So Few? Women in Science, Technology, Engineering, and Mathematics (STEM)", AAUW research report. Hämtad 2019-12-16 från https://www.aauw.org/research/why-so-few/.

Hirdman, Yvonne, Urban Lundberg & Jenny Björkman (red.) (2012), *Sveriges historia 1920-1965*, Stockholm: Norstedts, 2012.

Holm, Hannes (2017), *Internetanslutna styrsystem i Sverige – En studie av Censys och Shodan*, FOI-R--4415--SE, Stockholm: Totalförsvarets forskningsinstitut.

Häggström, Olle (2019), "Vår framtid med artificiell intelligens innebär stora möjligheter och stora risker", *Fysikaktuellt* nr 1, feb. 2019, s. 14-19.

Infrastruktur för digitalisering (2019), *Analys av aktörskedjor för beskrivning av roller och ansvar*, Bredbandsforum, https://bredbandsforum.se/media/1253/infrastruktur-foer-digitalisering-arbetsgrupp-18.zip, hämtad 2019-12-05.

Ingemarsdotter, Jenny (2019), *The Masculine Modern Woman: Pushing Boundaries in the Swedish Popular Media of the 1920s*, New York: Routledge, s. 141-188.

IVA (2019), *Digitalisering för ökad konkurrenskraft*, IVA-M 499, Kungl. Ingenjörsvetenskapsakademien, https://www.iva.se/globalassets/projekt/201902-iva-digitalisering-slutrapport-l.pdf, hämtad 2019-12-05.

Jasanoff, Sheila (2016), *The Ethics of Invention: Technology and the Human Future*, New York: W.W. Norton & Company

Jing, Qi, Anthanasios V. Vasilakos, Jiafu Wan, Jingwei Lu & Dechao Qui (2014), ”Security of the Internet of Things: perspectives and challenges”, *Wireless Netw*., 20(8), 2481-2501, https://doi.org/10.1007/s11276-014-0761-7.

Jonsson, Daniel K., Jenny Ingemarsdotter, Bengt Johansson, Niklas H. Rossbach, Christoffer Wedebrand, Camilla Eriksson, *Civilt försvar i gråzon*, FOI-R--4769--SE, Stockholm: Totalförsvarets forskningsinstitut.

Kahneman, Daniel (2013), *Tänka, snabbt och långsamt* [översättning: Pär Svensson], Stockholm: Månpocket.

Kamrani, Farzad, Mikael Wedlin & Ioana Rodhe (2016), *Internet of Things: Security and Privacy Issues*, FOI-R--4362--SE, Stockholm: Totalförsvarets forskningsinstitut.

Kosinski, Michael, David Stillwell & Thore Graepel (2013), ”Private traits and attributes are predictable from digital records of human behavior”, *Proceedings of the National Academy of Sciences of the United States of America (PNAS), 110*(15), 5805–5805, https://doi.org/10.1073/pnas.1218772110.

Lindgren, Ida, Christian Østergaard Madsen, Sara Hofmann & Ulf Melin (2019), ”Close encounters of the digital kind: A research agenda for the digitalization of public services”, *Government Information Quarterly*, 36(3), 427–436, https://doi.org/10.1016/j.giq.2019.03.002.

Lundin, Per (2014), *Bilsamhället: Ideologi, expertis, och regelskapande i efterkrigstidens Sverige*, Stockholm: Stockholmia förlag.

Lupton, Deborah (2016), ”Digital Risk Society” i Adam Burgess, Alberto Alemanno och Jens Zinn (red.), *The Routledge Handbook of Risk Studies*, London: Routledge.

Löfgren, Orvar (2000), “Kulturella kompressioner: till hastighetens etnologi” i Gösta Arvastson, Birgitta Meurling & Per Peterson (red.), *Etnologin inför 2000-talet*, Uppsala: Gustav Adolfs akad.

Mackenzie, Adrian & Theo Vurdubakis (2011), “Codes and Codings in Crisis: Signification, Performativity and Excess”, *Theory, Culture & Society*, 28(6), https://doi.org/10.1177%2F0263276411424761.

McGregor, Lorna, Daragh Murray & Vivian Ng (2019), ”International Human Rights Law as a framework for algorithmic accountability”, *International & Comparative Law Quarterly*, 68(2), 309–343, https://doi.org/10.1017/S0020589319000046.

Modlitba, Paulina (2018), ”Fyra förändrande drivkrafter för AI i vården” i Eva Regårdh och Sofie Pehrsson (red.), *Livet med AI*, Stockholm: Stiftelsen för strategisk forskning, s. 17-21.

Moore, Gordon. E. (1965), ”Cramming more components onto integrated circuits”, *Electronics*, 38(8), återutgiven i *IEEE Solid-State Circuits Society Newsletter*, 11(3), https://doi.org/10.1109/N-SSC.2006.4785860.

Mosenia, Arsalan, Xiaoliang Dai, Prateek Mittal och Niraj K. Jha (2018), ”PinMe: Tracking a Smartphone User around the World”, *IEEE Transactions on Multi-Scale Computing Systems*, 4(3), 420–435, https://doi.org/10.1109/TMSCS.2017.2751462.

MSB (2009), *Faller en – faller då alla? En slutredovisning från KBM:s arbete med samhällskritiska beroenden*, Myndigheten för samhällsskydd och beredskap, https://www.msb.se/siteassets/dokument/amnesomraden/krisberedskap-och-civilt-forsvar/stod-i-att-analysera-beroenden/faller-en---faller-da-alla.pdf, hämtad 2019-12-05.

MSB (2012), *Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter*, MSB367-12, Myndigheten för samhällsskydd och beredskap, https://www.msb.se/sv/publikationer/reflektioner-kring-samhallets-skydd-och-beredskap-vid-allvarliga-it-incidenter--en-studie-av-konsekvenserna-i-samhallet-efter-driftstorningen-hos-tieto-i-november-2011/, hämtad 2019-12-05.

MSB (2014), *Vägledning till ökad säkerhet i industriella informations- och styrsystem*, MSB718, Myndigheten för samhällsskydd och beredskap, https://www.msb.se/sv/publikationer/vagledning-till-okad-sakerhet-i-industriella-informations-och-styrsystem/, hämtad 2019-12-05.

MSB (2015), *Informationssäkerhet – trender 2015*, MSB 779, Myndigheten för samhällsskydd och beredskap, https://www.msb.se/sv/publikationer/informationssakerhet--trender-2015/, hämtad 2019-12-05.

MSB (2018a), *Framtida utveckling som kan påverka arbetet med samhällsskydd och beredskap – en uppdatering*, MSB1245, Myndigheten för samhällsskydd och beredskap, https://www.msb.se/sv/publikationer/framtida-utveckling-som-kan-paverka-arbetet-med-samhallsskydd-och-beredskap--en-uppdatering-studie/, hämtad 2019-12-05.

MSB (2018b), *IoT-relaterade risker: Begrepp och kategorisering*, MSB1248, Myndigheten för samhällsskydd och beredskap, https://www.msb.se/sv/publikationer/iot-relaterade-risker--begrepp-och-kategorisering/, hämtad 2019-12-05.

MSB (2019), *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022*, MSB1351, Myndigheten för samhällsskydd och beredskap, https://rib.msb.se/filer/pdf/28804.pdf, hämtad 2019-12-05.

Naydenov, Rossen, Dimitra Liveri, Lionel Dupre, Eftychia Chalvatzi & Christina Skouloudi (2015, december), *Big Data Security: Good Practices and Recommendations on the Security of Big Data Systems*, Enisa, http://doi.org/10.2824/13094.

Nilsson, Nils J. (2010), *The Quest for Artificial Intelligence: A History of Ideas and Achievements*, Cambridge University Press.

Nilsson, Mattias, Linus J. Luotsinen, Johan Schubert & Peter Svenmarck (2017), *Djupa neuronnät: sårbarheter och vilseledning*, FOI MEMO 6252, Stockholm: Totalförsvarets forskningsinstitut.

O'Neil, Cathy (2017), *Weapons of Math Destruction*, New York: Broadway Books.

OECD (2018), *Reviews of Digital Transformation: Going Digital in Sweden*, hämtad från https://www.oecd.org/sweden/going-digital-in-sweden.pdf.

OWASP (2018), *Automated Threat Handbook Web Applications*, hämtad från https://www.owasp.org/images/3/33/Automated-threat-handbook.pdf.

Polák, Petr (2017), "The productivity paradox: A metaanalysis", *Information Economics and Policy*, 38, 38-54, https://doi.org/10.1016/j.infoecopol.2016.11.003.

Prins, J.E.J., Dennis Broeders & H.M. Griffioen (2012), "iGovernment: A new perspective on the future of government", *Computer Law & Security Review*, 28(3), 273–282, https://doi.org/10.1016/j.clsr.2012.03.010.

PTSFS 2015:2, *Post- och telestyrelsens föreskrifter om krav på driftsäkerhet*, Stockholm: Post- och telestyrelsen.

Qvarsell, Roger, "Hot eller möjlighet? om maskinen som människans problemtyngda följeslagare" i Lotten Wiklund & Magdalena Tafvelin Heldner, *Du sköna nya människa*, Daedalus årsbok 2015, Stockholm: Tekniska Museet, s. 144–163.

Ransbotham, Sam, Robert G. Fichman, Ram Gopal & Alok Gupta (2016), "Ubiquitous IT and Digital Vulnerabilities", *Information Systems Research*, 27(4), https://doi.org/10.1287/isre.2016.0683.

Regårdh, Eva & Sofie Pehrsson (red.), *Livet med AI*, Stockholm: Stiftelsen för strategisk forskning, https://strategiska.se/med-ai-kommer-manga-jobb-forsvinna-men-inte-mitt/livet-med-ai-novus/, hämtad 2019-12-05.

Rakar, Fredrik (2018), *Lärprojekt Trelleborgsmodellen – Från rebell till modell*, Rhetikfabriken, https://moten.trelleborg.se/welcome-sv/namnder-styrelser/arbetsmarknadsnamnden/arbetsmarknadsnamnden-2018-06-11/agenda/larprojekt-trelleborgsmodellen-002pdf, hämtad 2019-12-05.

Ranerup, Agneta & Helle Zinner Henriksen (2019), ”Value positions viewed through the lens of automated decision-making: The case of social services”, *Government Information Quarterly*. 36(4), https://doi.org/10.1016/j.giq.2019.05.004.

Regeringskansliet (2016), *Nationell strategi för samhällets informations- och cybersäkerhet*, Skr. 2016/17:213, Justitiedepartementet, https://www.regeringen.se/rapporter/2018/07/skr.-201617213-bilaga-uppdatering-om-genomforandet/, hämtad 2019-12-05.

Regeringskansliet (2017a), *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi*, Dnr: N2017/03643/D, Näringsdepartementet, https://www.regeringen.se/informationsmaterial/2017/05/for-ett-hallbart-digitaliserat-sverige---en-digitaliseringsstrategi/, hämtad 2019-12-05.

Regeringskansliet (2017b), *Hur Sverige blir bäst i världen på att använda digitaliseringens möjligheter – en skrivelse om politikens inriktning*, Skr. 2017/18:47, https://www.regeringen.se/rattsliga-dokument/skrivelse/2017/11/skr.-20171847/, hämtad 2019-12-05.

Regeringskansliet (2017c), *Nationell säkerhetsstrategi*, Statsrådsberedningen, https://www.regeringen.se/informationsmaterial/2017/01/nationell-sakerhetsstrategi/, hämtad 2019-12-05.

Regeringskansliet (2018a), *Nationell inriktning för artificiell intelligens*, Artikelnr. N2018.14, Näringsdepartementet, https://www.regeringen.se/informationsmaterial/2018/05/nationell-inriktning-for-artificiell-intelligens/, hämtad 2019-12-05.

Regeringskansliet (2018b), *Granskning av Transportstyrelsens upphandling av it-drift*, Ds 2018:6, Näringsdepartementet, https://www.riksdagen.se/sv/dokument-lagar/dokument/departementsserien/granskning-av-transportstyrelsens-upphandling-av_H6B46, hämtad 2019-12-05.

Regeringskansliet och SKL (2016), *Vision e-hälsa 2025 – gemensamma utgångspunkter för digitalisering i socialtjänst och hälso- och sjukvård*, S2016/01874/FS, Socialdepartementet.

Renda, Andrea (2019), *Artificial Intelligence – Ethics, governance and policy challenges: Report of a CEPS Task Force*, Brussels: Centre for European Policy Studies, https://www.ceps.eu/ceps-publications/artificial-

intelligence-ethics-governance-and-policy-challenges/, hämtad 2019-12-05.

RIR 2019:14, ”Enklare att starta företag – statliga insatser för en digital process”, Riksrevisionen, 14 maj 2019, hämtad 2019-12-04 från https://www.riksrevisionen.se/rapporter/granskningsrapporter/2019/enklare-att-starta-foretag---statliga-insatser-for-en-digital-process.html.

Royal Society (2017), *Machine learning: the power and promise of computers that learn by example*, London: The Royal Society, https://royalsociety.org/topics-policy/projects/machine-learning/, hämtad 2019-12-05.

Royal Society (2018), *Portrayals and perceptions of AI and why they matter*, London: The Royal Society, https://royalsociety.org/topics-policy/projects/ai-narratives/, hämtad 2019-12-05.

Ruin, Hans (2018), ”Den envisa myten om intelligenta maskiner”, *Svenska dagbladet*, 28 december 2018, https://www.svd.se/ai-inget-att-oroa-sig-for--men-overtron-pa-teknik-ar-det, hämtad 2018-12-05.

Runeby, Nils (red.) (1998), *Framstegets arvtagare*, Europas idéhistoria del 5, Stockholm: Natur och Kultur.

Russell, Stuart J. and Peter Norvig (1995), *Artificial Intelligence: A Modern Approach*, Engelwood Cliffs, NJ: Prentice-Hall, Inc.

Ryan, Kenneth John, Joseph V. Brady, Robert E. Cooke, Dorothy I. Height m.fl. (1979). *The Belmont Report*, https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html, hämtad 2019-12-05.

Scharre, Paul (2018), *Army of None: Autonomous Weapons and the Future of War*, New York: W. W. Norton & Company.

Schneier, B. (2017), “Click Here to Kill Everyone”, *New York Magazine Intelligencer*, http://nymag.com/intelligencer/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html, hämtad 2019-10-21. Artikeln finns även tillgänglig på https://www.schneier.com/essays/archives/2017/01/click_here_to_kill_e.html.

Schwab, Klaus (2016), *The Fourth Industrial Revolution*, Geneva: World Economic Forum.

Schön, Lennart (2017), *Sweden’s Road to Modernity*, Lund: Studentlitteratur.

Siösteen, Bengt (1969), *Vårt ekonomiska försvar i blickpunkten*, Stockholm: Överstyrelsen för ekonomiskt försvar.

SKL (2017), *Artificiell intelligens: Möjligheter för välfärden*, Sveriges kommuner och landsting, https://skl.se/download/18.1284479015a26d3e16d5373/1486739509125/Artificiell+intelligens.pdf, hämtad 2019-12-05.

SKL (2018a), *Automatisering av arbete: Möjligheter och utmaningar för kommuner, landsting och regioner*, Sveriges kommuner och landsting, https://webbutik.skl.se/bilder/artiklar/pdf/5408.pdf, hämtad 2019-12-05.

SKL (2018b), *Automatiserad ärendehantering: Att frigöra tid för värdeskapande arbete*, Sveriges kommuner och landsting, https://webbutik.skl.se/bilder/artiklar/pdf/5409.pdf, 2019-12-05.

SKL (2019), *Ekonomirapporten, oktober 2019 – Om kommunernas och regionernas ekonomi*, Sveriges kommuner och landsting, https://webbutik.skl.se/bilder/artiklar/pdf/7585-549-3.pdf, hämtad 2019-12-05.

Skovdahl, Bernt (1998), ”Framstegskapplöpningen” i Nils Runeby (red.), *Framstegets arvtagare*, Stockholm: Natur och kultur, s. 145-165.

Snickars, Pelle (2014), *Digitalism: när allting är internet*, Stockholm: Volante.

SOU 1962: 32, *Automatiskt databehandling: Betänkande avgivet av kommittén för maskinell databehandling* .

SOU 1979: 93, *ADB och samhällets sårbarhet: Överväganden och förslag.*

SOU 1986: 12, *Datorer, sårbarhet, säkerhet: En slutrapport från SÅRB*

SOU 1999:134, *Framtidssäker IT-infrastruktur för Sverige.*

SOU 2013:31, *En digital agenda i människans tjänst – Sveriges digitala ekosystem, dess aktörer och drivkrafter*.

SOU 2014:13, *En digital agenda i människans tjänst – en ljusnande framtid kan bli vår*.

SOU 2015:23, *Informations- och cybersäkerhet i Sverige strategi och åtgärder för säker information i staten betänkande*.

SOU 2015:91, *Digitaliseringens transformerande kraft – vägval för framtiden*.

SOU 2015:28, *Gör Sverige i framtiden - digital kompetens*.

SOU 2015:65, *Om Sverige i framtiden – en antologi om digitaliseringens möjligheter*

SOU 2016:85, *Digitaliseringens effekter på individ och samhälle – fyra temarapporter*.

SOU 2016:89, *För digitalisering i tiden*.

SOU 2017:39, *Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning.*

SOU 2017:114, *Reboot – omstart för den digitala förvaltningen*.

SOU 2018:25, *Juridik som stöd för förvaltningens digitalisering*.

SOU 2019:59, *Samlade åtgärder för korrekta utbetalningar från välfärdssystemen*.

Speilkramp, Mathias (red.) (2019), *Automating Society: Taking Stock of Automated Decision-Making in EU*, AlgorithmWatch, https://algorithmwatch.org/wp-content/uploads/2019/01/Automating_Society_Report_2019.pdf, hämtad 2019-12-05.

Stafford, Christian (2016, 15 december), *IoT security issues and vulnerabilities*, webcast, TechTarget, https://searchcompliance.techtarget.com/video/IoT-security-issues-and-vulnerabilities, hämtad 2019-10-21.

Stenérus-Dover, Ann-Sofie, Johan Bengtsson och Matilda Olsson (under utgivning), *IT-incidenter på statliga myndigheter: Orsaker till utebliven rapportering och polisanmälan*, Stockholm: Totalförsvarets forskningsinstitut.

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams och Adam Hahn (2015), *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82, revision 2, National Institute of Standards and Technology, http://dx.doi.org/10.6028/NIST.SP.800-82r2.

Summerton, Jane (1998), ”Stora tekniska system: En introduktion till forskningsfältet” i Pär Blomqvist & Arne Kaijser (red.), *Den konstruerade världen: Tekniska system i historiskt perspektiv*, Stockholm: Brutus Östlings Bokförlag Symposion.

Susskind, Jamie (2018), *Future Politics: Living Together in a World Transformed by Tech*, Oxford: Oxford University Press.

Sveriges Riksbank, 2018. *Riksbankens e-kronaprojekt*, Rapport 2, hämtad 2019-12-16 från https://www.riksbank.se/sv/betalningar--kontanter/e-krona/e-kronarapporter/e-kronaprojekt-rapport-2/.

Sveriges Riksbank, 2019. *Så betalar svenskarna 2019*, hämtad 2019-12-02 från https://www.riksbank.se/globalassets/media/rapporter/sa-betalar-svenskarna/2019/svenska/sa-betalar-svenskarna-2019.pdf.

Swaling, Vidar Hedtjärn (2015), *Beroende av korrekt tid i elsystem*, FOI Memo 5069, Stockholm: Totalförsvarets forskningsinstitut.

Swaling, Vidar Hedtjärn & Jessica Johansson (2018), *NCS3 Studie – IoT-relaterade risker och strategier* , FOI-R--4591--SE, MSB 2017-1554, Stockholm: Totalförsvarets forskningsinstitut.

Swaling, Vidar Hedtjärn & Karin Mossberg Sonnek (2016), *NCS3 – Beroenden till industriella informations- och styrsystem*, FOI-R--4280--SE, MSB 2015-1075, Stockholm: Totalförsvarets forskningsinstitut.

Swaling, Vidar Hedtjärn, Fredrik Malmberg Andersson & Jonas Clausen Mork (2016), *NCS3 – Gammalt är inte äldst*, FOI-R--4292--SE, MSB 2015--6559, Stockholm: Totalförsvarets forskningsinstitut.

Swaling, Vidar Hedtjärn & Fredrik Malmberg Andersson (2018), *NCS3 Förstudie – Bortom sakernas internet*, FOI-R--4643--SE, MSB 2016-3606, Stockholm: Totalförsvarets forskningsinstitut.

Swaling, Vidar Hedtjärn, Kia Wiklundh & Karina Fors (2017), *Civila aktörers förmåga att stödja Försvarsmakten - Elektroniska kommunikationer*, FOI Memo 6146, Stockholm: Totalförsvarets forskningsinstitut.

Tegmark, Max (2017), *Life 3.0: Being Human in the Age of Artificial Intelligence*, New York: Alfred A. Knopf.

Valassi, Christian & Martin Karresand (2019), *Komponenter på avstånd*, FOI-R--4757--SE, Stockholm: Totalförsvarets forskningsinstitut.

Vedder, Anton & Laurens Naudts (2017), ”Accountability for the use of algorithms in a big data environment”, *International Review of Law, Computers & Technology*, 31(2), 206–224. https://doi.org/10.1080/13600869.2017.1298547.

Verizon (2018), “2018 Data Breach Investigations Report, 11th edition”. Hämtad 2019-12-04 från https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf.

Vetenskapsrådet (2018), *Att motverka överbelastning av samhällsviktiga webbplatser: Slutrapport 2018 från projekt Särimner*, Stockholm: Vetenskapsrådet, https://www.pts.se/sv/dokument/rapporter/internet/2018/rapport-sarimner-2018/, hämtad 2019-12-05.

Vinnova (2018), *Artificiell intelligens i svenskt näringsliv och samhälle: Analys av utveckling och potential*, Vinnova rapport 2018:08, https://www.vinnova.se/publikationer/artificiell-intelligens-i-svenskt-naringsliv-och-samhalle/, hämtad 2019-12-05.

Wajcman, Judy (2007), “From Women And Technology To Gendered Technoscience”, *Information, Community and Society*, 10:3, 287-298, https://doi.org/10.1080/13691180701409770.

Wahlgren, Peter (2018), ”Reglering av Artificiell Intelligens” i Eva Regårdh & Sofie Pehrsson (red.), ”*Livet med AI”,* Stockholm: Stiftelsen för strategisk forskning, s. 52-57.

World Economic Forum (2019). *The Global Risks Report 2019, 14th Edition*, Geneve: World Economic Forum, https://www.weforum.org/reports/the-global-risks-report-2019, hämtad 2019-12-05.

Wormbs, Nina (2010), ”Det digitala imperativet” i Jonas Andersson & Pelle Snickars (red.), *Efter The Pirate Bay*, Stockholm: Kungliga Biblioteket, s. 140-150.

Wormbs, Nina (2018), ”Om ny teknik för framtiden” i Eva Regårdh & Sofie Pehrsson (red.), *Livet med AI*, Stockholm: Stiftelsen för strategisk forskning, s. 58-63.

Wyatt, Sally (2008), “Feminism, Technology and The Information Society: Learning from the Past, Imagining the Future”, *Information, Community & Society*, 11:1, 111-130, https://doi.org/10.1080/13691180701859065.

Yudkowsky, Eliezer (2008), *Artificial Intelligence as a Positive and Negative Factor in Global Risk*, Machine Intelligence Research Institute, http://intelligence.org/files/AIPosNegFactor.pdf, hämtad 2019-12-05.

FOI

ISSN 1650-1942

www.foi.se