

# Informationspåverkan, ekonomisk desinformation och Sveriges finansiella stabilitet

Forskningsledare: Gustav Almqvist

Myndigheten för  
psykologiskt försvar



HOUSE OF GOVERNANCE  
AND PUBLIC POLICY


**Rapporten är finansierad av Myndigheten för psykologiskt försvar.  
Författarna ansvarar själva för rapportens innehåll och slutsatser.**

Informationspåverkan, ekonomisk desinformation och Sveriges finansiella stabilitet

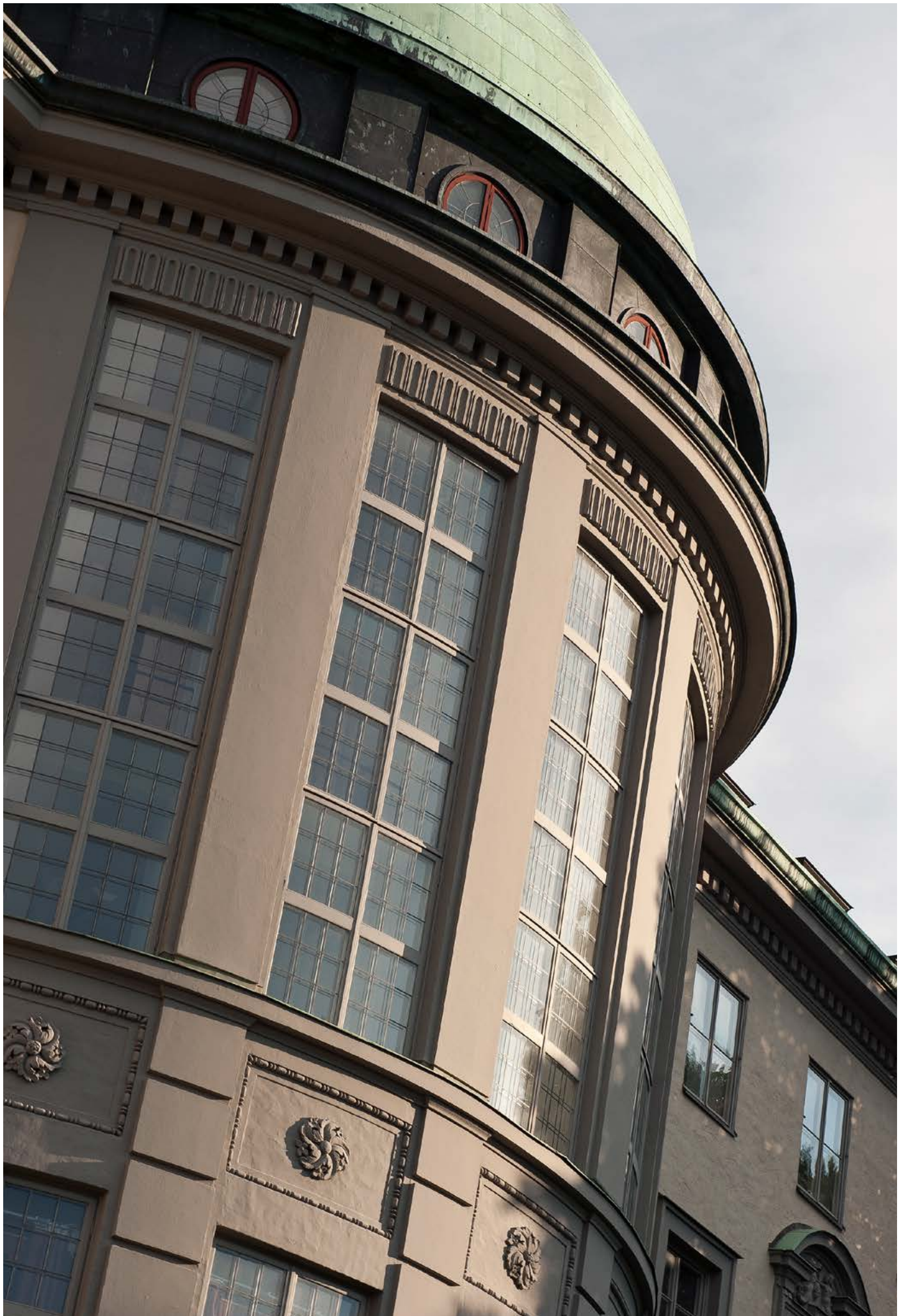
Utgivningsår: 2026

Foto framsida: Juliana Wolf Garcindo

Grafisk design & illustrationer: Erika Granstrand



Informationspåverkan,  
ekonomisk desinformation  
och Sveriges finansiella stabilitet



# Sammanfattning

Den moderna marknadsekonomi är ett intrikat system för utbyten av varor och tjänster via pengar. Dess stabilitet fordrar tillit organisationer, medborgare och institutioner emellan. Informationspåverkan och desinformation kan användas av främmande makt i syfte att skada Sverige. Vidareutvecklingen av artificiell intelligens möjliggör nya sätt på vilka så kan ske. Syftet med föreliggande rapport har varit att översiktligt identifiera och diskutera några av de sätt på vilka det i så fall skulle kunna tänkas påverka Sveriges finansiella stabilitet. Forskningsledare har ekon. dr Gustav Almqvist vid Handelshögskolan i Stockholm, SSE House of governance and public policy, varit. De forskningsmetoder som använts har varit litteraturstudier av relevanta vetenskapliga publikationer inom området, databassökningar omfattande såväl svenska som internationella nyhetsmedier, och halvstrukturerade expertintervjuer med forskare och andra experter i Sverige, Storbritannien, Frankrike och USA. Risker har identifierats på tre olika nivåer: mikro-, meso- och makronivå. De redovisade riskerna på mikronivå är investeringsbedrägerier, manipulerade språkmodeller och falskmynteri. Presenterade risker på mesonivå är mullvadar, ryktesspridning och kontraktsvåld. På makronivå är de risker som diskuteras propaganda, konspirationsteorier och fasader. Ett antal risksegment – särskilt utsatta eller mottagliga samhällsgrupper – identifieras. Möjliga resiliensstärkande insatser i form av informations-, utbildnings- och kontrollåtgärder föreslås.

Nyckelord: *Informationspåverkan, desinformation, misinformation, finansiell stabilitet*

# Innehållsförteckning

<b>Sammanfattning</b>	5
<b>Inledning</b>	9
<b>Mikronivå</b>	
Investeringsbedrägerier	15
Språkmodeller	23
Falskmynteri	27
<b>Mesonivå</b>	
Mullvadar	29
Ryktesspridning	34
Kontraktsvåld	38
<b>Makronivå</b>	
Propaganda	42
Konspirationsteorier	45
Fasader	47
<b>Diskussion</b>	49
<b>Forskarlag</b>	51

”Desinformation, manipulering av information ökar. Det splittar våra samhällen. Inte bara urholkar det förtroendet för sanningen – det handlar om själva demokratin”.

**Ursula von der Leyens linjetal, Strasbourg, 10 september 2025,  
forskarlagets översättning**



”Det handlar om hela västvärlden. Om vad vi står för, våra idéer och allt vi vill bevara för våra barn och barnbarn – ett fungerande, öppet samhälle och stabila demokratier”

**Michael Claessons huvudanförande, Handelshögskolan i Stockholm,  
26 november 2025**



# Inledning

Ekonomer har länge studerat det ekonomiska systemets organisation och ordning: hur företag och marknader för produkter, tjänster, arbete eller kapital, bankväsenden och handelssystem – tillsammans med politiska och legala institutioner – upprätthåller en fungerande ekonomisk ordning.<sup>1</sup> Centralt för upprätthållandet av och stabiliteten hos sådana system – ekonomier – är tillit människor och organisationer emellan.<sup>2</sup> Att medborgarna i ett land i tillräcklig utsträckning litar på pengars funktion, tillgångars (såväl finansiella som icke-finansiella) beständiga realiserbara värde, centralbankers kompetens, finans- och penningpolitikens avsikter, samt tillsyn och reglerings effektivitet är fundamentalt för den nationella ekonomins fungerande och utveckling. Likaså för dess motståndskraft mot störningar och hot.

I ett intrikat system präglad av ömsesidiga beroenden aktörer emellan, som den moderna marknadsekonomin, är sårbarheterna ofrånkomligen många. Sommaren år 2017 lamslogs exempelvis en betydande del av världshandelns sjötransporter och logistik för en tid av cyberattacken Notpetya.<sup>3</sup> Enligt amerikanska och brittiska regeringsuttalanden var det högst sannolikt Ryssland och Kreml som via rysk underrättelsetjänst och militär planlade och utförde attacken. Via en så kallad kryptomask, skadlig kod, i ett ukrainskt bokföringsprogram raderades information på datorer och servrar i syfte att bland annat skada Ukrainas finansiella sektor, regeringsfunktioner och energiinfrastruktur.<sup>4</sup> I Ukraina var en av konsekvenserna att bankomater och betalningssystem landet över drabbades av allvarliga driftsstörningar och att flera bankers kontorsdatorer och hemsidor slogs ut. Statliga Oschadbank liksom OTP bank, Privatbank Sberbank och Ukrsotsbank drabbades alla.<sup>5,6</sup>

Den skadliga koden spreds dessutom från ett lokalt kontor i ukrainska Odessa vidare även inom Mærsk, det stora internationella sjöfarts- och logistikföretaget med huvudkontor i Danmark, vars verksamhet så kom att saboteras. Mærskes IT-system slogs ut, dess kontorsdatorer kraschade, såväl elektroniska dörr- som telefonsystem upphörde att fungera. Hamnar från Mumbai till Rotterdam och Los Angeles tvingades stänga. Redan de direkta, omedelbara ekonomiska skadorna för Maersk uppgick till motsvarande ett par miljarder svenska kronor. (De totala kostnaderna för Notpetya-attacken var en magnitudordning större än så.)

1 Coase, R.H. (1977). "Economics and Contiguous Disciplines." In *The Organization and Retrieval of Economic Knowledge*, ed. Mark Perlman, 481–491. Boulder, CO: Westview Press

2 Williamson, O. E. (1993). Calculativeness, trust, and economic organization. *Journal of Law and Economics*, 36(1), 453–486

3 Av samma slag som HermeticWiper, som användes i anslutning till den fullskaliga invasionen av Ukraina.

4 <https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks>

5 <https://www.foi.se/rest-api/report/FOI-R--4774--SE>

6 Åtminstone en rysk bank påverkades också.

Statliga cyberattacker är en sofistikerad form av tre klassiska krigföringsmetoder: sabotage, spionage och subversion.<sup>7</sup> Även informationspåverkan och desinformation kan användas som icke-militära inslag i hybridkrigsföring av främmande makt och så, direkt eller indirekt, avsiktligt eller oavsiktligt, drabba ett annat land; dess företag, medborgare eller intressen. Att skydda Sveriges ekonomi och dess finansiella stabilitet inför den sortens risker är därför naturligt av stor vikt. Vissa sorters informationspåverkan och desinformation kan ha till syfte att undergräva medborgarnas tillit till pengars funktion, tillgångars beständiga värde, centralbankers kompetens, finans- och penningpolitikens avsikter, samt tillsyn och regleringars effektivitet, det vill säga det som tidigare i denna rapport anförts som grundläggande förutsättningar för det ekonomiska systemets funktion och motståndskraft.

I en omfattande internationell enkätundersökning om globala risker, med forskare och experter som svarande, bedömdes desinformation och misinformation vara den risk med förväntat värst konsekvenser världen över under den kommande tvåårsperioden.<sup>8,9</sup> EU-kommissionens ordförande Ursula von der Leyen fastslog i sitt linjetal i Strasbourg hösten 2025 att ”desinformation och manipulering av information ökar. Det splittrar våra samhällen. Inte bara urholkar det förtroendet för sanningen – det handlar om själva demokratin” (forskarlagets översättning). För närvarande pågår en revolutionerande teknologisk utveckling inom generativ artificiell intelligens (AI) som möjliggör snabb, kostnadseffektiv och trovärdig produktion och distribution av texter, bilder och videor – vilket förbättrar förutsättningarna för de aktörer som ämnar ägna sig åt informationspåverkan och desinformation. En enkätundersökning med ett representativt urval (n=1050) av Sveriges vuxna befolkning visar att mer än fyra av fem svarande tror att Sverige kommer att drabbas av falsk och vilseledande information från främmande makt under de närmaste fem åren, och tre av fyra oroas specifikt av AI:s roll i det. Bara drygt var fjärde respondent anser Sveriges beredskap tillräcklig inför det hotet.<sup>10,11,12</sup>

Med fokus på hur främmande makt tidigare har, eller i framtiden skulle kunna använda, desinformation och informationspåverkan för att skada Sveriges finansiella stabilitet har denna forskningsrapport skrivits. Arbetet har letts av Gustav Almqvist, doktor i ekonomi och forskare bland annat vid Handelshögskolan i Stockholms SSE House of government and public policy, och expert inom kunskapsområdet ekonomisk psykologi. Finansiering av studien har erhållits från Myndigheten för psykologiskt försvar.

7 Rid, T. (2012). Cyber war will not take place. *Journal of strategic studies*, 35(1), 5-32.

8 Närmast före extremväder, militära konflikter, politisk polarisering och cyberattacker. Det bedömdes även vara den fjärde värsta risken på 10 års sikt. Med globala risker avsågs sådana som till exempel skulle kunna ha en ”signifikant påverkan på världens BNP”.

9 [https://reports.weforum.org/docs/WEF\\_Global\\_Risks\\_Report\\_2025.pdf](https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf)

10 Samtidigt som två av tre befarar att en ekonomisk kris kommer att inträffa i Sverige inom de närmaste 5 åren.

11 <https://mpf.se/publikationer/publikationer/2025-06-23-opinioner-2025---halvarsmatning>

12 Även näringslivet oroas. Samma tendens som i Sveriges allmänhet erhålls när chefer globalt tillfrågas.

## Nyckelbegrepp

**Informationspåverkan:** Kommunikationsinsatser ämnade att förändra människors uppfattningar, attityder eller beteenden

**Desinformation:** Felaktig eller manipulerad information som sprids med flit för att skada en person, organisation eller ett land

**Misinformation:** Falsk information som inte nödvändigtvis har skapats för att orsaka skada

**Finansiell stabilitet:** Jämviktstillstånd i vilket det finansiella systemets kärnfunktioner och legitimitet upprätthålls samtidigt som det motstår störningar

Den amerikanske ekonomen Frank Knight gjorde redan för mer än 100 år sedan åtskillnad på begreppen risk och osäkerhet.<sup>13</sup> Med risk avsåg han situationer i vilka sannolikheten för olika utfall kunde beräknas i procent. Med osäkerhet avsåg han situationer som var så svåröversäglbara att det inte gick. En annan ekonom, engelsmannen John Maynard Keynes, kom att ansluta sig till en liknande uppfattning: ”Den bemerkelse i vilket jag använder begreppet är den i vilken förutsättningen för ett europeiskt krig är osäker [...] Beträffande dessa frågor finns ingen vetenskaplig basis på vilken sannolikheten kan beräknas. Vi vet helt enkelt inte”.<sup>14</sup> Ämnet för det tvärvetenskapliga forskningsområde som ändå, trots svårigheten, sysslar med den sortens epistemologiska frågor kallas bedömningar under osäkerhet.

På en presskonferens år 2002 sade USAs försvarsminister Donald Rumsfeldt:

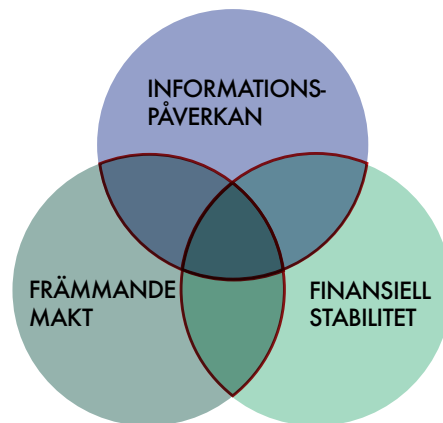
**”Rapporter som säger att något *inte* har hänt intresserar mig alltid. Därför att det, som vi vet, förvisso finns kända, kända saker. Sådant vi vet att vi känner till. Men det finns därutöver även okända, okända – som vi inte vet att vi inte känner till. Och genom vårt lands historia, liksom i andra fria länders, är det de senare som brukar vara de svåraste fallen”**

Att som i föreliggande rapport värdera om och i så fall hur främmande makt tidigare har, eller i framtiden skulle kunna använda, desinformation för att skada Sveriges finansiella stabilitet är en bedömning under osäkerhet. Det är, som Knight och Keynes skrev, omöjligt att på ett fullständigt sätt exakt uppskatta sannolikheten för alla sådana händelser som kan tänkas ske. Kanske är det också, som Rumsfeldt sade, de oss ännu okända fallen som kan vålla samhället störst skada. Arbetet som legat till grund för denna rapport har av praktiska skäl syftat till att översiktligt adressera de kända

<sup>13</sup> Knight, F.H. (1921). *Risk, uncertainty and profit*. New York: A.M. Kelley.

<sup>14</sup> Keynes, J. M. (1937). The general theory of employment. *The quarterly journal of economics*, 51(2), 209-223, ss. 213.

sorternas risker. Dels presenteras därför några av de dokumenterade exemplen på hur främmande makt eller organisationer i deras närhet eller periferi ägnat sig åt dylikt globalt; dels analyseras aktuella samhälleliga och teknologiska företeelser och trender som främmande makt realistiskt *skulle kunna* utnyttja.



Forskarlagets metodik har inbegripit följande:

- Arkivsökningar omfattande såväl svenska som internationella nyhetsmedier
- Litteraturstudier av relevant forskning, identifikation av fallstudier
- Djupintervjuer med forskare och experter i Sverige, Storbritannien, Frankrike och USA

Arbetet har mynnat ut i en förteckning över nio distinkta risker, samtliga av hög aktualitet. Riskerna har schematiskt klassificerats på endera av tre nivåer: mikro-, meso- eller makronivå. Risker på mikronivå är sådana som först drabbar enskilda individer i det ekonomiska systemet, värdepappersbedrägerier riktade mot småsparare till exempel. Om tillräckligt många svenska privatinvestorer luras på pengar via AI-genererade bilder på centralbankschefen och falska chatmeddelanden från näringslivsprofiler (se vidare på sida 20) är det en risk på mikronivå. Så småningom, aggregerat, kan den få destabiliserade och förtroendeskadande effekter. Risker på mesonivå drabbar först organisationer. Ekonomiskt spionage inifrån ett företag eller en finansiell institution – det är en risk på mesonivå. Samma sak med en överbelastnings- eller kursmanipulationsattack mot en aktiehandelsplats som tvingar börsen att stänga eller leder till ogiltigförklarade aktieaffärer i efterhand. Detsamma med ryktesspridning om banker ämnade att få sparare att begära ut sina insättningar därifrån: bankrusning, vilket i tillräcklig skala skulle kunna föranleda konkurs (se sida 34). Likadant med ett dataintrång hos en officiell nyhetsbyrå åtföljd av publikationen av ett falskt pressmeddelande i syfte att skada ett lands valuta eller företags aktiekurs (sida 37). Likaså desinformation ämnad att skada ett företags varumärke eller anseende. Som tillhörande makronivån återfinns framtagande och distribution av propaganda och konspirationsteorier som når nyhetsflödet, liksom opinionsbildande fasadorganisationer (sida 48).

Även om de utnyttjar olika sårbarheter i det ekonomiska systemet har de i det följande redovisade riskerna på mikro-, meso och makronivå alla det gemensamt att de, enskilt eller tillsammans, kan ha viss destabiliserande effekt – både samhällsekonomiskt och finansiellt.

**Stärk resiliensen:** Fortsatt forskning inom området rekommenderas

## Expertintervjuer

1. **Prof. Todd Helmus**, senior forskare, RAND Corporation, USA
2. **Emil Larsson**, industridoktorand, Försvarshögskolan & Karlstads universitet, Sverige
3. **Sahil Shah**, verkställande direktör, Say no to disinfo, Storbritannien
4. **Prof. Richard Wahlund**, professor, Handelshögskolan i Stockholm, Sverige
5. **Dr. Staffan Truvé**, teknikchef & medgrundare, Recorded future, Sverige
6. **Malcolm Murray**, forskningschef, SaferAI, Frankrike
7. **Dr. Per-Erik Nilsson**, senior forskare, Totalförsvarets forskningsinstitut, Sverige



**”De kan byta taktik. Jag tror inte att de siktar in sig på finansiella marknader än. Problemet är att de skulle kunna göra det. Så det finns mycket värde i er studie. Att tänka på vilka de potentiella angreppsvektorerna är och hur det går att skydda sig mot dem.”**

Todd Helmus

**”Den största risken är att urholka trovärdigheten hos institutioner och system, att man tappar förtroendet för den svenska kronan eller för banker eller för samhällsinstitutioner”**

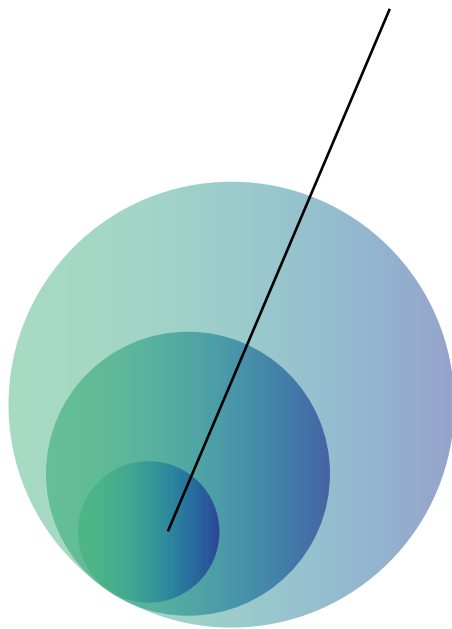
Emil Larsson



**”Om du ville påverka finansiell stabilitet, skulle du troligen börja med en sårbar bank med skakiga finanser. Sedan gå vidare till medelstora banker och därefter större banker. Och till sist påverka valutorna och centralbanken. Attacken skulle ske lager på lager över tid och minska förtroendet gradvis”**

Sahil Shah

# MIKRONIVÅ



# Investeringsbedrägerier

Bland de första investeringsbedrägerierna var de kedjebrev som i slutet av 1800-talet cirkulerade i USA, där läs- och skrivkunnigheten då nyss hade ökat. Brevens innehöll en lista på namn där du skrev till ditt eget längst ned och förväntades skicka pengar till den vars namn stod högst upp, stryka över det, och sedan sända brevet vidare. Ett sådant bedrägeri kallas numera för ett pyramidspel. De är vanliga även i den moderna ekonomin. De förmodligen mest omfattande pyramidspelen hittills var de albanska som vid tiden för sina sammanbrott inbegrep mer än en miljon människor, två tredjedelar av befolkningen, och vars kollaps år 1997 förde landet till randen av ekonomiskt sammanbrott.

**Definition:** *pyramidspel* – olagligt investeringsupplägg där avkastningen i toppen av pyramiden kommer från nya pengainsättningar i botten

Mer nyligen, i västvärlden, utmärkte sig främst den amerikanske fondförvaltaren Bernie Madoffs motsvarighet. Han ledde under flera decennier ett investeringsbedrägeri som uppdagades under finanskrisen 2008 och som orsakade drabbade småsparare, banker och pensionsfonder förluster om hundratals miljarder kronor. Ett ännu modernare och mer aktuellt amerikanskt exempel är fallet Forsage. Det marknadsfördes under ett par år intensivt via reklam på Youtube, Facebook och Telegram och som inför sina offer beskrevs som ett sätt att tjäna snabba pengar på kontrakt på blockkedjeplattformarna Ethereum (ETH), Tron (TRX) och Binance (BNB). En granskning av SEC, US Securities and Exchange Commission, USA:s motsvarighet till Finansinspektionen, visade dock att det rörde sig om ett pyramidspel och åtal väcktes efter att systemet kollapsat. (Detaljerna finns bland annat att läsa i rättsfallet *SEC vs. Okholnikhov et al.* från 2022.)<sup>15</sup> Även Onecoin, en bluffkryptovaluta lanserad av Ruja Ignatova, då Kryptodrottningen kallad (numera internationellt efterlyst), var pyramidspelsliknande organiserad. Så var även ett omfattande kryptobedrägeri riktat mot kinesiska pensionärer för vilket en kvinna nyligen dömdes till 11 års fängelse i Storbritannien.<sup>16</sup>

→ **Risksegment:** Äldre småsparare med låg kunskap om värdepapper och ovana vid IT

<sup>15</sup> Hock, B., & Button, M. (2023). Why do people join pyramid schemes?. *Journal of Financial Crime*, 30(5), 1130-1139.  
<sup>16</sup> <https://www.bbc.com/news/articles/cvg4w1g9ezko>

Pyramidspel är vanliga. Ungefärliga siffror från Storbritannien och USA översatta till svenska förhållanden skulle peka på en presumtiv årlig prevalens om mellan 10 000 och 50 000 drabbade (dvs 0.1-0.5 procent av befolkningen). Vad många pyramidspel genom historien har haft gemensamt är att de opportunistiskt utnyttjat sårbarheten som funnits i förhoppningar om snabb rikedom i kombination med finansiell okunskap och/eller bristande finansiell tillsyn. I det post-kommunistiska Albanien var det efter många decennier som ytterst isolerad diktatur få som överhuvudtaget ordentligt förstod värdepappers funktion och vilka institutioner som var tillförlitliga och inte. I fallet Forsage, ett kvartssekel senare och 800 mil därifrån, var det blockkedjor och decentraliserad finansteknologi (DeFi) som utgjorde lockelsen och drev på investeringsivern – utan tillräcklig eftertanke och kontroll.

**”Vi människor gillar helt enkelt möjligheter att utan större besvär vinna mycket. Den möjliga vinsten är samtidigt något vi skulle gå miste om ifall vi inte hängde på! Det senare aktiverar vår förlustaversion, det vill säga att vi reagerar starkt negativt på att förlora något, även om det gäller en imaginär vinst”**

Richard Wahlund



Foto: Juliana Wolf Garcindo

Ett med pyramidspelet mycket närbesläktat fenomen, med desinformation och marknadsmanipulation som inslag, är de så kallade pumpa-och-dumpa-bedrägerierna. I det sena 1980-talets USA:s började mindre nogräknade aktiemäklare att med aggressiva telefonsäljningsmetoder rekommendera frimärksaktier (eng. penny stocks). Frimärksaktierna tillhörde lågt värderade bolag, inte noterade på de etablerade börserna. Mäklarna som förmedlade aktierna brydde sig, tvärtemot vad de sade småspararna, egentligen inte om bolagens lönsamhet eller framtidsutsikter. De hade redan köpt på sig många av aktierna till lågt pris och var ute efter att trissa upp kursen. Sedan sålde de dem när priset var som högst.

Pumpa-och-dumpa-bedrägerier är vanliga ännu och har länge utnyttjat framväxten av ny teknik. På 1980-talet var det telefon och telefax. I dag är det internet och sociala media. De moderna organisationer som ägnar sig åt det arbetar internationellt, helst i fristäder där de för en tid kan undkomma polis.<sup>17</sup> I USA har SEC hösten 2025 grundat en ny insatsgrupp för att bekämpa en våg av pumpa-och-dumpa-bedrägerier i frimärksaktier tillhörande kinesiska bolag, som via amerikanska mellanhänder då först registreras på mindre aktiemarknadsplatser i USA. Det efter att FBI noterat en fyrdubbling av antalet inrapporterade fall. *Financial times* rapporterade ursprungligen att ett antal kinesiska företag under loppet av bara några dagar plötsligt tappat 80 procent av sitt

<sup>17</sup> Barnes, P. (2017). Stock market scams, shell companies, penny shares, boiler rooms and cold calling: The UK experience. *International Journal of Law, Crime and Justice*, 48, 50-64.

marknadsvärde (närmare 4 miljarder dollar) efter att först marknadsförts aggressivt i chattgrupper på Whatsapp och i sociala media.<sup>18</sup><sup>19</sup> Bedragarna påstås enligt bland annat *Dagens industri* ha kopplingar till Iran och Ryssland. I Sverige har Finansinspektionen, FI, i slutet av kalenderåret 2025, hittills utfärdat varningar för 148 olika aktörer inblandade i bedrägerier.<sup>20</sup>

Utöver frimärkesaktier är det på marknaderna för kryptovalutor och meme-aktier som pumpa-och-dumpa-bedrägerierna växer snabbast. På forum och i sociala media haussas då tillgångarna under en period, för att säljas när priserna stigit tillräckligt. Sådana försök samexisterar dock med ordinarie marknadsförhållanden som just för dessa tillgångsslag alltid präglas av mycket hög volatilitet och en spekulationsdriven marknadslogik, vilket försvårar gränsdragningen mellan marknadsmanipulation och normalt fungerande.

” Kryptokampanjer är den mest förekommande påverkan på nätet kopplat till ekonomi”

Staffan Truvé



**Frimärksaktie:** är en aktie med mycket lågt marknadsvärde och pris per aktie. Handlas utanför de stora börserna och kännetecknas av hög spekulationsgrad och låg likviditet

**Meme-aktie:** är en aktie vars prisrörelser i huvudsak drivs av virala trender och samordnat beteende i sociala media snarare än av företagets fundamentala värde

**Kryptovaluta:** är en digital tillgång som exempelvis fungerar som betalningsmedel i ett decentraliserat nätverk där transaktioner registreras i en gemensam blockkedja och verifieras genom kryptografiska metoder i stället för genom banker eller myndigheter

**NFT:** är en unik, icke-utbytbar digital token på en blockkedja som fungerar som ett ägar- och ursprungsbevis för en viss tillgång

Man ska inte överdriva skillnaderna mellan de sparare som investerar i kryptovalutor och de som inte gör det.<sup>21</sup> Samtidigt är ett rimligt antagande att överrepresenterade i riskgruppen för att drabbas just av pumpa-och-dumpa-bedrägerier i kryptovalutor och meme-aktier är spekulationsvilliga unga män med intresse för alternativa investeringar, DeFi, kryptovalutor, NFT:er (eng. non-fungible tokens) och som värdepappershandlar aktivt. Aktie- och kryptomissbruk, en psykologisk beroendeproblematik som snabbt ökar i omfattning, är exempelvis vanligast i detta segment.

18 <https://www.ft.com/content/38c9815b-8ccc-40d5-bcbf-cfdb8b73ffa6>

19 <https://www.ft.com/content/955a8008-6657-4049-b190-4a92c5ad9fcc>

20 <https://www.fi.se/sv/publicerat/nyheter/2025/148-varningar-hittills-i-ar--bedragarna-anvander-flera-nya-metoder>

21 Aiello, D., Baker, S. R., Balyuk, T., Di Maggio, M., Johnson, M. J., & Kotter, J. D. (2023). *Who invests in crypto? Wealth, financial constraints, and risk attitudes* (No. w31856). National Bureau of Economic Research.

→ **Risksegment:** Unga vuxna män med hög riskvilja, spekulationsbenägna i sitt sparande

Deras informationsinhämtning baseras sällan uteslutande på traditionella medier, som affärs- eller dagspress, utan inbegriper ofta podcasts och sociala medier-profiler inriktade på investeringar (så kallade finfluencers – se mer på sida 47). De läser internetforum och deltar i chattgrupper ibland knutna till specifika värdepappershandelsappar och -plattformar. Det är inte så att de nödvändigtvis brister i kunskap. Som i alla segment på privatsparmarknaden finns alla kunskapsnivåer representerade.<sup>22</sup> Däremot exponeras de för fler och delvis annorlunda investeringsrisker eftersom de handlar i volatila, mindre reglerade tillgångsslag med värderingscykler präglade av spekulation snarare än fundamentala faktorer. Minst 80 procent av alla nya kryptovalutor som lanserats har i efterhand visat sig antingen utgöra misslyckade satsningar eller bedrägerier.<sup>23</sup>

**”Medan vanliga valutor oftast, men inte alltid, skyddas av riksbanker och politiska beslut finns det idag inget sådant ansvarstagande för kryptovalutor. Detta gör sådana valutor mycket volatila eftersom tron på dem kan variera stort över tid. Det är ett stort problem och innebär ett risktagande för oinsatta konsumenter”**

Richard Wahlund

AI används idag vid en majoritet av alla kryptobedrägerier – som i och med det blivit mer realistiska och svårupptäckta. Konventionell internetbedrägeribekämpning bygger i regel på statiska regler för detektion och flaggning av misstänkt innehåll. Men AI skapar ett mer dynamiskt innehåll. Det i form av deepfakear, phishing, falska hemsidor, investeringsbotar och fejkhandelsplattformar. AI kan nyttjas för att kringgå tvåfaktori-identifiering (2FA). Chatbotar på Discord och Telegram, påhittat kundtjänst och röstkloning kan allt göras med AI.<sup>24</sup>

**Definition:** *deepfake* – AI-manipulerade ljud, bilder eller videor som felaktigt får det att framstå som att en person sagt eller gjort något

Att motverka denna utveckling ställer nya krav såväl på lagstiftning och brottsbekämpning som på teknikutveckling. Fördjupat internationellt samarbete krävs.<sup>25</sup> Hösten 2025 väckte amerikanska justitiedepartementet åtal mot Prinsgruppens (eng. Prince

22 Jmf. Samuelsson, E., Levinsson, H., & Ahlström, R. (2023). Financial literacy, personal financial situation, and mental health among young adults in Sweden. *Journal of Financial Literacy and Wellbeing*, 1(3), 541-564.

23 Lyandres, E., & Rabetti, D. (2023). Initial coin offerings: a review. SSRN 4534554.

24 <https://www.chainalysis.com/blog/ai-artificial-intelligence-powered-crypto-scams/>

25 Shah, M., & Mustafa, F. (2025). The Evolution of Digital Asset Scams: How Cybercrime Syndicates Exploit Financial Systems.

Group) ordförande, den kambodjanske medborgaren Chen Zhi, även känd som Vincent. I samband med det beslagtogs Bitcoin (BTC) till ett värde om cirka 150 miljarder kronor. Organisationen anklagas för att driva storskalig bedrägeriverksamhet av typen *Sha Zhu Pan*, vilket på svenska kan översättas som grisslakt.<sup>26</sup> Metoden går ut på att lura av privatpersoner deras sparpengar via svindlerier i industriell skala. Verksamheten bedrivs ofta från smarttelefondatacenter – så kallade telefonfarmar – med hundratals hyllmeter av smarta telefoner som teknisk infrastruktur.

Många av de mänskliga utförarna av bedrägerierna i Kambodja och andra länder i Asien påstått ha underkastats tvångsarbete under fängelseliknande former. I militärjuntans Myanmar, nära gränsen till Thailand, påstås bedrägeriarbetsläger – skyddade av murar och väpnade vaktorn – hålla tusentals människor fångna.<sup>27</sup> Under ledning av vad som tros vara kinesiska bedrägerisyndikat används där generativ AI i form av sofistikerade deepfakear för att, i videokommunikation med sina offer, få slavarbetarna att se ut eller låta på ett visst sätt i syfte att maximera svindleriernas effektivitet. Det engelska mediahuset *BBC* har exempelvis intervjuat en befriad bangladeshisk man som berättar att han inför sina manliga offer i mellanöstern AI-framställdes som en attraktiv ung kvinna.<sup>28</sup> Även i Indien har en omfattande cyberbedrägeriindustri växt fram på landsbygden.<sup>29</sup>



**AI är redan väldigt kraftfullt för desinformation och phishing. Samtidigt är frågan vad som händer när AI snart gör saker och ting snyggare och mer sofistikerade. Det blir ett än kraftigare verktyg”**

Emil Larsson

Konsumentskyddande åtgärder, tillsyn och regleringar av sparprodukter och finansiell rådgivning i Sverige avser i typfallet affärsförbindelser mellan ett aktiebolag (till exempel en bank) och en vuxen privatperson. Men för mindre nogräknade aktörer inbegripna i ekonomisk brottslighet eller verkande i oreglerade nischer på den svarta eller grå finansmarknaden är även minderåriga ett segment. Således förekommer såväl bedrägeriförsök som vilseledande marknadsföring även på okonventionella plattformar där detta segment vistas, till exempel på dejtingappar eller i onlinedatorspel (särskilt i sådana där konsumtion och betalningar sker). På båda sorternas plattformar kan konton dessutom kapas.

➔ **Risksegment:** Minderåriga med hög internetnärvaro utan föräldrainsyn

26 <https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged>

27 <https://www.theguardian.com/global-development/2025/sep/08/myanmar-military-junta-scam-centres-trafficking-crime-syndicates-kk-park>

28 <https://www.bbc.com/news/articles/c5yr7j18edjo>

29 <https://www.theguardian.com/technology/2025/oct/30/scamming-became-the-new-farming-inside-india-cybercrime-villages>

Kontokapningar i kriminellt syfte är redan vanligt förekommande – och biometriska lösenord har sedan en tid tillbaka setts som en motåtgärd. Men i och med AI-teknologins utveckling är biometriska lösenord nu inte längre säkra, varken de baserade på ansikts- eller röstigenkänning. Så har bland annat bekräftats av Open AI:s VD Sam Altman. Det finns likafullt banker som använder sådana kundidentifikationsmetoder. Trots att det numera är enkelt att kлона någons röst redan med vanliga AI-verktyg som Elevenlabs, Speechify, Playht eller Lovo.<sup>30</sup>

Även med en icke-biometrisk identifikationsteknologi som 2FA, eller BankID, med vilken ungefär 18 miljoner identifikationer sker varje dag, finns risker. ID-kapningar kan ske och föranleda otillbörliga köp eller finansiella transaktioner. Eller så kan tekniken saboteras, med långtgående kortsiktiga samhällseffekter exempelvis på betalningar.



**Risken för operationer mot BankID och Swish är väldigt hög**

Staffan Truvé



**I Sverige har vi till exempel BankID som är väldigt sårbart faktiskt**

Emil Larsson



**Stärk resiliensen:** *”Utbilda allmänheten om hur AI kan manipulera verkligheten – så att man inte faller offer för bedrägerier”* – Malcolm Murray

Ekonomiska brottslingar har varit snabba och framgångsrika i att anamma nya kommunikationssätt. År 2020 kapades i en koordinerad operation ett antal Twitterkonton tillhörande internationellt kända personer som de amerikanska tidigare presidenterna Barack Obama och Joe Biden som lockbeten i ett kryptobedrägeri. I Sverige har bedragare bland annat avslöjats med att använda falska videor i sociala media med riksbankschef Erik Thedéen i samma syfte, vilket tvingade Sveriges riksbank att utfärda en varning till allmänheten.<sup>31</sup> Chattgrupper där kända näringslivs- eller sociala medier-profilers namn missbrukats har också förekommit, bland annat rapporteras en svensk entreprenör så ha lurats på 12 miljoner kronor i en kryptosvindling.<sup>32</sup> Ett av Sveriges största aktieforum tvingades länge stänga på grund av mängden bedräglig och marknadsmanipulerande information.<sup>33</sup>

<sup>30</sup> <https://innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf>

<sup>31</sup> <https://tt.omni.se/riksbanken-varnar-for-fejkvideor-med-thed-en/a/al6yy2>

<sup>32</sup> <https://www.di.se/nyheter/catena-media-grundaren-blastes-pa-12-miljoner-tank-jag-ar-for-smart/>

<sup>33</sup> <https://www.svd.se/a/G38qaJ/nu-ska-aktieforumen-rensas-upp>

Även om motivet bakom den sortens brottslighet förstås i första hand är ekonomiskt, och inte syftar till att utgöra informationspåverkan, kan det ändå indirekt få förtroendeskadande effekt både för organisationer och individer vars identiteter missbrukats. Det leder även till att statliga och finansiella institutioner tvingas dementera falsk information.

**”Det är en uppenbar risk. Lätta, snabba deep-fakes av alla möjliga offentliga personer”**

Emil Larsson

Främmande makt må förvisso, åtminstone enligt öppna källor, sällan ha ertappats med att i informationspåverkande syfte initiera, finansiera, framta eller distribuera information om investeringsbedrägerier. Dock är de, både direkt och indirekt, aktivt verksamma inom samma ekosystem som de aktörer som gör det med ekonomiskt motiv – och kan över tid i olika skeden tänkas ha gemensamma intressen med dem.



**Vissa fristående grupper anlitas av statliga aktörer för att utföra attacker och jag är säker på att kriminella hackergrupper är beredda att agera för pengar”**

Todd Helmus

Det finns tekniska och organisatoriska kompetenser som antingen är gemensamma eller komplementära – varför samarbete skulle kunna ske (liksom upprättande av fristäder). Baserad i Asien finns Lazarus (eller APT38), den ökända nordkoreanska hackergruppen, idag specialiserad på kryptostölder, och en av regimens nyckelfinansiärer (gruppen sägs enskilda år ha bidragit med uppemot 5% av landets BNP). Tidigare har Lazarus stulit stora pengabelopp genom att infiltrera Swift-systemet för banköverföringar och bland annat hacka Bangladesh centralbank. Det var en välplanerad stöld som, om den lyckats fullt ut, hade genererat närmare en miljard dollar. (Istället blev bytet 81 miljoner dollar.)<sup>34</sup> De hackade även kryptobörsen Bybit och stal ETH till ett värde om 15 miljarder kronor.<sup>35</sup> Deras kryptovalutastölder var inledningsvis koncentrerade till Sydkorea (av ideologiska skäl) men internationaliserades snabbt (av ekonomiska skäl) till att omfatta åtminstone ett 30-tal länder i Europa, Asien och Nordamerika. Stölderna beräknas hittills ha uppgått till ett värde motsvarande 3 miljarder dollar.<sup>36</sup> De arbetar brett med dataintrång, phishing och trojanska hästar men kan likaså använda egenutvecklade smarttelefonapplikationer, falska NFT-annonser eller riktade LinkedInmeddelanden.

Baserade bland annat i Östeuropa finns organisationer, avdelningar och celler specialiserade på storskalig informationsdistribution främst i sociala media. Den så kallade ryska internetforskningsbyrån har exempelvis ertappats med att använda falska konton på X (tidigare Twitter) för informationspåverkande politiska syften. (Det vill säga

<sup>34</sup> <https://www.bbc.com/news/stories-57520169>

<sup>35</sup> <https://www.bbc.com/news/articles/c2kgndwwd7lo>

<sup>36</sup> För en översikt, se exempelvis: <https://go.recordedfuture.com/hubfs/reports/cta-2023-1130.pdf>

vad som kommit att kallas trollfabriker.)<sup>37</sup> Exakt hur arbetet i en trollfabrik är, eller i framtiden kan tänkas bli, organiserat är svårt att utifrån öppna källor besvara. Vissa forskare spekulerar i att informationsframtagandet ännu för en tid kommer att fordra visst arbete utfört av en människa – medan samordningen av, gradvis än större och mer sofistikerade, botnät redan kan automatiseras helt.<sup>38</sup>

**Definition:** *trollfabrik* – organiserat skapande och spridning av vilseledande eller polariserande innehåll på nätet via falska konton.

Investeringsbedrägerier och stölder baserade på ekonomisk desinformation medför stora samhällsekonomiska kostnader. De ingår ibland i ett ekonomiskt ekosystem som underbygger spekulation på ett sätt som negativt kan påverka individens privatekonomier. Stölder av finansiella tillgångar sker ibland i sådan skala att de kan få smärre finansiellt destabiliserande effekter – som vid kuppen mot Bangladesh centralbank. Hittills tycks den sortens ageranden främst ha utgjort ekonomiskt motiverad organiserad brottslighet. Det är dock inte omöjligt att i framtiden se främmande makt systematiskt möjliggöra eller delta i dylik verksamhet för att åstadkomma den sorts finansiellt destabiliserande och förtroendeskadliga konsekvenser som, som bieffekter, följer i dess spår. Så skulle exempelvis kunna ske genom att upplåta några av de resurser för storskalig informationspåverkan som nu främst används för politiskt destabiliserande och propagandistiska syften utomlands till att också, mer riktat, sprida även detta slags information åt samarbetsorganisationer. Alternativt kan en ekonomiskt motiverad aktör anlitas och påverkas via ekonomiska incitament. Vidare tyder den oproportionerligt höga förekomsten av ekonomiskt motiverade cyberangrepp i Ukraina sedan Rysslands invasion av landet, som bland andra det amerikanska teknikföretaget Microsoft registrerat, på att det om ett land blir måltavla i militära och informationspåverkande syften *även* medför en ökad förekomst av ekonomiskt motiverad cyberbrottslig aktivitet.<sup>39</sup>

”

**Tänk dig själv om du skulle starta en trollfabrik idag. Det är klart du skulle ha en AI-assistent så att varje person kan producera tusen gånger så mycket spam.”**

Emil Larsson

**”Det är relativt väl dokumenterat att en del länder använder cyberoperationer för ekonomiska ändamål. Det vore överraskande om inte flera länder försökte påverka finansiella system i väst, ibland via grupper kopplade till staten”**

Sahil Shah



37 Linvill, D. L., & Warren, P. L. (2020). Troll factories: Manufacturing specialized desinformation on Twitter. *Political Communication*, 37(4), 447-467.

38 Marcondes, F. S., Almeida, J. J., & Novais, P. (2024). An exploratory design science research on troll factories. *Integrated Computer-Aided Engineering*, 31(1), 95-115.

39 <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=1>

# Språkmodeller

Stora språkmodeller (eng. large language models, LLM) tilldrar sig mycket av uppmärksamhet i AI-utvecklingen av idag. Open AI:s Chat GPT har sedan den lanserades utgjort en av de snabbast växande tekniktjänsterna någonsin, sett till antalet användare.

De stora språkmodellerna möjliggör dels för hotaktörer att bättre planera sitt agerande, genom att bistå dem strategiskt, och dels att öka sin effektivitet genom att låta dem automatisera delar av sitt arbete. Det amerikanska teknikföretaget Anthropic offentliggjorde hösten 2025 att dess språkmodell, Claude, använts vid en storskalig cyberattack utförd av en kinesiskunderstödd grupp (GTG-1002) med ett 30-tal organisationer som mål. Såväl datastölder som intrång utfördes simultant med hög automatiseringsgrad. Mellan 80 och 90 procent av de taktiska operationerna under angreppet utfördes helt automatiserat.<sup>40</sup>

Till riskerna med de stora språkmodellerna hör även de tidigare i rapporten diskuterade deepfakearna. Medelst sådana kan desinformation lätt produceras.



**Stora språkmodeller är mest relevanta för den finansiella stabiliteten eftersom de kan skapa vilseledande text, ljud, bilder och video”**

Malcolm Murray



Utöver möjligheterna till text-, ljud-, bild- och videoproduktion är det förstaså att redan de stora språkmodellernas förmåga till informationssökning och -sammanställning utgör ett dramatiskt teknologiskt framsteg. De använder sig desutom av en kommunikationsstil vars konverserande språkliga ton och form, och användarvänliga gränssnitt, gör dem särskilt övertygande för deras användare. De har, rätt använda, potential att vederlägga konspirationsteorier, enligt en studie i den vetenskapliga tidskriften *Science*.<sup>41</sup> De kan, fel använda, emellertid även göra individer mer mottagliga för informationspåverkan. Forskare vid Storbritanniens AI-säkerhetsinstitut, universitetet i Oxford, London school of economics and political science, Stanford University samt MIT har nyligen i en serie omfattande experiment visat att språkmodeller kan få dig att ändra politiska åsikter på mindre än 10 minuters konversation.<sup>42</sup>

<sup>40</sup> <https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf>

<sup>41</sup> Costello, T. H., Pennycook, G., & Rand, D. G. (2024). Durably reducing conspiracy beliefs through dialogues with AI. *Science*, 385(6714), eadq1814.

<sup>42</sup> <https://www.ft.com/content/31e528b3-9800-4743-af0a-f5c3b80032do>

Experimenten omfattade nästan 77 000 deltagare i Storbritannien. I dem användes 19 olika språkmodeller, däribland flaggskeppsmodeller från amerikanska Open AI, Meta och X för att diskutera förvalda politiska frågor med deltagarna. Teknologin visade sig effektiv i att påverka deras politiska åsikter, delvis beroende på hur den instruerats. Särskilt effektiv var den när den på ett resonerande, vänligt sätt – snarare än moraliserande eller konfrontativt – lade fram övertygande information och argument anpassade efter individen.<sup>43</sup> Experimenten bevisar således att inte bara informationssammanställningen utan även konversationsstilen har psykologisk effekt på individernas uppfattningar.



**Om man tittar på de psykologiska utvärderingar som gjorts för stora språkmodeller överträffar de i allmänhet även de mest inflytelserika och övertygande mänskliga rösterna”**

Sahil Shah

Sålunda finns en överhängande risk att skraddarsydda språkmodeller (eng. custom GPT, generative pre-trained transformer) i samma övertygande form men baserade på tendensiöst innehåll kan komma att användas i informationspåverkande syfte.<sup>44</sup> Dessa syften kan vara förenliga med spridandet av ekonomisk desinformation så som falska faktapåståenden om till exempel en bank eller en valuta, konspirationsteorier om aktörer inom näringsliv, finans- eller penningpolitik, alternativt investeringsbedrägerier. Teknologin skulle även kunna användas som verktyg för att lura sig till känslig information.

Språkmodeller möjliggör dessutom att budskap mer effektivt kan skraddarsys för att påverka specifika mikrosegment. Med det avses mindre grupper i befolkningen eller till och med enskilda individer.

**”Det handlar inte om segmentering i ordets traditionella bemärkelse där ett segment avser en i förväg definierad grupp. Inte ens en i efterhand definierad grupp. Vad AI möjliggör är istället att ’lära’ sig att finna eller åstadkomma det en påverkare är intresserad av. En prompt skulle alltså kunna vara en fråga om vilket budskap som genererar bäst avsedd respons, där det inte spelar någon roll vilka individer det är som agerar på ett visst sätt, bara att så många som möjligt agerar i linje med den påverkan man vill åstadkomma”**

Richard Wahlund

Vidare tyder forskning de senaste åren på att stora språkmodeller, Chat GPT inräknad, är mer än önskvärt mottagliga för manipulation via så kallad dataförgiftning (eng. data poisoning). Eftersom stora språkmodeller tränas på och använder sig av information på internet är de sårbara för de datas kvalitet. De tycks emellertid anmärkningsvärt vara

<sup>43</sup> <https://arxiv.org/html/2507.13919v1>

<sup>44</sup> Goldstein, J. A., & Sastry, G. (2023). The coming age of AI-powered propaganda. *Foreign Affairs*, 7.

så att redan i sammanhanget försvinnande små informationsmängder, ett par hundra falska dokument, kan räcka för att på förutsägbara sätt snedvrider deras slutsatser kopplade till specifika frågor. Så även för stora språkmodeller med miljarder parameterinställningar tränade på enorma informationsmängder.<sup>4546</sup> De forskningsresultaten indikerar sålunda att stora språkmodeller har en större mottaglighet för informationspåverkan än man skulle kunna tro.



**Stora språkmodeller kan producera psykologiskt manipulerande kampanjer, skraddarsydda för olika subgrupper, i massiv skala, både som text, ljud och video. Kombinationen med botar och fejkade konton gör spridningen och förstärkningen mycket enklare och billigare”**

Sahil Shah



**LLM:er gör att attacker kan utföras mycket billigare och i större skala. Kostnaden för spear phishing-attacker har blivit mycket lägre vilket gör att man kan personalisera mycket enklare. Alla kan bli Cambridge Analytica”**

Staffan Truvé

Kombinationen av å ena sidan dess övertygande kommunikationsstil och å andra sidan dess mottaglighet för informationspåverkan gör att språkmodeller medför risker. Det är förvisso så att de ledande aktörerna i branschen för närvarande vidtar försiktighetsåtgärder. Chat GPT-ägaren Open AI har exempelvis startat en enhet som ska testa och identifiera sårbarheter bland annat för radikalisering eller framkallade villfarelser inklusive så kallade AI-psykosor.

Samtidigt skymtar en branschtrend i USA, där de största teknikbolagen har sina säten, av att informationsspridningen på internet och i sociala media måhända återliberaliseras. Det efter ett antal års något mer långgående ambitioner om faktakontroll och motverkande av desinformation, både under coronapandemin och inför de senaste amerikanska presidentvalen. (Frågor som dock nu kommit att politiseras inrikespolitiskt efter att de stora teknikföretagen av vissa anklagats för censur.) Meta har omorganiserat sin faktakontroll och tycks förlita sig alltmer på att användarkollektivet rapporterar olämpligt innehåll. X, tidigare Twitter, har reducerat sin personalstyrka och sagt upp externa rådgivare anlitate för att motverka näthat. Youtube har återaktiverat kontroversiella profilers tidigare avstängda konton, Tiktok likaså.<sup>474849</sup>

45 <https://www.nature.com/articles/s41591-024-03445-1>

46 <https://arxiv.org/pdf/2510.07192>

47 <https://www.theguardian.com/media/2023/dec/07/2024-elections-social-media-content-safety-policies-moderation>

48 [https://misinfoforeview.hks.harvard.edu/wp-content/uploads/2025/07/ozturan\\_declining\\_information\\_quality\\_20250711.pdf](https://misinfoforeview.hks.harvard.edu/wp-content/uploads/2025/07/ozturan_declining_information_quality_20250711.pdf)

49 <https://www.theguardian.com/technology/2025/jan/07/meta-facebook-instagram-threads-mark-zuckerberg-remove-fact-checkers-recommend-political-content>

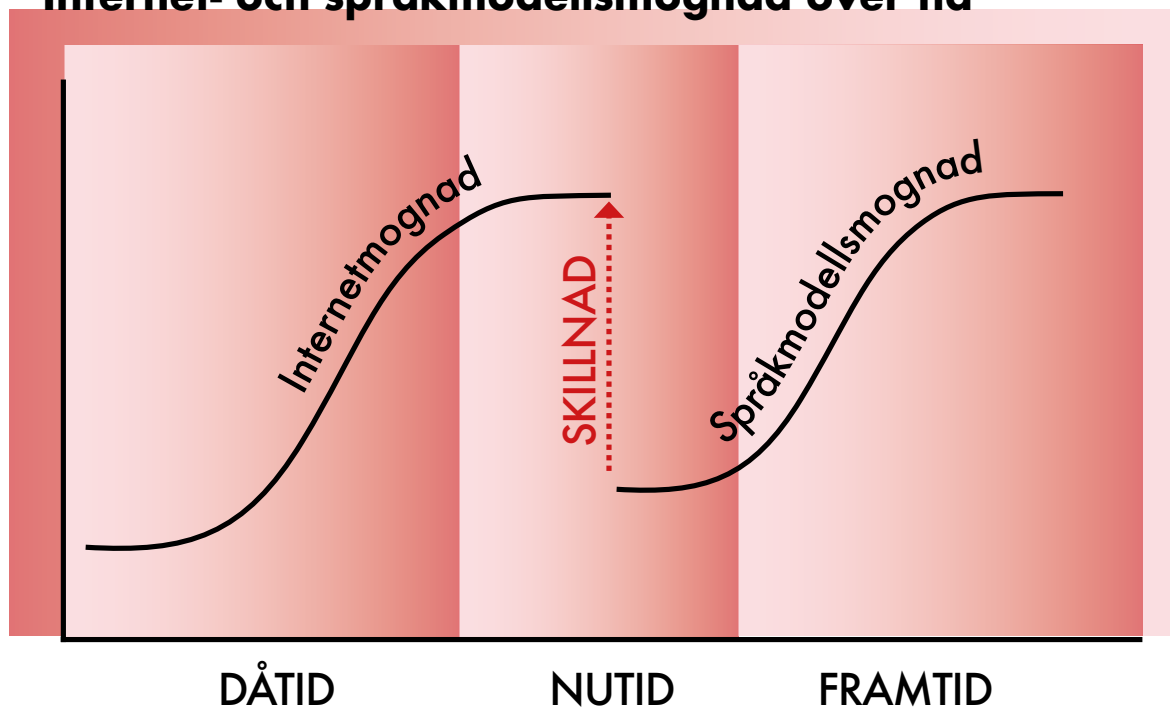
Därför är det i dagsläget svårt att förutspå i vilken utsträckning och på vilka sätt självreglering inom branschen faktiskt kommer att ske. Det är heller inte självklart att bedöma den matematisk-tekniska svårigheten i att upptäcka och motverka dataförgiftning och de stora teknikbolagens intresse att prioritera det.

## ”AI-kunnigheten i befolkningen är fortfarande låg”

Malcolm Murray

Det finns sannolikt ännu för en tid, åtminstone på medellång sikt, ett tidsfönster under vilket riktad informationspåverkan via språkmodeller, i den utsträckning det kommer att användas, har potential att vara särskilt effektiv. Det eftersom medborgarnas erfarenhet som användare av den nya teknologin ännu är begränsad jämfört med den mognad som kännetecknar det konventionella internetanvändandet i Sverige.

### Internet- och språkmodellsmognad över tid



MIKRONIVÅ

# Falskmynteri

Falskmynteriet har en lång historia. Under det amerikanska inbördeskriget ökade exempelvis förekomsten i sådan utsträckning att uppemot varannan amerikansk dollar i omlopp i mitten av 1800-talet tros ha varit falsk.<sup>5051</sup> Falskmynteri har även länge använts militärt.

Operation Andreas var en storskalig falskmynteriplan initierad av Nazityskland år 1939 i syfte att urholka det brittiska pundets status som världsvaluta. Idén var att mängder av falska fempundsedlar, omöjliga att skilja från äkta, skulle släppas över Storbritannien med flygplan. Propagandaminister Joseph Goebbels kallade det ”en grotesk plan” (tys. ”einen grotesken plan”). Operationen inleddes och inom loppet av ett par år var tillverkningen avancerad nog att reproducera sedlar i princip identiska med originalen såväl till papperskvalitet som utseende. Man hade även lyckats knäcka den brittiska centralbankens kod bakom sedlarnas serienummer. Under sitt senare namn, operation Bernhard, kom verksamheten även att innefatta andra valutor, däribland amerikanska dollar, och de falska sedlarna användes bland annat som betalmedel i underrättelseverksamheten.

Under 2000-talet har det återkommande ryktats om förekomsten av Superdollar (eng. *Supernotes*), ytterst förfinade förfalskningar av amerikanska 100-dollarsedlar. Nordkorea, ett land med en lång historia av falskmynteri, har beskyllts för inblandning.<sup>52</sup>

I ett alltmer kontantfritt svenskt samhälle är bland många medborgare kännedomen om hur landets sedlar och mynt faktiskt ser ut anmärkningsvärt låg. Det utgör en sårbarhet.<sup>53</sup> Samtidigt är den inrapporterade förekomsten av falskmynteri i Sverige mycket låg (ett par miljoner kronor årligen) även om det förstås finns ett betydande mörkertal. Samma sak med förfalskade postväxlar och checkar.

→ **Risksegment:** Medborgare utan kunskap om landets giltiga sedlar och mynt

Det går att föreställa sig att Sveriges digitala betalningsinfrastruktur drabbas av tekniska problem eller sabotage. Om så långvarigt sker blir tillgången till kontanta betalmedel viktig för att upprätthålla inhemsk konsumtion. Det är, snarare än under normala omständigheter, kanske särskilt just i ett sådant scenario som de destabiliserande och förtroendskadliga effekterna av falskmynteri vore som allra störst.

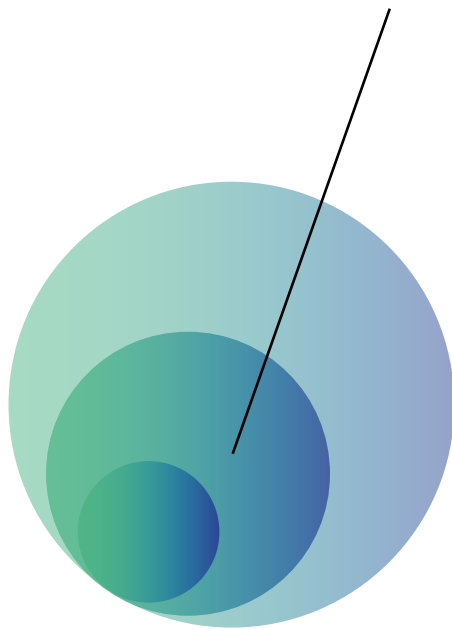
50 <https://www.govinfo.gov/content/pkg/CHRG-109shrg28241/pdf/CHRG-109shrg28241.pdf>

51 <https://www.congress.gov/crs-product/IF11414>

52 <https://sgp.fas.org/crs/row/RL33324.pdf>

53 <https://www.riksbank.se/sv/betalningar--kontanter/sa-betalar-svenskarna/betalningsrapport-2025/sakerhet-effektivitet-och-tillganglighet/ar-betalningar-i-sverige-sakra/antalet-falsa-sedlar-har-minskat-fran-en-hog-niva/>

# MESONIVÅ



# Mullvadar

Spionerihistorien innehåller flera välkända exempel inom ekonomins område. Kanske de allra kändaste är anklagelserna mot den inflytelserike ekonomen Harry Dexter White (1892-1948) vid det amerikanska finansdepartementet. White var central för både Morgenthauplanen (en preventiv strategi för att försämra Tysklands ekonomi efter Andravärldskriget) och Bretton Woodssystemet (ett dollarbaserat internationellt valutasystem åren 1945-1971). Han initierade Internationella valutafonden (IMF) och Världsbanken. Men han har även beskyllts för att samtidigt ha varit sovjetisk spion.

Ekonomispionage och industrispionage skapar återkommande stora problem i företagssektorn. Chefen för MI5, Storbritanniens underrättelsetjänst, har exempelvis avslöjat att ett enskilt industrispionage i form av stöld av immaterialrättsligt skyddad information en gång, vid ett enda tillfälle, kostade ett brittiskt företag motsvarande 8 miljarder kronor i uteblivna affärer på grund av en därmed försämrad förhandlingsposition.<sup>54</sup>

**Definitioner:** *Ekonomispionage* syftar till att komma i besittning av statliga eller privata affärshemligheter i syfte att avsiktligt gynna främmande makt. *Industrispionage* är det samma som ekonomispionage med skillnaden att syftet är att gynna ett annat företag<sup>55</sup>

Ekonomi- och industrispionage förekommer frekvent i forsknings- och teknikintensiva sektorer. Den kinesiska kemiingenjören Xiaorong You, Shannon kallad, dömdes exempelvis till 14 års fängelse i USA för ett ekonomispionage i miljardkronorsklassen mot Coca-Cola.<sup>56</sup> Även universitet och statsförvaltningar världen över drabbas ofta.<sup>57</sup> Säkerhetspolisen har sedan länge dokumenterat ett intresse från främmande makt för svensk forskning.<sup>58</sup> Antingen kan utländska gästforskare spionera (vilket exempelvis misstänks ha skett vid Karolinska institutet år 2005) eller så kan rekryteringsförsök av svenska forskare eller doktorander ske, i vad som ofta inleds som initiativ till forskningssamarbeten vid vetenskapliga konferenser.

Det vore naivt att anta att banker och finansiella institutioner inte också skulle kunna drabbas. Särskilt som ekonomihistorien, som tidigare nämnts, innehåller flera sådana fall. Dessutom är närbesläktade företeelser, som insiderhandel, någorlunda vanligt förekommande.

54 Button, M. (2020). Economic and industrial espionage. *Security Journal*, 33(1), 1-5.

55 Wagner, R. E. (2012). Bailouts and the potential for distortion of federal criminal law: Industrial espionage and beyond. *Tulane Law Review*, 86(5), 1017-1055.

56 <https://www.occrp.org/en/news/us-sentences-chemist-for-theft-of-coca-cola-secrets-worth-120-million>

57 <https://www.di.se/nyheter/varningen-totalitara-stater-suger-ut-svenska-universitet/>

58 <https://sakerhetspolisen.se/download/18.328e5ae9195250d81d04ad/1741953348924/Lägesbild%202024-2025.pdf>

→ **Risksegment:** Forsknings- och teknikintensiva organisationer, fintechbolag inkluderade

Direkta risker med möjliga implikationer för Sveriges finansiella stabilitet är läckor av marknadspåverkande information, till exempel sådan som förekommer i börsnoterade bolags kvartalsrapporter eller i protokollen från beslutsmöten vid finansiella institutioner innan dessa offentliggjorts. Främmande makt kan offentliggöra dylik information i förtroendeskadligt eller marknadsdestabiliserande syfte. Med det senare kan även finnas ekonomiska motiv.

Hösten 2025 noterades ett larmföretag på Stockholmsbörsen. Kort därpå utsattes företaget för ett dataintrång, vid vilket stora mängder kundinformation stals. Nyheten ledde till en tillfällig nedgång i bolagets aktiekurs om cirka 5 procent. Den som kan förutspå en sådan aktieprisnedgång kan tjäna pengar på det genom så kallad blankning.

**Definition:** *Blankning* – att sälja aktier man inte äger genom att först låna dem, sälja till aktuellt marknadspris, och senare köpa tillbaka dem för att återbetala aktielånet. Vinst uppstår om priset fallit så att de kan köpas tillbaka billigare än de såldes

Vad som på ytan såg ut som ett ryskt cybersäkerhetsföretag vid namn M-13 visade sig häromåret egentligen ha utgjort en fasad för en helt annan sorts verksamhet: insiderhandel baserad på stulna pressmeddelanden. Via datorintrång stals pressmeddelanden av amerikanska börsnoterade bolag, däribland biltillverkaren Tesla, innan marknadsinformationen i dem offentliggjorts. Var informationen sämre än marknaden förväntade sig blankade gärningsmännen aktien i förväg, och tjänade så uppemot en miljard kronor. Enligt amerikansk affärsmedia var operationen sanktionerad av den ryska federala säkerhetstjänsten, FSB.<sup>59</sup>



”**Jag kan se icke-statliga aktörer intressera sig för att blanka marknaden. Och om Ryssland kunnat underminera de västerländska kapitalmarknaderna hade de älskat det**”

Todd Helmus

Utöver ekonomispionage kan mullvadar utföra infiltrationer i syfte att upptäcka eller skapa organisatoriska eller tekniska sårbarheter som främmande makt eller andra aktörer sedan kan använda. De kan även sälja information till högstbjudande, exempelvis om säkerhetsbrister.

<sup>59</sup> <https://www.cnn.com/2024/08/01/putins-trader-how-russian-hackers-stole-millions-from-us-investors.html>

Det förekommer vidare en teori om att de så kallade kvantdatorernas utveckling gör att konventionellt krypterad information inte ännu, men snart, kommer att kunna dekrypteras. Därför kan försöken till stölder av krypterade medicinska eller finansiella data redan nu tänkas tillta enligt strategin: skörda nu, dekryptera sen (eng. harvest now, decrypt later).

I Operation drömjobb – som först avslöjades av ett israeliskt cybersäkerhetsföretag – använde nordkoreanska hackare, som tros tillhöra Lazarusgruppen, falska jobberbjudanden som metod. Under skenanställningsintervjuer lurades offren att ladda ner datorvirus som i sin tur möjliggjorde datastölder och fjärrstyrning av deras datorer. I vissa fall stals sedan kryptovaluta. I andra fall var syftet ekonomispionage. Exempelvis tycks gruppen under en period ha inriktat sig på företag som utvecklat drönarteknologi, vilken sålunda fallit i orätta händer.<sup>60</sup>

Nordkoreanska mullvadar har även ertappats med att i stor skala under falska identiteter distansarbeta i USA, bland annat som programmerare. Det i syfte att inifrån organisationerna utföra ekonomispionage eller cyberbrott. Eller helt enkelt för lörens skull (de kan utföra flera jobb samtidigt). Tillvägagångssättet har bland annat varit sådant att de först konstruerat falska meritförteckningar och profiler på LinkedIn (ibland med stulna identiteter, ibland med fingerade) med AI-genererade profilbilder och antagna namn. Sedan har de framgångsrikt använt AI-applikationer under urvalprocessen, i allt från personliga brev till själva anställningsintervjuerna, för att framställa sig så som krävts för att erbjudas jobben. Med hjälp av mellanhänder i USA har de sedan kunnat hämta ut företagsdatorer med tillgång till bolagens IT-system, vilket gett dem möjlighet att fingera att de visserligen distansarbetat, men åtminstone gjort så på plats i USA, trots att de egentligen befunnit sig på andra sidan världen. Vissa mellanhänder har förfogat över så många företagsdatorer att liknelsen med en laptopfarm har använts.<sup>61</sup> Mullvadarna har även under falska identiteter förfogat över bankkonton i USA. Ryskt spionage rapporteras istället snarare ske via en gigliknande rekryteringsstruktur.<sup>62</sup>

Polisen i Hong Kong har nyligen offentliggjort att en anställd vid ekonomiavdelningen på ett internationellt företag där lurades att utföra en pengaöverföring om mer än en kvarts miljard kronor till bedragare. Det efter att så ha beordrats vid ett digitalt möte med flera kollegor, ekonomichefen inräknad, som i efterhand alla visade sig ha varit deepfakeade kopior av dem.<sup>63</sup>

En konsultrapport om AI-baserade identitetsbedrägerier<sup>64</sup> visar att deepfakear ökat explosionsartat på senare år. De är den tredje vanligaste sortens identitetsbedrägeri i finanssektorn (efter kontokapning och kortbedrägeri/nätfiske). De utförs antingen av sminkade skådespelare (vars utseende sedan redigeras digitalt) eller så filmas,

60 <https://thehackernews.com/2025/10/north-korean-hackers-lure-defense.html>

61 <https://edition.cnn.com/interactive/2025/08/05/world/north-korea-it-worker-scheme-vis-intl-hnk/index.html>

62 <https://www.svd.se/a/dRXGao/nytt-ryskt-spionupplagg-pressar-sverige-liknar-gig-ekonomi>

63 <https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk>

64 Signicat (2025). The battle against AI-driven identity fraud. Rapport.

exempelvis under ett digitalt möte, en skärm på vilken det i realtid visas en deepfake. Metoderna används mot banker vid falska låneansökningar, liksom vid investeringsbedrägerier. Det förekommer även injektionsattacker där förinspelade filmer planteras i IT-system, exempelvis i angrepp på onboardingprocesser hos banker, fintech- eller telekombolag.

**Stärk resiliensen:** *”Utbildning är det absolut viktigaste komponenten för att få folk att fatta vad de inte ska göra. Alltså psykologisk resiliens, så att man inte skickar pengar när någon ringer och säger att man måste. Det gäller hela vägen från statlig nivå till företagsnivå.”* – Staffan Truvé

AI är förvisso orsaken till problemets förekomst – men används även i dess bekämpning. AI kan nämligen analysera röstvariation, blodflöde i ansiktet, ansiktsuttryck och mimik för att skilja en äkta video från en falsk.<sup>65</sup> Bland föreslagna sätt på vilka organisationer kan motverka problemet nämns ofta internutbildningar och säkrare företagsrutiner.

**Stärk resiliensen:** *”Stärk skyddet på banker, företag och myndigheter. AI kan automatisera och skala upp attacker snabbt”* – Malcolm Murray

I svensk statsförvaltning, liksom i andra länder, finns många avdelningar där ekonomisk information hanteras, sammanställs och rapporteras. Denna information ligger sedan till grund för myndigheters, näringslivets och regeringens beslutsfattande. Informationen är även marknadspåverkande. Den innefattar fakta som sysselsättnings-, inflations- och konjunktursiffror. Penningpolitiska beslut baseras på sådana data. Det går att föreställa sig att liknande data skulle manipuleras inifrån av främmande makt, eller att tillgången till dem skulle försvåras (exempelvis med kryptomask eller ransomware). Federal Reserve, den amerikanska centralbanken, utsattes under en femårsperiod för ett femtiotal dataintrång som utländska aktörer misstänks ha legat bakom.<sup>66</sup> Danmarks centralbank har också utsatts för en sådan attack. Det av hackergruppen kallad Mysiga björnen (eng. Cozy bear) med påstådda band till rysk underrättelsetjänst, GRU.<sup>67</sup>

→ **Risksegment:** Ekonomiska institutioner, finansdepartement och myndigheter

<sup>65</sup> En gemensam standard tas fram av Coalition for Content Provenance and Authenticity, C2PA, för att underlätta det – men även EU-kommissionens AI-kontor arbetar med frågan. För en översikt, se exempelvis Helmus, T. (2022). Artificial intelligence, deepfakes, and disinformation. *Perspective*: RAND Corporation.

<sup>66</sup> <https://www.theguardian.com/business/2016/jun/01/federal-reserve-hackings-cybersecurity-espionage>

<sup>67</sup> <https://cyberscoop.com/solarwinds-hackers-russia-denmark-bank/>

En sak som sker i USA för närvarande är att penningpolitiken där politiseras. Ledamöter i Federal Reserve, den amerikanska riksbanken, har under politiska påtryckningar bytts ut efter bedrägerianklagelser baserade på läckta dokument om gamla bolåneansökningar. Dess ordförande har offentligt kritiserats av presidenten. En mer politiserad penningpolitik medför nya möjligheter för externa påtryckningar och informationspåverkan. Historien lär oss att mullvadar och ekonomiskt spionage tidigare har förekommit på hög tjänstemannanivå vid ekonomiska institutioner.

**“Har man en person på en inflytelserik plats i en nation, sitter man då på komprometterande material på den personen kan det vara bra, men då kanske det inte handlar om att den personen ska förmås att bli propagandist, utan kanske snarare jobba med att försinka saker eller ifrågasätta”**

Per-Erik Nilsson



Det skulle också gå att föreställa sig manipulationer av externredovisning i enskilda företag inifrån, eller i många företag samtidigt utifrån via affärs- eller bokförings-system, vilket skulle kunna få marknadsdestabiliserande effekter.

→ **Risksegment:** Tillhandahållare av ekonomirelaterade IT-system och data

De allvarliga konsekvenserna av det amerikanska energibolaget Enrons konkurs vintern 2001 (som kostade aktieägarna många hundra miljarder kronor) följde av att dess redovisning under lång tid manipulerats. I inledningen av denna rapport nämndes som bekant även att den ryska Notpetya-attacken mot Ukraina började just i ett bokföringssystem och så kom att hårt drabba banksektorn.

# Ryktesspridning

Svenska storbanker med verksamhet i Baltikum, särskilt en av dem, har vid flera tillfällen utsatts för ryktesspridning. Vid ett tillfälle fick falska rykten via SMS och den ryskspråkiga motsvarigheten till Twitter om att banken skulle hotas av konkurs enligt massmedia lettiska kunder att ta ut 130 miljoner kronor.<sup>68</sup> Andra gånger, både i Baltikum och på senare år i Ukraina, har liknande rykten kunnat avse ländernas valuta eller dess bankomater – det vill säga påståenden om att de inhemska pengarna antingen skulle ha tappat i värde eller vara på väg att ta slut.

Målet med sådan ekonomisk desinformation är att orsaka en så kallad bankrusning (eng. bank run). Det som händer vid en bankrusning är att banken får likviditetsproblem om det normalt väldigt osannolika skulle hända och alltför många kunder begär ut sina insatta pengar samtidigt.<sup>69</sup> Främmande makt tycks med viss framgång tidigare ha experimenterat med att orkestrera bankrusningar i Östeuropa och svenska banker har då drabbats. Förnyade sådana försök har å ena sidan bättre förutsättningar att föranleda snabba förlopp idag, eftersom information sprids än lättare. (När Silicon Valley Bank i USA fick ekonomiska bekymmer, vilket sedermera renderade i indraget banktillstånd, spreds nyheten fort på sociala media. Under en och samma dag registrerades uttagsförsök till ett värde om nästan en halv biljon kronor, det högsta beloppet som hittills noterats.)<sup>70</sup>



Foto: Minh Nguyen - Own work, CC BY-SA 4.0

**Den första sociala media-drivna bankrusningen.**

68 <https://www.svt.se/nyheter/inrikes/swedbank-rykte-utreds-av-polis>

69 Brown, M., Trautmann, S. T., & Vlahu, R. (2017). Understanding bank-run contagion. *Management Science*, 63(7), 2272-2282.

70 <https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1580&context=ncbi>

Å andra sidan ger samma snabbhet i informationsspridning företag och myndigheter bättre möjlighet att omgående vederlägga felaktiga rykten och kommunicera garantier för spararnas insättningar.

**”För de allra flesta banker i Sverige finns ett insättningskydd. Sådana sparmedel skulle alltså inte påverkas av en konkurs, förutom att man kanske inte kommer ha tillgång till dem under en viss tid (innan de ersatts av staten). De flesta känner till detta skydd, vilket torde dämpa allmän oro och panik. Sedan handlar allt om vilka motåtgärder – om de är berättigade – övriga bankvärlden eller staten skulle sätta in, hur snabbt och i vilken omfattning. Allt detta gör en bankrusning i Sverige föga sannolik. Men skulle en sådan hända kan banken absolut gå i konkurs”**

Richard Wahlund

Forskningen om aktiemarknadens reaktioner på företagsnyheter tyder på att det bara är sanna nyheter som får genomslag i aktiepriset över tid (effekten av falska nyheter är kortvarig). På samma sätt är det förmodligen svårt att baserat på rakt igenom falsk rykesspridning orkestrera en fulländad bankrusning. Den felaktiga informationen skulle kunna dementeras trovärdigt (och statliga garantier vid behov träda i kraft). Däremot kan det tänkas möjligt att lyckas om rykesspridningen baseras på åtminstone delvis sann information. Att den avser en bank med reella ekonomiska problem, till exempel. När det gäller främmande maktens eventuella möjlighet att orsaka bankrusningar kan man således spekulera i att den största risken kanske inte är att de skulle sprida rena lögnerna utan snarare om de råkade känna till skadliga sanningar.

→ **Risksegment:** *“Om du ville påverka den finansiella stabiliteten skulle du troligen börja med en sårbar bank med skakiga finanser”* – Sahil Shah

I ett uppmärksammat brittiskt fältexperiment testades nyligen hur AI-genererade och -distribuerade nyhetsartiklar med falsk information om bankkriser och -konkurser påverkade människors intention att vilja ta ut pengar från sina bankkonton. Resultaten indikerade att desinformation med ekonomiskt innehåll kan få reella konsekvenser.<sup>71</sup>

Att infrastrukturen för digitala betalningar kan störas eller slås ut, utan tillräckliga reserver av kontanter, varken i hushålls- eller samhällsledet, är en annan risk. Ukraina har under den ryska invasionen av landet utsatts för riktade angrepp mot såväl betalssystem som bankomater.

**”Attacker mot betalssystem och sånt, det är ju bara att räkna med”**

Per-Erik Nilsson

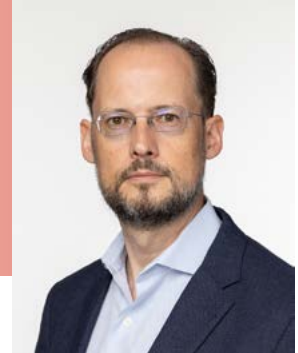
<sup>71</sup> [https://www.saynotodisinfo.com/\\_files/ugd/438ee6\\_d9f4506bfd2e43218b96f716bae91ce1.pdf](https://www.saynotodisinfo.com/_files/ugd/438ee6_d9f4506bfd2e43218b96f716bae91ce1.pdf)

Tokenisering är en modern teknologi som möjliggör betalning via virtuellt betalkort i mobiltelefonen eller smartklockan. Det är relativt informationssäkert. Det kräver dock, till skillnad mot ett fysiskt betalkort, ett fungerande kommunikationsnät för att kunna användas som betalmedel.

Inom EU pågår arbetet med att utveckla en digital Euro ämnad för betalningar. Och i Sverige har Riksbanken genomfört ett pilotprojekt om en möjlig e-krona.<sup>72</sup>

**”Att hacka Swish helt skulle kunna skapa kortvarigt kaos, eftersom en viss andel av betalningarna går via Swish. Kryptovalutor har ännu inte stor effekt på den riktiga ekonomin – även när Nordkorea stjal Bitcoin påverkas inte börserna som helhet. Den dag vi får en e-krona eller motsvarande digital valuta kan det bli annorlunda”**

Malcolm Murray



Ett möjligt samband mellan risken för bankrusning och e-valutor är att omvandlingar av en medborgares på banken insatta pengar till digitala, som en e-krona, ur bankens perspektiv skulle kunna föranleda ökade insättningsuttag. Oförutsedda större sådana omvandlingar, måhända koordinerade, skulle i så fall kunna skapa likviditetsutmaningar och exempelvis förvärra skeenden som de som dokumenterats i Baltikum och Ukraina. Även stablecoins, e-pengar baserade på teknik för distribuerade liggare (DLT), som blockkedjor, och vars värde knyts till en annan tillgång (exempelvis en viss valuta), kan medföra liknande risker enligt bland andra Sveriges riksbanks bedömning.<sup>73</sup>

## **”Man förvånas över att simulerade bank runs inte har hänt redan”**

Staffan Truvé

Även om falska nyheters effekt på börser och tillgångspriser som tidigare nämnts är kortvariga har de under en begränsad tid destabiliserande verkan – och upphovsmännen kan dessutom använda sådana prisfluktuationer för att berika sig själva samt de stater eller organisationer de företräder (exempelvis via blankning). Nyhetsbyrån AP:s

<sup>72</sup> <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2024/e-kronapiloten-etapp-4.pdf>

<sup>73</sup> <https://www.riksbank.se/globalassets/media/rapporter/staff-memo/svenska/2025/stablecoins-kan-ge-bättre-betalningar-men-risker-kvarstar.pdf>

Twitterkonto hackades 2013 och publicerade en nyhet om explosioner vid Vita huset, vilket omgående fick aktiemarknaden att reagera (men sedan snabbt korrigeras). Samma sak skedde våren 2025 när X-kontot Walter Bloomberg, ett fiktivt namn, felaktigt informerade om en 90-dagars paus av de amerikanska importtullarna, misinformation som spreds vidare av etablerade medier och fick aktiemarknaden att påverkas.<sup>74</sup>



**Falskt inlägg som fick börsen att reagera.**

De senaste tio åren har andra kända marknadspåverkande desinformationskampanjer omfattat falska förvärvsnyheter om Twitteraktien (+8%), ett påhittat pressmeddelande om att ett franskt byggbolag skulle efterhandskorrigera sin externredovisning (-18%), att kryptovalutan ETHs grundare skulle ha omkommit i en bilolycka (-40 miljarder kr), ett påhittat brev undertecknat av Larry Fink, BlackRocks VD, samt uppiktade konkursrykten om Metro Bank i Storbritannien (-11%).<sup>75</sup> En AI-genererad bild föreställande en explosion vid Pentagon delades på Twitter (och spreds därifrån vidare i ryska propagandakanaler).<sup>76</sup> Qatars officiella nyhetsbyrå har hackats och falska uttalanden från Emiren publicerats, vilket utlöste en diplomatisk kris, och en omfattande marknadsmanipulationsplan om att skada landets ekonomi genom att exploatera dess fasta växelkurs mot dollarn sägs senare ha planerats av en bank i Luxembourgen på uppdrag av en investeringsfond i Förenade Arabemiraten (anklagelser som emellertid bestridits).



**”Banker har tydliga strukturer för cyberrisker med definerat ansvar men desinformation är svårare att hantera eftersom deras system ofta inte kopplar sociala medierdata till exempelvis uttagsdata. Historiskt har det varit få incidenter. Så få banker har flerlayersförsvar för tidig upptäckt och kontroll av kundfriktion och sociala media”**

Sahil Shah

<sup>74</sup> <https://edition.cnn.com/2025/04/07/media/fake-news-x-post-caused-market-whiplash>

<sup>75</sup> <https://s3.amazonaws.com/media.mediapost.com/uploads/EconomicCostOfFakeNews.pdf>

<sup>76</sup> <https://www.theguardian.com/technology/2023/may/22/pentagon-ai-generated-image-explosion>

# Kontraktsvåld

Den organiserade brottsligheten är ett betydande samhällsproblem i Sverige. Dess utbredning har skapat en växande marknad för kontraktsvåld: våld-på-beställning (eng. violence-as-a-service).<sup>77</sup> Med det avses vad som av vissa har liknats vid en gängbrottslighetens gigekonomi.

I grupper på Telegram, Tiktok, Discord och Snapchat annonseras det öppett efter utförare av sprängningar, skjutningar och mord. Sådana grupper kan ha tiotusentals medlemmar.<sup>78</sup> Såväl svenska som amerikanska underrättelseuppgifter bekräftar att åtminstone ett kriminellt nätverk verksamt i Sverige åtagit sig kontraktsvålduppdrag åt regimen i Iran via dess underrättelse- och säkerhetsministerium.<sup>79</sup><sup>80</sup> Således föreligger idag etablerade affärsrelationer mellan främmande makt och den organiserade brottsligheten i Sverige.

Internationella medieuppgifter, som bekräftats av Richard Moore, chef för Storbritanniens underrättelsetjänst (MI6), gör gällande att Ryssland använder en snarlik rekryteringsmetod som de svenska kriminella gängerna i sökandet efter utförare av sabotage i Europa. Annonser om avgränsade beställningsuppdrag – gig – mot betalning (ofta i kryptovaluta).<sup>81</sup> Uppdragen inbegriper såväl sabotage som sprängningar, mordbränder, hot och våld – men även förmedlandet av hotfulla budskap och annan propaganda, till exempel via graffiti.

En etablerad plattform (marknadsplats) med huvudmän (kunder), uppdragsförmedlare (mäklare), och uppdragstagare (leverantörer) finns alltså redan representerad i Sverige. Det samtidigt som främmande makt dokumenterat organiserat tidigare beställningsuppdrag så, såväl i Sverige som i andra länder. Det gör att förutsättningar finns för att den befintliga marknadsstrukturen skulle kunna komma att användas även för den senare sortens kontraktsvåld i högre utsträckning i framtiden. Även desinformation-på-beställning förekommer och är organiserat på liknande sätt.<sup>82</sup>

**”Ryska ´aktiva åtgärder´: det är mutor, mord, utpressning...”**

Per-Erik Nilsson

77 <https://www.reuters.com/world/europe/sweden-mulling-social-media-age-limit-stop-gangs-recruiting-young-people-2024-12-09/>

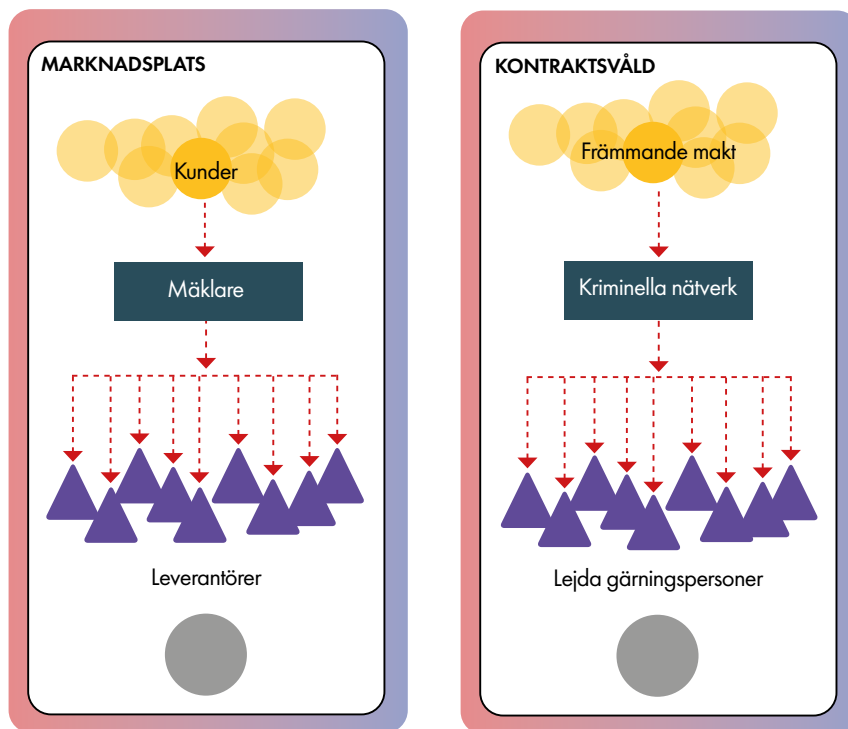
78 <https://www.sverigesradio.se/artikel/stor-chattgrupp-som-rekryterade-unga-till-vald-stangdes-ner>

79 <https://www.sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2024-05-30-iran-anvander-kriminella-i-sverige.html>

80 <https://www.state.gov/sanctioning-the-foxtrot-network>

81 <https://www.reuters.com/world/russias-suspected-sabotage-campaign-steps-up-europe-2024-10-21/>

82 <https://euvsdisinfo.eu/the-rise-of-the-disinformation-for-hire-industry/>



Parallellt med ovan beskrivna utveckling har hotbilden från den organiserade brottsligheten mot näringslivsföreträdare i Sverige ökat. Bland annat i och med flera utpressningsförsök.

➔ **Risksegment:** Enskilda förmögna entreprenörer och företagsledare

Det finns ett dubbelt riktningssamband mellan uppmärksammade våldsdåd och informationspåverkan. Dels såtillvida att informationspåverkan, som konspirationsteorier och propaganda (se kommande kapitel), kan få mottagliga individer i befolkningen att radikaliseras och agera våldsamt. Dels i att uppmärksammade våldshandlingar efteråt får informationspåverkande effekt i det samhälle där de skett. Terrorism fungerar exempelvis på båda de sätten. Det amerikanska fallet med den så kallade Unabombaren, den våldsbejakande teknik- och civilisationskritikern Ted Kaczynski (1942-2023), vars manifest under hot publicerades i tidningen *Washington post*, illustrerar detta tydligt. Kaczynski var ursprungligen påverkad av ett filosofiskt tankegods som han själv vidareutvecklade i konspiratorisk riktning. Senare kom hans dåd att radikaliserade andra och inspirera dem till liknande handlingar.<sup>8384</sup> Slutligen upptogs han i populärkulturen som en antietablissemangssymbol.

83 Barnett, B. A. (2015). 20 years later: A look back at the Unabomber manifesto. *Perspectives on Terrorism*, 9(6), 60-71.  
84 Fleming, S. (2022). The Unabomber and the origins of anti-tech radicalism. *Journal of Political Ideologies*, 27(2), 207-225.

I USA står Luigi Mangione åtalad för mordet på sjukförsäkringsbolaget United healthcares verkställande direktör Brian Thompson, som sköts till döds i anslutning till bolagets stämma.<sup>85</sup> Även om det alltjämt finns frågetecken om bakgrunden till mordet, och Mangione nekar till brott, är de flesta bedömare överens om att mordet bör förstås mot bakgrund av de återkommande politiska kritiska utspel som skett – och de konspirationsteorier som förekommit – riktade mot amerikanska sjukförsäkringsbolag i allmänhet och United healthcare i synnerhet. (Negativ opinion har alltså föregått dådet.) Det är dessutom så att mordet i efterhand mötts av skilda politiska reaktioner i befolkningen. Vissa har av ideologiska skäl tagit den misstänkte i försvar. (Dådet har alltså efteråt polariserat opinionen).

När det skedde föranledde dådet först omgående negativa aktieprisreaktioner, även för konkurrenter i samma bransch, vilka emellertid blev kortvariga. Noterbart är dock att dådet tycks ha haft en viss kvardröjande negativ effekt på det drabbade bolagets aktiepris. Det bland annat eftersom de polariserade reaktionerna på händelsen bidragit till att uppmärksamma utmaningar med bolagets affärsmodell. Fallet visar således att uppmärksammade våldsdåd och informationspåverkan kan samspela på ett sätt som blir marknadspåverkande, åtminstone för ett enskilt bolag, och som samtidigt kan accentuera polarisering av inhemsk politisk opinion.



**Muralmålning  
i New York**

Foto: @italiaotg/X

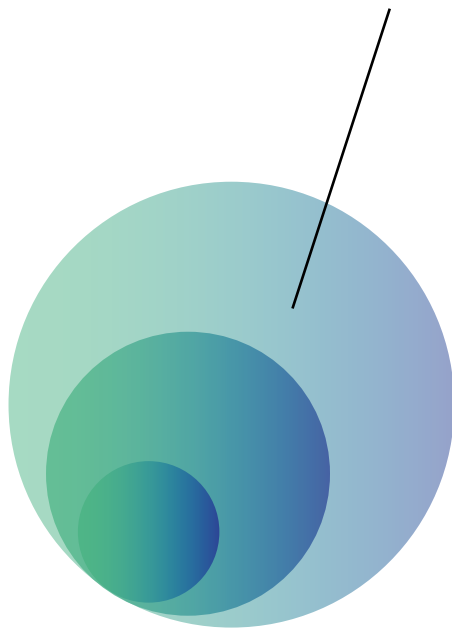
→ **Risksegment:** Kontroversiella bolag vars verksamhet kommit att politiseras

Det föreligger sammanfattningsvis en risk att utvecklingen av kontraktvåld i den fysiska världen – till sin organisationsstruktur – på sikt kan komma att spegla vad som för närvarande sker med cyberangrepp i den digitala världen. Rapporten Microsoft digital defense report 2025 identifierar exempelvis en aktuell trend bland cyberangrepp i riktning mot att hotaktörer använder sig mindre av centraliserad kontroll (eng. command-and-control, C2) och mer av gigmarknadsliknande decentraliserade nätverk (eng. peer-to-peer, P2P) dolda bakom lager av blockkedjeteknologi och information på den mörka webben (eng. darkweb).<sup>86</sup>

<sup>85</sup> <https://www.ft.com/content/1fb41957-26cb-49b2-820c-b16941a280c9>

<sup>86</sup> <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=1>

# MAKRONIVÅ



# Propaganda

Propaganda är ett ord som kommer av latinets *propagare*. Det betyder att sprida. Ordet började användas av katolska kyrkan under Påve Gregorius XV i början av 1600-talet. Det benämnde då ett kontor ansvarigt för kyrkans missionsverksamhet. Ett kontor vars syfte var att sprida katolicismens budskap och så bidra till dess seger över protestantismen under reformationen, som pågick då. Dess namn var *Congregatio de propaganda fide* (sv. Församlingen för trons spridning) eller som det förkortat kallades: propaganda.

Det var dock inte förrän under andra halvan av 1800-talet som ordet propaganda i Europa började användas om politisk påverkan och med negativa konnotationer. Dittills hade det uppfattats neutralt, som vi idag använder verbet informera. Men så började många av folkrörelserna vid tiden framemot förrförra sekelskiftet att använda sig av tidningar, flygblad och affischer i mobiliserandet av folkmassorna för just sin politiska sak. Under Första världskriget kom propagandan så att bli en självklar del av krigsapparaten.

Sverige är sedan ett antal år tillbaka föremål för islamistisk propaganda. Irans revolutionsgarde utförde, enligt officiella svenska myndighetsuppgifter, till exempel en propagandaoperation i Sverige i anslutning till de omtalade koranbränningarna sommaren 2023. I ett massutskick av 15 000 textmeddelanden uppmanades mottagarna att hämnas.<sup>87</sup>

Information av det slaget har implikationer för näringslivet. Al-Azhar, den sunni-muslimska utbildningsinstitutionen med säte i Egypten, uppmanade vid samma tid till bojkott av svenska varor.<sup>88</sup> Houthirebellerna i norra Yemen förbjöd import från Sverige.<sup>89</sup> De ekonomiska skadeverkningarna var förvisso obetydliga.<sup>90</sup> Såväl landets som enskilda företags anseenden kan dock ha påverkats.<sup>91</sup> Liknande skeenden är redan vanliga internationellt. De geopolitiska spänningarna mellan Kina och Australien ledde häromåret till kinesisk spridning av anti-australiensisk propaganda, följt av uppmaningar till bojkott av australienska varor och företag, samt slutligen strafftullar på korn. Under Gazakriget har kända amerikanska restaurangkedjor som McDonalds och Starbucks periodvis bojkottats i Egypten och Jordanien.

87 <https://apnews.com/article/sweden-iran-quran-burnings-revolutionary-guard-309f5f12aac2fc4e9a064bb0ffd313ee>

88 <https://apnews.com/article/sweden-government-turkey-stockholm-religion-ec5b282005f79be13ffe9baec473b5c5>

89 <https://www.reuters.com/world/middle-east/yemens-houthi-authorities-ban-swedish-imports-over-koran-burning-2023-07-08/>

90 <https://www.sverigesradio.se/artikel/how-quran-burnings-hit-swedish-companies-in-the-middle-east>

91 <https://si.se/omvarldens-reaktioner-pa-koranbranningar-i-sverige-sommaren-2023/>

**”Den som kommer först med ett påstående och blir betrodd avseende detta har i normala fall en fördel. Den som därefter försöker försvara sig skall ju få folk att ändra sig, och människor har i normalfallet svårare att ändra sig än att ta till sig något helt nytt. I vissa fall kan effekten bli långvarig, till exempel om smutskastningskampanjen fortsätter”**

Richard Wahlund

En allt vanligare typ av hemsidor innehåller recensioner av företag och deras tjänster eller produkter. Även i kommentarsfälten på företags sociala mediakonton kan omdömen lämnas. Sådana kan utnyttjas för propagandistiska syften, automatiserat med AI. Den brittiska biltillverkaren Jaguar lanserade häromåret vad som visade sig bli en politiskt kontroversiell reklamfilm.<sup>92</sup> Reklamfilmen möttes med starka reaktioner i sociala media och hade, av mestadels negativa skäl, redan sitt första dygn setts närmare 50 miljoner gånger.<sup>93</sup> Det amerikanska ölvarumärket Budweiser genomled ett liknande förlopp efter en likaledes kontroversiell reklam år 2023 vilket resulterande i en bojkott och minskad inhemsk försäljning.<sup>94</sup> I Skandinavien hände samma sak flygbolaget SAS år 2020.<sup>95</sup> Sådana skeenden kan låna sig väl till främmande makt. Dels som underlag för egenproducerad propaganda, dels som möjlighet för dem att i kommentarsfält eller sociala media underblåsa sådana polariserande meningsskiljaktigheter, till exempel via trollfabriker.



**Mer och mer propaganda riktas mot privata företag i syfte att skada deras varumärken”**

Todd Helmus



En artikel i den vetenskapliga tidningen *Nature* menar att annonsering är en viktig finansieringskälla för propagandahemsidor men att annonsörerna ofta är ovetande därom.<sup>96</sup> Därutöver är den ryska metoden att etablera falska nyhetshemsidor påminnande om äkta, som i den omtalade Operation Doppelgänger, väl känd.<sup>97</sup> I en senare propagandaoperation, Copycop (även benämnd Storm-1516), har åtminstone 200 nya falska hemsidor används i propagandistiskt syfte. Hemsidorna har härmat förlagor i form av nyhetshemsidor likväl som politiska organisationer – ibland till och med utgett sig för att vara faktakontrollsidor. De har omfattat många olika länder (från Armenien

92 <https://www.youtube.com/watch?v=rLtF1rghfng>

93 <https://www.foxbusiness.com/media/jaguar-dubbed-bud-light-2-0-after-releasing-modernist-rebranding-ad-androgynous-models-no-cars>

94 <https://www.bbc.com/news/business-66398296>

95 <https://www.forbes.com/sites/davidnikel/2020/02/13/is-anything-truly-scandinavian-the-bizarre-sas-ad-controversy-explained/>

96 <https://www.nature.com/articles/s41586-024-07404-1>

97 <https://mpf.se/download/18.7cfffbee41969f6d83e115221/1747230166207/Beyond%20Operation%20Doppelganger.pdf>

till Kanada) och språk (från tyska till swahili). Operationen rapporteras understödjas av det Moskva-baserade Centret för geopolitisk expertis och GRU. AI – mer precist Metas Llama 3-språkmodell, baserad på öppen källkod – tros ha använts för informationsframställningen.<sup>98</sup>

**Stärk resiliensen:** *“Vi detekterar påverkansoperationer genom detektion av anomalier i nyhetsflöden. Som till exempel när nyheter bara förekommer på ett visst språk”*  
– Staffan Truvé

Mycket propaganda är rena fabrikationer. Liksom vid informationspåverkan med falska företagsnyheter kan man föreställa sig att sådan, uppenbart felaktig propaganda, är mindre effektiv än om den baserats på åtminstone delvis faktamässigt sann information.

## “Bra propaganda bygger på i alla fall ett korn av sanning”

Per-Erik Nilsson

Det är dessutom välkänt inom den psykologiska forskningen att vi människor tenderar att vara ganska lättpåverkade, även av felaktig eller selektivt utvald information, så länge den stämmer överens med våra befintliga uppfattningar.<sup>99</sup>

→ **Risksegment:** Medborgare med åsikter förenliga med den propaganda för vilken de utsätts

Detta gör politiskt polariserande ämnen som brottsbekämpning, invandring eller miljöfrågor särskilt tacksamma för den som vill skapa eller distribuera propaganda. Samma sak med större politiska händelser som folkomröstningar, allmänna val eller demonstrationer. Direkta implikationer för det svenska näringslivet kan exempelvis propaganda om frågor som militärexport, arbetskraftsinvandring och industrietableringar ha. Likaså ämnen som utrikeshandel med kontroversiella bolag eller regimer i vissa andra länder. Även pensions- och investeringsfonders beslut kan politiseras och deras investeringar föranleda kritik och påtryckningar, vilket exempelvis norska SPU (Statens pensionsfond utland), den så kallade oljefonden, fått erfaras.<sup>100</sup>

98 <https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-ru-2025-0917.pdf>

99 Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of general psychology*, 2(2), 175-220.

100 <https://www.ft.com/content/f6b34e71-2b3e-43ad-99a9-558a34f56853>

# Konspirationsteorier

Konspirationsteorier är samlingsnamnet för idéer om att hemliga sammansvärjningar organiserade av inflytelserika grupper egentligen styr viktiga skeenden i världen. Att den amerikanska månlandningen år 1969 egentligen inte skulle ha ägt rum (utan spelats in i en filmstudio) är ett klassiskt exempel på en konspirationsteori. Att utomjordingar skulle ha besökt Jorden, vilket tystats ned av statsmakterna, och kanske alltjämt förvaras nedfrysta på en militärbas i öknen, är en annan känd konspirationsteori. Likaså att reguljära passagerarflygplan skulle släppa ut kemikalier för att påverka medborgarna psykologiskt. Eller dricksvattnet förgiftas av samma skäl. Påstått röstfusk vid politiska val är också det en vanlig konspirationsteori. Eller att telefonnätet 5G i hemlighet skadar hälsan. Coronapandemin, under vilken många konspirationsteorier cirkulerade, blev mångas inkörsport till konspiratoriskt tänkande – vilket, åtminstone sedan dess, tycks öka i omfattning i samhället.<sup>101</sup>

”Konspirationsteorier fungerar utifrån ett antal socialpsykologiska principer om hur vi människor reagerar på olika företeelser som testats empiriskt och visat sig fungera i verkligheten”

Richard Wahlund



Även näringslivet och samhällsekonomin är föremål för konspirationsteorier. De kan ibland avse särskilt förmögna individer. Den ungersk-amerikanske investeraren, miljardären George Soros, har exempelvis figurerat i många konspirationsteorier med politiska förtecken internationellt. I Sverige har liknande anklagelser ibland riktats mot industrifamiljen Wallenberg. Sammankomster där politiker och näringslivsföreträdare möts, som de i schweiziska Davos eller svenska Almedalen eller de i Bilderberggruppen, omgärdas också av konspirationsteorier. Många ekonomiska konspirationsteorier har antisemitiska förtecken. Som när judiska intressegrupper och banker (exempelvis bankirfamiljen Rotchild) anklagats för att tillsammans i hemlighet styra världsekonomin.<sup>102</sup> IMF och Världsbanken har även de varit föremål för konspirationsteorier. Det finns även ekonomiska konspirationsteorier av mer vardagligt slag.<sup>103</sup> Som att livsmedelsbutiker skulle placera mjölken längst in i butiken för att främja sin försäljning.

Såväl penningpolitiken som de finansiella marknaderna förekommer även de i konspirationsteorier.<sup>104</sup> De kan innehålla idéer om att det monetära systemet eller

101 Granados Samayoa, J. A., Moore, C. A., Ruisch, B. C., Boggs, S. T., Ladanyi, J. T., & Fazio, R. H. (2022). A gateway conspiracy? Belief in COVID-19 conspiracy theories prospectively predicts greater conspiracist ideation. *Plos one*, 17(10), e0275502.

102 Lockwood, E. (2021). The antisemitic backlash to financial power: Conspiracy theory as a response to financial complexity and crisis. *New Political Economy*, 26(2), 261-270.

103 Furnham, A. (2013). Commercial conspiracy theories: A pilot study. *Frontiers in Psychology*, 4(379) 1-5.

104 Braun, B. (2016). Speaking to the people? Money, trust, and central bank legitimacy in the age of quantitative easing. *Review of international political economy*, 23(6), 1064-1092.

aktiemarknaden arrangerats för att gynna de redan förmögna på de mindre bemedla- des bekostnad.<sup>105</sup> Inte sällan sprids sådana konspirationsteorier, direkt eller indirekt, tillsammans med uppmaningar om att investera i alternativa tillgångsslag som guld eller kryptovalutor (som alternativ till fiat-pengar). Ibland kan de misstänkliggöra och så bidra till att urholka förtroendet för konventionell penningpolitik och kapitalförvalt- ning eller det vanliga pensionssystemet.

Införandet av en digital euro eller e-krona skulle säkerligen åtföljas av desinformation. Dels av kriminella som bedrägeriförsök. Dels av andra aktörer av informationspåver- kansskäl.

Konspirationsteorier om den digitala euron och e-kronan cirkulerar redan. Exempelvis påstås de digitala valutornas egentliga syfte av konspirationste- oretiker vara att ersätta kontanta pengar med digitala för att möjliggöra en striktare ekonomisk övervakning av medborgarna.<sup>106</sup><sup>107</sup> I en enkätundersökning utförd av forskare vid King's College i London sommaren 2023, med ett urval representativt för den vuxna befolkningen i Storbritannien som svarande (n=2274), instämde mer än var tredje (35%) i påståendet: "Centralbankers digitala valutor kommer användas av regeringen för att kontrollera människors pengar och begränsa deras frihet".<sup>108</sup>



**Rysk anti-EU-propaganda, även om den är riktad mot EU som institution, påverkar indirekt förtroendet även för euron"**

Staffan Truvé

### **Konspirationsteori som en av tre instämmer i:**

**"Centralbankers digitala valutor kommer användas av regeringen för att kontrollera människors pengar och begränsa deras frihet"**

De flesta akademiska definitionerna av vad en konspirationsteori är koncentrerar sig på hur vi människor tänker inför dem, inte om de råkar vara sanna eller falska.<sup>109</sup> Således är det per definition möjligt att konspirationsteorier ibland visar sig stämma (dvs att hemliga sammansvärjningar faktiskt skett). Betydligt oftare är det dock så att en faktisk händelse eller ett indicium selektivt tolkas överdrivet konspiratoriskt. I ett demokratiskt marknadsekonomiskt land som Sverige är medborgarnas förtroende centralt för samhällets funktion och långsiktiga stabilitet. Därför är det farligt om ekon- omiska konspirationsteorier skapas, förfinas eller distribueras av främmande makt i syfte att skada detta förtroende.

105 Fiagbenu, M. E. (2022). The stock market is rigged? Conspiracy beliefs and distrust predict lower stock market participation. *Applied Cognitive Psychology*, 36(5), 978–995.

106 <https://www.france24.com/en/live-news/20250326-ecb-s-digital-euro-sparks-flurry-of-online-misinformation>

107 <https://www.politico.eu/article/digital-euro-currency-conspiracy-theory-marc-friedrich-jorg-meuthen-european-central-bank-surveillance/>

108 <https://www.kcl.ac.uk/policy-institute/assets/conspiracy-belief-among-the-uk-public.pdf>

109 Napolitano, M. G., & Reuter, K. (2023). What is a conspiracy theory?. *Erkenntnis*, 88(5), 2035-2062.

# Fasader

I den moderna informationsekonomin blir det allt svårare att veta vem som egentligen ligger bakom den information som sprids och når allmänhetens kännedom. Influera-re (eng. influencers) – populära profiler på sociala media – kan ha en räckvidd större än vanliga mediahus. Influera-re med inriktning på ekonomi (eng. finfluencers) delar ofta investeringstips och metoder för att snabbt bli rik. På Tiktok har innehåll med hashtagarna #moneytok och #investing 16 miljarder respektive 9 miljarder visningar. Regleringarna, individanpassningen och försiktigheten som präglar vanlig finansiell rådgivning saknas dock där. På sociala media kan marknadsföring inte sällan vara dold eller missledande. Det kan i allmänhet vara svårt för mediakonsumenter att skilja informationskällor av olika kvalitet åt.<sup>110</sup>



**Jag är mycket orolig över journalistikens benägenhet att följa med utvecklingen i sociala medier i hopp om att kunna konkurrera med de nya utmanarna, på bekostnad av journalistisk kvalitet”**

Richard Wahlund

Eftersom influera-re i det moderna medialandskapet kommit att nå sådan räckvidd, och åtnjuter sådan trovärdighet, kan de av främmande makt komma att utsättas för informationspåverkan.

Om så sker har till exempel en podcastvärd inte nödvändigtvis samma redaktionella och källkritiska kompetens som en nyhetsredaktion och riskerar sålunda att oavsiktligt agera misinformationsspridare och så även skänka legitimitet åt desinformation. Exem- plen är oräkneliga på hur propaganda och konspirationsteorier spridits av influera-re som riskerar att utnyttjas av hotaktörer.

**”Det behövs fasader.  
Trovärdigheten är viktig och  
influera-re ger dem både det  
och uppmärksamhet”**

Todd Helmus

<sup>110</sup> <https://www.dn.se/debatt/nyhetsjournalistiken-overlever-inte-utan-lasarnas-fortroende/>

Användandet av fasader är en kardinalmetod vid främmande makts informationspåverkan, även icke-digitalt. I Storbritannien anklagas exempelvis falska kinesiska affärsmän för försök till så kallad elitrekrytering (eng. elite capture), det vill säga personlig påverkan i syfte att åstadkomma pro-kinesiska ideologiska omvändningar hos inflytelserika individer. De påstås i England ha riktat in sig på självaste Prins Andrew (numera Andrew Mountbatten Windsor) via ett affärssamarbete.<sup>111</sup>

→ **Risksegment:** Påverkbara individer tillhörande samhällseliten

I Tyskland sägs en allmän konstfotografiutställning egentligen ha utgjort en rysk påverkansoperation.<sup>112</sup> Rysk-ortodoxa kyrkor i Sverige kan ha varit fasader åt Kreml.<sup>113</sup>

Intresseorganisationen Det kinesiska kommunistpartiets enhetsfront bedriver informationspåverkan åt landet internationellt.<sup>114</sup> Så har även skett via den välkända operationen Spamouflage, baserad på falska sociala mediakonton.<sup>115</sup> Dess andra våg fick nyligen Meta att stänga ner tusentals falska konton som spridit desinformation.<sup>116</sup>

Ett politiskt partis kontroversiella pro-ryska reklamkampanj i Oslos tunnelbana inför det norska parlamentsvalet uppges egentligen ha finansierats av en norsk affärsman med verksamhet i Ryssland.<sup>117</sup>

Privata företag, stiftelser, forskningsinstitut, intresse- och frivilligorganisationer kan alla utgöra fasader och användas för sofistikerad informationspåverkan. Denna vore då sannolikt påminnande om konventionell lobbyingverksamhet innefattande allmänna, opinionsbildande initiativ i massmedia eller personliga, relationsbaserade sådana inom politik och näringsliv.

**Stärk resiliensen:** *“Efterforska, inom ramen för befintlig lagstiftning, vilka som egentligen stöder och finansierar organisationer som verkar i sektorer med implikationer för Sveriges näringsliv, politik, forskning och finansiella stabilitet”* – Gustav Almquist

111 <https://www.bbc.com/news/articles/cm2evegmz98o>

112 <https://www.reuters.com/investigations/russia-linked-propaganda-campaign-pushes-undercut-german-support-ukraine-2025-02-18/>

113 <https://www.svt.se/nyheter/lokalt/vastmanland/har-svarar-prasten-pa-anklagelserna-mot-rysk-ortodoxa-kyrkan-i-vasteras-inga-ryska-pengar>

114 <https://www.bbc.com/news/articles/c878evdp758o>

115 <https://apnews.com/article/china-disinformation-network-foreign-influence-us-election-a2b396518baf-d8e36635a3796c8271d7>

116 <https://time.com/6310040/chinese-influence-operation-meta/>

117 [https://www.nrk.no/norge/for-partileiaren\\_hevdar-at-dette-er-mannen-som-betalte-for-den-omstridde-partikampanjen-1.17425503](https://www.nrk.no/norge/for-partileiaren_hevdar-at-dette-er-mannen-som-betalte-for-den-omstridde-partikampanjen-1.17425503)

# Diskussion

I föreliggande forskningsrapport har olika riskområden identifierats via forskarlagets efterforskningar och analyser. I respektive kapitel har dokumenterade exempelhändelser och möjliga scenarier med potentiella implikationer för Sveriges finansiella stabilitet diskuterats. Redan de exempelhändelser och scenarier som hittills i rapporten redogjorts för tecknar, enskilt men framförallt sammantaget, en något oroväckande bild, både i nuläget och inför framtiden.

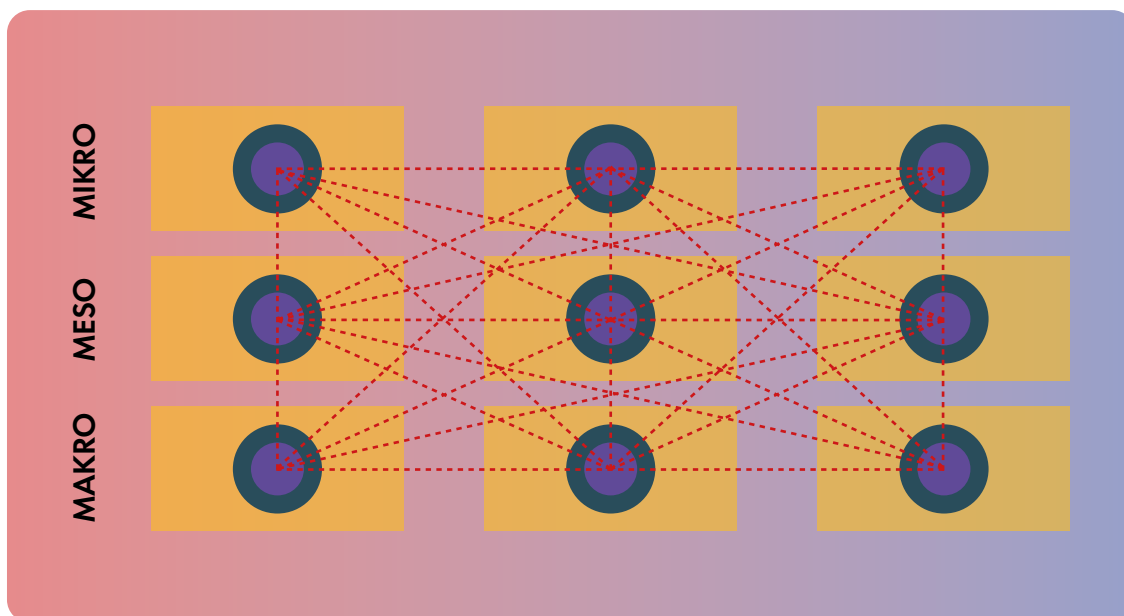
Investeringsbedrägerier lär framöver, i och med AI-utvecklingen, öka i såväl omfattning som sofistikeradhet. Språkmodeller kommer att missbrukas av illvilliga aktörer. Falskmynteri, liksom andra modernare metoder, med negativ inverkan på samhällets betalningsinfrastruktur lär fortgå. Ryktesspridning, exempelvis desinformation som misskrediterar banker och företag, kommer även fortsättningsvis att spridas. Mullvadar ska komma att infiltrera fler organisationer och institutioner och industrispionage ske. Kontraktsvåld mot näringslivsföreträdare är även i framtiden att vänta. Propaganda riktad mot Sverige som land och uppvigling mot svenska näringslivsintressen har ingetdera inträffat för sista gången. Konspirationsteorier om det finansiella systemet, valutor och centralbanker kommer fortsatt att cirkulera framgent. Fasader i de ideella, idéburna och politiska sektorerna, liksom inom forskning och (sociala) media, lär återkommande utnyttjas av främmande makt.

Samtidigt är huvudansvarig forskares samlade bedömning att det inte är de ovanstående riskerna i sina nuvarande former och under normala omständigheter som skulle kunna få den starkaste finansiellt destabiliserande effekten för Sverige. Inte ens om de, som befarat, skulle öka i förekomst.

Mer betydande konsekvenser skulle förmodligen kunna uppstå vid särskilda tillfällen: när Sverige politiskt eller ekonomiskt befann sig i en känslig eller sårbar situation, vilket främmande makt strategiskt-oppportunistiskt skulle kunna utnyttja. Den svenska NATO-ansökan innebar exempelvis en såväl inrikes- som utrikespolitisk utsatthet som hotaktörer de facto försökte exploatera via informationspåverkan. Liknande tillstånd av ekonomisk utsatthet skulle till exempel kunna orsakas av statsfinansiella problem, större kronkursförändringar, förestående privatiseringar eller börsnoteringar, oförutsedda bolagskonkurser eller betydande kreditförluster eller likviditetsproblem i banksektorn. Likaså av politiska beslut som införandet av en e-krona eller svenskt inträde i eurovalutasamarbetet. Hotaktörer skulle då kunna utnyttja sådana tillfällen att åsamka skada som och när möjlighet gavs.

Det allra mest riskfulla scenariot vore emellertid om främmande makt angrep frågan mer strategiskt än vad som hittills dokumenterats. Det vill säga med mer långsiktighet, koordinering, genomtänkt planering och ekonomisk kompetens.

Med en liknelse går det att betrakta de nio olika riskområden som identifierats i rapporten som en samling reglage. De olika sätt på vilka de planerat – sekventiellt eller simultant – skulle kunna aktiveras, och kombineras, av främmande makt i syfte att åstadkomma största möjliga finansiella instabilitet: däri återfinns troligen den allra största risken för Sverige.



**Den för Sverige enskilt största faran utgörs inte av någon enskild risk utan av de sätt på vilka olika metoder kan komma att kombineras eller användas i särskilt känsliga situationer.**

Sveriges befolkning har hög tilltro till samhällets institutioner. I allmänhet är tilliten medborgare och organisationer emellan god. Civil beredskap finns. Det skyddar i någon utsträckning mot effekterna av informationspåverkan. De resiliensstärkande insatser i form av informations-, utbildnings- och kontrollåtgärder som föreslagits i denna rapport rekommenderas som komplement därtill. Även om så sker kommer det dock under överskådlig framtid förbli så att ämnet för denna rapport representerar en reell risk för Sverige och dess allierade. Främmande makts förmåga finns nog, den dag de också har viljan.

# Forskarlag



Foto: Sofia Runarsdotter

## **Dr. Gustav Almqvist, Forskningsledare**

Doktor i företagsekonomi från Handelshögskolan i Stockholm och forskare vid SSE House of governance and public policy och Stockholm school of economics institute for research. Expert inom forskningsområdet ekonomisk psykologi.

## **Dr. Sofie Sagfossen, Senior forskare**

Doktor i företagsekonomi från Handelshögskolan i Stockholm och Associate professor vid Kristiania university of applied sciences i Oslo. Expert bland annat på digitalisering och konsumenters interaktion med ny teknologi.



Foto: Karl Gabor

## **Leon Nudel, Forskningsassistent**

Masterexamen i företagsekonomi från Handelshögskolan i Stockholm och arbetande som journalist. Har i forskningsprojektet arbetat med omvärldsanalys, mediesökningar och expertintervjuer.

## **Maria Wilow, Forskningsassistent**

Kandidatexamen i företagsekonomi från Handelshögskolan i Stockholm och studerande vid dess masterprogram i business och management. Har i forskningsprojektet arbetat med research relaterad till den så kallade tredje uppgiften.



Myndigheten för  
psykologiskt försvar



HOUSE OF GOVERNANCE  
AND PUBLIC POLICY