GÖTEBORGS UNIVERSITET

JOURNALISTIK, MEDIER OCH KOMMUNIKATION

RISKKOMMUNIKATION VID SAMHÄLLELIGA CYBERKRISER

Gabriella Sandstig

Arbetsrapport nr 94

JMG

Riskkommunikation vid samhälleliga cyberkriser

Författare: Gabriella Sandstig

Finansiering: Rapporten är beställd och finansierad av Myndigheten för samhällsskydd och beredskap (MSB) inom ramen för projektet *Risk- och beredskapskommunikation för ett robust digitalurbant samhälle* (DRUCOM) under ledning av projektledare Mats Eriksson vid Örebro Universitet.

ISSN 1101-4679
Datum 2025-06-30
Institutionen för journalistik, medier och kommunikation
Göteborgs universitet
www.gu.se/jmg

Innehåll

Sammanfattning 6

Inledning 8

Cyberrisker och samhälleliga cyberkriser 8

Bakgrund 11

Riskkommunikation 11

Krisberedskap och medborgarens egna ansvar 12

Vad individen kan göra själv 13

Disposition av resultat och analys 14

Riskuppfattningar 15

Antagonistiska hot toppar bland riskerna 17

Kön och ålder formar riskuppfattning 18

Kapabilitet och beredskap 20

Stark tillit till den egna förmågan 21

Socioekonomi avgör krisförmågan 22

Många vill förbereda sig mot cyberrisker 23

Hög riskuppfattning och självtillit motiverar 23

Fokus på basåtgärder för skydd 24

Tre vägar till beredskap: rusta, medvetandegöra och värna relationer 25

Olika drivkrafter bakom olika åtgärder 26

Riskperceptionsparadoxen 27

Kapabilitetsbrist minskar motivationen 28

Låg tillit och inkomst förklarar passivitet 29

Hög självtillit och låg riskuppfattning ger acceptans 29

Slutsatser och rekommendationer 30

Gör budskapet relevant för att nå fram 30

Anpassa kommunikationen till olika grupper 30

Stötta socioekonomiskt svagare grupper i samhället 31
Främja engagemang och samverkan i närområdet 31
Studiens begränsning 32
Referenser 33
Bilaga 1 Uppdrag 38
Bilaga 2 Tabellbilaga 40

Sammanfattning

Cyberattacker har under de senaste åren rankats som några av de främsta globala riskerna. Men också cyberhot riktade mot en enskild kommun kan leda till stora störningar i samhällsservicen. Kommuner har ett särskilt ansvar att kommunicera risker till relevanta intressenter, inte minst medborgarna som bor i kommunen. Detta för att medborgarna ska ha tillförlitlig och relevant information för att kunna bedöma riskerna som kan drabba dem, minska deras sårbarhet och öka deras beredskap inför ett framtida hot. En grundförutsättning för det arbetet är kunskap om vad medborgarna faktiskt vet och är beredda att göra för att skydda sig.

I denna rapport presenteras resultat från projektet *Risk- och beredskapskommunikation för ett robust digitalurbant samhälle* (DURCOM). Resultaten rör medborgarnas föreställningar om cyberrisker i jämförelse med andra risker, vilka åtgärder de är motiverade att vidta i händelse av en samhällelig cyberkris samt nycklar till varför de är eller inte är motiverade att vidta åtgärder för att skydda sig. Resultaten baseras på kontrollgruppens svar (n=879) i en större experimentstudie genomförd inom ramen för Medborgarpanelen 2022.

Antagonistiska hot, alltså fientliga hot som krig eller cyberattacker och kollaps av nationella bank- och betalsystem toppar medborgarnas riskuppfattningar. Medborgarna har också en hög tillit till den egna förmågan att hantera en cyberkris om den skulle hända idag. Majoriteten är också beredda att vidta åtgärder för att förbereda sig inför cyberrisker. Det finns tre olika typer av åtgärder som medborgarna är beredda att vidta för att skydda sig från en cyberkris. Den första handlar om att förbereda sig praktiskt, exempelvis genom att ha extra kontanter hemma. Den andra åtgärden handlar om att vara medveten och smart i sin vardag, genom att exempelvis ha flera bankkort från olika banker, gärna med kredit. Den tredje typen av åtgärd handlar om relationer. Att ha ett nätverk av människor som man litar på, som man kan samarbeta och byta varor och tjänster med i en kris.

Vad man är beredd att göra handlar ofta om vilka resurser man har. Individer med hög utbildning är mer benägna att vidta medvetna, planerade åtgärder. De som känner stark tillit till andra – till exempel i sitt grannskap – är i högre grad beredda att satsa på relationer som en del av sin beredskap. Det här visar att det inte räcker att bara ha resurser, som utbildning eller pengar – det måste också finnas möjligheter att använda dem i praktiken. Beredskap handlar alltså inte bara om vad man har, utan också om vilka villkor man lever under. För att stärka beredskapen i samhället är det därför viktigt att kommunicera på ett sätt som främjar engagemang, samarbete och lokalt nätverkande. När medborgarna får stöd att använda sina resurser – oavsett om det handlar om kunskap, pengar eller kontakter – ökar chanserna att de faktiskt vidtar åtgärder inför en cyberkris.

En viktig anledning till att medborgarna inte är motiverade att förbereda sig inför en cyberkris är att de helt enkelt saknar eller har få möjligheter – de har för lite pengar eller andra resurser för att kunna agera. En annan anledning är att de accepterar risken – för att de har en hög tillit till sin egen förmåga att hantera krisen om den skulle inträffa, eller helt enkelt inte uppfattar risken som särskilt hög. Det innebär att det finns stöd för den så kallade riskperceptionsparadoxen. Förklaringen till att människor trots att de har en hög riskuppfattning inte förbereder sig för en kris, är för att de saknar resurser eller för att de accepterar risken. Inte bara när det gäller olika naturliga kriser, utan också för sociala eller antagonistiska och avsiktliga kriser som en cyberkris. Däremot är stödet svagt för förklaringen att människor låter bli att förbereda sig för att de anser att det är någon annans ansvar.

En viktig slutsats är att de flesta medborgare är villiga att vidta åtgärder för att skydda sig från cyberrisker. Vad man som myndighet och kommun kan tänka på för att hjälpa medborgarna att förbereda sig för eller hantera samhälleliga cyberkriser, är att:

- Använda riskkommunikationsmodeller som fångar medborgarnas uppmärksamhet och som gör budskapet relevant. Detta genom innehåll av budskapsåtgärder som stärker medborgarnas tillit till sin egen förmåga att hantera cyberkrisen om den skulle inträffa.
- Det kan behövas särskilda insatser för att stötta socialt och ekonomisk svagare grupper i samhället inför och i samband med samhälleliga cyberkriser.
- Olika kommunikationsinsatser kan behövas för att motivera olika grupper att förbereda sig inför en samhällelig cyberkris.
- För att optimalt använda medborgarnas samlade resurser inför eller i samband med samhälleliga cyberkriser, att främja kommunikationsinsatser som betonar engagemang, tillit och samarbete i närområdet.

Inledning

Cyberrisker och samhälleliga cyberkriser

Cyberrisker är ett växande hot mot både organisationer och mot samhället (Zhang and Borden, 2020). Hoten omfattar allt från bristande säkerhet i informationssystem, till medvetna angrepp av olika slag. Det kan handla om dataintrång där känsliga data kan hamna i orätta händer, eller riktade attacker där angriparna kräver en lösensumma för att hindra spridningen av den skadliga kod de släppt lös i informationssystemen. Cyberrisker kan också vara riktade mot enskilda individer (Amin, 2019). Exempel på en sådan cyberrisk är så kallat nätfiske, där individer luras att lämna ut personlig information genom att klicka på länkar i e-postmeddelanden. En av de mer omfattande och tvärvetenskapliga definitionerna av cyberrisker är att:

> ”Cyberrisker är ett resultat av användningen av informations- och kommunikationsteknik (IKT), som hotar konfidentialitet, tillgänglighet eller integritet för digitala data och tjänster, och leder till affärsavbrott, infrastrukturfel eller andra materiella skador.” (Eling och Schnell, 2016:12).

De konsekvenser av cyberrisker som är i fokus för denna rapport är de samhälleliga. Medvetna angrepp som olika former av cyberattacker som slår ut infrastrukturer har under de senaste åren också rankats som några av de främsta globala riskerna (WEF, 2019; WEF, 2025a). Detta eftersom cyberrisker är snabba och skalbara, och en cyberattack har potential att snabbt få mycket stor spridning (Elestedt, Nilsson och Rosenvinge, 2021).

Att de ekonomiska konsekvenserna av en cyberattack är stora kan illustreras av lösensumma-attacken med spridningen av viruset WannaCry 2017, där över 230,000 datorer i 150 länder orsakade ekonomiska förluster till ett värde av 8 miljarder dollar (Wirth, 2017). Det motsvarar utgifterna för rättsväsendet i Sverige för ett helt år. Om man beaktar de infrastrukturella konsekvenserna för samhället menar Försvarsmakten att en cyberattack är lika skadlig som ett väpnat angrepp (Karlsson, 2022). Utan till exempel Bank-ID och Swish som används av i stort sett alla folkbokförda svenskar för att göra att bankärenden eller betala med, stannar Sverige (Cervenka, 2025). Också när påverkan av en cyberattack är begränsad kan attackens konsekvenser få negativa följdeffekter som bristande förtroende för det finansiella systemet eller för de aktörer som ska hantera krisen (Elestedt, m.fl, 2021). Även begränsade cyberattacker mot en organisation eller en kommun kan leda till stora störningar i samhällsservicen (Lindström, 2024). Ett exempel är överbelastningsattacken mot Sveriges Television i juni 2025. Här sattes nyheter i allmänhetens tjänst ur spel. Detta eftersom angripare genom att sända in en stor mängd data till SVT, täppte igen informationskanalerna som hindrade dem från att sända nyheter. Vid attacken mot

exempelvis Kumla kommun 2024 krävde angriparna en lösensumma för att inte läcka känslig information (Lindström, 2024). Det tog till exempel Kalix kommun ett halvår att återhämta sig fullständigt efter en motsvarande attack 2021. Attacken ledde till stora störningar i kommunens samhällsservice och svårigheter för kommuninvånarna att införskaffa livsnödvändiga förnödenheter som livsmedel, drivmedel och medicin.

Källorna till cyberrisker som beskrivits ovan kan vara antagonistiska, men de kan också uppkomma till följd av slump, mänskliga misstag eller bristande säkerhetsarbete (Strupczewski, 2021). Cyberrisker kan också bero på naturolyckor som exempelvis översvämningar som slår ut elen (ibid). Men det är de antagonistiska cyberriskerna som cyberattacker och databedrägerier eller desinformation som ligger bakom de höga riskuppfattningarna (WEF, 2025b). Det är också cyberrisker i betydelsen medvetna angrepp som är i fokus för denna rapport. Angreppen som avses är på samhällsnivå. Hot mot enskilda individer i form av identitetsangrepp eller nätfiske berörs inte i denna rapport.

Frågor om cybersäkerhet står också högt på allmänhetens agenda (Amin, 2019). Det kan dock vara svårt att förstå vad en cyberrisk innebär utan särskilda teknikkunskaper. Eller för den delen att som kommunikatör visualisera en cyberrisk. När cyberrisker ska illustreras används ofta digitala siffror på en datorskärm. Eller så ser man ryggtavlan på en yngling med huvtröja dold i ett mörkt rum sittande vid sin dator. Cyberrisker är alltså för den enskilda individen inte helt enkla att begripa. Men inte heller som praktiker är de enkla att kommunicera. Dels för att kommunikatörerna är i händerna på IT-experterna, dels för att cyberrisker inte är enkla att visualisera. Cyberrisker medför alltså stora utmaningar för både medborgarna och för kommunikatörer.

Men vad vet vi om i vilken utsträckning invånarna är förberedda för en samhällelig cyberkris? Det finns studier som värderat och undersökt hur man hanterar cybersäkerhetsrisker (Busby, Green, och Hutchison 2017; He, Devine, och Zhuang 2018) och hur cyberrisker kommuniceras via medierna (Xu, Murphy, Xu m.fl., 2021). Men forskningen om hur vi bäst kommunicerar cyberrisker för att höja medvetenheten och få invånarna att förbereda sig är fortfarande i sin linda (Zhang och Borden, 2020; Sandstig och Eriksson, 2024).

Detta är en anledning till att projektet *Risk- och beredskapskommunikation för ett robust digitalurbant samhälle, Digital Urban Risk Communication* (DURCOM) med hjälp av ett experiment prövade effekterna av olika former av ansvarsbudskap på medborgarnas föreställningar om deras eget ansvar och deras intention att förbereda sig utifrån ett krisscenario som skildrade en cyberattack mot en kommun samtidigt som det skett attacker mot nationella bank- och betalsystem som ligger nere (Sandstig och Eriksson, 2024).

Scenariot var inspirerat av händelserna i Kalix vintern 2021 samt MSB-projektet *Om betalsystemet kraschar*.

> Föreställ dig att din kommun och nationella bank- och betaltjänster till följd av IT-attacker drabbats av en kollaps. Det leder till stora störningar i kommunens samhällsservice samt svårigheter att införskaffa livsnödvändiga förnödenheter som livsmedel, drivmedel och medicin. Det är oklart när saker kan börja fungera igen, men bedömningen är att det kan dröja flera veckor eller månader. Du vänder dig till de nyhetskällor du litar på för att få mer information om läget.

Resultatet visar att budskapen där myndigheterna tar nästan allt ansvar, inte leder till att medborgarna minskar sin egen ansvarsmedvetenhet. Ansvarsbudskap där ansvaret är delat mellan myndigheterna och den enskilda individen, var det som ökade medborgarna ansvarsmedvetenhet. Men det gjorde också ansvarsbudskap där myndigheterna frånsade sig allt ansvar, där medborgaren lämnades åt sitt eget öda att lösa situationen, och inte hade något annat val. Inga av ansvarsbudskapen ledde till en ökad intention att förbereda sig för en cyberkris (ibid).

I denna rapport presenteras en vidarebearbetning av resultat från DURCOM. Resultaten rör medborgarnas föreställningar om cyberrisker i jämförelse med andra risker, vilka åtgärder medborgarna är motiverade att vidta i händelse av en cyberkris samt nycklar till varför medborgarna är eller inte är motiverade att vidta åtgärder för att skydda sig. Resultaten baseras på kontrollgruppens svar (n=879), alltså de medborgare som *inte* tog del av budskapen i experimentstudien, genomförd inom ramen för Medborgarpanelen 2022.

Bakgrund

I denna bakgrund beskrivs inledningsvis skälen till att risker kommuniceras, vad som är utmärkande för riskkommunikationens karaktär inom samhällsvetenskapen, samt de utmaningar som särskilt gäller cyberrisker. Detta för att öka förståelsen för vad som är möjligt att åstadkomma med riskkommunikation och vilka begränsningar som finns. För att i slutet av rapporten kunna resonera kring rekommendationer beskrivs därför också några av de instruktiva budskapsmodeller som används för att motivera medborgarna att vidta åtgärder för att skydda sig vid en samhällskris. Den teori och tidigare forskning som används för att analysera resultaten beskrivs i direkt anslutning till resultat och analyskapitlen *Riskuppfattningar*, *Kapabilitet och beredskap* samt *Riskperceptionsparadoxen*. Bakgrunden avslutas med det forskningen och Myndigheten för samhällsskydd och beredskap (MSB) visat att individen kan göra själv.

Riskkommunikation

Skälen till att kommunicera risker kan vara flera. Ett vanligt skäl är för att informera eller utbilda (Fischhoff, 1995). Detta för att fylla ett förmodat kunskapsgap hos medborgarna (ibid). När det gäller cyberrisker, kan riskkommunikation användas för att höja medborgarnas riskmedvetenhet. Detta är fördelaktigt i händelse av en kris, eftersom en hög riskmedvetenhet hos medborgarna underlättar kommunikationen av rekommendationer till medborgarna i ett krisläge (Backman, 2021). Andra skäl för att kommunicera risker är för att uppmuntra medborgarna att förbereda sig och vidta skyddsvärda handlingar inför en förmodad kris (Covello, von Winterfeld, och Slovic, 1986). Detta genom att ändra, förstärka eller avråda från ett visst beteende (ibid). Det är också just att uppmuntra till handling, eller att motivera medborgarna att vidta skyddsvärda handlingar, som i huvudsak skiljer riskkommunikationen från kriskommunikationen (Sjöberg, Moen och Rundmo, 2004). Detta helt enkelt eftersom vid en kris har risken redan inträffat och är uppenbar. Genom ”*Hesa Fredrik”* och *Viktigt meddelande till allmänheten* (VMA) använder vi också riskkommunikation för att varna och sprida nödinformation (Covello, m.fl, 1986). Avslutningsvis använder vi riskkommunikation för att bjuda in medborgarna till att vara med och lösa gemensamma problem och konflikter (ibid). Det kan handla om miljöfrågor, som var kärnkraftsavfall ska förvaras. Eller så kan det handla om hälsofrågor, som hälsoguider som många kommuner använde under covid-19 för att öka vaccinationsviljan i utsatta områden. Det kan också användas i frågor om säkerhet där trygghetsvandringar används som metod. Riskkommunikation skiljer sig alltså från kriskommunikation främst genom att den behöver jobba lite extra på att motivera medborgarna att vidta förebyggande åtgärder. Detta

eftersom hotet ännu inte aktualiserats, och därför inte med självklarhet uppfattas som relevant. Men i likhet med kriskommunikation kan riskkommunikation också förekomma under en pågående kris. Exempelvis i form av riskkommunikation för att få medborgarna att vaccinera sig under pågående covid-19 pandemi. Riskkommunikation har sedan forskningen om den inleddes definierats som:

> ”En interaktiv process av utbyten av information och åsikter mellan individer, grupper och institutioner, som omfattar flera olika budskap om riskens karaktär och andra meddelanden, inte enbart om risk, som uttrycker omtanke, åsikter eller reaktioner på riskmeddelanden eller riktat mot juridiska och institutionella omständigheter i riskhanteringen” (NRC, 1989).

Att beakta i kommunikationen av cyberrisker är att både kommuners och individers beroende av digitala tjänster (Backman, 2021; Chodakowska, KaŃdula och Przybylska, 2022) och kommunikationen med medborgarna har ökat (Hatcher, Meares och Heslen, 2020). Generellt finns det här också en utmaning i det inbyggda spänningsfältet mellan den upplyste och engagerade medborgarens ökade krav på myndigheternas öppenhet och transparens i en demokrati som ett led i ansvarsutkrävande, och myndigheternas krav på att skydda känslig information (Macmanus, Caruson och McPhee, 2012). Det finns också stora skillnader mellan kommuner till följd av kunskapsgapet mellan IT-experter och generalister (Caruson m.fl., 2012). Det finns med andra ord inbyggda utmaningar i att kommunicera cyberrisker till medborgarna att ta särskild hänsyn till som skiljer sig från att kommunicera andra risker (se Sandstig, Boholm och Berlin, kommande).

Krisberedskap och medborgarens egna ansvar

Vad medborgarna kan göra för att ta ansvar för sin egen säkerhet är på agendan (Sandstig, 2019). Beredskapspolitiken har i flera länder under det senaste decenniet, av ekonomiska skäl förändrats (RFR 2015/16 RFR3). Detta eftersom resurserna inte räcker för att hjälpa alla. Om de som kan klara sig själv en tid i krisens början, räcker resurserna till dem som är mest i nöd (ibid). Beredskapspolitiken har präglats av en ökad ansvarsförskjutning – från staten till de regionala och lokala samhällsnivåerna, och slutligen till hushållen och individerna (SFS 2015:1052).

Vi vet en hel del om hur man effektivt förmedlar ett riskbudskap för att motivera medborgarna att förbereda sig för olika kriser. Det finns flera olika modeller, och de har alla sina styrkor och svagheter. Extended Parallell Process Model (EPPM) av Witte (1992) har fokus på själva utformandet av budskapen för att åstadkomma den önskade påverkan. Den liksom sin föregångare Protection Motivation Theory (PTM) av Rogers (1983) bygger på att i

budskapet betona att sannolikheten för att risken inträffar är hög och/eller genom att betona att konsekvenserna om risken inträffar är hög, inducera oro och/eller rädsla för att mottagarna därigenom ska uppmärksamma budskapet och anse att det är tillräckligt relevant att vidta åtgärder för att undvika negativa konsekvenser och skydda sig. Eftersom användningen av skrämseltaktik kan urholka förtroendet för avsändaren betonar vidareutvecklingen av EPPM att det efter att man fångat mottagarens uppmärksamhet är mycket viktigt att också lugna eller trygga mottagaren efter att budskapet gått fram (Witte and Allen, 2000). Det görs genom att visa på vilka handlingar som bör vidtas för att undvika att drabbas av risken och att åtgärderna är effektiva (’response-efficacy’) samt att stärka mottagaren i att denne kan klara av att hantera risken (’self-efficacy’) (Ruiter, Kessels, Peters, m.fl., 2014). EPPM har också använts för att förmedla budskap om cybersäkerhetsrisker (Zhang and Borden, 2020). IDEA, Internalization, Distribution, Explanation and Action av Sellnow och Sellnow (2017; 2019) är en modell som har fokus på det kunskapsmässiga, känslomässiga och beteendemässiga lärandet som sker i kommunikationen. Detta genom att effektivisera utformningen av budskapen så att mottagarna förstår och följer instruktioner i budskapet. Gemensamt för EPPM och IDEA är att de förutom att välja de mest lämpade kanalerna, pålitliga avsändare och medel för att göra meddelandena relevanta, är det genom att betona tilliten till den egna förmågan och övertyga om vilka handlingar man behöver vidta för att kunna avvärja risken, krisen eller att förbereda sig (Johanson and Sandstig, 2024).

Vad individen kan göra själv

Varje vecka görs transaktioner till ett värde av 20 miljarder kronor med elektroniska och digitala betalningsmetoder. Men om alla digitala betalningar i Sverige slås ut av en hackerattack återstår kontanter som enda betalmedel. Enligt Riksbankens finns ett stort kontantlager som kan användas i en sådan krissituation, och det är snarare distributionen som kan bli ett problem. Medborgaren kan förbereda sig för cyberkriser genom att ha 2 000 kronor i olika valörer tillgängliga hemma (MSB, 2018), och rekommendationerna har i den senaste broschyren *Om kriget eller krisen kommer*, uppdaterats med att också ha andra betallösningar som flera olika bankkort och digitala tjänster (MSB, 2024). I den senaste broschyren finns också rekommendationer för att skydda sin egen digitala säkerhet. MSB rekommenderar här medborgarna att skapa långa lösenord, inte klicka på länkar i mejl eller öppna bilagor från okända avsändare, installera säkerhetsuppdateringar direkt och säkerhetskopiera viktiga data till molntjänster (ibid). Men vi tänker och agerar olika beroende på vilken typ av risk det handlar om, och cyberkriser kan också ha så kallade kaskadeffekter, där även el, värme och vattenförsörjning slås ut som kräver andra

förberedelser. Cyberriskernas kaskadeffekter och de åtgärder medborgarna är motiverade att vidta, är något som undersöks vidare under stycket resultat och analyskapitlet *Kapabilitet och beredskap*.

Men det finns också, som nämndes i stycket om riskkommunikation, särskilda utmaningar med att kommunicera just cyberrisker till medborgarna. Detta eftersom medborgarna, organisationer och myndigheter på flera sätt är beroende av digitala lösningar, och därför också är mer sårbara. Den fria tillgången till information och pressfrihet som är grundbulten i västerländska demokratier, har lyfts fram som relevant för kommunikationen av risker och i tider av kris (Sellnow, Ulmer, Seeger och Littlefield, 2009; Sellnow och Seeger, 2016). Kommunikationen bygger på etiska ställningstaganden kring hur allmänheten ska kunna göra informerade val (Sellnow och Seeger, 2016). Detta eftersom valet kan påverka individens framtid och i en förlängning individens möjligheter att minska risker eller krisers negativa konsekvenser för individen (ibid). Det finns här en inbyggd motsättning mellan myndigheternas krav på öppenhet och transparens och organisationers och myndigheters krav på säkerhet och att skydda integritets- eller försvarskänsliga data.

Att beakta medborgarna i arbetet med cyberrisker och samhälleliga cyberkriser är här viktigt. Detta för att kommunen har ett särskilt ansvar att kommunicera risker till relevanta intressenter, där medborgarna är en del (Rabe, Sataøen, Lindskog och Eriksson, 2024). Men också för att medborgarna behöver ha tillgång till tillförlitlig och relevant information. Allt för att de ska kunna bedöma riskerna som kan drabba dem, minska deras sårbarhet och öka deras beredskap inför ett framtida hot.

Disposition av resultat och analys

Nedan presenteras en vidarebearbetning av andra data från DURCOM-projektet än de som publicerats från budskapsexperimentet vid en samhällelig cyberkris (Sandstig och Eriksson, 2024). I kapitlet riskuppfattningar, presenteras och analyseras medborgarnas riskuppfattningar om cyberrisker i relation till andra hot och risker, och avslutas med några olika karaktärsdrag som utmärker dem med låga respektive höga riskuppfattningar om cyberrisker. Därefter följer ett kapitel om kapabilitet och beredskap, där medborgarnas tillit till sin egen förmåga att hantera en cyberkris presenteras och analyseras. Här presenteras och analyseras även medborgarnas motivation, och åtgärder de är beredda att vidta inför cyberrisker. Presentationen och analysen av resultaten avslutas med kapitlet om riskperceptionsparadoxen, dvs svaren på varför inte medborgarna förbereder sig för en cyberkris fastän de har höga riskuppfattningar.

Rapporten avslutas med ett kapitel om praktiska implikationer, och vad man som myndighet och kommun kan tänka på för att hjälpa medborgarna att förbereda sig för eller hantera samhälleliga cyberkriser.

Riskuppfattningar

För att förstå vad en cyberrisk är och bedöma om risken är hög eller låg behöver den jämföras med andra risker. De som arbetar med att bedöma risker gör riskanalyser. Inte sällan skiljer sig expertens och lekmannens bedömningar åt. Det finns en grupp av forskare som intresserat sig mer för att överbrygga kunskapsgapet mellan expertens bedömning och lekmannens. Medan det finns andra som mer intresserat sig för att förklara hur det kommer sig att vi har de uppfattningar om risker som vi har. Till exempel att vi bedömer nya risker som högre än de vi känner till. Sedan finns det ytterligare en grupp forskare som intresserat sig för hur vi genom att kommunicera risker kan få människor att förbereda sig.

Studier av riskkommunikation är alltså nära förknippat med studier av riskuppfattningar. Det kan handla om vad experter och individer har för uppfattning om olika typer av risker, allt från miljökatastrofer till vardagliga säkerhetsrisker som trafikolyckor. I denna studie är det individens riskuppfattning som är relevant eftersom riskuppfattningen spelar en stor roll för att motivera individer till att undvika, mildra eller anpassa sig till risker (Sjöberg, Moen och Rundmo, 2004). Det finns i huvudsakliga två inriktningar, som kan bidra med att förklara hur individer förbereder sig för en kris: den kunskapsorienterade och den mer socialt kunskapsorienterade. Kunskapsorienterade modeller har fokus på individens upplevelse av kontroll över risken, sannolikheten för att risken ska inträffa, katastrofens konsekvenser, graden av frivillighet och typen av hot eller risk som ska bedömas (Fischhoff, Slovic, Lichtenstein, Read och Combs, 1978). Senare varianter tar även hänsyn till känslor (Slovic, 1987) av oro och rädsla (Lowenstein, Weber, Hsee och Welch, 2001). Förutom ovanstående har användandet av skrämsel i riskkommunikation varit särskilt vanligt och framgångsrikt för att kommunicera hälsorisker och få individer att uppmärksamma budskapet (se Kasperson, 2014).

De med socialt kunskapsorienterade modellerna tar även hänsyn till sociala faktorer, men menar dessutom att riskuppfattningarna föregår beteendet (Lindell och Perry, 2004; Rogers, 1983). Inom forskningen söker man förklara hur individens benägenhet att vidta skyddsvärda handlingar påverkas av riskuppfattning, tidigare erfarenheter av kriser, beslut rörande hur hotet ska avvärjas, tilliten till den egna förmågan att avvärja hotet och tilliten till hur effektiv den skyddsvärda handlingen är. Sambandet mellan riskuppfattning och benägenhet att vidta

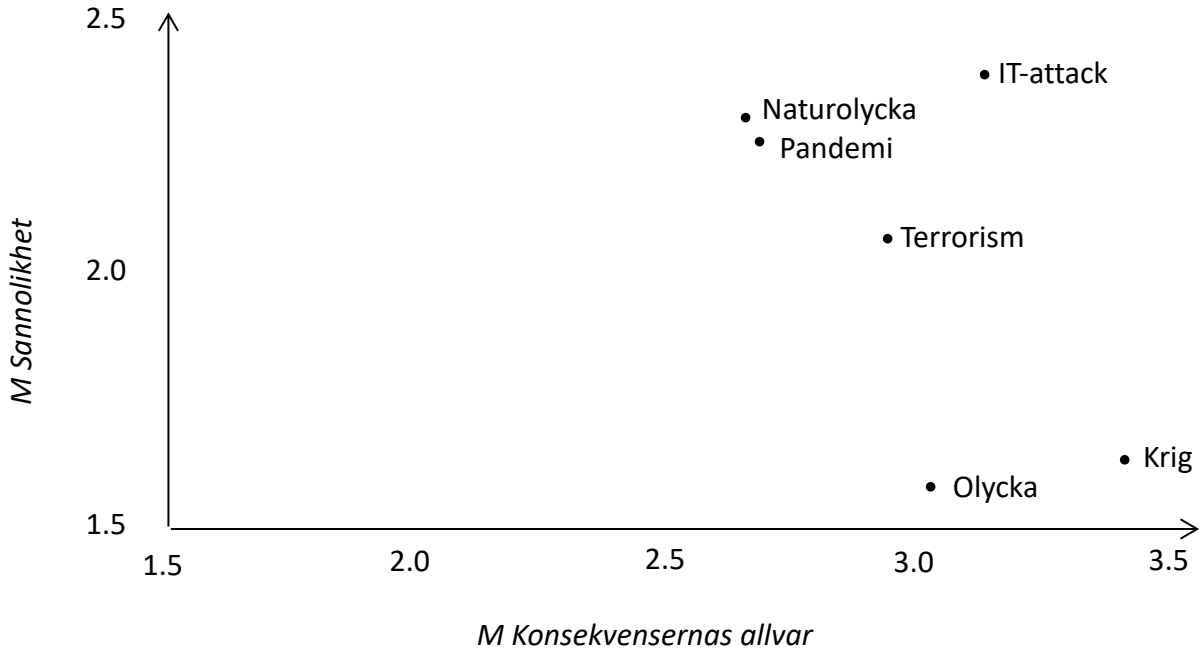
åtgärder inte är helt klarlagt. Men det finns flera studier som visat att individer med låg riskuppfattning är mindre benägna att vidta beredskapsåtgärder än individer med hög.

Det sociala perspektivet på risk, som vi använder oss av i denna studie, innefattar också det psykologiska perspektivet på risk i betydelsen av att det täcker upp för såväl reella som konstruerade risker och såväl uppfattade som upplevda risker. Det sociala perspektivet på risk bygger på en föreställning att människor ser på världen genom en uppsättning socialt och kulturellt filtrerade betydelser eller mening förmedlat genom familj, vänner, medierna med flera (Renn, 1992). Varför behöver vi då det sociala perspektivet på risk? Det tekniska perspektivet som tillämpas i arbetet med informationssäkerhetsrisker handlar mycket om att minimera risker. Det är givetvis centralt, men riskhantering handlar om så mycket mer. Det sociala perspektivet kan här användas för att föra in värderande så kallade normativa aspekter i policyhantering. Detta genom att till exempel: få med medborgarnas ståndpunkter som associeras med risken, främja rättvisa och institutionellt förtroende i reducerandet av ojämlikhet och sårbarheter, bredda så att fler intressenter kan delta i beslutsfattandet samt genom att identifiera medborgarnas oro. Risk som en del i en social process tar alltså hänsyn till att individens riskuppfattning färgas av nyhetsmedierna, vänner och bekanta, det demokratiska samhällets värderingar med mera. Oavsett perspektivet på risk, är den minsta gemensamma nämnaren när riskuppfattningar mäts, att sannolikheten för att risken ska inträffa samt graden av allvarligheten av dess konsekvenser skattas (Sandstig, 2010).

Antagonistiska hot toppar bland riskerna

Hur stora uppfattas då riskerna med cyberkriser vara? Detta jämfört med andra typer av risker – ur medborgarens perspektiv? Ett vanligt sätt att bedöma risker är att fråga hur sannolikt det är att något händer, och hur allvarliga konsekvenser det i så fall skulle få. I studien undersöktes därför hur respondenterna uppfattade sannolikheten och konsekvenserna av olika risk- och krisscenarier på lokal nivå, det vill säga i deras hemkommun.

Figur 1 Riskuppfattningar av sex olika hot eller risker som skulle kunna förekomma i medborgarnas kommun inom de närmaste 12 månaderna (medelvärde mellan 1-4)



Kommentar: För frågornas formulering, svarsalternativ, utfall, N-värden se bilaga 2 tabell B1. *Källa*: Medborgarpanelen 2022.

Bland de sex olika typer av hot och risker som mättes skattas sannolikheten att en cyberattack och kollaps av nationella bank- och betaltjänster skulle kunna inträffa inom de närmaste 12 månaderna högst (*M*=2,49). Det är högre än skattningen av sannolikheten för en naturolycka (skogsbrand, kraftig storm, orkan eller översvämning) (*M*=2,28), ytterligare en pandemi eller epidemi (*M*=2,28) (svaren är insamlade 25/5–15/6 2022 i samband med att covid-19 pandemin börjat klinga av), terrordåd eller annat organiserat våld (*M*=2,19), krig eller en motsvarande militär konflikt (*M*=1,60) (Ryssland gick in i Ukraina 24 feb 2022) eller

en större olycka med utsläpp av gifter eller radioaktivitet (*M*=1,58) (se figur 1, se bilaga 2 tabell B1ff).

Även när det gäller bedömningen av konsekvensernas allvar, skattas en cyberattack högt (*M*=3,11). Bara skattningen av krig eller motsvarande militär konflikt skattas högre (*M*=3,43). Men också de andra hoten och riskerna vi efterfrågat som en större olycka med gift eller radioaktivitet (*M*=2,97), terrordåd (*M*=2,93), pandemi (*M*=2,68) eller en naturolycka (*M*=2,60) skattas ganska högt.

Om vi tar hänsyn till både bedömningen av riskens sannolikhet och konsekvens, framgår att de antagonistiska hoten eller riskerna, krig (*M*=3,46) och cyberattacker (*M*=3,19), toppar medborgarnas riskuppfattningar. Att bedömningen av såväl sannolikheten som konsekvensernas allvar när det gäller en cyberattack och kollaps av nationella bank- och betaltjänster skattas högst eller näst högst går att tolka som att risken är angelägen för medborgarna.

Kön och ålder formar riskuppfattning

Lennart Sjöberg (2004) utvecklade den så kallade psykometriska modellen dels för att kunna mäta för att kunna jämföra riskuppfattningar, dels för att kunna förklara och förstå vad som kan ligga bakom att individer har olika riskuppfattningar. Forskningen har visat stora skillnader mellan riskuppfattningen för den egna personens del och för andras. Kvinnor och män bedömer risker olika och det finns även samband mellan vissa personlighetsdrag och riskuppfattningar. I stycket som följer fördjupas analysen av riskuppfattningarna, främst med syfte att undersöka hur inflytelserika faktorer som är kända sedan tidigare påverkar. Det handlar i stort om bakrundsindikatorer som kön, ålder, utbildning, inkomst samt förtroendet för institutioner och mellanmänsklig tillit.

Med hjälp av en så kallad regressionsanalys, går det att fastställa den självständiga effekten av de sedan tidigare välkända faktorerna på riskuppfattningarna. Av förklaringsfaktorerna har alla utom utbildningsnivå signifikanta självständiga effekter på riskuppfattningarna (se bilaga 2 tabell B2ff). Nedan beskrivs de huvudsakliga och mest intressanta sambanden. Kön har, med undantag för riskuppfattningen av krig (där ålder har den största självständiga effekten), den största självständiga effekten oavsett risk ($b_{\text{cyberattacker}}$= -,20***, $b_{\text{större olycka}}$= -,21***, $b_{\text{terrordåd}}$= ,15***, $b_{\text{skogsbrand}}$= -,22*** och b_{pandemi}= -,17***). Att kvinnor har en högre riskuppfattning än män när det gäller cyberattacker, större olycka, skogsbrand och en pandemi, förklarar då från närmare en femtedel upp till närmare en fjärdedel av

riskuppfattningen. Att män har en högre riskuppfattning är kvinnor för terrordåd förklarar en sjättedel av riskuppfattningen. Även den självständiga effekten av ålder är stor. Ju yngre personen är, desto högre är riskuppfattningen för krig (b_{krig}= -,18***), cyberattacker ($b_{cyberattacker}$= -,07*), större olycka ($b_{större\ olycka}$= -,11**), skogsbrand eller motsvarande ($b_{skogsbrand}$= -,07*). Inkomst har också en självständig effekt på riskuppfattningen av krig (b_{krig}= ,08*). Ju högre inkomst desto högre riskuppfattning för krig.

Tabell 1 Karakteristika idealtyper som förklarar olika riskuppfattningar

	Riskuppfattning	
Hot eller risk	Låg	Hög
Krig eller en motsvarande…	Äldre man med låg inkomst.	Ung kvinna med hög inkomst.
Cyberattack och kollaps…	Äldre man.	Ung kvinna.
Större olycka med utsläpp…	Äldre man med låg mellanmänsklig tillit i allmänhet men hög tillit till människorna i området där man bor.	Ung kvinna med hög mellanmänsklig tillit i allmänhet men låg tillit till människorna i området där man bor.
Terrordåd eller annat…	Kvinnor med högt förtroende för regeringen.	Män med lågt förtroende för regeringen.
Skogsbrand, kraftig storm…	Äldre man.	Ung kvinna.
Ytterligare en pandemi…	Man med högt förtroende för kommunen och hög tillit till människorna i området där man bor.	Kvinna med lågt förtroende för kommunen och låg tillit till människor i området där man bor.

Baserat på regressionsanalysen (se bilaga 2 tabell B2ff) kan vi nu också teckna de idealtyper som har en hög eller låg riskuppfattning för olika risker. En medborgare med en hög riskuppfattning kan för alla de riskerna vi efterfrågar, med undantag för terrordåd, sannolikt beskrivas som en kvinna (tabell 1ff). Detta medan en medborgare med en låg riskuppfattning sannolikt kan beskrivas som en man. Även medborgarens ålder är utmärkande, och för några av riskerna också personens inkomstnivå, tillit till andra och förtroende för kommunen eller regeringen. En medborgare med en hög riskuppfattning för krig eller motsvarande militär konflikt kan troligtvis beskrivas som en ung kvinna med hög inkomst. Medan en medborgare med låg riskuppfattning för motsvarande risk kan beskrivas som en äldre man med låg inkomst. En medborgare med en hög riskuppfattning för en cyberattack men också för naturolyckor som skogsbrand, kraftig storm och liknande kan sannolikt beskrivas som en ung kvinna. Detta medan en medborgare med en låg riskuppfattning kan beskrivas som en äldre

man. En medborgare med en hög riskuppfattning för en större olycka eller motsvarande kan sannolikt beskrivas som en ung kvinna med en hög mellanmänsklig tillit i allmänhet, men med en låg tillit till människor i området där man bor. Detta i motsats till en medborgare med en låg riskuppfattning av en större olycka eller motsvarande, som kan beskrivas som en äldre man med låg mellanmänsklig tillit i allmänhet, men med en hög tillit till människorna i området där man bor. En medborgare med en hög riskuppfattning för terrordåd kan sannolikt beskrivas som en man med lågt förtroende för regeringen. Medan en medborgare med en låg riskuppfattning kan beskrivas som en kvinna med högt förtroende för regeringen. En medborgare med en hög riskuppfattning för ytterligare en pandemi eller en epidemi kan troligtvis beskrivas som en kvinna med låg tillit till människor i området där hon bor och med ett lågt förtroende för kommunen hon bor i. Detta medan en medborgare med låg riskuppfattning för motsvarande risk kan beskrivas som en man med högt förtroende för människorna i området där han bor och med ett högt förtroende för kommunen han bor i.

En viktig slutsats är att kön (med undantag för krig eller motsvarande militär konflikt där ålder förklarar mest), och i viss mån ålder är den enskilt starkaste förklaringsfaktorn för de flesta av de risker vi efterfrågat (se bilaga 2 tabell B2). Vi vet sedan tidigare att det är enklare att nå dem med en hög riskuppfattning med information om rekommenderat skyddsvärt beteende innan eller under en kris. Vi vet också att en hög riskuppfattning oftast hänger ihop med en hög oro (se Sandstig, 2010). Något som i sin tur leder till att medborgarna själv söker information om riskerna. Resultaten aktualiserar frågor om det krävs särskilt riktade kommunikationsinsatser inriktade på att höja mäns (oftast äldre mäns) medvetenhet om dessa risker, där cyberrisker är en sådan risk, för att lyckas med den riktade risk- och kriskommunikationen inför eller vid samhällskriser.

Kapabilitet och beredskap

Kapabilitet är den förmåga som motsvarar individens verkliga möjligheter att utföra handlingar de själv vill och önskar göra, som de uppfattar som värde- eller meningsfulla (Sen, 1993). I en krissituation kan det handla om förmågor som överlevnadsförmåga, demokratisk förmåga, ansvarsfördelning liksom social förmåga att avläsa beteende via vänner och via nyhetsmedier (Johansson m.fl., 2023). Men det räcker inte med att ha resurser eller vissa förmågor utan man behöver också befinna sig i ett sammanhang där dessa förmågor kan realiseras (Nussbaum, 2011).

Även tilliten till den egna förmågan att kunna skydda sig själv och andra i händelse av en risk eller en kris (’self-efficacy’), har visat sig spelar en stor roll för hur man handlar i en

krissituation (Frisby, Sellnow, Lane m.fl, 2013). Inom forskningen om risk- och kriskommunikation försöker man därför i själva budskapen skruva på olika parametrar som riskens aktualitet och konsekvensernas allvar samt visa på handlingar som framgångsrikt avvärjer hot, för att öka individens tillit till sin egen förmåga samt tillit till att åtgärderna är effektiva (’response efficacy’). Detta för att tilliten till den egna förmågan, också har visat sig spela en avgörande roll för i vilken utsträckning man förbereder sin inför en kris (se exempelvis under covid-19 pandemin, Sandstig och Dahlin Ivanoff, 2021).

Stark tillit till den egna förmågan

Majoriteten, närmare två tredjedelar av medborgarna, 65 procent har en ganska eller mycket hög tillit till sin egen förmåga att hantera situationen i scenariot om det skulle hända idag (tabell 2ff). Detta medan motsvarande andel som svarat ganska eller mycket låg tillit var 35 procent (*M*=2,67).

Tabell 2 Tillit till den egna förmågan att hantera en cyberkris om den hände idag (procent)

Ingen tillit alls	6
Ganska låg tillit	32
Ganska hög tillit	54
Mycket hög tillit	8
Total procent	100
Totalt antal	872

Kommentar: Frågans formulering: *Om du utgår från IT attackerna i scenariot, vilken tillit har du till din egen förmåga att kunna klara dig utan allvarliga skador?* Svarsalternativen var i fallande ordning: ”Ingen tillit alls”, ”Ganska låg tillit”, Ganska hög tillit”, ”Mycket hög tillit”. N=872. *Källa*: Medborgarpanelen 2022.

Att närmare två tredjedelar har en ganska eller mycket hög tillit till sin egen förmåga att hantera situationen i scenariot, är högt. Detta om vi jämför med resultaten på motsvarande fråga som ställdes till allmänheten i den nationella SOM-undersökningen i det initiala skedet av covid-19 pandemin 2020. Där hade närmare hälften av respondenterna en ganska eller mycket hög tillit till den egna förmågan (Sandstig och Dahlin Ivanoff, 2021). Det är dock tal om två olika risker, som inte med självklarhet låter sig jämföras. Här skiljer sig inledningsvis konsekvensernas allvar och möjligheten att hantera konsekvenserna åt. En möjlig anledningen till skillnaderna i tillit till den egna förmågan handlar då om att förmågan att hantera konsekvenserna. Att smittas av coronaviruset och klara sig utan allvarliga skador, skulle kunna upplevas som utanför ens kontroll och allvarligare eftersom man kan mista

livet, än konsekvenserna av ett cyberangrepp. Men det är också skillnader mellan sannolikheten av att drabbas, och att själv kunna minska sannolikheten. En annan möjlig anledning är då att det rådde mycket osäkerhet i det initiala skedet av covid-19 pandemin om hur man skulle kunna klara sig om man väl smittades. Det vi sedan tidigare vet är att osäkerhet är sådant som ökar individens riskuppfattning och oro men också sannolikhetsbedömning att man ska drabbas av risken.

Socioekonomi avgör krisförmågan

Det finns i huvudsak tre förklaringar till en hög tillit till den egna förmågan (Bandura, 1977). Den första förklaringen är att man har erfarenhet av att hantera likartade kriser, den andra är att man tagit del av handlingsråd om hur risken effektivt ska avvärjas genom att observera hur andra man känner gör eller via medierna eller via kampanjer, och den tredje förklaringen är att man helt enkelt som medborgare är bättre rustad rent resursmässigt för att kunna hantera konsekvenserna om man drabbas (ibid). Eftersom de flesta medborgarna saknar erfarenheter av cyberattacker, ter sig den förklaringen osannolik. Även om vi ofta lär genom att se hur andra gör, är det inte heller särskilt vanligt att man känner någon som drabbats av en cyberattack. Det är också sparsmakat med beskrivningar i medierna eller i kampanjer vilka åtgärder man kan vidta inför eller vid en cyberattack, varför inte heller någon av observerade handlingsråd är en trolig förklaring i sammanhanget. Den mer troliga förklaringen, är de resonemang som handlar om kapabilitet och resiliens, alltså individens resursfaktorer, som exempelvis högre inkomstnivå för att kunna motstå ett glapp i inkomst vid en cyberattack (Bandura, 1977).

Av de resurs- och bakgrundsfaktorer vi kontrollerat för förklarar medborgarens sociala och ekonomiska resurser i form av tillit till andra människor i området där man bor (*b*= ,13*) och inkomstnivå (*b*= ,12***) mest av den självständiga effekten på tilliten till den egna förmågan att hantera situationen i scenariot om det skulle hända idag (se bilaga 2 tabell B3ff). Ju högre tillit till människor i området där man bor, och ju högre inkomst, desto högre tillit till den egna förmågan att hantera en cyberattack om den skulle hända i morgon. Men även kön (*b*= ,09*) och ålder (*b*= -,09**), har en självständig effekt på tilliten till den egna förmågan. Det är främst unga män som har en hög tillit till den egna förmågan. I analyser av kapabilitet i samband med covid-19 pandemin sågs ålder som en fysisk resursfaktor (Sandstig och Dahlin Ivanoff, 2021). Ju yngre man var desto större möjligheter hade man att kunna återhämta sig från viruset. Vi behöver dock hålla i åtanke att tilliten till den egna förmågan är självskattad, och vi vet inte om svaren speglar faktisk förmåga, eller snarare en överskattad eller förväntad självbild av förmåga. Här vet vi till exempel från undersökningar av upplevd otrygghet att det finns en tendens att män underdriver sina svar (Sandstig, 2010).

Många vill förbereda sig mot cyberrisker

Majoriteten, 59 procent, av medborgarna är i ganska eller mycket stor utsträckning beredda på att förbereda sig för en cyberattack och kollaps av nationella bank- och betaltjänster, likt den i scenariot (tabell 3ff). Detta medan motsvarande andel som i ganska eller mycket liten utsträckning är beredda på att förbereda sig för motsvarande är 41 procent (*M*=2,63).

Tabell 3 Beredskap för att förbereda sig för en cyberkris (procent)

I mycket liten utsträckning	7
I ganska liten utsträckning	34
I ganska stor utsträckning	49
I mycket stor utsträckning	10
Total procent	100
Totalt antal	869

Kommentar: Frågans formulering: *I vilken utsträckning är du beredd att förbereda dig inför IT-attacker likt dem i scenariot?* Svarsalternativen var i fallande ordning: ”I mycket liten utsträckning”, ”I ganska liten utsträckning”, ”I ganska stor utsträckning”, ” I mycket stor utsträckning”. N=869. *Källa*: Medborgarpanelen 2022.

Hög riskuppfattning och självtillit motiverar

Av de bakgrunds- samt sociala och ekonomiska resursfaktorer vi kontrollerat för saknas det i en sådan grundmodell självständiga effekter på medborgarnas beredskap att vidta åtgärder inför en cyberkris (se bilaga 2 tabell B4ff). Om vi däremot utökar modellen med faktorer som framförts av forskningen som riskuppfattning och tilliten till den egna förmågan ökar modellens förklaringskraft där den förklarar 17 procent medborgarnas motivation att vidta åtgärder inför cyberkriser. Tilliten till den egna förmågan (*b*= ,40***) förklarar mest av den självständiga effekten på motivationen att vidta åtgärder. Ju högre tilliten till den egna förmågan, desto mer beredda är medborgarna att vidta åtgärder för att förbereda sig för en cyberkris. Även riskuppfattningen av cyberhot har en självständig effekt på motivationen att vidta åtgärder. Det är främst bedömningen av konsekvensernas allvar (*b*= ,12***) men också bedömningen av sannolikheten att risken ska inträffa (*b* = ,10**) som har effekt på motivationen att vidta åtgärder.

Fokus på basåtgärder för skydd

Medborgarna ställdes därefter en fråga om *vilka* åtgärder de skulle vara villiga att vidta för att själv förbereda sig för cyberattacker liknande den i scenariot. Den primära åtgärden, som valdes av 80 procent av de tillfrågade var att samla innehåll som vatten, mat, batteriradio etcetera i en beredskapslåda (se tabell 4ff). Att ha extra kontanter hemma för att räcka ett par veckor och att söka information om de lokala riskerna och hur man skyddar sig valdes som en åtgärd av nästan tre fjärdedelar av de tillfrågade.

Den åtgärd som i lägst utsträckning valdes var att ha kontanter hemma för att låna ut till närmaste grannar (15 %). Mycket få (41 respondenter) angav andra sätt på det öppna svarsalternativet och endast 1 procent (8 respondenter) svarade att de inte var beredda att vidta några åtgärder.

Tabell 4 Åtgärder som medborgarna är beredda att vidta för att förbereda sig inför cyberattacker likt dem i scenariot (procent)

Åtgärder	
Samla ihop en krisberedskapslåda (vatten, mat, batteridriven radio etc.)	80
Ha kontanter hemma som räcker för att klara mig i flera veckor	75
Ta reda på information om de lokala hoten och riskerna och hur man kan skydda sig	71
Ha extra mediciner hemma	67
Ha goda relationer till grannar och näringsidkare för utbyte av varor och tjänster	52
Hjälpa andra genom att inte hamstra förnödenheter	42
Skriva en att-göra-lista/plan för hushållet som beskriver i vilken ordning/hur man ska agera	39
Ha flera bankkort med olika utgivare, samt kredit på någon av dessa	38
Ha tillgång till extra bränsle eller drivmedel	37
Ha en större summa kontanter hemma som jag kan låna ut till närmaste grannar	15
Andra sätt:	5
Jag är inte beredd att vidta några åtgärder	1

Kommentar: Frågans formulering: *Vilka av följande åtgärder är du beredd att vidta för att förbereda dig inför IT-attacker likt dem i scenariot? Flera alternativ kan kryssas i.* Svarsalternativen var i fallande ordning: ”Ta reda på information om vilka de lokala hoten och riskerna är och hur man kan skydda sig”, ”Skriva en att-göra-lista med en plan för hushållet som beskriver i vilken ordning och hur man ska agera”, ”Samla ihop en krisberedskapslåda (vatten, mat, batteridriven radio etc.)”, ”Ha extra mediciner hemma”, ”Ha tillgång till extra bränsle eller drivmedel”, ”Ha kontanter hemma som räcker för att klara mig i flera veckor”, ”Ha goda relationer till grannar och näringsidkare i mitt närområde för utbyte av varor och tjänster”, ”Ha flera bankkort med olika utgivare, samt kredit på någon av dessa”, ”Ha en större summa kontanter hemma som jag kan låna ut till närmaste grannar”, ”Hjälpa andra genom att inte hamstra förnödenheter”, ”Andra sätt:_____”, ”⊗Jag är inte beredd att vidta några åtgärder”. N=825. *Källa*: Medborgarpanelen 2022.

En slutsats är alltså att många sammankopplar en samhällelig cyberkris med en allmän hemberedskap. Eller helt enkelt att förbereda sig för en samhällelig cyberkris ses som en del av hemberedskapen.

I den fördjupade analysen av fritextsvaren på frågan beskrevs följande andra sätt, de flesta relaterade till att förebygga genom att hantera samhälleliga konsekvenser av en cyberkris: olika former av självförsörjning av vatten, värme, mat, el och drivmedel. Exempelvis med svar som ”Egen äldre brunn, egenodlade grönsaker inklusive inläggningar under åtminstone viss del av året”, ”Förberedande genom att veta vad för växter som är ätliga och inte”, ”Kunskap om hur man bäst tar hand om kläder så de håller eller i alla fall kan lagas”, ”Ha ett elverk hemma så att jag kan driva en kyl och frys samt en vedeldad spis för värme och matlagning”, ”Ha en cykel” eller ”Jag har förnödenheter på två olika ställen och skulle klara mig bra utan pengar och drivmedel som jag har i en speciell tank”. Men också såväl altruistiska alternativ som att hjälpa andra både praktiskt och psykiskt, genom att upplåta sitt hem, eller bidra med IT-kunskap eller ett värnande om demokratin och den mellanmänskliga tilliten och att inte bidra till social oro genom att dämpa spridningen av panik och desinformation på nätet förekom. Några åtgärder var mer drastiska som att beväpna sig och göra motstånd mot dem som orsakade krig.

Tre vägar till beredskap: rusta, medvetandegöra och värna relationer

En faktoranalys av hur medborgarnas svar på de åtgärdsalternativ som efterfrågas hänger ihop med varandra (se tabell 5), visar att det går att urskilja tre olika åtgärdsdimensioner: *att rusta materiellt*, *att vara medveten* och *att värna relationer*.

Tabell 5 Tre dimensioner i de åtgärder medborgarna är beredda att vidta för att förbereda sig inför cyberattacker likt dem i scenariot

Åtgärder	*Att rusta materiellt*	*Att vara medveten*	*Att värna relationer*
Samla ihop en krisberedskapslåda (vatten, …	,732	,044	-,030
Ha kontanter hemma som räcker för att …	,659	-,100	,111
Ha extra mediciner hemma	,613	,289	-,005
Ha tillgång till extra bränsle eller drivmedel	,528	,065	,219
Upprätta åtgärdslista och plan för hushållet …	,181	,684	,014
Ta reda på information om de lokala hoten …	,034	,623	,031
Ha flera bankkort med olika utgivare, samt …	-,048	,524	,165
Hjälpa andra genom att inte hamstra ...	-,167	,093	,745
Ha goda relationer till grannar och …	,254	-,024	,648
Ha en större summa kontanter hemma som …	,220	,224	,467

Kommentar: Faktoranalysen inkluderar de 10 åtgärdsalternativ som presenteras i tabell 4. Metod: Roterad komponentmatris. *Källa*: Medborgarpanelen 2022.

Det innebär att om en medborgare svarat på en av frågorna i den aktuella dimensionen har de med stor sannolikhet också svarat på de andra åtgärdsförslagen i samma dimension.

Åtgärderna medborgarna är beredda att vidta är av tre olika typer (se tabell 5). Den första, *att rusta materiellt*, handlar om basåtgärder vid samhällskriser dvs att samla ihop en krisberedskapslåda eller att ha extra resurser av kontanter, eller mediciner hemma eller ha tillgång till extra drivmedel. Den andra, *att vara medveten*, handlar om att kunna planera för en cyberkris genom att upprätta en åtgärdslista för hushållet, att ta reda på information om hur man skyddar sig, eller att ha flera bankkort med olika utgivare, med kredit på något. Den tredje, *att värna relationer*, handlar om att hjälpa andra genom att inte hamstra förnödenheter, ha goda relationer för utbyte av varor och tjänster eller att ha en större summa kontanter hemma för att kunna låna ut till grannar.

Olika drivkrafter bakom olika åtgärder

På motsvarande sätt som för riskuppfattningarna går det att med en regressionsanalys få fram några karakteristiska idealtyper för vilka typer av åtgärder som medborgarna är motiverade att vidta (se tabell 6, se bilaga 2 tabell B5ff).

Tabell 6 Karakteristika idealtyper som förklarar vilka typer av förberedande åtgärder medborgarna är villiga att åta sig för att skydda sig från en cyberkris

	Motivation	
Typer av åtgärder	Låg	Hög
Att rusta materiellt	Ung man.	Äldre kvinna.
Att medvetandegöra	Låg utbildning och lågt förtroende för regeringen.	Hög utbildning och högt förtroende för regeringen.
Att värna relationer	Man med lågt förtroende för regeringen.	Kvinna med högt förtroende för regeringen.

Sammanfattningsvis varierar karaktärsdragen för åtgärderna medborgarna är villiga att åta sig för att skydda sig från en cyberkris. Det är mer sannolikt att en äldre kvinna kan tänka sig att förbereda sig materiellt genom att exempelvis ha en krisberedskapslåda och extra mediciner hemma, snarare än en ung man. Detta medan det är mer troligt att en högutbildad med ett högt förtroende för regeringen kan tänka sig att förbereda sig genom att exempelvis ha en åtgärdsplan och ta reda på mer information, än en med låg utbildning och ett lågt förtroende för regeringen. Det är på motsvarande sätt mer sannolikt att en kvinna med högt förtroende för regeringen är motiverad att värdera och värna relationer, än en man med lågt förtroende för regeringen.

Riskperceptionsparadoxen

Inom forskningen om risker (se Goerlandt och Li, 2021) om främst naturkatastrofer har man försökt att förstå varför individer inte förbereder sig eller vidtar åtgärder även om deras riskmedvetenhet och riskuppfattning om risken är hög. Riskperceptionsparadoxen, hävdar att en ökad riskuppfattning inte nödvändigtvis leder till ökade förberedelser, och föreslår tre förklaringar till varför. Även om individer förstår risken så accepterar de den, eller så tror de inte att de själv är ansvariga utan förskjuten ansvaret, eller så saknar de möjligheter, resurser eller förmågan att hantera risken (Wachinger, Renn, Begg och Kuhlicke, 2013).

Kapabilitetsbrist minskar motivationen

De medborgare som i ganska eller mycket *liten* utsträckning angav att de var beredda att förbereda sig för en cyberattack och kollaps av nationella bank- och betaltjänster, likt den i scenariot fick följdfrågan: *Om du i mycket eller ganska låg utsträckning är beredd att förbereda dig inför IT-attacker, vilka är dina huvudsakliga skäl till att inte förbereda dig? Flera alternativ kan kryssas i*. De svarsalternativ som i huvudsak erbjöds utifrån förklaringarna i perceptionsparadoxen var: ”Jag anser att det är någon annans ansvar”; ”Jag accepterar risken om IT-attackerna skulle inträffa”; Jag har inga eller små möjligheter att förbereda mig”; eller andra skäl som ”Jag har prioriterat bort att förbereda mig eller har inte tid för det”, eller ”Andra skäl:” med möjlighet att ange skäl på det öppna svarsalternativet.

Närmare hälften (47%) av dem som svarat anger att de har små eller inga möjligheter att förbereda sig (kapabilitetsbrist) (se tabell 7ff). Detta medan närmare en tredjedel (30%) accepterar risken om cyberattackerna skulle inträffa. En fjärdedel har prioriterat bort det. I motsats till tidigare forskning om i huvudsak naturolyckor (Goerlandt och Li, 2021), anges svaret att det är någon annans ansvar av få individer. Endast av var sjätte medborgare (15%) anger att det är någon annans ansvar, och 9 procent (eller 30 respondenter) har angett andra skäl.

Tabell 7 Andel som angett olika skäl för att inte förbereda sig för en cyberkris (procent)

Skäl för att inte förbereda sig	
Jag har inga möjligheter att förbereda mig	47
Jag accepterar risken	30
Jag har prioriterat bort att förbereda mig	25
Det är någon annans ansvar	15
Andra skäl	9

Kommentar: Till de respondenter som svarat att de i mycket eller ganska låg utsträckning är beredda att vidta åtgärder ställdes frågan: *Om du i mycket eller ganska låg utsträckning är beredd att förbereda dig inför IT-attacker, vilka är dina huvudsakliga skäl till att inte förbereda dig? Flera alternativ kan kryssas i.* Svarsalternativen var i fallande ordning: ”Jag anser att det är någon annans ansvar”; ”Jag accepterar risken om IT-attackerna skulle inträffa”; Jag har inga eller små möjligheter att förbereda mig”; ”Jag har prioriterat bort att förbereda mig eller har inte tid för det”; ”Andra skäl:” med möjlighet att ange skäl på det öppna svarsalternativet. Andel som angett kryss av alla dem som svarat på frågan. N=336.
Källa: Medborgarpanelen 2022.

I en fördjupad analys av fritextsvaren på det öppna svarsalternativet är de vanligaste andra skäl som anges att man ansåg att sannolikheten att det skulle hända var låg, att det var för stort att ta in eller att man redan var förberedd. Ett exempel på ett svar som sammanfattar alla tre skälen är:

”Det känns ganska orimligt att förbereda sig för eventuellt kaosartade situationer, då det kan bli hur många scenarion som helst och då skulle jag bara gå omkring och oroa mig. Vi har det basala hemma, resten får lösa sig beroende på situation. ”.

Även kapabilitetsbrister i form av bristande kunskap eller medvetenhet beskrevs, ansvarsförskjutning till stat, kommun och banker, samt att man helt enkelt ansåg att man var för lat.

Låg tillit och inkomst förklarar passivitet

När det gäller de skäl, medborgarna angett till varför de inte är motiverade att förbereda sig går det att, utifrån de faktorer vi frågat efter, att förklara med bakgrundsfaktorer som ålder, och sociala och ekonomiska faktorer som inkomst, tillit till människor i området där man bor, tilliten till sin egen förmåga samt konsekvensernas allvar (bilaga 2 tabell B7ff).

Om vi ser till skälet att ange *att man inte har någon möjlighet att förbereda sig*, alltså en kapabilitetsbrist, går det också att främst förklara med resursbrister i form av att man i lägre utsträckning litar på människor i området där man bor (*b*= -,20*), har en lägre inkomst (*b*= -,17**) och har en lägre tillit till den egna förmågan (*b*= -,17**).

Hög självtillit och låg riskuppfattning ger acceptans

Skälet att ange *att man accepterar risken*, går att förklara med att man har en högre tillit till sin egen förmåga (*b*=,21***) och en lägre bedömning av allvaret av riskens konsekvenser (*b*= -,15**) (se bilaga 2 tabell B7).

Att ange *att man har prioriterat bort det* kan förklaras med att man är ung (*b*= -,38***) (se bilaga 2 tabell B7). Inga av de faktorer vi frågat efter, förklara *att man angett skälet att det är någon annans ansvar*.

Slutsatser och rekommendationer

En viktig slutsats är att de flesta medborgare är villiga att vidta åtgärder för att skydda sig från samhälleliga cyberrisker. Men vad kan man som myndighet och kommun tänka på för att hjälpa medborgarna att ha tillförlitlig och relevant information? Detta för att kunna bedöma cyberrisker som kan drabba dem, minska deras sårbarhet och öka deras beredskap inför ett framtida hot.

Gör budskapet relevant för att nå fram

Forskningen visar att cyberrisker är högt upp på medborgarnas agenda, och analysen i denna rapport visar att krig och cyberrisker toppar medborgarnas riskuppfattningar. Det vi vet är att en hög riskuppfattning hänger ihop med en ökad oro för dessa risker. En ökad oro kan leda till något negativt för dem som redan är oroliga, och i förlängningen kan oron också urholka förtroendet för avsändare, till exempel myndigheterna eller kommunerna. Men ur kommunikationshänseende är en hög riskuppfattning fördelaktigt. Detta eftersom det motiverar medborgarna att söka information och att vidta åtgärder för att förbereda sig. De råd som rapporten kommer fram till kan därför till synes verka motsägelsefulla.

En rekommendation att som myndighet eller som kommun tänka på vid kommunikation med medborgarna är därför att använda eller fortsätta att använda riskkommunikationsmodeller som EPPM eller IDEA. Detta eftersom de inte bara fångar medborgarnas uppmärksamhet och som gör budskapet relevant utan som också tryggar och dämpar den eventuella oron. Det är viktigt att behålla balansen mellan att motivera och instruera. Oron dämpas genom att budskapet också innehåller budskapsåtgärder som instruerar vilka åtgärder som kan vidtas för att hantera risken och som övertygar om att åtgärderna är effektiva. Som att exempelvis ha extra kontanter hemma, att ha flera bankkort med olika utgivare, med kredit på något samt att ha goda relationer i närområdet. Dessa budskap dämpar oron och stärker medborgarnas tillit till sin egen förmåga att hantera cyberkrisen om den skulle inträffa.

Anpassa kommunikationen till olika grupper

Analysen i denna rapport visar att det främst är kvinnor, inte sällan unga kvinnor, som har höga riskuppfattningar av cyberrisker och andra risker. Detta medan män, inte sällan unga

män, har en lägre. En hög riskuppfattning är oftast fördelaktig i kommunikations-sammanhang. Detta eftersom förutsättningarna att motivera individen att söka information eller att kommunicera uppmaningar till att vidta skyddsvärda åtgärder, är goda. Men en hög riskuppfattning kan också vara problematisk eftersom den medför en högre oro. En oro som behöver tryggas upp så att oron inte tar över. De äldre männens lägre riskuppfattning gör dem svårare att motivera att förbereda sig för cyberkriser. Eller med andra ord en rekommendation till myndigheter och kommuner är att det kan krävas olika informationsinsatser för att motivera olika grupper att förbereda sig inför cyberkriser.

Stötta socioekonomiskt svagare grupper i samhället

Vidare visar analysen i denna rapport att medborgarnas tillit till sin egen förmåga att hantera en cyberkris om den skulle hända idag, är hög. Den höga tilliten förklaras främst av sociala och ekonomiska resursfaktorer som tillit till människor i området där man bor och inkomstnivå. Majoriteten av medborgarna är också beredda att vidta åtgärder för att förbereda sig inför cyberrisker. En hög riskuppfattning och en hög tillit till den egna förmågan att hantera en cyberkris, är det som främst förklarar motivationen för att vidta åtgärder. Resultaten i denna studie talar alltså också för användningen eller den fortsatta användningen av riskkommunikationsmodeller som EPPM och IDEA som också innehåller budskapsåtgärder som stärker medborgarnas tillit till sin egen förmåga.

Men det pekar också på utmaningar för myndigheter och kommuner, att stärka beredskapen hos de mest socialt och ekonomiskt utsatta i samhället. Detta talar för den inriktning på kapabilitet som tar hänsyn till att det förutom att man kan ha exempelvis utbildnings- eller ekonomiska resurser, att det också behöver finnas villkor för att kunna använda dem.

Främja engagemang och samverkan i närområdet

Det finns tre olika typer av åtgärder som medborgarna är beredda att vidta för att skydda sig från en cyberkris. Den första handlar om att förbereda sig praktiskt, exempelvis genom att ha extra kontanter hemma. Den andra åtgärden handlar om att vara medveten och smart i sin vardag, genom att exempelvis ha flera bankkort från olika banker, gärna med kredit. Den tredje typen av åtgärd handlar om relationer. Att ha ett nätverk av människor som man litar på, som man kan samarbeta och byta varor och tjänster med i en kris. Vad man är beredd att göra hänger ofta ihop med vilka resurser man har. Personer med hög utbildning är mer benägna att vidta medvetna, planerade åtgärder. De som känner stark tillit till andra – till exempel i sitt grannskap – är i högre grad beredda att satsa på relationer som en del av sin beredskap. Det här visar att det inte räcker att bara ha resurser, som utbildning eller pengar

– det måste också finnas möjligheter att använda dem i praktiken. Beredskap handlar alltså inte bara om vad man har, utan också om vilka villkor man lever under. För att stärka beredskapen i samhället är det därför viktigt att kommunicera på ett sätt som främjar engagemang, samarbete och lokalt nätverkande. När medborgarna får stöd att använda sina resurser – oavsett om det handlar om kunskap, pengar eller kontakter – ökar chanserna att de faktiskt vidtar åtgärder inför en cyberkris.

Kommunerna är också stora arbetsgivare. Medborgarna är inte bara invånare utan flera arbetar också inom kommunen som ska fungera också när det inte är en kris. Om man drabbas av en cyberkris, drabbas man inte bara som en medborgare utan också som en arbetstagare. Många är beroende av att hemsjukvården, skolan, energiförsörjningen, vattentillförsels och sophämtningen fungerar. Det mesta är beroende av dessa system idag, där systemen inte är separerade, utan uppblandade.

En viktig anledning till att medborgarna inte är motiverade att förbereda sig inför en cyberkris är att de helt enkelt saknar eller har få möjligheter – de har för lite pengar eller andra resurser för att kunna agera. En annan anledning är att de accepterar risken – för att de har en hög tillit till sin egen förmåga att hantera krisen om den skulle inträffa, eller helt enkelt inte uppfattar risken som särskilt hög. Det innebär att det finns stöd för den så kallade riskperceptionsparadoxen. Alltså förklaringen att människor trots att de har en hög riskuppfattning inte förbereder sig för en kris, för att de saknar resurser eller för att de accepterar risken. Inte bara när det gäller olika naturkriser, utan också för sociala kriser som en cyberkris. Däremot är stödet svagt för förklaringen att människor låter bli att förbereda sig för att de tycker att det är någon annans ansvar.

För att optimalt använda medborgarnas samlade resurser inför eller i samband med samhälleliga cyberkriser, är en rekommendation till myndigheter och kommuner att främja kommunikationsinsatser som betonar engagemang, tillit och samarbete i närområdet.

Studiens begränsning

Studien har en begränsning som hänger ihop med det ursprungliga syftet inom ramen för DURCOM-projektet. Att pröva orsakssamband inom ramen för ett experiment, där representativitet i data inte är prioriterat. Datat som använts är trots allt representativt utifrån att ha stratifierats utifrån kön, men däremot inte avseende att ha stratifierats efter ålder och utbildning. Medborgarnas utbildning och ålder är alltså något högre i populationen som undersökts än bland medborgarna. Resultaten går alltså att generalisera i relation till kön, men när det gäller resultaten i relation till ålder och utbildning bör de tolkas med försiktighet.

Referenser

Amin, Z. (2019). A practical road map for assessing cyber risk, *Journal of Risk Research*, 22(1), 32–43, DOI: 10.1080/13669877.2017.1351467

Backman, S. (2021). Conceptualizing cyber cries. J*ournal of Contingencies and Crisis Management, 29, 429–438*. DOI: 10.1111/1468-5973.12347

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioural change. *Psychological Review*, 84(2), 191–215. DOI: 10.1037/0033-295X.84.2.191

Busby, J.S., Green, B. and Hutchison, D. (2017). Analysis of affordance, time, and adaptation in the assessment of industrial control system cybersecurity risk. *Risk Analysis 37*(7), 1298–1314. DOI: 10.1111/risa.12681

Caruson, K., MacManus, S. A., and McPhee, B.D. (2012). Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success. *Homeland Security & Emergency Management*, 9(2), 1–22. DOI: 10.1515/jhsem-2012-0003

Cervenka, A. (2025). Svenska bankers makt har blivit en säkerhetsrisk. 29/4-2025 Aftonbladet. https://www.aftonbladet.se/nyheter/kolumnister/a/W0KAnQ/cervenka-svenska-bankers-makt-har-blivit-en-sakerhetsrisk Hämtad 30/4-2025.

Chodakowska, A., Kańduła, S., and Przybylska, J. (2022). Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done. *Lex Localis – Journal of Local Self-Government*, 20(1), 161–192. DOI:10.4335/20.1.161-192(2022)

Covello, V.T., von Winterfeldt., D. and Slovic, P. (1986). *Risk communication: A Review of the Literature*. Washington, DC: National Science Foundation.

Eling, M., Schnell, W. (2016). Ten key questions on cyber risk and cyber risk insurance. *Technical Report 2016*. The Geneva Association, Zurich. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-risk-10_key_questions.pdf Hämtad 2/1-2025.

Elestedt, L., Nilsson, U. och Rosenvinge, C-J. (2021). En cyberattack kan påverka den finansiella stabiliteten. *Ekonomisk kommentar nr 8. Sveriges Riksbank*.

Fischhoff, B. (1995). Risk Perception and Communication Unplugged: Twenty Years of Process. *Risk Analysis*, 15(2), 137–145. DOI: 10.1111/j.1539-6924.1995.tb00308.x

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. and Combs, B. (1978). How Safe Is Safe Enough? A Psychometric Study of Attitudes Towards Technological Risks and Benefits. *Policy Sciences*, 9, 127–152.

Frisby, B.N., Sellnow, D.D., Lane, D.L., Veil, S.R. and Sellnow, T.L. (2013). Instruction in crisis situations: Targeting learning preferences and self-efficacy. *Risk Management*, 15 (4), 250–271.

Goerlandt, F., and Li, J. (2022). Forty years of risk analysis: A scientometric overview. *Risk Analysis,* 42(10), 2253–2274. DOI: 10.1111/risa.13853

Hatcher, W., Meares, W.L., and Heslen, J. (2020). The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices. *Journal of Cyber Policy*, 5(2), 302–325. DOI: 10.1080/23738871.2020.1792956

He, M., Devine, L. and Zhuang. J. (2018). Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach. *Risk Analysis* 38(2), 215–225. DOI: 10.1111/risa.12878

Johansson, B. and Sandstig, G. (2024). Instruction as self-protection. In Sellnow, T.L. and Sellnow, D.D., (Eds.) *Communicating Risk and Safety*, 321–338. DOI: 10.1515/9783110752427-019

Kasperson, R. (2014). Four questions for risk communication. *Journal of Risk Research*, 17(10), 1233–1239. DOI: 10.1080/13669877.2014.900207

Lindell M.K. and Perry, R.W. (2004). *Communicating Environmental Risk in Multiethnic Communities*. Thousand Oaks, CA: Sage.

Lindström, K. (2024). Ransomwareattack mot Kumla kommun – känsliga uppgifter har läckt. 6/11-2024 *Computer Sweden*. https://computersweden.se/article/3600010/ransomwareattack-mot-kumla-kommun-kansliga-uppgifter-har-ackt.html#:~:text=Kumla%20drabbades%20i%20l%C3%B6rdags%20av%20en%20ransomwareattack%20och,l%C3%A4cka%20ut%20k%C3%A4nslig%20information%20som%20de%20kommit%20%C3%B6ver. Hämtad 17/5 2025.

Lowenstein, G.F., Weber, E.U., Hsee, C.K. and Welch, N. (2001). Risk as Feelings. *Psychological Bulletin*, 127(2), 267–286. DOI:10.1037/0033-2909.127.2.267

Macmanus, S., Caruson, K. and McPhee, B.D. (2012). Cybersecurity at the Local Government Level: Balancing Demands for Transparency and Private Rights. *Journal of Urban Affairs*, 35(4), 451–470. DOI: 10.1111/j.1467-9906.2012.00640.x

Myndigheten för samhällsskydd och beredskap (MSB), (2018). *Om krisen eller kriget kommer*. Karlstad: MSB.

Myndigheten för samhällsskydd och beredskap (MSB), (2024). *Om krisen eller kriget kommer*. Karlstad: MSB. Myndigheten för samhällsskydd och beredskap (MSB), (2018) *Om krisen eller kriget kommer*. Karlstad: MSB.

National Research Council (NRC). (1989). *Improving Risk Communication*. Washington, DC: National Academy Press.

Nussbaum M.C. (2011). *Creating Capabilities: The Human Development Approach*. Cambridge: Belknap Press.

Rabe, L., Sataøen, H.L., Lidskog, R. and Eriksson, M. (2024): Making risk communication in practice: dimensions of professional logics in risk and vulnerability assessments, *Journal of Risk Research*, 1–15. DOI: 10.1080/13669877.2024.2328199

Renn, O. (1992). Concepts of Risk: A Classification, 53-79. In Krimsky, Sheldon and Golding, Dominic (Eds.) *Social Theories of Risk.* Westport, US.: Praeger Publishers.

RFR 2015/16 RFR3. Om krisen eller kriget kommer – en uppföljning av informationsinsatser till allmänheten om den enskildes ansvar och beredskap. Stockholm: Riksdagstryckeriet.

Rogers, R.W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. In *Social Psychophysiology: A sourcebook*, edited by Cacioppo, John, and Richard E. Petty. New York, USA: Guilford Press.

Ruiter, R.AC., Kessels, L.T.E K., Peters, G.Y., and Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology* 49(2), 63–70. DOI: 10.1002/ijop.12042

Sandstig, G., Eriksson, M. (2024). Shared responsibility or not? A responsibility messages experiment during a cyber crisis in designing for risk communication. *Journal of Risk Research*, 27(10), 1163-1179. DOI: 10.1080/13669877.2024.2387351

Sandstig, G., Boholm, M., Berlin, J. (forthcoming). A Paradox of Cybersecurity? The Democratic Deficit in Municipal Work to Raise Citizens' Risk Awareness.

Sandstig, G. och Dahlin Ivanoff, S. (2021). Tilltron till den egna förmågan under coronapandemin. I Ulrika Andersson, Anders Carlander, Marie Grusell och Patrik Öhberg (red) *Ingen anledning till oro (?).* Göteborg: SOM-institutet, Göteborgs universitet.

Sandstig, G. (2019). Riskkommunikation och krisberedskap i väst - av nöd och lust. I Carlander, A., Öhberg, P. och Mellander, E. (red.) *Ingen kommer undan kulturen*. Göteborg: SOM-Institutet, Göteborgs universitet.

Sandstig, G. (2010). *Otrygghetens landskap. En kartläggning av otryggheten i stadsrummet och en analys av bakomliggande orsaker, med fokus på mediernas roll*. Doktorsavhandling. Göteborg: Institutionen för journalistik, medier och kommunikation (JMG), Göteborgs universitet.

Sellnow, T.L. and Seeger, M.W. (2016). *Theorizing Crisis Communication*. Wiley-Blackwell.
Sellnow, D.D., Derek R.L., Sellnow, T.L. and Littlefield. R.S. (2017). The IDEA model as a best practice for effective instructional risk and crisis communication. *Communication Studies*, 68(5), 552–567. DOI: 10.1080/10510974.2017.1375535

Sellnow, D.D. and Sellnow, T.L. (2019). The IDEA model for effective instructional risk and crisis communication by emergency managers and other key spokespersons. *Journal of Emergency Management*, 17(1), 67–78. DOI: 0.5055/jem.2019.0399

Sellnow, T.L., Ulmer, R.R., Seeger, M.W., and Littlefield, R.S. (2009). *Effective Risk Communication. A Message–Centered Approach*. Springer.

Sen, A. (1993). Capability and well-being. In: Nussbaum, M. and Sen, A. (eds.) *The quality of life*. Oxford: Clarendon Press.

SFS 2015:1052. Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Regeringskansliet.

Sjöberg, L., Moen B-E., and Rundmo, T. (2004). *Explaining risk perception: An evaluation of the psychometric paradigm in risk perception research*. Trondheim, Norway: Rotunde publikasjoner.

Slovic, P. (1987). Perception of Risk. *Science*, 236(4799), 280–285. DOI: 10.1126/science.3563507

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, 135 (105143), 1-10. DOI: 10.1016/j.ssci.2020.105143

Karlsson, J. (2022). ”Cyberangrepp kan få lika stora konsekvenser som pansarvagnar”. 14/1-2022 Sveriges Television (SVT).

Wachinger, G., Renn, O., Begg, C. and Kuhlicke, C. (2013). The risk perception paradox—implications for governance and communication of natural hazards. *Risk analysis*, 33(6), 1049–1065. DOI: 10.1111/j.1539-6924.2012.01942.x

Wirth, A. (2017). Hardly ever a dull moment: The ongoing cyberthreats of 2017. B*iomedical Instrumentation & Technology*, 51(5), 431–433. DOI: 10.2345/0899-8205-51.5.431.

Witte, K. and Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. Health Education & Behavior 27(5). 591–615. DOI: 10.1177/109019810002700506

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, 59(4), 329–349. DOI: 10.1080/03637759209376276

World Economic Forum (WEF) (2025). The global risks report 2025. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf Hämtad 6/2-2025.

World Economic Forum (WEF) (2019). The global risks report 2019. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf. Hämtad 6/2-2025.

Xu, W., Murphy, F., Xu, X., Xing, W. (2021). Dynamic communication and perception of cyber risk: Evidence from big data in media. *Computers in Human Behavior*, 122, 106851. DOI: 10.1016/j.chb.2021.106851

Zhang, X.A. and Borden, J. (2020). How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research*, 23(10), 1336–1352. DOI: 10.1080/13669877.2019.1646315

Bilaga 1 Uppdrag

I projektet *Risk- och beredskapskommunikation för ett robust digitalurbant samhälle, Digital Urban Risk Communication* (DURCOM) prövade vi inom ramen för Medborgarpanelen 2022 (i fält 25/5–15/6) med hjälp av ett experiment effekterna av olika former av ansvarsbudskap på medborgarnas föreställningar om deras eget ansvar och deras intention att förbereda sig utifrån ett krisscenario som skildrade en cyberattack mot en kommun samtidigt som det skett attacker mot nationella bank- och betalsystem som ligger nere (scenariot var inspirerat av händelserna i Kalix vintern 2021 samt MSB-projektet *Om betalsystemet kraschar*). Krisscenariot vi använde oss av i experimentet var:

> Föreställ dig att din kommun och nationella bank- och betaltjänster till följd av IT-attacker drabbats av en kollaps. Det leder till stora störningar i kommunens samhällsservice samt svårigheter att införskaffa livsnödvändiga förnödenheter som livsmedel, drivmedel och medicin. Det är oklart när saker kan börja fungera igen, men bedömningen är att det kan dröja flera veckor eller månader. Du vänder dig till de nyhetskällor du litar på för att få mer information om läget.

Resultat från budskapsexperimentet har bearbetats och publiceras i en vetenskaplig artikel (Sandstig and Eriksson, 2024). Men utöver resultaten från själva budskapsexperimentet, finns där resultat baserade på kontrollgruppens svar (*n*=879), alltså de som tog del av krisscenariot ovan men som inte tog del av budskapsmanipuleringarna, som vi tror kan vara av intresse att bearbeta vidare. Detta för att lära oss mer om:

> Vad medborgarna har för föreställningar om cyberrisker, vilka åtgärder medborgarna är motiverade att vidta i händelse av ett motsvarande scenario i verkligheten samt nycklar till varför medborgarna inte är motiverade att vidta åtgärder. Även en variansanalys av hur medborgarna är beredda att vidta åtgärder hänger ihop är möjlig, samt en vidare bearbetning av svaren på de öppna frågorna om åtgärder medborgarna är beredda att vidta respektive skälen till att de inte är beredda att vidta några åtgärder. I den utsträckning det är möjligt går det också att bryta ner svaren utifrån de bakgrundsfrågor och frågor om förtroende och tillit som ställts.

Datat är representativt utifrån att ha stratifierats utifrån kön, men däremot inte avseende att ha stratifierats efter ålder och utbildning. Medborgarnas utbildning och ålder är alltså något högre i populationen än bland medborgarna.

I dagsläget vet medborgarna ganska lite om hur de ska förbereda sig eller vad de förväntas göra vid en cyberattack. De har via broschyren *Om krisen eller kriget kommer* informerats om att de ska ha kontanter hemma i olika valörer, men utöver det var det sparsamt. I den senaste broschyren har råden utökats med att ha andra betallösningar som bankkort och digitala tjänster. Även information och digital säkerhet har tillförts. Medborgaren uppmanas att skapa långa lösenord med en kombination av bokstäver, siffror och symboler, inte klicka på länkar i mejl och inte öppna inte bilagor från okända avsändare, installera säkerhetsuppdateringar direkt etcetera.

Söker man efter information på kommunernas hemsidor saknas det i stort helt information om cyberrisker och hur man som medborgare förväntas agera. Detta trots att konsekvenserna av en cyberattack enligt försvaret kan bli lika allvarliga som vid ett krig. Vi ställde dels frågan ”I vilken utsträckning är du beredd att förbereda dig inför IT-attacker likt dem i scenariot?” följt av frågan ” Vilka av följande åtgärder är du beredd att vidta för att förbereda dig inför IT-attacker likt dem i scenariot?” med tio fasta svarsalternativ som valts utifrån erfarenhetskunskap, och ett öppets svarsalternativ där medborgarna själv fick ange åtgärder de var motiverade att vidta. De medborgare som i låg utsträckning angav att de var beredda att vidta några åtgärder ställdes följdfrågan ”Om du i mycket eller ganska låg utsträckning är beredd att förbereda dig inför IT-attacker, vilka är dina huvudsakliga skäl till att inte förbereda dig?” med fyra fasta svarsalternativ baserade på tidigare forskning om andra typer av risker, samt ett öppet svarsalternativ.

Baserat på dessa frågor skulle det gå att uttala sig om 1) hur stor andel av populationen som kan tänka sig att vidta 2) vilka åtgärder och i vilken utsträckning samt hur svaren grupperar sig dvs vilka typer av medborgare som svarar vilka åtgärder. Det går också att utifrån medborgarnas svar på den öppna frågan att undersöka 3) vilka andra typer av åtgärder som medborgarna kan tänka sig att åta som vi inte ställt frågor om. Utifrån de medborgare som i låg eller ingen utsträckning är beredda att förbereda sig går det också att 4) uttala sig om hur stor andel som inte förbereder sig beroende på de förklaringar som tidigare förts fram inom forskningen om perceptionsparadoxen främst utifrån naturrisker. Men det går också utifrån medborgarnas svar på den öppna frågan om anledningarna till att man inte förbereder sig undersöka 5) vilka andra typer av skäl som förs fram som vi inte ställt frågor om. I den utsträckning materialet tillåter går det också att bryta ner svaren på kön, ålder, utbildning, inkomst, förtroendet på en rad olika institutioner, mellanmänsklig tillit i allmänhet samt tillit till människorna i området där man bor.

Bilaga 2 Tabellbilaga

Tabell B1 Riskuppfattningar av sex olika hot eller risker som skulle kunna förekomma i medborgarnas kommun inom de närmaste 12 månaderna (medelvärde)

Hot eller risk	*Sannolikhet*	*Konsekvens*	*Total*
Krig eller en motsvarande militär konflikt	1,60	3,43	3,46
Cyberattack och kollaps av nationella bank- och betaltjänster	2,49	3,11	3,19
Större olycka med utsläpp av gifter eller radioaktivitet	1,58	2,97	3,02
Terrordåd eller annat organiserat våld	2,19	2,93	2,97
Skogsbrand, kraftig storm, orkan eller översvämning	2,28	2,60	2,82
Ytterligare en pandemi eller en epidemi	2,28	2,68	2,81

Kommentarer: Sannolikhetsfrågans formulering: *Hur troligt bedömer du att det är att nedanstående kommer att inträffa i din kommun inom de närmaste 12 månaderna?* Svarsalternativen från vänster till höger var: ”Inte alls troligt”, ”Inte särskilt troligt”, ”Ganska troligt”, ”Mycket troligt”. $N_{sannolikhet}$=873--879. Konsekvensfrågans formulering: Hur allvarliga bedömer du att konsekvenserna blir för dig om din kommun skulle drabbas av nedanstående inom de närmaste 12 månaderna? Svarsalternativen från vänster till höger var: ”Inte alls allvarliga”, ”Inte särskilt allvarliga”, ”Ganska allvarliga”, ”Mycket allvarliga”. Total är en sammanslagning av MAX (Sannolikhet, Konsekvens). $N_{konsekvens}$=868--872. $N_{riskuppfattning}$=847. *Källa*: Medborgarpanelen 2022.

Tabell B2 Effekten av bakgrunds-, socio-ekonomiska faktorer, förtroende- och tillitsfaktorer på olika riskuppfattningar (ostandardiserad regressionskoefficient b-värde, samt signifikans p-värde)

	Krig…	*Cyber-attack…*	*Större olycka…*	*Terror-dåd…*	*Skogs-brand…*	*Pandemi…*
Kön	-0,08*	-0,20***	-0,21***	0,15***	-0,22***	-0,17***
Ålder	-0,18***	-0,07*	-0,11**	-0,03	-0,07*	-0,05
Utbildning	0,07	0,00	-0,01	0,00	-0,05	0,00
Inkomst	0,08*	0,04	0,06	0,05	-0,03	-0,07
Förtr. kommunen	0,03	-0,04	0,01	-0,01	-0,06	-0,11**
Förtr. regeringen	-0,01	0,03	0,03	-0,10*	0,03	0,07
Tillit andra i allm.	0,01	0,02	0,11*	-0,05	0,04	0,04
Tillit andra i omr.	0,02	-0,04	-0,13**	-0,03	-0,01	-0,11*
R^2	0,05	0,04	0,06	0,03	0,05	0,05
Antal svarande	826	826	825	825	826	826

Kommentar: För frågans formulering och svarsalternativ se tabell B1. * p<.05; ** p<.01; ***p<.001. Kön (1=Kvinna, 2=Man), Ålder (Under 30år=1…6=70 år eller äldre), Utbildning (1…4), Inkomst (1...3), Förtroende för din kommun (1…4), Förtroende för regeringen (1…4), Mellanmänsklig tillit i allmänhet (1…7), Mellanmänsklig tillit i området där man bor (1…7). *Källa*: Medborgarpanelen 2022.

Tabell B3 Effekten av bakgrundsfaktorer, förtroende- och tillitsfaktorer på tilliten till den egna förmågan att hantera situationen i scenariot om det skulle hända idag (ostandardiserad regressionskoefficient b-värde, samt signifikans p-värde)

	Tilliten till den egna förmågan
Kön	0,09**
Ålder	-0,09**
Utbildning	0,00
Inkomst	0,12***
Förtroende för kommunen	0,00
Förtroende för regeringen	-0,07
Tillit till andra människor i allmänhet	0,03
Tillit till andra människor i området där jag bor	0,13*
R^2	0,05
Antal svarande	826

Kommentar: Frågans formulering: *Om du utgår från IT attackerna i scenariot, vilken tillit har du till din egen förmåga att kunna klara dig utan allvarliga skador?* Svarsalternativen i fallande ordning var: ”Ingen tillit alls”; ”Ganska låg tillit”; ”Ganska hög tillit”; Mycket hög tillit”. * p<.05; ** p<.01; ***p<.001. Kön (1=Kvinna, 2=Man), Ålder (Under 30år=1…6=70 år eller äldre), Utbildning (1…4), Inkomst (1…3), Förtroende för din kommun (1…4), Förtroende för regeringen (1…4), Mellanmänsklig tillit i allmänhet (1…7), Mellanmänsklig tillit i området där man bor (1…7). *Källa*: Medborgarpanelen 2022.

Tabell B4 Effekten av bakgrundsfaktorer, förtroende- och tillitsfaktorer samt riskuppfattningar på medborgarnas beredskap att vidta åtgärder inför en cyberkris (ostandardiserad regressionskoefficient b-värde, samt signifikans p-värde)

	Modell 1	*Modell II*
Kön	-0,04	-0,04
Ålder	0,04	0,08
Utbildning	0,00	0,00
Inkomst	-0,04	-0,08**
Förtroende för kommunen	-0,01	0,01
Förtroende för regeringen	0,04	0,05
Tillit till andra människor i allmänhet	-0,02	-0,01
Tillit till andra människor i området där jag bor	0,05	0,01
Tillit till min egen förmåga	-	0,40***
Riskuppfattning, sannolikhetsbedömning	-	0,10**
Riskuppfattning, konsekvensernas allvar	-	0,12***
R^2	0,00	0,17
Antal svarande	824	813

Kommentar: Frågans formulering*: I vilken utsträckning är du beredd att förbereda dig inför IT-attacker likt dem i scenariot?* Svarsalternativen i fallande ordning var: ”I mycket liten utsträckning”; ”I ganska liten utsträckning”; ”I ganska stor utsträckning”; I mycket stor utsträckning”. * p<.05; ** p<.01; ***p<.001. Kön (1=Kvinna, 2=Man), Ålder (Under 30år=1…6=70 år eller äldre), Utbildning (1…4), Inkomst (1...3), Förtroende för din kommun (1…4), Förtroende för regeringen (1…4), Mellanmänsklig tillit i allmänhet (1…7), Mellanmänsklig tillit i området där man bor (1…7), Riskuppfattning sannolikhet (1…4), Tillit till egen förmåga (1…4), Riskuppfattning konsekvensernas allvar (1…4). *Källa*: Medborgarpanelen 2022.

Tabell B5 Effekten av bakgrundsfaktorer, förtroende- och tillitsfaktorer på åtgärdsdimensionen att rusta materiellt, att medvetandegöra och att värdera relationer, som medborgarna är beredda att vidta (ostandardiserad regressionskoefficient b-värde, samt signifikans p-värde)

	Att rusta materiellt	*Att medvetande-göra*	*Att värna relationer*
Kön	-0,10**	0,04	-0,08*
Ålder	0,07*	0,06	-0,06
Utbildning	0,01	0,13***	0,00
Inkomst	0,08	0,04	0,01
Förtroende för kommunen	-0,06	-0,02	0,03
Förtroende för regeringen	0,02	0,12**	0,09*
Tillit till andra människor i allmänhet	-0,09	-0,01	0,07
Tillit till andra människor i området	0,10	-0,06	0,06
R^2	0,02	0,02	0,03
Antal svarande	825	825	825

Kommentar: Åtgärdsdimensionerna ovan bygger på ett index av 10 utvalda åtgärder som ställdes (Fråga: *Vilka av följande åtgärder är du beredd att vidta för att förbereda dig inför IT-attacker likt dem i scenariot? Flera alternativ kan kryssas i*. Svarsalternativen var i fallande ordning: ”Ta reda på information om vilka de lokala hoten och riskerna är och hur man kan skydda sig”, ”Skriva en att-göra-lista med en plan för hushållet som beskriver i vilken ordning och hur man ska agera”, ”Samla ihop en krisberedskapslåda (vatten, mat, batteridriven radio etc.)”, ”Ha extra mediciner hemma”, ”Ha tillgång till extra bränsle eller drivmedel”, ”Ha kontanter hemma som räcker för att klara mig i flera veckor”, ”Ha goda relationer till grannar och näringsidkare i mitt närområde för utbyte av varor och tjänster”, ”Ha flera bankkort med olika utgivare, samt kredit på någon av dessa”, ”Ha en större summa kontanter hemma som jag kan låna ut till närmaste grannar”, ”Hjälpa andra genom att inte hamstra förnödenheter”. Fritextsvaret ”Andra sätt:_____”, samt ”⊗Jag är inte beredd att vidta några åtgärder” ingår inte i indexen. De tre dimensionerna: Att rusta materiellt; Att medvetandegöra; respektive Att värna relationer, är medelvärdesindex baserade på svarsalternativen grupperade enligt tabell 5. * p<.05; ** p<.01; ***p<.001. Kön (1=Kvinna, 2=Man), Ålder (Under 30år=1…6=70 år eller äldre), Utbildning (1…4), Inkomst (1...3), Förtroende för din kommun (1…4), Förtroende för regeringen (1…4), Mellanmänsklig tillit i allmänhet (1…7), Mellanmänsklig tillit i området där man bor (1…7). *Källa*: Medborgarpanelen 2022.

Arbetsrapporter från Institutionen för journalistik, medier och kommunikation (2001-)

1. Annika Bergström & Ingela Wadbring (2001) Medierna i vardagslivet. En metodologisk skiss över hur det är möjligt att använda dagböcker som insamlingsmetod i medieforskningen.
2. Kent Asp & Magnus Fredriksson (2001) Bilavgaserna och den allmänna opinionen. Åsikter och handlingsberedskap.
3. Tomas Andersson Odén (2002) 2001 års publicistiska bokslut. En rapport om 36 tidningars bokstäver - i siffror.
4. Gabriella Sandstig (2002) Organisation och kön. En strategisk litteraturöversikt av ämnesområdena organisation och kön applicerat på forskningsprojektet ”Kvinnorna i journalistkulturen”.
5. Therese Eriksson (2002) Gratistidningsmarknaden i Sverige 2001.
6. Rudolf Antoni (2002) Publikens publik. Aktuell forskning kring användning och värdering av medier.
7. Rudolf Antoni & Therese Eriksson (2002) Läsvanestudien. En tabellrapport.
8. Gabriella Sandstig (2003) Orons platser. En granskning av människors upplevelser av rädsla och otrygghet.
9. Tomas Andersson Odén (2003) 2002 års Publicistiska bokslut. Del 1 Om tidningars redaktioner och innehåll.
10. Ingela Wadbring (2003) 2002 års Publicistiska bokslut. Del 2 Om läsares och medarbetares syn på tidningar.
11. Tomas Andersson Odén & Ingela Wadbring (2003) Teknisk rapport för publicistiska bokslut.
12. Mariann Björkemarken (2003) Jönköpings Lokal-TV Förening. Utvecklingen av en lokalTVverksamhet.
13. Kent Asp (2003) Medieval 2002 - partiskheten och valutgången. En studie av valrörelsens medialisering.
14. Petra Sintorn (2003) Publicistiska bokslut - hyllvärmare eller redskap för förändring?
15. Oscar Westlund (2003) Betala för nyheter på internet?
16. Bengt Johansson, Lisa Henricsson & Annelie Karlsson (2003) Hur farligt är Göteborg? Risker i GP:slokalnyheter.
17. Gabriella Sandstig (2004) Att undersöka otrygghet - en metodstudie.

18. Tomas Andersson Odén (2004) 2003 års Publicistiska bokslut. Del 1 Om tidningars redaktioner och innehåll.
19. Ulrika Andersson (2004) 2003 års Publicistiska bokslut. Del 2 Sportens olika sidor: männens och de manliga sporternas revir.
20. Josefine Sternvik (2004) Ögonrörelser och dagstidningsläsning - en forskningsöversikt.
21. Valpuri Mäkinen (2004) En tidning för alla? Om invandrares användning av och attityder till medier i allmänhet och dagstidningar i synnerhet.
22. Eva Berglie (2004) Jakten på lycka. En teoriutvecklande studie av tredjepersonseffekten.
23. Åsa Nilsson (2004) Mediersräckvidd. En Jämförelse av mätmetoder och undersökningar.
24. Oscar Westlund (2004) www.lokaltidning.se . Prenumeranters attityder till sin lokaltidning och nättidningsläsning.
25. Karin Fogelberg (2005) Media Literacy. En diskussion om medieundervisning.
26. Mira Öhlin (2005) Fågel, fisk eller... Om klassresenärers medievanor.
27. Tomas Andersson Odén (2005) 2004 år publicistiska bokslut. Om tidningars redaktioner och innehåll.
28. Anna Maria Jönsson (2005) Mångfalden i journalistkåren - studier av social Sammansättning, samhällssyn och nyhetssyn i den svenska journalistkåren.
29. Tomas Andersson Odén (2005) President Chavez i press, radio och TV. Mediebevakningen av folkomröstningskampanjen iVenezuela, augusti 2004.
30. Ulrika Andersson (2005) Journalister och deras läsare. En studie av tidningsjournalisters syn på läsare ochläsarundersökningar.
31. Ulrika Andersson, Ingela Wadbring (2005) I gratistidningsland.
32. Carl Bergholtz, Johan Olsson (2005) Unga dagstidningsläsare i ny mediesituation.
33. Åsa Nilsson, Lennart Weibull, Annette Hill (2005) Synen på icke-fiktion i TV.Resultatredovisning.
34. Ulrika Andersson (2005) Nya svenskar och svenska medier.
35. Ulf Wallin, Johannes Bjerling, Christoffer Lärkner (2006) Barnen i nyheterna om tsunamin. En studie av mediernas rapportering under första månaden.
36. Oscar Westlund (2006) Media and Communication studies in Sweden. Disciplinary Boundary Construction - a theoretical contribution to Theory of Science.
37. Oscar Westlund (2006) Känslor av medieförtroende.
38. Kent Asp (2006) Journalistkårens partisympatier.
39. Jonas Ohlsson (2006) Partiernas press .

40. Ulrika Hedman (2006) Har ni nåt webbigt? En fallstudie av Göteborgs-Postens flerkanalspublicering: Redaktionell organisering och arbetsrutiner, nyhetsvärde samt medielogik.
41. Anna Bolin (2006) In whose interest? A journalists`view of their responsibilities and possibilities within the mainstream press in Sri Lanka.
42. Kent Asp (2006) Rättvisa nyhetsmedier. Partiskheten under 2006 års medievalrörelse.
43. Marina Ghersetti (2007) Bilden av funktionshinder. En studie av nyheter i Sveriges Television.
44. Malin Dellgran (2007) Konsten att förhandla. Om journalister i en kommersiell tv-kultur.
45. Johannes Bjerling (2007) Partiledarutfrågningarna i SVT 2006.
46. Ulrika Andersson (2007) Fokus på unga vuxna. Sociala förändringar och växande medieutbud skapar nya medievanor bland unga.
47. Oscar Westlund (2007) Mobiltelefonianvändning. En forskningsöversikt.
48. Jonas Ohlsson (2007) Göteborgsakademiker 2006. Medieinnehav och medieanvändning bland unga högutbildade.
49. Ingela Wadbring (2007) Från annonsblad till tidningar. Decenniers utveckling av lokala gratistidningar.
50. Oscar Westlund (2007) Mobiltelefonen som multimedium och nyhetsmedium. Ett användarperspektiv.
51. Gabriella Sandstig (2007) Förtroendet för polisen. En analys av medborgarnas syn på polisen och dess roll i samhället 1986 - 2006.
52. Sandra Byström, Björn Danielsson, Bengt Johansson (2007) Regionala TV□nyheter i medielogikens tid. En studie av Västnytts bevakning av Västra Götalandsregionen.
53. Mathias A Färdigh (2008) Mediesystem i Europa. En studie av de europeiska ländernas mediesystem utifrån ett användarperspektiv.
54. Tomas Andersson Odén, Johannes Bjerling (2008) A-press med borgerliga ägare.
55. Therese Blomqvist, Maja Norin (2009)”Sjuning, åttning, nining, tidning!” Förskolebarns föreställningar om dagstidningen.
56. Ulrika Hedman (2009) Läsarmedverkan: Lönande logiskt lockbete. Nättidningarnas användarskapade innehåll ur ett redaktionellt ledningsperspektiv.
57. Magnus Ekström, Björn Granstrand (2009) Dagstidningen på 3,5 tum? En nutids- och framtidsstudie av svensk dagspress förhållande till mobila tjänster.

58. Johan Cedersjö, Roger Gustavsson (2009) Hot eller möjlighet? En kvantitativ studie av svenska landsortsbaserade dagspressjournalisters inställning till användarskapat innehåll.
59. Marina Ghersetti (2009) Personer med invandrarbakgrund i SVTs nyhetsprogram. En innehållsanalys av Rapport, Aktuellt, Sportnytt och Kulturnyheterna 2001.
60. Marina Ghersetti (2009) Terrorattackerna i USA. Sveriges Radios rapportering om den 11 september 2001.
61. Monica Löfgren Nilsson (2009) Kvinnor, män och nyheter i televisionen. En innehållsstudie av ämnen och källor under 45 år.
62. Johannes Bjerling, Jonas Ohlsson (2010) En introduktion till logistisk regressionsanalys.
63. Diana Jacobsson (2010) Viruset och vaccinet. En undersökning av pressens rapportering kring vaccinationen i samband med svininfluensan 2009.
64. Marina Ghersetti, Tomas A. Odén (2010) Snöovädret i medierna vintern 2009- 2010.
65. Marina Ghersetti (2011) Olika men ändå lika. Rapporteringen om riksdagsvalet 2010 i fem stora pappers- och webbtidningar.
66. Mira Hjort, Signe Oskarsson, Madelene Szabó (2011) Jättekliv eller tidsfördriv. En studie i hur svenska journalister använder sociala medier som arbetsverktyg.
67. John Rejnäs, Martin Gunséus (2011) GP.se - om publiken själv får välja. En studie i publikens delningsvärdering.
68. Carl Malmer (2012) Professionell men personlig. En publikstudie av läsares uppfattningar om journalisters aktivitet på twitter.
69. Ingrid Lord (2013) Institutioners organisatoriska lärande från samhällskriser. En studie av redaktioner, myndigheter och resebyråer i samband med tsunamivarningen 2012.
70. Magnus Fredriksson, Josef Pallas (2014) Den medialiserade myndigheten. En analys av svenska myndiheters anpassningar till medielogiken.
71. Anna Erwander, Hugo Lindkvist (2014) ”Det här var dagen då anonyma tonåringar via sociala medier startade ett upplopp i Göteborg”. En studie över gestaltningen i fyra svenska tidningar av gatuoroligheterna i samband med ”Instagramhändelserna” i Göteborg i december 2012.
72. Martin Spaak (2015) Falska larm och äkta stormar. En studie av allmänhetens syn på myndigheter och medier i sambandmed SMHI:s varning inför stormen Simone 2013.
73. Maria Edström, Josefine Jacobsson (2015) Räkna med kvinnor. Global Media Monitoring Project. Nationell rapport Sverige.
74. Maria Jervelycke Belfrage (2016) Både slumpmässig och planerad. Ungas nyhetskonsumtion i sociala medier.

75. Monica Löfgren Nilsson (2017) Journalisternas trygghetsundersökning. Journalisters utsatthet under 2016.
76. Maria Jervelycke Belfrage (2018) ”Om jobb och bostäder och hur det ligger till i andra länder - det är ju det man vill veta mer om”. En studie om ungas behov av nyheter och samhällsinformation i den digitala medieekologin.
77. Magnus Fredriksson, Daniel Lövgren, Josef Pallas (2018) Bortom uppdraget. En analys av svenska myndigheters kommunikationsaktiviteter under Almedalsveckan.
78. Maria Jervelycke Belfrage (2018) Tvåstegshypotesen och teorin om opinionsledare – i en ny och snabbt föränderlig medieekologi.
79. Magnus Fredriksson, Mathias Färdigh, Anton Törnberg (2018) Den kommunikativa blicken. En analys av principerna för svenska kommuners kommunikationsverksamheter.
80. Orla Vigsö (2019) Satirteckningar i svensk dagspress 1890-2017.
81. Magnus Fredriksson, Christian Mossberg (2020) En fråga om tillgång, kvalité och arbetsvillkor. Mediebilden av äldreomsorgen i fyra svenska lokaltidningar.
82. Jacob Sohlberg, Bengt Johansson (2020) “Uppgifterna om det misstänkta knivdådet är ännu osäkra…” Ett experiment om användandet av journalistiska osäkerhetsmarkörer.
83. Tim Segerberg (2020) Det motståndskraftiga förtroendet. Kriser och institutionellt förtroende i Sverige 1986-2017.
84. Peter Esaiasson, Bengt Johansson, Marina Ghersetti & Jacob Sohlberg (2020) Kriskommunikation och segregation i en pandemi – hur boende i utsatta områden informerade sig om coronaviruset våren 2020.
85. Ulla Carlsson (2020) Yttrandefrihet och medier i en orostid. Anteckningar inför Pressfrihetsdagen den 3 maj 2020.
86. Magnus Fredriksson (2021) Att (re)presentera staten. En analys av svenska myndigheters märken och logotyper 1974–2019.
87. Maria Edström & Josefine Jacobsson (2021) Räkna med Kvinnor 2020. Global Media Monitoring Project 2020. Nationell rapport Sverige.
88. Peter M. Dahlgren (2021) Medieinnehåll och mediekonsumtion under coronapandemin. Datoriserade metoder för insamling och analys av stora mängder text- och mediedata.
89. Bengt Johansson, Jesper Strömbäck, Sofia Johansson & Felix Andersson (2022) Sårbarhet för informationspåverkan.
90. Ulrika Andersson (2023) JOURNALIST ’18. Huvudresultat från den svenska journalistundersökningen.
91. Orla Vigsö (2024) Den politiska marknaden. Politisk sociologi som ram för analys av partipolitisk kommunikation.

92. Bengt Johansson, Sofia Johansson, Pavel Rodin & Alice Srugies (2024) Falsk och missvisande information i sociala medier under samhällskriser.
93. Aikaterini Roka (2025) Far-Right Populist Rhetoric: Gendered Enemy Construction and Performative Masculinity.