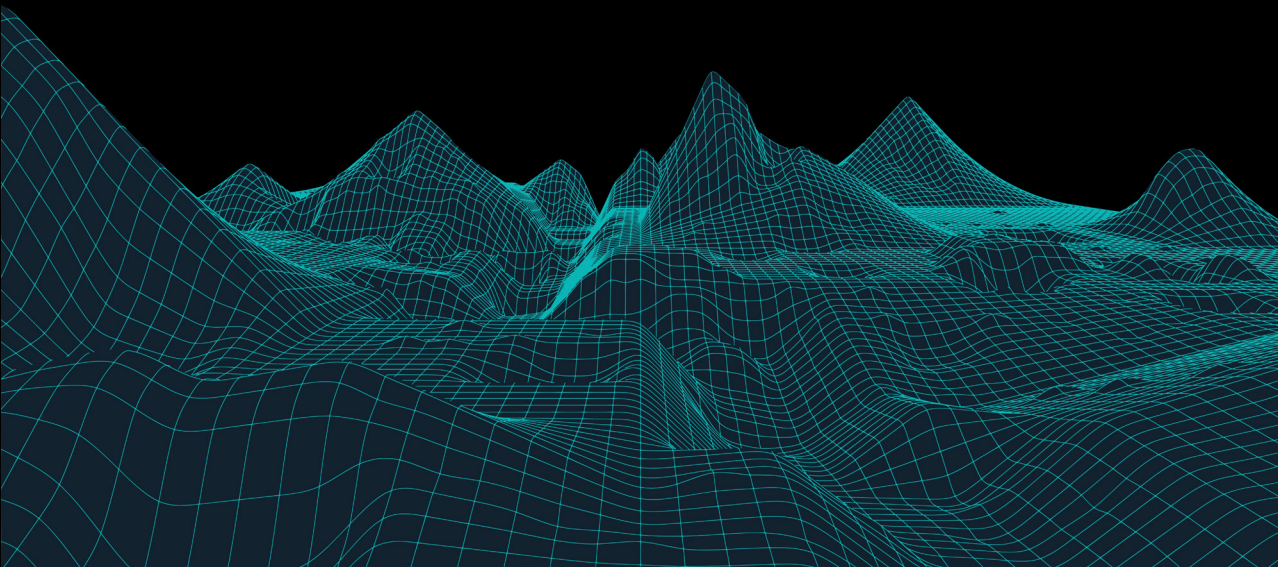




Den nya informationsmiljöns topografi

Teknik, människa och strategi i osäkerhetens tidevarv

Per-Erik Nilsson, Sofia Olsson och Ivar Ekman

Per-Erik Nilsson, Sofia Olsson och Ivar Ekman

Den nya informationsmiljöns topografi

Teknik, människa och strategi i osäkerhetens tidevarv

Titel	Den nya informationsmiljöns topografi – Teknik, människa och strategi i osäkerhetens tidevarv
Title	The Topography of the New Information Environment – Technology, Humans, and Strategies in Unruly Times
Rapportnr	FOI-R--5342--SE
Månad	December
Utgivningsår	2022
Antal sidor	124
ISSN	1650-1942
Uppdragsgivare	Försvarsmakten
Forskningsområde	Operationsanalys och strategisk planering
FoT-område	Inget FoT-område
Projektnr	GEM222301S
Godkänd av	Johannes Malminen
Ansvarig avdelning	Försvarsanalys

Bild: Shutterstock (Stock Illustration-ID: 1374680897), Anton Dzyna

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bland annat innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Föreliggande rapport beskriver utvecklingen av den digitala informationsmiljön i relation till militärstrategisk kommunikation. Rapporten är disponerad kring tre teman: a) informationstekniska förutsättningar för att kommunicera i informationsmiljön; b) människan som målgrupp för kommunikation i informationsmiljön; och c) hur militära aktörer har arbetat och arbetar för att kommunicera strategiskt i informationsmiljön.

Det övergripande syftet med rapporten är att ge Försvarsmakten underlag för att utveckla en ökad förmåga i informationsmiljön, vilket inbegriper underlag för vidare kunskapsutveckling inom såväl Försvarsmaktens som akademins ramar.

Det specifika syftet med rapporten är att beskriva några av de mest grundläggande aspekterna av informationsmiljön för att utveckla strategisk kommunikation med fokus på skydd och verkan i informationsmiljön, samt att identifiera vad som åsyftas med begreppet i sig och hur andra statliga aktörer har tagit sig an denna problematik.

Rapportens huvudsakliga slutsatser beträffande utvecklad förmåga för skydd och verkan i informationsmiljön är:

- Militär förmåga i informationsmiljön är en mycket komplex utmaning, särskilt för demokratiska rättsstater där förtroende för myndigheter och stater är avgörande.
- För ökad förmåga avseende skydd och verkan i informationsmiljön krävs en god kunskap om tekniska, mänskliga, politiska och juridiska förutsättningar för att verka i den.
- Arbetet med att utveckla förmåga för skydd och verkan i informationsmiljön bör struktureras med hänsyn till ovanstående punkter – vad gäller såväl ledning som sakkunskap och tillsyn. I en mening handlar det om att skynda långsamt, bland annat genom att utgå från den kunskap och förmåga som redan finns, såväl generellt som inom den aktuella organisationen, att lära sig från andra länders erfarenheter och sträva efter öppenhet i kommunikationen kring arbetet med att utveckla förmåga i informationsmiljön.

Nyckelord: Strategisk kommunikation, informationsmiljö, informationsteknik, kognition, desinformation, vilseledning och propaganda.

Summary

This report is a narrative description of the emergence and development of the digital information environment. The report is structured around three themes: a) the information technological preconditions related to communication; b) the human being as a target audience for communication; and c) how military actors work with strategic communication.

The purpose of the report is to provide the Swedish Armed Forces with a conceptual framework to further develop their communicative capabilities in the information environment.

The specific aim of the report is to conceptualize the information environment, describe some of the fundamental pillars for operating in the information environment, and discuss how other actors have approached these challenges.

The central conclusions from the report are:

- The development of military capabilities adapted to the digital information environment is highly complex, especially for liberal democratic and rights-based states to whom trust in the democratic institutions is imperative.
- The development of appropriate and effective capabilities necessitates an empirically grounded and continuously developing knowledge about the overlapping technical, human, strategic, and legal conditions of the information environment.
- The continued development of capabilities should be based on expertise, oversight, and transparency. Desired effects should moreover be measured against available resources and experiences from other actors.

Keywords: Strategic Communications, Information Environment, Information Technology, Cognition, Disinformation, Deception, and Propaganda.

Förord

De senaste decenniernas snabba informationstekniska utveckling har på djupet förändrat förutsättningarna för mänsklig kommunikation. I en alltmer säkerhetspolitiskt osäker omvärld har utvecklingen inneburit nya möjligheter för skapande och spridande av information, både i informerande och propagandistiska syften.

Flera storpolitiska händelser har riktat strålkastarljuset på den enande såväl som splittrande kraften information kan ha – från den amerikanske presidenten Donald Trumps flexibla förhållningssätt till sanning, de massiva vågor av konspirations-teorier som spreds under covid-pandemin, till ryska aktörers försök att genom desinformation och påverkan spä på politiska splittringar i Europa och USA. Särskilt har Rysslands invasioner av Ukraina påvisat att kampen om informationsmiljön utgör en central front i modern krigföring.

Många stater runt om i världen har insett vikten av att utveckla förmåga för skydd och verkan i informationsmiljön. Den här rapporten har skrivits på uppdrag av Försvarsmakten inom ramen för projektet ”Ökad förmåga i den kognitiva informationsmiljön” och syftar till att ge Försvarsmakten underlag för vidare förmågeutveckling i informationsmiljön.

För rapporten står tre författare, men långt fler analytiker och forskare på FOI har deltagit i processen att framställa den. Särskilt tack riktas till Niklas Rossbach, Ida Selbing och Ola Svenonius som har granskat rapporten, samt Sebastian Cancino, Victoria Enkvist, Miranda Forsgren, Maria Refors Legge och Pontus Winther som har bidragit med värdefulla kommentarer under arbetets gång. Ett stort tack riktas vidare till kollegorna på Europeiska kompetenscentret för motverkande av hybrid-hot i Helsingfors och Natos kunskapscenter för strategisk kommunikation i Riga.

Innehåll

Utförlig sammanfattning	7
1 Inledning	9
1.1 Syfte och frågeställningar	10
1.2 Bakgrund.....	10
1.3 Metod	14
1.4 Disposition	15
2 Ny teknik, nya utmaningar	17
2.1 Ny informationsteknik och nya nätverk.....	18
2.2 Kampen om de nya plattformarna	25
2.3 Informationsmiljön och det nya kriget.....	36
2.4 Avslutande diskussion	43
3 Ny miljö, gammal människa.....	45
3.1 Ny design möter gammal uppmärksamhet.....	46
3.2 Det gamla minnet möter det digitala arkivet.....	53
3.3 Motivation möter datadriven propaganda.....	58
3.4 Avslutande diskussion	66
4 Ny förmåga, gamla strategier	69
4.1 Gammal strategi möter den nya informationsmiljön.....	70
4.1.1 Ryssland	71
4.1.2 Kina	75
4.1.3 USA.....	76
4.1.4 Andra länder i Väst	81
4.2 Ny förmåga, nya utmaningar	84
4.3 Avslutande diskussion	85
5 Sammanfattande slutsatser	89
6 Referenser.....	91

Utförlig sammanfattning

Människan befinner sig i begynnelsen av en digital tidsålder. Som aldrig förr är människor över hela jorden sammanflätade i en mängd av sociala, ekonomiska, politiska och kulturella nätverk. Dessa nätverk har till stor del möjliggjorts av utvecklingen av digital och fysisk infrastruktur genom vilken information flödar i oöverskådlig mängd. Utvecklingen ställer många och svåra utmaningar för hur aktörer kan och bör förhålla sig till denna nya digitala och nätverksbaserade verklighet.

För att konceptualisera dessa nätverk har forskare och praktiker kommit att använda begreppet ”informationsmiljö”. Begreppet är dock omtvistat och gränserna för vad som ingår är otydliga. Syftet med den här rapporten är att klargöra informationsmiljöns topografi med fokus på skydd och verkan i tider av konflikt och krig.

Den här rapporten utgår från en bred arbetsdefinition av informationsmiljön: Informationsmiljön består av nätverksrelationer mellan informationsteknik, information och aktörer.

Dagens informationsmiljö kännetecknas av en snabb och oförutsägbar teknisk utveckling. Ny teknologi och nya tekniker skapas och sprids innan deras samhällsliga och politiska konsekvenser förstås. Forskning, lagar och regler blir snabbt obsoleta. Informationsmiljön bidrar även till ett uppluckrande av gränser – inte bara geografiska, utan även gränserna mellan statliga och privata aktörer och konceptuella gränser mellan krig och fred (det som brukar benämnas gråzonen).

Det pågår i dag en kamp mellan såväl statliga som privata aktörer om att kontrollera informationsmiljön. Digitala plattformar, i synnerhet sociala medier, har likt internets infrastruktur i ökande grad kommit i fokus för stormakternas rivalitet och rör frågor som kontroll av teknisk utveckling och informationskontroll.

Medan informationskrigföring är ett tusenårigt fenomen har dagens tekniska utveckling inneburit att digital kommunikation blivit en integrerad del av modern krigföring. Informationskrigföring består av två förgreningar: en teknisk och en psykologisk. Till den tekniska räknas cyberoperationer, men även teleoperationer. Till den psykologiska förgreningen, som är i fokus för föreliggande rapport, räknas informations- och påverkansoperationer.

Den digitala informationsmiljön påverkar människan på många olika sätt. Forskningen om relationen mellan informationsmiljön och människan är i sin linda och i många fall motsägelsefull, men några grundläggande observationer kan ändå göras.

För att förstå hur människan påverkas är kognition centralt, och då inte minst uppmärksamhet. Lättkonsumerade och ofta negativt inramade budskap tenderar att

lättare fånga människans uppmärksamhet än djuplodande och komplexa budskap. Vidare är människor selektiva i hur vi inhämtar och avfärdar information, samtidigt som vi tenderar att överskatta just vår egen förmåga att ställa oss över våra egna kognitiva begränsningar.

Kognition sker dock inte i ett vakuum. Människan är en affektiv och social varelse. Kognition bör således förstås i relation till hur den samspelar med känslor och identitet (social, kulturell, etnisk och politisk), där relationen mellan gruppen och individen handlar lika mycket om gruppen i individen som individerna i gruppen. Detta är särskilt viktigt i förståelsen av hur informationspåverkan fungerar eftersom det är när påverkan sker på grupp- eller samhällsnivå som konsekvenserna får en större effekt.

En något förbisedd aspekt i militärstrategisk kommunikation är digitala subkulturer och de olika medieekologier som har vuxit fram på internet, vars snabbhet i att svärmarbeta fram information är enastående – likaså är deras potential att sprida falskheter och desinformation i multiplattforma informationsoperationer.

Effekten av manipulation och propaganda som sker i informationsmiljön är dock svår att mäta – precis som att de exakta orsakerna för polarisering är svåra att isolera från varandra. Informationsmiljöns potential för manipulation och påverkan ska heller inte överskattas.

Militära institutioner över hela världen arbetar i dag med att öka sin förmåga i informationsmiljön – till den grad att man kan skönja en kapprustning på området. Arbetet präglas mycket av skillnaderna i att utveckla denna förmåga i ett auktoritärt kontra ett demokratiskt sammanhang. Baserat på politiska, ideologiska, kulturella, juridiska och administrativa skillnader finns ett uppenbart större handlingsutrymme hos auktoritära stater att dra nytta av skuggsidorna i informationsmiljöns förändrade terräng. Samtidigt finns en styrka hos demokratiska rättsstater gällande mer grundläggande värderingar och friheter, som kan ha både offensiva (locka, övertyga) och defensiva (kritiskt tänkande, mångfald, förtroende) effekter.

För ökad förmåga avseende skydd och verkan i informationsmiljön krävs en god kunskap om tekniska, mänskliga, politiska och juridiska förutsättningar för att verka i den. Militär förmåga i informationsmiljön är en mycket komplex utmaning, särskilt för demokratiska rättsstater där förtroende för myndigheter och stater är avgörande.

Arbetet med att utveckla förmåga för skydd och verkan i informationsmiljön bör struktureras mot bakgrund av ovanstående slutsatser – vad gäller såväl ledning som sakkunskap och tillsyn. I en mening handlar det om att skynda långsamt, bland annat genom att utgå från den kunskap och förmåga som redan finns, såväl generellt som inom den aktuella organisationen, att lära sig från andra länders erfarenheter och att sträva efter öppenhet i kommunikationen kring arbetet med att utveckla förmåga i informationsmiljön.

1 Inledning

I en videoselfie inspelad på en smarttelefon får betraktaren följa Ukrainas president Volodymyr Zelenskyy när han går igenom korridorer i ett hus i centrala Kiev. Presidenten är orakad, han är påtagligt trött men hans blick är allvarlig. Han går mot ett skrivbord och sätter sig. Telefonen placeras på skrivbordet. Han lyfter blicken från telefonens kamera. I samma ögonblick tar en annan kamera över och videoselfien blir en direktsänd tv-sändning från presidentpalatset. Inom loppet av 30 sekunder har sändningen som helhet rört sig från personlig inramning av medborgaren Zelenskyy, som precis som miljontals andra ukrainare dokumenterar sin uppslitna vardag med sina telefoner, till en president som i tv talar till nationen.¹

Det här är bara ett av otaliga exempel på hur Zelenskyy och hans medarbetare har producerat innehåll som rör sig över etablerade genrer, appellerar till känslor och empati, manar den ukrainska befolkningen till motstånd och omvärlden till militärt och politiskt stöd. Under det ryska invasionskriget av Ukraina har sociala medier fyllts av bilder och filmer från kriget – ukrainska soldater på frontlinjen visar stridsmoral och förmåga, den civila befolkningen visar motståndskraft och den gamla ukrainska antisovjetiska folksången ”Ett rött olvon vid ängen” (*Oy u luzi chervona kalyna*) har genom sociala medier blivit en kampsång för det ukrainska folket, nationellt som internationellt.²

Det ryska invasionskriget har kallats det första TikTok-kriget, vilket åsyftar den stora roll som sociala medier har haft och fortfarande har.³ Detta är i sig förvisso inget nytt för just detta krig, men det kan förstås som en eskalering av den utveckling av den digitala informationsmiljön som har kunnat bevitnas de senaste decennierna. Det är en utveckling som har gett upphov till en omfattande produktion av teorier, texter och praktiska tillämpningar hos såväl civila som militära aktörer.

Den här rapporten är en berättande syntes av forskning om den nya informationsmiljöns utveckling. Den börjar med att behandla hur ny teknik har skapat nya förutsättningar för kommunikation och spridandet av information, för att sedan

¹ Videon var ett svar på rysk desinformation att Zelenskyy skulle ha gömt sig eller vara på flykt. Se: Reis Thebault och Hannah Knowles (2022), ”In Appearances from Presidential Office in Kyiv, Zelensky Says Russian Forces Are ‘All War Criminals’”, *The Washington Post*, 8 mars: <https://www.washingtonpost.com/world/2022/03/08/ukrainian-president-zelensky-kyiv-video-message/> [2022-08-14].

² Se: Ilona Kivva (2022), ”The story of the song ‘In the meadow, a red kalyna’. It has changed during the whole epochs of national liberation war”, *Zaborona*, 13 april: <https://zaborona.com/en/the-story-of-the-song-in-the-meadow-a-red-kalyna-it-has-changed-during-the-whole-epochs-of-national-liberation-war/> [2022-07-12].

³ Se vidare: Ivar Ekman och Per-Erik Nilsson (2022), *Folkets underrättelsetjänst - öppna källor, ”OSINT” och Ukraina*, FOI Memo: 7888, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI%20Memo%207888> [2022-07-10].

diskutera vad som händer med människan som både drivit på denna utveckling och befinner sig mitt i den. Slutligen riktas fokus mot hur olika stater med civila och militära medel sökt kontrollera och dra nytta av den nya digitala informationsmiljön. Givet informationsmiljöns föränderliga karaktär är det en berättelse utan slut.

1.1 Syfte och frågeställningar

Forskningen om den nya informationsmiljön är i sin linda. Den är bitvis motsägelsefull och under snabb utveckling. Trots detta finns det generella slutsatser att dra utifrån dagens kunskapsläge. För att rama in informationsmiljön huvudsakliga karaktärsdrag söker föreliggande rapport att svara på fyra frågor:

- Vilka är den nya informationsmiljöns mest grundläggande informationstekniska aspekter?
- Hur påverkas människan kognitivt och socialt av den nya informationsmiljön?
- Hur har olika stater sökt förstå och kontrollera den nya informationsmiljön?
- Hur ser samspelet mellan informationsteknik, människan och strategisk kommunikation ut i den nya informationsmiljön?

Med utgångspunkt i dessa frågor är syftet med rapporten att utreda den mångfacetterade komplexitet som omgärdar den nya informationsmiljön och att skapa en gemensam grund för hur den kan förstås samt förutsättningarna för att verka i den.

Som sådan är ambitionen att rapporten ska ge Försvarmakten underlag för att utveckla sin förmåga i informationsmiljön, vilket inbegriper vidare kunskapsutveckling inom såväl Försvarmaktens som akademins ramar.

1.2 Bakgrund

Informationsmiljön är ett omtvistat och svårt begrepp att definiera. Det är på inget sätt unikt för informationsmiljön, utan gäller för merparten av begrepp som används för att konceptualisera och förklara sociala och naturliga fenomen.⁴ För att rama in informationsmiljön utgår den här rapporten från en bred arbetsdefinition: *Informationsmiljön är en beskrivning av nätverksrelationer mellan informationsteknik, information och aktörer.*⁵

⁴ Detta refereras vanligtvis till som essentiellt omtvistade begrepp och kommer från filosofen Walter B. Gallie. Se: Walter B. Gallie (1955), "Essentially Contested Concepts", *Proceedings of the Aristotelian Society: New Series* 56 (1955 - 1956): 167-198.

⁵ Definition från: Patrick D. Allen och Dennis P. Gilbert Jr. (2010), "Qualifying the Information Sphere as a Domain", *Journal of Information Warfare* 9(3): 39-50, s. 42-43. Jämför med Försvarmaktens

Inom forskningen och i militär doktrin beskrivs informationsmiljön ofta i relation till de fem krigsdomänerna: land, sjö, luft, rymd och cyber (för vidare diskussion se kapitel 2). Informationsmiljön flyter in i alla dessa domäner. Att bedriva en militärövning kan handla lika mycket om att kommunicera förmåga till en presumtiv motståndare som att öva soldater för strid.

Vidare läggs ofta mänsklig kognition till begreppet i stil med ”den kognitiva informationsmiljön”.⁶ Kognition, så som det förstås i den här rapporten, syftar till de processer genom vilka sinnesintryck omvandlas, reduceras, utvecklas, lagras, återkallas och används.⁷ Det innebär att kognition handlar om perception, uppmärksamhet, beslutsfattande, problemlösning och inläring. Att tala om den kognitiva dimensionen av informationsmiljön handlar således om att rikta fokus på hur information påverkar människans förmåga att uppfatta omvärlden och sig själv, tänka kring dem och att medvetet eller omedvetet handla baserat på dessa uppfattningar. Kognition är dock, precis som informationsmiljö, ett omtvistat begrepp. För vissa handlar kognition strikt om vad som händer i en individs hjärna medan det för andra är ett vidare begrepp som inbegriper hur människors kognition är djupt inbäddad i sociala relationer.

Som framgår i rapporten är informationsmiljön en sammanflätning av information, teknik, människa och relationer dem emellan. Det kan då ifrågasättas vad begreppet kognitiv egentligen bidrar till förståelsen av informationsmiljön, eftersom informationsmiljön per definition handlar om människor, vilket innebär att den alltid står i relation till kognition.

En annan sammanflätad relation i informationsmiljön rör det civila och militära. Dagens digitala informationsmiljö består av både globala och regionala nätverksrelationer där gränserna mellan civil och militär informationsteknik suddas ut. Eftersom en rad olika aktörer tolkar vad informationsmiljön är och vilka handlingar som är legitima i den, är frågor om ekonomi, samhälle, politik och maktförhållanden lika viktiga som kognition.

Att informationsmiljön, kommunikation och militär strategi hör ihop är inget nytt. Militära teoretiker har diskuterat dessa relationer i mer än två millennier – från Sun Zi, Napoleon och Clausewitz till 1900-talets institutionalisering av propaganda. Informationsmiljön är dock mer komplex i dag än i tidigare historiska epoker. Det är inte första gången i historien som teknisk utveckling relaterat till informationsmiljön upplevs som ny och svårhanterbar – från tryckpressen till telegrafan och

definition av informationsmiljön: Sofia Olsson, Anna McWilliams, Per-Erik Nilsson och Patrik Thunholm (2022), *Militärstrategisk kommunikation i den kognitiva informationsmiljön*, FOI-R--5307--SE, Totalförsvarets forskningsinstitut, Stockholm:
<https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--5307--SE> [2022-08-02].

⁶ Den svenska Försvarsmakten använder denna benämning. Se: Olsson, McWilliams, Nilsson och Thunholm, *Militärstrategisk kommunikation*, s. 13.

⁷ Ulric Neisser (2014), *Cognitive Psychology* (Psychology Press: London och New York), s. 4. För en svensk grundläggande definition, se: Psykologilexikon, ”Kognition”, Natur & Kultur, 2022: <https://www.psykologiguiden.se/psykologilexikon/?Lookup=kognition> [2022-08-12].

dagens internet. Däremot förefaller föreställningen att aktörer med kommunikation kan styra informationsmiljön, särskilt med narrativ och olika typer av informationsoperationer, ha blivit mer framträdande än under tidigare epoker, av såväl civila som militära aktörer.⁸

Utan tvivel har dagens informationstekniska utveckling skapat nya förutsättningar för kommunikation som för endast några decennier sedan var science fiction. Napoleon använde oljemålningar, teateruppsättningar och bulletiner i tryckpress för att måla upp en grandios självbild som en slipad militär strateg. I dag används memer, högupplösta drönarbilder från slagfältet och en myriad digitala plattformar som sprids till miljontals användare världen över inom loppet av sekunder. De interageras med, tas ur kontext, förvrängs och ges nya meningar. Kostnaderna för denna interaktiva kommunikation är låga och att säkerställa den ursprungliga avsändaren är svårt. Civila kan mobiliseras för militära syften med några tangenttryckningar. Det ukrainska Ministeriet för digital transformation har till exempel använt de sociala medieplattformarna Telegram och Twitter för att rekrytera en it-armé av frivilliga. Genom Telegram koordineras olika typer av it-attacker mot ryska mål.⁹

Inom forskning och militär doktrin har det sedan 90-talet diskuterats hur den nya digitala informationsmiljön kan förstås och kontrolleras. Det har gett upphov till en rad övergripande frågor som är viktiga att ha i åtanke: Vad utgör egentligen grundpelarna i den här miljön? Handlar modern krigsföring kanske än mer om att kontrollera informationsmiljön än tidigare? Kan den överhuvudtaget kontrolleras? Om inte, hur kan strategiskt önskad effekt uppnås?

Det finns i dag otaliga artiklar, böcker, rapporter och doktriner som berör dessa frågor. I Väst har de till största del berörts inom ramen för vad som har kommit att kallas för strategisk kommunikation, som i sig är ett omtvistat begrepp. En grundläggande definition av strategisk kommunikation är att det handlar om *kommunikation som utförs av en aktör (organisation, företag, myndighet eller stat) i syfte att implementera en organisations målsättning*.¹⁰

⁸ Thomas Colley (2020), "Strategic Narratives and War Propaganda", i *The Sage Handbook of Propaganda*, red. Paul Baines, Nicholas O'Shaughnessy och Nancy Snow (London: Sage): 38-55.

⁹ Telegramgruppen heter i sin engelska upplaga IT ARMY of Ukraine. Se: Tom Simonite och Gian M. Volpicelli (2022), "Ukraine's Digital Ministry Is a Formidable War Machine", *Wired*, 17 mars: <https://www.wired.com/story/ukraine-digital-ministry-war/> [2022-06-22]; Vera Bergengruen (2022), "How Telegram Became the Digital Battlefield in the Russian-Ukraine War", *Time*, 21 mars: <https://time.com/6158437/telegram-russia-ukraine-information-war/> [2022-07-17].

¹⁰ För en diskussion om strategisk kommunikation som akademisk subdisciplin inom medie- och kommunikationsvetenskap, se: Kirk Hallahan, Derina Holtzhausen, Betteke van Ruler, Dejan Verčič och Krishnamurthy Sriramesh (2007), "Defining Strategic Communication", *International Journal of Strategic Communication* 1(1): 3-35; Howard Nothhaft, Kelly Page Werder, Dejan Verčič och Ansgar Zerfass (2018), "Strategic Communication: Reflections on an Elusive Concept", *International Journal of Strategic Communication* 12(4): 352-366.

För att kommunicera strategiskt finns åtminstone tre centrala utmaningar. Den första är *teknisk* och handlar om hur precist information kan sändas ut. Den andra är själva *budskapet* och handlar om att klargöra vad som ska kommuniceras samt att säkerställa att önskad mening når rätt målgrupp. Den sista är *effekt* och handlar om hur målgruppen tolkar budskapet och agerar enligt önskad effekt.¹¹ Beroende på vilken förståelse den kommunicerande aktören har av både strategi och kommunikation följer olika modeller för hur strategisk kommunikation bör genomföras.¹² Det *strategiska* i strategisk kommunikation innebär dock att det är den organisatoriska målsättningen som står i fokus och inte målen för en viss kommunikationsinsats.¹³

Att använda strategisk kommunikation i informationsmiljön i en militär kontext är dock inte samma sak som exempelvis i den kommersiella sektorn. I en militär kontext handlar det om en stats och nations överlevnad och inte huruvida ett företag lyckas tränga igenom mediebruset för att sälja mer av sina produkter.¹⁴ Militärstrategisk kommunikation måste av nödvändighet vara mer dynamisk eftersom dess befogenheter är avhängiga rådande beredskapsläge och till syvende och sist handlar om liv och död.¹⁵

Forskningen om informationsmiljön och strategisk kommunikation i relation till militär förmåga är ett spretigt ämnesområde. Både forskningen om och institutionaliseringen av strategisk kommunikation och informationsmiljön kännetecknas av inflation av modeller och begrepp: informationsmiljö, informationsdomän, informationsarena, informationskrig, psykologisk krigföring och försvar, kognitiv krigföring och motståndskraft, cyberkrigföring med mera.¹⁶ Detta är i sig inget anmärkningsvärt. I forskningsvärlden sker en ständig omvärdering och utveckling av teorier och begrepp för att söka begripliggöra människans komplexitet både som individ och som del i olika samhällen. I en digital tidsålder har människa, samhälle

¹¹ Se: Richard A. Poisel (2013), *Information Warfare and Electronic Warfare Systems* (Norwood: Artech House), s. 5. För diskussion om budskap, utformning och övertygelse, se: Craig Hayden och Emily T. Metzgar (2019), "Strategic Communication and Security", i *The Handbook of Communication and Security*, red. Bryan C. Taylor och Hamilton Bean (New York: Taylor & Francis), 185-202, s. 186.

¹² Det finns åtminstone tre sätt att förstå kommunikation: 1) som en ensidig process med sändare och mottagare; 2) som en tvåsidig och meningsskapande process; 3) som en mångfacetterad och föränderlig process där meningsskapande är en dynamisk och högst kontextuell process. För vidare diskussion, se: Betteke van Ruler (2018), "Communication Theory: An Underrated Pillar on Which Strategic Communication Rests", *International Journal of Strategic Communication* 12(4): 367-381.

¹³ Jesper Falkheimer och Mats Heide (2014), *Strategisk kommunikation: En introduktion* (Lund: Studentlitteratur), s. 15.

¹⁴ En grundläggande skillnad är att militärt inriktad strategisk kommunikation handlar om en stats och dess samhälles överlevnad till skillnad från företag som söker framgång i den kommersiella sektorn. Se vidare: Vladimir Vyklický och Vendula Divišová (2021), "Military Perspective on Strategic Communications as the 'New Kid on the Block': Narrating the Czech Military Deployment in Afghanistan and the Baltic States", *International Journal of Strategic Communication* 15(3): 231-252.

¹⁵ För en övergripande diskussion om likheter och skillnader mellan civil och militär strategisk kommunikation, se: Gary F. Keller, "The Influence of Military Strategies on Business Planning", *International Journal of Business and Management* 3(5), 2008: 129-134.

¹⁶ Keir Giles (2016), *Handbook of Russian Information Warfare*, NATO Defense College, Rom: s. 5.

och teknik dock blivit alltmer integrerade och utvecklingen inom vissa aspekter av denna integration sker så pass snabbt att det är lönlöst att tro att den kan kontrolleras fullt ut.

En viktig men svår utmaning för den som vill kommunicera strategiskt i informationsmiljön är därför att utveckla en begreppsapparat som är långsiktig och inte går vilse i detaljer eller dras med i en begreppsinflation där det senaste modebegreppet i forskningsvärlden snarare kan förvirra än klargöra. Vidare är det avgörande att begreppen som används för att beskriva informationsmiljön och strategier för att verka i den tydligt kommunicerar vad deras syften är. I en demokratisk rättsstat bör inte myndigheter utöva påverkan mot den egna befolkningen medelst manipulation av information, varför begrepp som leder tankarna till krigföring rörande den egna befolkningen kan leda till missförstånd eller, som diskuteras i kapitel 4, leda praktiker in i en bana som inte är förenlig med rådande lagstiftning och grundläggande medborgerliga fri- och rättigheter.

1.3 Metod

Rapporten är en syntes av forskning och dokumenterad erfarenhet. Det betyder att de perspektiv som presenteras i rapporten är de av författarna identifierade huvudragen inom litteraturen, vilket innebär att flera alternativa perspektiv har utelämnats. För läsaren som vill fördjupa sig och få en mer nyanserad bild hänvisas till notapparaten som utöver referenser innehåller kommentarer och hänvisningar för vidare läsning. Det ska understrykas att den använda forskningen till en dominerande grad är anglosaxisk samt under snabb utveckling. Det innebär att forskningens generaliserbarhet ska tolkas med försiktighet.

Genomgående har sökningar i forskningsdatabaser använts, och sedan kompletterats med snöbollsmetoden för att söka vidare fördjupning och nyansering.¹⁷

Rapporten utgår från fyra typer av källor. För det första är rapporten en forskningsöversikt av litteratur från en bred variation av discipliner inom samhällsvetenskap, humaniora och datavetenskap med tematisk inriktning mot teknik och samhälle, kognitionsforskning, evolutions- och socialpsykologi, strategisk kommunikation, propaganda, militärhistoria och krigsvetenskap. Relevant forskning har identifierats genom sökningar i relevanta forskningsdatabaser och i vetenskapliga tidskrifter.

¹⁷ Snöbollsmetoden är en vedertagen metod inom samhällsvetenskaplig forskning och är särskilt användbar för litteraturoversikter. I korta ordalag innebär metoden att forskare utgår från grundkällor inom forskningsfältet för att genom dessa identifiera både tidigare och efterföljande forskning. För en översikt av metoden, se: Claes Wohlin (2014), "Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering", *EASE '14: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, artikel 38: 1-10.

För det andra är rapporten en litteraturöversikt av journalistiskt arbete, rapporter från icke-statliga aktörer och nedskrivna erfarenheter från praktiker inom rapportens tematik.

För det tredje är rapporten en översiktlig studie av andra staters och mellanstatliga organisationers doktriner och arbete inom området strategisk kommunikation och informationskrigföring.

Slutligen bygger rapporten på samtal med analytiker, forskare och praktiker både inom och utanför Sveriges gränser, och särskilt vid Europeiska kompetenscentret för motverkande av hybridhot i Helsingfors, Natos kunskapscenter för strategisk kommunikation i Riga och under Natos konferens för strategisk kommunikation *Riga Stratcom Dialogue* 25-26 maj 2022.

Som har påpekats fokuserar rapporten på de nya aspekterna av informationsmiljön, vilket innebär att fokus riktas mot informationsteknik och digital kommunikation. Det betyder dock inte att fysiska aspekter av kommunikation är mindre viktiga. Från ett strategiskt kommunikativt perspektiv, där all verksamhet i en organisation antas kommunicera, är handlingar och institutionaliserat minne lika viktiga.¹⁸ Om något har den nya informationsmiljön bidragit till att snabbt synliggöra när ord inte lever upp till handling.

1.4 Disposition

Rapporten är disponerad kring tre teman: a) informationstekniska förutsättningar för att verka i informationsmiljön; b) människan som målgrupp för kommunikation i informationsmiljön; och c) hur militära aktörer har arbetat och arbetar för att kommunicera strategiskt i informationsmiljön. I rapportens andra kapitel – ”Ny teknik, nya utmaningar” – diskuteras den nya informationsmiljöns utveckling i relation till informationsteknik, fysisk och digital infrastruktur, hur internet har förändrat informationsmiljön samt hur den nya informationsmiljön har gett upphov till nya förståelser av konflikt och krig.

Rapportens tredje kapitel – ”Ny miljö, gammal människa” – fokuserar på relationen mellan informationsmiljön och människan. Här diskuteras särskilt kognitiva och samhälleliga aspekter av digitaliserad kommunikation och information med fokus på uppmärksamhet, minne och identitet.

Det fjärde kapitlet – ”Ny förmåga, gamla strategier” – går igenom hur olika statliga aktörer har sökt hantera informationsmiljön. Fokus riktas mot vilka strategiska och juridiska lärdomar som kan dras för att utveckla förmåga i informationsmiljön. Här diskuteras särskilt USA, Ryssland och Kina.

¹⁸ Se till exempel: Nina Jankowicz (2020), *How to Lose the Information War: Russia, Fake News, and the Future of Conflict* (London och New York: I. B. Tauris), s. 200.

Varje kapitel avslutas med en diskussion kring hur respektive kapitels kärnpunkter relaterar till frågor om strategisk kommunikation och kommunikativ förmåga i den nya informationsmiljön. Rapporten som helhet avslutas med sammanfattande slutsatser som kan ligga till grund för vidare utveckling av förmåga och forskning inom militärstrategisk kommunikation.

2 Ny teknik, nya utmaningar

För femton år sedan klev Steve Jobs, en av grundarna till it-bolaget Apple Inc., upp på en scen i en fylld konferenssal under företagets årliga event MacWorld. Till applåder konstaterade Jobs att det till och från kommer revolutionerande produkter som förändrar allt. Han berättade om hur fantastiskt det vore att ha en produkt som alltid är uppkopplad, som kan spela upp musik och film, surfa på internet och, inte minst, samtidigt fungera som telefon – en iPhone. När han nämnde det sista skrattade publiken till. Med entusiasm ställde han en retorisk fråga till publiken: ”Hajar ni?! Det här är inte längre separata prylar. Det är en!” Publiken brast ut i jubel.

Apples iPhone var inte den första smarta telefonen på marknaden, men dess avancerade teknik och användarvänlighet var ett avgörande steg i att revolutionära människans relation till digital teknik.¹ Handhållna och kroppsburna enheter är i dag en integrerad del av vardagen för allt från informationsinhämtning, kommunikation och dokumentation till insamlandet av biometrisk data.² Vissa forskare framhåller till och med att enheter av detta slag har blivit en integrerad del av vad det är att vara människa i dag.³

Informationsmiljön har funnits så länge människor har funnits, men de senaste decenniernas tekniska utveckling har förändrat den radikalt. I dag beräknas ca 63 procent av världens befolkning ha tillgång till internetuppkoppling, varav 90 procent använder smarta telefoner. Därtill spenderar en person i genomsnitt 7 timmar om dagen uppkopplad. Merparten av tiden ägnas åt sociala medier, vilka i dag används av fler än 4,5 miljarder människor.⁴

¹ Vissa forskare ser populariseringen och utvecklingen av den smarta telefonen som själva startskottet för den digitala tidsåldern. Se till exempel: Kevin Kelly (2016), *The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future* (New York: Penguin Random House), s. 8.

² Biometrisk data är personuppgifter som handlar om en persons fysiska, fysiologiska eller beteendemässiga kännetecken. De möjliggör och kan bekräfta en persons identitet, exempelvis genom ansiktsgenkänning eller fingeravtryck. Generellt kan biometrisk data delas in i två kategorier: biologiskt och beteendemässig. Den biologiska utgörs av sådant som fingeravtryck, ansikte, ögoniris, vener med mera. Den beteendemässiga utgörs av sådant som tangentbordstrykningsdynamik och röst, men även namnunderskrift och gångstil. Se: Integritetsskyddsmyndigheten (2021), ”Biometri”, 5 maj: <https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/arbetsliv/biometri/> [2022-07-07]; World Bank (2019), *ID4D Practitioner's Guide: Version 1.0 (October 2019)*, Washington DC, World Bank.

³ Se till exempel den mångvetenskapliga akademiska skolbildningen nymaterialism (*new materialism*) som för samman teorier från post- och antihumanism, kritisk och spekulativ realism, kaosteori och tillblivelsefilosofi: Matthias Leese och Marijn Hoijtink (2019), ”How (Not) to Talk about Technology: International Relations and the Question of Agency”, i *Technology and Agency in International Relations*, red. Marijn Hoijtink och Matthias Leese (Routledge: Abingdon och New York), 1-23.

⁴ Om tid uppkopplad, global internettillgång och användning av smarta telefoner för att surfa, se: Simon Kemp (2022), ”Digital 2022: April Global Statshot Report”, *Datareportal*, 21 april: <https://datareportal.com/reports/digital-2022-april-global-statshot> [2022-05-30]. Om global användning av sociala medier, se: Simon Kemp (2022), ”Global Social Media Statistics”, *Datareportal*:

Dagens informationsmiljö är ett omfattande nätverk av teknik, data- och informationsflöden och aktörer som interagerar med en rad olika syften. Informationsmiljön möjliggör gränslösa utbyten av data och information samtidigt som den är bunden till tekniska, geografiska och kontextuella gränser som påverkar varje användares uppfattning av den. Den digitala informationsmiljöns komplexitet och snabba föränderlighet är en svårnavigerad miljö som innebär nya förutsättningar för att verka i den.

Med fokus på informationstekniska aspekter, diskuterar det här kapitlet förutsättningar för att verka i dagens digitalt dominerade informationsmiljö. Fokus riktas mot hur framväxten av internetbaserad kommunikation och infrastruktur har lett till en ständigt expanderande digitalisering av vardagen, miljöns nya former av relationer mellan aktörer, data och information samt hur informationsmiljön har blivit en integrerad del i förståelsen av modern krigföring.

2.1 Ny informationsteknik och nya nätverk

Elva år innan den smarta telefonens genombrott, 1996, blev ”internet” årets julklapp i Sverige.⁵ Då var Ines Uusmann (S) kommunikationsminister. Det var en tid då informationsteknik diskuterades flitigt i offentligheten. Uusmann kom att bli särskilt känd för ett felaktigt attribuerat uttalande: ”Internet är en fluga.” Det hon faktiskt sa var: ”Jag vågar inte ha någon alldeles bestämd uppfattning men jag tror inte att folk i längden kommer att vilja ägna så mycket tid, som det faktiskt tar, åt att surfa på nätet... Att sitta och surfa på nätet tar en himla massa tid. Vad är det bra för?”⁶

Uusmanns uttalande är lätt att förlöjliga i dag. Hon var dock inte ensam om denna prognos.⁷ I själva verket har många av 1900-talets tekniska framsteg tagits emot med skepsis av politiska ledare.⁸ Vid tiden var också internet en plats för de insatta

<https://dataportal.com/social-media-users> [2022-07-07]. I Sverige använder 9 av 10 medborgare internet dagligen, 100 procent av studerande har en smart telefon, 9 av tio använder digitala samhällstjänster och 7 av 10 har uppkopplade prylar. Se vidare: Jenny Andersson (2021), *Svenskarna och internet 2021*, Internetstiftelsen: <https://svenskarnaochinternet.se/app/uploads/2021/09/internetstiftelsen-svenskarna-och-internet-2021.pdf> [2022-08-15].

⁵ Det handlade om internetpaketet som inkluderade modem, internetabonnemang, diskett eller en CD-skiva samt en instruktionsbok för att koppla upp sig på internet.

⁶ Internetstiftelsen, ”Internet är en fluga”: <https://www.internetmuseum.se/tidslinjen/internet-ar-en-fluga/> [2022-06-02].

⁷ För exempel på skepsis till internets potential såväl som flera av de tidigare grundarnas oro för att internet redan på 90-talet visade tecken på att kommersialiseras samt ha en negativ inverkan på människan, se: Alexis C. Madrigal (2019), ”The People Who Hated the Web Even Before Facebook”, *The Atlantic*, 19 mars: <https://www.theatlantic.com/technology/archive/2019/03/people-who-hated-web-even-before-facebook/584932/> [2022-08-05].

⁸ För exempel på politiska ledare och skepsis inför tekniska framsteg, se: Glenn Diesen (2021), *Great Power Politics in the Fourth Industrial Revolution: The Geoeconomics of Technological Sovereignty* (London och New York: I. B. Tauris), s. 4.

– nördarna – vars åtkomst byggde på långsamma kabelmodem och bestod av svårnavigerade hemsidor och tidiga former av sociala chattrum.⁹

Vare sig man sätter startskottet för den digitala tidsåldern till 70-talets datorer, 90-talets popularisering av internet, eller Steve Jobs lansering av iPhone 2007, så har den en historia på några få decennier – knappt en ögonblinkning i människans historia.¹⁰ Utvecklingen av ny teknologi och nya tekniker går nu så fort att människan arbetar med att retroaktivt benämna, förstå och civilisera dem.¹¹

I dag är internet det globala hjärtat i den digitala informationsmiljön. Som påpekats kan dagens internet konceptuellt sett härledas långt bak i historien.¹² Det är dock först på 1950-talet som det går att tala om något som påminner om dagens datorbaserade digitala och nätverksbaserade kommunikation. Ett känt exempel är det amerikanska flygvapnets radarsystem *Semi-Automatic Ground Environment* (SAGE) genom vilket enkla datorer kunde kommunicera med varandra via modem.¹³ År 1957 hände dock något revolutionerande som fick det amerikanska Försvarsdepartementet att reagera: Sovjet lyckades skjuta upp Sputnik 1, den första satelliten i rymden. Som svar på detta sjuksattes en rad projekt inom raket-, elektronik- och atomforskning. År 1958 föddes *Advanced Research Projects Agency* (ARPA), med syftet att främja forskning och utveckling för militärt bruk.¹⁴ Med olika finansieringsprogram involverades den amerikanska akademien och snabbt ökade datorkraft och effektivitet. Flera forskare var här drivande i att utveckla teorier om datorbaserade nätverk. Särskilt inflytelserik blev psykologen Joseph C. R. Licklider på Massachusetts Institute of Technology (MIT) med sin idé om ett ”galaktiskt nätverk”, som utöver att främja vetenskaplig utveckling skulle främja social interaktion mellan människor.¹⁵

På University of California Los Angeles (UCLA) arbetade datorvetaren Leonard Kleinrock, specialiserad inom datorbaserad kommunikation, tillsammans med en grupp studenter med att realisera dessa teorier. Den 2 september 1969 lyckades de med bedriften att skicka databytes mellan två datorer. Enligt Kleinrock var detta

⁹ Se: Jakob Svensson (2021), *Wizards of the Web: An Outsiders Journey Into Tech Culture, Programming, and Mathemagics* (Göteborg: Nordicom), s. 52.

¹⁰ Konceptuellt sett kan internets historia vara minst 400 år gammal när teorier om att samla, lagra och effektivt dela information teoretiserades kring efter 1500-talets vetenskapliga revolution i Europa. Se: Marshall T. Poe (2011), *A History of Communications: Media and Society from the Evolution of Speech to the Internet* (Cambridge och New York: Cambridge University Press), s. 204-215.

¹¹ För fullständigt resonemang, se: Kelly, *Understanding the 12*, s. 9.

¹² Bland annat utvecklade Sovjetunionen OGAS, Storbritannien NPL, och i Sverige fanns ett projekt, Tidas, som leddes av statliga Vattenfall och genom ett datorbaserat övervakningssystem kunde minska risken för störningar i kraftsystemen. Se översikt av internets historia på Internetstiftelsens digitala internetmuseum: Internetstiftelsen, ”Internetmuseum”: <https://www.internetmuseum.se/> [2022-07-07].

¹³ Licklider blev sedan chef över ARPA:s *Information Processing Techniques Office* (IPTO). Se vidare: Michael A. Banks (2008), *On the Way to the Web: The Secret History of Internet and Its Founders* (Berkely och New York: Apress), s. 2-3.

¹⁴ Namnet ändrades sedermera till *Defense Advanced Research Projects Agency* (DARPA).

¹⁵ Banks, *On the Way*, s. 3.

”internets första livstecken”.¹⁶ Kort därefter skickade Kleinrock det första digitala meddelandet till en dator på Stanford University – ARPANET var fött. År 1973 var fyrtio datorer uppkopplade till ARPANET. Samma år anslöts datorer från Norge och Storbritannien och det amerikanska ARPANET blev ett internationellt nätverk.

År 1980 var över 70 institutioner och 5 000 användare anslutna till internet.¹⁷ Den 1 januari 1983 homogeniserades det framväxande internet genom övergången till en standard för nätverkskommunikation med *Transmission Control Protocol* och *Internet Protocol* (TCP/IP), vilket innebar att alla datorer som inte följde efter kopplades bort från internet.¹⁸ Under samma period öppnades internet (ARPANET) för civila och kommersiella aktörer medan den amerikanska militären skulle använda ett nytt och säkrare nätverk kallat MILNET.¹⁹

Med ett internet som var öppet för civila och kommersiella intressen började en snabb och experimentell utveckling att ta fart. Av särskild vikt är den brittiske fysikern Tim Berners-Lee vid Europeiska organisationen för kärnforskning (CERN), som med en grupp forskare i början av 90-talet började utveckla ett nytt index som kunde binda samman databaser. Resultatet blev *Hypertext Markup Language* (HTML) som utöver att sammanbinda databaser möjliggjorde att bilder och video kunde visas över internet. För att precisera hur data skickades mellan olika noder i internet utvecklades *Hypertext Transfer Protocol* (HTTP) och för att lätt kunna hitta data på internet skapades *Uniform Resource Identifier* (URI) som sedan blev *Uniform Resource Locator* (URL).²⁰ Berners-Lees skapelse kallades *World Wide Web* och offentliggjordes av CERN 1992.²¹

Internets framväxt är tillsammans med teknologiska framsteg och en rad tekniska utvecklingar signifikant för den tredje industriella revolutionen. Under 90-talet sker en rad viktiga händelser som har satt ramarna för dagens informationsmiljö. Vita Huset och FN lanserade webbsidor, företag som Amazon och eBay bidrog starkt till kommersialiseringen av internet, trådlös dataöverföring slog igenom i industrin och Google lanserade sin sökmotor. Under det följande årtiondet lanseras molnteknik, sociala medier slår igenom, stordata blir ett koncept, 3G blir standard, *blockchaintekniken* presenteras, den amerikanska internetleverantören AOL börjar erbjuda gratistjänster som finansieras genom reklam och en grupp företag lanserar IPSO-alliansen för att standardisera IP för sakernas internet (*Internet of Things*, IoT).²²

¹⁶ Original: ”That was the first breath of life the Internet ever took.” Fritt citerad i Banks, *On the Way*, s. 5.

¹⁷ Peter W. Singer och Emerson T. Brooking (2019), *LikeWar – The Weaponization of Social Media* (New York: First Mariner Books edition), s. 37.

¹⁸ Banks, *On the Way*, s. 78.

¹⁹ Singer och Brooking, *LikeWar*, s. 38.

²⁰ Singer och Brooking, *LikeWar*, s. 38.

²¹ Banks, *On the Way*, s. 193.

²² Om den tredje industriella revolutionen, se: Jeremy Rifkin (2011), *The Third Industrial Revolution: How Lateral Power is Transforming Energy, the Economy, and the World* (New York: Palgrave Macmillan).

Sedan ett drygt decennium befinner vi oss i den fjärde industriella revolutionen som hittills kännetecknas av en snabb utveckling av maskininlärning och artificiell intelligens (AI),²³ 5G, automatisering, robotik, additiv tillverkning, vidareutvecklad blockchainteknik, en expansion av sakernas internet, kroppens internet, kvantumdataorer, nanoteknik, neuroteknik, bioteknik, genetisk modifiering med mera.²⁴ För industrin förväntas en tilltagande sammansmältning av civil och militär teknik, så kallad dubbel användning (*dual use*), som högst sannolikt kommer att innebära förändringar vad gäller exempelvis automatisering inom produktion och autonomi hos fordon. Den här omfattande digitaliseringen har påverkat och omformat förutsättningarna för hur människor lever sina liv – samhälleligt, politiskt, ekonomiskt och militärt.²⁵

Bortom protokoll, index och mjukvara består internet av fysisk infrastruktur - radiomaster, fiberkablar, satelliter, datacenter, serverhallar med mera. Den fysiska infrastrukturen kan förstås som det första av fyra lager. Det andra lagret består av kommunikationsoperatörer som hanterar dataöverföring oberoende av vilken internetleverantör eller operatör som förmedlar uppkoppling till en användare. Det tredje lagret består av operatörer som erbjuder internetuppkoppling och i det fjärde lagret återfinns alla de individer, företag och statliga aktörer som erbjuder digitala och nätbaserade tjänster.²⁶ De tre övre lagren utgör den digitala infrastrukturen. Kopplat till detta arbetar nationella och internationella organisationer med att säkra internets funktion och infrastruktur via bland annat standardisering av dataöverföringsprotokoll och tilldelande av IP-adresser.²⁷

²³ AI är ett omdebatterat och ofta missförstått begrepp. Mycket av det som i dagligt tal ses som AI är i själva verket avancerade kalkyleringssystem, som exempelvis IBM:s schackalgoritm Deep Blue. I dag finns så kallad analytisk AI som har kognitionsliknande funktioner. Mänskligt inspirerad AI som skulle kunna visa emotionell intelligens är under utveckling medan mänskligt AI som skulle uppvisa ovanstående parametrar tillsammans med empati och sociala färdigheter förefaller i skrivande stund vara mer vision än ett realistiskt mål. Se: Andreas Kaplan (2022), *Artificial Intelligence, Business and Civilization: Our Fate Made in Machines* (London och New York: Routledge).

²⁴ Diesen, *Great Power*, s. 4. Att särskilt 5G-nätet sannolikt kommer att öka dataöverföringshastigheten väsentligt är de flesta överens om, men det finns vissa kontextuella förutsättningar som kommer leda till att hastigheten varierar beroende på geografisk räckvidd. Enligt Post- och telestyrelsen kommer hastigheter som uppnås bero på bland annat vilka frekvensband internetoperatören i ett område använder och på tillgång till master. För Sveriges del skulle det innebära stora investeringar för att uppnå maxhastighet med 5G. Samtidigt kan 5G använda mer av radiospektrumet liksom sammanlänka med satellitnätverk, vilket i teorin innebär att nätet kan täcka ännu större delar av världen. Se: Post- och telestyrelsen, "Allmänt om 5G." <https://www.pts.se/sv/5g/allmant-om-5g/> [2022-07-08].

²⁵ Diesen, *Great Power*, s. 4.

²⁶ Se vidare: Joacim Forsén (2021), "Vem bestämmer egentligen över internet?" Internetkunskap: <https://internetkunskap.se/artiklar/sa-funkar-internet/vem-bestammer-egentligen-over-internet/> [2022-06-22]. För en diskussion om den svenska infrastrukturen, se: Kungliga Ingenjörsvetenskapsakademien (2019), *Digitalisering för ökad konkurrenskraft*: <https://www.iva.se/globalassets/projekt/201902-iva-digitalisering-slutrapport-l.pdf> [2022-08-04].

²⁷ Exempel på dessa är FN:s Internet Governance Forum (IGF), de amerikanska Internet Corporation for Assigned Names and Numbers (ICANN) och Internet Assigned Numbers Authority (IANA) samt det europeiska Réseaux IP Européens - Network Coordination Centre (RIPE NCC).

Både digital och fysisk infrastruktur ägs i dag till stor del av privata företag, vissa med starkare koppling till olika statsmakter än andra.²⁸ Många konkurrerande intressen som profitjakt, kontroll, övervakning och tillgång till fri information tävlar om att sätta ramarna för dagens och framtidens internet. Att dominera it-infrastruktur, internet och tillhandahållandet av olika typer av tjänster och digitala plattformar för att vinna fördelar inom ekonomi, handel och informationsutbyte är tätt sammankopplat med makt och kontroll över den digitala informationsmiljön. Att kontrollera informationsteknisk infrastruktur är således ett sätt att kontrollera den digitala informationsmiljön.²⁹

Kontrollen över internets infrastruktur har, som framgår ovan, varit starkt dominerad av statliga och privata aktörer i USA och Västeuropa. Den här dominansen utmanas dock i tilltagande grad av andra aktörer, inte minst av Kina. I den kinesiska statsstyrda strategin för digital kommunikation läggs stora resurser på utveckling av maskininlärning och AI, blockchainteknik, molnbaserad datoranvändning och datainsamling samt utbyggnad och kontroll över fysisk infrastruktur som undervattenskablar.³⁰ Kinesiska aktörer söker också standardisera egna informationstekniska protokoll för att konkurrera med rådande standarder.³¹ Brist på förståelse av hur fysisk och digital infrastruktur är sammankopplade med privata och statliga intressen har lett till att statliga aktörer har tagit beslut som riskerar nationell säkerhet.³²

Kontroll över infrastruktur innebär vidare att stater kan stänga ner tillgången till internet såväl som telefoni.³³ I själva verket har närmare 80 procent av världens befolkning en begränsad tillgång till internet.³⁴ Att stänga ner internet för en tid eller mer permanent innebär höga politiska och ekonomiska kostnader som står i

²⁸ I nedstigande ordning är de fem största företagen Amazon (USA), Alphabet Inc. (USA), Meta (USA), Tencent Holdings (Kina) och Alibaba (Kina). Se: Andrew Bloomenthal (2022), *World's Top Ten Internet Companies*, Investopedia, 17 mars: <https://www.investopedia.com/articles/personal-finance/030415/worlds-top-10-internet-companies.asp> [2022-08-04].

²⁹ Diesen, *Great Power*, s. 108.

³⁰ Charles Mok (2022), "The Making of China's Future Internet: A Closer Look on the Fourteenth Five-Year Plan on Digital Economy", Friedrich Naumann Foundation, 18 februari: <https://www.freiheit.org/taiwan/making-chinas-future-internet> [2022-08-02].

³¹ Stacie Hoffmann, Dominique Lazanski och Emily Taylor (2020), "Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet", *Journal of Cyber Policy* 5(2): 239-264.

³² Ett emblematiskt svenskt fall är Transportstyrelsens upphandling av it-drift. Se: Thomas Bull (2018), *Granskning av Transportstyrelsens upphandling av it-drift*, Ds 2018:6, Näringsdepartementet, Regeringskansliet, Stockholm: <https://data.riksdagen.se/fil/FB3C8AF9-BE36-4E7F-A09B-80D12887C189> [2022-09-15].

³³ Steven Feldstein (2022), *Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?*, Carnegie Endowment for International Peace, Washington: https://carnegieendowment.org/files/Feldstein_Internet_shutdowns_final.pdf [2022-07-17].

³⁴ Freedom House (2021), *Freedom on the Net: The Global Drive to Control Big Tech*, s. 4: https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf [2022-08-02].

relation till uppskattad vinst av att begränsa medborgares tillgång till information.³⁵ Andra metoder för att begränsa tillgången till informationsmiljön är att strypa bandbredden, vilket innebär att internetuppkopplingens hastighet kraftigt reduceras.³⁶ Beroende på hur mycket hastigheten reduceras kan nödvändiga internetjänster fortsätta att fungera, men samtidigt skapa utmattning bland användare och begränsa dem från att ta del av mer bandbreddskrävande information. Exempelvis fungerar endast sms och röstsamtal när mobilnätet reduceras till 2G.³⁷ Att begränsa internet har visat sig ligga i auktoritära regimers intresse när de vill stävja informationstillgång och proteströrelser. Det kan vara effektivt även om många exempel visar på motsatsen.³⁸

Den iranska regimen har vid flertalet tillfällen använt metoder av de slag som nämns ovan för att begränsa medborgares tillgång till information. År 2021 stängdes internet flera gånger i delar av landet för att hindra spridning av bilder och information om hur protester våldsamt slogs ner.³⁹ I Ryssland har medborgarnas tillgång till bland annat Instagram, Twitter och Facebook begränsats med anledning av det ryska invasionskriget i Ukraina. Fram till juni 2022 hade över 7 500 webbplatser blockerats av den ryska riksåklagarens kansli och tillgång till inhemska nyhetsmedier, såväl som utländska nyhetsmedier (till exempel BBC, Deutsche Welle och Radio Free Europe), har begränsats på bred front.⁴⁰ De ryska åtgärderna syftar till att begränsa för Ryssland missgynnande informationsspridning.⁴¹ Som ett resultat har användningen av virtuella privata nätverk (VPN), som anonymiserar internetanvändaren och låter denne kringgå vissa begränsningar, ökat markant i Ryssland.⁴²

³⁵ Beräkningar visar på att aktiv nedstängning av internet under 2021 kostade den globala ekonomin \$5,45 miljarder, vilket är en kostnadsökning på 36 procent jämfört med 2020. Se: Samuel Woodhams och Simon Migliano (2022), "Government Internet Shutdowns Cost \$ 5,5 Billion in 2021", *Top10VPN*, 4 januari: <https://www.top10vpn.com/research/cost-of-internet-shutdowns/2021/> [2022-06-30].

³⁶ Den engelska termen är *dynamic frequency scaling* eller så kallad *throttling*. För en diskussion om olika metoder för att begränsa eller stänga internet, se: Feldstein, *Government Internet*, s. 10.

³⁷ Woodhams och Migliano, "Government Internet."

³⁸ Under den arabiska våren valde den egyptiska regeringen att stänga ner all internet- och mobiltelefonkommunikation under delar av den tid som det folkliga upproret mot det rådande styret pågick. Eftersom både mobiltelefonin och internettillgången stängdes ner hade människor inget annat val än att gå ut på gatorna och till Tahrirtorget, vilket var den centrala platsen för de folkliga protesterna. Det fick alltså en motsatt effekt och ledde snarare till att fler människor samlades. I slutänden ledde protesterna till att den dåvarande egyptiska presidenten avgick. Singer och Brooking, *LikeWar*, s. 85-86; Paolo Gerbaudo (2012), *Tweets and the Streets: Social Media and Contemporary Activism* (London: Pluto Press), s. 15-16.

³⁹ Woodhams och Migliano, "Government Internet."

⁴⁰ Samuel Woodhams och Simon Migliano (2022), "Websites Blocked in Russia Since Ukraine Invasion", *Top10VPN*, 21 juni: <https://www.top10vpn.com/research/websites-blocked-in-russia/> [2022-06-30].

⁴¹ Feldstein, *Government Internet*, s. 12.

⁴² Med VPN kan en användare dölja sin IP-adress, men det är inget hundra procentigt skydd mot att bli identifierad. Triangulering av andra parametrar, som operativsystem, datormodell, kakor och så vidare, utgör digitala fingeravtryck som kan användas för att avslöja vem som sitter bakom ett tangentbord. Det förefaller även som att allt fler ryska medborgare letar sig ut på *Dark Web* för o censurerad kommunikation och information. *Dark Web* är ett paraplybegrepp för en rad olika mörka nätverk, vilket

Stater som Iran, Ryssland och Kina har dessutom uttryckt ambitioner och tagit steg för att förverkliga ett autonomt internet (så kallat *splinternet*), det vill säga ett internet avskuret från det globala internet.⁴³ Det kinesiska företaget Huawei arbetar exempelvis med att utveckla en decentraliserad internetinfrastruktur (DII), som kan konkurrera med rådande standarder för dataöverföring.⁴⁴ Regionala nätverk styrda av auktoritära stater kan leda till ett mer toppstyrt och lättkontrollerat nätverk än det globala internet. Under det ryska invasionskriget av Ukraina visar sig detta bland annat i Rysslands försök att ta kontroll över den fysiska och digitala infrastrukturen för att på så vis ta kontroll över informationsflöden.⁴⁵

Det är dock inte enbart auktoritära stater som ser fördelar i att skapa regionala former av internet. Sedan 2020 har frågan om ”digital suveränitet” hamnat på agendan för EU.⁴⁶ Fokuset skiljer sig dock från exempelvis Kina och Ryssland. Inom EU diskuteras frågan bland annat i relation till att säkra digital infrastruktur från antagonistiska aktörer, att utveckla en konkurrenskraftig digital industri samt att värna om medborgares tillgång till fri information.

Inom den privata sektorn finns det både aktörer som arbetar för att värna om det fria internet och aktörer som ser fördelar med att begränsa fria flöden av information och data. Profitdrivna företag inom till exempel e-handel och strömmad underhållning söker på olika sätt utmanövra alternativa tjänster (lagliga som olagliga) och ta allt större marknadsandelar.⁴⁷

innebär att de är lokaliserade bortom det indexerade internet. En populär variant är TOR-nätverket som använder sig av *.onion*-adresser. Se: Connor Perrett (2022), ”Russia’s Internet Censorship Is Forcing Citizens to Turn to the Dark Web and VPNs for News, Social Media”, *Business Insider South Africa*, 17 mars: <https://www.businessinsider.co.za/what-happens-social-media-and-news-go-dark-in-russia-2022-3> [2022-07-17]. För en analys av populära tjänster, se: Yael Grauer (2022), *Security and Privacy of VPNs Running on Windows 10*, Consumer Reports och Digital Lab: <https://digital-lab-wp.consumerreports.org/2021/12/07/consumer-reports-digital-lab-evaluates-the-security-and-privacy-of-vpns-running-on-windows-10/> [2022-07-30]. Ett annat exempel från Ryssland är när internet stängdes i Moskva och Sankt Petersburg i samband med protester till stöd för Aleksej Navalnyj under januari 2021. Se: Woodhams och Migliano, ”Government Internet.”

⁴³ Om *splinternet*, se: Scott Malcomson (2016), *Splinternet: How Geopolitics and Commerce are Fragmenting the World Wide Web* (London och New York: OR Books). Om Ryssland, se: Anna Litvinenko (2021), ”Re-Defining Borders Online: Russia’s Strategic Narrative on Internet Sovereignty”, *Media and Communication* 9(4): 5-15; Carolina Vendil Pallin (2022), *Rysslands inte så suveräna internet och kriget i Ukraina*, FOI Memo 7925, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI%20Memo%207925> [2022-09-15].

⁴⁴ Se: Hoffmann, Lazanski och Taylor”, Standardising the Splinternet.”

⁴⁵ Rapporter från kriget visar att ukrainska aktörer, som motverkan, har förstört fysisk infrastruktur i regioner som är på väg att förloras. Se: Roman Shemakov (2022), ”War in Ukraine Is Fundamentally Changing the Relationship Between the Internet and Geopolitics”, *Global Voices*, 28 juli: <https://globalvoices.org/2022/07/28/war-in-ukraine-is-fundamentally-changing-the-relationship-between-the-internet-and-geopolitics/> [2022-08-07].

⁴⁶ Se: Julia Pohle (2020), *Digital Sovereignty. A New Key Concept of Digital Policy in Germany and Europe*, Konrad-Adenauer-Stiftung, Berlin: <https://www.econstor.eu/bitstream/10419/228713/1/Full-text-report-Pohle-Digital-sovereignty.pdf> [2022-08-20].

⁴⁷ Malcomson, *Splinternet*, s. 140-152.

Den digitala informationsmiljön befinner sig otvivelaktigt i skärningspunkterna av stormaktsrivalitet, geoekonomi och teknikutveckling som sannolikt kommer att styra utvecklingen in på okända vägar.⁴⁸ Hur framtidens internet kommer att se ut är svårt att slå fast. Om något är kommunikationsminister Uusmanns uttalande en påminnelse om att vara ödmjuk och vidsynt inför den framtida utvecklingen.⁴⁹

2.2 Kampen om de nya plattformarna

”Vår planet har aldrig varit så liten som den är nu. Givet den snabbt ökande pulsen av både fysisk och verbal kommunikation har den krympt – relativt sett så klart. Vi har pratat om det här förut, men aldrig på just det här sättet. Vi har aldrig pratat om det faktum att vem som helst... på endast några minuter kan lära sig vad jag gör, vad jag vill eller vad jag skulle vilja göra.”⁵⁰

Citatet kommer från en essä av den ungerske författaren Frigyes Karinthy. I essän elaborerar Karinthy med hypotesen om sex handslag (*six degrees of separation*), alltså att han skulle kunna finna en koppling till vilken person han än kunde komma på i sex steg eller mindre. För Julius Caesar eller aztekerna hade detta varit omöjligt. I en tid då människan visste mindre om en annan kontinent än vad vi i dag vet om mars hade de inte kunnat finna relationer till människor på andra kontinenter ens med 300 steg, skriver Karinthy. I essän beskriver Karinthy en fascination och fasa för en ny värld som på en och samma gång expanderar och krymper. Karinthys essä publicerades 1929.

Nästan 70 år senare, 1997, startade den amerikanske entreprenören Andrew Weinreich företaget och webbsidan SixDegrees.com. Han föreställde sig en digital plattform där alla användare kunde indexera sina sociala relationer. SixDegrees hade som mest 3,5 miljoner användare men såldes redan två år efter sin start och lades ner år 2000.⁵¹ Samma år sprack den uppblåsta it-bubblan och tilltron till it-branschen ruckades, för en stund. Kort därefter började en ny generation av unga it-entreprenörer att träda fram. De hade växt upp i tandem med populariseringen av

⁴⁸ Diesen, *Great Power*, s. 43.

⁴⁹ Nya tekniska lösningar förändrar ständigt förutsättningar och möjligheter. Under det pågående kriget i Ukraina har exempelvis den ukrainska tillgången till internet kompletterats genom StarLink, en satellitbaserad internetjänst från SpaceX. Upprätthållandet av internet har möjliggjort att både stridande och civila har kunnat dela bilder och information om vad som händer på marken. Se: Vivek Wadhwa och Alex Salkever (2022), ”How Elon Musk’s Starlink Got Battle-Tested in Ukraine”, *Foreign Policy*, 4 maj; <https://foreignpolicy.com/2022/05/04/starlink-ukraine-elon-musk-satellite-internet-broadband-drones/> [2022-07-15].

⁵⁰ Original. ”Planet Earth has never been as tiny as it is now. It shrunk—relatively speaking of course—due to the quickening pulse of both physical and verbal communication. This topic has come up before, but we had never framed it quite this way. We never talked about the fact that anyone on Earth, at my or anyone’s will, can now learn in just a few minutes what I think or do, and what I want or what I would like to do.” Frigyes Karinthy citerad i: Steven Levy (2020), *Facebook: The Inside Story* (New York: Blue Rider Press), s. 15.

⁵¹ Levy, *Facebook*, s. 15.

internet och personatorer. År 2004 registrerar Mark Zuckerberg domänen Facebook.com med ambitionen att inte bara skapa ett digitalt samhälle – han ville skapa en digital värld som speglade den verkliga.⁵² Grunden som hade lagts via internet och tidiga pionjärer solidifierades.⁵³ Globala sociala relationer, användargenererade digitala arkiv och encyklopedier som Wikipedia, fildelning via direktöverföring och ThePirateBay.org, en expanderande e-handel och en integrering av digitala nätverk i människans liv följde. De digitala plattformarnas tid var här.

Sociala medieplattformar är av särskilt intresse för informationsmiljöns utveckling. Sociala medier är i grund och botten internetbaserade och digitala plattformar som möjliggör skapande och utbyte av användargenererade data.⁵⁴ Sociala medier är dock inga neutrala kommunikationsmedier, utan resultaten av tekniska förutsättningar och deras grundares ideologiska visioner.⁵⁵

Det finns i dag en mängd olika sociala medieplattformar, alla med sina specifika karaktärsdrag, funktioner och tilltänkta målgrupper. I genomsnitt använder en internetanvändare sju olika sociala medieplattformar under en månad och i skrivande stund är de mest använda plattformarna globalt (i fallande ordning) Facebook, YouTube, WhatsApp, Instagram, WeChat och TikTok.⁵⁶ De större sociala medieplattformarna är i det närmaste globala och har en mångfald av användare. Andra plattformar är populära hos en specifik samhällsgrupp eller i en särskild kontext. Det handlar exempelvis om generationsaspekter (där vissa plattformar är mer populära bland yngre och vice versa), könsskillnader och kulturella och politiska kontexter, liksom tillgången till internet i stort.⁵⁷

⁵² Singer och Brooking, *LikeWar*, s. 42.

⁵³ Innan Facebook och under Facebooks tidiga år fanns en lång rad alternativ. Myspace var det första digitala sociala nätverket att nå en global publik och i Sverige dominerade Lunarstorm med sina 1,2 miljoner användare. För en diskussion om dessa och andra exempel, se: Simeon Edosomwan, Sitalaskshmi Kalangot Prakasan, Doriane Kouame, Jonelle Watson och Tom Seymour (2011), "The History of Social Media and its Impact on Business", *The Journal of Applied Management and Entrepreneurship* 16(3): 79-91.

⁵⁴ En generell definition: "Social Media is a group of Internet-based applications...that allow the creation and exchange of user generated content." Andreas M. Kaplan och Michael Haenlein (2010), "Users of the World, Unite! The Challenges and Opportunities of Social Media", *Business Horizons* 53: 59-68.

⁵⁵ Kenneth Boyte (2017), "An Analysis of the Social-Media Technology, Tactics, and Narratives Used to Control Perception in the Propaganda War Over Ukraine", *Journal of Information Warfare* 16(1): 88-111, s. 88.

⁵⁶ Kemp, "Global Social Media Statistics."

⁵⁷ Globalt sett är det fler män än kvinnor som använder sociala medier och det finns stora skillnader världen över. I Sydasiens är skillnaden som mest påtaglig, där männen står för 71 procent av den totala användningen av sociala medier. I Västafrika och Västasien/Mellanöstern är också skillnaden mellan kvinnlig och manlig användning av sociala medier betydande. Majoriteten av de personer globalt som inte har tillgång till internet är kvinnor och flickor, och även här finns betydande geografiska skillnader i hur jämställd tillgången mellan könen är. Se: International Telecommunication Union (2022), *Global Connectivity Report 2022*, ITU Publications, Genève: <https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/> [2022-08-05]; Simon Kemp (2021), "Social Media Users", *Datareportal*: <https://datareportal.com/social-media-users> [2022-07-01].

De sociala medieplattformarnas bakomliggande teknik påverkar inte bara användarupplevelsen utan också vilken typ av innehåll som har lättare att spridas och bli populärt (viralt) på den specifika plattformen.⁵⁸ De mer meddelandebaserade plattformarna, som WhatsApp och Telegram, är relativt enkla, där avsändare skickar direktmeddelanden till varandra eller deltar i användargrupper där upplagda meddelanden kan läsas kronologiskt. De mer samhällsorienterade (*community based*) plattformarna som Facebook, Twitter och TikTok bygger, utöver basala direktmeddelandefunktioner, på att genom automatiserade funktioner förse användaren med innehåll. En optimistisk tolkning är att användare förses med innehåll som denne vill ha. En mer pessimistisk är att användare förses med innehåll som håller dem kvar på plattformarna enligt den enkla devisen ju fler användare som stannar på en plattform, desto större potential för exponering av reklam (för vidare diskussion se kapitel 3).

Automatiserade funktioner bygger i dag till stor del på algoritmer. Inom datorprogrammering åsyftar algoritmer instruktioner som löser specifika problem. Datorprogram och automatiserade funktioner består i regel av en mängd olika algoritmer.⁵⁹ I tilltagande grad blir de en integrerad del av allt från storindustri, börshandel, medicin och arbetsmarknad till, för den som vill, matlagning.⁶⁰ På flera av de stora sociala medieplattformarna bidrar algoritmer till att styra flöden av innehåll, vilket innebär att de i viss mån avgör vad en användare konsumerar för typ av information. De kan således förstås som agendasättare som påverkar användares val, preferenser och handlingar.⁶¹ Oavsett är algoritmer skapade av människor, med matematik och programmering, samt utvecklas med mänskligt beteende som träningsdata. Det betyder att mänskligt beteende, fördomar, missuppfattningar, intressen, preferenser och så vidare både kan skrivas in i algoritmer och förstärkas genom träningsdata, och således bli en påverkande del i denna automatisering.⁶²

Givet deras makt är det slående hur lite som fortfarande är känt om algoritmerna och människorna bakom dem. Det finns en dubbelsidighet kring algoritmernas makt. Samtidigt som algoritmbaserade lösningar säljs in som mer objektiva, snabba och kostnadseffektiva än mänskliga, kan algoritmers misslyckanden att leva upp till

⁵⁸ Om viralt innehåll och sociala medier, se: Singer och Brookings, *LikeWar*, s. 118-147. Om viral marknadsföring, se: Itai Himelboim och Guy J. Golan (2019) "A Social Networks Approach to Viral Advertising: The Role of Primary, Contextual, and Low Influencers", *Social Media + Society* 5(3): 1-13.

⁵⁹ Se vidare: Jenna Burrell och Marion Fourcade (2021), "The Society of Algorithms", *Annual Review of Sociology* 47: 213-37.

⁶⁰ Om automatisering, algoritmer och samhällsutveckling, se: Marc Schuilenburg och Rik Peeters, red. (2021), *The Algorithmic Society: Technology, Power, and Knowledge* (London och New York: Routledge).

⁶¹ Svensson, *Wizards of the Web*, s. 14.

⁶² För en genomgående diskussion och analys, se: Cathy O'Neil (2016), *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York: Crown).

utlovad effekt rättfärdigas med den mänskliga faktorn. En central fråga blir således om algoritmer kan hållas ansvariga om felen ligger i deras design.⁶³

Zuckerbergs vision om att skapa ett digitalt socialt nätverk som inte bara kopplade samman människor utan speglade den verkliga världen är redan förlegat. Sociala mediealgoritmer speglar inte verkligheten – de är i allra högsta grad delaktiga i att skapa den, med alla sina mänskliga fel och brister.⁶⁴

Utöver de stora sociala medieplattformarna finns i dag ett i det närmaste oöverskådligt utbud med stor variation i det som erbjuds. Vissa garanterar krypterad information medan andra säger sig värna det fria ordet genom att garantera öppen men anonym debatt. Sedan internets tidiga dagar har det funnits plattformar som ligger utanför storpublikens blickfång. Det tog till exempel relativt lång tid innan så kallade krypterade tjänster som Encrochat och bildtavlor (*imageboards*) som 2chan, 4chan, 8chan (i dag 8kun) och KiwiFarms nåddes av det offentliga strålkastarljus. Sammanhangen genom vilka de har blivit kända är brottslighet, politisk extremism och konspirationsteorier. Dagens breda utbud innebär att envar kan finna sitt eget digitala samhälle, vilket i sin tur har gett upphov till en bred palett av olika medieekologier med specifika sociala och kulturella koder.⁶⁵

Vid sidan av de digitala plattformarnas expansion har det skapats en stor variation av nya aktörer: hackers som både skapar och förstör digital infrastruktur;⁶⁶ troll som använder sociala medier för att provocera, påverka och hänga ut användare;⁶⁷ svärmarbetande (*crowdsourcing*) användare som driver opinionsfrågor, konspirationer, gör prediktioner och bildar it-arméer;⁶⁸ och influerare (*influencers*) som har följarskaror som trumfar de stora traditionella mediernas följare i miljontal.⁶⁹

⁶³ Resonemang parafraaserat från: Svensson, *Wizards of the Web*, s. 14-15.

⁶⁴ Svensson, *Wizards of the Web*, s. 16.

⁶⁵ Om alternativa plattformar och den så kallade *alt-tech*, se: Joan Donovan, Becca Lewis och Brian Friedberg, (2019), "Parallel Ports: Sociotechnical Change from the Alt-Right to Alt-Tech", i *Post-Digital Cultures of the Far Right: Online Actions and Offline Consequences in Europe and the US*, red. Maik Fielitz och Nick Thurston (Bielefeld: Transcript), 49-65. Om medieekologier, se: Per-Erik Nilsson (2021), *Från skitpostning till folk mord: ensamagerande våldsvarkare, ideologi och accelerationism i den digitala tidsåldern*, FOI-R--5257--SE, Totalförsvarets forskningsinstitut, Stockholm.

⁶⁶ Se: Patrick Burkart och Tom McCourt (2019), *Why Hackers Win: Power and Disruption in the Network Society* (Oakland: University of California Press).

⁶⁷ Se: Clint Watts (2018), *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News* (New York: Harper-Collins), s. 79-100.

⁶⁸ Se: Daren C. Brabham (2013), *Crowdsourcing* (Cambridge och London: The MIT Press).

⁶⁹ Definition av influencer: "One form of microcelebrities who document their everyday lives from the trivial and mundane, to exciting snippets of the exclusive opportunities in their line of work. Influencers are the shapers of public opinion who persuade their audience through the conscientious calibration of personae on social media, as supported by 'physical' space interactions with their followers in the flesh to sustain their accessibility, believability, emulatability, and intimacy—in other words, their 'reliability'." Crystal Abidin och Mats Ots citerade i: Brandi Watkins (2021), "Introduction", i *Research Perspectives on Social Media Influencers and their Followers*, red. Brandi Watkins, (Lanham, Boulder, New York och London: Lexington Books), 1-6.

Möjligheten för riktad och skräddarsydd marknadsföring är stor och sammanblandningen mellan underhållning och kommersiella intressen är i dag troligtvis större än någonsin.⁷⁰

Den digitala informationsmiljöns utveckling och särskilt sociala medier har inneburit stora förändringar i hur människor konsumerar information, inte minst nyheter. Relativt få aktörer utgjorde tidigare journalistikens grindvakter och avgjorde vem som fick höras och på vilka villkor.⁷¹ Alternativ fanns men de var begränsade i sin räckvidd. I och med internet och teknisk utveckling har relationen mellan konsument och producent förändrats och informationsmiljön har utvecklats till att innehålla i det närmaste oändliga alternativ. Det som idag motsvarar dåtidens piratradio har en potentiellt global räckvidd genom poddradion och vem som helst kan starta sin egen alternativa nyhetskanal på någon av de många digitala plattformarna.⁷² Barriärerna för att göra sin röst hörd i det offentliga samtalet har blivit lägre,⁷³ på gott och ont (se vidare diskussion i kapitel 3).

Nyhetsmedielogiken har förändrats, digitaliserats, anpassat sig och även drivit på förändringen.⁷⁴ I dag uppger närmare hälften av den amerikanska befolkningen att de konsumerar nyheter via sociala medier ofta (19 procent) eller ibland (29 procent).⁷⁵ I Sverige syns liknande mönster, dock med stora generationsskillnader.⁷⁶

⁷⁰ Om influencers och marknadsföring, se: Daniel Belanche, Luis V. Casalo, Marta Flavián och Sergio Ibáñez-Sánchez (2021), "Understanding Influencer Marketing: The Role of Congruence Between Influencers, Products, and Consumers", *Journal of Business Research* 132: 186-195; Ronda Mariani (2020), "Evaluation of Brand-Sponsored Influencers and Tactics Across Industries", i *Research Perspectives on Social Media Influencers and their Followers*, red. Brandi Watkins (Lanham, Boulder, New York och London: Lexington Books), 65-86.

⁷¹ Se: Peter Bro och Filip Wallberg (2014), "Digital Gatekeeping", *Digital Journalism* 2(3): 446-454. För en analys hur journalistiken anpassas till de nya förhållandena, se: Patrick Walters (2021), "Reclaiming Control: How Journalists Embrace Social Media Logics While Defending Journalistic Values", *Digital Journalism* [online first]: 1-20.

⁷² Om poddradion som ljudmedium och dess utveckling, se: Jemily Rime, Chris Pike och Tom Collins (2022), "What is a podcast? Considering Innovations in Podcasting Through the Six-Tensions Framework", *New Media Technologies* [online first]: 1-23.

⁷³ Jesper Strömbäck, Åsa Wikforss, Kathrin Glüer, Torun Lindholm och Henrik Oscarsson (2022), "Introduction: Toward Understanding Knowledge Resistance in High-Choice Information Environments", i *Knowledge Resistance in High-Choice Information Environments*, red. Jesper Strömbäck, Åsa Wikforss, Kathrin Glüer, Torun Lindholm och Henrik Oscarsson (London och New York: Taylor and Francis), 1-28.

⁷⁴ Se till exempel: Natalie Fenton (2010), "Drowning or Waving? New Media, Journalism, and Democracy", i *New Media, Old News*, red. Natalie Fenton (London och Thousand Oaks: Sage), 3-16; Steve Hill och Paul Bradshaw (2018), *Mobile-First Journalism: Producing News for Social and Interactive Media* (New York: Routledge); Jorge Vázquez-Herrero, María-Cruz Negreira-Rey och Xosé López-García (2020), "Let's Dance the News! How the News Media Are Adapting to the Logic of TikTok", *Journalism* [online first].

⁷⁵ Se: Mason Walker och Katerina Eva Matsa (2021), "News Consumption Across Social Media in 2021", Pew Research Center: <https://www.pewresearch.org/journalism/2021/09/20/news-consumption-across-social-media-in-2021/> [2022-08-01].

⁷⁶ I åldrarna 15–24 år konsumeras nyheter till 43 procent via Instagram, 37 procent via Facebook och 31 procent via YouTube. I åldrarna 24–44 år är siffrorna: Facebook 36 procent, SVT 31 procent, SR 31 procent och kvällstidning 30 procent. I åldrarna 45–64 år: SVT 60 procent, SR 49 procent, TV4 43 procent och morgontidning 41 procent. Slutligen, i åldrarna 75–79 år: SVT 81 procent, SR 61 procent,

Ett resultat av sociala mediers tilltagande dominans i nyhetsrapportering är tendensen att endast rubriker och korta, lättsmälta nyhetsslag premieras, samtidigt som urvalet av nyheter i viss mån är styrt av algoritmer.⁷⁷

Ett förändrat utbud av nyheter har även inneburit förändrade relationer mellan konsument och producent. I en tid då var och en med handhållna enheter och grundläggande it-kunskaper kan producera, eller åtminstone förment imitera, kvalitativ journalistisk kan gränserna mellan källa, konsument och producent suddas ut (för vidare diskussion om propaganda och desinformation, se kapitel 3).⁷⁸

Snabbheten i spridandet av användargenererade data och information via digitala plattformar som sociala medier innebär även att de i otaliga fall når konsumenten långt mycket snabbare än traditionella medier. Att vara först innebär möjlighet till agendasättande.⁷⁹ De närmast obegränsade vägarna att ta del av information från ett oändligt antal källor och traditionella medier som tävlar med nya informationskanalers snabbhet ställer högre krav på medborgare och beslutsfattare att värdera information. Källkritik och mediekunskap, så kallad digital läskunnighet, lyfts inom forskningen som en alltmer viktig angelägenhet, minst lika mycket för beslutsfattare som för den gemene medborgaren.⁸⁰

Digital läskunnighet handlar om att förstå den digitala informationsmiljöns kommunikativa förutsättningar. Viss forskning pekar på att det är ett viktigt verktyg för att stärka motståndskraften mot desinformation samt vilseledande och falsk

TV4 59 procent och morgontidning 56 procent. Catharina Bucht (2021), *Mediebarometern: Tema Generationer*, Nordicom, Göteborg, s. 27, 38, 48 och 59:

<https://www.nordicom.gu.se/sv/publications/mediebarometern-2019-tema-generationer> [2022-08-05].

⁷⁷ Jesper Strömbäck, Hajo Boomgaarden, Elena Broda, Alyt Damstra, Elina Lindgren, Yariv Tsfati och Rens Vliegthart (2022), "From Low-Choice to High-Choice Media Environments – Implications for Knowledge Resistance", i *Knowledge Resistance in High-Choice Information Environments*, red. Jesper Strömbäck, Åsa Wikforss, Kathrin Glüer, Torun Lindholm och Henrik Oscarsson (London och New York: Taylor and Francis), 49-68, s. 53.

⁷⁸ Om fejkade nyheter, begreppsdefinitioner och forskningsläge, se: Ali Khan, Kathryn Brohman och Shamel Addas (2022), "The Anatomy of 'Fake News': Studying False Messages as Digital Objects", *Journal of Information Technology* 37(2): 122-143.

⁷⁹ Om agendasättande och sociala medier, se: Pablo Barbera, Andreu Casas, Jonathan Nagler, Patrick J. Egan, Richard Bonneau, John T. Jost och Joshua A. Tucker (2019), "Who Leads? Who Follows? Measuring Issue Attention and Agenda Setting by Legislators and the Mass Public Using Social Media Data", *American Political Science Review* 113(4): 883-901; Fabrizio Gilardi, Theresa Gessler, Maël Kubli och Stefan Müller (2022), "Social Media and Political Agenda Setting", *Political Communication* 39(1): 39-60.

⁸⁰ Inom svenskspråkig forskning används ofta begreppet digital litteracitet, från engelskans *digital literacy*. Bristen på digital läskunnighet blev till exempel iögonfallande tydlig av hur lite amerikanska beslutsfattare förstod vad sociala medier är under utfrågningen av Zuckerberg i Kongressen 2018. Se: Diesen, *Great Power*, s. 192; Emily Stewart (2018), "Lawmakers Seem Confused About What Facebook Does — And How to Fix It", *The Guardian*, 10 april: <https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations> [2022-07-14].

information,⁸¹ medan annan forskning indikerar att digital läskunnighet inte har någon påverkan på själva spridandet av desinformation och falskheter.⁸²

Även om det är användarna som i huvudsak skapar innehållet på digitala plattformar är det andra aktörer som styr och äger infrastrukturen. Företagen som äger plattformarna och den underliggande infrastrukturen är, som understrukits, en del av en profitdriven logik och ekonomisk storpolitik. Bakom de digitala plattformarna (sociala medier, sökmotorer, kommunikationstjänster och så vidare) står it-bolag som kinesiska ByteDance och Tencent och amerikanska Alphabet, Meta och Twitter. Företagens ställningstaganden, reglering av innehåll, ägandeförhållanden och relationer till statliga intressen påverkar miljarder människors dagliga liv. I många fall är det bolagens egna regelverk och kontrollinstanser som reglerar innehållet på plattformarna, vilket ger dem stor makt i det offentliga samtalets utformande. It-bolagen som står för övergripande infrastruktur har även makt att styra över andra digitala plattformar av mindre storlek. Efter stormningen av Kapitolium i Washington DC beslutade exempelvis Amazon, Apple och Google att sluta tillhandahålla sociala medieplattformen Parler med förevändningen att den stred mot användarvillkor som förbjöd uppvigling till våld.⁸³ Av liknande anledning stängde Twitter president Donald Trumps konto på plattformen.⁸⁴

Här spelar samhällsklimat och samhällssystem som de digitala plattformarna verkar i en stor roll. I ett marknadsliberalt och demokratiskt samhälle är det lagar, regler och folklig opinion som direkt eller indirekt reglerar bolagens manöverutrymme. Monopolliknande strukturer och opportunistik kan dock innebära att det är svårt att väga rättsstatliga principer mot opinionsdriven opportunistik. I auktoritära stater är bolagen ofta tätt sammanflätade med den politiska makten varför gränserna mellan företagens och statens intressen är långt ifrån självklara.⁸⁵

⁸¹ Andrew M. Guess, Michael Lerner, Benjamin Lyons, Jacob M. Montgomery, Brendan Nyhan, Jason Reifler, and Neelanjan Sircar (2020), "A Digital Media Literacy Intervention Increases Discernment Between Mainstream and False News in the United States and India", *PNAS* 117(27): 15536-15545.

⁸² Nathaniel Sirlin, Ziv Epstein, Antonio A. Arechar och David G. Rand (2021), "Digital Literacy Is Associated with More Discerning Accuracy Judgments but not Sharing Intentions", *Harvard Kennedy School Misinformation Review* 2(6): 1-13. För vidare diskussion, se: Ola Svenonius, Elsa Isaksson och Johannes Lindgren (2022), *Countering Mis- and Disinformation: A Narrative Review of Reactive Measures*, FOI-R--5263--SE, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--5263--SE> [2022-09-15].

⁸³ Brian Fung (2021), "Parler Has now Been Booted by Amazon, Apple and Google", *CNN Business*, 11 september: <https://edition.cnn.com/2021/01/09/tech/parler-suspended-apple-app-store/index.html> [2022-08-05].

⁸⁴ Kate Konger och Mike Isaac (2021), "Twitter Permanently Bans Trump, Capping Online Revolt", *The New York Times*, 12 januari: <https://www.nytimes.com/2021/01/08/technology/twitter-trump-suspended.html> [2022-08-02].

⁸⁵ Om kinesiska statens relationer med kinesiska teknikbolag, se: Paul Charon och Jean-Baptiste Jeangène Vilmer (2021), *Chinese Influence Operations: A Machiavellian Moment*, Institut de Recherche Stratégique de l'Ecole Militaire, Paris: <https://www.irsem.fr/report.html> [2022-07-11].

Den grundläggande affärsmodellen för företag som bygger på användardata är en expanderande och asymmetrisk återkopplings slinga (*feedback loop*). Ju mer integrerade digitala plattformar blir i det vardagliga livet, desto mer beroende av dem blir människor. Ju större del av den digitala marknaden, desto större makt. Företagen är dock beroende av användare för att å ena sidan sälja sina produkter, å andra sidan få tillgång till deras data för att vidareutveckla de digitala plattformarna och bli än mer precisa i att rikta reklam och behålla användare på den ena eller andra plattformen.⁸⁶

Data har kommit att omtalas som den nya oljan som likt den tidiga oljeboomen har gett upphov till en ny marknad.⁸⁷ I själva verket är de digitala plattformarna inte ens huvudsyftet i många bolags affärsmodeller, utan just de användardata de genererar. Data har blivit en strategisk resurs för att träna algoritmer vars användningsområden sträcker sig långt bortom att få användare på Facebook eller TikTok att köpa choklad, smink eller en ny bil.

I denna aspekt har så kallade privata informationsmäklare (*data brokers*) kommit att få en alltmer central roll. Informationsmäklare samlar in data och information från användare för att sedan sälja dem vidare till en tredje part. Innan internets genomslag handlade detta ofta om persondata från offentliga register. I dag samlas i det närmaste oöverskådliga mängder data och digital information från internets användare in, bland annat från de stora digitala plattformarna och via så kallade kakor (*cookies*) som kan användas för att spåra webbanvändande. Många enskilda användare surfar på webben och gillar inlägg på diverse plattformar i ovetskap om att deras digitala trafik och användardata lagras. Aggregerade data och information (*big data*) är, utöver att träna algoritmer, ett viktigt verktyg för att utveckla metoder för skydd och verkan i informationsmiljön, men informationsindustrin rör sig inte sällan i en laglig gråzon.⁸⁸

Ett exempel på detta är det amerikanska företaget Team Cymru. Företaget säger sig övervaka över 90 procent av internets trafik. En del i affärsmodellen är att de delges data av aktörer som utgör den fysiska och digitala infrastrukturen i informationsmiljön, för att i gengäld upptäcka och avvärja hot mot infrastrukturen. En visselblåsare har via nyhetsmedia dock varnat för att Cymru inte endast lagrar aggregerade data och information, utan detaljerade persondata med metoder som exempelvis kringgår VPN (via så kallade *netflow data*). Några av deras kunder är

⁸⁶ Se: Directorate for Financial and Enterprise Affairs (2016), *Big Data: Bringing Competition Policy to the Digital Era*, DAF/COMP 2016/14, Organisation for Economic Co-operation and Development (OECD), s. 10: [https://one.oecd.org/document/DAF/COMP\(2016\)14/en/pdf](https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf) [2022-08-05].

⁸⁷ The Economist (2017), "Data is Giving Rise to a New Economy", 6 maj: <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy> [2022-08-09].

⁸⁸ Se vidare: Henrik Twetman och Gundars Bergmanis-Korats (2020), *Data Brokers and Security: Risks and Vulnerabilities Related to Commercially Available Data*, NATO Strategic Communications Centre of Excellence, Riga: https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf [2022-09-23].

amerikanska polisiära och militära myndigheter vars hantering och användande av den här typen av data och information är oklar, vilket i USA har väckt frågor om personlig integritet och ytterligare lagstiftning för att skydda den.⁸⁹

Ett annat relaterat exempel är skandalen kring dataanalysföretaget Cambridge Analytica som uppdagades 2016. Genom att samla användardata från närmare 87 miljoner Facebookanvändare skapade företaget psykologiska profiler som inkluderade karaktärsdrag och personliga egenskaper. Informationen användes sedan som underlag för att skapa riktade annonser, bland annat i den amerikanska presidentvalskampanjen och Brexitomröstningen 2016.⁹⁰ Användares data blev här, utan användarnas vetskap eller egentliga medgivande, en faktor i avgörande politiska skeenden.

Givet den enorma mängd persondata som finns på olika digitala plattformar sker påtryckningar från statliga aktörer att tillhandahålla data, i såväl brottspreventiva syften som i övervakningssyften. I USA har exempelvis den federala polisen (FBI) sökt tillgång till data från bland annat Facebook och Twitter för att proaktivt upptäcka hot mot nationell säkerhet.⁹¹ Den ryska sociala medieplattformen VK (en rysk variant av Facebook) har utsatts för påtryckningar om att dela de privata data de har sagt att de ska skydda. I VK:s fall handlade det om att den ryska federala säkerhetstjänsten 2013 efterfrågade data om ukrainska användare som protesterade mot den proryske presidenten Viktor Janukovyč.⁹² I skrivande stund har det uppdagats att TikTok har delgett amerikanska persondata till aktörer i den kinesiska staten.⁹³

En grundläggande problematik som omgärdar de digitala plattformarna, it-bolagen och deras relationer till statliga aktörer är transparens – transparens om algoritmers utformning, transparens om hantering av persondata och transparens om vad som

⁸⁹ Se: Joseph Cox (2022), "Revealed: US Military Bought Mass Monitoring Tool That Includes Internet Browsing, Email Data", *Motherboard: Vice*, 21 september: <https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data> [2022-09-23].

⁹⁰ Se: Carole Cadwalladr och Emma Graham-Harrison (2018), "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach", *The Guardian*, 17 mars: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> [2022-07-30]; Alexandra Ma och Ben Gilbert (2019), "Facebook Understood how Dangerous the Trump-Linked Data Firm Cambridge Analytica Could Be much Earlier than It Previously Said. Here Is Everything that's Happened Up until Now", *Business Insider*, 23 augusti: <https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3?r=US&IR=T> [2022-06-29].

⁹¹ Jeff Horwitz och Dustin Volz (2019), "FBI Surveillance Proposal Sets Up Clash With Facebook", *The Wall Street Journal*, 8 augusti: https://www.wsj.com/articles/fbi-and-facebook-potentially-at-odds-over-social-media-monitoring-11565277021?mod=hp_lead_pos1 [2022-08-01].

⁹² Thomas Brewster (2022), "Telegram's Billionaire Found Says He's Never Provided Ukrainians' Data to Russia", *Forbes*, 7 mars: <https://www.forbes.com/sites/thomasbrewster/2022/03/07/telegrams-billionaire-founder-says-hes-never-provided-ukrainians-data-to-russia/> [2022-07-17].

⁹³ Alex Barinka (2022), "TikTok Confirms Some China-Based Employees Can Access US User Data", *Bloomberg*, 1 juli: <https://www.bloomberg.com/news/articles/2022-07-01/tiktok-says-some-china-based-employees-can-access-us-user-data> [2022-07-05].

delas och i vilka syften.⁹⁴ Som exempel kan en extern forskare med tillgång till Twitters applikationsprogrammeringsgränssnitt (API) med enkla medel få mer än 30 informationspunkter på ett enskilt meddelande som bland annat rör geolokalisering, språk, använd enhet, följare och vilka som gillat meddelandet. Medan forskare hålls till strikta etiska riktlinjer och lagar för att skydda persondata kan denna typ av data med lätthet användas för att kartlägga individer. Det kan således antas att i takt med att plattformarnas användningsområden expanderar, expanderar även it-bolagens möjlighet till att samla in data som kan användas för att bland annat analysera och kartlägga informationsspridning under krig, men även identifiera individer och förfina strategier och teknik i propagandistiska syften.

De digitala plattformarna, i synnerhet sociala medier, har likt internets infrastruktur blivit en del av stormaktsrivalitetens återkomst och rör frågor som kontroll av teknisk utveckling och informationskontroll.⁹⁵ Ett exempel är USA:s hållning gentemot de kinesiska sociala medieplattformarna TikTok (ByteDance) och WeChat (Tencent). Dessa förbjöds av president Donald Trump genom en presidentorder 2020. I den hänvisas till datasäkerhet och dataintegritet på grundval av att användargenererade data kan användas i antagonistiska syften som spionage och utpressning, inte minst mot den kinesiska diasporan i USA.⁹⁶ När president Joe Biden tillträdde upphävdes förbudet men Bidenadministrationen betonade samtidigt att översyn av utländskt ägda plattformar fortsatt skulle tillämpas.⁹⁷ Diskussioner om

⁹⁴ Se: Frank Pasquale (2015), *Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge och London: Harvard University Press), s. 61-80.

⁹⁵ Spänningen mellan delar av Väst och Kina är även framträdande i diskussioner kring Huawei och företagets vilja att investera i olika typer av it-infrastruktur. I bland annat Sverige, USA, Storbritannien och Australien har det handlat om nationella 5G-nät. I Sverige motiverades beslutet att utestänga Huawei från det svenska 5G-nätet med att Huaweis ägarstruktur gör att företaget bedöms ha starka drivkrafter att agera i överensstämmelse med kinesiska statliga mål och det styrande kommunistpartiets nationella strategier. Det hänvisades också till Säkerhetspolisens bedömning att den kinesiska partistaten och underrättelsetjänsten kan utöva påtryckningar mot Huawei. De amerikanska handelssanktionerna gentemot företaget bedömdes sannolikt kunna innebära svårigheter för företaget att på sikt tillhandahålla nödvändiga produkter. Utestängningen av ZTE, ett annat kinesiskt teknologiföretag, motiverades på liknande sätt. Huawei överklagade PTS:s beslut men i juni 2022 meddelade kammarrätten i Stockholm att beslutet står fast. Se Kammarrätten (2022), *Dom i mål nr 5222-21*, Stockholm, 22 juni; Post- och telestyrelsen (2020), *Beslut 2020-10-20. Godkännande av sökande samt tillkommande villkor i auktion av frekvensbanden 3,5 GHz och 2,3 GHz*, Dnr: 18-8496, Stockholm; Tim Rühlig och Maja Björk (2020), *What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe*, UI Paper 2020/1, Utrikespolitiska institutet, Stockholm.

⁹⁶ Amerikanska företag och individer tilläts inte göra reklam på plattformarna och det var inte tillåtet att ladda ner programmen via amerikanska digitala kommersiella plattformar. Se: Geoffrey Gertz (2020), "Why Is the Trump Administration Banning TikTok and WeChat?", *Up front – Brookings*, 7 augusti: <https://www.brookings.edu/blog/up-front/2020/08/07/why-is-the-trump-administration-banning-tiktok-and-wechat/> [2022-06-30].

⁹⁷ Jeanne Whalen och Ellen Nakashima (2021), "Biden Revokes Trump's TikTok and WeChat Bans, but Sets Up a Security Review of Foreign-Owned Apps", *The Washington Post*, 9 juni: <https://www.washingtonpost.com/technology/2021/06/09/tiktok-ban-revoked-biden/> [2022-06-30].

att öka regleringen även av de stora amerikanska bolagen har tilltagit, i synnerhet vad gäller datahantering och deras monopolliknande andelar av den digitala marknaden.⁹⁸

Att medvetenheten om persondatas skyddsvärde har ökat de senaste åren är tydligt, och statliga aktörer har tagit steg för att lagstifta även bortom infrastruktur. EU-kommissionen har exempelvis föreslagit lagstiftning som ska reglera digitala tjänster inom EU. Ett av de två huvudmålen är att ”skapa en säkrare digital miljö i vilken fundamentala rättigheter för alla användare av digitala tjänster är skyddade”.⁹⁹ I syfte att stärka medborgares integritet har EU infört regleringar på detta område. Ett exempel är förordningen *General Data Protection Regulation* (GDPR) som antogs på EU-nivå 2016 och trädde i kraft 2018.¹⁰⁰

Det är för tidigt att utvärdera vilken effekt den typen av regional lagstiftning får på de tjänster som används i den gränslösa terräng som den nya digitala informationsmiljön utgör. De stora digitala plattformarna har dock dels på egen hand, dels på grund av extern påverkan från beslutsfattare såväl som användare, genomfört och väntas införa ett starkare skydd av persondata.¹⁰¹ En rad privata aktörer erbjuder och säljer tredjepartslösningar för att skydda den enskildes integritet i den digitala informationsmiljön med alltifrån webbläsare och krypterade meddelandetjänster till VPN.¹⁰² Vare sig kommersialiseringen av persondata eller riktade informationskampanjer är något nytt och inte heller kommersialiseringen av personlig integritet.¹⁰³ Däremot förefaller marknaden för båda dessa aspekter av

⁹⁸ Se: Cecilia Kang (2021), ”Lawmakers, Taking Aim at Big Tech, Push Sweeping Overhaul of Antitrust”, *The New York Times*, 29 juni: <https://www.nytimes.com/2021/06/11/technology/big-tech-antitrust-bills.html> [2022-08-05]; Wilson C. Freeman och Jay B. Sykes (2019), *Antitrust and Big Tech*, CBS Report R45910, Congressional Research Service, Washington, 11 september: <https://sgp.fas.org/crs/misc/R45910.pdf> [2022-08-05].

⁹⁹ Original: ”[To] create a safer digital space in which the fundamental rights of all users of digital services are protected.” Regleringen motiveras bland annat med risker för spridning av desinformation och att dagens digitaliserade samhälle och ekonomi har lett till att det finns några få plattformar (dvs. företag) som kontrollerar viktiga ekosystem i den digitala ekonomin. Dessa företag, menar kommissionen, har blivit grindvakter med makt att reglera vem och vilka som får delta. Se sammanfattning av resonemanget: Europakommissionen (2022), *The Digital Services Act Package*, 5 juli: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> [2022-07-11].

¹⁰⁰ Europaparlamentet och Europeiska rådet (2016), Förordning (EU) 2016/679, *Europeiska unionens officiella tidning*, 4 maj: L119/1-L119/88.

¹⁰¹ Under covidpandemin har sociala medieplattformars arbete med att identifiera och hindra desinformation och falskhet intensifierats. För en analys, se: Nandita Krishnan, Jiayan Gu, Rebekah Tromble och Lorien C. Abrams (2021), ”Research Note: Examining how Various Social Media Platforms have Responded to Covid-19 Misinformation”, *Harvard Kennedy School Misinformation Review* 6(2): 1-25.

¹⁰² Om privatliv som digital handelsvara, se: Stacy-Ann Elvy (2017), ”Paying for Privacy and the Personal Data Economy”, *Columbia Law Review* 117(6): 1369-1460.

¹⁰³ Se: Craig D. Tindall (2003), ”Argus Rules: The Commercialization of Personal Information”, *Journal of Law, Technology, & Policy* 1: 181-202.

persondata expandera markant, inte minst med privata aktörer som erbjuder avancerade analyser av öppna källor, faktakollar och analys av desinformation.¹⁰⁴

Sedan författaren Karinthus diagnos av det tidiga 1900-talets möjligheter för global kommunikation har hans ord blivit än mer sanna. Samtidigt pekar regionalisering av fysisk och digital infrastruktur samt ekonomiska och politiska intressen för att kontrollera informationsmiljön kopplat till de stora it-bolagens centraliserade plattformisering på att internets framtid som ett globalt nätverk är osäker.¹⁰⁵ Oavsett kommer detta i relation till nya tekniska utvecklingar och förändrade användarmönster sannolikt innebära att terrängen i den digitala informationsmiljön i morgon kommer att skilja sig från i dag.

2.3 Informationsmiljön och det nya kriget

Dagens digitala informationsmiljö består av ständigt nya nätverk, nya aktörer, nya plattformar och således nya förutsättningar, inte minst för konflikt och krig. Det moderna slagfältet har förändrats och digitaliserats. Kinetisk krigföring är fortfarande av stor vikt, men möjligheterna att bedriva krig via information har ökat. Gränserna mellan krig och fred samt civila och militära aktörer blir alltmer otydliga.¹⁰⁶

Inom forskningen och i doktrinutveckling har det utvecklats många olika begrepp för att konceptualisera dessa förändrade förhållanden i relation till krig och kon-

¹⁰⁴ Den så kallade privata OSINT-sektorn växer exempelvis genom olika produkter som erbjuds av stora mediebolag, säkerhetsföretag, icke-statliga organisationer och privatpersoner. För vidare diskussion, se: Quirine A. Eijkman och Daan Weggemans (2012), "Open Source Intelligence and Privacy Dilemmas: Is it Time to Reassess State Accountability?" *Security and Human Rights* 23(4): 285-296; Damien Van Puyvelde (2017), "Privatisation", i *The Palgrave Handbook of Security, Risk and Intelligence*, red. Robert Dover, Huw Dylan och Michael S. Goodman (London: Palgrave Macmillan), 297-314. För en översikt av aktörer i Europa, se: European Digital Media Observatory (2022), "Repository: Fact-Checking Initiatives in the EU (and in the UK)": <https://edmo.eu/fact-checking-activities/> [2022-08-08].

¹⁰⁵ En möjlig utveckling är att blockchaintechniken kommer att möjliggöra ett mer decentraliserat och mindre toppstyrt internet. Samtidigt kan en ökad plattformisering och monopolisering av fysisk och digital infrastruktur innebära en mer kontrollerad informationsmiljö. Lägg därtill stater som regionaliserar infrastrukturen för att kunna koppla att hårdare grepp om den. Se vidare: Massimo Ragnedda och Giuseppe Destefanis (2020), "Blockchain: A disruptive technology", i *Blockchain and Web 3.0: Social, Economic, and Technological Challenges*, red. Massimo Ragnedda och Giuseppe Destefanis (Oxon och New York: Routledge), 1-11; Pew Research Center (2019), "Experts Optimistic About the Next 50 Years of Digital Life": <https://www.pewresearch.org/internet/2019/10/28/experts-optimistic-about-the-next-50-years-of-digital-life/> [2022-08-08].

¹⁰⁶ För fullständigt resonemang, se: Isaac R. Porche III (2020), *Cyberwarfare: An Introduction to Information-Age Conflict* (Boston och London: Artech House), s. 10. En liknande problematik gäller juridiska definitioner av konflikt och krig. I den svenska regeringsformen är till exempel krig ytterst vagt definierat, vilket kan ses som en styrka i och med att den politiska makten och rättsapparaten är mer flexibel, samtidigt som gränserna på konfliktskalan blir otydliga. Se: Inger Österdahl (2021), "Krig eller fred: Om regeringsformens definition av krig", *Svensk Juristtidning* 105: 261-276.

flikt. De mest centrala är informations- och cyberkrig som en del av hybrid krigsföring.¹⁰⁷ Gråzonen har introducerats som ett koncept för att fånga utrymmet på konfliktskalan mellan krig och fred. I gråskalan är gränserna mellan civila och militära aktörer, kriminella handlingar och krigshandlingar allt svårare att dra.¹⁰⁸

Det här leder till viktiga frågor om existerande begreppsapparater, koncept och juridiska ramverk för att hantera den nya världen. I en värld där den digitala informationsmiljön är i det närmaste allomfattande, om informations- och cyberkrig inte alltid sker i öppen konflikt eller i krig, hur ska deras motsats – fred – förstås? Hur kan till exempel det skyddsvärda identifieras och avgränsas utan att hela, eller delar av, samhället stängs av och militariserar? Om gränserna mellan krig och fred suddas ut, hur ska statliga institutioner byggda för en annan tid hantera dem? Hur väl fungerar Clausewitz klassiska aktörsmodell i en tid när befolkningen, de styrande och militären alla kan vara både offer och deltagare i de nya informations- och cyberkrigen?¹⁰⁹

Den kontinuerliga uppluckringen av gränser, sammanflätningen av fenomen och koncept för att fånga detta är tydlig i diskussioner kring relationen mellan informationsmiljön och de konventionella krigsdomänerna land, sjö, luft, rymd och, på senare tid, cyber. De fyra första domänerna definieras av sin avgränsade geografi medan den sista, cyber, inte har någon. Den definieras i stället av en ständigt föränderlig informationsteknik. I och med att informationstekniken blir en alltmer integrerad del i de övriga domänerna har flertalet forskare och praktiker kommit att ifrågasätta den här uppdelningen.¹¹⁰

Av särskilt intresse för denna rapport är dock relationen mellan informationsmiljön och cyberdomänen. Medan informationskrigsföring är en mångtusenårig företeelse är cyberkrigsföring ny.¹¹¹ En generell definition av informationskrigsföring är att

¹⁰⁷ Om hybrid krigsföring, cyber och information, se: David Betz (2019), "The Idea of Hybridity", i *Hybrid Conflicts and Information Warfare*, red. Ofer Fridman, Vitaly Kabernik och James C. Pearce (Lynne Rienner Publishers: Boulder och London), 9-24.

¹⁰⁸ Allen och Gilbert, "Qualifying the Information", s. 39.

¹⁰⁹ Clausewitz modell bygger på tre aktörer: regeringen (politiken), folket (civilsamhället) och armén (militären). För vidare diskussion om konsekvenser krig, konflikt och informationsmiljön, se: Matthew Ford och Andrew Hoskins (2022), *Radical War: Data, Attention and Control in the Twenty-First Century* (London: Hurst Publishers), s. 6, 72 och 200.

¹¹⁰ Se: Cholpon Abdyaeva (2020), *Information Warfare Operations in the Cyber Domain*, OIIP - Austrian Institute for International Affairs: <https://www.oaip.ac.at/cms/media/107-working-paper-cyberspace-in-the-context-of-hybrid-warfare.pdf> [2022-08-08]; Allen och Gilbert, "Qualifying the Information"; Michael P. Kreuzer (2021), "Cyberspace is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age", *The Strategy Bridge*, 8 juli <https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age> [2022-07-14]; Porche III, *Cyberwarfare*, s. 26; Sergey Sanovich (2019), "Russia: The Origins of Digital Misinformation", i *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, red. Samuel C. Woolley och Philip N. Howard (Oxford och New York: Oxford University Press), 21-40.

¹¹¹ Christopher Whyte, A. Trevor Thrall och Brian M. Mazanec (2021), "Introduction", i *Information Warfare in the Age of Cyber Conflict*, red. Christopher Whyte, A. Trevor Thrall och Brian M. Mazanec (London och New York: Routledge), 1-10, s. 3.

det, i syfte att främja militär eller strategisk vinst, handlar om en medveten manipulering eller användande av information av en aktör mot en motståndare för att påverka de val och beslut som motståndaren gör.¹¹² Det ska dock understrykas att det i dag sker i en tid av cyberkrigföring. Inom ramen för informationskrigföring handlar cyberoperationer till stor del om digitaliserade data, medan informationsoperationer ofta gör det, men långt ifrån uteslutande. I informationskrigföring är informationen vapen – den är inte endast digital och rör människan både som individ och kollektiv. Metoder inom cyberkrigföring kan dock användas för att manipulera och komma åt information som sedan kan användas i antagonistiska syften.¹¹³

Offensiva cyberoperationer riktar sig mot datorbaserade nätverk för att på olika sätt störa nätverken eller för att samla dold information vars konsekvenser sträcker sig långt utanför den digitala världen. Det kan handla om att underminera en motståndares förmågor (civila som militära), slå ut kritiska funktioner och infrastruktur, samt spionage.¹¹⁴ Offensiva cyberattacker kan dock vara svåra att attribuera eftersom, som en forskare uttrycker det, skillnaden mellan cyberkrig, cyberspionage och cyberbrott ofta handlar om ett par tangentryck.¹¹⁵ Vidare är ett av syftena med många cyberoperationer att de utförs i det fördolda varför deras kommunikativa syfte inte är givet på förhand.¹¹⁶

¹¹² Original: "The deliberate manipulation or use of information by one party on an adversary to influence the choices and decisions that the adversary makes in order for military strategic gain." I: Whyte, Thrall och Mazanec, *Introduction*, s. 2.

¹¹³ Whyte, Thrall och Mazanec, *Introduction*, s. 1.

¹¹⁴ Ett av de mer kända och tidiga exemplen är USA:s och Israels attack mot den iranska uranriktningsanläggningen i Natanz som gick under namnet Stuxnet. Stuxnet var en så kallad mask, skadlig kod, som genom att spridas i anläggningens nätverk orsakade fysisk skada genom att, bland annat, göra att turbiner började spinna för fort och således slets ut. Se: David Albright, Paul Brannan och Christina Walrond (2010), *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*, Institute for Science and International Security (ISIS), 22 december: https://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf [2022-08-07]. Återkommande exempel på utförda cyberangrepp är exempelvis överbelastningsattacker (distributed denial of service, DDoS) och utpressningsattacker (ransomware). Överbelastningsattacker överbelastar nätverk med datatrafik och gör dem således obrukbara. Se vidare: Henrik Karlzén (2020), *Cyberoperationer, en slutrapport*, FOI-R--5072--SE, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--5072--SE> [2022-08-08]. Två svenska exempel på utpressningsattacker är matvarukedjan Coop, som tvingades stänga efter att det amerikanska it-företaget Kaseya, vars tjänster Coop använde, utsattes för en attack 2021 och Kalix kommun, som tvingades återgå till papper och penna för att klara dagligverksamheten när de utsattes för en attack 2022. Se: Viktor Eriksson (2021), "Efter Coop-hacket – Kaseya säger att de har fått krypteringsnyckeln", *Computersweden*, 23 juni: <https://computersweden.idg.se/2.2683/1.753896/efter-coop-hacket-kaseya-sager-att-de-fatt-en-krypteringsnyckeln> [2022-06-01]; Nils Stahle, (2022) "It-attacken mot Kalix kommun – detta har hänt", *SVT Norrbotten*, 25 januari: <https://www.svt.se/nyheter/lokalt/norrboten/it-attacken-mot-kalix-kommun-detta-har-hant> [2022-06-01].

¹¹⁵ Whyte, Thrall och Mazanec, *Introduction*, s. 5.

¹¹⁶ Se vidare: Jonas Hallberg, Johan Bengtsson och Henrik Karlzén (2016), *Beskriva och bedöma hot mot IT-system. Varför är det svårt?* FOI-R--4330--SE, Totalförsvarets forskningsinstitut, Stockholm; Thomas Rid (2022), "Why You Haven't Heard About the Secret Cyberwar in Ukraine." *The New York Times*, 18 mars; Vidar Hedtjäm Swaling och Jessica Johansson (2018), *NCS3 studie – IoT-relaterade*

Informationskrigföring är till skillnad från cyberkrigföring långt mer heterogen och agnostisk i sina metoder. På så vis definieras informationskrigföring efter önskad effekt – att påverka och förändra vad en målgrupp vet och tror om sig själva och sin omvärld i syfte att påverka och förändra beteenden i målgruppen.¹¹⁷ Informationskrigföring är på så vis mer omfattande och kan, men behöver inte, inbegripa cyberoperationer.¹¹⁸ I stället för att se information och cyber som särskilda, kan det inom den digitala informationsmiljöns ramar vara mer fruktbart att se dem som två poler i ett spektrum.¹¹⁹ Ur detta perspektiv kan en övergripande konceptualisering göras där informationskrigföring delas upp i två förgreningar – en teknisk och en psykologisk/kognitiv. Till den tekniska räknas då cyberoperationer, men även teleoperationer. Till den psykologiska eller kognitiva förgreningen räknas informations- och påverkansoperationer.¹²⁰

Oavsett hur relationen mellan informationsmiljön och cyberdomänen förstås har den digitala informationsmiljön gett upphov till nya hotbilder och en Pandoras ask av informationsspridning, propaganda, vilseledning och övervakning (se vidare kapitel 3 och 4). Dagens era av desinformationsinriktad propaganda kan sägas ha sin historiska start i början av 1920-talet. Under mellankrigstiden förändrades kommunikationens förutsättningar, inte minst via radions spridning, som var de resurssvagas vapen. Efter andra världskriget professionaliserades desinformationskampanjer. Under Kalla krigets tidiga dagar var amerikanska underrättelsetjänster drivande i denna utveckling som benämndes politisk krigföring. I östblocket talades det i stället om desinformation. Syftet för båda sidorna var att spä på redan existerande konflikter inom respektive politiska styren och använda en blandning av fakta och falskheter för att vilseleda motståndaren. På 1970-talet utvecklade östblocket sina förmågor som blev alltmer sofistikerade och aktiva. De omtalades också som aktiva åtgärder (*active measures*, se vidare i kapitel 4). Efter en tid av nedtrappning har det senaste årtiondet bevitnat en återkomst av aktiva åtgärder som med den digitala informationsmiljön som spelplan blivit alltmer avancerade.¹²¹

En tydlig utveckling av hur modern propaganda bedrivs är dess datadrivna och automatiserade karaktär. Det handlar om en kostnadseffektiv form av digital desinformation och informationsmanipulation genom användning av algoritmer som under överseende av mänskliga aktörer distribuerar vilseledande information över sociala nätverk.¹²² En metod som använts sedan internets tidigare dagar är fejkade

risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem, FOI-R--4591--SE, Totalförsvarets forskningsinstitut, Stockholm.

¹¹⁷ Porche III, *Cyberwarfare*, s. 52.

¹¹⁸ Whyte, Thrall och Mazanec, *Introduction*, s. 7.

¹¹⁹ För vidare diskussion, se: Nina A. Kollars och Michael B. Petersen (2019), "Feed the Bears, Starve the Trolls", *The Cyber Defense Review* 14-15: 145-160, s. 149.

¹²⁰ Porche III, *Cyberwarfare*, s. 26.

¹²¹ För en kort historik, se: Thomas Rid (2021), *Active Measures: The Secret History of Disinformation and Political Warfare* (London: Profile Books), s. 6-8.

¹²² Parafraisering av original: "Computational propaganda is a term that neatly encapsulates this recent phenomenon - and emerging field of study - of digital misinformation and manipulation. As a

konton med kallade strumpdockor (*sockpuppets*), vilket innebär att falska konton används för att lura och bedra andra användare. Den automatiserade versionen av strumpdockor är nätverk av fejkade konton, som kan vara mer eller mindre avancerade i funktionerna de kan utföra – vanligtvis fungerar de likt en digital megafon för att amplifiera olika budskap med syfte att flytta fokus från en typ av information genom att dränka informationsmiljön med annan typ av information (*denial of information attacks*) och att gilla eller ogilla utvalda användares konton på sociala medier.¹²³ Nätverk av detta slag kan modifieras och anpassas efter önskad effekt och bli en flexibel och kostnadseffektiv infrastruktur för digital kommunikation.¹²⁴ I samband med Brexit framkom det exempelvis att samma nätverk som spridit pro-Brexitinnehåll tidigare hade spridit pro-palestinskt innehåll.¹²⁵

Tillsammans med spridandet av information finns det i dag många alternativ för att manipulera och skapa falsk information i form av text, ljud, bild, video och memer (se kapitel 3 för vidare diskussion).¹²⁶ Ett alternativ som bedöms bli ett allt vanligare inslag i desinformations- och påverkanskampanjer är så kallade *deepfakes* – manipulerade eller syntetiserade bilder, ljud och videor möjliggjorda med hjälp av en maskininlärningsteknik som kallas generativa motståndarnätverk (*generative adversarial networks*, GAN). Det handlar om att lära algoritmer att imitera mänskligt utseende och beteende för att modifiera det, eller att skapa nytt.¹²⁷ En känd

communicative practice, computational propaganda describes the use of algorithms, automation, and human curation to purposefully manage and distribute misleading information over social media networks.” Samuel C. Woolley och Philip N. Howard (2019), ”Introduction: Computational Propaganda Worldwide”, i *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, red. Samuel C. Wolley och Philip N. Howard (Oxford och New York: Oxford University Press), 3-20, s. 4.

¹²³ Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, Paul Scharre, Thomas Zeitoff, Bobby Filar, Hyrum Anderson, Heather Roff, Gregory C. Allen, Jacob Steinhardt, Carrick Flynn, Seán Ó hÉigearthaigh, Simon Beard, Haydn Belfield, Sebastian Farquhar, Clare Lyle, Rebecca Crotoft, Owain Evans, Michael Page, Joanna Bryson, Roman Yampolskiy och Dario Amodi (2018), *Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation och OpenAI: <https://static.rasnet.ie/documents/news/2018/02/ai-report.pdf> [2022-04-10].

¹²⁴ Alfonsas Juršėnas, Kaspars Karlauskas, Eimantas Ledinauskas, Gediminas Maskeliūnas och Julius Ruseckas (2021), *The Double-Edged Sword of AI: Enabler of Disinformation*, NATO Strategic Communications Centre of Excellence, Riga, s. 17-18: <https://stratcomcoe.org/pdfs/?file=/publications/download/The-Double-Edged-Sword-of-AI-DIGITAL-FINAL.pdf?zoom=page-fit> [2022-08-07]; Samuel C. Woolley och Douglas Guilbeault (2019), ”United States: Manufacturing Consensus Online”, i *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, red. Samuel C. Wolley och Philip N. Howard (Oxford och New York: Oxford University Press), 185-211.

¹²⁵ Arild Bergh (2019), *Social Network Centric Warfare – Understanding Influence Operations in Social Media*, FFI-rapport 19/01194, Forsvarets forskningsinstitutt, Oslo, s. 16.

¹²⁶ Begreppet mem myntades av biologen Richard Dawkins 1976. Mem åsyftar en kulturell enhet som likt en biologisk gen kan spridas, förökas och förändras över tid. Se vidare: Singer och Brooking, *LikeWar*, s. 189-190.

¹²⁷ Se: Cristian Vaccari och Andrew Chadwick (2020), ”Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News”, *Social Media + Society* 6(1): 1-13.

deepfake föreställer den tidigare amerikanska presidenten Barack Obama och är så pass trovärdigt gjort att det är mycket svårt att se att den som faktiskt talar och agerar är någon annan, i detta fall filmregissören Jordan Peele.¹²⁸ Under inledningsfasen av Rysslands invasion av Ukraina cirkulerade en deepfake där president Zelenskyj meddelar att Ukraina ”ger upp” och en annan video där president Putin meddelar att Ryssland och Ukraina har slutit fred. Båda videorna var dock av så pass låg kvalitet att de snabbt kunde avskrivas som falska.¹²⁹

Utvecklingen av maskininlärning och AI:s relation till informationsmiljön expanderar. Särskilt tre aspekter är centrala. För det första har AI inneburit en expansion av redan existerande hot. Framtida kostnadsreduktioner för kodning och teknik kommer sannolikt innebära att en större mängd aktörer kommer att ha tillgång till olika former av AI för antagonistiska syften. För det andra kan AI-tekniken även leda till en större distansering mellan människa och handling, vilket kan sänka känslomässiga, etiska och moraliska trösklar i gråzonen och i krig.¹³⁰ Slutligen kommer AI-teknik att effektivt kunna utföra uppgifter som människor inte kan, vilket leder till nya typer av hot som i dag kan vara svåra att förutsäga. Med största sannolikhet kommer dessa typer av tekniker att bli långt mer avancerade och än svårare att avslöja, och sudda ut gränserna för artificiell och reell kommunikation och information.¹³¹

Nya hotbilder relaterade till den digitala informationsmiljön kommer sannolikt att behöva blicka brett för att räkna in ny teknik, nya plattformar och nya aktörer. En något förbisedd aspekt inom forskningslitteraturen som rör militärstrategisk kommunikation är digitala subkulturer och de olika medieekologier som har vuxit fram på internet, vars snabbhet i att svärmarbeta fram information är enastående – likaså är deras potential att sprida falskheter och desinformation i multiplattforma informationsoperationer.¹³² En annan aspekt är den expanderande svarta marknaden för

¹²⁸ BuzzFeedVideo (2018), ”You Won’t Believe What Obama Says In This Video! ;)”, *YouTube*, 17 april: <https://www.youtube.com/watch?v=cQ54GDm1eL0> [2022-06-30].

¹²⁹ Digital Forensic Research Lab (2022), ”Russian War Report: Hacked News Program and Deepfake Video Spread False Zelensky Claims”, *Atlantic Council*, 16 mars: <https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelensky-claims/> [2022-06-30]; Reuters Fact Check (2022), ”Fact Check- Doctored Video Appears to Show Putin Announcing Peace”, *Reuters*, 17 mars: <https://www.reuters.com/article/factcheck-putin-address-idUSL2N2VK1CC> [2022-06-30].

¹³⁰ Distansering åsyftar här att automatisering av våld kan leda till att moraliska kopplingar som vanligtvis finnas när människor begår handlingar kan kopplas bort. Det kan exempelvis handla om drönarkrigföring när en mänsklig operatör kan befinna sig tusentals kilometer från sitt mål. Se vidare: Michael J. Boyle (2015), ”The Legal and Ethical Implications of Drone Warfare”, *The International Journal of Human Rights* 19(2): 105-126; Paul Lushenko (2021), ”Review of the Special Issue ‘Robotics Autonomous Systems and Warfare’”, *Small Wars and Insurgencies* 31, 4 June 2020”, *Small Wars & Insurgencies* 32(3): 550-570.

¹³¹ Se: Brundage et al, *The Malicious Use*.

¹³² Se: Tom Wilson och Kate Starbird (2021), ”Cross-platform Information Operations: Mobilizing Narratives & Building Resilience through both ‘Big’ & ‘Alt’ Tech”, *Proceedings of the ACM on Human-Computer Interaction* 5(CSCW2, 345): 1-32.

cyberattacker och desinformationskampanjer. Kriminella och antagonistiska statliga aktörer erbjuder olika typer av tjänster, bland annat via så kallade trollfabriker.¹³³ Tjänsterna är högst anpassningsbara efter beställarens ekonomiska resurser och önskade effekt. Priserna börjar vid ett par tusen kronor och sträcker sig till miljontals kronor. Desinformationstjänsterna är avancerade och har möjlighet att publicera i såväl mer tveksamma forum som etablerade nyhetskanaler. Desinformationskampanjer kan även synkroniseras genom att spridas som nyheter i traditionella medier och amplifieras via sociala medieplattformar.¹³⁴

Utmaningarna och de nya hotbilderna som följer ur den digitala informationsmiljön är många och föränderliga. Ovan har några centrala aspekter berörts. Ett grundproblem med att hantera informationskrigets utmaningar är avsaknaden av internationella normer. Det finns heller ingen tydlig etablerad praxis (proportionalitetsprincip) för hur och med vilka medel informations- eller cyberattacker ska bemötas.¹³⁵

I takt med att tekniken lett till nya förmågor för antagonistiska informationsoperationer har defensiva strategier utvecklats. Ett emblematiskt exempel är när den ryska hackergruppen FancyBear hackade den franska presidentkandidaten Emmanuel Macrons kampanjservrar 2017 i syfte att smutskasta honom genom att läcka känslig information. Macronkampanjen, som hade blivit förvarnad av franska it- och underrättelsemyndigheter, visste inte hur de skulle försvara sig mot själva angreppet, men hade däremot placerat felaktig och vilseledande information på servrarna. När själva läckan skedde var mycket av informationen uppenbart falsk, vilket bidrog till att potentiellt skadlig information drunnade i informationsflödet samt att läckans trovärdighet underminerades. Den här så kallade Macronläckan visar på de suddiga gränserna mellan cyber- och informationsoperationer. Macronkampanjen använde sig av både en form av klassisk cyberoperationsmetod, så kallad honungsfälla (*honeypot*), samt falsk information i vilseledande syfte, en klassisk informationsoperation.¹³⁶

Teknikutveckling har varit, och kommer med säkerhet att fortsätta vara, en del i kapprustningen om att kontrollera den digitala informationsmiljön, vilket kommer att ställa krav på en bred kunskap och kompetens för att navigera miljön, utöver

¹³³ Se vidare: Philip N. Howard (2020), *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives* (Yale University Press: New Haven och London).

¹³⁴ Insikt Group (2019), *The Price of Influence: Disinformation in the Private Sector*, Recorded Future - Cyber Threat Analysis: <https://go.recordedfuture.com/hubfs/reports/cta-2019-0930.pdf> [2022-07-15].

¹³⁵ Whyte, Thrall och Mazanec, "Introduction", s. 7.

¹³⁶ Om Macronläckan, se: Jean-Baptiste Jeangène Vilmer (2019), *The "Macron Leaks" Operation: A Post-Mortem*, Atlantic Council och Institut de recherche stratégique de l'École militaire: <https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem/> [2022-08-08]. Om honungsfällor, se: Henrik Karlzén (2021), *Honungsfällor - Att vilseleda och studera cyberangripande*, FOI-R--5217--SE, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--5217--SE> [2022-08-08].

dess rent kommunikativa aspekter. Slutligen har informationsmiljöns snabba utveckling inneburit att politiskt beslutsfattande och lagstiftning inte har följt med, vilket har inneburit att informationsmiljön genomsyras av politiska och juridiska gråzoner.¹³⁷

2.4 Avslutande diskussion

Arbetsdefinitionen av informationsmiljön som *en beskrivning av nätverksrelationer mellan informationsteknik, information och aktörer*, fångar väl in den informationstekniska utvecklingen som beskrivits i detta kapitel. Det framgår dock snabbt att alla fyra begrepp i definitionen – nätverksrelationer, informationsteknik, information och aktörer – är djuplodande och kan utforskas i mer detalj än vad som ges utrymme för i denna rapport.

För att planera för strategisk kommunikation och informationsoperationer i informationsmiljön är det av vikt att förstå dess grundläggande fysiska och digitala infrastruktur, eftersom informationsmiljön är sammanflätad med globala såväl som lokala tekniska, sociala, politiska och ekonomiska strukturer som styrs av en bred variation samt konkurrerande intressen och aktörer.

Givet snabba informationstekniska utvecklingar och en föränderlig geopolitisk maktordning kommer sannolikt den digitala informationsmiljön att bli än mer heterogen och svårnavigerad. För att inte utgå från gårdagens förståelse av informationsmiljön vid planering för strategisk kommunikation och informationsmiljöer bör begreppet förstås som föränderlig och formbar. Det kan komma att innebära att konventionella förståelser av domäner inte alltid lämpar sig för att förstå den nya verkligheten.

Inom forskningen utvecklas mångvetenskapliga och tvärdisciplinära teorier och metoder som visar på vikten av att bredda perspektiven för att analysera och förstå den här utvecklingen. Det handlar om att inte se humaniora, samhälls-, teknik- och datavetenskap som separata block, utan som olika perspektiv som tillsammans kan användas för att förklara de stora dragen i samhällsutvecklingen såväl som detaljerade analyser av data- och informationsflöden i informationsmiljön.¹³⁸

¹³⁷ För en genomgående diskussion om det arbete som genomförs för motverka desinformation i EU, se: Judit Bayer, Bernd Holznapel, Katarzyna Lubianiec, Adela Pintea, Josephine B. Schmitt, Judit Szakács och Erik Uskiewicz (2021), *Disinformation and Propaganda – Impact on the Functioning of the Rule of Law and Democratic Processes in the EU and its Member States*, Europaparlamentet, Bryssel: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653633/EXPO_STU\(2021\)653633_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653633/EXPO_STU(2021)653633_EN.pdf) [2022-08-29].

¹³⁸ Nya tvärvetenskapliga skolbildningar har etablerats det senaste decenniet, som exempelvis nymaterialism och digital humaniora. Se exempelvis: William E. Connolly, (2013) "The 'New Materialism' and the Fragility of Things", *Millennium - Journal of International Studies* 41(3): 399–412; Diana Coole (2013), "Agentic Capacities and Capacious Historical Materialism: Thinking with New Materialisms in the Political Sciences. Millennium", *Journal of International Studies* 41(3): 451–469. Om social datateori och metodutveckling, se: Justin Grimmer, Margaret E. Roberts och Brandon

Ingen enskild individ kommer att kunna inrymma all den expertis som krävs för att på djupet förstå den digitala informationsmiljöns förutsättningar för strategisk kommunikation och informationsoperation, varför en bred variation av kompetenser behövs för att navigera den framtida informationsmiljön.

M. Stewart (2022), *Text as Data: A New Framework for Machine Learning and the Social Sciences* (Princeton och Oxford: Princeton University Press); Simon Lindgren (2020), *Data Theory* (Cambridge och Medford: Polity Press).

3 Ny miljö, gammal människa

Hösten 2014 blev den ryske journalisten Vitaly Bespalov anställd på en mediebyrå i Sankt Petersburg. I ett fyravåningshus på Savhuskinagatan 55 skulle han arbeta som ”content manager”, eller snarare informationskrigare. Vad han inte då visste var att han hade blivit en del av den ryska trollfabriken *Internet Research Agency* (IRA). Hans första uppdrag var att arbeta inom projektet ”Ukraina 2”. I projektet skrev han artiklar som publicerades på webbsidan worldukraine.com.ua, där ”.ua” lagts till för att ge sken av att vara ukrainsk. Artiklarna handlade om Rysslands annektering av Krim och dess eftermäle.

Mer specifikt arbetade han med att ändra gängse benämningar på de stridande parterna. I stället för att prata om den ryska sidan som ”terrorister” och ”separatister” benämndes de som ”milis”, vilket hade en mer legitim och positiv klang. Den ukrainska armén tillskrevs epitetet ”nationalgarde” och ”frivilligbataljon” eftersom dessa benämningar var associerade med element från den ukrainska extremhögern.

Bespalov arbetade på bottenvåningen i IRA:s byggnad. Här skapade han och hans kollegor innehåll till falska ukrainska nyhetssidor. På andra våningen fanns sociala medieavdelningen där bland annat memer skapades för spridning i sociala medier. På tredje våningen arbetade Bespalovs kollegor med att skriva blogginlägg. Med påhittade ukrainska identiteter kritiserade de det ukrainska styret, såväl som amerikansk Rysslandspolitik. Bloggarna utgjorde även underlag för första våningens ”nyheter”. På fjärde våningen låg fokus på att amplifiera spridningen av det skapade innehåll.¹

IRA:s verksamhet tog fart i en tid när optimismen kring internet började ersättas av pessimism, när det hade blivit tydligt att sociala medier i sig är ett ypperligt verktyg för att inte bara kanalisera redan existerande politiska omständigheter, utan för att påverka användares uppfattningar om verkligheten genom att manipulera information.

¹ Resonemanget bygger på David Patrikarakos diskussion om Arabiska våren och IRA. För fullständiga referenser, se: David Patrikarakos (2021), ”Homo Digitalis Enters the Battlefield”, i *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*, red. Timothy Clack och Robert Johnson (London och New York: Routledge), 34-44, s. 34-35. För mer information om IRA och ryska trollfabriker, se: Neil MacFarquhar (2018), ”Inside the Russian Troll Factory: Zombies and a Breakneck Pace”, *The New York Times*, 18 februari: <https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html> [2022-07-11]; Aric Toler (2018), ”Anatomy of a Russian 'Troll Factory' News Site”, *Bellingcat*, 8 juni: <https://www.bellingcat.com/resources/case-studies/2018/06/08/anatomy-russian-troll-factory-news-site/> [2022-07-11].

I dag är det få forskare som pratar om den digitala informationsmiljön i entydigt optimistiska ordalag.² Som tidigare diskuterats (kapitel 2), understryks dock ofta i forskningen att pessimismen kring digitala medier inte handlar om digitala medier i sig – de är varken bra eller dåliga.³ Det är människans relation till dem som är av vikt – det är människor som skapar dem, skapar deras funktioner och producerar och konsumerar innehåll.

I det här kapitlet diskuteras den digitala informationsmiljöns relation till människans kognition, alltså perception, uppmärksamhet, beslutsfattande, problemlösning och inläring.⁴ Ur ett strategiskt kommunikativt perspektiv handlar kapitlet om förutsättningarna för att förstå målgrupper och hur olika kommunikativa strategier, både informativa och disruptiva, påverkar dessa. Forskningen på dessa områden är i sin linda och ska tolkas med försiktighet eftersom kausala samband mellan digitala medier, kognition och sociala relationer inte är entydiga. I det här kapitlet berörs fyra centrala aspekter av den här relationen: a) hur den tekniska designen i den digitala informationsmiljön kan påverka människan i stort, samt hur den påverkar människans b) uppmärksamhet, c) minne och d) motivation.⁵

3.1 Ny design möter gammal uppmärksamhet

Med sociala medieplattformar har uppmärksamhet blivit en handelsvara, och en global uppmärksamhetsekonomi har vuxit fram.⁶ Många av plattformarna är designade för att stimulera människans uppmärksamhet och människans hunger

² För analyser och diskussioner om utmaningar med informationsmiljön och demokratins framtid, se: Jamie Bartlett (2018), *The People vs Tech: How Internet is Killing Democracy* (London: Ebury Press); Justin E. Smith (2022), *The Internet Is Not What You Think It Is: A History, a Philosophy, a Warning* (Princeton: Princeton University Press); James Williams (2018), *Stand Out of Our Light: Freedom and Resistance in the Attention Economy* (Cambridge och New York: Cambridge University Press). Jämför med till exempel Eric Schmidt och Jared Cohens teknikoptimism från 2013 om att kommunikationsteknologi skulle undergräva auktoritära staters legitimitet: Eric Schmidt och Jared Cohen (2013), *The New Digital Age: Transforming Nations, Business, and Our Lives* (New York: Vintage Books), s. 75.

³ För en introduktion till relationen mellan människa och den digitala informationsmiljön, se: Martin Korte (2020), "The Impact of the Digital Revolution on Human Brain and Behavior: Where Do We Stand?", *Dialogues in Clinical Neuroscience* 22(2): 101-111.

⁴ För centrala aspekter om relationen mellan människa och digitala medier se: Joseph Firth, John Torous, Brendon Stubbs, Josh A. Firth, Genevieve Z. Steiner, Lee Smith, Mario Alvarez-Jimenez, John Gleeson, Davy Vancampfort, Christopher J. Armitage och Jerome Sarris (2019), "The 'Online Brain': How the Internet May Be Changing Our Cognition", *World Psychiatry* 18(2): 119–129.

⁵ Resonemanget utgår från den så kallade MAD-modellen. MAD står för *motivation, attention, och design*. Tillägget som görs i den här rapporten är minne. Se: William J. Brady, M. J. Crockett och Jay J. Van Bavel (2020), "The MAD Model of Moral Contagion: The Role of Motivation, Attention, and Design in the Spread of Moralized Content Online", *Perspectives on Psychological Science* 15(4): 978–1010.

⁶ Se: Thomas Davenport och John Beck (2001), *The Attention Economy: Understanding the New Currency of Business* (Boston: Harvard Business Scholl Press).

efter uppmärksamhet förefaller vara omätlig.⁷ Uppmärksamhet förstås här som tudelad. Å ena sidan handlar det om en kognitiv funktion, å andra sidan om uppmärksamhet i bemärkelsen att bli socialt uppmärksammas.⁸ Den nya informationsmiljön erbjuder en hel värld av stimulans för båda dessa former av uppmärksamhet.

Flertalet sociala medieplattformar lever på att sälja reklam och att samla in data från användare.⁹ Ju fler användare, desto fler potentiella konsument, och desto mer data. Data används för att träna algoritmer att blir mer effektiva – för att göra reklamen mer träffsäker och, än bättre, ge användarna mer av vad de visar att de vill ha. För den enskilde som vill ha uppmärksamhet är möjligheterna oändliga. Inom loppet av sekunder kan en direktlänk skapas till en global publik. Andra användare ger likes, kommenterar, upprörs, förfasas och sprider meddelanden vidare. Snabbheten i kommunikationen och informationsflödena har blivit ett signum – allt händer här och nu. Responsen ska ofta vara direkt, annars blir den obsolet.¹⁰ Eftertänksamhet och det offentliga samtalets grindvakter har fått en svårkontrollerad konkurrens.¹¹

Människans kognitiva förmågor har utvecklats under hundratusentals år utan digitala medier, och den enorma kognitiva stimulans som dagens informationsmiljö erbjuder innebär nya utmaningar för människan.¹² Även om hungern efter uppmärksamhet är omätlig är människans uppmärksamhet begränsad.¹³ Människan förefaller vara relativt dålig på att göra flera saker samtidigt och forskning pekar

⁷ Williams, *Stand Out*, s. 10.

⁸ Smith, *The Internet*, s. 27-40.

⁹ Data är avgörande för att utveckla framtida tekniska innovationer och för att förfinas existerande datordrivna produkter. Data är i sig varken bra eller dåligt, frågan är hur den används. Om data och metadata (*Big Data*), se: James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh och Angela Hung Byers (2011), "Big Data: The Next Frontier for Innovation, Competition, and Productivity", *McKinsey Global Institute*: www.mckinsey.com/mgi/publications/big_data/pdfs/MGI_big_data_full_report.pdf [2022-07-11]; Bernard Marr (2022), *Data Strategy: How to Profit from a World of Big Data, Analytics and Artificial Intelligence* (London, New York och Daryaganj: Kogan Page).

¹⁰ Kelly, *Understanding the 12*, s. 40.

¹¹ Jeffrey Baptist och Julian Gluck (2021), "The Gray Legion: Information Warfare Within Our Gates", *Journal of Strategic Security* 14(4): 37-55.

¹² Jägar- och samlarsamhället har ofta getts som referens för vad människans biologiska sammansättning är skapad för. Inom evolutionsforskning har detta dock sedan en tid omvärderats. Teorier om att människans genetiska sammansättningar och funktioner förändras ständigt i relation till sin omgivning har fått genomslag. Ju mer omgivningen förändras desto snabbare verkar förändringar ske, och utifrån ett evolutionärt perspektiv är biologiska förändringar som kräver 10, 20 eller 30 generationer ett ögonblick. Evolution kan med andra ord vara relativt snabb. För vidare diskussion se: Agnar Helgason, Axel W. Einarsson, Valdis B. Guðmundsdóttir, Ásgeir Sigurðsson, Ellen D. Gunnarsdóttir, Anuradha Jagadeesan, S. Sunna Ebenesersdóttir, Augustine Kong och Kári Stefánsson (2015), "The Y-Chromosome Point Mutation Rate in Humans", *Nature Genetics* 47: 453-457; John Hawks, Eric T. Wang, Gregory M. Cochran, Henry C. Harpending och Robert K. Moyzis (2007), "Recent Acceleration of Human Adaptive Evolution", *PNAS* 104(52): 20753-20758.

¹³ Se: Paul Atchley och Sean Lane (2014), "Cognition in the Attention Economy", *Psychology of Learning and Motivation* (61): 133-177, s. 137.

på att ju fler saker som görs, desto sämre blir den fokuserade uppmärksamheten.¹⁴ Den fokuserade uppmärksamheten krävs för att rikta människans kognitiva förmågor. En begränsad förmåga att fokusera uppmärksamheten mot ett mer kognitivt krävande göromål kan resultera i en bristande förmåga att förstå större sammanhang (global uppmärksamhet), att koncentrera sig (fasthållen uppmärksamhet) och att sälla bort irrelevanta intryck för ett specifikt göromål (selektiv uppmärksamhet).¹⁵

Inom forskningen analyseras och debatteras till vilken grad människans uppmärksamhet kan manipuleras och vilseledas. Flertalet teorier om filterbubblor och ekokammare har förts fram.¹⁶ Även om inga entydiga svar kan ges ska riskerna med information som distraktion inte underskattas – uppmärksamhet kan riktas ner i ett djupt kaninhål av uppmärksamhetslockande nonsens, riktas bort från en särskild händelse eller distraheras genom ett överflöd av information så att ingenting till slut är värt ens uppmärksamhet.¹⁷

I uppmärksamhetsekonomin kan tävlingen om att monopolisera människans uppmärksamhet ses som en konstant överbelastningsattack – se på Netflix och samtidigt svara på sms, se en tio sekunder lång filmsnutt på en katt som hoppar in i en låda på Instagram, kolla mejlen, se en 15 sekunder lång film på TikTok av ukrainska soldater som spränger en rysk stridsvagn, svara på sms, läsa om en president som sparkar en försvarsminister med fem ord på Twitter, och hela tiden följa handlingen i filmen.¹⁸

¹⁴ Om multitasking och effekt på kognition se: Maria Vedeckina och Francesca Borgonovi (2021), "A Review of Evidence on the Role of Digital Technology in Shaping Attention and Cognitive Control in Children", *Frontiers in Psychology* 12(611155): 1-22. Inom psykologin skiljs uppgifter som kräver riktad och fokuserad uppmärksamhet från inlärda uppgifter som blir kognitivt automatiserade. I det senare fallet kan riktad och fokuserad uppmärksamhet få effekten att den automatiserade processen störs. Se: Athley och Lane, "Cognition in", s. 141-145.

¹⁵ Se: Firth et al, "The 'Online Brain'."

¹⁶ För en översikt, se: Ludovic Terren och Rosa Borge-Bravo (2021), "Echo Chambers on Social Media: A Systematic Review of the Literature", *Review of Communication Research* 9: 99-118.

¹⁷ I litteraturen om propaganda finns både historiska och samtida exempel på vad som kan kallas strategisk distraktion. Se till exempel: Johan Farkas och Christina Neumayer (2020), "Disguised Propaganda from Digital to Social Media", i *Second International Handbook of Internet Research*, red. Jeremy Hunsinger, Matthew M. Allen och Lisbeth Klastrup (Dordrecht: Springer), 707-724; Robert Johnson och Timothy Clack (2021), "Introduction: The World Information War", i *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*, red. Timothy Clack och Robert Johnson (London och New York: Routledge), 1-18.

¹⁸ Twitters nuvarande begränsning för meddelanden är 280 karaktärer vilket är cirka 40 till 60 ord. Den 9 november avskedade den amerikanske presidenten Donald Trump försvarsministern Mark Esper med orden: "Mark Esper has been terminated." Se: Guy Snodgrass (2020), "Trump Fires Secretary Of Defense Mark Esper Via Tweet", *Forbes*, 9 november: <https://www.forbes.com/sites/guysnodgrass/2020/11/09/trump-fires-secretary-of-defense-mark-esper-via-tweet/?sh=2ccb3d9c66bd> [2022-07-04]. Om multitasking, se: Leo Yeykelis, James J. Cummings och Byron Reeves (2014), "Multitasking on a Single Device: Arousal and the Frequency, Anticipation, and Prediction of Switching Between Media Content on a Computer", *Journal of Communication* 64(1): 167-92.

Människan är vidare en affektiv varelse som föredrar en person eller en sak framför en annan, utvärderar för- och nackdelar, känner på olika sätt och har riktade känslor – hat, kärlek, upphetsning, ånger och rädsla.¹⁹ När nya händelser sker och nya kontakter skapas stimuleras människans känsloliv och specifika emotioner som ånger, skuld, rädsla och glädje. Men när det nya blir det normala tenderar det att bli tråkigt.²⁰ I dag, när det normala är ett konstant flöde av information som kan ge upphov till en känsla av konstant föränderlighet, kan rädslan att missa det nya leda till ännu mer konsumtion av information.²¹

Förmågan till reflektion och eftertanke, som kräver fokuserad uppmärksamhet, kan förstås som att den tävlar med lockelsen i snabb affektiv stimulans som är mindre uppmärksamhetskrävande.²² I den här tävlingen pekar forskning på att människan tenderar att välja det senare: emojis, GIF:ar, bilder, memer och sekundlånga videor ackompanjerade av rörande musik som väcker starka känslor är framgångsrika format.²³ Den konstanta belastningen av kognitiva intryck kan leda till att människor får svårare att inte ge vika för frestelsen till kortsiktig och lättillgänglig stimulans, vilket i extremfall kan leda till ett patologiskt beroende av internet och digitala medier.²⁴ Omfattningen och effekten detta kommer att ha på människan i ett längre tidsperspektiv återstår att se.²⁵

Känslor är inte bara sammanflätade med andra kognitiva förmågor; de är en integrerad del av hur människor uppfattar världen och tar beslut, och intuition som bygger på moraliska omdömen föregår allt som oftast djupare värderingar och

¹⁹ Se: Lasana T. Harris och Susan T. Fiske (2006), "Dehumanizing the Lowest of the Low: Neuroimaging Responses to Extreme Out-Groups", *Psychological Science* 17(10): 847–853.

²⁰ Susan T. Fiske och Shelley E. Taylor (2021), *Social Cognition: From Brains to Culture* (Los Angeles och London: Sage) s. 401.

²¹ Om rädslan att missa något, också kallad FOMO (*fear of missing out*), se: Lee Hadlington och Karen Murphy (2018), "Is Media Multitasking Good for Cybersecurity? Exploring the Relationship Between Media Multitasking and Everyday Cognitive Failures on Self- Reported Risky Cybersecurity Behaviors", *Cyberpsychology, Behavior, and Social Networking* 21(3): 168-172.

²² Se: Firth et al, "The Online Brain".

²³ Se: Beata Biały (2017), "Social Media - From Social Exchange to Battlefield", *The Cyber Defense Review* 2(2): 69-90; Megan Boler och Elizabeth Davis, red. (2020), *Affective Politics of Digital Media: Propaganda by Other Means* (London och New York: Routledge).

²⁴ Atchley och Lane, "Cognition in", s. 162. WHO har till exempel klassificerat internetberoende som en diagnos: Internet Addiction (IA). Det är dock omtvistat om det är internet och digitala medier självt som är orsaken, eller om de är facilitatorer för redan existerande diagnoser och beroenden. Se: Shilpa Suresh Bisen och Yogesh M. Deshpande (2018), "Understanding internet addiction: a comprehensive review", *Mental Health Review Journal*, 23(3): 165-184.

²⁵ I dag är digitala medier och barns användarvanor omtvistade. Viss forskning pekar på att de yngre generationerna som vuxit upp med digitala medier och mobila dataenheter (*digital natives*) får sämre förmåga till fördjudad uppmärksamhet samt att de digitala användarvanorna leder till att andra sysslor bortprioriteras (till exempel idrott och läsläsning), se: Yvonne Andersson (2016), *Ungar & medier 2021: En statistisk undersökning av ungas medievanor och attityder till medieanvändning*, Statens medieråd, Stockholm; Kep Kee Loh och Ryota Kanai (2016), "How Has the Internet Reshaped Human Cognition?", *Neuroscientist* 22: 506-20.

resonemang.²⁶ Alla känslor ger dock inte samma nivå av stimulans eller upphetsning.²⁷ Flertalet studier påvisar att om det finns två alternativ av dåliga nyheter, varav en gör läsaren ledsen och den andra arg, är sannolikheten större att den senare delas.²⁸ En förklaring är att högaffektiva emotioner (som ilska, avsky och förvåning) stimulerar människan till handling mer än lågaffektiva emotioner (som sorg, förnöjdhet och tillfredsställelse). Och till skillnad från lågaffektiva emotioner, som kan bredda uppmärksamhetsförmågan och göra människor mer mottagliga för olika former av information, tenderar högaffektiva emotioner att avgränsa människans uppmärksamhetsförmåga.²⁹

I den digitala informationsmiljön sprids rykten, falska nyheter och desinformation, särskilt med en affektiv inramning, långt mycket snabbare än faktagranskade nyheter.³⁰ Att dela innehåll som är uppseendeväckande har i många fall blivit en kulturell norm för att få slå igenom i uppmärksamhetsekonomin – att få andra att reagera och interagera i affekt.

För den som vill förfasas över någonting är moralpaniken bara en svajp eller ett klick bort.³¹ I uppmärksamhetsekonomin är moralpaniken ett sätt att rikta uppmärksamhet. En persons missöde blir lätt allas missöde inom loppet av sekunder och för många är det oslagbar underhållning. Det pågår otaliga parallella interaktiva och improviserade teaterscener med sina egna dramer, konflikter, passion och glöd.³² I många fall spelar sakfrågors sanningshalt inte över huvud taget någon roll eftersom en uppdiktad uppseendeväckande nyhet antas förmedla en större sanning.³³

²⁶ Om känslor och kognition, se: Luiz Pessoa, Margo McKenna Benoit, Eva Gutierrez och L.G. Ungerleider (2020), "Neural Processing of Emotional Faces Requires Attention", *Proceedings of the National Academy of Sciences* 99(17): 11458–11463; Justin Storbeck och G. L. Clore (2007), "On the Interdependence of Cognition and Emotion", *Cognition and Emotion* 21(6): 1212–1237.

²⁷ Inom engelsk psykologi används begreppet *arousal* vilket på svenska betyder upphetsning generellt och inte är att förväxla med endast sexuell upphetsning.

²⁸ Alberto Acerbi (2019), "Cognitive Attraction and Online Misinformation", *Palgrave Communications* (5)15: 1-7. Se vidare om hur exempelvis negativt inramad statistik uppfattas som mer sann än positivt inramad statistik: Elina Lindgren, Torun Lindholm, Rens Vliegthart, Hajo G. Boomgaarden, Alyt Damstra, Jesper Strömbäck och Yariv Tsfati (2022), "Trusting the Facts: The Role of Framing, News Media as a (Trusted) Source, and Opinion Resonance for Perceived Truth in Statistical Statements", *Journalism & Mass Communication Quarterly* [online first]: 1-24.

²⁹ Se: Eddie Harmon-Jones, Tom F. Price och Philip A. Gable (2012), "The Influence of Affective States on Cognitive Broadening/Narrowing: Considering the Importance of Motivational Intensity", *Social and Personality Psychology Compass* 6(4): 314–32; Josef Lazar, Oren Kaplan, Terri Sternberg och Robert E. Lubow (2012), "Positive and Negative Affect Produce Opposing Task-Irrelevant Stimulus Preexposure Effects: Correction to Lazar, Kaplan, Sternberg, & Lubow (2011)", *Emotion* 12(3): 591-604, s.592.

³⁰ Brady et al. "The MAD Model", s. 999; Soroush Vosoughi, Deb Roy och Sinan Aral (2018), "The Spread of True and False News Online", *Science* 359(6380): 1146-1151.

³¹ Om moralpanik och digitala medier, se: Christopher J. Ferguson (2018), "The Evolutionary Roots of Media-Based Moral Panics", i *Evolutionary Psychology and Digital Games*, red. Johannes Breuer, Daniel Pietschmann, Benny Liebold och Benjamin P. Lange, (Routledge: London och New York), 118-129.

³² Jeffrey M. Berry och Sarah Sobieraj (2014), *The Outrage Industry: Political Opinion Media and the New Incivility* (New York och Oxford: Oxford University Press), s. 7-8.

³³ Se: Rid, *Active Measures*, s. 426-428.

Människans affektiva uppmärksamhet söker, och söks ständigt upp av, nya intryck. Människor är ofta jäviga till förmån för sin egen självbild. Det handlar om hur människor tenderar att selektivt välja att ta till sig information som stödjer existerande åsikter och trosuppfattningar (konfirmationsbias) samtidigt som motstridig information väljs bort (motbevisningsbias).³⁴ När det kommer till moraliska uppfattningar om rätt och fel, som är en starkt påverkande del av konfirmationsbias, kan det vara svårt att rationellt legitimera varför en åsikt premieras framför en annan utöver att det känns rätt.³⁵

Konfirmations- och motbevisningsbias kan ses som både svagheter och styrkor hos människan.³⁶ De är styrkor eftersom de hjälper människor att dra slutsatser baserat på tidigare erfarenhet och komma till beslut – ett konstant omvärderande av ståndpunkter och åsikter skulle leda till handlingsförlamning. De är svagheter eftersom människor inte alltid är medvetna om hur tidigare erfarenheter och preferenser påverkar beslutsfattande. Vidare är människor generellt sätt inte bara selektiva i hur de inhämtar och avfärdar information, utan har en tendens att över-skatta just sin egen förmåga att ställa sig över sina egna kognitiva begränsningar.³⁷

Människans begränsade uppmärksamhet, affektiva predisponeringar och konfirmationsbias kan leda till en form av tunnelseende, som är ett väldokumenterat fenomen inom såväl politiskt beslutsfattande och underrättelseanalys som i det vardagliga livet.³⁸ Det kan handla om till exempel så kallad positiv illusion där en beslutsfattare överskattar sin egen förmåga och nedvärderar en motståndares, med

³⁴ Małgorzata Kossowska, Gabriela Czarnek, Ewa Szumowska and Paulina Szwed (2022), "Striving for Certainty: Epistemic Motivations and (Un)Biased Cognition", i *Knowledge Resistance in High-Choice Information Environments*, red. Jesper Strömbäck, Åsa Wikforss, Kathrin Glüer, Torun Lindholm och Henrik Oscarsson (London och New York: Taylor and Francis), 207-221, s. 210ff.

³⁵ För vidare diskussion om kultur, moral och intuition, se: Jonathan Haidt (2013), "Moral Psychology for the Twenty-First Century", *Journal of Moral Education* 42(3): 281-297.

³⁶ Martie Haselton, Gregory A. Bryant, Andreas Wilke, David A. Frederick, Andrew Galperin, Willem E. Frankenhuis och Tyler Moore (2009), "Adaptive Rationality: An Evolutionary Perspective on Cognitive Bias", *Social Cognition* 27(5): 733-763.

³⁷ Se: Daniel Kahneman (2011), *Thinking Fast and Slow* (New York: Farrar, Straus and Giroux), s. 39ff. Det ska dock understrykas att detta är högst kontextuellt samt att det inom psykologisk forskning är omtvistat exakt vad bias är och hur det kan mätas. Om människor förstås som en rationellt kalkylerande individ kan bias förklara varför människor inte agerar enligt denna premiss. Vissa forskare framhåller att människor i stället bör förstås som heuristiska varelser som av nödvändighet behöver ta beslut på relativt få observationer och förkunskap, samt att människor är relativt bra på detta. Med andra ord, att bias fyller viktiga funktioner för att människor ska kunna fungera och navigera sin omvärld. Se vidare: Gerd Gigerenzer och Henry Brighton (2009), "Homo Heuristicus: Why Biased Minds Make Better Inferences", *TOPICS* 1(1): 107-143.

³⁸ Om tunnelseende och kognitiva flaskhalsar, se: Atchley och Lane, "Cognition in the Attention Economy", s. 137-138. Om tunnelseende, beslutsfattning och hur rationellt tänkande avsmalnar i takt med eskalerande konflikt, se: Dominic D. P. Johnson och Dominic Tierney (2011), "The Rubicon Theory of War: How the Path to Conflict Reaches the Point of No Return", *International Security* 36(1): 7-40. Om tunnelseende och kognitiv bias i underrättelsearbete, se: Martha Whitesmith (2020), *Cognitive Bias in Intelligence Analysis: Testing the Analysis of Competing Hypotheses Method* (Edinburgh: University of Edinburgh Press).

resultatet att den förste väljer konfrontation.³⁹ Ett annat exempel är den så kallade exponeringseffekten, som innebär att ju fler gånger en människa exponeras för en viss sorts information, desto större blir sannolikheten att människan ser informationen som sann eller avtrubbas av informationen, beroende på vad det är informationen förmedlar.⁴⁰ Ytterligare ett exempel är den så kallade fortsatta inflytelseeffekten, som innebär att människor tenderar att fortsätta tro och bete sig som om en viss information vore sann, trots bättre vetande.⁴¹ Ett sista exempel är accentuerings- eller betoningseffekten, som bidrar till att förenkla och skärpa människans fokus mot det som bedöms vara av extra vikt i omgivningen. Detta sker genom att kategorisera, stereotypisera och förenkla omgivningen (bra eller dåligt, ofarligt eller farligt, svart eller vitt) för att kognitivt orientera sig i den.⁴²

Människans kognitiva begränsningar har sannolikt alltid varit utsatta för olika former av manipulation, och inom propagandalitteraturen finns det gott om historiska exempel på hur enskilda individer blir offer för sina egna kognitiva förmågor och begränsningar.⁴³ I en digitaliserad informationsmiljö som är designad för att kapitalisera på människans uppmärksamhet expanderar möjligheterna att överbelasta människans kognitiva begränsningar i snabb takt.⁴⁴ När människor inte bara riktar sin uppmärksamhet mot det som ger affektiv stimulans, utan söker efter intryck som bekräftar den enskildes åsikter i tron om att just *jag* är fri från kognitiva begränsningar, riskerar människor att själva lägga grunden för sin egen manipulation och fastna i disparata ekokammare, filterbubblor och känslorridor med radikalt olika uppfattningar om vad som är sant och falskt, rätt och fel.⁴⁵ Viss forskning visar även att själva delandet av information på sociala medier kan

³⁹ John M. Friend and Bradley Thayer (2015), "War and Aggression", i *Evolutionary Perspectives on Social Psychology*, red. Virgil Zeigler-Hill, Lisa L. M. Welling och Todd K. Shackelford (New York och London: Springer), 375-386, s. 376-377.

⁴⁰ I grunden handlar exponeringseffekten om att människor utvecklar preferenser för människor, saker och information som människan känner igen. För en utförligare diskussion om exponeringseffekten, se: Robert B. Zajonc (1968), "Attitudinal Effects of Mere Exposure", *Journal of Personality and Social Psychology: Monograph Supplement* 9(2): 1-27.

⁴¹ Om inflytelseeffekten, se: Irene P. Kan, Kendra L. Pizzonia, Anna B. Drummey och Eli J. V. Mikkelsen (2021), "Exploring factors that mitigate the continued influence of misinformation", *Cognitive Research: Principles and Implications* 6(76): 1-33.

⁴² Michael A. Hogg och Dominic Abrams (2006), *Social Identifications: A Social Psychology of Intergroup Relations and Group Processes* (London och New York: Routledge), s. 62 och 77.

⁴³ Se: Mark Connelly, Jo Fox, Stefan Goebel och Ulf Schmidt (2019), "Prologue: 'Power and Persuasion': Propaganda into the Twenty-First Century", i *Propaganda and Conflict: War, Media and Shaping the Twentieth Century*, red. Mark Connelly, Jo Fox, Stefan Goebel och Ulf Schmidt (London och New York: Bloomsbury), 1-11.

⁴⁴ Se: Aaron Delwiche (2020), "Computational Propaganda and the Rise of the Fake Audience", i *The Sage Handbook of Propaganda*, red. Paul Baines, Nicholas O'Shaughnessy och Nancy Snow (Los Angeles och London: Sage), 105-125.

⁴⁵ Se: Alicia Wanless and Michael Berk (2020), "The Audience is the Amplifier: Participatory Propaganda", i *The Sage Handbook of Propaganda*, red. Paul Baines, Nicholas O'Shaughnessy och Nancy Snow (Los Angeles och London: Sage), 85-104; Jonathan Hopkin och Ben Rosamond (2018), "Post-Truth Politics, Bullshit and Bad Ideas: 'Deficit Fetishism' in the UK", *New Political Economy* 23(6): 641-655. Begreppet känslorridor är hämtat från: Katarina Barrling och Cecilia Garne (2022), *Saknad: På spaning efter landet inom oss* (Mondial: Stockholm).

innebära att den som delar tror sig kunna informationen som, utan att ens ha läst informationen. Det kan innebära att uppfattningen av vad som delas inte nödvändigtvis stämmer överens med det faktiskt delade innehållet.⁴⁶

I den ständigt föränderliga informationsmiljön kommer både gamla och nya aktörer att använda nya strategier och tekniker som tillsammans med ny kunskap om mänsklig kognition som dels kan leda till nya möjligheter för mänsklig utveckling, dels till manipulation och påverkan. För propagandisten, som de sociala mediekrigarna i Sankt Petersburg, som inte låter sig begränsas av grundläggande rättsstatliga principer, erbjuder den nya digitala informationsmiljön en ständigt expanderande verktygslåda som kan användas för att manipulera och utnyttja människans kognitiva förmåga för egna syften.⁴⁷

3.2 Det gamla minnet möter det digitala arkivet

När den brittiske AI-forskaren Robert Elliot Smith återvände till London efter en semester i Frankrike 2014 upptäckte han något märkligt. När han tittade igenom sina semesterbilder som han hade fotat med sin iPhone såg han en bild som inte riktigt stämde överens med hans uppfattning om vad som hade hänt. Under en middag hade två bilder tagits på honom och hans fru. På den ena bilden log han, men inte hon, och vice versa på den andra. Han laddade upp bilderna till Googles digitala fotoplattform så att hans fru kunde få avgöra vilken av bilderna hon gillade bäst. Vad han inte visste var att han hade aktiverat Googles AutoAwesome-funktion. Det är en algoritmbaserad funktion som automatiskt förbättrar bilder. På Roberts fotoplattform fanns inte längre bara två foton – ett tredje foto hade lagts till automatiskt av AutoAwesome. På det tredje fotot log både Robert och hans fru. Den algoritmbaserade funktionen hade med andra ord skapat ett minne som aldrig hade hänt.⁴⁸

Att den digitaliserade informationsmiljön har förändrat hur kunskap erhålls och förvaras är bortom allt tvivel.⁴⁹ Uppslagsverk, sökmotorer och sociala medieflöden är en form av digitala arkiv som i allt större utsträckning lagrar mänskliga

⁴⁶ Se: Adrian F. Ward, Jianqing (Frank) Zheng och Susan M. Broniarczyk (2022), "I Share, Therefore I Know? Sharing Online Content - Even Without Reading It - Inflates Subjective Knowledge", *Journal of Consumer Psychology* [online first].

⁴⁷ Timothy Clack and Louise Selisny (2021), "From Beijing Bloggers to Whitehall Writers", i *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*, red. Timothy Clack och Robert Johnson (London och New York: Routledge), 259-280, s. 283.

⁴⁸ För Smiths egen berättelse och bild, se: Robert Elliot Smith (2014), "It's Official: AIs Are Now Re-Writing History", *Robert Elliot Smith's Blog*, 5 oktober: <https://www.robertelliottsmith.com/blog/530> [2022-06-26].

⁴⁹ För en översikt, se: Lise Jaillant, Katie Aske, Eirini Goudarouli och Natasha Kitcher (2022), "Introduction: Challenges and Prospects of Born-Digital and Digitized Archives in the Digital Humanities", *Archival Science* [online first].

relationer, beteenden, erfarenheter och kunskap. Sett ur ett historiskt perspektiv är detta en fortsatt utveckling på människans relation till att fysiskt distansera sig från minnet – att minne lagras på en annan plats än i människans hjärna.

I antikens och medeltidens Europa var det till exempel ett tecken på djup kunskap att kunna minnas och recitera. Att minnas var en konstform (mnemoteknik) som behövde tränas upp.⁵⁰ Kunskapen var på så vis lagrad i den mänskliga hjärnan och en fysisk del av människan.

Den distanserade relationen till kunskap har skapat oro tidigare i historien.⁵¹ När tryckpressen spreds runt om i Europa kunde minnen och kunskap lagras och bevaras i en omfattning som tidigare varit omöjlig. Världens samlade kunskap kunde skrivas ner och förvaras i bibliotek. Varje individ med läskunskap kunde bilda sig och ta del av människans rika historia och kunskap. Samtidigt hördes oroade röster om informationsöverflöd.

Memorerad kunskap har självfallet inte försvunnit i dag, men i en tid då människor förefaller få en alltmer distanserad relation till minne, när informationens signum är överflöd och ytlig uppmärksamhet, väcks frågan hur den distanserade relationen till minne påverkar människan. Det slentrianmässiga googlandet för att ta reda på fakta är en tydlig symbol för en djuplodande förändring i människans distanserade relation till minne. När relationen till minnet blir distanserad behöver kunskapen ständigt sökas upp. I uppmärksamhetsekonomens distraherande lockelser riskerar den uppsökta kunskapen att glömmas bort lika snabbt som den hittades, för att sökas upp om och om igen.⁵²

Viss forskning pekar på att den här distanseringen påverkar människans förmåga att minnas genom att människan överlåter vissa minnesfunktioner till internet.⁵³ Det semantiska minnet skulle då vara särskilt utsatt, alltså det minne som lagrar kunskap om människans omvärld. När det semantiska minnet ersätts av ett digitalt minne kan även människans transaktiva minne förändras. Det transaktiva minnet, som är en form av kollektivt minne, har varit en avgörande del i hur kollektiv kunskap har förvalts och förmedlats.⁵⁴ När lättillgängliga digitala arkiv utgör det kollektiva transaktiva minnet behöver dock ingen enskild människa minnas något för det kollektivas skull – internet vet. Och när digitala arkiv lagrar allt behöver

⁵⁰ Se: Frances Yates (1999), *Selected Works Volume III - The Art of Memory* (London och New York: Taylor and Francis), s. 1-81.

⁵¹ Se: Ann M. Blair (2010), *Too Much to Know: Managing Scholarly Information before the Modern Age* (New Haven och London: Yale University Press), s. 11-61.

⁵² Se: Justin E. Smith, *The Internet*, s. 14-49.

⁵³ Inom forskningen talas det digital amnesi och "Google-effekten." Den här forskningen ska dock tolkas försiktigt eftersom den har visat sig svår att replikera. Se: Betsy Sparrow, Jenny Liu och Daniel M. Wegner (2011), "Google Effects on Memory: Cognitive Consequences of Having Information at Our Fingertips", *Science* 333: 776-778.

⁵⁴ Se: Kyle Lewis och Benjamin Herndon (2011), "Transactive Memory Systems: Current Issues and Future Research Directions", *Organization Science* 22(5): 1254-1265.

ingen längre minnas var information är lagrad – internet vet. Böcker, vänner och samhället är inte längre avgörande för att minnas – eftersom internet vet.⁵⁵

Forskningen om de reella effekterna på människans minne och kognitiva förmågor i allmänhet är i sin linda och ska tolkas försiktigt. Människan har levt i ett digitalt samhälle i ett par decennier. Människans hjärna och kognitiva förmågor har utvecklats under miljontals år och intressanta hypoteser produceras och testas för att utröna hur relationen mellan det digitala arkivet och det transaktiva minnet påverkar människans kognitiva förmåga – till exempel att det skulle kunna leda till ett verkligt kollektiv och globalt digitalt-mänskligt medvetande och en ökad förmåga för teoretisk abstraktion, kreativitet och spatialt (rumsligt) tänkande.⁵⁶ Oavsett hur detta utvecklas pekar forskningen på att människans kognitiva förmågor har börjat integreras med den digitala informationsmiljön, på gott och ont.

Relationen mellan människans minne och teknisk design väcker frågan om till vilken grad minnet är manipulerbart. I detta avseende är exponeringseffektens relation till minne intressant. Som redan har diskuterats innebär exponeringseffekten att ju fler gånger ett påstående repeteras, desto större blir sannolikheten att människor tror på det. En anledning verkar vara att minnet ofta sviker. Ju mer tid som passerar från att den ursprungliga informationskällan har konsumerats (lästs, betraktats, upplevts eller hörts), desto större blir sannolikheten att minnet om vad som egentligen hänt eller var sant förvrängs.⁵⁷ När detaljkunskap faller i glömska verkar den lätt kunna manipuleras.⁵⁸

Baserat på dessa insikter är sannolikheten stor att AI-forskaren Smith inte skulle ha reflekterat över det autokorrigerade och förfalskade fotot om han hade tittat på

⁵⁵ Firth et al, "The 'Online Brain'", s. 125; Korte, "The Impact", s. 108.

⁵⁶ Se: Vaughan Bell, Dorothy V. M. Bishop och Andrew K. Przybylski (2015), "The Debate over Digital Technology and Young People", *BMJ*: h3064; Richard Heersmink (2016), "The Internet, Cognitive Enhancement, and the Values of Cognition", *Minds and Machines* 26: 389-407; Daniel M. Wegner och Adrian F. Ward (2013), "The Internet Has Become the External Hard Drive for Our Memories", *Scientific American* 309: 58-61.

⁵⁷ Se: Norbert Schwarz och Madeline Jalbert (2021), "When (Fake) News Feels True: Intuitions of Truth and the Acceptance of Correction of Misinformation", i *The Psychology of Fake News: Accepting, Sharing, and Correcting Misinformation*, red. Rainer Greifeneder, Mariela E. Jaffé, Eryn J. Newman och Norbert Schwarz (London och New York: Routledge), 73-89.

⁵⁸ I en studie fick försökspersoner höra följande påstående, som presenterades som sant: "Den första animerade filmen spelades in i Frankrike." Efter en tid fick de höra påståendet: "Den första animerade filmen spelades in i England." Även detta påstående presenterades som sanning och försökspersonerna accepterade det som just sanning. Ett annat påstående var: "Krokodiler sover med stängda ögon." Efter en tid fick de höra: "Krokodiler sover med öppna ögon." Även detta accepterades som sanning. När försökspersonerna utsattes för samma påståenden men i närtid kunde de utan problem skilja de olika påståenden åt. Ju mer tid som passerar, desto sämre blir människor på att komma ihåg detaljer. I stället kommer de ihåg ytlig information: "animerad film" och "något europeiskt land" eller "krokodiler" och "ögon". I studien diskuteras huruvida det överhuvudtaget är lönt att bemöta falska påståenden eftersom det riskerar att bekräfta det falska påståendet. I stället kan det vara mer effektivt att endast fokusera på det korrigerande påståendet. Se: Teresa Garcia-Marques, Rita R. Silva, Rolf Reber och Christian Unkelbach (2015), "Hearing a Statement Now and Believing the Opposite Later", *Journal of Experimental Social Psychology* 56: 126-129.

fotot vid ett senare tillfälle. Smiths berättelse är ett vardagligt och relativt harmlöst exempel på när samtiden manipuleras i realtid, men det ger upphov till frågor om vad det egentligen är vi minns.

I den ryska trollfabriken IRA i Sankt Petersburg arbetade journalisten Bespalov med att manipulera nyheter om den ryska illegala annekteringen av Krim genom att med små ändringar av begrepp skapa en konnotation mellan Ukraina och högerextremism. Sett i dagens ljus är det tydligt att det ryska narrativet om att avnazifiera Ukraina inte startade den 24 februari 2022. I många delar av Väst har det ryska narrativet med rätta beskrivits som historielöst och befängt av både journalister och experter.⁵⁹ Mot bakgrund av människans begränsade uppmärksamhet, selektiva minne och exponeringseffekten över tid kopplat till den dalande rapporteringen av det ryska invasionskriget,⁶⁰ kan det finnas en risk att vad människor utanför Ukraina kommer att komma ihåg är något om "Ukraina" och "nazister", vilket i sin tur skulle vara ett öppet mål för anakronistisk manipulation.

I en värld där människor i tilltagande grad förlitar sig på en rad olika digitala arkiv och sökmotorer för att navigera ostrukturerad information blir det digitala arkivet inte endast en fråga om saklighet, utan en reell maktfaktor. Att inkludera något i historieskrivning betyder att något annat exkluderas.⁶¹ Människans samtid förstås i relation till historia och människans historia används regelbundet för att legitimera vissa typer av handlanden i samtiden – vem har rätt till vad baserat på vilka historiska händelser?⁶² Arkiv är makt i den mening att det handlar om styre över vad som institutionaliseras som minne.⁶³ I dag lägger exempelvis både Ryssland och Kina stora resurser på att styra och kontrollera respektive regims anakronistiska historieskrivningar bland annat för att legitimera sin egen politik, kontrollera sin egen befolkning och i Rysslands fall motivera anfallskrig.⁶⁴

⁵⁹ Se till exempel: Stuart A. Thompson (2022), "4 Falsehoods Russians Are Told About the War", *The New York Times*, 10 mars: <https://www.nytimes.com/2022/03/10/technology/disinformation-russia-ukraine.html> [2022-06-27]. Se det öppna brevet från 300 forskare specialiserade på nazism, folkmord och Andra världskriget: "Statement by Scholars of Genocide, Nazism and World War II", *Googledocs*, 25 februari 2022: https://docs.google.com/document/d/1Lg3p8A3XtedJSISegDDLIPY45FVFzxpK0pxOoeUh_MI/edit [2022-06-27].

⁶⁰ Pågående arbete av Simon Hellman och Per-Erik Nilsson (FOI) av svensk och internationell nyhetsrapportering om den utökade invasionen av Ukraina samt explicit uttryckt stöd till Ukraina på Twitter.

⁶¹ Historieskrivning har alltid varit en fråga om makt. Kvinnor har till exempel exkluderats ur stora delar av historieskrivningen som i många fall har varit centraliserad kring män inom makt, diplomatik, politik, administration och krig. Historia skrivs ofta om för att legitimera olika former av samtida maktrelationer, inte sällan utifrån en etnocentrisk lins. Se till exempel forskning inom kvinnohistoria och kulturstudier: Helaine Silverman (2011), *Contested Cultural Heritage: Religion, Nationalism, Erasure, and Exclusion in a Global World* (New York: Springer).

⁶² Joan M. Schwartz och Terry Cook (2002), "Archives, Records, and Power: The Making of Modern Memory", *Archival Science* 2: 1-19, s. 3.

⁶³ Schwartz och Cook, "Archives, Records", s. 7.

⁶⁴ Om Ryssland, se till exempel: Peter Pomerantsev och Michael Weiss (2014), *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, The Institute of Modern Russia och The

De som kontrollerar de digitala arkiven besitter i dag potentiellt sett makten att inte bara välja ut vad som utgör människans individuella minne utan även det kollektiva minnet, människans historia.⁶⁵ I dag handlar detta långt ifrån om en en tydlig bild. Kollektivt skapade arkiv som Wikipedia visar på potentialen i att demokratisera arkiv av detta slag – därav den ryska regimens intresse att förfölja ryska Wikipediaredaktörer som för fram en annan bild än regimens av kriget i Ukraina.⁶⁶

I dagens informationsmiljö kan minnen och historia manipuleras på en rad olika sätt – ett foto ändras, en historisk artefakt manipuleras, ett konto raderas, en bit av historien har aldrig hänt.⁶⁷ Ett exempel på det sistnämnda är den syriske journalisten Al-Mutez Billah som under kriget i Syrien dokumenterade brott mot mänskligheten – från den syriska regimens brott till IS brutala styre.⁶⁸ Han spred till stor del sin dokumentation via YouTube. När YouTube 2017 implementerade sina nya riktlinjer för stötande och våldsamt innehåll raderades Billahs konto eftersom dokumentationen bröt mot dem. Eftersom Billah hade dött till följd av sitt arbete fanns ingen som kunde återskapa kontot och en del av historien var raderad. Sedan dess har initiativet Syrian Archive arbetat med att restaurera och lagra Billahs (och andras) dokumentation, och fler liknande initiativ skapas i en strid ström.⁶⁹

När intresset för en fråga dalar och uppmärksamheten riktas mot det senaste nya blir således kontrollen över minnet central. Om information inte längre lagras fysiskt inom människan utan i digitala tjänster och servrar, blir kontrollen över människans kollektiva minne en fråga som rör alltifrån ägande av informationsteknik och digitala minnesplattformar till manipulation av och cyberattacker mot dessa. Med tillgången till digitala arkiv kan vem som helst hämta lagrad information för att i en kreativ anakronism bekräfta just sin förutbestämda uppfattning av vad det egentligen var som hände. För vem har tid att rikta fördjupad uppmärksamhet mot något som redan är passé?

Interpreter, New York:

https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev_The_Menace_of_Unreality.pdf [2022-07-09]; Bohdan Vitvitsky (2022), "Disarming Putin's History Weapon", *Atlantic Council*, 23 januari: <https://www.atlanticcouncil.org/blogs/ukrainealert/disarming-putins-history-weapon/> [2022-07-09]; Anton Weiss-Wendt (2020), *Putin's Russia and the Falsification of History* (London och New York: Bloomsbury). Om Kina, se: Charon och Jeangène Vilmer, *Chinese Influence*.

⁶⁵ Se: Jaillant et al, "Introduction: Challenges"; Beatrice Cannelli och Marta Musso (2022), "Social Media as Part of Personal Digital Archives: Exploring Users' Practices and Service Providers' Policies Regarding the Preservation of Digital Memories", *Archival Science* 22: 259-283.

⁶⁶ Masha Borak (2022), "Doxxed, Threatened, and Arrested: Russia's War on Wikipedia Editors", *Rest of World*, 5 september: <https://restofworld.org/2022/russias-6-month-war-on-wikipedia/> [2022-09-15].

⁶⁷ För en historisk analys av arkivens betydelse för minne och historia samt risken för vad Cox kallar en "samhällelig alzheimer", se: Richard J. Cox (2008), *Personal Archives and a New Archival Calling: Readings, Reflections and Ruminations* (Duluth: Litwin Books), s. 167. Se även: Rid, *Active Measures*, s. 432.

⁶⁸ Se: Sarah-Mai Dang och Alena Strohmaier (2018), "Collective Collecting: The Syrian Archive and the New Challenges of Historiography", *VIEW Journal of European Television, History, and Culture* 14(7): 1-15.

⁶⁹ Se: Ivan Szekely (2017), "Do Archives Have a Future in the Digital Age?", *Journal of Contemporary Archive Studies* 4(2): 1-16.

3.3 Motivation möter datadriven propaganda

Under den amerikanska presidentvalskampanjen 2016 startades ett konto på Facebook med namnet "Blacktivist" (svart-aktivist). Kontot framstod som ännu ett konto som ville lyfta frågor om svarta amerikaners rättigheter och polisvåld inom ramen för Black Lives Matter-rörelsen (BLM) i USA. Med 360 000 följare var kontot till och med större än ett officiellt BLM-konto. Via kontot samlades pengar in, demonstrationer organiserades och uppblåsta och polariserande politiska budskap fördes ut, vilket i sig inte är särskilt anmärkningsvärt. Det visade sig dock snart att kontot inte drevs av vare sig BLM eller någon enskild amerikansk BLM-aktivist. Kontots digitala spår pekade mot Ryssland och IRA i Sankt Petersburg.⁷⁰ Vid sidan av denna typ av konton hade ryska trollfabriker startat andra konton som stod för raka motsatsen, som saluförde öppet våldsbejakande budskap till aktivister i den amerikanska vitmaktsmiljön.⁷¹ IRA klev med andra ord rakt in i det amerikanska kulturkriget – på båda sidor.⁷²

Det här är bara ett i raden av exempel där ryska aktörer, med fejkade konton, botar och reklamkampanjer, använder informationsmiljöns digitala plattformar, varav många i sig själva är designade att utnyttja människors kognitiva sårbarheter, för att förstärka redan existerande splittringar i syfte att främja ryska intressen.⁷³ Den här typen av propaganda, som inom forskningen kallas för amplifierad propaganda, används flitigt i dag av såväl statliga som icke-statliga aktörer för att föra ut desinformation och falska narrativ med målet att vilseleda, polarisera, radikalisera, rekrytera och så misstro mot både demokratiska institutioner och etablerade fakta.⁷⁴

Det här väcker frågan om vad det är som motiverar människor att agera på det ena eller andra sättet. Eftersom människor är sociala varelser är identitet en viktig faktor i detta avseende.

⁷⁰ Se nyhetsrapportering om fallet: Sam Levin, Olivia Solon och Shaun Walker (2017), "'Our Pain for Their Gain': The American Activists Manipulated by Russian Trolls", *The Guardian*, 21 oktober: <https://www.theguardian.com/world/2017/oct/21/russia-social-media-activism-blacktivist> [2022-06-29]; Donie O'Sullivan och Dylan Byers (2017), "Exclusive: Fake Black Activist Accounts Linked to Russian Government", *CNN Business*, 28 september: <https://money.cnn.com/2017/09/28/media/blacktivist-russia-facebook-twitter/index.html> [2022-06-29].

⁷¹ För en analys, se: William J. Aceves (2019), "Virtual Hatred: How Russia Tried to Start a Race War in the United States", *Michigan Journal of Race & Law* 24: 177-250.

⁷² Om det så kallade kulturkriget, se: Shadi Hamid (2022), "The Forever Culture War", *The Atlantic*, 8 januari: <https://www.theatlantic.com/ideas/archive/2022/01/republicans-democrats-forever-culture-war/621184/> [2022-06-29].

⁷³ Ryssland och det tidigare Sovjet har sökt utnyttja den amerikanska "rasfrågan" sedan 1920-talet, se: Aceves, "Virtual Hatred", s. 185.

⁷⁴ Se: Woolley och Howard, *Computational Propaganda*.

Identitet kan förstås som de både medvetna och omedvetna berättelser människor berättar om sig själva och andra.⁷⁵ En gängse förståelse av identitet är att det rör tre överlappande dimensioner. Den första är det individuella planet och handlar om självidentitet – vem är jag? Det andra planet handlar om relationer – vem är jag i relation till dig och du i relation till mig? Det tredje handlar om gruppidentitet eller kollektiv identitet – vilka är vi?⁷⁶ Identiteter är vidare formade av både biologiska och kulturella faktorer.⁷⁷ I en mening är både den individuella och kollektiva identiteten relationell eftersom människor skapar både själv- och gruppidentiteter i relation till vad de inte är.⁷⁸

En människas identitet är således mångdimensionell, men den består även av en rad olika komponenter. Kön, etnicitet, klass, sexualitet, nationalitet, medborgarskap, upplevda erfarenheter, utbildning och preferenser spelar alla in i hur olika människors identiteter förstås av dem själva och av andra. En och samma person kan identifiera sig som stockholmare, svensk och europé, men helst identifiera sig med staden Berlin. Samma person kan se sig som ekonomiskt liberal och värdekonservativ såväl som en kristen förespråkare av liberal demokrati och religionsfrihet. Slutligen kan personen vara en man, en förälder, ett syskon och som under pseudonym i sociala medier tycker om att trola och dreva mot meningsmotståndare.⁷⁹

Identitetsdimensionerna och identitetskomponenter är föränderliga och kontextuella. En människa kan identifiera sig mer med den ena eller andra komponenten, en eller flera komponenter kan helt åsidosättas, de kan komplettera varandra och de kan konkurrera med varandra.⁸⁰ I människans historia har dessa identitetskomponenter varit relativt stabila vid en given tid och plats. På en övergripande nivå har uppdelningar av sociala grupper i ”vi” och ”de” en lång historia och förefaller ha varit en integrerad del av hur människor interagerar på gruppnivå. Otaliga exempel visar hur uppdelningar av det här slaget sker genom att etniska identiteter

⁷⁵ Se till exempel: Dan P. McAdams och Kate C. McLean (2013), ”Narrative Identity”, *Current Directions in Psychological Science* 22(3): 233-238.

⁷⁶ Se: Vivian L. Vignoles, Seth J. Schwartz och Koen Luyckx (2011), ”Introduction: Toward an Integrative View of Identity”, i *Handbook of Identity Theory and Research: Volume I*, red. Vivian L. Vignoles, Seth J. Schwartz och Koen Luyckx (New York: Springer), 1-29.

⁷⁷ Forskningen är långt ifrån entydig om hur exakt kognition och identitet samt kultur och biologi samspelar. För en diskussion med utgångspunkt i sociokognitiv forskning, se: Michael D. Berzonsky (2011), ”A Social-Cognitive Perspective on Identity Construction”, i *Handbook of Identity Theory and Research: Volume I*, red. Vivian L. Vignoles, Seth J. Schwartz och Koen Luyckx (New York: Springer), 51-75.

⁷⁸ Om identitet och så kallad andrefiering, se: Henri Tajfel, red. (1982), *Social identity and Intergroup Relations* (Cambridge: Cambridge University Press); Stephen Harold Riggins (1997), ”The Rhetoric of Othering”, i *The Language and Politics of Exclusion: Others in Discourse*, red. Stephen Harold Riggins (Thousand Oaks: Sage), 1-30.

⁷⁹ Omskrivet exempel från: Amartya Sen (2006), *Identity and Violence: The Illusion of Destiny* (New York: W.W. Norton & Co), s. 19.

⁸⁰ En individ kan till exempel identifiera sig som soldat, vilket innebär att vederbörande ser sig som lojal mot nationen, tuff, dedikerad och redo att göra det yttersta i strid, medan samma individs kristna identitet betonar lojalitet mot gud, att vara ömsint, osjälvisk och värdera livet som sådant högre än något annat. Se: Hogg och Abrams, *Social Identifications*, s. 2.

blir överordnade alla andra former av identiteter. Särskilt förefaller etnicitet ha legat till grund för att identifiera en given grupps kollektiva identitet som, kopplat till etnocentrism och xenofobi, har använts för att särskilja sig från andra grupper och således bevara den egna gruppens sociala och kulturella karaktär.⁸¹ Samtidigt visar historien att den mening människor tillskriver sina egna identiteter och andras inte är universella och givna på förhand, utan institutionaliseras genom berättelser, riter och myter om var en given grupp kommer från och vart den är på väg.⁸²

Även om en överordnad identitets specifika uttryck inte är givna på förhand tenderar människor att radikaliserar dem när de är eller upplevs som hotade.⁸³ Detta gäller både inom en grupp och i relation till andra grupper. Inom en grupp tenderar gruppens överordnade identitet att premieras framför individers multipla identiteter, vilket kan leda såväl till auktoritära utdröningar av mångfald och avvikelser som enande identitetsskapanden som lägger grunden för kollektivt handlande.⁸⁴ I relation till andra grupper, särskilt i tider av konflikt och i krig, tenderar bron mellan ”vi” och ”de” att rämna, när ”de” tillskrivs förenklande och särskiljande identiteter (stereotyper).⁸⁵ När ryska IRA blandar sig i det amerikanska kulturkriget har de identifierat att det i det amerikanska samhället finns samhällsgrupper med överordnade identiteter som kan förstärkas ännu mer.

Att individer blir offer för desinformation och amplifierad propaganda i den digitala informationsmiljön är väl känt.⁸⁶ En individ som påverkas görs inte så i ett vakuum. Relationen mellan gruppen och individen handlar lika mycket om

⁸¹ Jim Sidanius och Robert Kurzban (2003), ”Evolutionary Approaches to Political Psychology”, i *Oxford Handbook of Political Psychology*, red. David O. Sears, Leonie Huddy och Robert Jervis (Oxford och New York: Oxford University Press), 146–181; Friend och Thayer (2015), ”War and Aggression”.

⁸² Se: Benedict Anderson (2006), *Imagined Communities: Reflections on the Origin and Spread of Nationalism* (London och New York: Verso); Michael Billig (1995), *Banal Nationalism* (London: Sage).

⁸³ Se: Gwendolyn Sasse och Alice Lackners analys av dessa processer i relation till Donbass efter 2014: Gwendolyn Sasse och Alice Lackner (2018), ”War and Identity: The Case of the Donbas in Ukraine”, *Post-Soviet Affairs* 34(2-3): 139-157.

⁸⁴ Se: Thomas Persson och Sten Widmalm (2022), ”Politisk tolerans och självcensur i orostider”, i *Du sköra nya värld*, SOM-undersökningen 2021, SOM-rapport nr 81, red. Ulrika Andersson, Henrik Oscarsson, Björn Rönnerstrand och Nora Theorin, 101-118: <https://www.gu.se/som-institutet/resultat-och-publikationer/bocker/du-skora-nya-varld> [2021-07-09]; Selin Kesebir (2012), ”The Superorganism Account of Human Sociality: How and When Human Groups Are Like Beehives”, *Personality and Social Psychology Review* 16(3): 233-261, s. 249.

⁸⁵ För socialpsykologisk, historisk och antropologisk forskning när överordnade identiteter tar över partikulära jag- och gruppidentiteter samt intragrupp- kontra intergruppidentitet, se: Hogg och Abrams, *Social Identifications*, s. 48ff; Mary Kaldor (2013), ”Identity and War”, *Global Policy* 4(4): 336-346. Om människan och så kallad svärmentalitet, se: Kesebir, ”The Superorganism.”

⁸⁶ Det finns självfallet flera olika reella och tänkbare scenarier när en person som faller till föga för desinformation och propaganda kan få ödesdiga konsekvenser. Exempelvis kan enskilda individer på centrala maktpositioner på egen hand påverka avgörande beslut. Ensamagerande terrorister är ett annat exempel på när enskilda påverkas och radikaliserar. En enskild persons förmåga att omvävla ett samhälle är i dag begränsad, men de kan däremot fungera som katalysatorer för sådana utvecklingar. Vidare kan så kallad stokastisk ideologi uppmåna individer att utföra terrordåd. Det handlar dock om en individ som agerar för ett kollektiv. För en diskussion, se: Per-Erik Nilsson (2021), *Från skitpostning till folkmord: ensamagerande våldssverkare, ideologi och accelerationism i den digitala tidsåldern*, FOI-R--5257--SE, Totalförsvarets forskningsinstitut, Stockholm.

gruppen i individen som individerna i gruppen.⁸⁷ Det är dock när det händer på grupp- eller samhällsnivå som konsekvenserna får en större och potentiellt aggregerad effekt.⁸⁸ Det kan då handla om exempelvis valpåverkan, minskad eller ökad försvarsvilja, våldsamma demonstrationer, stormningar av parlament, terrorattentat och folkmord.⁸⁹ Vad en aggregerad utkomst är står i relation till önskad effekt. En främmande makt som till exempel söker påverka ett val kan rikta in sig på relativt små väljargrupper eftersom utkomsten av ett val på marginalen kan avgöras av ett fåtal väljare. Den här typen av påverkan handlar inte nödvändigtvis om att rikta en grupp mot det ena eller andra alternativet, utan det kan lika väl handla om att ingjuta misstro till det politiska systemet som sådant.⁹⁰

För att förstå hur människor motiveras att tycka, tänka, känna och agera på det ena eller andra sättet är kollektiv identitet, världsbilder och ideologi centrala. Världsbilder handlar om hur individer och kollektiv förstår sin omvärld medan ideologi handlar om hur de tycker att omvärlden borde vara, hur världen ska förbli som den är eller förändras till vad den borde vara, och vilka medel som är legitima att använda för att nå detta mål. Världsbilder lägger således grunden för ideologier som normativa och motiverar till olika typer av handlingar.⁹¹

Sociala relationer är generellt sett viktiga för människor som sociala varelser. Individers beteenden motiveras ofta av grupptillhörighet för att passa in i den ena eller den andra gruppen.⁹² Skillnader mellan strikt individuella åsikter, moral och

⁸⁷ Hogg och Abrams, *Social Identifications*, s. 3 och 15.

⁸⁸ Se: Rainer Greifeneder, Mariela E. Jaffé, Eryn J. Newman och Norbert Schwarz (2021), "What is New and True About Fake News?", i *The Psychology of Fake News: Accepting, Sharing, and Correcting Misinformation*, red. Rainer Greifeneder, Mariela E. Jaffé, Eryn J. Newman och Norbert Schwarz (London och New York: Routledge), 1-8.

⁸⁹ Det här är inte nytt för digitala medier. Våldsamheter, revolutioner, terrorattentat och folkmord har en lång och omfattande historia som inte involverar digitala medier. Om sociala medier som faciliterande faktor för samhällsomvälvande rörelser, se till exempel: Gerbaudo, *Tweets and the Streets*. För en analys av sociala medier och terrorism, se: Majid Khosravi-Nik och Mohammedwesam Amer (2022), "Social Media and Terrorism Discourse: The Islamic State's (IS) Social Media Discursive Content and Practices", *Critical Discourse Studies* 19(2): 124-143. För en analys av sociala mediernas roll i folkmordet i Myanmar, se: Kyle Rapp (2021), "Social Media and Genocide: The Case for Home State Responsibility", *Journal of Human Rights* 20(4): 486-502; Jenifer Whitten-Woodring, Mona S. Kleinberg, Ardeh Thawngmung och Myat The Thitsar (2020), "Poison if You Don't Know How to Use It: Facebook, Democracy, and Human Rights in Myanmar", *The International Journal of Press/Politics* 25(3): 407-425. Om desinformation och upprinnelsen till stormningen av den amerikanska kongressen, se: Center for an Informed Public, Digital Forensic Research Lab, Graphika och Stanford Internet Observatory (2021), *The Long Fuse: Misinformation and the 2020 Election*, Stanford Digital Repository, Election Integrity Partnership. v1.3.0: <https://stacks.stanford.edu/file/druid:tr171zs0069/EIP-Final-Report.pdf> [2022-07-08].

⁹⁰ För en diskussion om hypotetiska scenarier i EU-länder, se: Bayer et al, *Disinformation and Propaganda*.

⁹¹ För en diskussion om världsbild och ideologi, se: Jason D. Brown (2019), *Reflective Practice of Counseling and Psychotherapy in a Diverse Society* (Cham: Springer Macmillan), s. 33-52. Uppdelningen mellan världsbild och ideologi är inte självklar, eftersom ideologier kan sägas vara världsbilder i sig, se till exempel: Marius S. Ostrowski (2021), *Ideology* (Cambridge: Polity Press).

⁹² Se: Matthew J. Hornsey (2008), "Social Identity Theory and Self-Categorization Theory: A Historical Review", *Social and Personality Psychology Compass* 2: 204-222; Anders Strindberg (2020), *Social*

normer är starkt kopplade till kollektiva åsikter, moral och normer och handlar således om kulturella aspekter av individ- och gruppidentitet samt deras världsbilder.⁹³ Social konsensus binder människor till varandra – människor är mer benägna att tro på något när fler från deras kollektiv tror på samma sak och ju mer familjär en källa är, desto mer pålitlig bedöms den vara.⁹⁴ Precis som att individer har en tendens att bli offer för sin egen kognitiva bias har grupper en tendens att bli offer för gruppbias som grundas i social konsensus och en källas status i gruppen.⁹⁵

Som tidigare påpekats är gruppidentiteter mångfacetterade och kan handla om allt ifrån familjen, klanen, staden eller nationen till etnicitet, ras, religion och politik.⁹⁶ Sedan mitten av 1800-talet har nationalstaten tilltagande institutionaliserats som den generellt sett överordnade ramen för kollektiva identiteter. Via centralisering av byråkrati, folkskolor, kultur och språk har identiteter och normer homogeniserats, och via historieskrivning, myter och riter har olika nationella folk getts en berättelse om vilka de är och vart de är på väg.⁹⁷ Den moderna nationalstatens framväxt har med andra ord skett via en relativ centralisering av kommunikation och information, på gott och ont. Den nya informationsmiljön adderar genom sin decentraliserade, nätverksbaserade och kaotiska karaktär ytterligare lager av komplexitet till skapandet och vidhållandet av gruppidentiteter.⁹⁸ Vem som är lojal mot vad är långt ifrån självklart i en tid då var och en kan ingå i transnationella identitetsgemenskaper där lojalitet riktas mot en sak eller ett ideologiskt mål, snarare än en stat och en nation.

Identity Theory and the Study of Terrorism and Violent Extremism, FOI-R—5062—SE, Totalförsvarets forskningsinstitut, Stockholm; Henri Tajfel och John C. Turner (1986), "The Social Identity Theory of Intergroup Behavior", *Psychology of Intergroup Relations* 5: 7–24.

⁹³ Brady, Crockett och Van Bavel, "The MAD Model".

⁹⁴ Schwarz och Jalbert, "When (Fake) News Feels True: Intuitions of Truth and the Acceptance of Correction of Misinformation."

⁹⁵ Se: Whitesmith, *Cognitive Bias*.

⁹⁶ Se vidare: Hogg och Abrams, *Social Identifications*.

⁹⁷ Det finns flera olika historiska skolbildningar om när nationell identitet egentligen utvecklades i Europa. Två skolbildningar har länge ställts emot varandra. Primordialister eller perennialister framhåller att nationer är naturligt definierade av folkslag och föregår nationalstatens formerande, medan modernister menar att nationstanken är en ny historisk företeelse som föddes i samband med nationalstaten. De senare menar att det är anakronistiskt att tala om nationer i dagens mening innan de amerikanska och franska revolutionerna. För vidare diskussion, se: Anderson, *Imagined Communities*; Ernest Gellner (1997), *Nationalism* (London: Weidenfeld and Nicolson); John R. Gillis (1994), "Memory and Identity: The History of a Relationship", i *Commemorations: The Politics of National Identity*, red. John R. Gillis (Princeton: Princeton University Press), 3-25; Adrian Hastings (1997), *The Construction of Nationhood: Ethnicity, Religion and Nationalism* (Cambridge: Cambridge University Press; Ruth Wodak, Rudolf de Cillia, Martin Reisigl och Karin Liebhart (2009), *The Discursive Construction of National Identity* (Edinburgh: Edinburgh University Press).

⁹⁸ Patrikarakos, "Homo Digitalis", s. 42.

Från ett perspektiv kan den nya informationsmiljön ses som mer demokratisk, samtidigt som den möjliggör ett överflöd av information, desinformation, konspirationstänkande och övervakning som kan skada demokratin.⁹⁹ Det här betyder dock inte att den nya informationsmiljön skulle premiera liberal demokrati. Den kan lika väl premiera illiberal demokrati (demokrati utan rättigheter) och odemokratisk liberalism (rättigheter utan demokrati).¹⁰⁰

Denna aspekt av kollektiva identiteter är särskilt tydlig i frågor som rör social och politisk polarisering.¹⁰¹ I den digitaliserade tillvaron finns en i det närmaste oändlig möjlighet att utveckla och leva ut alternativa versioner av människors ”jag”.¹⁰² Det finns likaså en hel värld av likasinnade att skapa gränsöverskridande sociala relationer med för att skapa egna normer, värderingar och beteenden. Detta innebär att individer kan identifiera sig med, visa lojalitet mot och lita på en hel palett av olika grupper och familjära källor både inom och utanför nationalstatens gränser.¹⁰³

Polarisering är komplext och drivs av en mångfald av faktorer, varav vissa berörs i detta kapitel.¹⁰⁴ Det är även viktigt att understryka att polarisering är ett utmärkande drag för välfungerande demokratiska rättsstater – från höger till vänster, konservativa till progressiva värderingar, arbetar- till borgarklass och stad till

⁹⁹ Om denna paradoxala aspekt i demokrati, se: Zac Gershberg och Sean Illing (2022), *The Paradox of Democracy: Free Speech, Open Media, and Perilous Persuasion* (Chicago: University of Chicago Press), s. 1-13.

¹⁰⁰ Yascha Mounk (2018), *The People Vs. Democracy: Why Our Freedom Is in Danger and How to Save It* (Cambridge: Harvard University Press), s. 14.

¹⁰¹ Inom forskningslitteraturen separeras ofta mellan elit- och gruppolarisering där den tidigare refererar till polarisering mellan beslutsfattare och den senare bland allmänheten. Se: Nolan McCarty (2019), *Polarization: What Everyone Needs to Know* (Oxford och New York: Oxford University Press), s. 13-14.

¹⁰² För forskningsöversikter om identitetsskapande online, se: Katalin Feher (2021), ”Digital Identity and the Online Self: Footprint Strategies – An Exploratory and Comparative Research Study”, *Journal of Information Science* 47(2): 192-205; Jiao Huang, Sameer Kumar och Chuan Hu (2021) ”A Literature Review of Online Identity Reconstruction”, *Frontiers of Psychology* 12: 696552.

¹⁰³ Gränsöverskridande och transnationella identiteter har funnits långt innan internet. Närliggande historiska exempel är till exempel olika typer av icke-statliga organisationer. Se: Kesebir, ”The Superorganism”, s. 252.

¹⁰⁴ För ingående diskussioner om psykologiska drivkrafter, se: Jan-Willem van Prooijen, red. (2021), *The Psychology of Political Polarization* (London och New York: Routledge). Om politisk polarisering och utmaningar mot liberaldemokratiska system, se: Jenna Bednar (2021), ”Polarization, Diversity, and Democratic Robustness”, *PNAS* 118(50): e2113843118. Om polarisering, kris och ideologisk intolerans, se: Michael W. Macy, Manqing Ma, Daniel R. Tabin, Jianxi Gao, och Boleslaw K. Szymanski (2021), ”Polarization and Tipping Points”, *PNAS* 118(50): e2102144118. Om polarisering och mediekonsumtion, se: Philipp Lorenz-Spreen, Lisa Oswald, Stephan Lewandowsky och Ralph Hertwig (2022), ”Digital Media Democracy: A Systematic Review of Causal and Correlational Evidence Worldwide” [working paper]: 1-40. Om algoritmer och digitala plattformar, se: Fernando P. Santos, Yphtach Lelkes och Simon A. Levin (2021), ”Link Recommendation Algorithms and Dynamics of Polarization in Online Social Networks”, *PNAS* 118(50): e2102141118. Om politisk polarisering över vetenskap, se: Roderik Rekker (2021), ”The Nature and Origins of Political Polarization Over Science”, *Public Understanding of Science* 30(4): 352–368. Om polarisering i Sverige, se: Henrik Oscarsson, Torbjörn Bergman, Annika Bergström och Johan Hellström (2021), *Demokraterådets rapport 2021: Polarisering i Sverige*, SNS Förlag, Stockholm.

landsbygd.¹⁰⁵ Demokratiska institutioner är i sina idealformer skapta för att hantera och balansera olika typer av polarisering och pluralism.¹⁰⁶ Relationerna mellan kommunikation, information, kultur och politik blir här centrala. Det är via kommunikation som information om människans kulturellt kodade världsåskådningar omsätts till politik.¹⁰⁷

Föreställningen om att polarisering stärks av att människor konsumerar radikalt olika typer av information är svår att belägga. Tvärtom pekar viss forskning på att människor i dagens informationsmiljö, på ett generellt plan, konsumerar en bredare palett av information än tidigare.¹⁰⁸ Detta till trots finns tecken på att polariserande kollektiva identiteter blir alltmer heterogena och homogena på en och samma gång.¹⁰⁹ En förklaring är att den digitala informationsmiljön bidrar till att förstärka särskilda kollektiva identiteter vars världsbilder radikaliserar på ett identitetsmässigt och affektivt plan.¹¹⁰

Från detta synsätt handlar alltså inte polarisering i många västliga liberala demokratier om att olika grupper konsumerar olika typer av information, utan att tolkningsramarna för hur informationen förstås polariseras och radikaliserar i grupperna.¹¹¹ Radikalt olika tolkningsramar om världens beskaffenhet (ontologi) och hur kunskap om världen skapas (epistemologi) kan underminera samhällen som bygger på tilltron och tilliten till demokrati, demokratiska institutioner och vetenskap.¹¹² I den nya informationsmiljön som präglas av uppmärksamhetsökonomins logik, moralpanik, kognitiv bias och människans vilja att tillhöra en

¹⁰⁵ För en diskussion om demokrati, polarisering och partiskhet, se: McCarty, *Polarization*, s. 19-21.

¹⁰⁶ Se: Arend Lijphart (1999), *Patterns of Democracy: Government Forms and Performance in Thirty-Six Countries* (New Havne: Yale University Press).

¹⁰⁷ Gershberg och Illing, *The Paradox*, s. 11.

¹⁰⁸ Se till exempel: Richard Fletcher och Joy Jenkins (2019), *Polarisation and the News Media in Europe*, Panel for the Future of Technology and the European Parliament, s. 32: [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634413/EPRS_STU\(2019\)634413_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634413/EPRS_STU(2019)634413_EN.pdf).

¹⁰⁹ För diskussion och analys av spatial polarisering och lokal homogenisering, se: Olivia J. Chu, Jonathan F. Donges, Graeme B. Robertson och Grigore Pop-Eleches (2021), "The Microdynamics of Spatial Polarization: A Model and an Application to Survey Data from Ukraine", *PNAS* 118 (50): e2104194118. Om digitala sociala nätverk, informationsdelning och polarisering, se: Christopher K. Tokita, Andrew M. Guess och Corina E. Tarnita (2021), "Polarized Information Ecosystems can Reorganize Social Networks via Information Cascades", *PNAS* 118(50). e2102147118.

¹¹⁰ Om affektiv polarisering, se: Shanto Iyengar, Yphtach Lelkes, Matthew Levendusky, Neil Malhotra och Sean J. Westwood (2019), "The Origins and Consequences of Affective Polarization in the United States", *Annual Review of Political Science* 22(7): 7.1–18; McCarty, *Polarization*, s. 61-68. För en nyanserande diskussion om politiska gruppers föreställda uppfattningar om varandra, se: Kai Ruggeri et al. (2021), "The General Fault in Our Fault Lines", *Nature: Human Behavior* 5: 1369-1380.

¹¹¹ Om epistemologisk polarisering, se: Fernando Broncano-Berrocal och J. Adam Carter (2021), *The Philosophy of Group Polarization: Epistemology, Metaphysics, Psychology* (London and New York: Routledge), s. 19-42.

¹¹² Se: Jennifer Kavanagh och Michael D. Rich (2018), *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life* (Santa Monica: Rand); Matthew Loveless (2021), "Information and Democracy: Fake News as an Emotional Weapon", i *Democracy and Fake News: Information Manipulation and Post-Truth Politics*, red. Serena Giusti och Elisa Piras (London och New York: Routledge), 64-76.

social grupp riskerar alltså gruppidentiteter, ”vi” och ”de”,¹¹³ inte bara att bli en fråga om olika åsikter, utan det blir en affektivt och negativt inramad fråga om vänner och fiender med resultatet att de gemensamma grunderna för samtal eroderas – frågan om fakta blir i värsta fall irrelevant eftersom var grupp har sina egna fakta.¹¹⁴

Gränslandet mellan fakta, opinion och fiktion har alltid varit suddig. Det nya i dagens informationsmiljö är möjligheten att med låg kostnad, snabbhet och global räckvidd utnyttja digitala plattformars design, data och människans kognitiva för-
mågor och sårbarheter för att rikta informationsflöden mot specifika mål-
grupper.¹¹⁵ I dag arbetar forskare, praktiker och beslutsfattare med att analysera och diskutera hur dessa hot mot liberal demokrati och vetenskap bäst kan mötas.¹¹⁶ Som diskuteras ingående i nästa kapitel har statliga och militära aktörer sedan ett par decennier utvecklat strategier och doktriner för att hantera och kontrollera denna nya informationsmiljö (se även kapitel 2). Det finns inga enkla svar och balansen mellan skydd, verkan och att bevara demokratiska grundprinciper är en utmaning.

Den nya informationsmiljön är komplex, och effekterna av manipulation och propaganda som sker i den är svåra att mäta – precis som att de exakta orsakerna för polarisering är svåra att isolera från varandra. Informationsmiljöns potential för manipulation och påverkan ska heller inte överskattas.¹¹⁷ Ett skickligt konstruerat narrativ som inte resonerar med människors upplevda verklighet riskerar att slå tillbaka och urholka tilliten till avsändaren.¹¹⁸ Likaså riskerar informations- och

¹¹³ Om fördärlig polarisering (*pernicious polarization*), det vill säga ömsesidigt missaktande grupper av ”vi” och ”de”, se: Jennifer McCoy och Murat Somer (2019), ”Toward a Theory of Pernicious Polarization and How It Harms Democracies: Comparative Evidence and Possible Remedies”, *The ANNALS of the American Academy of Political and Social Science* 681: 234-270.

¹¹⁴ Se: Tomas Ståhl, Maarten P. Zaal och Linda J. Skitka (2016), ”Moralized Rationality: Relying on Logic and Evidence in the Formation and Evaluation of Belief Can Be Seen as a Moral Issue”, *pLoS ONE* 11(11): 1-38; Jay J. Van Bavel, Steve Rathje, Elizabeth Harris, Claire Robertson och Anni Sternisko (2021), ”How Social Media Shapes Polarization”, *Trends in Cognitive Science* 25(11): 913-916.

¹¹⁵ Se: Loveless, ”Information and Democracy”, s. 68; Howard, *Lie Machines*, s. xvi.

¹¹⁶ För översikter om åtgärder, se: Samantha Bradshaw, Lisa-Maria Neudert och Philip N. Howard (2018), *Government Responses to Malicious Use of Social Media*, NATO Stratcom CoE, Riga: https://stratcomcoe.org/pdfjs/?file=/publications/download/web_nato_report_-_government_responses-1.pdf?zoom=page-fit [2022-07-09]; Daniel Fried och Alina Polyakova (2018), *Democratic Defense Against Disinformation*, Atlantic Council och EU Disinfo Lab: https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FINAL.pdf [2022-07-09]. För en diskussion om och analys av åtgärder i en svensk kontext, se: Ola Svenonius (2022), *Varning – desinformation! Allmänhetens syn på psykologiskt försvar*, FOI-R—5264—SE, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--5264--SE> [2022-07-09].

¹¹⁷ För en utförligare diskussion om påverkanskampanjers begränsade möjlighet att ändra människors beteenden på en populationsnivå, se: Claes Wallenius (2022), ”Do Hostile Information Operations Really Have the Intended Effects? A Literature Review”, *Journal of Information Warfare* 21(2):1-15.

¹¹⁸ Till exempel var folkopinionen i USA inför den USA-ledda invasionen av Irak 2003 låg (52 procent för och 42 procent emot). Efter en lång politisk och massmedial kampanj om massförstörelsevapen och demonisering av Saddam Hussein steg siffrorna avsevärt (60 procent för) för att en månad efter

påverkansoperationer som inte innehåller element av reella konsekvenser eller hot att eka tomt, på gott och ont.¹¹⁹ Vidare finns en risk att ett ensidigt fokus på informationspåverkan, desinformation, narrativ och propaganda leder till att ensidigt tekniska och administrativa lösningar söks på utmaningar som rör relationerna mellan teknik, människa och samhälle.¹²⁰ Om ett grundelement i amplifierad propaganda som leder till ökad polarisering är reella geopolitiska, kulturella, sociala och ekonomiska förhållanden, ligger orsaken till en lyckad propagandakampanj kanske mer i strukturella problem i det samhälle som utsätts för kampanjen, än i kampanjen själv.¹²¹

3.4 Avslutande diskussion

I det här kapitlet har människans relation till den nya informationsmiljön diskuterats. Utgångspunkten har varit hur teknisk design relaterar till uppmärksamhet, minne och motivation.

I arbetsdefinitionen av informationsmiljön som *en beskrivning av nätverksrelationer mellan informationsteknik, information och aktörer*, bör aktörer, utifrån dessa slutsatser, inte endast förstås som fristående agenter som verkar i informationsmiljön. De är en integrerad del av den. Precis som den informationstekniska infrastrukturen är inbäddad i globala och lokala strukturer är mänskliga aktörer inbäddade i evolutionsbiologiska, kognitiva, sociala, kulturella, religiösa och politiska strukturer. Att rikta kommunikation mot olika målgrupper är således komplext och kräver utöver kunskap om informationsmiljöns informationstekniska förutsättningar även kulturell, samhällelig, politisk och regional kunskap samt språklig kompetens för att vara värd namnet.

Den nya, digitalt präglade informationsmiljön är långt mer heterogen och kaotisk än tiden då informationsmiljön till stor grad var centraliserad via stater, etablerade

invasionen stiga än mer (72-80 procent beroende på källa). Ett år efter, när det hade uppdragats att det aldrig funnits några massförstörelsevapen, uttryckte 67 procent att de hade vilseletts och att kriget hade startats på felaktiga premisser. Se: Richard Ned Lebow (2010), *Why Nations Fight: Past and Future Motives for War* (Cambridge och New York: Cambridge University Press), s. 8.

¹¹⁹ Se: Colley, "Strategic Narratives".

¹²⁰ Vissa forskare talar om detta som en kortsiktig *whac-a-mole*-strategi som omöjligtvis kommer att kunna tävla med en föränderlig informationsmiljö. Se till exempel: Williams, *Stand Out*, s. 114; Jankowicz, *How to Lose*, s. 1-20.

¹²¹ Yascha Mounk framhåller till exempel att den amerikanska liberala demokratin har byggt på tre grundprinciper som i dag utmanas: 1) Efterkrigstiden när liberaldemokratiska stater konsoliderades präglades av ekonomisk optimism med bland annat ökande levnadsstandard. I dag har mycket av den optimismen ersatts av pessimism där resursfördelning har kommit att ses som ett nollsummespel; 2) Liberala demokratier har fram till relativt nyligen dominerats av en etnisk grupp. Demografiska förändringar genom invandring har, beroende på tolkning, lett till eller använts som förevändning att skapa etniska konflikter; 3) Med framväxten av digital kommunikation har det offentliga samtalets grindvakter till stor del försvunnit. Extrema röster som tidigare marginaliserats har i dag en megafon med en global åhörarskara. Se: Mounk, *The People*, s. 15. Det är samhälleliga trender av denna art som ofta används i amplifierad propaganda. Se: Jankowicz, *How to Lose*, s. 206-207; Peter Pomerantsev (2020), *This Is Not Propaganda: Adventures in the War Against Reality* (London: Faber & Faber).

mediekanaler och kulturproducenter. Det innebär att propaganda tidigare kunde kontrolleras lättare, medan den nya å ena sidan är mer svårkontrollerad och å andra sidan ger upphov till långtgående möjligheter för riktade informationskampanjer.

Samtidigt innebär informationsmiljöns heterogena och kaotiska karaktär att målgrupper för riktade kampanjer är ytterst komplexa. Forskare och praktiker har länge understrukt att kommunikationsmodeller som bygger på enkla sändare-mottagare-principer är förlegade, och likaså föreställningar om att kommunikation och information kan kontrolleras.¹²² Mening skapas i processer där individuella aspekter av kognition sammansmälter med sociala, kulturella och politiska aspekter såväl som med den digitala kommunikationens logiker och tekniska förutsättningar.

En cynisk slutsats är att ett framgångsrecept för dem som söker slå igenom i informationsmiljöns brus är att erbjuda enkla grundläggande och polariserande narrativa ramar om ”vi” och ”de” som bygger på underliggande sociala och politiska meningsskiljaktigheter, missnöjen och upplevda oförrätter, som hamras in med korta uppmärksamhetslockande budskap.¹²³ I en mening förefaller lyckade informationskampanjer handla mer om att skapa och manipulera den narrativa inramningen av vissa informationsflöden, för att lägga grunden till hur framtida information tolkas.¹²⁴ Utan tvekan kommer teknisk utveckling och vidare kunskap om människa och kognition öppna dörrar för mer avancerade former av manipulation såväl som ökad kognitiv förmåga.¹²⁵

Den beskrivna utvecklingen kan verka dystert. Som tidigare har påpekats ska forskningen tolkas med försiktighet. Den digitala informationsmiljön har stor potential att stärka mänskligt samarbete och demokratisera tillgången till ofiltrerad information. Den digitala framtiden är inte huggen i sten. I en omfattande intervjustudie med 50 forskare och experter på informationsteknik och kommunikation diskuteras många positiva möjligheter som kan komma att realiseras.¹²⁶ En tilltagande sammanflätning av människa och maskin, tillsammans med vetenskapliga framsteg, kan leda till friskare och längre liv. Tunga och repetitiva arbetsuppgifter kan tas över helt av AI, vilket ger människan mer tid för kreativitet och fritid. En mer

¹²² Derina Holtzhausen och Ansgar Zerfass (2015), ”Strategic Communication Opportunities and Challenges of the Research Area”, i *The Routledge Handbook of Strategic Communication*, red. Derina Holtzhausen och Ansgar Zerfass (New York: Routledge), 1-17, s. 7.

¹²³ Schwarz och Jalbert, ”When (Fake).”

¹²⁴ För en diskussion om narrativ inramning, se: Jarred Prier (2017), ”Commanding the Trend: Social Media as Information Warfare”, *Strategic Studies Quarterly* 11(4): 50-85.

¹²⁵ För en introduktion till neurovetenskap, krigföring och etiska frågor, se: James Giordano, red. (2015), *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns* (Boca Raton, London och New York: CRC Press). För en historisk och samtida analys av kognitiv manipulering, se: Joel E. Dimsdale (2021), *Dark Persuasion: A History of Brainwashing from Pavlov to Social Media* (New Haven och London: Yale University Press).

¹²⁶ Se: Stansberry, Anderson och Rainie, *Experts Optimistic*.

uppkopplad och sammanlänkad värld där svärmarbete leder till mer visdom i stället för manipulation, samarbete i stället för polarisering.

Den nya informationsmiljön är varken bra eller dålig, men den är en förutsättning för hur många människor världen över lever sina liv. Precis som det är människor som i slutändan påverkas i denna miljö är det upp till människor att avgöra hur den kommer att användas. Detta är temat för nästa kapitel.

4 Ny förmåga, gamla strategier

Samma dag som ryska styrkor påbörjade den fullskaliga invasionen av Ukraina, den 24 februari 2022, började information spridas på flera sociala medier om stora ryska förluster i form av nedskjutna stridsflygplan. Det skulle röra sig om så många som sex ryska plan som skjutits ner över Kiev – alla av en och samma ukrainska pilot, som fick det slagkraftiga smeknamnet, tillika hashtaggen, #ghostofkyiv ("Kievs vålnad"). Ett kort filmklipp som påstods visa en av nedskjutningarna spreds och fick miljontals tittare på såväl Twitter och TikTok som Telegram. Berättelsen om den modiga piloten plockades snabbt upp av traditionella medier över hela världen.¹

Snart framkom information som gjorde historien om Kievs vålnad mindre sannolik. Filmen, visade det sig, var ett klipp från det avancerade flygsimulatorspelet Digital Combat Simulator som först hade laddats upp på YouTube.² Ukrainska försvarsmyndigheter ville inte svara på specifika frågor om vem piloten var, samtidigt som de hyllade honom i sociala medier – nu för att ha skjutit ner inte sex, utan tio ryska plan.³ Det var först i slutet av april som ukrainska flygvapnet erkände att någon enskild pilot som skjutit ner så många plan inte existerade.⁴ Det hela hade rört sig om klassisk propaganda – som nyttjade den nya informationsmiljön, där information kan skapas och spridas av vem som helst, och sedan förstärkas av medier och myndigheter, i detta sammanhang i syfte att stärka ukrainarnas försvarsvilja och även stödet till Ukraina utomlands.⁵

Myten om #ghostofkyiv väckte frågan om hur långt en demokratisk stat kan gå när det gäller att föra fram desinformation. Men den speglar också den nya informationsmiljöns utveckling som beskrivits i föregående kapitel. Den ständigt utvecklande digitala tekniken som sköljer över informationsmiljön och förändrar den på djupet; de nya relationer, geografier och aktörer som skapats i den informationsmiljö som uppstått; människans varierande sätt att hantera och påverkas av denna

¹ Se exempelvis Daniel Miller (2022), "Who Is the 'Ghost of Kyiv'? Tale of Ukrainian Fighter Pilot Trends on Social Media", *Fox 2 Detroit*, 25 februari: <https://www.fox2detroit.com/news/ghost-of-kyiv-tale-of-ukrainian-fighter-pilot-trends-social-media> [2022-07-04]; Marca.com (2022), "La leyenda del 'Fantasma de Kiev', el piloto héroe de Ucrania", *Marca*, 25 februari: <https://www.marca.com/tiramillas/actualidad/2022/02/25/62189812ca4741f3518b4575.html> [2022-07-04]

² Dan Evon (2022), "Is This 'Ghost of Kyiv' Video Real?", *Snopes*, 25 februari: <https://www.snopes.com/fact-check/is-this-ghost-of-kyiv-video-real/> [2022-07-04].

³ Free Media Holding (2022), "легендарний український пілот 'привид киева' вже збив 10 російських літаків – сбу", *Kanal 5*, 27 februari: <https://www.5.ua/ukrayina/lehendamyi-ukrainskyi-pilot-pryvvyd-kyieva-vzhe-zbyv-10-rosiiskykh-litakiv-sbu-269515.html> [2022-07-04].

⁴ Emma Bubola (2022), "Ukraine Acknowledges that the 'Ghost of Kyiv' Is a Myth", *New York Times*, 1 maj: <https://www.nytimes.com/2022/05/01/world/europe/ghost-kyiv-ukraine-myth.html> [2022-07-04].

⁵ Thomas Novelty (2022), "Ukraine's Fighter Ace 'Ghost of Kyiv' May Be a Myth, But It's Lethal as War Morale", *Military.com*, 2 mars: <https://www.military.com/daily-news/2022/03/02/ukraines-fighter-ace-ghost-of-kyiv-may-be-myth-its-lethal-war-morale.html> [2022-07-06].

ständigt föränderliga nya verklighet – allt detta öppnar för frågan om hur institutioner och organisationer bäst anpassar sig. Detta väcker frågan om och vilka nya förmågor som behövs, särskilt i militära sammanhang.

I det här kapitlet beskrivs och analyseras delar av den militära utveckling som skett i omvärlden i förhållande till den nya informationsmiljön, med fokus på nationella militärmakter.⁶ Särskilt diskuteras Ryssland, Kina och USA, men viktiga lärdomar från andra länder i Väst belyses också. Det är en berättelse om de vitt skilda förutsättningar att verka i informationsmiljön som präglar auktoritära stater i förhållande till demokratier – vad gäller gränser mellan interna och externa förmågor, liksom gränserna mellan krig, fred och det som kallas gråzon. Men det är också en berättelse om en klassisk ”aktion-reaktionssekvens,”⁷ med åtföljande risk för kapprustning i informationsmiljön, som är värd att ha i åtanke givet de svåra praktiska och strategiska avvägningar som måste göras i en så djupt mänsklig och politiskt komplicerad terräng som informationsmiljön.

4.1 Gammal strategi möter den nya informationsmiljön

Kalla krigets slut och Sovjetunionens fall ledde till en tid av optimism för många. Ett splittrat Europa kunde enas. Den liberaldemokratiska, marknadsekonomiska och globaliserande världsordningen antogs ha segrat. Internationella institutioner, handel och allsköns samarbeten skulle föra världen samman.⁸ Den här bilden började dock sakta att krackelera med aggressiv internationell politik från auktoritära stater, i synnerhet Ryssland och Kina. Sedan ett drygt decennium har det inom forskning om internationella relationer funnits något av en konsensus om att

⁶ Mellanstatliga militära organisationer, i synnerhet Nato, har under ett antal år arbetat med frågor som berör militär förmåga i den nya informationsmiljön. Till skillnad från nationella militärmakter har dock Nato inte samma utmaning i att kommunicera med en nationell befolkning, och är dessutom i praktiken mest inriktad på konkreta operationer, varför en analys av Natos förmågeutveckling i detta sammanhang lämnas därhän. För vidare diskussion, se: Mark Laity (2018), ”NATO and Strategic Communications”, *Three Swords Magazine* 33/2018: 65-72:

https://www.jwc.nato.int/images/stories/threeswords/NATO_STRATCOM_2018.pdf [2022-07-11].

⁷ Edward N. Luttwak (2001), *Strategy: The Logic of War and Peace* (Cambridge: Belknap Press of Harvard University Press), s. 22-23. Det finns även tydliga historiska ekon från en liknande utveckling under mellankrigstiden, där Nazityskland tog intryck av Storbritanniens och USA:s propagandaverksamhet under Första världskriget, och byggde sin propagandaapparat som ett svar på den, se Nolan Higdon (2020), *Anatomy of Fake News* (Oakland: University of California Press), s. 110.

⁸ Här åsyftas den inflytelserika amerikanska statsvetaren Francis Fukuyamas analys av konsekvenserna av Kalla krigets slut som slutet på historien. Fukuyamas uttalande ökade den optimism som den amerikanske sociologen Daniel Bell uttryckte i sina analyser om ideologiernas död i mitten av 1900-talet. För vidare diskussion, se: Beate Jahn (2019), ”The Sorcerer’s Apprentice: Liberalism, Ideology, and Religion in World Politics”, *International Relations* 33(2): 322-337.

världen är på väg in i en ny era av stormaktsrivalitet.⁹ Det är i denna kontext, tillsammans med den tekniska utveckling som beskrivits ovan, som intresset för att kontrollera informationsmiljön på allvar börjar slå rot bland världens stormakter. Rysslands, Kinas och USA:s olika kulturella och militära förutsättningar gav tidigt upphov till olika uppfattningar av hur informationsmiljön bäst förstås och kontrolleras.

Nation	Definition
Kina	Informationsmiljön är sammanlänkande aktiviteter där information skapas, formas, utbyts, flödar och lagras, vilket påverkar individer och kollektivt medvetande, informationsinfrastruktur och informationen i sig själv.
Ryssland	Informationsmiljön är en ny plats för mänsklig kommunikation och aktiviteter. Den integrerar hela världens nätverk, databaser och information till ett stort sammanlänkat landskap där olika kulturella och etniska egenskaper påverkar interaktionens natur mellan landskapets beståndsdelar.
USA	Informationsmiljön är den aggregerade summan av individer, organisationer och system som samlar, behandlar och sprider information och agerar baserat på den.

Figur 1 – Rysslands, Kinas och USA:s konceptualiseringar av motsvarande begrepp för informationsmiljön, fritt översatt från: Porche III, *Cyberwarfare*, s. 3.

4.1.1 Ryssland

Under 00-talet inträffade en rad så kallade färgrevolutioner i olika länder i den post-sovjetiska sfären – i Georgien, Ukraina och Kirgizistan. I Väst tolkades dessa händelser som led i demokratiseringsprocesser, som uttryck för folkligt missnöje och som effekter av Västs mjuka makt – det vill säga den lockelse och attraktion som finns i friheten och välståndet som präglar etablerade liberala demokratier.¹⁰

Inom ryska maktcirkel tolkades utvecklingen annorlunda. Där etablerades snabbt en analys som pekade mot ett illegitimt användande av modern informationsteknik och nyhetsmedier för att bygga opinioner, där en från utlandet styrd och finansierad elit genomdrev vad som i praktiken var organiserade kupper.¹¹ Den här

⁹ Se exempelvis: Hal Brands (2018), "Democracy vs Authoritarianism: How Ideology Shapes Great-Power Conflict", *Survival* 60(5): 61-114; Matthew Kroenig (2020), *The Return of Great Power Rivalry: Democracy Versus Autocracy from the Ancient World to the U.S. and China* (New York: Oxford University Press); Yascha Mounk (2021), "Democracy on the Defense: Turning Back the Authoritarian Tide", *Foreign Affairs* 100(2): 163-173; Joseph S. Nye Jr. (2015), *Is the American Century over?* (Cambridge och Malden: Polity).

¹⁰ Se exempelvis: Matthew Kroenig, Melissa McAdam och Steven Weber (2010), "Taking Soft Power Seriously", *Comparative Strategy*, 29(5), s. 422-423; Andrew Wilson (2005), *Ukraine's Orange Revolution* (New Haven: Yale University Press), s. 187.

¹¹ För vidare diskussion om hur Putin och den ryska säkerhetspolitiska eliten tolkade revolutionerna, se: Andrei Soldatov och Michael Rochlitz (2018), "The *Siloviki* in Russian Politics" i *The New Autocracy*:

övergripande analysen ledde till en intensiv debatt inom det ryska säkerhets-politiska etablissemanget om hur det nya hotet bäst skulle bemötas, där just befolkningens möjligheter att protestera mot den politiska ledningen, pådrivna av en förändrad, digitaliserad informationsmiljö, sågs som särskilt hotfulla.¹²

Det som följde var en snabb kodifiering av ”informationskonfrontation” och ”informationskrigföring” i centrala ryska säkerhetspolitiska skrivelser,¹³ en kodifiering som drevs på ytterligare av kriget i Georgien 2008, upproren i Mellanöstern och Nordafrika 2011 och Maidanprotesterna i Ukraina 2014.¹⁴ Den ryska nationella säkerhetsstrategin konstaterade redan 2009, mot bakgrund av det som skett i den post-sovjetiska sfären, att ”det globala informationskriget intensifieras”.¹⁵ I den nationella militärdoktrinen som publicerades 2014 identifierades ”användandet av informations- och kommunikationsteknologier för militär-politiska syften” som ett av de huvudsakliga externa militära hoten.¹⁶ Det handlade om sådant som ”det kombinerade användandet av militär makt och politik, ekonomi, information och andra icke-militära medel som realiserar genom användandet av befolkningens protest-potential.”¹⁷

Det är det här som i många sammanhang kommit att kallas ”Gerasimov-doktrinen”,¹⁸ efter en uppmärksammat artikel från 2013 av den ryska generalstabschefen Valerij Gerasimov, där han nästan ordagrant använde formuleringar som finns i de officiella dokumenten. Han skrev till exempel: ”Fokus för applicerade konfliktmetoder har skiftat i riktning mot brett användande av politiska, ekonomiska, informationsmässiga, humanitära och andra icke-militära metoder – applicerade i koordination med protest-potentialen hos befolkningen.”¹⁹ I Väst kom artikeln att tolkas som en offensiv omformulering av den ryska militära doktrinen,²⁰ men i verkligheten handlade det alltså om en rysk regim som tyckt sig kunna

Information, Politics, and Policy in Putin's Russia, red. Daniel Treisman (Washington D.C.: Brookings Institute Press), 83-108.

¹² För en fullödig genomgång av den här utvecklingen, se: Ulrik Franke (2015), *War by Non-Military Means: Understanding Russian Information Warfare*, FOI-R--4065--SE, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4065--SE> [22022-07-12].

¹³ Inom ryskt militärstrategiskt tänkande har begreppen informationskonfrontation och informationskrigföring figurerat sedan slutet av Kalla kriget. För en genomgång och analys av ryskt militärstrategiskt vetenskapligt och doktrinärt tänkande, se: Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn och Khrystyna Holynska (2022), ”Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation”, RAND Corporation: https://www.rand.org/pubs/research_reports/RRA198-8.html.

¹⁴ Franke, *War by non-military*, s. 16.

¹⁵ Franke, *War by non-military*, s. 11.

¹⁶ Franke, *War by non-military*, s. 13.

¹⁷ Franke, *War by non-military*, s. 13.

¹⁸ Begreppet är i dag så pass etablerat att det har en egen Wikipediasida, se: Wikipedia (2022), ”Gerasimov Doctrine”: https://en.wikipedia.org/wiki/Gerasimov_doctrine [2022-07-06].

¹⁹ Citerad i: Mark Galeotti (2020), *Russian Political War: Moving Beyond the Hybrid* (London och New York: Routledge), s. 27.

²⁰ Se exempelvis: Guillaume Lasconjarias och Jeffrey A. Larsen (2015), *NATO's Response to Hybrid Threats* (Rome: NATO Defense College), s. 10.

identifiera en västlig förmåga som man nu var tvungen att anpassa sig till. Som en forskare påpekar är de ryska doktrinära resonemangen i grund och botten defensiva – det är en ”mörk bild av världen” som målas upp, där ”informationskrigföring mot Ryssland är utbrett”, vilket också innebär att de är mycket knapphändiga om rysk offensiv förmågeutveckling.²¹

Den precisa kopplingen mellan denna defensiva doktrinära utveckling på högsta ryska nivå och de offensiva förmågor som Ryssland under Vladimir Putin utvecklat under det senaste decenniet är svår att belägga med precision, i synnerhet vad gäller den militära dimensionen. Informationskrigföring sker ofta i gråzonen och ligger traditionellt någonstans i utrymmet mellan underrättelseverksamhet och andra militära förmågor och är därför ofta hemliga – i ännu högre grad i auktoritära stater. Vidare innebär den ryska strategin att det inte görs någon konceptuell uppdelning mellan informationsoperationer och cyberoperationer, utan de är snarare två sidor av samma mynt.²² Det är tydligt att den ryska tolkningen av informationskrigföring är mycket bred och inkluderar många olika delar av statsapparaten såväl som privata aktörer. Exempelen på ökade ryska militära aktiviteter i informationsmiljön, såväl internationellt som nationellt, är många och välbelagda.²³

I samband med ockupationen av Krim och den första ryska invasionen av Donbass 2014 genomfördes aktiviteter som av Nato:s dåvarande överbefälhavare kallades ”det mest otroliga informations-*blitzkrieg* vi sett i informationskrigets historia”.²⁴ Det handlade då om traditionell propaganda, framför allt med hjälp av tv, riktad mot den rysktalande befolkningen i Ukraina. Men den ryska militära underrättelsetjänsten GRU var också mycket aktiv på sociala medier med att skapa falska konton på såväl Facebook som ryska Vkontakte (numera VK), där avancerade subversionskampanjer lanserades för att framställa den ukrainska militären som styrd av USA.²⁵ Även under det amerikanska presidentvalet 2016 var enheter från den ryska militära underrättelsetjänsten djupt inblandade i bland annat det uppmärksammade hackandet av det Demokratiska partiets mejlservrar och spridningen av materialet på Wikileaks.²⁶ Nu senast under den fullskaliga invasionen

²¹ Franke, *War by non-military*, s. 22.

²² Den konceptuella uppdelningen görs i stället mellan informationstekniska operationer och informationspsykologiska operationer. Se: Giles, *Handbook of Russian*, s. 9.

²³ För en övergripande bild av den ryska förmågeutvecklingen ur ett Natoperspektiv, se Keir Giles (2016), *Handbook of Russian Information Warfare*, NATO Defense College, London:

<https://www.ndc.nato.int/download/downloads.php?icode=506>; för ingående genomgång och analys av rysk aktiviteter i Väst och i Afrika, se: Emman El-Badawy, Sandun Munasinghe, Audu Bulama Bukarti och Beatrice Bianchi (2022), *Security, Soft Power, and Regime Support: Spheres of Russian Influence in Africa*, Tony Blair Institute for Global Change, London:

<https://institute.global/sites/default/files/articles/Security-Soft-Power-and-Regime-Support-Spheres-of-Russian-Influence-in-Africa.pdf> [2022-09-15]; Bilyana Lilly (2022), *Russian Information Warfare: Assault on Democracies in the Cyber Wild West* (Annapolis: Naval Institute Press).

²⁴ Citerad i: Philip Seib (2021), *Information at War: Journalism, Disinformation and Modern Warfare* (Cambridge: Polity), s. 137.

²⁵ Rid, *Active Measures*, s. 353-358.

²⁶ Rid, *Active Measures*, s. 377.

av Ukraina 2022 är det tydligt att omvärlden lärt sig mer om den ryska förmågan och därför agerat mer proaktivt,²⁷ men ryska informationsinsatser har trots det varit omfattande och åtminstone bitvis framgångsrika.²⁸

Vad som är verkligt nytt är dock svårt att säga. Mycket av den informationskrigföring som på senare år diskuterats och, vad det verkar, operationaliserats i rysk säkerhetspolitik och doktrin, har djupa historiska rötter. Det kommunistiska Sovjetunionen etablerade tidigt en form av gränslös ”politisk krigföring”,²⁹ djupt rotad i leninistisk teori, där framför allt underrättelsetjänsterna organiserade och utförde aktiva åtgärder (från ryskans *активные мероприятия*) i form av desinformationskampanjer och andra påverkansoperationer. Detta var framför allt riktat mot den egna befolkningen, men skedde även i resten av världen, utan några egentliga juridiska eller moraliska begränsningar och utan en åtskillnad mellan krigstillstånd och fred.³⁰ Det finns tydliga bevis för att delar av den kultur och struktur som låg bakom detta överlevde Sovjetunionens kollaps.³¹ Steget att återaktivera och modernisera förmågor av det här slaget var därför inte långt i ett alltmer auktoritärt och militariserat Ryssland under Vladimir Putin. Samtidigt visar forskning att den nya digitala informationsmiljön har gjort de ryska aktiva åtgärderna än mer aktiva – men att de samtidigt är mindre precisa.³²

Som diskuterats i föregående kapitel är det ytterst svårt att skapa en helhetsbild av och mäta effekten av dessa förmågor i informationsmiljön. Enligt en forskare har detta bidragit till att västliga samhällen, som ”kastats in i tvivel och direkta identitetskriser” orsakade av internets spridning och alla dess sidoeffekter, ”både över-skattar och, i ovanligare fall, underskattar hotet och potentialen hos desinformationskampanjer – och hjälper därmed till att öka potentialen i just det hotet”.³³

²⁷ Christopher Bronk, Gabriel Collins och Dan Wallach (2022), *Cyber and Information Warfare in Ukraine: What Do We Know Seven Months In?* Baker Institute Issue Brief 09.06.22, Rice University's Baker Institute for Public Policy, Houston: <https://doi.org/10.25613/69E1-WZ16> [2022-09-21].

²⁸ Se exempelvis Carl Miller (2022), ”Who's Behind #IStandWithPutin?”, *The Atlantic*, 5 april: <https://www.theatlantic.com/ideas/archive/2022/04/russian-propaganda-zelensky-information-war/629475/> [2022-06-15]

²⁹ Galeotti, *Russian Political*, s. 2, med hänvisning till ett memo av den berömda amerikanska diplomaten George Kennan från 1948.

³⁰ För en nyanserande bild av hur detta pågått och förändrats mellan 1920 och 2020, se: Rid, *Active Measures*.

³¹ För en detaljerad bild av hur sovjetisk desinformation om amerikansk biologisk krigföring överlevde Sovjetunionens kollaps, plockades upp av rysk underrättelsetjänst (i flera fall av samma individer) och kom att bli del av kampanjer riktade mot Ukraina efter 2014, se: Milton Leitenberg (2020), ”False Allegations of Biological-Weapons Use from Putin's Russia”, *Nonproliferation Review* 27(4-6): 425-442.

³² Fri översättning av: ”Active measures have become more active, but less measured”). I: Rid, *Active Measures*, s. 434.

³³ Rid, *Active Measures*, s. 434.

4.1.2 Kina

Även Kina har under de senaste två decennierna utvecklat såväl doktrin som förmåga i den nya informationsmiljön. Eftersom Kina är en leninistisk stat kontrollerad av det Kinesiska Kommunistpartiet (KKP) är kopplingen mellan partistatens grundläggande ideologi och strukturer och förmågan i informationsmiljön ännu tydligare än i Ryssland. Arbetet sker brett och strukturerat i flera delar av partiapparaten, bland annat i Centrala propagandaavdelningen, Centrala avdelningen för enhetsfronten och i partikontrollerade Folkets befrielsearmé (FBA). Såväl roller som metoder att föra ut budskap och nå effekt är ofta överlappande.³⁴ Traditionellt har KKP:s fokus varit på den interna kinesiska informationsmiljön, liksom Taiwan och diasporagrupper, men i takt med Kinas växande internationella intressen har fokus i ökande grad riktats även mot andra länder och regioners informationsmiljöer.³⁵ Ett exempel är den globala tv-kanalen CGTN, China Global Television Network, som kontrolleras av partiets propagandaavdelning.

Den rent militära förmågan kretsar kring en doktrin som formulerades 2003, som kallas för ”de tre formerna av krigföring” och inbegriper psykologisk krigföring, opinionskrigföring och juridisk krigföring.³⁶ Enligt den uppdaterade doktrinen från 2010 ska all kinesisk militär personal tränas i detta. Eftersom FBA är en partikontrollerad organisation är målet för den här verksamheten KKP:s fortsatta maktinnehav, varför den i grund och botten är en politisk verksamhet. Det rör sig, med andra ord, om just den breda ”politiska krigföring” som existerade i Sovjetunionen.³⁷ Som i den ryska kontexten beskrivs Västs, och i synnerhet USA:s, antagna försprång i informationskrigföring både som en inspiration och utmaning att komma ikapp.³⁸ Kina har även anammat konceptet mjuk makt (*soft power*) – att framställa Kommunistpartiet och landet som attraktivt via diplomati, kultur, politik och handel – för att vinna delar av det internationella samfundets hjärta och själ (*hearts and minds*).³⁹

Det som är känt kring den organisation och de förmågor som specifikt utvecklats inom FBA rör såväl traditionella medier – tv, radio och bokförlag – som cyberförmågor.⁴⁰ Målet för verksamheten är framför allt Taiwan, men aktiviteter har

³⁴ Charon och Jeangène Vilmer, *Chinese Influence*, s.15-16.

³⁵ För en genomgång av Enhetsfrontens arbete, även i Sverige, se: Oscar Almén (2020), *The Chinese Communist Party and the Diaspora – Beijing’s Extraterritorial Authoritarian Rule*, Stockholm: FOI-R--4933--SE, Totalförsvarets forskningsinstitut, Stockholm:
<https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4933--SE> [2022-07-12].

³⁶ Psykologisk krigföring är riktad mot motståndarens militär, och syftar till att övertyga dem om att fortsatt motstånd är hopplöst; opinionskrigföring handlar om att övertyga utvalda målgrupper att Kinas sak är den rätta; och juridisk krigföring har syftet att instrumentalisera juridiska principer för att uppnå militära fördelar, Charon och Jeangène Vilmer, *Chinese Influence*, s. 45-51.

³⁷ Charon och Jeangène Vilmer, *Chinese Influence*, s. 46.

³⁸ Charon och Jeangène Vilmer, *Chinese Influence* s. 47.

³⁹ Se: Kingsley Edney, Stanley Rosen och Ying Zhu (2020), ”Introduction”, i *Soft Power with Chinese Characteristics: China’s Campaigns for Hearts and Minds*, red. Kingsley Edney, Stanley Rosen och Ying Zhu (London och New York: Routledge), 1-23.

⁴⁰ Charon och Jeangène Vilmer, *Chinese Influence* s. 99ff.

också riktats mot informationsmiljöer i Väst med USA som främsta mål,⁴¹ men även Sverige.⁴² Det finns också ett tydligt intresse hos FBA att anamma ryska metoder – såväl den ryska kanalen RT som den ryska inblandningen i det amerikanska presidentvalet 2016 har studerats av kinesiska militära analytiker.⁴³ Det finns också tecken på större koordination mellan Ryssland och Kina i den internationella informationsmiljön – inte minst i samband med det pågående kriget i Ukraina.⁴⁴

4.1.3 USA

Även i USA har frågor om den militära dimensionen av den förändrade informationsmiljön diskuterats länge. Faktum är att diskussionen går nära ett århundrade tillbaka i tiden. År 1937 skapades Institute for Propaganda Analysis som tog fram ett sjupunktsprogram för att kategorisera och möta propaganda i den då nya informationsmiljön.⁴⁵ Vad gäller utvecklingen i förhållande till den moderna informationsmiljö som diskuteras i denna rapport var det under slutet av 90-talet och början av 00-talet som USA börjar utveckla koncept för strategisk kommunikation i teori och praktik. Grunden lades i en rapport av *Defense Science Board Task Force* (DSB) publicerad 2001 av Försvarsdepartementet och Utrikesdepartementet.⁴⁶ I rapporten definieras en ”s sofistikerad strategisk kommunikation” som förmågan att ”sätta agendan och skapa kontexter som utökar förmågan att nå politiska, ekonomiska och militära mål”, vilket över tid ”kan leda till att forma utländska uppfattningar på sätt som främjar amerikanska intressen”.⁴⁷ Som sådan var det en bred kommunikativ strategi som skulle inbegripa både militära och civila statliga och icke-statliga aktörer. Vidare lyftes vikten av att integrera informationsoperationer med militära operationer (luft, land, sjö och *special operations*).⁴⁸ Strategisk kommunikation kom att ses som ett vapen i det globala kriget om idéer (*war of ideas*).⁴⁹

⁴¹ Charon och Jeangène Vilmer, *Chinese Influence*, s.122.

⁴² Anledningen till att Sverige, och andra nordiska länder, är föremål för kinesiska påverkansoperationer grundar sig enligt Charon och Jeangène Vilmer i att Sverige ses som en geografiskt viktig inkörsport till Arktis och EU, samt att Sverige har haft en relativt oreglerad lagstiftning för utländska investeringar, vilket Kina har utnyttjat för strategiskt ägande. För vidare diskussion, se: Charon och Jeangène Vilmer, *Chinese Influence*, s. 521-538.

⁴³ Charon och Jeangène Vilmer, *Chinese Influence* s. 622.

⁴⁴ Se exempelvis: Ingram Niblock, Samantha Hoffman och Jake Wallis (2022), ”Chinese and Russian Propaganda Work in Tandem to Blame the West for War in Ukraine”, *The Strategist*, Australian Strategic Policy Institute, 26 maj: <https://www.aspistrategist.org.au/chinese-and-russian-propaganda-work-in-tandem-to-blame-the-west-for-war-in-ukraine/> [2022-07-05]

⁴⁵ Se: Mark Connelly et al, ”Power and Persuasion”, s. 2.

⁴⁶ Se: Defense Science Board Task Force (2001), *Report of the Defense Science Board Task Force on Managed Information Dissemination*, Washington, DC: Department of Defense, Washington.

⁴⁷ Defense Science Board Task Force, Report of the Defense, s. 2.

⁴⁸ Defense Science Board Task Force, Report of the Defense, s. 2.

⁴⁹ Jente Althuis (2021), ”How U.S. Government Fell in and out of Love with Strategic Communications”, *Defence Strategic Communications* 10: 71-110, s. 92.

Utvecklingen av den amerikanska strategiska kommunikationen skedde parallellt med kriget mot terrorismen och invasionerna av Afghanistan och Irak.⁵⁰ En rad offensiva strategier utvecklades för att verka i informationsmiljön. Till exempel sjösattes *Office for Strategic Influence* (OSI) 2001. Syftet var att skapa informationskampanjer för att bekämpa islamistisk extremism. Initiativet väckte mycket kritik och anklagades för att vara en propagandafabrik. Fem månader efter att det skapats lade försvarsminister Donald Rumsfeld ner OSI.⁵¹ Under 00-talet växte dock en konsensus fram om vikten av strategisk kommunikation, samtidigt som det fanns en osäkerhet om vad det egentligen var och hur det skulle implementeras, vilket ledde till otaliga rapporter och en mängd definitioner och modeller.⁵² I konceptutvecklingen underströks dock i tilltagande grad att strategisk kommunikation handlade lika mycket om vad som sades som vad som gjordes.⁵³

En anledning till detta fokus var ett ökande glapp mellan ord och handling under kriget mot terrorismen, då bilden av USA som en försvarare av liberal demokrati och mänskliga rättigheter kom att ifrågasättas, både av opinionen hemmavid och utomlands.⁵⁴

En annan typ av kritik kom också att riktas mot den egna förmågan att verka i informationsmiljön. År 2007 gav försvarsminister Robert Gates uttryck för detta när han påpekade att al-Qaida var bättre på kommunikation än USA:

”Public relations uppfanns av USA, trots det är vi bedrövliga på att kommunicera till resten av världen vad vi är för typ av samhälle, om frihet och demokrati samt om vår politik och våra mål. Det är rent ut sagt pinsamt att al-Qaida är bättre på att kommunicera sitt budskap på internet än USA. Som en utländsk diplomat frågade för ett par år sedan: ’Hur kommer det sig att en man i en grotta lyckades slå världens främsta kommunikationssamhälle i just kommunikation?’ Snabbhet, flexibilitet och kulturell relevans är inga begrepp som kommer i åtanke när amerikansk strategisk kommunikation diskuteras.”⁵⁵

I början av 10-talet övergav Försvarsdepartementet strategisk kommunikation som koncept med motiveringen att det ledde till mer förvirring och ineffektivitet snarare än ökad förmåga.⁵⁶ En förändrad realpolitisk verklighet gjorde även att fo-

⁵⁰ Se exempelvis: E. Leigh Armistead, red. (2007), *Information Warfare: Separating Hype from Reality* (Sterling, VA: Potomac Books).

⁵¹ Se: Susan L. Gough och Frank Jones (2003), *The Evolution of Strategic Influence*, U.S. Army War College, Pennsylvania, s. 31.

⁵² Althuis (2021), ”How U.S.”, s. 94.

⁵³ Obamaadministrationen publicerade till exempel en strategi som skulle synkronisera ord med handling. Se: United States – White House (2009), *National Framework for Strategic Communications*, Homeland Security Digital Library: <https://www.hsdl.org/?abstract&did=27301> [2022-07-16].

⁵⁴ Se till exempel: Gene E. Bigler (2007), ”Strategic Communications and the Decline of US Soft Power”, i *Global Legal Challenges: Command of the Commons, Strategic Communications, and Natural Disasters*, red. Michael D. Carsten (Newport: Naval War College), 217-234.

⁵⁵ Fri översättning av citat i: Althuis (2021), ”How U.S.”, s. 96. Se även: Colley, ”Strategic Narratives”, s. 38.

⁵⁶ Se: George E. Little, Assistant to the Secretary of Defense (2012), *Memorandum for Commanders of the Combatant Commands, Office of the Assistant Secretary of Defense, 20301—1400*, Pentagon,

kus riktades mot vad som sågs som en snabbt ökad förmåga hos Kina och i synnerhet Ryssland.⁵⁷ Intressant nog förefaller den ”mjuka makt” som Ryssland identifierade som så hotfull – och som Kina i viss mån anammat – inte figurera mycket i militära texter och doktriner,⁵⁸ även om ämnet ånyo har börjat uppmärksammas i debatten.⁵⁹ Inte heller den amerikanska pluralismen – den frihet, demokrati och kultur Robert Gates pratade om – har varit i fokus, i motsats till en rysk förmåga som har sina rötter i kommunistiska idéer om ett samhällsomfattande ”politiskt krig”.⁶⁰ Det har i stället handlat mycket om USA:s oförmåga att anpassa sina militära och säkerhetspolitiska strukturer till sina huvudmotståndares mer ”avancerade” syn på krig.⁶¹ I vissa sammanhang uttrycks visserligen behovet av att bygga motståndskraft underifrån med icke-militära verktyg som utbildning och ett

Washington: https://foreignpolicy.com/wp-content/uploads/2015/01/121206_brooksmemo.pdf [2022-07-16].

⁵⁷ Se exempelvis: Emilio J. Iasiello (2017), ”Russia’s Improved Information Operations: From Georgia to Crimea”, *The US Army War College Quarterly: Parameters* 47(2): 51-63, s. 7.

⁵⁸ Den amerikanska mjuka makten handlar om att främja amerikanska intressen med bland annat ekonomiska medel, att bygga goda internationella relationer och sprida värderingar. En viktig del, både mot den egna befolkningen och mot främmande makt, har varit och är amerikansk kulturproduktion – filmer, tv-serier och dataspel. Försvarsdepartementet och CIA har till exempel en lång relation till den amerikanska kulturindustrin och har varit involverade i otaliga filmproduktioner. Flertalet journalister och forskare har analyserat denna relation som en form av institutionaliserad propaganda. Försvarsdepartementet menar dock att syftet med dessa samarbeten är att säkerställa att den amerikanska militären och händelser framställs korrekt samt att känslig information inte avslöjas. Om mjuk makt och USA, se: Victoria de Grazia (2021), ”Soft-Power United States Versus Normative Power Europe: Competing Ideals of Hegemony in the Post– Cold War West, 1990-2015”, i *Soft Power Internationalism: Competing for Culture Influence in the 21st Century Global Order*, red. Burcu Baykurt och Victoria de Grazia (New York: Columbia University Press), 19-59. För journalistik och forskning om Pentagons relationer till Hollywood, se: Matthew Alford (2010), *Reel Power: Hollywood Cinema and American Supremacy* (London och New York: Pluto Press); David L. Robb (2004), *Operation Hollywood: How the Pentagon Shapes and Censors the Movies* (New York: Prometheus Books). Om Försvarsdepartementet och populärkultur, se: Carl Boggs och Tom Pollard (2016), *The Hollywood War Machine: U.S. Militarism and Popular Culture* (London och New York: Routledge). Om CIA:s relation till Hollywood, se: Tricia Jenkins (2012), *The CIA in Hollywood: How the Agency Shapes Film and Television* (Austin: University of Texas Press). Om Försvarsdepartementet och dataspelsindustrin, se: Tim Lenoir och Luke Caldwell (2018), *The Military Entertainment Complex* (Massachusetts och London: Harvard University Press). För Försvarsdepartementets syn på verksamheten, se: Katie Lange (2018), ”How & Why the DOD Works With Hollywood”, *Inside DoD*, U.S. Department of Defense, 28 februari: <https://www.defense.gov/News/Inside-DOD/Blog/article/2062735/how-why-the-dod-works-with-hollywood/> [2022-07-12].

⁵⁹ Kyle Wolfley diskuterar exempelvis hur mjuk makt till stor del har setts som en icke-militär fråga – för militären har hård makt (*hard power*) i stället varit i fokus. Han menar dock att särskilt Kinas anammande av mjuk makt som strategi för internationellt inflytande, men även Rysslands liknande strategier, nödvändiggör att militären införlivas i ett strategiskt tänkande om mjuk makt. Se: Kyle Wolfley (2021), *Military Statecraft and the Rise of Shaping in World Politics* (New York: Rowman & Littlefield). Det kan också argumenteras att den amerikanska militären länge har varit en del av projicerandet av mjuk makt, vilket inte är en självklarhet. Beroende på målgrupp kan dissonans uppstå kring vem som meddelar (militär) och vem som beslutar (politik), vilket kan leda till en bild av ökad militarisering av USA. Se: Bigler, ”Strategic Communications”.

⁶⁰ Detta har dock understrukits i Natopublikationer, se till exempel: Giles, *Handbook of Russian*.

⁶¹ Media Ajir och Bethany Vaillant (2018), ”Russian Information Warfare: Implications for Deterrence Theory”, *Strategic Studies Quarterly* 12(3): 70-89.

stärkande av demokratin på hemmaplan för att stärka motstånd- och attraktionskraften hos det egna samhället,⁶² men i det stora hela har mycket fokus legat på hur den militära strukturen bör förändras för att möta ett ökande hot i informationsmiljön.

Under 10-talet blev den här diskussionen tydlig i officiella militära styrdokument. År 2016 offentliggjorde det amerikanska försvarsdepartementet en ”*Strategi för operationer i informationsmiljön*”. Där konstaterar dåvarande försvarsministern Ash Carter att såväl statliga som icke-statliga aktörer ”använder olika förmågor [i informationsmiljön] för att utnyttja, störa och slå ut ledningssystem och annan kritisk infrastruktur; för att sprida propaganda och desinformation; för att driva på intern splittring; för att rekrytera och söka finansiellt stöd; och för att bygga legitimitet för sina handlingar och samtidigt misskreditera legitimiteten hos andra”.⁶³ Svaret var att börja strukturera den amerikanska militären för att kunna ”identifiera fientliga och potentiellt fientliga hot...och uppbåda förmågor för att kunna påverka, underminera och erodera en motståndares eller potentiell motståndares vilja”.⁶⁴

Den amerikanska strategin för informationsmiljön betonar att militär verksamhet kräver nära koordination med andra delar av statsapparaten (liksom allierade, internationella partner och den privata sektorn).⁶⁵ Den betonar också det viktiga med att kunna vara aktiv även i fredstid (”*the steady-state*”), men att det innebär utmaningar med större begränsningar att ta hänsyn till.⁶⁶ Här är det också värt att understryka de olika förutsättningar som råder i en demokratisk rättsstat som USA och länder som Kina och Ryssland. Till exempel får den amerikanska militären enligt lag inte ”använda medel för publicitet eller propaganda inom Förenta staterna.”⁶⁷ Den här skrivningen är otydlig i hur den relaterar till operationer i informationsmiljön (varken ”propaganda” eller ”publicitet” definieras i lagen), men i det större sammanhanget är det ändå tydligt att USA – i motsats till i synnerhet mindre länder – är ett land med mycket militär verksamhet utomlands, varför det kan antas att huvuddelen av den nya förmåga som ska byggas upp ska användas utanför USA:s gränser.⁶⁸ Detta har också blivit tydligt under 2022, när stora sociala medieplattformar stängt ett antal fejkade konton som kopplats till den amerikanska militären och som riktat propaganda mot ett antal länder i framför allt

⁶² Se exempelvis: James Curtis (2021), ”How to Defeat the Info-Warfare ‘Triad of Deception’”, *National Defense*, 5 augusti: <https://www.nationaldefensemagazine.org/articles/2021/8/5/how-to-defeat-the-info-warfare-triad-of-disruption> [2022-06-15].

⁶³ United States Department of Defense (2016), *Strategy for Operations in the Information Environment*: <https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf> [2022-06-17].

⁶⁴ United States Department of Defense, *Strategy for*, s. 5.

⁶⁵ United States Department of Defense, *Strategy for*, s. 6.

⁶⁶ United States Department of Defense, *Strategy for*, s. 6.

⁶⁷ United States Code (2011), ”10 U.S.C. Section 2241”, U.S. Government Publishing Office: <https://www.govinfo.gov/content/pkg/USCODE-2011-title10/html/USCODE-2011-title10-subtitleA-partIV-chap134-subchapI-sec2241.htm> [2022-06-17].

⁶⁸ Congressional Research Service (2021), *Defense Primer: Information Operations*: <https://sgp.fas.org/crs/natsec/IF10771.pdf> [2022-06-17].

Centralasien och Mellanöstern – något som också sätter fokus på frågan om hur långt en demokrati bör gå när det kommer till att föra fram sina ståndpunkter.⁶⁹

Sedan strategin publicerades 2016 har den operationaliserats i flera steg. Den amerikanska militärens huvuddoktrin ändrades i juli 2017 för att omfatta information som en sjunde gemensam funktion.⁷⁰ Den innefattar ”hantering och användning av information och dess avsiktliga integration med de övriga gemensamma funktionerna för att påverka relevanta aktörers uppfattningar, beteenden, handlingar eller icke-handlingar, liksom mänskligt och automatiserat beslutsfattande”.⁷¹ Detta följdes 2018 av ett ”gemensamt koncept för operationer i informationsmiljön”, där sexton ”nödvändiga förmågor” listas, gällande både operationalisering och institutionalisering.⁷² Listan är lång och kommer inte att beskrivas i detalj, men som exempel kan nämnas att det under förmågan ”genomföra integrerade fysiska och informationsmässiga aktiviteter för att uppnå psykologiska effekter” beskrivs att den amerikanska militären ”tillsammans med övriga regeringsmakten, allierade och partner ska utveckla och kommunicera ett konsekvent, trovärdigt och tilltalande narrativ till relevanta aktörer”.⁷³ Konceptet listar också elva risker med dess genomförande, bland annat ”risken för eskalation och oavsiktliga konsekvenser” och att ”tillämpningen av informationsförmåga skulle kunna leda till förvirring gällande militärens roll och ansvar”.⁷⁴

I en utvärdering som genomfördes 2021 av Government Accountability Office (GAO – en motsvarighet till den svenska Riksrevisionen) görs dock tydligt att mycket av det som 2016 sattes upp som målsättningar gällande en ökad förmåga inte har förverkligats, trots den vidare konceptutvecklingen.⁷⁵ Rapporten pekar i synnerhet på låga investeringar och bristande ledarskap, och gör tydligt att den amerikanska militären fortfarande befinner sig i en process där integrationen av informationsoperationer är en både institutionell och konceptuell utmaning.⁷⁶

⁶⁹ Graphika och Stanford Internet Observatory (2022), *Unheard Voice – Evaluating Five Years of Pro-Western Covert Influence Operations*: https://public-assets.graphika.com/reports/graphika_stanford_internet_observatory_report_unheard_voice.pdf [2022-09-20]

⁷⁰ United States Joint Chiefs of Staff (2017), *Doctrine for the Armed Forces of the United States*, s. 19: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf [2022-06-17]. De övriga funktionerna är *command and control, intelligence, fires, movement and maneuver, protection och sustainment*.

⁷¹ United States Joint Chiefs of Staff, *Doctrine for*, s. 19.

⁷² United States Joint Chiefs of Staff (2018), *Joint Concept for Operating in the Information Environment (JCOIE)*, s. 31-40: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf [2022-06-17].

⁷³ United States Joint Chiefs of Staff, *Joint Concept*, s. 37.

⁷⁴ United States Joint Chiefs of Staff, *Joint Concept*, s. 41.

⁷⁵ United States Government Accountability Office (2021), *Information Environment: DOD Operations Need Enhanced Leadership and Integrated Capabilities*: <https://www.gao.gov/assets/gao-21-525t.pdf> [2022-06-17].

⁷⁶ United States Government Accountability Office, *Information Environment*, s. 7-15

4.1.4 Andra länder i Väst

Diskussioner om och arbeten med att utveckla förmågan i den nya informationsmiljön är inte begränsade till stormakterna. Förmågeutveckling går under många och varierande beteckningar – *informationsoperationer*, *(militär)strategisk kommunikation*, *hybridkrigföring* och *psykologiskt försvar* – och har dryftats ordentligt i såväl organisationer som Nato⁷⁷ som i praktiskt taget alla västliga länder.

Ett exempel är Norge, där det norska Forsvaret för närvarande driver ett projekt med syfte att ”förbättra Forsvarets förmåga till att bidra till nationell strategisk kommunikation”.⁷⁸ Även här pekas mycket mot Rysslands ökande förmåga att verka i informationsmiljön som huvudanledningen till att utveckla den norska, samtidigt som en utmaning som identifieras är den ”inbyggda asymmetri” som finns i den flexibilitet Ryssland har att ”operera mindre bundet än mer demokratiska stater med lagar och fungerande maktfördelning”.⁷⁹ Den norska rapporten betonar också behovet av att omdefiniera hur man ser på olika beredskapslägen – i synnerhet ”normaltillståndet”, alltså fred.⁸⁰ Samtidigt är det tydligt att den norska militära förmågan i informationsmiljön ska vara en integrerad del av en politiskt styrd nationell strategisk kommunikation.⁸¹

Ett annat exempel är Storbritannien, där ett antal militära strategi- och styrdokument det senaste decenniet lyft fram vikten av att utveckla informationsaspekten av militär förmåga. Den konceptuella nivån i det brittiska arbetet är slående avancerad och ambitiös (se ett talande exempel i figur 3). Det är tydligt att en av de grundläggande utgångspunkterna är att informationsaspekten av statlig makt ska utövas koordinerat, i en ”*whole-of-government*”-metod, där försvaret är en integrerad del av hela statsmaktens informations- och kommunikationsstrategier.⁸²

⁷⁷ Laity, ”NATO and”, s. 65-73.

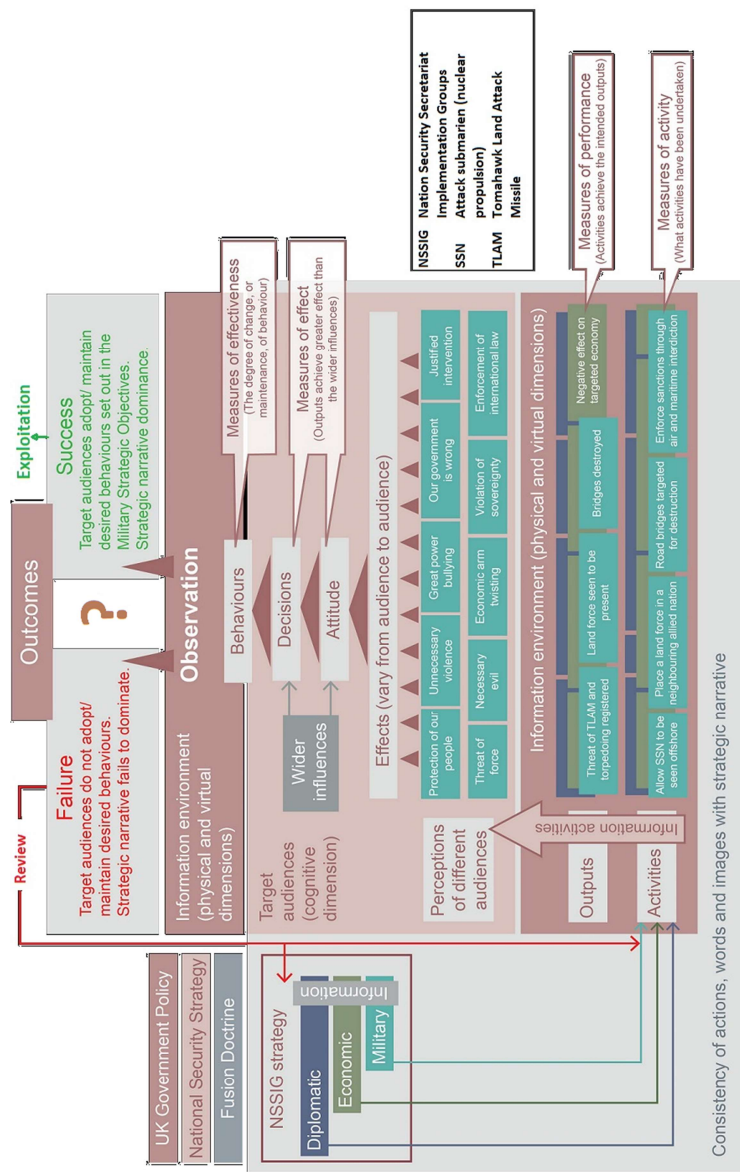
⁷⁸ Brede I. Hertenberg och Jonas Bjønebye (2021), *Prosjekt MilStratKom: Militærstrategisk Kommunikasjon og Forsvarets bidrag til Nasjonal Strategisk Kommunikasjon - intern utredningsrapport till det norske Forsvaret*, Haeret, Oslo, s. 3.

⁷⁹ Hertenberg och Bjønebye, ”Prosjekt MilStratKom”, s. 5 och 9.

⁸⁰ Hertenberg och Bjønebye, ”Prosjekt MilStratKom”, s. 6.

⁸¹ Hertenberg och Bjønebye, ”Prosjekt MilStratKom”, s. 3.

⁸² Se framför allt: UK Ministry of Defence (2019), *Defence Strategic Communication: An Approach to Formulating and Executing Strategy*, Joint Doctrine Note 2/19: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804319/20190523-dcdc_doctrine_uk_Defence_Strategic_Communication_jdn_2_19.pdf [2022-07-12]; UK Ministry of Defence (2021), *Integrated Operating Concept*, Development, Concepts and Doctrine Centre: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014659/Integrated_Operating_Concept_2025.pdf [2022-07-12].



Figur 3 - Den kompletta modellen för det tillänkta strategiska planerandet av brittisk militär kommunikation, se: UK Ministry of Defence, *Defence Strategic*, s. 19. MOD Crown Copyright©

Utöver ett ambitiöst strategiskt planerande har Storbritanniens militär kommit långt med att utveckla den mer operativa förmågan i informationsmiljön, med brittiska arméns 77:e brigad som det tydligaste exemplet.⁸³ Enheten, vars verksamhet till stor del är hemligstämplad, skapades 2015 och målsättningen då var att den skulle ha 1 500 anställda, både militära och civila.⁸⁴ Syftet med brigaden är att ”utmana svårigheterna med modern krigföring genom att använda icke-dödliga metoder och legitima icke-militära påtryckningsmedel för att förändra beteenden hos motståndare och deras stridskrafter”.⁸⁵ Enligt medierapporter ägnar sig 77:e brigaden åt att analysera olika målgrupper, aktörer och motståndare, att följa utvecklingen av attityder och känslor genom att analysera stora mängder data från sociala medier, samt att själva producera och sprida innehåll på en rad digitala plattformar.⁸⁶

Under sina verksamhetsår har dock den 77:e brigaden varit kontroversiell, i synnerhet vad gäller frågan om dess verksamhet även riktas mot brittiska medborgare, och inte bara används i samband med militära operationer utomlands.⁸⁷ Detta blev särskilt aktuellt när det framkom att 77:e brigaden gav den brittiska regeringen stöd att ”bekämpa desinformation” i samband med covidpandemin.⁸⁸ Det gav upphov till kritik,⁸⁹ liksom ett antal konspirationsteorier kopplade till debatten om covid,⁹⁰ vilket följdes av att den brittiska regeringen förnekade att 77:e brigaden ”genomför operationer riktade mot inhemsk brittisk publik”.⁹¹

⁸³ Rid, *Active Measures*, s. 126.

⁸⁴ Ewen MacAskill (2015), ”British Army Creates Team of Facebook Warriors”, *The Guardian*, 31 januari: <https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade> [2022-06-22].

⁸⁵ För öppen information om brigaden, se: British Army, ”77th Brigade: Influence and Outreach”, hemsida: <https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/> [2022-06-22].

⁸⁶ Carl Miller (2018), ”Inside the British Army’s Secret Information Warfare Machine”, *The Wired*, 14 november: <https://www.wired.co.uk/article/inside-the-77th-brigade-britains-information-warfare-military> [2022-06-22].

⁸⁷ Greg Russell (2019), ”’Vile’ Abuse After SNP MP Says Boris Bots Attack Scotland”, *The National*, 24 augusti: <https://www.thenational.scot/news/17858200.vile-abuse-snp-mp-says-boris-bots-attack-scotland/> [2022-06-22].

⁸⁸ Gov.uk (2020), ”COVID Support Force: the MOD’s Contribution to the Coronavirus Response”, 12 juni: <https://www.gov.uk/guidance/covid-support-force-the-mods-contribution-to-the-coronavirus-response> [2022-06-22].

⁸⁹ Chris King och David Miller (2020), ”UK Information Operations in the Time of Coronavirus”, *Daily Maverick*, 30 september: <https://www.dailymaverick.co.za/article/2020-09-30-uk-information-operations-in-the-time-of-coronavirus/> [2022-06-22].

⁹⁰ David Walker (2022), ”Coalition of Chaos? Nasty Nats and Anti-Vaxxers United in Belief about '77th Brigade' Conspiracy Theory”, *Scottish Daily Express*, 8 januari: <https://www.scottishdailyexpress.co.uk/news/scottish-news/coalition-chaos-nasty-nats-anti-25875307> [2022-06-22].

⁹¹ George Allison (2021), ”MoD denies 77th Brigade has Conducted Operations against Scotland”, *UK Defence Journal*, 26 oktober: <https://ukdefencejournal.org.uk/mod-denies-77th-brigade-has-conducted-operations-against-scotland/> [2022-06-22].

4.2 Ny förmåga, nya utmaningar

Som gjorts tydligt i såväl belysningen av den nya informationsmiljön som i den korta genomgången av hur synen på förmågeutvecklingen i den här miljön sett ut i ett antal länder under de senaste decennierna är både manövrering och definiering fortsatta utmaningar, i synnerhet i demokratiska stater. I vilka sammanhang en utvecklad förmåga ska användas, vem som ska utöva den och av vilket slag den ska vara är alltså omdebatterat.

En given förutsättning för militärstrategisk verksamhet i informationsmiljön är att den tenderar att ske i sammanhang där gränsdragning är svårt. I en värld där information rör sig så fritt som i dag är de fysiska landgränserna nästan utsuddade ur ett informationsperspektiv; gränsen mellan krig och fred är otydlig och gränsen mellan aktiva fientliga handlingar och legitim åsiktsbildning är ofta svår att dra. Bakom detta ligger också problemet att identifiera och attribuera specifika handlingar i den moderna informationsmiljön. Det är de här förutsättningarna som ofta brukar sammanfattas i begreppet ”gråzon” – en zon där vanliga hållpunkter, juridiska såväl som geografiska och politiska, är suddiga.⁹²

Vad kan då hända när en demokratiskt styrd rättsstat med lagar och fungerande maktfördelning, där lagen tydligt definierar gränser mellan hemlandet och omvärlden liksom mellan fred och krig, ändå försöker utveckla den här förmågan? Ett land som det är värt att dröja vid med den här frågan i åtanke är Kanada. År 2015 påbörjade den kanadensiska försvarsmakten ett initiativ för att öka förmågan i form av ”militärstrategisk kommunikation”.⁹³ Det var ett vittomfattande projekt som i stora drag hade samma ursprung som liknande initiativ i andra länder (förändringarna i informationsmiljön i kombination med antagonistiska makters ökade aktiviteter).⁹⁴ På många sätt siktade det mot att utveckla liknande förmågor – att kunna utföra ”informationsoperationer [...] som kan riktas, nå effekt, påverka och attackera till stöd för militära operationer”.⁹⁵ Men i det kanadensiska fallet gick det snett. Fem år senare, under hösten 2020, havererade projektet till följd av bred, negativ uppmärksamhet i kanadensiska medier. Rubriken på en av artiklarna som skrevs om projektet lød: ”Kanadas militär vill etablera en ny organisation som ska använda propaganda och andra tekniker för att påverka kanadensare.”⁹⁶

⁹² Om gråzonsproblematik och definitioner, se: Daniel K. Jonsson, Jenny Ingemarsdotter, Bengt Johansson, Niklas H. Rossbach, Christoffer Wedebrand och Camilla Eriksson (2019), *Civilt försvar i gråzon*, FOI-R--4769--SE, Totalförsvarets forskningsinstitut, Stockholm, s. 24-41: <https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4769--SE> [2022-08-08].

⁹³ David Pugliese (2015), ”Chief of the Defence Staff Gen. Jon Vance and the ‘Weaponization of Public Affairs’”, *Ottawa Citizen*, 21 september: <https://ottawacitizen.com/news/national/defence-watch/chief-of-the-defence-staff-gen-jon-vance-and-the-weaponization-of-public-affairs> [2022-06-22].

⁹⁴ Canada National Defence (2017), *Strong, Secure, Engaged – Canada’s Defence Policy*, s. 53: <http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf> [2022-06-22].

⁹⁵ Canada National Defence, *Strong, Secure*, s. 41.

⁹⁶ David Pugliese (2020), ”Canadian Military Wants to Establish New Organization to Use Propaganda, Other Techniques to Influence Canadians”, *Ottawa Citizen*, 2 november:

I en efterföljande post mortem-rapport från den oberoende organisationen *Canadian Global Affairs Institute* konstateras att det för den kanadensiska militären absolut finns ett behov av ”en verksamhetsöverskridande, gemensam, integrerad civil/militär förmåga [i informationsmiljön], med skickliga utövare som opererar med passande instruktioner, lämplig befogenhet, effektiv styrning och genuin tillsyn för att ge stöd åt inhemska och internationella operationer”.⁹⁷ Det var dock inte det som skapats under projektets gång. I stället rörde det sig om ett illa styrt projekt med vaga instruktioner, som kom att präglas av både gränsdragnings-, legalitets- och legitimitetsproblem.

Det finns mycket att tillägga om omständigheterna kring fallet med det kanadensiska projektet. I det här sammanhanget räcker det med att konstatera de centrala felsteg som förefaller ha gjorts. Det handlade dels om att gränsen mellan vad som kan göras i samband med operationer utomlands och vad som kan göras inhemskt i Kanada var suddig och överskreds.⁹⁸ Dels handlade det om hur gränsen mellan informerande myndighetskommunikation (som på engelska kallas *public affairs*) och offensiva militära informationsoperationer (*information operations* och *PSYOPS*) kom att lösas upp under projektets gång, både organisatoriskt och i den praktiska verksamheten.⁹⁹ Under allt detta verkade det enligt rapporten ha funnits en bristande förankring i och förståelse för den existerande lagstiftningen, liksom avsaknad av målenlig uppdatering av interna riktlinjer, föreskrifter och policyer.¹⁰⁰

4.3 Avslutande diskussion

Den både likriktade och heterogena utveckling av nya militära förmågor i informationsmiljön som beskrivits ovan har skett i många länder. Den har drivits av en dynamik som både berott på förändringar i själva miljön och ett slags konkurrens där motståndarens uppfattade förmåga lett till motåtgärder, vilket drivit vidare utveckling – med andra ord, ett slags kapprustning.

Den initiala arbetsdefinitionen av informationsmiljön som *en beskrivning av nät-verksrelationer mellan informationsteknik, information och aktörer*, kan mot bakgrund av hur militära aktörer förstår informationsmiljön, kompletteras med att

<https://ottawacitizen.com/news/national/defence-watch/canadian-military-to-establish-new-organization-to-use-propaganda-other-techniques-to-influence-canadians> [2022-06-22].

⁹⁷ Brett Boudreau (2022), *The Rise and Fall of Military Strategic at National Defence 2015-2021: A Cautionary Tale for Canada and NATO and a Roadmap for Reform*, Canadian Global Affairs Institute, s. 3.

⁹⁸ Det som fick mest uppmärksamhet rörde hur den kanadensiska militären under coronapandemin samlade information om kanadensare på sociala medier. Boudreau, *The Rise and Fall*, s. 48-50.

⁹⁹ Boudreau, *The Rise and Fall*, s. 24-27.

¹⁰⁰ Boudreau, *The Rise and Fall*, s. 25-26.

militärstrategisk kommunikation handlar om *koordinerade kommunikativa handlingar och strategier i syfte att uppfylla nationellt uppsatta mål genom att informera eller påverka utvalda målgrupper*.¹⁰¹

Det står dock klart att det finns fundamentala skillnader i utvecklingen mellan det som sker i auktoritära och i demokratiska länder. Baserat på politiska, ideologiska, kulturella, juridiska och administrativa skillnader finns ett uppenbart större handlingsutrymme hos auktoritära stater att dra nytta av de skuggsidor i informationsmiljöns förändrade terräng som beskrivits i detalj i tidigare kapitel. Samtidigt finns en styrka hos demokratiska rättsstater – som uppmärksamats av de auktoritära länderna, men i mycket lägre grad av de demokratiska – gällande mer grundläggande värderingar och friheter, som kan ha både offensiva (locka, övertyga) och defensiva (kritiskt tänkande, mångfald, förtroende) effekter.¹⁰²

Oavsett dessa fundamentala skillnader – som givet inriktningen på mycket av det som skrivits och gjorts i informationsmiljön under senare år är väl värda att utreda närmare – behöver liberala demokratier fortsätta att utveckla nya förmågor även på ett mer praktiskt, operativt plan. Slutsatserna av de ansträngningar som gjorts hittills, och som beskrivits ovan, är dock att det inte är en lättvindig uppgift.

Utmaningarna gäller särskilt verksamhetens *dimensioner*: Kan – och bör – en demokrati koordinera och rikta sina informationsinsatser så brett att det når samma effekt som auktoritära staters myndighetsöverskridande politiska krigföring? Och vad är resultatet om så inte sker? Men det gäller även verksamhetens *inriktning* och *sammanhang*. Insatser i informationsmiljön kopplade till militära operationer i utlandet är en sak (även om det fortfarande finns frågor kring användandet av ”svart” propaganda, som de fejkade amerikanska konton som nyligen avslöjades), men vad ska militären göra på hemmaplan, och i fredstid? Gråzonen har blivit viktigare, men många kämpar fortfarande med gränsdragningsfrågorna, att hitta en balans mellan att aktivt försvara demokratin i informationsmiljön och samtidigt undvika att skada friheterna som hör till samma demokratis fundament.

Oavsett vilka vägar som väljs finns viktiga lärdomar för att skapa militärstrategisk kommunikation i rapporten om det havererade kanadensiska initiativet som beskrevs ovan. Den avslutas med en lista över rekommendationer, varav flera har tydlig bäring på det arbete som pågår i andra demokratiska länder.¹⁰³ Där konstateras att militär förmåga i informationsmiljön är en mycket komplex utmaning. Därför bör arbetet med utveckling struktureras därefter – vad gäller såväl ledning som sakkunskap och tillsyn. Vidare menar rapportförfattaren att det är viktigt att

¹⁰¹ Parafraserad definition av: "[S]trategic communication as coordinated actions, messages, images, and other forms of signaling or engagement intended to inform, influence, or persuade selected audiences in support of national objectives." Från: Christopher Paul (2011), *Strategic Communication: Origins, Concepts, and Current Debates* (Santa Barbara, Denver och Oxford: Praeger), s. 3.

¹⁰² För vidare diskussion om styrkor och svagheter i liberala demokratier och auktoritära regimer på den storpolitiska arenan, se: Kroenig, *The Return*.

¹⁰³ Boudreau, *The Rise and Fall*, s. 69-75.

utgå både från den kunskap och förmåga som redan finns inom organisationen, och från de erfarenheter som samlats i andra länder. Men den kanske viktigaste lärdomen från det kanadensiska projektet är att förtroende är avgörande i liberala demokratier, varför öppenhet i kommunikationen kring arbetet med att utveckla förmåga i informationsmiljön är centralt.

5 Sammanfattande slutsatser

Syftet med den här rapporten är att klargöra konturerna för informationsmiljön med fokus på skydd och verkan i tider av konflikt och krig,

Rapporten har utgått från en bred arbetsdefinition av informationsmiljön: *Informationsmiljön är en beskrivning av nätverksrelationer mellan informationsteknik, information och aktörer.*

Dagens informationsmiljö kännetecknas av en snabb och oförutsägbart teknisk utveckling. Ny teknologi och nya tekniker skapas och sprids innan deras samhällsliga och politiska konsekvenser förstås. Forskning, lagar och regler blir snabbt obsoleta. Informationsmiljön bidrar även till ett uppluckrande av gränser – inte bara geografiska, utan även konceptuella, som den mellan krig och fred (det som brukar benämnas gråzonen).

Det pågår i dag en kamp mellan såväl statliga som privata aktörer om att kontrollera informationsmiljön. Digitala plattformar, i synnerhet sociala medier, har likt internets infrastruktur i ökande grad kommit i fokus för stormakternas rivalitet och rör frågor som kontroll av teknisk utveckling och informationskontroll.

Medan informationskrigföring är ett tusenårigt fenomen har dagens tekniska utveckling inneburit att digital kommunikation blivit en integrerad del av modern krigföring. Informationskrigföring består av två förgreningar: en teknisk och en psykologisk. Till den tekniska räknas cyberoperationer, men även teleoperationer. Till den psykologiska förgreningen, som är i fokus för föreliggande rapport, räknas informations- och påverkansoperationer.

Den digitala informationsmiljön påverkar människan på många olika sätt. Forskningen om relationen mellan informationsmiljön och människan är i sin linda och i många fall motsägelsefull, men några grundläggande observationer kan ändå göras.

För att förstå hur människan påverkas är kognition centralt, och då inte minst uppmärksamhet. Lättkonsumerad och ofta negativt inramade budskap tenderar att lättare fånga människans uppmärksamhet än djuplodande och komplexa budskap. Vidare är människor selektiva i hur vi inhämtar och avfärdar information, samtidigt som vi tenderar att överskatta just vår egen förmåga att ställa oss över våra egna kognitiva begränsningar.

Kognition sker dock inte i ett vakuum. Människan är en affektiv och social varelse. Kognition bör således förstås i relation till hur den samspelar med känslor och identitet (socialt, kulturellt, etniskt och politiskt), där relationen mellan gruppen och individen handlar lika mycket om gruppen i individen som individerna i gruppen. Detta är särskilt viktigt i förståelsen av hur informationspåverkan fungerar eftersom det är när påverkan sker på grupp- eller samhällsnivå som konsekvenserna får en större effekt.

En något förbisedd aspekt i militärstrategisk kommunikation är digitala subkulturer och de olika medieekologier som har vuxit fram på internet, vars snabbhet i att svärmarbeta fram information är enastående – likaså är deras potential att sprida falskheter och desinformation i multiplattforma informationsoperationer.

Effekten av manipulation och propaganda som sker i informationsmiljön är dock svår att mäta – precis som att de exakta orsakerna för polarisering är svåra att isolera från varandra. Informationsmiljöns potential för manipulation och påverkan ska heller inte överskattas.

Militära institutioner över hela världen arbetar i dag med att öka sin förmåga i informationsmiljön – till den grad att man kan skönja en kapprustning i området. Arbetet präglas mycket av skillnaderna i att utveckla denna förmåga i ett auktoritärt kontra ett demokratiskt sammanhang. Baserat på politiska, ideologiska, kulturella, juridiska och administrativa skillnader finns ett uppenbart större handlingsutrymme hos auktoritära stater att dra nytta av skuggsidorna i informationsmiljöns förändrade terräng. Samtidigt finns en styrka hos demokratiska rättsstater gällande mer grundläggande värderingar och friheter, som kan ha både offensiva (locka, övertyga) och defensiva (kritiskt tänkande, mångfald, förtroende) effekter.

För ökad förmåga avseende skydd och verkan i informationsmiljön krävs en god kunskap om tekniska, mänskliga, politiska och juridiska förutsättningar för att verka i den. Militär förmåga i informationsmiljön är en mycket komplex utmaning, särskilt för demokratiska rättsstater där förtroende för myndigheter och stater är avgörande.

Arbetet med att utveckla förmåga för skydd och verkan i informationsmiljön bör struktureras mot rapportens slutsatser – vad gäller såväl ledning som sakkunskap och tillsyn. I en mening handlar det om att skynda långsamt, bland annat genom att utgå från den kunskap och förmåga som redan finns, såväl generellt som inom den aktuella organisationen, att lära sig från andra länders erfarenheter och att sträva efter öppenhet i kommunikationen kring arbetet med att utveckla förmåga i informationsmiljön.

6 Referenser

- Abdyraeva, C. 2020. *Information Warfare Operations in the Cyber Domain*. OIIP - Austrian Institute for International Affairs: <https://www.oaip.ac.at/cms/media/107-working-paper-cyberspace-in-the-context-of-hybrid-warfare.pdf> [2022-08-08].
- Acerbi, A. 2019. "Cognitive Attraction and Online Misinformation." *Palgrave Communications* (5)15: 1-7.
- Aceves, W. J. 2019. "Virtual Hatred: How Russia Tried to Start a Race War in the United States." *Michigan Journal of Race & Law* 24: 177-250.
- Ajir, M. och B. Vailliant. 2018. "Russian Information Warfare: Implications for Deterrence Theory." *Strategic Studies Quarterly* 12(3): 70-89.
- Albright, D., P. Brannan och C. Walrond. 2010. *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*. Institute for Science and International Security (ISIS), 22 december: https://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf [2022-08-07].
- Allen P. D. och D. P. Gilbert Jr. 2010. "Qualifying the Information Sphere as a Domain." *Journal of Information Warfare* 9(3): 39-50.
- Allison, G. 2021. "MoD denies 77th Brigade Has Conducted Operations against Scotland." *UK Defence Journal*, 26 oktober: <https://ukdefencejournal.org.uk/mod-denies-77th-brigade-has-conducted-operations-against-scotland/> [2022-06-22].
- Almén, O. 2020. *The Chinese Communist Party and the Diaspora – Beijing's Extraterritorial Authoritarian Rule*. Stockholm: FOI-R--4933—SE, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4933--SE> [2022-07-12].
- Alford, M. 2010. *Reel Power: Hollywood Cinema and American Supremacy*. London och New York: Pluto Press.
- Althuis, J. 2021. "How U.S. Government Fell in and out of Love with Strategic Communications." *Defence Strategic Communications* 10: 71-110.
- Anderson, B. 2006. *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. London och New York: Verso.

- Andersson, J. 2021. *Svenskarna och internet 2021*, Internetstiftelsen:
<https://svenskarnaochinternet.se/app/uploads/2021/09/internetstiftelsen-svenskarna-och-internet-2021.pdf> [2022-08-15].
- Andersson, Y. 2016. *Ungar & medier 2021: En statistisk undersökning av ungas medievanor och attityder till medieanvändning*. Statens medieråd, Stockholm.
- Atchley, P. och S. Lane. 2014. "Cognition in the Attention Economy." *Psychology of Learning and Motivation* (61): 133-177.
- Banks, M. A. (2008). *On the Way to the Web: The Secret History of Internet and Its Founders*. Berkely och New York: Apress.
- Baptist, J. och J. Gluck. 2021. "The Gray Legion: Information Warfare Within Our Gates." *Journal of Strategic Security* 14(4): 37-55.
- Barbera, P., A. Casas, J. Nagler, P. J. Egan, R. Bonneau, J. T. Jost och J. A. Tucker. 2019. "Who Leads? Who Follows? Measuring Issue Attention and Agenda Setting by Legislators and the Mass Public Using Social Media Data." *American Political Science Review* 113(4): 883-901.
- Barinka, A. 2022. "TikTok Confirms Some China-Based Employees Can Access US User Data." *Bloomberg*, 1 juli:
<https://www.bloomberg.com/news/articles/2022-07-01/tiktok-says-some-china-based-employees-can-access-us-user-data> [2022-07-05].
- Bartlett, J. 2018. *The People vs Tech: How Internet is Killing Democracy*. London: Ebury Press.
- Barrling, K. och C. Garne. 2022. *Saknad: På spaning efter landet inom oss*. Mondial: Stockholm.
- Bayer, J., B. Holznagel, K. Lubianiec, A. Pinteá, J. B. Schmitt, J. Szakács och E. Uskiewicz. 2019. *Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States*. PE 608.864, Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies of the Union, European Union.
- Bednar, J. 2021. "Polarization, Diversity, and Democratic Robustness." *PNAS* 118(50): e2113843118.
- Belanche, D., L. V. Casaló, M. Flavián och S. Ibáñez-Sánchez. 2021. "Understanding Influencer Marketing: The Role of Congruence between Influencers, Products and Consumers." *Journal of Business Research* 132: 186-195.

- Bell, V., D. V. M. Bishop och A. K. Przybylski. 2015. "The Debate over Digital Technology and Young People." *BMJ*: h3064.
- Bergengruen, V. 2022. "How Telegram Became the Digital Battlefield in the Russian-Ukraine War." *Time*, 21 mars: <https://time.com/6158437/telegram-russia-ukraine-information-war/> [2022-07-17].
- Bergh, A. 2019. *Social Network Centric Warfare – Understanding Influence Operations in Social Media*. FFI-rapport 19/01194, Forsvarets forskningsinstitut, Oslo.
- Berry, J. M. och S. Sobieraj. 2014. *The Outrage Industry: Political Opinion Media and the New Incivility*. New York och Oxford: Oxford University Press.
- Berzonsky, M. D. 2011. "A Social-Cognitive Perspective on Identity Construction", i *Handbook of Identity Theory and Research: Volume I*, redigerad av V. L. Vignoles, S. J. Schwartz och K. Luyckx, 51-75. New York: Springer.
- Betz, D. 2019. "The Idea of Hybridity," i *Hybrid Conflicts and Information Warfare*, redigerad av O. Fridman, V. Kabernik och James C. Pearce, 9-24 Lynne Rienner Publishers: Boulder och London.
- Biały, B. 2017. "Social Media - From Social Exchange to Battlefield." *The Cyber Defense Review* 2(2): 69-90.
- Bigler, G. E. 2007. "Strategic Communications and the Decline of US Soft Power," i *Global Legal Challenges: Command of the Commons, Strategic Communications, and Natural Disasters*, redigerad av M. D. Carsten, 217-234. Newport: Naval War College.
- Billig, M. 1995. *Banal Nationalism*. London: Sage.
- Blair, A. M. 2010. *Too Much to Know: Managing Scholarly Information before the Modern Age*. New Haven och London: Yale University Press.
- Bloomenthal, A. 2022. *World's Top Ten Internet Companies*. Investopedia, 17 mars: <https://www.investopedia.com/articles/personal-finance/030415/worlds-top-10-internet-companies.asp> [2022-08-04].
- Boggs, C. och T. Pollard. 2016. *The Hollywood War Machine: U.S. Militarism and Popular Culture*. London och New York: Routledge.
- Boler, M. och E. Davis, red. 2020. *Affective Politics of Digital Media: Propaganda by Other Means*. London och New York: Routledge.

- Borak, M. 2022. "Doxxed, threatened, and arrested: Russia's war on Wikipedia editors." *Rest of World*, 5 september: <https://restofworld.org/2022/russias-6-month-war-on-wikipedia/> [2022-09-15].
- Boudreau, B. 2022. *The Rise and Fall of Military Strategic at National Defence 2015-2021: A Cautionary Tale for Canada and NATO and a Roadmap for Reform*. Canadian Global Affairs Institute.
- Boyle, M. J. 2015. "The Legal and Ethical Implications of Drone Warfare." *The International Journal of Human Rights* 19(2): 105-126.
- Boyte, K. 2017. "An Analysis of the Social-Media Technology, Tactics, and Narratives Used to Control Perception in the Propaganda War Over Ukraine." *Journal of Information Warfare* 16(1): 88-111.
- Bradshaw, S., L-M. Neudert och P. N. Howard. 2018. *Government Responses to Malicious Use of Social Media*. Nato Stratcom CoE, Riga: https://stratcomcoe.org/pdfjs/?file=/publications/download/web_nato_report_-_government_responses-1.pdf?zoom=page-fit [2022-07-09].
- Brady, W. J, M. J. Crockett och J. J. Van Bavel. 2020. "The MAD Model of Moral Contagion: The Role of Motivation, Attention, and Design in the Spread of Moralized Content Online." *Perspectives on Psychological Science* 15(4): 978 –1010.
- Brabham, D. C. 2013. *Crowdsourcing*. Cambridge och London: The MIT Press.
- Brands, H. 2018. "Democracy vs Authoritarianism: How Ideology Shapes Great-Power Conflict." *Survival* 60(5): 61-114.
- Brewster, T. 2022. "Telegram's Billionaire Found Says He's Never Provided Ukrainians' Data to Russia." *Forbes*, 7 mars: <https://www.forbes.com/sites/thomasbrewster/2022/03/07/telegrams-billionaire-founder-says-hes-never-provided-ukrainians-data-to-russia/> [2022-07-17].
- British Army. "77th Brigade: Influence and Outreach." Hemsida: <https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/> [2022-06-22].
- Bro, P. och F. Wallberg. 2014. "Digital Gatekeeping." *Digital Journalism* 2(3): 446-454.
- Broncano-Berrocal, F. och J. A. Carter. 2021. *The Philosophy of Group Polarization: Epistemology, Metaphysics, Psychology*. London and New York: Routledge.

- Bronk, C., G. Collins och D. Wallach. 2022. *Cyber and Information Warfare in Ukraine: What Do We Know Seven Months In?* Baker Institute Issue Brief 09.06.22, Rice University's Baker Institute for Public Policy, Houston: <https://doi.org/10.25613/69E1-WZ16> [2022-09-21].
- Brown, J. D. 2019. *Reflective Practice of Counseling and Psychotherapy in a Diverse Society*. Cham: Springer Macmillan.
- Brundage, M., S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, A. Dafoe, P. Scharre, T. Zeitzoff, B. Filar, H. Anderson, H. Roff, G. C. Allen, J. Steinhardt, C. Flynn, S. Ó hÉigearthaigh, S. Beard, H. Belfield, S. Farquhar, C. Lyle, R. Crootof, O. Evans, M. Page, J. Bryson, R. Yampolskiy och D. Amodoi. 2018. *Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute. University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation och OpenAI: <https://static.rasset.ie/documents/news/2018/02/ai-report.pdf> [2022-04-10].
- Bubola, E. 2022. "Ukraine Acknowledges that the 'Ghost of Kyiv' Is a Myth." *New York Times*, 1 maj: <https://www.nytimes.com/2022/05/01/world/europe/ghost-kyiv-ukraine-myth.html> [2022-07-04].
- Bucht, C. 2021. *Mediebarometern: Tema Generationer*. Nordicom, Göteborg: <https://www.nordicom.gu.se/sv/publications/mediebarometern-2019-tema-generationer> [2022-08-05].
- Bull, T. 2018. *Granskning av Transportstyrelsens upphandling av it-drift*. Ds 2018:6, Näringsdepartementet, Regeringskansliet, Stockholm: <https://data.riksdagen.se/fil/FB3C8AF9-BE36-4E7F-A09B-80D12887C189> [2022-09-15].
- Burrell, J., och M. Fourcade. 2021. "The Society of Algorithms." *Annual Review of Sociology* 47: 213-37.
- Burkart, P. och T. McCourt. 2019. *Why Hackers Win: Power and Disruption in the Network Society*. Oakland: University of California Press.
- BuzzFeedVideo. 2018. "You Won't Believe What Obama Says In This Video! ;)." *YouTube*, 17 april: <https://www.youtube.com/watch?v=cQ54GDm1eL0> [2022-06-30].

- Cadwalladr, C. och E. Graham-Harrison. 2018. "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." *The Guardian*, 17 mars:
<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> [2022-07-30].
- Canada National Defence. 2017. *Strong, Secure, Engaged – Canada's Defence Policy*: <http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf> [2022-06-22].
- Cannelli, B. och M. Musso. 2022. "Social Media as Part of Personal Digital Archives: Exploring Users' Practices and Service Providers' Policies Regarding the Preservation of Digital Memories." *Archival Science* 22: 259-283.
- Center for an Informed Public, Digital Forensic Research Lab, Graphika och Stanford Internet Observatory. 2021. *The Long Fuse: Misinformation and the 2020 Election*. Stanford Digital Repository, Election Integrity Partnership. v1.3.0: <https://stacks.stanford.edu/file/druid:tr171zs0069/EIP-Final-Report.pdf> [2022-07-08].
- Charon, P. och J-B. Jeangène Vilmer. 2021. *Chinese Influence Operations: A Machiavellian Moment*. Institut de Recherche Stratégique de l'Ecole Militaire, Paris: <https://www.irsem.fr/report.html> [2022-07-11].
- Chu, O. J., J. F. Donges, G. B. Robertson och G. Pop-Eleches. 2021. "The Microdynamics of Spatial Polarization: A Model and an Application to Survey Data from Ukraine." *PNAS* 118 (50): e2104194118.
- Clack, T. och L. Selisny. 2021. "From Beijing Bloggers to Whitehall Writers," i *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*, redigerad av Timothy Clack och Robert Johnson, 259-280. London och New York: Routledge.
- Coole, D. 2013. "Agentic Capacities and Capacious Historical Materialism: Thinking with New Materialisms in the Political Sciences. Millennium." *Journal of International Studies* 41(3): 451–469.
- Colley, T. 2020. "Strategic Narratives and War Propaganda." I *The SAGE Handbook of Propaganda*, redigerad av Paul Baines, Nicholas O'Shaughnessy och Nancy Snow, 38-55. London: Sage.
- Congressional Research Service. 2021. *Defense Primer: Information Operations*: <https://sgp.fas.org/crs/natsec/IF10771.pdf> [2022-06-17].

- Connelly, M., J. Fox, S. Goebel och U. Schmidt. 2019. "Prologue: 'Power and Persuasion': Propaganda into the Twenty-First Century," i *Propaganda and Conflict: War, Media and Shaping the Twentieth Century*, redigerad av M. Connelly, J. Fox, S. Goebel och U. Schmidt, 1-11. London och New York: Bloomsbury.
- Connolly, W. E. 2013. "The 'New Materialism' and the Fragility of Things." *Millennium - Journal of International Studies* 41(3): 399–412.
- Cox, J. 2022. "Revealed: Us Military Bought Mass Monitoring Tool That Includes Internet Browsing, Email Data." *Motherboard: Vice*, 21 september: <https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data> [2022-09-23].
- Cox, R. J. 2008. *Personal Archives and a New Archival Calling: Readings, Reflections and Ruminations*. Duluth: Litwin Books.
- Curtis, J. 2021. "How to Defeat the Info-Warfare 'Triad of Deception'." *National Defense*, 5 augusti: <https://www.nationaldefensemagazine.org/articles/2021/8/5/how-to-defeat-the-info-warfare-triad-of-disruption> [2022-06-15].
- Dang, S-M., och A. Strohmaier. 2018. "Collective Collecting: The Syrian Archive and the New Challenges of Historiography." *VIEW Journal of European Television History and Culture* 14(7): 1-15.
- Davenport, T. och J. Beck. 2001. *The Attention Economy: Understanding the New Currency of Business*. Boston: Harvard Business School Press.
- De Grazia, V. 2021. "Soft-Power United States Versus Normative Power Europe: Competing Ideals of Hegemony in the Post– Cold War West, 1990–2015," i *Soft Power Internationalism: Competing for Culture Influence in the 21st Century Global Order*, redigerad av Burcu Baykurt och Victoria de Grazia, 19-59. New York: Columbia University Press.
- Defense Science Board Task Force. 2001. *Report of the Defense Science Board Task Force on Managed Information Dissemination*. Department of Defense, Washington.
- Delwiche, A. 2020, "Computational Propaganda and the Rise of the Fake Audience", i *The SAGE Handbook of Propaganda*, redigerad av P. Baines, N. O'Shaughnessy och N. Snow, 105-125. Los Angeles och London: Sage.
- Diesen, G. 2021. *Great Power Politics in the Fourth Industrial Revolution: The Geoeconomics of Technological Sovereignty*. London och New York: I. B. Tauris.

- Digital Forensic Research Lab. 2022. "Russian War Report: Hacked News Program and Deepfake Video Spread False Zelenskyy Claims." *Atlantic Council*, 16 mars: <https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/> [2022-06-30].
- Dimsdale, J. E. 2021. *Dark Persuasion: A History of Brainwashing from Pavlov to Social Media*. New Heaven och London: Yale University Press.
- Directorate for Financial and Enterprise Affairs. 2016. *Big Data: Bringing Competition Policy to the Digital Era*. DAF/COMP 2016/14, Organisation for Economic Co-operation and Development (OECD): [https://one.oecd.org/document/DAF/COMP\(2016\)14/en/pdf](https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf) [2022-08-05].
- Donovan, J., B. Lewis och B. Friedberg. 2019. "Parallel Ports: Sociotechnical Change from the Alt-Right to Alt-Tech", i *Post-Digital Cultures of the Far Right: Online Actions and Offline Consequences in Europe and the US*, redigerad av M. Fielitz och N. Thurston, 49-65. Bielefeld: Transcript.
- Edney, K., S. Rosen och Y. Zhu (2020). "Introduction", i *Soft Power with Chinese Characteristics: China's Campaigns for Hearts and Minds*, redigerad av K. Edney, S. Rosen och Y. Zhu, 1-23. London och New York: Routledge.
- Edosomwan, S., S. Kalangot Prakasan, D. Kouame, J. Watson och T. Seymour. 2011. "The History of Social Media and its Impact on Business." *The Journal of Applied Management and Entrepreneurship* 16(3): 79-91.
- Eijkman Q. A. och D. Weggemans (2012), "Open Source Intelligence and Privacy Dilemmas: Is it Time to Reassess State Accountability?" *Security and Human Rights* 23(4): 285-296
- Ekman, I. och Nilsson, P-E. 2022. *Folkets underrättelsetjänst - öppna källor, "OSINT" och Ukraina*, FOI Memo: 7888, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI%20Memo%207888> [2022-07-10].
- El-Badawy, E., S. Munasinghe, A. Bulama Bukarti och B. Bianchi. 2022. *Security, Soft Power, and Regime Support: Spheres of Russian Influence in Africa*. Tony Blair Institute for Global Change, London: <https://institute.global/sites/default/files/articles/Security-Soft-Power-and-Regime-Support-Spheres-of-Russian-Influence-in-Africa.pdf> [2022-09-15];
- Elvy, S-A. 2017. "Paying for Privacy and the Personal Data Economy." *Columbia Law Review* 117(6): 1369-1460.

- Eriksson, V. 2021. "Efter Coop-hacket – Kaseya säger att de har fått krypteringsnyckeln." *Computersweden*, 23 juni: <https://computersweden.idg.se/2.2683/1.753896/efter-coop-hacket-kaseya-sager-att-de-fatt-en-krypteringsnyckeln> [2022-06-01].
- Europeiska kommissionen. 2022. *The Digital Services Act Package*. 5 juli: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> [2022-07-11].
- Europaparlamentet och Europeiska rådet. 2016. Förordning (EU) 2016/679. *Europeiska unionens officiella tidning*, 4 maj: L119/1-L119/88.
- European Digital Media Observatory. 2022. "Repository: Fact-Checking Initiatives in the EU (and in the UK)": <https://edmo.eu/fact-checking-activities/> [2022-08-08].
- Evon, D. 2022. "Is This 'Ghost of Kyiv' Video Real?" *Snopes*, 25 februari: <https://www.snopes.com/fact-check/is-this-ghost-of-kyiv-video-real/> [2022-07-04].
- Falkheimer, J. och M. Heide. 2014. *Strategisk kommunikation: En introduktion*. Lund: Studentlitteratur.
- Farkas, J. and C. Neumayer. 2020. "Disguised Propaganda from Digital to Social Media," i *Second International Handbook of Internet Research*, redigerad av J. Hunsinger, M. M. Allen och L. Klastrup, 707-724. Dordrecht: Springer.
- Feher, K. 2021. "Digital Identity and the Online Self: Footprint Strategies – An Exploratory and Comparative Research Study." *Journal of Information Science* 47(2): 192-205.
- Feldstein, S. 2022. *Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?* Carnegie Endowment for International Peace, Washington: https://carnegieendowment.org/files/Feldstein_Internet_shutdowns_final.pdf [2022-07-17].
- Fenton, N. 2010. "Drowning or Waving? New Media, Journalism, and Democracy," i *New Media, Old News*, redigerad av N. Fenton, 3-16. London och Thousand Oaks: Sage.
- Ferguson, C. J. 2018. "The Evolutionary Roots of Media-Based Moral Panics." I *Evolutionary Psychology and Digital Games*, redigerad av Johannes Breuer, Daniel Pietschmann, Benny Liebold och Benjamin P. Lange, s. 118-129. Routledge: London och New York.

- Firth, J., J. Torous, B. Stubbs, J. A. Firth, G. Z. Steiner, L. Smith, M. Alvarez - Jimenez, J. Gleeson, D. Vancampfort, C. J. Armitage, and J. Sarris. 2019. "The 'Online Brain': How the Internet May Be Changing Our Cognition." *World Psychiatry* 18(2): 119–129.
- Fiske, S. T. och S. E. Taylor. 2021. *Social Cognition: From Brains to Culture*. Los Angeles och London: Sage.
- Fletcher, R. och J. Jenkins. 2019. *Polarisation and the News Media in Europe*. Panel for the Future of Technology and the European Parliament: [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634413/EPRS_STU\(2019\)634413_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634413/EPRS_STU(2019)634413_EN.pdf).
- Ford, M. och A. Hoskins. 2022. *Radical War: Data, Attention and Control in the Twenty-First Century*. London: Hurst Publishers.
- Forsén, J. 2021. "Vem bestämmer egentligen över internet?" Internetkunskap: <https://internetkunskap.se/artiklar/sa-funkar-internet/vem-bestammer-egentligen-over-internet/> [2022-06-22].
- Franke, U. 2015. *War by Non-Military Means: Understanding Russian Information Warfare*. FOI-R—4065--SE, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4065--SE> [2022-07-12].
- Free Media Holding. 2022. "легендарний український пілот 'привид києва' вже збив 10 російських літаків – сбу." *Kanal 5*, 27 februari: <https://www.5.ua/ukrayina/lehendarnyi-ukrainskyi-pilot-pryvyd-kyieva-vzhe-zbyv-10-rosiiskykh-litakiv-sbu-269515.html> [2022-07-04].
- Freedom House. 2021. *Freedom on the Net: The Global Drive to Control Big Tech*: https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf [2022-08-02].
- Freeman, W. C. och J. B. Sykes. 2019. *Antitrust and "Big Tech"*, CBS Report R45910. Congressional Research Service, Washington, 11 september: <https://sgp.fas.org/crs/misc/R45910.pdf> [2022-08-05].
- Fried, D. och A. Polyakova. 2018. *Democratic Defense Against Disinformation*, Atlantic Council och EU Disinfo Lab: https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FIN AL.pdf [2022-07-09].
- Friend, J. M. och B. Thayer. 2015. "War and Aggression," i *Evolutionary Perspectives on Social Psychology*, redigerad av V. Zeigler-Hill, L. L. M. Welling och T. K. Shackelford, 375–386. New York och London: Springer.

- Fung, B. 2021. "Parler has now been booted by Amazon, Apple and Google." *CNN Business*, 11 september:
<https://edition.cnn.com/2021/01/09/tech/parler-suspended-apple-app-store/index.html> [2022-08-05].
- Galeotti, M. 2020. *Russian Political War: Moving Beyond the Hybrid*. London och New York: Routledge.
- Gallie, W. B. (1955). "Essentially Contested Concepts." *Proceedings of the Aristotelian Society: New Series* 56 (1955 - 1956): 167-198.
- Garcia-Marques, T., R. R. Silva, R. Reber och C. Unkelbach. 2015. "Hearing a Statement now and Believing the Opposite Later." *Journal of Experimental Social Psychology* 56: 126–129.
- Gellner, E. 1997. *Nationalism*. London: Weidenfeld and Nicolson.
- Gerbaudo, P. 2012. *Tweets and the Streets: Social Media and Contemporary Activism*. London: Pluto Press.
- Gershberg, Z. och S. Illing. 2022. *The Paradox of Democracy: Free Speech, Open Media, and Perilous Persuasion*. Chicago: University of Chicago Press.
- Gertz, G. 2020. "Why Is the Trump Administration Banning TikTok and WeChat?," *Up front – Brookings*, 7 augusti:
<https://www.brookings.edu/blog/up-front/2020/08/07/why-is-the-trump-administration-banning-tiktok-and-wechat/> [2022-06-30].
- Gigerenzer, G. och H. Brighton. 2009. "Homo Heuristicus: Why Biased Minds Make Better Inferences." *TOPICS* 1(1): 107-143.
- Gilardi, F., T. Gessler, M. Kubli och S. Müller. 2022. "Social Media and Political Agenda Setting." *Political Communication* 39(1): 39-60.
- Giles, K. 2016. *Handbook of Russian Information Warfare*. NATO Defense College, Rom.
- Gillis, J. R. 1994. "Memory and Identity: The History of a Relationship," i *Commemorations: The Politics of National Identity*, redigerad av J. R. Gillis, 3-25 (Princeton: Princeton University Press).
- Giordano, J., redigerad av. 2015. *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns*. Boca Raton, London och New York: CRC Press.

- Grauer, Y. 2022. *Security and Privacy of VPNs Running on Windows 10*. Consumer Reports och Digital Lab: <https://digital-lab-wp.consumerreports.org/2021/12/07/consumer-reports-digital-lab-evaluates-the-security-and-privacy-of-vpns-running-on-windows-10/> [2022-07-30].
- Gough, S. L. och F. Jones. 2003. *The Evolution of Strategic Influence*. U.S. Army War College, Pennsylvania.
- Gov.uk. 2020. "COVID Support Force: the MOD's contribution to the coronavirus response." 12 juni: <https://www.gov.uk/guidance/covid-support-force-the-mods-contribution-to-the-coronavirus-response> [2022-06-22].
- Graphika och Stanford Internet Observatory. 2022. *Unheard Voice – Evaluating Five Years of Pro-Western Covert Influence Operations*: https://public-assets.graphika.com/reports/graphika_stanford_internet_observatory_report_unheard_voice.pdf [2022-09-20]
- Greifeneder, R., M. E. Jaffé, E. J. Newman och N. Schwarz. 2021. "What is New and True About Fake News?," i *The Psychology of Fake News: Accepting, Sharing, and Correcting Misinformation*, redigerad av R. Greifeneder, M. E. Jaffé, E. J. Newman och N. Schwarz, 1-8. London och New York: Routledge.
- Grimmer, J., M. E. Roberts och B. M. Stewart. 2022. *Text as Data: A New Framework for Machine Learning and the Social Sciences*. Princeton och Oxford: Princeton University Press.
- Grisé, M., A. Demus, Y. Shokh, M. Kepe, J. W. Welburn och K. Holynska. 2022. "Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation." RAND Corporation: https://www.rand.org/pubs/research_reports/RRA198-8.html.
- Guess, A. M., M. Lerner, B. Lyons, J. M. Montgomery, B. Nyhan, J. Reifler och N. Sircar. 2020. "A Digital Media Literacy Intervention Increases Discernment Between Mainstream and False News in the United States and India," *PNAS* 117(27): 15536-15545.
- Hadlington, L. och K. Murphy. 2018. "Is Media Multitasking Good for Cybersecurity? Exploring the Relationship Between Media Multitasking and Everyday Cognitive Failures on Self-Reported Risky Cybersecurity Behaviors." *Cyberpsychology, Behavior, and Social Networking* 21(3): 168-172.
- Haidt, J. 2013. "Moral Psychology for the Wwenty-First Century." *Journal of Moral Education* 42(3): 281-297.

- Hallahan, K., D. Holtzhausen, B. van Ruler, D. Verčič och K. Sriramesh. 2007. "Defining Strategic Communication." *International Journal of Strategic Communication* 1(1): 3–35.
- Hallberg, J., J. Bengtsson och H. Karlzén. 2016. *Beskriva och bedöma hot mot IT-system. Varför är det svårt?* FOI-R--4330--SE, Totalförsvarets forskningsinstitut, Stockholm.
- Hamid, S. 2022. "The Forever Culture War." *The Atlantic*, januari 8: <https://www.theatlantic.com/ideas/archive/2022/01/republicans-democrats-forever-culture-war/621184/> [2022-06-29].
- Harmon-Jones, E., T. F. Price och P. A. Gable. 2012. "The Influence of Affective States on Cognitive Broadening/Narrowing: Considering the Importance of Motivational Intensity." *Social and Personality Psychology Compass* 6(4): 314–32
- Harris, L. T., och S. T. Fiske. 2006. "Dehumanizing the Lowest of the Low: Neuroimaging Responses to Extreme Out-Groups." *Psychological Science* 17(10): 847–853.
- Haselton, M., G. A. Bryant, A. Wilke, D. A. Frederick, A. Galperin, W. E. Frankenhuis och T. Moore. 2009. "Adaptive Rationality: An Evolutionary Perspective on Cognitive Bias." *Social Cognition* 27(5): 733-763.
- Hastings, A. 1997. *The Construction of Nationhood: Ethnicity, Religion and Nationalism*. Cambridge: Cambridge University Press.
- Hawks, J., E. T. Wang, G. M. Cochran, H. C. Harpending och R. K. Moyzis. 2007. "Recent Acceleration of Human Adaptive Evolution." *PNAS* 104(52): 20753-20758.
- Hayden, C. och E. T. Metzgar (2019). "Strategic Communication and Security," i *The Handbook of Communication and Security*, redigerad av Bryan C. Taylor och Hamilton Bean, 185-202 (New York: Taylor & Francis).
- Hedtjärn Swaling, V. och J. Johansson. 2018. *NCS3 studie – IoT-relaterade risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem*. FOI-R—4591—SE, Totalförsvarets forskningsinstitut, Stockholm.
- Heersmink R. 2016. "The Internet, Cognitive Enhancement, and the Values of Cognition." *Minds and Machines* 26: 389 - 407.

- Helgason, A., A. W. Einarsson, V. B. Guðmundsdóttir, Á. Sigurðsson, E. D. Gunnarsdóttir, A. Jagadeesan, S. S. Ebenesersdóttir, A. Kong och K. Stefánsson. 2015. "The Y-Chromosome Point Mutation Rate in Humans." *Nature Genetics* 47: 453–457.
- Hertenberg, B. I. och J. Bjønebye. 2021. *Prosjekt MilStratKom: Militærstrategisk Kommunikasjon og Forsvarets bidrag til Nasjonal Strategisk Kommunikasjon - intern utredningsrapport till det norske Forsvaret*, Haeret, Oslo.
- Higdon, N. 2020. *Anatomy of Fake News*. Oakland: University of California Press.
- Hill, S. och P. Bradshaw. 2018. *Mobile-First Journalism: Producing News for Social and Interactive Media*. New York: Routledge.
- Himmelboim, I. och G. J. Golan. 2019. "A Social Networks Approach to Viral Advertising: The Role of Primary, Contextual, and Low Influencers." *Social Media + Society* 5(3): 1-13.
- Hoffmann, S., D. Lazanski och E. Taylor. 2020. "Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet." *Journal of Cyber Policy* 5(2): 239-264.
- Hogg, M. A. och D. Abrams. 2006. *Social Identifications: A Social Psychology of Intergroup Relations and Group Processes*. London och New York: Routledge.
- Holtzhausen, D. och A. Zerfass. 2015. "Strategic Communication Opportunities and Challenges of the Research Area," i *The Routledge Handbook of Strategic Communication*, redigerad av D. Holtzhausen och A. Zerfass, 1-17. New York: Routledge.
- Hopkin, J. och B. Rosamond. 2018. "Post-truth Politics, Bullshit and Bad Ideas: 'Deficit Fetishism' in the UK." *New Political Economy* 23(6): 641-655.
- Hornsey, M. J. 2008. "Social Identity Theory and Self-Categorization Theory: A Historical Review." *Social and Personality Psychology Compass* 2: 204–222.
- Horwitz, J. och D. Volz. 2019. "FBI Surveillance Proposal Sets Up Clash With Facebook." *The Wall Street Journal*, 8 augusti: https://www.wsj.com/articles/fbi-and-facebook-potentially-at-odds-over-social-media-monitoring-11565277021?mod=hp_lead_pos1 [2022-08-01].
- Howard, P. N. 2020. *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*. Yale University Press: New Haven och London.

- Huang, J., S. Kumar and C. Hu. 2021. "A Literature Review of Online Identity Reconstruction." *Frontiers of Psychology* 12: 696552.
- Iasiello, E. J. 2017. "Russia's Improved Information Operations: From Georgia to Crimea," *The US Army War College Quarterly: Parameters* 47(2): 51-63.
- Insikt Group. 2019. *The Price of Influence: Disinformation in the Private Sector. Recorded Future - Cyber Threat Analysis*: <https://go.recordedfuture.com/hubfs/reports/cta-2019-0930.pdf> [2022-07-15].
- Integritetsskyddsmyndigheten. 2021. "Biometri." 5 maj: <https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/arbetsliv/biometri/> [2022-07-07].
- International Telecommunication Union. 2022. *Global Connectivity Report 2022*. ITU Publications, Genève: <https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/> [2022-08-05].
- Internetstiftelsen. "Internet är en fluga": <https://www.internetmuseum.se/tidslinjen/internet-ar-en-fluga/> [2022-06-02].
- Internetstiftelsen. "Internetmuseum": <https://www.internetmuseum.se/> [2022-07-07].
- Iyengar, S., Y. Lelkes, M. Levendusky, N. Malhotra och S. J. Westwood. 2019. "The Origins and Consequences of Affective Polarization in the United States." *Annual Review of Political Science* 22(7): 7.1–18.
- Jaillant, L., K. Aske, E. Goudarouli och N. Kitcher. 2022. "Introduction: Challenges and Prospects of Born-Digital and Digitized Archives in the Digital Humanities." *Archival Science* [online first].
- Jahn, B. 2019. "The Sorcerer's Apprentice: Liberalism, Ideology, and Religion in World Politics." *International Relations* 33(2): 322-337.
- Jankowicz, N. 2020. *How to Lose the Information War: Russia, Fake News, and the Future of Conflict*. London och New York: I. B. Tauris.
- Jeangène Vilmer, J-B. 2019. *The "Macron Leaks" Operation: A Post-Mortem*. Atlantic Council och Institut de recherche stratégique de l'École militaire: <https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem/> [2022-08-08].
- Jenkins, T. 2012. *The CIA in Hollywood: How the Agency Shapes Film and Television*. Austin: University of Texas Press.

- Johnson, D. D. P. och D. Tierney. 2011. "The Rubicon Theory of War: How the Path to Conflict Reaches the Point of No Return." *International Security* 36(1): 7–40.
- Johnson, R. och T. Clack. 2021. "Introduction: The World Information War." i *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*, redigerad av Timothy Clack och Robert Johnson, 1-18. London och New York: Routledge.
- Jonsson, D. K., J. Ingemarsdotter, B. Johansson, N. H. Rossbach, C. Wedebrand och C. Eriksson. 2019. *Civilt försvar i gråzon*. FOI-R--4769--SE, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4769--SE> [2022-08-08].
- Juršėnas, A., K. Karlauskas, E. Ledinauskas, G. Maskeliūnas och J. Ruseckas. 2021. *The Double-Edged Sword of AI: Enabler of Disinformation*. NATO Strategic Communications Centre of Excellence, Riga: <https://stratcomcoe.org/pdfjs/?file=/publications/download/The-Double-Edged-Sword-of-AI-DIGITAL-FINAL.pdf?zoom=page-fit> [2022-08-07].
- Kahneman, D. 2011. *Thinking Fast and Slow*. New York: Farrar, Straus and Giroux.
- Kaldor, M. 2013. "Identity and War." *Global Policy* 4(4): 336-346.
- Kammarrätten. 2022. *Dom i mål nr 5222-21*. Stockholm, 22 juni.
- Kan, I. P., K. L. Pizzonia, A. B. Drummey och E. J. V. Mikkelsen. 2021. "Exploring Factors that Mitigate the Continued Influence of Misinformation." *Cognitive Research: Principles and Implications* 6(76): 1-33.
- Kang, C. 2021. "Lawmakers, Taking Aim at Big Tech, Push Sweeping Overhaul of Antitrust." *The New York Times*, 29 juni: <https://www.nytimes.com/2021/06/11/technology/big-tech-antitrust-bills.html> [2022-08-05].
- Kaplan, A. 2022. *Artificial Intelligence, Business and Civilization: Our Fate Made in Machines*. London och New York: Routledge.
- Kaplan, A. M. och M. Haenlein. 2010. "Users of the world, unite! The Challenges and Opportunities of Social Media." *Business Horizons* 53: 59-68.

- Karlzén, H. 2020. *Cyberoperationer, en slutrapport*. FOI-R--5072--SE, Totalförsvarets forskningsinstitut, Stockholm:
<https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--5072--SE>
 [2022-08-08].
- Karlzén, H. 2021. *Honungsfällor - Att vilseleda och studera cyberangripare*. FOI-R--5217--SE, Totalförsvarets forskningsinstitut, Stockholm:
<https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--5217--SE>
 [2022-08-08].
- Kavanagh, J. och M. D. Rich. 2018. *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*. Santa Monica: Rand.
- Kee Loh, K. och R. Kanai. 2016. "How Has the Internet Reshaped Human Cognition?" *Neuroscientist* 22: 506 - 20.
- Keller, G. F. "The Influence of Military Strategies on Business Planning." *International Journal of Business and Management* 3(5), 2008: 129-134
- Kelly, K. 2016. *The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future*. New York: Penguin Random House.
- Kemp, S. 2022. "Digital 2022: April Global Statshot Report." *Datareportal*, 21 april: <https://datareportal.com/reports/digital-2022-april-global-statshot>
 [2022-05-30]
- Kemp, S. 2022. "Global Social Media Statistics." *Datareportal*:
<https://datareportal.com/social-media-users> [2022-07-07].
- Kemp, S. 2021. "Social Media Users." *Datareportal*:
<https://datareportal.com/social-media-users> [2022-07-01].
- Kesebir, S. 2012. "The Superorganism Account of Human Sociality: How and When Human Groups Are Like Beehives." *Personality and Social Psychology Review* 16(3): 233-261.
- Khan A., K. Brohman och S. Addas. 2022. "The Anatomy of 'Fake News': Studying False Messages as Digital Objects." *Journal of Information Technology* 37(2): 122-143.
- KhosraviNik, M. och M. Amer. 2022. "Social Media and Terrorism Discourse: The Islamic State's (IS) Social Media Discursive Content and Practices." *Critical Discourse Studies* 19(2): 124-143.

- King, C. och D. Miller. 2020. "UK Information Operations in the Time of Coronavirus." *Daily Maverick*, 30 september:
<https://www.dailymaverick.co.za/article/2020-09-30-uk-information-operations-in-the-time-of-coronavirus/> [2022-06-22].
- Kivva, I. 2022. "The Story of the Song 'In the Meadow, a Red Kalyna'. It Has Changed During the Whole Epochs of National Liberation War." *Zaborona*, 13 april: <https://zaborona.com/en/the-story-of-the-song-in-the-meadow-a-red-kalyna-it-has-changed-during-the-whole-epochs-of-national-liberation-war/> [2022-07-12].
- Kollars, N. A., och M. B. Petersen. 2019. "Feed the Bears, Starve the Trolls." *The Cyber Defense Review* 14-15: 145-160.
- Konger, K. och M. Isaac. 2021. "Twitter Permanently Bans Trump, Capping Online Revolt." *The New York Times*, 12 januari:
<https://www.nytimes.com/2021/01/08/technology/twitter-trump-suspended.html> [2022-08-02].
- Korte, M. 2020. "The Impact of the Digital Revolution on Human Brain and Behavior: Where do We Stand?" *Dialogues in Clinical Neuroscience* 22(2): 101-111.
- Kossowska, M., G. Czarnek, E. Szumowska and P. Szwed. 2022. "Striving for Certainty: Epistemic Motivations and (Un)Biased Cognition," i *Knowledge Resistance in High-Choice Information Environments*, redigerad av J. Strömbäck, Å. Wikforss, K. Glüer, T. Lindholm och H. Oscarsson, 207-221. London och New York: Taylor and Francis.
- Kreuzer, M. P. 2021. "Cyberspace is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age." *The Strategy Bridge*, 8 juli: <https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age> [2022-07-14].
- Krishnan, N., J. Gu, R. Tromble och L. C. Abroms. 2021. "Research Note: Examining how Various Social Media Platforms have Responded to Covid-19 Misinformation." *Harvard Kennedy School Misinformation Review* 6(2): 1-25.
- Kroenig, M. 2020. *The Return of Great Power Rivalry: Democracy Versus Autocracy from the Ancient World to the U.S. and China*. New York: Oxford University Press.
- Kroenig, M., M. McAdam och S. Weber. 2010. "Taking Soft Power Seriously." *Comparative Strategy*, 29(5), s. 422-423.

- Kungliga Ingenjörsvetenskapsakademien. 2019. *Digitalisering för ökad konkurrenskraft*: <https://www.iva.se/globalassets/projekt/201902-iva-digitalisering-slutrapport-l.pdf> [2022-08-04].
- Laity, M. 2018. "NATO and Strategic Communications." *Three Swords Magazine* 33/2018: 65-72:
https://www.jwc.nato.int/images/stories/threeswords/NATO_STRATCOM_2018.pdf [2022-07-11].
- Lange, K. 2018. "How & Why the DOD Works With Hollywood." *Inside DoD*, U.S. Department of Defense, 28 februari:
<https://www.defense.gov/News/Inside-DOD/Blog/article/2062735/how-why-the-dod-works-with-hollywood/> [2022-07-12].
- Lasconjarias, G. och J. A. Larsen. 2015. *NATO's Response to Hybrid Threats*. Rome: NATO Defense College.
- Lazar, J., O. Kaplan, T. Sternberg och R. E. Lubow. 2012. "Positive and Negative Affect Produce Opposing Task-Irrelevant Stimulus Preexposure Effects: Correction to Lazar, Kaplan, Sternberg, & Lubow (2011)." *Emotion* 12(3): 591-604, s. 592.
- Lebow, R. N. 2010. *Why Nations Fight: Past and Future Motives for War*. Cambridge och New York: Cambridge University Press.
- Leese, M och M. Hoijtink. 2019. "How (Not) to Talk about Technology: International Relations and the Question of Agency," i *Technology and Agency in International Relations*, red. M. Hoijtink och M. Leese, , 1-23. Routledge: Abingdon och New York.
- Leigh Armistead, E., redigerad av. 2007. *Information Warfare: Separating Hype from Reality*. Sterling, VA: Potomac Books.
- Leitenberg, M. 2020. "False Allegations of Biological-Weapons Use from Putin's Russia." *Nonproliferation Review* 27(4-6): 425-442.
- Lenoir, T. och L. Caldwell. 2018. *The Military Entertainment Complex*. Massachusetts och London: Harvard University Press.
- Levin, S., O. Solon och S. Walker. 2017. "'Our Pain for Their Gain': The American Activists Manipulated by Russian Trolls." *The Guardian*, oktober 21: <https://www.theguardian.com/world/2017/oct/21/russia-social-media-activism-blacktivist> [2022-06-29].
- Levy, S. 2020. *Facebook: The Inside Story*. New York: Blue Rider Press.
- Lewis, K. och B. Herndon. 2011. "Transactive Memory Systems: Current Issues and Future Research Directions." *Organization Science* 22(5): 1254-1265.

- Lijphart, A. 1999. *Patterns of Democracy: Government Forms and Performance in Thirty-Six Countries*. New Haven: Yale University Press.
- Lilly, B. 2022. *Russian Information Warfare: Assault on Democracies in the Cyber Wild West*. Annapolis: Naval Institute Press.
- Lindgren, E., T. Lindholm, R. Vliegthart, H. G. Boomgaarden, A. Damstra, J. Strömbäck och Y. Tsifti. 2022. "Trusting the Facts: The Role of Framing, News Media as a (Trusted) Source, and Opinion Resonance for Perceived Truth in Statistical Statements." *Journalism & Mass Communication Quarterly* [online first]: 1-24.
- Lindgren, S. 2020. *Data Theory*. Cambridge och Medford: Polity Press.
- Little, G. E., Assistant to the Secretary of Defense. 2012. *Memorandum for Commanders of the Combatant Commands, Office of the Assistant Secretary of Defense, 20301—1400*. Pentagon, Washington:
https://foreignpolicy.com/wp-content/uploads/2015/01/121206_brooksmemo.pdf [2022-07-16].
- Litvinenko, A. 2021. "Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty," *Media and Communication* 9(4): 5-15.
- Lorenz-Spreen, P., L. Oswald, S. Lewandowsky och R. Hertwig. 2022. "Digital Media Democracy: A Systematic Review of Causal and Correlational Evidence Worldwide" [working paper]: 1-40.
- Loveless, M. 2021. "Information and Democracy: Fake News as an Emotional Weapon," i *Democracy and Fake News: Information Manipulation and Post-Truth Politics*, redigerad av S. Giusti och E. Piras, 64-76. London och New York: Routledge.
- Lushenko, P. 2021. "Review of the Special Issue 'Robotics Autonomous Systems and Warfare,' *Small Wars and Insurgencies* 31, 4 June 2020," *Small Wars & Insurgencies* 32(3): 550-570.
- Luttwak, E. N. 2001. *Strategy: The Logic of War and Peace*. Cambridge: Belknap Press of Harvard University Press.
- Ma, A. och B. Gilbert. 2019. "Facebook Understood how Dangerous the Trump-Linked Data Firm Cambridge Analytica Could Be much Earlier than It Previously Said. Here Is Everything that's Happened Up until Now." *Business Insider*, 23 augusti: <https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3?r=US&IR=T> [2022-06-29].

- MacAskill, E. 2015. "British Army Creates Team of Facebook Warriors." *The Guardian*, 31 januari: <https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade> [2022-06-22].
- MacFarquhar, N. 2018. "Inside the Russian Troll Factory: Zombies and a Breakneck Pace." *The New York Times*, 18 februari: <https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html> [2022-07-11].
- Macy, M. W., M. Ma, D. R. Tabin, J. Gao och B. K. Szymanski. 2021. "Polarization and Tipping Points." *PNAS* 118(50): e2102144118.
- Madrigal, A. C. 2019. "The People Who Hated the Web Even Before Facebook." *The Atlantic*, 19 mars: <https://www.theatlantic.com/technology/archive/2019/03/people-who-hated-web-even-before-facebook/584932/> [2022-08-05].
- Malcomson, S. 2016. *Splinternet: How Geopolitics and Commerce are Fragmenting the World Wide Web*. London och New York: OR Books.
- Manyika, J., M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh och A. Hung Byers. 2011. "Big Data: The Next Frontier for Innovation, Competition, and Productivity." *McKinsey Global Institute*: https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/big%20data%20the%20next%20frontier%20of%20innovation/mgi_big_data_exec_summary.pdf [2022-07-11].
- Marcacom. 2022. "La leyenda del 'Fantasma de Kiev', el piloto héroe de Ucrania," *Marcacom*, 25 februari: <https://www.marca.com/tiramillas/actualidad/2022/02/25/62189812ca4741f3518b4575.html> [2022-07-04].
- Mariani, R. 2020. "Evaluation of Brand-Sponsored Influencers and Tactics Across Industries," i *Research Perspectives on Social Media Influencers and their Followers*, redigerad av B. Watkins, 65-86. Lanham, Boulder, New York och London: Lexington Books.
- Marr, B. 2022. *Data Strategy: How to Profit from a World of Big Data, Analytics and Artificial Intelligence*. London, New York och Daryaganj: Kogan Page.
- McAdams, D. P. och K. C. McLean. 2013. "Narrative Identity." *Current Directions in Psychological Science* 22(3): 233-238.
- McCarty, N. 2019. *Polarization: What Everyone Needs to Know*. Oxford och New York: Oxford University Press.

- McCoy, J. och M. Somer. 2019. "Toward a Theory of Pernicious Polarization and How It Harms Democracies: Comparative Evidence and Possible Remedies." *The ANNALS of the American Academy of Political and Social Science* 681: 234-270.
- Miller, C. 2022. "Who's Behind #IStandWithPutin?" *The Atlantic*, 5 april: <https://www.theatlantic.com/ideas/archive/2022/04/russian-propaganda-zelensky-information-war/629475/> [2022-06-15]
- Miller, C. 2018. "Inside the British Army's Secret Information Warfare Machine." *The Wired*, 14 november: <https://www.wired.co.uk/article/inside-the-77th-brigade-britains-information-warfare-military> [2022-06-22].
- Miller, D. 2022. "Who Is the 'Ghost of Kyiv'? Tale of Ukrainian Fighter Pilot Trends on Social Media." *Fox 2 Detroit*, 25 februari: <https://www.fox2detroit.com/news/ghost-of-kyiv-tale-of-ukrainian-fighter-pilot-trends-social-media> [2022-07-04].
- Mok, C. 2022. "The Making of China's Future Internet: A Closer Look on the Fourteenth Five-Year Plan on Digital Economy." Friedrich Naumann Foundation, 18 februari: <https://www.freiheit.org/taiwan/making-chinas-future-internet> [2022-08-02].
- Mounk, Y. 2018. *The People Vs. Democracy: Why Our Freedom Is in Danger and How to Save It*. Cambridge: Harvard University Press.
- Mounk, Y. 2021. "Democracy on the Defense: Turning Back the Authoritarian Tide." *Foreign Affairs* 100(2): 163-173.
- Neisser, U. 2014. *Cognitive Psychology*. Psychology Press: London och New York.
- Niblock, I., S. Hoffman och J. Wallis. 2022. "Chinese and Russian Propaganda Work in Tandem to Blame the West for War in Ukraine." *The Strategist*, Australian Strategic Policy Institute, 26 maj: <https://www.aspistrategist.org.au/chinese-and-russian-propaganda-work-in-tandem-to-blame-the-west-for-war-in-ukraine/> [2022-07-05]
- Nilsson, P-E. 2021. *Från skitpostning till folkmord: ensamagerande våldsverkare, ideologi och accelerationism i den digitala tidsåldern*. FOI-R--5257--SE, Totalförsvarets forskningsinstitut, Stockholm.
- Nothhaft, H., K. Page Werder, D. Verčič och A. Zerfass (2018). "Strategic Communication: Reflections on an Elusive Concept." *International Journal of Strategic Communication* 12(4): 352-366.

- Novelly, T. 2022. "Ukraine's Fighter Ace 'Ghost of Kyiv' May Be a Myth, But It's Lethal as War Morale." *Military.com*, 2 mars: <https://www.military.com/daily-news/2022/03/02/ukraines-fighter-ace-ghost-of-kyiv-may-be-myth-its-lethal-war-morale.html> [2022-07-06].
- Nye Jr., J. S. 2015. *Is the American Century over?* Cambridge och Malden: Polity.
- O'Neil, C. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.
- O'Sullivan, D. och D. Byers. 2017. "Exclusive: Fake Black Activist Accounts Linked to Russian Government." *CNN Business*, september 28: <https://money.cnn.com/2017/09/28/media/blacktivist-russia-facebook-twitter/index.html> [2022-06-29].
- Olsson, S., A. McWilliams, P-E. Nilsson och P. Thunholm. 2022. *Militärstrategisk kommunikation i den kognitiva informationsmiljön*. FOI-R--5307--SE, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--5307--SE> [2022-08-02].
- Ekengren Oscarsson, H., T. Bergman, A. Bergström och J. Hellström. 2021. *Demokratirådets rapport 2021: Polarisering i Sverige*. SNS Förlag, Stockholm.
- Ostrowski, M. S. 2021. *Ideology*. Cambridge: Polity Press.
- Pasquale, F. 2015. *Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge och London: Harvard University Press.
- Patrikarakos, D. 2021. "Homo Digitalis Enters the Battlefield," i *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*, redigerad av Timothy Clack och Robert Johnson, 34-44. London och New York: Routledge.
- Paul, C. 2011. *Strategic Communication: Origins, Concepts, and Current Debates*. Santa Barbara, Denver och Oxford: Praeger.
- Perrett, C. 2022. "Russia's Internet Censorship Is Forcing Citizens to Turn to the Dark Web and VPNs for News, Social Media." *Business Insider South Africa*, 17 mars: <https://www.businessinsider.co.za/what-happens-social-media-and-news-go-dark-in-russia-2022-3> [2022-07-17].

- Persson, T. och S. Widmalm. 2022. "Politisk tolerans och självcensur i orostider," i *Du sköra nya värld*, SOM-undersökningen 2021, SOM-rapport nr 81, redigerad av U. Andersson, H. Oscarsson, B. Rönnerstrand och N. Theorin, 101-118: <https://www.gu.se/som-institutet/resultat-och-publikationer/bocker/du-skora-nya-varld> [2021-07-09].
- Pessoa, L., M. McKenna Benoit, E. Gutierrez och L.G. Ungerleider. 2020. "Neural processing of emotional faces requires attention." *Proceedings of the National Academy of Sciences* 99(17): 11458–11463
- Pew Research Center. 2019. "Experts Optimistic About the Next 50 Years of Digital Life": <https://www.pewresearch.org/internet/2019/10/28/experts-optimistic-about-the-next-50-years-of-digital-life/> [2022-08-08].
- Poe, M. T. 2011. *A History of Communications: Media and Society from the Evolution of Speech to the Internet*. Cambridge och New York: Cambridge University Press.
- Pohle, J. 2020. *Digital Sovereignty. A New Key Concept of Digital Policy in Germany and Europe*. Konrad-Adenauer-Stiftung, Berlin: <https://www.econstor.eu/bitstream/10419/228713/1/Full-text-report-Pohle-Digital-sovereignty.pdf> [2022-08-20].
- Poisel, R. A. 2013. *Information Warfare and Electronic Warfare Systems*. Norwood: Artech House.
- Pomerantsev, P. 2020. *This Is Not Propaganda: Adventures in the War Against Reality*. London: Faber & Faber.
- Pomerantsev, P. och Weiss, M. 2014. *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, The Institute of Modern Russia och The Interpreter, New York: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomera ntsev__The_Menace_of_Unreality.pdf [2022-07-09].
- Porche III, I. R. 2020. *Cyberwarfare: An Introduction to Information-Age Conflict*. Boston och London: Artech House.
- Post- och telestyrelsen. "Allmänt om 5G.": <https://www.pts.se/sv/5g/allmant-om-5g/> [2022-07-08].
- Post- och telestyrelsen. 2020. *Beslut 2020-10-20. Godkännande av sökande samt tillkommande villkor i auktion av frekvensbanden 3,5 GHz och 2,3 GHz*. Dnr: 18-8496, Stockholm.
- Prier, J. 2017. "Commanding the Trend: Social Media as Information Warfare." *Strategic Studies Quarterly* 11(4): 50-85.

- Psykologilexikon. 2022. "Kognition." Natur & Kultur:
<https://www.psykologiguide.se/psykologilexikon/?Lookup=kognition>
 [2022-08-12].
- Pugliese, D. 2015. "Chief of the Defence Staff Gen. Jon Vance and the 'Weaponization of Public Affairs'." *Ottawa Citizen*, 21 september:
<https://ottawacitizen.com/news/national/defence-watch/chief-of-the-defence-staff-gen-jon-vance-and-the-weaponization-of-public-affairs> [2022-06-22].
- Pugliese, D. 2020. "Canadian Military Wants to Establish New Organization to Use Propaganda, Other Techniques to Influence Canadians." *Ottawa Citizen*, 2 november: <https://ottawacitizen.com/news/national/defence-watch/canadian-military-to-establish-new-organization-to-use-propaganda-other-techniques-to-influence-canadians> [2022-06-22].
- Ragnedda, M. och G. Destefanis. 2020. "Blockchain: A disruptive technology," i *Blockchain and Web 3.0: Social, Economic, and Technological Challenges*, redigerad av M. Ragnedda och G. Destefanis, 1-11. Oxon och New York: Routledge.
- Rapp, K. 2021. "Social Media and Genocide: The Case for Home State Responsibility." *Journal of Human Rights* 20(4): 486-502.
- Rekker, R. 2021. "The Nature and Origins of Political Polarization Over Science." *Public Understanding of Science* 30(4): 352–368.
- Reuters Fact Check. 2022. "Fact Check-Doctored Video Appears to Show Putin Announcing Peace." *Reuters*, 17 mars:
<https://www.reuters.com/article/factcheck-putin-address-idUSL2N2VK1CC>
 [2022-06-30].
- Rid, T. 2021. *Active Measures: The Secret History of Disinformation and Political Warfare*. London: Profile Books.
- Rid, T. 2022. "Why You Haven't Heard About the Secret Cyberwar in Ukraine." *The New York Times*, 18 mars.
- Rifkin, J. 2011. *The Third Industrial Revolution: How Lateral Power is Transforming Energy, the Economy, and the World*. New York: Palgrave Macmillan.
- Riggins, S. H. 1997. "The Rhetoric of Othering," i *The Language and Politics of Exclusion: Others in Discourse*, redigerad av S. H. Riggins, 1-30 (Thousand Oaks: Sage).
- Rime, J., C. Pike och T. Collins. 2022. "What is a podcast? Considering Innovations in Podcasting Through the Six-Tensions Framework." *New Media Technologies* [online first]: 1-23.

- Robb, D. L. 2004. *Operation Hollywood: How the Pentagon Shapes and Censors the Movies*. New York: Prometheus Books.
- Ruggeri, K. et al. 2021. "The General Fault in Our Fault Lines." *Nature: Human Behaviour* 5: 1369-1380.
- Russell, G. (2019). "'Vile' Abuse after SNP MP Says Boris Bots Attack Scotland." *The National*, 24 augusti:
<https://www.thenational.scot/news/17858200.vile-abuse-snp-mp-says-boris-bots-attack-scotland/> [2022-06-22].
- Rühlig, T. och M. Björk. 2020. *What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe*. UI Paper 20202/1, Utrikespolitiska institutet, Stockholm.
- Sanovich, S. 2019. "Russia: The Origins of Digital Misinformation," i *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, redigerad av S. C. Woolley och P. N. Howard, 21-40. Oxford och New York: Oxford University Press.
- Santos, F. P., Y. Lelkes och S. A. Levin. 2021. "Link recommendation algorithms and dynamics of polarization in online social networks." *PNAS* 118(50): e2102141118.
- Sasse, G. och A. Lackner. 2018. "War and Identity: The Case of the Donbas in Ukraine." *Post-Soviet Affairs* 34(2-3): 139-157.
- Schmidt, E. och J. Cohen. 2013. *The New Digital Age: Transforming Nations, Businesses, and Our Lives*. New York: Vintage Books.
- Schwartz, J. M. och T. Cook. 2002. "Archives, Records, and Power: The Making of Modern Memory." *Archival Science* 2: 1-19.
- Schwarz, N. och M. Jalbert. 2021. "When (Fake) News Feels True: Intuitions of Truth and the Acceptance of Correction of Misinformation," i *The Psychology of Fake News: Accepting, Sharing, and Correcting Misinformation*, red. R. Greifeneder, M. E. Jaffé, E. J. Newman och N. Schwarz, 73-89 (London and New York: Routledge).
- Seib, P. 2021. *Information at War: Journalism, Disinformation and Modern Warfare*. Cambridge: Polity.
- Sen, A. 2006. *Identity and Violence: The Illusion of Destiny*. New York: W.W. Norton & Co.
- Schuilenburg, M. och R. Peeters, redigerad av. 2021. *The Algorithmic Society: Technology, Power, and Knowledge*. London och New York: Routledge.

- Shemakov, R. 2022. "War in Ukraine Is Fundamentally Changing the Relationship Between the Internet and Geopolitics." *Global Voices*, 28 juli: <https://globalvoices.org/2022/07/28/war-in-ukraine-is-fundamentally-changing-the-relationship-between-the-internet-and-geopolitics/> [2022-08-07].
- Sidanius, J. och R. Kurzban. 2003. "Evolutionary Approaches to Political Psychology," i *Oxford Handbook of Political Psychology*, redigerad av D. O. Sears, L. Huddy och R. Jervis, 146-181. Oxford och New York: Oxford University Press.
- Silverman, H. 2011. *Contested Cultural Heritage: Religion, Nationalism, Erasure, and Exclusion in a Global World*. New York: Springer.
- Simonite, T. och G. M. Volpicelli. 2022. "Ukraine's Digital Ministry Is a Formidable War Machine." *Wired*, 17 mars: <https://www.wired.com/story/ukraine-digital-ministry-war/> [2022-06-22].
- Singer, P. W., och E. T. Brooking. 2019. *LikeWar – The Weaponization of Social Media*. New York: First Mariner Books Edition.
- Sirlin, N., Z. Epstein, A. A. Arechar och D. G. Rand. 2021. "Digital Literacy Is Associated With more Discerning Accuracy Judgments but not Sharing Intentions," *Harvard Kennedy School Misinformation Review* 2(6): 1-13.
- Smith, J. E. 2022. *The Internet Is Not What You Think It Is: A History, a Philosophy, a Warning*. Princeton: Princeton University Press.
- Smith, R. E. 2014. "It's Official: AIs Are Now Re-Writing History." *Robert Elliot Smith's Blog*, 5 oktober: <https://www.robertelliottsmith.com/blog/530> [2022-06-26].
- Snodgrass, G. 2020. "Trump Fires Secretary Of Defense Mark Esper Via Tweet." *Forbes*, 9 november: <https://www.forbes.com/sites/guysnodgrass/2020/11/09/trump-fires-secretary-of-defense-mark-esper-via-tweet/?sh=2ccb3d9c66bd> [2022-07-04].
- Sparrow, B., J. Liu och D. M. Wegner. 2011. "Google Effects on Memory: Cognitive Consequences of Having Information at Our Fingertips." *Science* 333: 776-778.
- Stahle, N. 2022. "It-attacken mot Kalix kommun – detta har hänt." *SVT Norrbotten*, 25 januari: <https://www.svt.se/nyheter/lokalt/norrbotten/it-attacken-mot-kalix-kommun-detta-har-hant> [2022-06-01].

- "Statement by Scholars of Genocide, Nazism and World War II." *Googledocs*, 25 februari 2022:
https://docs.google.com/document/d/1Lg3p8A3XtedJSIScgDDLIPY45FVFzxpK0pxOoeUh_MI/edit [2022-06-27].
- Stewart, E. 2018. "Lawmakers Seem Confused About What Facebook Does — And How to Fix It." *The Guardian*, 10 april: <https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations> [2022-07-14].
- Strindberg, A. 2020. *Social Identity Theory and the Study of Terrorism and Violent Extremism*. FOI-R--5062--SE, Totalförsvarets forskningsinstitut, Stockholm.
- Storbeck, J. och G. L. Clore. 2007. "On the Interdependence of Cognition and Emotion." *Cognition and Emotion* 21(6): 1212–1237.
- Strömbäck, J., H. Boomgaarden, E. Broda, A. Damstra, E. Lindgren, Y. Tsifti och R. Vliegenthart. 2022. "From Low-Choice to High-Choice Media Environments – Implications for Knowledge Resistance," i *Knowledge Resistance in High-Choice Information Environments*, redigerad av J. Strömbäck, Å. Wikforss, K. Glüer, T. Lindholm och H. Oscarsson, 49-68. London och New York: Taylor and Francis.
- Strömbäck, J., Å. Wikforss, K. Glüer, T. Lindholm och H. Oscarsson. 2022. "Introduction: Toward Understanding Knowledge Resistance in High-Choice Information Environments," i *Knowledge Resistance in High-Choice Information Environments*, redigerad av J. Strömbäck, Å. Wikforss, K. Glüer, T. Lindholm och H. Oscarsson, 1-28. London och New York: Taylor and Francis.
- Ståhl, T., M. P. Zaal och L. J. Skitka. 2016. "Moralized Rationality: Relying on Logic and Evidence in the Formation and Evaluation of Belief Can Be Seen as a Moral Issue." *PLoS ONE* 11(11): 1-38.
- Suresh Bisen, S. och Y. M. Deshpande. 2018. "Understanding Internet Addiction: A Comprehensive Review." *Mental Health Review Journal* 23(3): 165-184.
- Svenonius, O. 2022. *Varning – desinformation! Allmänhetens syn på psykologiskt försvar*. FOI-R--5264--SE, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--5264--SE> [2022-07-09].

- Svenonius, O., E. Isaksson och J. Lindgren. 2022. *Countering Mis- and Disinformation: A Narrative Review of Reactive Measures*. FOI-R--5263--SE, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--5263--SE> [2022-09-15].
- Svensson, J. (2021). *Wizards of the Web: An Outsiders Journey Into Tech Culture, Programming, and Mathemagics*. Göteborg: Nordicom.
- Szekely, I. 2017. "Do Archives Have a Future in the Digital Age?" *Journal of Contemporary Archive Studies* 4(2): 1-16.
- Tajfel, H., redigerad av. 1982. *Social Identity and Intergroup Relations*. Cambridge: Cambridge University Press.
- Tajfel, H. och J. C. Turner. 1986. "The Social Identity Theory of Intergroup Behavior." *Psychology of Intergroup Relations* 5: 7–24.
- Terren, L. och R. Borge-Bravo. 2021. "Echo Chambers on Social Media: A Systematic Review of the Literature." *Review of Communication Research* 9: 99-118.
- The Economist. 2017. "Data is Giving Rise to a New Economy." 6 maj: <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy> [2022-08-09].
- Thebault, R. och H. Knowles. 2022. "In Appearances from Presidential Office in Kyiv, Zelensky Says Russian Forces Are 'All War Criminals'." *The Washington Post*, 8 mars: <https://www.washingtonpost.com/world/2022/03/08/ukrainian-president-zelensky-kyiv-video-message/> [2022-08-14].
- Thompson, S. A. 2022. "4 Falsehoods Russians Are Told About the War." *The New York Times*, 10 mars: <https://www.nytimes.com/2022/03/10/technology/disinformation-russia-ukraine.html> [2022-06-27].
- Tindall, C. D. 2003. "Argus Rules: The Commercialization of Personal Information," *Journal of Law, Technology, & Policy* 1: 181-202.
- Tokita, C. K., A. M. Guess och C. E. Tarnita. 2021. "Polarized Information Ecosystems Can Reorganize Social Networks via Information Cascades." *PNAS* 118(50). e2102147118.
- Toler, A. 2018. "Anatomy of a Russian 'Troll Factory' News Site." *Bellingcat*, 8 juni: <https://www.bellingcat.com/resources/case-studies/2018/06/08/anatomy-russian-troll-factory-news-site/> [2022-07-11].

Twetman, H. och G. Bergmanis-Korats. 2020. *Data Brokers and Security: Risks and Vulnerabilities Related to Commercially Available Data*, NATO Strategic Communications Centre of Excellence, Riga:
https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf [2022-09-23],.

UK Ministry of Defence. 2019. *Defence Strategic Communication: An Approach to Formulating and Executing Strategy*, Joint Doctrine Note 2/19:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804319/20190523-dcdc_doctrine_uk_Defence_Stratategic_Communication_jdn_2_19.pdf [2022-07-12].

UK Ministry of Defence. 2021. *Integrated Operating Concept*. Development, Concepts and Doctrine Centre:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014659/Integrated_Operating_Concept_2025.pdf [2022-07-12].

United States – White House. 2009. *National Framework for Strategic Communications*. Homeland Security Digital Library:
<https://www.hsdl.org/?abstract&did=27301> [2022-07-16].

United States Code. 2011. "10 U.S.C. Section 2241." U.S. Government Publishing Office: <https://www.govinfo.gov/content/pkg/USCODE-2011-title10/html/USCODE-2011-title10-subtitleA-partIV-chap134-subchapI-sec2241.htm> [2022-06-17].

United States Department of Defense. 2016. *Strategy for Operations in the Information Environment*:
<https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf> [2022-06-17].

United States Joint Chiefs of Staff. 2017. *Doctrine for the Armed Forces of the United States*:
https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf [2022-06-17].

United States Joint Chiefs of Staff. 2018. *Joint Concept for Operating in the Information Environment (JCOIE)*:
https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf [2022-06-17].

United States Government Accountability Office. 2021. *Information Environment: DOD Operations Need Enhanced Leadership and Integrated Capabilities*: <https://www.gao.gov/assets/gao-21-525t.pdf> [2022-06-17].

- Vaccari, C. and A. Chadwick. 2020. "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News." *Social Media + Society* 6(1): 1-13.
- Van Bavel, S. Rathje, J. J., E. Harris, C. Robertson och A. Sternisko. 2021. "How Social Media Shapes Polarization." *Trends in Cognitive Science* 25(11): 913-916.
- Van Prooijen, J-W., redigerad av. 2021. *The Psychology of Political Polarization*. London och New York: Routledge.
- Van Puyvelde, D. 2017. "Privatisation," i *The Palgrave Handbook of Security, Risk and Intelligence*, redigerad av R. Dover, H. Dylan och M. S. Goodman, 297-314. London: Palgrave Macmillan.
- Van Ruler, B. (2018). "Communication Theory: An Underrated Pillar on Which Strategic Communication Rests." *International Journal of Strategic Communication* 12(4): 367-381.
- Vázquez-Herrero, J., M-C. Negreira-Rey och X. López-García. 2020. "Let's Dance the News! How the News Media Are Adapting to the Logic of TikTok," *Journalism* [online first].
- Vedechinka, M. och F. Borgonovi. 2021. "A Review of Evidence on the Role of Digital Technology in Shaping Attention and Cognitive Control in Children." *Frontiers in Psychology* 12(611155): 1-22.
- Vendil Pallin, C. 2022. *Rysslands inte så suveräna internet och kriget i Ukraina*. FOI Memo 7925, Totalförsvarets forskningsinstitut, Stockholm: <https://www.foi.se/rapportsammanfattning?reportNo=FOI%20Memo%207925> [2022-09-15].
- Vignoles, V. L., S. J. Schwartz och K. Luyckx. 2011. "Introduction: Toward an Integrative View of Identity," i *Handbook of Identity Theory and Research: Volume I*, redigerad av V. L. Vignoles, S. J. Schwartz och K. Luyckx, 1-29 (New York: Springer).
- Vitvitsky, B. 2022. "Disarming Putin's History Weapon." *Atlantic Council*, 23 januari: <https://www.atlanticcouncil.org/blogs/ukrainealert/disarming-putins-history-weapon/> [2022-07-09].
- Vosoughi, S., D. Roy och S. Aral. 2018. "The Spread of True and False News Online." *Science* 359(6380): 1146-1151.
- Vyklický, V. och V. Divišová. 2021. "Military Perspective on Strategic Communications as the 'New Kid on the Block': Narrating the Czech Military Deployment in Afghanistan and the Baltic States." *International Journal of Strategic Communication* 15(3): 231-252.

- Wadhwa, V. och A. Salkever. 2022. "How Elon Musk's Starlink Got Battle-Tested in Ukraine." *Foreign Policy*, 4 maj: <https://foreignpolicy.com/2022/05/04/starlink-ukraine-elon-musk-satellite-internet-broadband-drones/> [2022-07-15].
- Walker, D. 2022. "Coalition of Chaos? Nasty Nats and Anti-Vaxxers United in Belief About '77th brigade' Conspiracy Theory." *Scottish Daily Express*, 8 januari: <https://www.scottishdailyexpress.co.uk/news/scottish-news/coalition-chaos-nasty-nats-anti-25875307> [2022-06-22].
- Walker, M. och K. E. Matsa. 2021. "News Consumption Across Social Media in 2021." Pew Research Center: <https://www.pewresearch.org/journalism/2021/09/20/news-consumption-across-social-media-in-2021/> [2022-08-01].
- Wallenius, C. 2022. "Do Hostile Information Operations Really Have the Intended Effects? A Literature Review." *Journal of Information Warfare*.
- Wanless, A. och M. Berk. 2020. "The Audience is the Amplifier: Participatory Propaganda," i *The Sage Handbook of Propaganda*, redigerad av P. Baines, N. O'Shaughnessy och N. Snow, 85-104. Los Angeles och London: Sage.
- Walters, P. 2021. "Reclaiming Control: How Journalists Embrace Social Media Logics While Defending Journalistic Values." *Digital Journalism* [online first]: 1-20.
- Ward, A. F., J. (F.) Zheng och S. M. Broniarczyk. 2022. "I Share, Therefore I Know? Sharing Online Content - Even Without Reading It - Inflates Subjective Knowledge." *Journal of Consumer Psychology* [online first].
- Watkins, B. 2021. "Introduction," i *Research Perspectives on Social Media Influencers and their Followers*, redigerad av B. Watkins, 1-6. Lanham, Boulder, New York och London: Lexington Books.
- Watts, C. 2018. *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News*. New York: Harper-Collins.
- Wegner, D. M. och A. F. Ward. 2013. "The Internet Has Become the External Hard Drive for Our Memories." *Scientific American* 309: 58 - 61.
- Weiss-Wendt, A. 2020. *Putin's Russia and the Falsification of History*. London och New York: Bloomsbury.

- Whalen, J. och E. Nakashima. 2021. "Biden Revokes Trump's TikTok and WeChat Bans, but Sets Up a Security Review of Foreign-Owned Apps." *The Washington Post*, 9 juni:<https://www.washingtonpost.com/technology/2021/06/09/tiktok-ban-revoked-biden/>
- Whitesmith, M. 2020. *Cognitive Bias in Intelligence Analysis: Testing the Analysis of Competing Hypotheses Method*. Edinburgh: University of Edinburgh Press.
- Whitten-Woodring, J., M. S. Kleinberg, A. Thawnghmung och M. T. Thitsar. 2020. "Poison if You Don't Know How to Use It: Facebook, Democracy, and Human Rights in Myanmar." *The International Journal of Press/Politics* 25(3): 407–425.
- Whyte, C., A. T. Thrall och B. M. Mazanec. 2021. "Introduction," i *Information Warfare in the Age of Cyber Conflict*, redigerad av C. Whyte, A. T. Hall och B. M. Mazanec, 1-10 (London och New York: Routledge).
- Williams, J. 2018. *Stand Out of Our Light: Freedom and Resistance in the Attention Economy*. Cambridge och New York: Cambridge University Press.
- Wilson, A. 2005. *Ukraine's Orange Revolution*. New Haven: Yale University Press.
- Wilson, T. och K. Starbird. 2021. "Cross-platform Information Operations: Mobilizing Narratives & Building Resilience through both 'Big' & 'Alt' Tech." *Proceedings of the ACM on Human-Computer Interaction* 5(CSCW2, 345): 1-32.
- Wikipedia. 2022. "Gerasimov Doctrine": https://en.wikipedia.org/wiki/Gerasimov_doctrine [2022-07-06].
- Wodak, R., R. de Cillia, M. Reisigl och K. Liebhart. 2009. *The Discursive Construction of National Identity*. Edinburgh: Edinburgh University Press.
- Wohlin, C. 2014. "Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering." *EASE '14: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, artikel 38: 1-10.
- Wolfley, K. 2021. *Military Statecraft and the Rise of Shaping in World Politics*. New York: Rowman & Littlefield.

- Woolley, S. C. och P. N. Howard. 2019. "Introduction: Computational Propaganda Worldwide," i *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, redigerad av S. C. Woolley och P. N. Howard, 3-20 (Oxford och New York: Oxford University Press).
- Woolley, S. och D. Guilbeault. 2019. "United States: Manufacturing Consensus Online," i *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, redigerad av S. C. Woolley och P. N. Howard, 185-211. Oxford och New York: Oxford University Press.
- Woodhams, S. och S. Migliano. 2022. "Government Internet Shutdowns Cost \$ 5,5 Billion in 2021." *Top10VPN*, 4 januari:
<https://www.top10vpn.com/research/cost-of-internet-shutdowns/2021/>
[2022-06-30].
- Woodhams, S. och S. Migliano. 2022. "Websites Blocked in Russia Since Ukraine Invasion." *Top10VPN*, 21 juni:
<https://www.top10vpn.com/research/websites-blocked-in-russia/>
[2022-06-30].
- World Bank. 2019. *ID4D Practitioner's Guide: Version 1.0 (October 2019)*. Washington DC, World Bank.
- Yates, F. 1999. *Selected Works Volume III - The Art of Memory*. London och New York: Taylor and Francis.
- Yeykelis, L., J. J. Cummings och B. Reeves. 2014. "Multitasking on a Single Device: Arousal and the Frequency, Anticipation, and Prediction of Switching Between Media Content on a Computer." *Journal of Communication* 64(1): 167 - 92.
- Zajonc, R. B. 1968. "Attitudinal Effects of Mere Exposure." *Journal of Personality and Social Psychology: Monograph Supplement* 9(2): 1-27.
- Österdahl, I. 2021. "Krig eller fred: Om regeringsformens definition av krig." *Svensk Juristtidning* 105: 261-276.

