Försvarshögskolan

Kriget i informationsmiljön

Om rysk informationskrigföring, organisatorisk resiliens och samverkan

---

War in the information environment

On Russian information warfare, organizational resilience and collaboration

Amanda Rönnkvist

VT 2024

Ledarskap och ledning för försvar, krishantering och säkerhet

Masteruppsats - ledarskap och ledning (30 hp)

Handledare: Sofia Nilsson

Examinator: Erik Berntsson

Innehållsförteckning

Sammanfattning

Informations- och kommunikationsteknologins snabba utveckling har resulterat i djupgående förändringar i Rysslands förståelse av krigföring, där informationskrigföring betraktas som en central del i landets säkerhetspolitiska arsenal. Sverige och svenska intressen har regelbundet varit måltavla för illasinnad informationspåverkan som en del av den ryska informationskrigföringen, och de riktade aktiviteterna väntas fortgå även under kommande år. Syftet med den här studien är att, genom en explorativ ansats med semistrukturerade intervjuer, bidra till fördjupad kunskap om rysk informationskrigföring i den svenska kontexten. Genom att studera organisatorisk resiliens och samverkan i förhållande till illasinnad informationspåverkan har studien sökt svar på vilka utmaningar svenska myndigheter upplever att de ställs för kopplat till rysk informationskrigföring, samt vilka strategier som anses gynnsamma för att motverka utmaningarna.

Empirin utgjordes av sju individuella, semistrukturerade intervjuer, vilka analyserades med induktiv tematisk analys. Resultaten kan sammanfattas i fyra teman: "restriktivitet eller transparens", "misstro eller tillit", "negligera eller förvänta" samt "isolering eller samverkan". Studiens slutsats är att myndigheter utan förväntningar om illasinnad informationspåverkan och med misstro från allmänheten, initialt tenderar att sluta sig och reagera med restriktivitet och isolering. Organisationer som istället förväntar sig att utsättas för illasinnad informationspåverkan och som har hög tilltro från allmänheten, kan framgångsrikt bibehålla transparens och god interorganisatorisk samverkan.

Nyckelord: Rysk informationskrigföring, illasinnad informationspåverkan, desinformation, organisatorisk resiliens, samverkan

Abstract

The rapid development of information and communication technologies has resulted in profound changes in Russia's understanding of warfare, with information warfare being considered a key part of its security policy arsenal. Sweden has regularly been targeted for malicious information influence as part of Russian information warfare, and the targeted activities are expected to continue in the coming years. The aim of this study is to contribute to the knowledge of Russian information warfare in the Swedish context through an exploratory approach with semi-structured interviews. By studying organizational resilience and collaboration in relation to malicious information influence, the study has sought answers to what challenges Swedish authorities perceive they face in relation to Russian information warfare, as well as what strategies are considered beneficial to counteract the challenges.

The empirical data consisted of seven individual, semi-structured interviews, which were then analyzed using inductive thematic analysis. The results show that challenges and favorable coping strategies can be summarized in the themes "restrictiveness or transparency", "distrust or trust", "neglect or expect" and "isolation or collaboration". The study concludes that authorities without expectations of malicious information influence and experiencing distrust from the public, initially tend to react with restrictiveness of information and isolation from other authorities. Organizations that do expect to be exposed to malicious information influence and that have high public trust can successfully maintain transparency and good inter-organisational cooperation.

Keywords: Russian information warfare, malign information influence, disinformation, resilience, inter-organizational cooperation

Förord

Ett stort tack riktas till var och en av er som på ett eller annat sätt har bidragit till arbetet i denna studie. Tack till alla ni som valt att ställa upp som respondenter och som bidragit med värdefulla perspektiv inom ett spännande och aktuellt ämnesområde. Att få ta del av era erfarenheter har varit både fängslande och inspirerande. Ert engagemang och viljan att bidra till ett bättre samhälle är otvivelaktigt, vilket är både beundransvärt och betryggande.

Tack till Sofia Nilsson för din genomgående varma tillgivenhet och betydelsefulla råd. Du har uppvisat en nyfikenhet, välvilja och hjälpsamhet utöver det vanliga, vilket har varit oerhört uppskattat under arbetets gång. Tack för din tid, din pedagogik och alla värdefulla lärdomar jag fått ta del av. Ett stort tack riktas även till Försvarshögskolan för givande studier inom området för försvar, krishantering och säkerhet. Med tanke på rådande säkerhetsläge kan jag inte föreställa mig ett bättre lärosäte att avhandla en masterexamen hos.

Avslutningsvis vill jag även tacka Patrik för allt stöd och engagemang du så hängivet och osjälviskt bidragit med. Vetskapen om att det finns människor med din ärlighet, genuinitet och kunskap, har gjort att jag betraktar mitt kommande yrkesliv med en stor dos spänning och förväntan. Tack!

Amanda Rönnkvist

27 maj 2024

Stockholm

Inledning

En orolig omvärld påverkar säkerhetsläget i Sverige och det allvarliga läget väntas bestå under en längre tid. Hotbilden mot Sverige är komplex och flera hot som terrorhot, cyberangrepp och andra länders underrättelseverksamhet överlappar och förstärker varandra. I början av 2024 presenterades Ryssland som det största hotet mot Sveriges säkerhet (Säkerhetspolisen, 2024). Rysslands säkerhetshotande verksamhet bedrivs på en bred front och inbegriper en mängd aktiviteter som bland annat underblåser splittring och polarisering. Informations- och kommunikationsteknologins snabba utveckling har resulterat i djupgående förändringar i Rysslands förståelse av krigföring, där informationskrigföring betraktas som en central del av landets säkerhetspolitiska arsenal (Hellman, 2021; Jonsson, 2019).

Användningen av information som ett vapen tillåter genomförandet av militära aktioner utan att behöva använda militär makt, på praktiskt taget vilken arena som helst (Jonsson, 2019). Med avsikten att påverka en motståndares val och beslut för att gagna det egna landets militära och strategiska vinst, drar Ryssland nytta av den stora mängden lättillgänglig information genom ett brett spektrum av aktiviteter och processer (Nilsson et al., 2022; Palmertz, 2021; Giles, 2016). Aktiviteterna är inte begränsade till krigstid, utan pågår kontinuerligt under fredstid och oberoende av relationen till motståndaren (Giles, 2016).

Sverige har i allt högre grad varit föremål för ett brett spektrum av ryska aktiviteter sedan 2014 (Kragh & Åsberg, 2017). Desinformation, förfalskade telegram och falska nyheter har dykt upp i det svenska informationslandskapet, där ryska politiker och diplomater har engagerat sig i svenska inrikespolitiska frågor om NATO och Östersjöns säkerhet. Kremlvänliga icke-statliga organisationer och icke-statliga organisationer som drivs av staten

har kommit att verka innanför Sveriges gränser, och rysk statlig TV har utmålat svenska politiker som Washingtons agenter (Kragh & Åsberg, 2017). Svenska journalister och diplomater som arbetar i Ryssland har utsatts för trakasserier och spionage. Därutöver finns exempel på aktörer i Sverige, såsom politiker, akademiker och tidningar, som medvetet eller omedvetet spelar en roll som påverkansagenter eller förmedlare av desinformation (Kragh & Åsberg, 2017). Sverige och svenska intressen har regelbundet varit måltavla för riktade aktiviteter, och den illasinnade informationspåverkan som del av Rysslands informationskrigföring väntas fortgå även under kommande år (Wagnsson, 2023; Giles, 2023). Chefer på olika nivåer inom svenska organisationer kommer att ställas inför utmaningar kopplat till rysk illasinnad informationspåverkan, varför det blir nödvändigt att implementera hanteringsstrategier. Att stärka organisatorisk resiliens för att motverka hotet är således av relevans för området för ledarskap och ledning, eftersom det är en central uppgift för ledare inom svenska myndigheter och organisationer.

Tidigare forskning

Under de senaste åren har det genomförts ett flertal viktiga studier i relation till hotet från rysk informationskrigföring. Wagnsson (2023) har genomfört en värdefull studie om hur Rysslands statligt sponsrade illasinnade informationspåverkan sprids över landsgränserna genom internationella medier, och hur det orsakar polarisering och underminerar förtroende, medier och demokrati. Hellman (2021) publicerade en studie om hur Ryssland använt covid-19 pandemin för att sprida ett negativt narrativ om Sverige i det statligt kontrollerade nyhetsmediet Sputnik. Inom området för desinformation bidrog Dowse och Bachmann (2022) med värdefulla insikter kopplat till hur desinformation används inom hybridkrigföring, samt motstrategier som kan användas för att hantera utmaningen.

Vidare finns en del forskning om hanteringsstrategier för informationspåverkan. Hellman och Wagnsson (2017) publicerade en artikel som föreslår olika strategier som demokratiska regeringar kan använda för att bemöta rysk informationskrigföring. Studien undersöker även hur strategierna överensstämmer med demokratiska värderingar, samt hur de kan bidra till att destabilisera eller stabilisera säkerhetsmiljön. Pamment, Northhaft, Agardh-Twetman och Fjällhed (2018) publicerade en omfattande rapport om både olika former av informationspåverkan, samt metoder och strategier för att motverka påverkansoperationer. Därutöver demonstrerade även Lei (2019) hur informationskrigföring kan brytas ner i nyckelkomponenter för att förstå och förebygga problemet.

Bortsett från de studier som belyser hotet från Ryssland, finns även en mängd studier som framhåller utmaningar inom det svenska beredskapssystemet, vilket skulle kunna försvåra arbetet att motverka rysk informationspåverkan. Degerman (2021) visade hur svenska offentliga organisationers ledningsdesign hämmade anpassningar efter förändrade förhållanden, samt att offentliga ledningar hindras från att skapa kännedom för organisationsstruktur och övergripande mål. Problemen påverkade organisationernas resilienta förmåga negativt. Därutöver har bland annat Deverell, Alvinius och Hede (2019) problematiserat samverkansprincipen genom att publicera två artiklar som visar hur flera faktorer påverkar interorganisatorisk samverkan i krissituationer. Artiklarna belyste hur vissa myndigheter får högre upplevd status vid krissituationer, medan andra myndigheter exkluderas från samverkan. Slutligen publicerade Ekengren, Engström och Rhinard (2021) en studie om hur Sverige misslyckades att agera under covid-19 pandemins tidiga skeden, vilket ledde till att pandemin utvecklade sig till en smygande kris.

Således demonstrerar tidigare forskning att det finns ett flertal studier om hur hotet från Ryssland och informationskrigföring yttrar sig, samt hur olika strategier kan användas för att motverka hotet. Ett antal studier belyser även befintliga brister inom det svenska krishanteringssystemet vid kriser som inträffat under de senaste åren, i synnerhet i samband med samverkan, vilket skulle kunna försvåra hantering av illasinnad informationspåverkan. Det finns emellertid fortfarande begränsad forskning i en svensk kontext som undersöker aktiviteter kopplade till rysk informationspåverkan gentemot Sverige och svenska intressen i syfte att gagna den egna agendan. Ryssland har en differentierad inställning till enskilda europeiska stater, vilket innebär att aktiviteter kopplat till informationspåverkan gentemot olika länder inte nödvändigtvis är detsamma (Kragh & Åsberg, 2017). Därutöver finns ett behov av forskning som fördjupar kunskapen om hur organisationer i Sverige arbetar i praktiken för att motverka och hantera Rysslands aktiviteter kopplat till illasinnad informationspåverkan.

Syfte och frågeställningar

Mot bakgrund av detta är det övergripande syftet med förevarande studie att, genom en explorativ ansats med semistrukturerade intervjuer, bidra till fördjupad kunskap om rysk informationskrigföring i den svenska kontexten. Även om det existerar tidigare forskning om illasinnad informationspåverkan, är forskningen i en svensk kontext begränsad. Mer specifikt avser studien undersöka både myndigheter som arbetar aktivt inom det svenska krishanteringssystemet, samt myndigheter som utsatts för rysk informationskrigföring - för att bidra till en fördjupad kunskap om organisatorisk resiliens och samverkan i förhållande till illasinnad informationspåverkan. Studien ämnar således besvara följande frågeställningar:

- Vilka utmaningar kan myndigheter uppleva i Sverige att de ställs inför kopplat till rysk informationskrigföring?
- Vilka strategier kan svenska myndigheter anse vara gynnsamma för att motverka utmaningar kopplat till rysk informationskrigföring?

Studien har avgränsats i flera hänseenden, däribland att fokusera på rysk informationskrigföring, illasinnad informationspåverkan och desinformation. Olika aktörer använder olika strategier och metoder för informationspåverkan, varför studien begränsats till Ryssland som hotaktör. Eftersom rysk informationskrigföring syftar till att polarisera samhällen, är det vanligt att just samhälleliga institutioner blir måltavla för illasinnad informationspåverkan. Av den anledningen har studien avgränsats till att intervjua respondenter som arbetar på myndigheter. Rapportens efterföljande disposition inleds med centrala teoretiska begrepp, följt av undersökningsmetod, resultat, diskussion samt avslutning.

Centrala teoretiska begrepp

Nedan följer en genomgång av studiens centrala teoretiska begrepp som anses nödvändiga för att få en förståelse för forskningsområdet. Avsnittet bör inte betraktas som ett teoretiskt ramverk, utan det finns en enorm begreppsapparat inom området, varför det är nödvändigt att redogöra för teoretiska utgångspunkter.

Informationsmiljön

De sammanflätade relationerna mellan information, teknik och aktörer utgör tillsammans den så kallade informationsmiljön (Nilsson et al., 2022). I dagsläget skapas och sprids ny

teknologi innan dess samhälleliga och politiska konsekvenser förstås helt, vilket medför att informationsmiljön i hög grad karaktäriseras av en snabb och oberäknelig teknisk utveckling. I takt med att informationsmiljön i allt större utsträckning domineras av komplex och snabbt föränderlig digitalisering, har informationsmiljön blivit svårnavigerad. Nya former av relationer mellan aktörer, data och information har utvecklats. Forskning, regler och lagar blir snabbt föråldrade och gränser luckras upp - både geografiska gränser, gränserna mellan statliga och privata aktörer, samt konceptuella gränser mellan krig och fred (Nilsson et al., 2022). Däremot påverkas den enskilde användarens uppfattning om informationsmiljön av de tekniska, geografiska och kontextuella gränser som denne är bunden till.

Hur förstås det ryska hotet?

Sveriges centrala krishanteringsaktörer definierar hotet från Ryssland med en mängd olika begrepp. Kombinationen av militära och icke-militära medel för att uppnå specifika mål i specifika situationer benämns av Must som icke-linjär krigföring, medan Försvarsberedningen och Försvarsmakten använder begreppet hybridhot för att beskriva samma fenomen (Appelgren et al., 2020). Begreppen beskriver en bred hotbild som inkluderar diplomatiska aktiviteter, militära operationer, informationsoperationer och ekonomiska medel, vilka kombineras och skräddarsys utifrån den specifika måltavlan. Eftersom den ryska hotbilden är väldigt omfattande har avgränsningar varit nödvändiga för att generera ett mer träffsäkert resultat.

Regeringen använder primärt begreppet påverkanskampanjer för att beskriva sammanhängande, centralt styrda organisationer som nyttjar ett brett spektrum av maktmedel för att åstadkomma en så stor effekt som möjligt (Appelgren et al., 2020).

Påverkanskampanjer kan således pågå under en längre tid genom ett flertal aktiviteter. Ett smalare begrepp är påverkansoperationer, som av Must och Säpo definieras som en statsaktörs synkroniserade och förnekbara verksamhet som främst innefattar spridning av missledande eller felaktig information (Appelgren et al., 2020). Påverkansoperationer är således konkreta aktiviteter som sker inom ramen för en påverkanskampanj. Området för påverkan omfattar en mängd olika påverkansaktiviteter för att influera individer, grupper och befolkningar. Den här studien avgränsas ytterligare till att enbart behandla informationsarenan, vilket föranleder en introduktion av begreppen informationskrigföring, illasinnad informationspåverkan och desinformation.

Informationskrigföring, illasinnad informationspåverkan och desinformation

Informationskrigföring kan beskrivas som en del av Rysslands förståelse av krig (Jonsson, 2019). Begreppet handlar om en aktörs medvetna manipulation eller användande av information mot en motståndare, med avsikten att påverka demokratiska val och beslut för att gagna militär eller strategisk vinst (Nilsson et al., 2022). Begreppet inkluderar användandet av information som ett verktyg, en måltavla, och som ett verksamhetsområde, vilket omfattar en mängd olika aktiviteter och processer (Giles, 2016). Vidare definieras informationskrigföring generellt utefter aktiviteternas avsedda effekt, där man eftersträvar påverkan och förändring hos målgruppens kunskap och tro om sig själva och sin omvärld (Nilsson et al., 2022). Syftet är att förändra och påverka målgruppens beteenden, vilket inte är begränsat till krigstid, utan även pågår under fredstid och oberoende av relationen till motståndaren (Giles, 2016). Informationskrigföring syftar till långsiktighet och lämpar sig väl för att beskriva Rysslands aktiviteter som en del av ett krig mot västvärlden. Sammantaget

anses informationskrigföring vara bäst lämpat att använda för att beskriva Rysslands långsiktiga aktiviteter i den aktuella studien.

Informationskrigföring utgörs av två komponenter: en teknisk och en psykologisk. Den tekniska aspekten inbegriper cyberoperationer, teleoperationer och elektronisk krigföring (Porche III, 2020). Aktiviteterna anspelar både på att attackera, försvara och skydda sig mot fienden. Den psykologiska förgreningen innefattar ovan definierade påverkansoperationer och informationspåverkan. Informationspåverkan handlar om maktutövning genom kommunikationsprocesser, vilket traditionellt sett haft en ideologisk prägel och varit en linjär företeelse, där avsändaren avser påverka en vidsträckt publik (Wagnsson, 2023). Begreppet inkluderar även den mottagande parten som dagligen utsätts för påverkan, både i positiv och negativ bemärkelse.

Den här studien kommer att fokusera på påverkan i negativ bemärkelse, då rysk informationspåverkan syftar till att försvaga motståndaren genom att splittra befolkningar och skada förtroendet för myndigheter, medier och demokratiska institutioner. Påverkan är interaktiv och beroende av att andra länders befolkningar sprider den vidare, samtidigt som olika budskap även kan anpassas till olika grupper (Wagnsson, 2023). Den illasinnade informationspåverkan kan belysas med begreppet “malign information influence”, vilken finansieras av auktoritära styren alternativt andra fientliga aktörer, och som sprids över nationsgränser (Wagnsson, 2023). Begreppet syftar till spridning av information med ett illasinnat uppsåt, vilket lämpar sig väl för den aktuella studien där det kommer att översättas till “illasinnad informationspåverkan”. En vanligt förekommande aktivitet inom illasinnad informationspåverkan är spridningen av desinformation, vilket innebär att information

medvetet skapas för att vilseleda, skada eller manipulera en person, en social grupp, en organisation eller ett land (Arce, 2024).

Rysslands illasinnade informationspåverkan drar nytta av den stora mängden lättillgänglig data genom många olika aktiviteter och processer för att stjäla, plantera, förbjuda, manipulera, förvränga eller förstöra information (Palmertz, 2021; Giles, 2016). Spridning av desinformation och budskap som underblåser och snedvrider den offentliga debatten i ett annat land är ett viktigt syfte. Ett land med interna stridigheter där politiker och allmänheten kämpar för att hitta gemensamma grunder, kommer ha lägre förmåga att begränsa och motverka den offensiva aktörens strategier och handlingar (Palmertz, 2021).

Den i det svenska informationslandskapet förekommande desinformationen visar att Ryssland besitter sofistikerad kunskap om svenska tjänstemän, diplomater och beslutsfattare (Kragh & Åsberg, 2017). Desinformationen förekommer även utanför det svenska informationslandskapet, exempelvis i rysk statstelevision, sociala medier och andra verktyg för masskommunikation. Till illustrativa exempel hör den ryska tidningen Sputniks artikel från 2015, som handlade om hur Sverige gjorde sig redo för att avfyra missiler mot ryska trupper från Gotland (Pamment et al., 2018). Det ursprungliga citatet spårades till en artikel från Sveriges Radio, där Gotlands landshövding berättade att det från Gotland var möjligt att avfyra missiler och försvara de fartyg som seglade mot St Petersburg. I artikeln togs citatet från sitt sammanhang och gav följaktligen intrycket att handla om svensk aggression mot Ryssland (Pamment et al., 2018). Senare publicerades en fransk version av artikeln som hävdade att en svensk tjänsteman påstått att Gotland är väl placerat för att bomba Ryssland, vilket gav ytterligare stöd till desinformationen.

Den aktuella studien kommer att avgränsas till att fokusera på Rysslands långsiktiga mål och strategier genom begreppet informationskrigföring, och dess enskilda aktiviteter genom begreppen illasinnad informationspåverkan och desinformation.

Organisatorisk resiliens som ett sätt att motverka informationspåverkan

Samhällets förmåga att upptäcka och motverka illasinnad informationspåverkan kallas för psykologiskt försvar (Andersson, 2023). På en organisatorisk nivå talar man om att stärka organisationens motståndskraft, eller organisatorisk resiliens. Organisatorisk resiliens handlar om en organisations förmåga att förutse potentiella hot, att effektivt hantera negativa händelser och att anpassa sig till förändrade förhållanden (Duchek, 2020). Förmågan att förutse potentiella hot inkluderar förmågan att observera och identifiera interna och externa händelseutvecklingar, samt förmågan att förbereda organisationen för oväntade händelser. Organisationer som bevakar omvärlden och har förmågan att identifiera tidiga signaler om kris kan reagera snabbt och således undvika eskalering (Duchek, 2020). Därutöver är det viktigt att organisationer förbereder sig för oväntade händelser genom att utveckla lämpliga återhämtningsplaner för kritiska verksamheter. Utbildningar och simuleringsövningar kan säkerställa att målen med planerna uppnås (Duchek, 2020).

Att effektivt hantera negativa händelser inbegriper både förmågan att acceptera ett problem och förmågan att utveckla och implementera lösningar för att hantera det (Duchek, 2020). Organisationer tenderar att förneka kritiska situationer i ett tidigt skede, vilket ofta medför att det tar för mycket tid att förstå och agera på dessa situationer. Att inte acceptera och hantera problem i ett tidigt skede kan medföra att de eskalerar till en kris, vilket bland annat visade sig under covid-19 pandemin. Den svenska regeringens misslyckande att agera under

pandemins första skeden gjorde att den utvecklade sig till en smygande kris (Ekengren et al., 2020). När en kris väl inträffar är det viktigt att skapa en gemensam förståelse för situationen inom organisationen, samt att vidta lämpliga åtgärder för att hantera situationen (Duchek, 2020). En viktig princip för att kollektivt förstå och hantera en kris är "bricolage", vilket handlar om förmågan att improvisera och lösa problem kreativt (Weick, 1993). Improvisation antas göra organisationer mindre sårbara eftersom det möjliggör en sammansättning av åtgärder som redan finns inom organisationens handlingsregister, till nya kombinationer. Det medför att om en viss åtgärd misslyckas i en krissituation, kan den ersättas med en ny åtgärd omedelbart (Duchek, 2020).

Organisatorisk resiliens inkluderar även förmågan att anpassa organisationen efter kritiska situationer, vilket handlar om organisatorisk utveckling och förmåga att undvika eller minska negativa konsekvenser av oväntade händelser i framtiden (Duchek, 2020). Förmågan att anpassa organisationen omfattar både reflektion och lärande, samt organisatorisk förändringsförmåga. Reflektion och lärande handlar om att reflektera över krissituationer och att inkorporera erhållna insikter i den befintliga kunskapsbasen. Organisationer kan också lära sig av incidenter och kriser som inträffat hos relaterade eller liknande organisationer (Duchek, 2020). För att därefter åstadkomma förändring behöver kunskapen omsättas till handlingar, vilket behöver genomsyra organisationens samtliga individuella delar. Det kräver god kompetens kopplat till organisationsförändringar. Precis som vid alla organisatoriska förändringar kan förändringar som sker till följd av kriser leda till olika typer av motstånd, vilket medför att organisatorisk anpassning även involverar behovet av att övervinna motstånd till förändring (Duchek, 2020).

Under flyktingkrisen 2015 uppvisade både icke-statliga organisationer, samt privata organisationer med betydelse för infrastrukturen, en god förmåga att anpassa sig för att nå övergripande mål, även då omständigheterna förändrades (Degerman, 2021). De faktorer som bidrog till organisationernas framgångar var förväntningar om att behöva hantera oväntade situationer, utrymme för flexibilitet i arbetsuppgifterna, främjande av autonomi hos personalen, samt en gemensam bild av problembeskrivningen och behoven på samtliga hierarkiska nivåer inom organisationerna (Degerman, 2021).

Offentliga organisationer med betydelse för infrastrukturen ställdes däremot inför utmaningar relaterat till organisationsdesign och offentlig styrning, vilket påverkade deras resilienta förmåga negativt (Degerman, 2021). Organisationsdesignen främjade inte anpassningar efter förändrade förhållanden, vilket medförde skillnader i anpassning mellan hierarkiska nivåer och roller. Medan den operativa personalen upplevde situationen som en kris och därmed ville anpassa organisationen, hade ledningen inte full insikt i den operativa verksamheten, och insåg därför inte behovet av att göra arbetsförändringar (Degerman, 2021). Sett till offentlig styrning är många offentliga organisationer vana vid att ständigt anpassa sin dagliga verksamhet på grund av skiftande politiska direktiv. Däremot får sällan den offentliga ledningen en chans att skapa förtrogenhet med strukturen och de övergripande målen, vilket medför hinder för autonomt arbete (Degerman, 2021).

I förevarande studie studeras organisatorisk resiliens utifrån interorganisatorisk samverkan mellan myndigheter, samt utifrån enskilda myndigheters hanteringsstrategier.

Hanteringsstrategier

Rysslands strävan efter att påverka och förändra målgruppers kunskap och tro om sig själva och sin omvärld tar sig uttryck i en mängd olika aktiviteter och processer, vilket gör det svårt att skilja på vad som hör till den vanliga politiska debatten och vad som är fientliga försök att manipulera den. Ett första steg för att motverka illasinnad informationspåverkan är därför att skapa en medvetenhet om vilka hot och sårbarheter man står inför, eftersom det skapar en förståelse för olika varningssignaler (Pamment et al., 2018). Genom att öka medvetenheten kan illasinnad informationspåverkan mildras, eftersom man skapar förtroende och legitimitet. När individen känner tillit till en organisation är den mindre benägen att tro på falsk eller manipulerad information (Pamment et al., 2018). När hot och sårbarheter har identifierats kan organisationen anta olika hanteringsstrategier för att förebygga och motverka illasinnad informationspåverkan och spridning av desinformation.

Samverkan

I Sverige är samverkan mellan myndigheter centralt för att upprätthålla organisatorisk resiliens. Samverkan kan definieras som olika aktörers samarbete mot gemensamt uppsatta mål (Alvinius et al., 2022). Samverkan är särskilt viktigt då komplexa och svårhanterliga händelser med en oviss utgång inträffar på en samhällsnivå. Samverkan kan ske både horisontellt mellan likställda självständiga parter, och vertikalt mellan överordnade och underordnade aktörer (Alvinius et al., 2022). Samverkan mellan myndigheter och samhällsaktörer sker i syfte att uppnå gemensamma mål, och begreppet antyder att inblandade aktörer är mer eller mindre likvärdiga (Deverell et al., 2019b). Däremot kan samverkan i hög grad upplevas som asymmetrisk, vilket påverkas av ett antal faktorer.

Myndigheters relation till krishanteringssystemet påverkar deras status i samverkanssituationer, vilket kan få konsekvenser för samverkan och prestationer (Deverell et al., 2019a). Traditionellt kvinnligt kodade institutioner uppfattas generellt ha lägre status i relation till traditionellt maskulint kodade organisationer, vilket kan bidra till exkludering vid samverkan. Organisationer med nära anknytning till den operationella, akuta verksamheten blir istället symboler för maskulinitet, vilket ger högre status vid samverkanssituationer (Deverell et al., 2019a). Vidare tenderar skillnader i mandat och klädsel bidra till statusskillnader. I traditionellt manligt kodade organisationer relaterade till krishanteringssystemet tenderar tjänstemän i beredskap (tib) att ha mer mandat än samma funktion i traditionellt kvinnligt kodade organisationer. På samma sätt tenderar uniformerade aktörer i operationella, akuta verksamheter tillskrivas högre status än mer strategiskt inriktade krishanteringsaktörer (Deverell et al., 2019a). När samverkan vilar på asymmetriska maktrelationer blir tillit allt viktigare, vilket kopplas till både individer och olika organisationer med deras status, resurser och kapacitet. Det innebär exempelvis att samarbeten mellan uniformerad och civilklädd personal kan påverkas av asymmetriska maktrelationer (Deverell et al., 2019a).

För att motverka asymmetriska maktrelationer i samverkanssammanhang kan ökad personkännedom, förändring av strukturer och språkbruk, kunskap om organisatoriska skillnader, samt stärkt kompetensutveckling, vara gynnsamma strategier (Deverell et al., 2019b). Genom att stärka kunskapen om varandra inom och mellan olika organisationer ökar både kunskap, trivsel och trygghet. Det främjar även uppbyggandet av ett gemensamt språk som förstås av samtliga inblandade aktörer, vilket gagnar samarbeten mellan organisationer med asymmetriska maktrelationer. Därutöver framhålls även kontinuerlig utbildning samt

kunskap om organisatoriska skillnader och kompetensområden är av stor vikt för att myndigheter i kris ska kunna arbeta mer effektivt med varandra (Deverell et al., 2019b).

Kommunikation

Eftersom rysk informationskrigföring äger rum i informationsmiljön, är det också i informationsmiljön man vill bemöta den. Det medför att kommunikatörer spelar en viktig roll i arbetet att förebygga, identifiera och möta illasinnad informationspåverkan. Arbetet att förebygga inkluderar huvudsakligen att skapa en medvetenhet om illasinnad informationspåverkan, att bygga förtroende genom strategisk kommunikation samt att förbereda generiska, kommunikativa budskap utifrån organisationens värderingar (MSB, 2019). En omfattande målgruppsanalys med syftet att ta fram kommunikationsverktyg är också en god åtgärd för att förbereda potentiell illasinnad informationspåverkan. Därefter är det viktigt att kartlägga organisationens sårbarheter och bedöma hur illasinnad informationspåverkan skulle kunna hota verksamheten och organisationens förmåga att uppfylla sitt uppdrag (MSB, 2019).

Eftersom illasinnad informationspåverkan förekommer i olika former finns även olika hanteringsstrategier för att bemöta dem. Hanteringsstrategier kan beskrivas i fyra nivåer, där valet av nivå bör vägas mot bedömningen av situationens allvar (MSB, 2019). Den första nivån handlar om att bedöma situationen, vilket är en neutral åtgärd som tillkännager en medvetenhet om situationen. Den andra nivån handlar om att informera allmänheten och relevanta intressenter om rådande situation och organisationens narrativ, vilket tillsammans med den första nivån lägger grunden för en faktabaserad respons (MSB, 2019). Den tredje nivån inbegriper kommunikativa åtgärder där organisationen förhåller sig till en specifik

position genom att argumentera för egen fakta och budskap i relation till desinformationen. Den fjärde och sista nivån handlar om att försvara organisationen genom att adressera specifika insatser mot angriparen (MSB, 2019).

Förhållningssätt

Forskning visar att när man planerar för olika hanteringsstrategier för desinformation kan man utgå från passivitet, reaktivitet, preaktivitet eller proaktivitet. Med utgångspunkten i att individen tenderar att hålla fast vid existerande övertygelser när det finns motstridiga bevis, handlar ett passivt förhållningssätt om att man inte ger ytterligare uppmärksamhet till falsk information (Dowse & Dov Bachmann, 2022). Desinformationen väntas således få en lägre grad av synlighet och följaktligen lägre effekt. Däremot medför det passiva förhållningssättet att man ger vika för motståndaren på informationsområdet, vilket resulterar i ett obestritt inflytande. Ett reaktivt förhållningssätt till desinformation relateras till försök att korrigera falsk information med korrekt information (Dowse & Dov Bachmann, 2022). Eftersom faktakorrigeringarna behöver uppnå samma läsekrets och genomslagskraft som den ursprungliga desinformationen, är strategin relativt begränsad i effektivitet. Dessutom tenderar falsk information att spridas längre och snabbare än sann information (Dowse & Dov Bachmann, 2022). Trots dessa begränsningar är reaktiva korrigeringar en vanligt förekommande strategi för att motverka desinformation.

Vidare handlar ett preaktivt förhållningssätt om att vidta åtgärder i väntan på falsk information, för att ta udden av dess effekter (Dowse & Dov Bachmann, 2022). Strategin kräver en förståelse för motståndarens motiv och de områden inom vilka motståndaren kan främja desinformation, för att därefter utveckla och sprida sanningsenlig information i ett

förebyggande syfte. Slutligen handlar det proaktiva förhållningssättet om att mer allmänt undvika eller mildra effekterna av desinformation (Dowse & Dov Bachmann, 2022). Utbildning och mediekompetens är generellt huvudsakliga prioriteringar, med syftet att åstadkomma analyser av information snarare än acceptans. Därutöver prioriteras insatser för att skapa förtroende för mediekällor.

Metod

I den här studien är problemställningen formulerad som öppna frågor med målet att beskriva vilka utmaningar som rysk informationskrigföring medför, samt vilka hanteringsstrategier som anses gynnsamma för att motverka utmaningarna. Med de frågeställningarna som utgångspunkt ansågs en kvalitativ metod med en explorativ ansats vara bäst lämpad. Valet av kvalitativ metod medför att resultatet inte kommer att vara representativt för hela populationen, vilket innebär att studien kan konstateras vara icke-generaliserande. Då kvalitativa studier generellt handlar om upplevelser, tolkningar och meningar, är det inte möjligt att dra slutsatser som gäller för alla som ingår i populationen (Frostling-Henningsson, 2017).

Undersökningsdesignen bestämdes utifrån att frågeställningarna var öppna och explorativa, där syftet var att kartlägga likheter och skillnader för ett fenomen. Det innebär att problemställningen kan beskrivas som oklar och deskriptiv. Medan en konkret och tydlig problemställning generellt är bäst lämpat för att pröva teorier eller hypoteser, är en explorativ ansats adekvat vid en oklar problemställning (Jacobsen, 2017). Vidare handlar en deskriptiv problemställning om att syftet är att kartlägga likheter och skillnader, snarare än att söka förklaringar till orsaken bakom ett fenomen.

Genomförande

För att generera relevant information som skulle besvara frågeställningarna ansågs individuella intervjuer vara bäst lämpade. Observationer och intervjuer hör till de vanligaste metoderna för att samla in kvalitativa data (Larsen, 2009). För att införskaffa relevant information och få en djup förståelse för ett fenomen vid en explorativ ansats, anses vanligtvis individuella intervjuer vara förmånligt (Jacobsen, 2017). Samtliga respondenter fick information om studien och förutsättningar för eget deltagande, inklusive beräknad tidsåtgång, i samband med att de kontaktades om deltagande i intervjun. Respondenterna ombads även att ge ett skriftligt, informerat samtycke till deltagande (se bilaga 1).

Intervjuerna hölls företrädesvis ansikte mot ansikte och på platser som respondenterna föreslog, med syftet att utföra intervjun på en plats där respondenten kände sig bekväm och avslappnad. Att ha platsen för intervjun i beaktning är viktigt på grund av kontexteffekten, vilket innebär att respondenten tenderar att uppträda annorlunda i en artificiell kontext jämfört med i en naturlig miljö (Jacobsen, 2017). Det medförde att vissa intervjuer genomfördes på respondentens arbetsplats, medan andra hölls på caféer eller restauranger i närheten av deras hem. Två av intervjuerna hölls digitalt på grund av bristande möjligheter att mötas i person. Att utföra intervjuer ansikte mot ansikte kan däremot anses vara fördelaktigt eftersom det berikar materialet med icke-verbal kommunikation, som kroppsspråk (Jacobsen, 2017).

Intervjuerna varade mellan 45-60 minuter. Samtliga respondenter tillfrågades om samtycke till att spela in ljudet av intervjun för senare transkribering. För att kunna hålla ett gott samtal

med ögonkontakt är det fördelaktigt att spela in intervjuerna, eftersom intervjuaren då inte behöver fokusera på att anteckna under intervjun. En del respondenter upplever det däremot som obekvämt att bli inspelad under intervjun, vilket betonar vikten av samtycke (Jacobsen, 2017). En av respondenterna hade önskemålet att inte bli inspelad, varvid anteckningar istället fördes under intervjutillfället. De övriga respondenternas intervjuer spelades in och transkriberades ordagrant.

Fortsättningsvis utfördes intervjuerna med hjälp av en semistrukturerad intervjuguide. Vid semistrukturerade intervjuer arbetar intervjuaren med en intervjuguide innehållandes på förhand definierade teman och huvudfrågor. Under intervjun lämnas däremot utrymme för avvikelser om respondenten skulle framhålla några oväntade och intressanta ämnen (Justesen & Mik-Meyer, 2013). I den här studien användes den semistrukturerade intervjun för att respondenterna skulle få reflektera över samma frågor, samtidigt som det möjliggjorde en explorativ ansats för att generera ny kunskap. Den semistrukturerade intervjuformen säkerställde även att samtliga ämnesområden avhandlades vid respektive tillfälle.

Ett alternativ till den semistrukturerade intervjun hade kunnat vara en ostrukturerad intervjuguide. Vid ostrukturerade intervjuer är intervjun inte planerad på förhand, utan det är primärt respondenten som styr samtalsstrukturen och definierar innehållet. Metoden kan vara lämplig för explorativa undersökningar där intervjuarens förhandskunskaper om ämnet är låga. Metoden är också lämplig då undersökningen behandlar känsliga ämnen där en intervjuguide riskerar att hämma samtalet och reflektioner (Justesen & Mik-Meyer, 2013). I den här studien var däremot intervjuarens förkunskaper relativt goda och centrala begrepp har konkretiserats för att bidra till förståelse för fenomenet. Det föranledde beslutet att använda en semistrukturerad intervjuguide.

Urval

För att samla in relevant information vid intervjuerna valdes respondenterna ut genom en kombination av strategiskt- och bekvämlighetsurval. Ett strategiskt urval innebär att respondenterna väljs ut baserat på kriteriet att en viss kunskap eller erfarenhet behöver erhållas (Jacobsen, 2017). Respondenternas kunskap och erfarenheter har varit det huvudsakliga urvalskriteriet. Eftersom rysk informationskrigföring många gånger gör statliga myndigheter till måltavla, i syfte att polarisera samhällen, var det viktigt att respondenterna arbetar på myndigheter. Därutöver fanns ett urvalskriterium att respondenterna antingen skulle arbeta inom beredskapsmyndigheter som spelar en roll sett till Sveriges psykologiska försvar, eller på myndigheter som utsatts för eller som har erfarenhet av att hantera illasinnad informationspåverkan. Att intervjua respondenterna från de olika perspektiven ansågs kunna bidra till kunskap om luckor däremellan, vad gäller upplevda utmaningar och gynnsamma hanteringsstrategier.

Sammantaget återfinns respondenter från Myndigheten för psykologiskt försvar, Svenska Institutet, Myndigheten för samhällsskydd och beredskap, Försvarsmakten, Polismyndigheten, Socialstyrelsen och Valmyndigheten. För att komma i kontakt med enskilda respondenter för intervjuer skickades e-post till myndigheternas officiella e-postadresser. Information om studien delgavs vid det steget, varvid kontakten därefter förmedlades till relevant person. Det innebär att urvalet av respondenter även grundades i bekvämlighet, där de valdes ut baserat på att de var enkla att få kontakt med. Bekvämlighetsurvalet är fördelaktigt när undersökningen lider av tidsbegränsningar, men kan

resultera i snedvridet resultat och brist på variation till den externa validitetens disfavör (Jacobsen, 2017).

Totalt intervjuades sju personer, eftersom det ansågs vara en rimlig mängd för att generera tillräcklig information för att utveckla en analys. Beroende på den tid och de resurser som finns tillgängliga för en studie, varierar antalet respondenter vanligtvis mellan 5-25 personer (Kvale & Brinkmann, 2014). Vanligtvis eftersträvas mättnad av information, vilket innebär att man slutar samla in information när kunskapen som genereras genom ytterligare insamling inte bidrar till något nytt (Jacobsen, 2017). Eftersom antalet intervjuer var få till antalet förutspåddes mättnad bli svårt att uppnå under den tillgängliga tiden. Däremot ansågs antalet respondenter vara tillräckliga för att få en rimlig representation utifrån givna förutsättningar.

Analysteknik - Tematisk analys

För att få en god överblick över textmaterialet användes meningskoncentrering som metod för att systematiskt och strukturerat kunna urskilja teman. Meningskoncentrering innebär att respondenternas utsagor sammandras till kortare formuleringar, där den huvudsakliga innebörden formuleras om i några få ord (Kvale & Brinkmann, 2014). Sammanhängande meningsenheter sammanfattades i nyckelord, för att därefter identifiera gemensamma komponenter som kunde bilda potentiella teman under vilka det kodade materialet sorterades. Därefter utvecklades de olika meningsenheterna och resulterade i fyra övergripande teman.

Ett exempel på hur meningskoncentrering gått till i förevarande studie är genom citatet “Ryska journalister har begärt ut offentlig information från svenska myndigheter, för att därefter förvränga informationen i sina egna medier på ett sätt som skadar svenska intressen.

Det resulterar i att drabbade myndigheter blir mer restriktiva gällande offentlig information.”. Citatet sammanfattades initialt som "utmaning relaterad till myndigheters transparens, exempel på hur Ryssland begränsar transparensen", vilket senare formulerades om till nyckelorden: utmaning och restriktivitet. I resultatet har nyckelorden därefter sorteras in under temat “Restriktivitet eller transparens”. I syfte att säkerställa dess relevans har det presenterade resultatet löpande kontrollerats mot undersökningens syfte och frågeställningar.

Forskningsetiska överväganden

Inom forskning har man ett personligt ansvar att säkerställa att forskningen utförs och rapporteras på ett korrekt och ärligt sätt samtidigt som undersökningsdeltagare måste skyddas (Graziano & Raulin, 2012). I den här studien har behandlingen av respondenternas personuppgifter följt Vetenskapsrådets rekommendationer för god forskningssed (2017), genom att uppfylla kraven för informerat samtycke och konfidentialitet. Informerat samtycke handlar om respondentens rätt till frivilligt deltagande, vilket behöver grundas i en medvetenhet och förståelse för eventuella risker och fördelar ett deltagande kan medföra. Det innebär att den som undersöks behöver vara i stånd att själv besluta om sitt deltagande, att deltagandet sker utan någon form av påtryckningar från omgivningen, att individen har tillräckligt med information om undersökningens syfte, samt att den ska ha förstått informationen (Jacobsen, 2017).

För att uppfylla kravet för informerat samtycke fick respondenterna information om studien (se bilaga 3) i god tid innan intervjutillfället ägde rum. Där framgick information om frivillighet gällande deltagande, studiens syfte, vilka personuppgifter som skulle samlas in, samt hur personuppgifterna skulle behandlas. Därutöver tydliggjordes respondenternas

rättigheter som inkluderade möjligheten till rättelse av felaktiga uppgifter och återkallelse av samtycke.

Kravet om konfidentialitet handlar om att forskaren måste hantera respondenternas utsagor på ett sätt så att de inte kan härledas till enskilda individer (Graziano & Raulin, 2012). För att uppfylla kravet lagrades respondenternas personuppgifter och det transkriberade materialet elektroniskt på en lösenordsskyddad dator, för att därefter raderas efter att arbetet examinerats. Därutöver har materialet i resultatet behandlats på ett sätt som gör att enskilda citat eller utsagor inte kan härledas till specifika respondenter.

Resultat

Resultatet från det insamlade materialet bygger på respondenternas utsagor och sammanfattas under fyra teman: “Restriktivitet eller transparens”, “Misstro eller tillit”, “Negligera eller förvänta” samt “Isolera eller samverka”. Teman framhåller restriktivitet, misstro, negligering och isolering som de utmaningar som myndigheter i Sverige upplever att rysk informationskrigföring medför. Resultatet visar att utmaningarna både kan relateras till informationspåverkan i sig, genom att skapa misstro, men även till de hanteringsstrategier man vill anta för att motverka informationspåverkan, där organisationen intuitivt tenderar att bli mer restriktiv, isolera sig och negligera illasinnad informationsspridning. Strategierna som anses gynnsamma för att motverka dessa utmaningar kan hänvisas till begreppens motpoler: transparens, tillit, förväntan och samverkan. Utvalda citat har omformulerats utan att förändra deras innebörd, med avsikten att bibehålla respondenternas konfidentialitet och förenkla läsning.

Restriktivitet eller transparens

Utifrån respondenternas utsagor framgår att framgångsrik illasinnad informationspåverkan riktar in sig på samhällets sårbarheter. I det öppna samhället där individen har rätt till yttrandefrihet och opinionsbildning, finns även möjligheter att utnyttja öppenheten för att sprida desinformation. Respondenterna beskriver det öppna samhället som en sårbarhet, vilket även Ryssland har identifierat. En av respondenterna förklarar det som att "även om Sverige har förhållandevis hög resiliens mot informationspåverkan jämfört med andra länder, så sprider Ryssland narrativ som påverkar Sverige i riktningar som går emot Sverige och svenska intressen".

Sårbarheten i det öppna samhället kan leda till utmaningar kopplat till restriktivitet. Det innebär att eftersom informationsmiljön inte är tydligt avgränsad utan hänger ihop i ett system, kan det svenska samhället påverkas av Rysslands icke-transparenta, restriktiva samhälle. Genom att begränsa medborgarnas rätt till opinion och yttrande kan de ryska aktörerna beskära vår demokrati och transparenta samhälle. Fortsättningsvis leder det öppenheten även till utmaningar relaterade till att motverka illasinnad informationspåverkan och spridning av desinformation, eftersom den intuitiva hanteringsstrategin är att bli mer restriktiv, vilket kränker individens rätt till åsikter.

Följande citat är ett exempel på risken att reagera genom restriktivitet när transparensen utnyttjas. "Ryska journalister har begärt ut offentlig information från svenska myndigheter, för att därefter förvränga informationen i sina egna medier på ett sätt som skadar svenska intressen. Det resulterar i att drabbade myndigheter blir mer restriktiva gällande offentlig information."

Även om det öppna samhället kan utnyttjas för att skapa mer restriktivitet, är respondenterna övertygade om att det är i det öppna och transparenta samhället som de viktigaste hanteringsstrategierna återfinns. För att försvara transparensen och bibehålla resiliens framkommer att en stärkt förmåga till källkritik hos allmänheten och den egna organisationens externa kommunikation är viktiga strategier. Respondenterna som arbetar på beredskapsmyndigheter ansåg att ett robust, transparent samhälle framförallt kräver en god förmåga till källkritik hos allmänheten, vilket är något som respondenter anser att skolan bör lära ut i större utsträckning. "Det är ju just den här transparensen vi vill försvara, så då är det viktigt att medvetandegöra allmänheten och utbilda i källkritik." När individen är källkritisk kommer desinformation identifieras i ett tidigare skede, vilket automatiskt leder till en begränsad spridning. Därutöver anses de fria, oberoende medierna och tankesmedjor vara en effektiv struktur i Sveriges resiliens i det avseendet, eftersom de ständigt granskar opinioner och således identifierar desinformation och illasinnad informationspåverkan. "Man bjuder in trollen till det öppna samhället, med det är också i det öppna samhället som trollen spricker i ljuset".

För att motverka illasinnad informationspåverkan belyser samtliga respondenter även den externa kommunikationen som ett viktigt verktyg. Information och kommunikation som riktas åt allmänheten behöver vara synkroniserad mellan myndigheter för att undvika att lämna utrymme för rykten och felaktiga tolkningar. Därutöver vill organisationerna bemöta information där information sprids. De organisationer som utsatts för illasinnad informationspåverkan kommunicerar på olika kanaler, på olika språk och mot olika målgrupper. En av respondenterna förklarar det som att "Vi vaccinerar i förväg genom att vi

har väldigt bred information på många olika språk. Det har blivit vårt viktigaste verktyg mot desinformation".

Syftet med kommunikationen är att tillgodose allmänheten med korrekt och tillförlitlig information. Att ge sig in i debatter och dementera falska uppgifter anses vara en ineffektiv strategi som snabbt tröttar ut en organisation, samtidigt som det ger onödig uppmärksamhet till desinformationen. "Du kan inte springa efter alla bollar, det är inte kostnadseffektivt och sliter ut en organisation ganska omgående". Istället vill man stärka det egna narrativet, vilket även fungerar som en förebyggande strategi då allmänheten kommer att vända sig till organisationen för att hitta faktagranskad information när det eftersöks. För att slå hål på myter sprider man den korrekta informationen brett och kvantitativt för att nå ut till en större population. Däremot läggs även fokus på att bemöta lokala organisationer och civilsamhället genom djupare, kvalitativ kommunikation.

Misstro eller tillit

Eftersom rysk informationskrigföring vanligtvis syftar till att polarisera samhällen, framhåller respondenterna misstro till myndigheter som en utmaning till följd av rysk informationskrigföring. Ur respondenternas utsagor framgår också att myndigheterna som upplever en högre grad av misstro från allmänheten drabbas hårdare av illasinnad informationspåverkan. Eftersom det finns en större misstro till myndigheten och dess kommunikation, får desinformationen bättre fäste och större spridning, vilket föder ytterligare misstro. Det leder till att organisationers externa kommunikation försvåras. En av respondenterna förklarade att "att informationen fick spridning föregicks av ett lågt förtroende av organisationen, vilket inte var något nytt för oss".

Misstro kan relateras både till den egna befolkningens misstro till myndigheter, men även till andra länders befolkningars misstro till Sverige. När andra länders befolkning upplever misstro till Sverige finns en ökad benägenhet att sprida desinformation vidare utomlands. En del respondenter uppger att andra länder inte har så mycket kunskap eller kännedom om Sverige, men att bilden av Sverige i utlandet trots det bedöms vara relativt positiv. I Ryssland skiljer sig bilden av Sverige mellan beslutsfattare och befolkning, där Sverigebilden hos beslutsfattare generellt är mer negativ. Ryska medborgares uppfattning om Sverige är däremot en nedåtgående trend, på grund av ensidiga medienarrativ som följer av att Ryssland inte har fria, oberoende medier. Inom Sverige skiljer sig allmänhetens förtroende för olika myndigheter.

> Det handlar om förtroende på olika sätt - förtroende från andra stater för Sverige, men också medborgarnas förtroende för Sverige. De största utmaningarna med att det sprids desinformation är att det skapar en oro i samhället som ruckar på det där förtroendet.

För att öka organisationens resiliens och motverka rysk illasinnad informationspåverkan, kan således tillitsfrämjande åtgärder stärkas. De respondenter som arbetar på myndigheter med hög tillit uppger att spridning av desinformation inte får samma effekt, eftersom antalet individer som söker korrekt information på myndighetens kanaler är många. För att stärka tilliten för organisationen belyser respondenterna öppenhet, ärlighet och transparens som viktiga element. Ett belysande citat är följande: “vi kommer ut med mycket förebyggande budskap som är mer tillitsbaserade, just i syfte att stärka tilliten till organisationen. Det gör vi även i relationsbyggande dialoger, där vi vänder oss mot en mängd organisationer och civilsamhället”.

Flera respondenter framhåller vikten av att inte linda in kommunikationen i syfte att skapa en falsk trygghet eller lugna befolkningen, utan att det istället är viktigt att förhålla sig sakligt och ärligt för att vinna allmänhetens förtroende. Respondenterna beskriver att det är viktigt att vara tydlig med den information man för fram, för att inte lämna rum åt funderingar. När myndigheterna är transparenta, öppna och tydliga med den information som kommuniceras om dem, ökar förtroendet från allmänheten. "Vi berättar som det är och att det tyvärr är skitdåligt just nu, och då måste vi göra någonting".

Negligera eller förvänta

En utmaning som framkom i det insamlade materialet berör identifiering och acceptans av illasinnad informationspåverkan. Inledningsvis belyser respondenterna omvärldsbevakning som ett viktigt verktyg för att identifiera spridning av desinformation och eventuell illasinnad informationspåverkan. I de fall spridning av desinformation har lett till stor negativ påverkan på organisationen har sådan omvärldsbevakning saknats eller varit bristfällig, vilket gjort att informationsspridningen negligerats. Samtidigt har organisationen även varit passiv i att acceptera spridningen av desinformation som problematisk, för att istället invänta en bedömning av situationen från expertmyndigheter innan åtgärder har vidtagits. Följande citat illustrerar detta.

> Det som hände var att det eskalerade i en otroligt snabb takt och i ofattbara proportioner, framförallt i sociala medier. Sen kontaktade Myndigheten för psykologiskt försvar oss och konstaterade att det är en desinformationskampanj. Men vi var inte beredda på att det skulle bli så omfattande, systematiskt och illasinnat.

En del respondenter beskriver att skillnader i perspektiv och världssyn mellan Sverige och Ryssland kan bidra till svårigheter för acceptans. Ett sådant exempel är Moskvapatriarkatet som är aktiva att kontrollera ryskortodoxa församlingar runtom i världen. En av respondenterna förklarade utmaningar att relatera de ryskortodoxa församlingarna till illasinnad informationspåverkan med följande citat: "det är ju en dimension som vi i sekulära Sverige kanske inte alltid lägger så stor vikt vid. Kyrkor är ju för de flesta en religiös upplevelse - det är bröllop, begravningar och dop."

Fortsättningsvis framgår det i materialet att de organisationer som förväntar sig att illasinnad informationspåverkan eller spridning av desinformation kommer att inträffa, är snabbare med att acceptera spridningen som problematisk. I de organisationerna arbetar man proaktivt med både omvärldsbevakning och planering av motstrategier vid eventuella händelser, utifrån förväntningar om att det kommer inträffa. Respondenterna förklarar att dessa organisationer identifierar aktörer som vanligtvis sprider desinformation och utövar illasinnad informationspåverkan, men även situationer där illasinnad informationspåverkan kan komma att inträffa mot den egna organisationen. "Vi är medvetna om vilka aktörer som utövar informationspåverkan och vilka strategier de använder, vilket gör att vi vet vad vi ska leta efter."

Därutöver finns en inställning att det inte är tillräckligt att bevaka omvärldsinformation som direkt berör den egna organisationen. Istället inkluderar omvärldsbevakningen även läget i andra länder och information som sprids om andra länders motsvarande organisationer, eftersom det tenderar att spilla över och även drabba den egna organisationen.

> Nu är man medveten om de problem som Sverige och världen står inför, och att inte prata om dem då är att vända ryggen åt den framspringande tigern. Till slut kommer den att ta dig, om du inte sett den och vidtagit åtgärder.

Således anses regelbunden omvärldsbevakning vara en viktig strategi för att kunna arbeta anpassat och agilt. Samtliga respondenter anser det viktigt att informationsmiljön följs på olika språk för att få en god inblick i vad det är för trender, information och rykten som sprids. Att enbart bevaka informationsmiljön är däremot inte tillräckligt, utan illasinnad informationspåverkan och desinformation behöver även accepteras som problematiskt. De organisationer som förväntar sig att spridning av desinformation och illasinnad informationspåverkan kommer att inträffa har sällan problem gällande acceptansen. Det medför att organisationerna vidtar åtgärder i ett tidigt skede istället för att låta situationen eskalera till en kris, vilket låter dem bibehålla kontroll över situationen. När det finns en förväntan om spridning av desinformation och illasinnad informationspåverkan blir således organisationerna proaktiva när det kommer till att agera. "Min organisation hade nog inte kunnat hamna i ett läge där illasinnad informationspåverkan får ett så stort fäste, utan det hade kommit motåtgärder i ett tidigare skede."

Isolera eller samverka

Respondenter beskriver isolering som en utmaning som följer illasinnad informationspåverkan och spridning av desinformation, eftersom de hybridhot som samhället står inför kräver att samhällets resurser används på ett effektivt sätt. Samverkan anses försvåras av att det i vissa fall är utmanande att veta vart gränserna mellan olika organisationer går. Respondenterna belyser att det både gäller geografiska gränser och

gränser kopplade till arbetsuppgifterna när en påfrestande situation uppstår. Medan vissa organisationer föredrar att förhålla sig relativt strikt till ansvarsprincipen och organisationens givna ansvarsområden, anser andra organisationer att det krävs ett förhållningssätt som ser till helheten. En av respondenterna beskrev det som att "man får liksom vara lite pragmatisk, kreativ och se till helheten, istället för att bara sitta och titta på vart gränsen mellan mitt uppdrag och ditt uppdrag går".

Sett till interorganisatorisk samverkan identifierades tydliga skillnader mellan beredskapsorganisationerna och de organisationer som utsatts för illasinnad informationspåverkan. Bland beredskapsorganisationer är samverkan systematiserad och rollfördelningar upplevs som tydliga. För myndigheter som inte normalt hör till beredskapsarbetet är rollfördelningen under kris däremot inte lika uppenbar, vilket försvårar den inledande samverkan eftersom organisationen tenderar att isolera sig från andra myndigheter i syfte att lösa den akuta problematiken kring illasinnad informationspåverkan. Nedanstående citat beskriver upplevda utmaningar sett till rollfördelning, när samverkan inte varit systematiserad sedan tidigare.

> När vi inte riktigt förstod omfattningen blev det lätt att vi agerade förstärkt på småsaker, men vi kan ju inte ge oss in i den enskilda historien - det är ju på systemnivå vi behöver befinna oss. Men det tog lite tid att förstå vad vår roll i det här systemet var, och vad vår roll var jämfört med andra myndigheter.

När omfattningen av den illasinnade informationspåverkan är större, blir tendenserna till isolering också det. Vidare beskrivs samverkan som resurskrävande, både på grund av den tid som behöver avsättas och personal med kunskap och förståelse för samverkan. I det

insamlade materialet framkommer upplevelser om att en del myndigheter som inte relateras till beredskapsarbetet inte avsätter särskilt stora resurser för samverkan eftersom man inte befunnit sig i situationer där det krävts. De organisationerna har vanligtvis inte heller speciellt god kännedom om beredskapsmyndigheterna och deras syfte, vilket kan bidra till visst motstånd till samverkan under krissituationer. "Man måste dedikera resurser till samverkan, strukturer och förmågor att kunna öva och utbilda. Beredskapsmyndigheterna har ofta mer av den vanan, vilket tenderar att göra samverkan lite lättare."

Trots instinktiva tendenser till isolering, anser respondenterna att samverkan är en viktig aspekt för att motverka och hantera illasinnad informationspåverkan. Bland respondenterna som arbetar på beredskapsmyndigheterna framgår att samverkan med andra beredskapsmyndigheter är regelbunden och systematiserad, samt att samverkan även sker innan en kris inträffar. Samverkansstrukturerna utvärderas och omstruktureras regelbundet, vilket medför att samverkan ofta sker relativt friktionsfritt dem emellan. Följande citat lämpar sig väl för att beskriva ett antal respondenters syn på samverkan ur det perspektivet.

> Myndigheternas självbestämmande har ju skapat en robusthet i det svenska samhället, men för att inte tappa mark så måste vi se över de här vattentäta skotten mellan myndigheterna. Vi behöver därför öka samverkansmöjligheterna mellan myndigheterna, inte minst när vi pratar om psykologiskt försvar.

Kopplat till illasinnad informationspåverkan sker samverkan i flera syften. En förebyggande hanteringsstrategi är att dela lägesbilder och information som framkommit i organisationernas funktioner för omvärldsbevakning. Bland de organisationer som arbetar aktivt med

omvärldsbevakning framkom att det fanns rutiner för att uppmärksamma berörda organisationer i de fall man identifierar informationsspridning som kan påverka dem.

> Även om vi inte har något tydligt uppdrag kopplat till just informationspåverkan så ingår vi i samverkansstrukturer där samverkan sker med viss regelbundenhet. Strukturen är byggd efter den struktur man hade velat ha samverkan under LVU-kampanjen. Tanken är att den är grunden för om man behöver hantera informationspåverkan, samordna information och kommunicera med allmänheten.

Därutöver anses samverkan vara ett viktigt verktyg för att lära sig från varandras erfarenheter. De respondenter som arbetar på myndigheter som utsatts för illasinnad informationspåverkan ser det som viktigt att sprida lärdomar till andra organisationer, vilket inkluderade både beredskapsmyndigheter och organisationer som inte tidigare utsatts för illasinnad informationspåverkan. I det insamlade materialet framkommer upplevelser om att samverkan i syfte att lära från erfarenheter gör samverkan mer systematiserad och regelbunden, samtidigt som de olika organisationernas roller och ansvarsområden klargörs. En del myndigheter ser även goda möjligheter att lära sig från organisationer i andra länder och blickar därför utanför Sveriges gränser sett till samverkan. I de fallen studerar man hur organisationerna i andra länder utsatts för illasinnad informationspåverkan och hur de hanterat det.

Diskussion

Resultatdiskussion

I det här avsnittet diskuteras studiens resultat mot bakgrund av tidigare forskning. Syftet med studien var att bidra till fördjupad kunskap om rysk informationskrigföring i en svensk kontext. För att uppnå syftet undersöktes vilka utmaningar som svenska myndigheter upplever att de ställs inför kopplat till rysk informationskrigföring, samt vilka strategier som anses gynnsamma för att motverka dessa utmaningar. Resultatet visar att utmaningarna och hanteringsstrategierna kan sammanfattas under fyra teman: "Restriktivitet eller transparens", "Misstro eller tillit", "Negligera eller förvänta" samt "Isolera eller samverka". Utmaningarna relateras till restriktivitet, misstro, negligera, samt isolera, medan framgångsrika hanteringsstrategier kopplas till transparens, tillit, förvänta och samverka. I det här avsnittet bidrar resultaten till fördjupad förståelse för tidigare forskning, vilket presenteras utifrån studiens fyra teman.

Restriktivitet eller transparens

Resultatet i den aktuella studien visar att respondenterna upplever att det öppna samhället är en sårbarhet som kan utnyttjas. Eftersom individen har rätt till opinionsbildning och yttrandefrihet, kan rätten att bilda opinion och yttra sig utnyttjas genom spridning av desinformation och illasinnad informationspåverkan. Den här delen av resultatet stöds av tidigare forskning om statliga och privata aktörer som lägger allt större fokus på att öka makten och kontrollera den komplexa, snabbföränderliga och svårnavigerade informationsmiljön (Nilsson et al., 2022). Där framhålls även att Ryssland har en förmåga att utnyttja demokratiska länders rätt till opinion och yttrandefrihet, genom att sprida budskap som underblåser polarisering och snedvrider den offentliga debatten (Palmertz, 2021). I den

här studien framkommer att organisationens intuitiva reaktion, när den utsätts för illasinnad informationspåverkan, är att agera med restriktivitet genom att begränsa mängden tillgänglig information. Restriktiviteten beskrivs som en stor utmaning eftersom den begränsar tillgänglig korrekt och tillförlitlig information, vilket gynnar ryska intressen. Därutöver kan det konstateras vara en direkt motsats till vad man strävar efter i det transparenta samhället, eftersom man istället går Rysslands intressen till mötes. En minskad grad av transparens skulle dessutom kunna medföra ytterligare polarisering i samhället.

Vidare belyser resultatet i förevarande studie att den icke-avgränsade informationsmiljön medför stora utmaningar sett till vilka hanteringsstrategier som är lämpliga att anta för att motverka illasinnad informationspåverkan, utan att kränka individens rätt till opinionsbildning och yttrandefrihet. Myndigheterna uppges ställas inför en balansgång mellan att bibehålla grundläggande demokratiska rättigheter, samt önskan om att förhindra spridning av information som kan skada förtroendet för den egna organisationen. Myndigheternas handlingsfrihet för att motverka illasinnad informationspåverkan begränsas till att enbart kunna bekämpa vilseledande information med den egna spridningen av korrekt information.

För att motverka utnyttjandet av det öppna samhället talar resultaten för korrekt och tillförlitlig kommunikation samt fria, oberoende medier. Respondenterna föreslår att utmaningen kopplat till restriktivitet kan hanteras med allmänhetens förmåga till källkritik eftersom det begränsar spridningen av desinformation i ett tidigt skede. I det fallet framhålls beredskapsmyndigheter som arbetar med utbildningar, där syftet är att åstadkomma analyser av information snarare än acceptans. Det kan förstås mot bakgrund av tidigare forskning som

framhåller ett proaktivt förhållningssätt i form av utbildning och mediekompetens som ett sätt att undvika eller mildra effekterna av desinformation (Dowse & Dov Bachmann, 2022).

Misstro eller tillit

I resultatet konstaterades att misstro till myndigheter är en utmaning relaterad till rysk informationskrigföring. Huruvida det finns tillit eller misstro till de olika myndigheterna har i studien baserats på respondenternas utsagor. Däremot hänvisade flertalet respondenter till olika studier, däribland Medieakademins förtroendebarometer (2023). Respondenterna hade således en medvetenhet om den tillit eller misstro som finns för organisationerna, och betonade det som av relevans sett till illasinnad informationspåverkan.

Utifrån respondenternas utsagor framgår att illasinnad informationspåverkan och spridning av desinformation ökar misstron för myndigheter. Det är också tydligt att myndigheter som har lägre förtroende från allmänheten drabbas hårdare av illasinnad informationspåverkan och spridning av desinformation. Följaktligen är det även svårt att implementera lämpliga hanteringsstrategier när organisationer har ett lägre förtroende, eftersom misstron till myndighetens kommunikation är högre. Vid tillfällen då förtroendet för Sverige är lägre blir effekten ännu starkare, eftersom det finns ett intresse i andra länder att sprida desinformation som i grund och botten härstammar från den enskilda myndigheten. Resultatet stärks av tidigare forskning om att individens benägenhet att tro på falsk eller manipulerad information är högre, när individen känner misstro till en organisation (Pamment et al., 2018).

Beroende på huruvida myndigheterna åtnjuter misstro eller tillit, påverkas deras alternativ till hanteringsstrategier. Organisationer med hög misstro som utsätts för illasinnad

informationspåverkan tenderar att initialt korrigera all falsk information med korrekt information, vilket kostar mycket tid och resurser. Dessutom bidrar det till att desinformationen får mer uppmärksamhet, vilket påverkar organisationen negativt. För att istället öka tilliten beskriver respondenterna att kommunikationen bör vara öppen, saklig och ärlig kommunikation. När en organisation har hög tillit är det enklare att hantera spridning av desinformation. I de fallen har organisationerna ingen anledning att ge uppmärksamhet åt desinformation, utan fokus läggs istället på att säkerställa transparens och korrekt information på egna kanaler. Organisationerna kan då nyttja sitt höga förtroende och istället för att argumentera med falsk information. De här myndigheterna är också duktiga på att vidta åtgärder innan desinformation börjar spridas, genom att se till att informationen alltid finns tillgänglig. Det finns en medvetenhet om sårbarheter och målgrupper, vilka aktörer som sprider desinformation och på vilka kanaler den sprids.

De olika förhållningssätten till kommunikation kan förstås mot bakgrund av tidigare forskning om hur organisationer antingen argumenterar för egen fakta och budskap i relation till desinformationen, eller försvarar den egna desinformationen (MSB, 2019). Mer ingående kan desinformation motverkas genom att anta ett passivt-, reaktivt-, preaktivt- eller proaktivt förhållningssätt i sin kommunikation (Dowse & Dov Bachmann, 2022). Medan myndigheter med hög misstro tenderar att anta ett reaktivt förhållningssätt, anser respondenterna att ett preaktivt förhållningssätt är den bäst lämpade strategin för att motverka misstro och främja tillit till myndigheten.

Negligera eller förvänta

Vidare visar studiens resultat på upplevda utmaningar kopplat till huruvida illasinnad informationspåverkan negligeras eller förväntas. Det framkommer att processer för identifiering, acceptans och implementering av lämpliga åtgärder inte bör ses som enskilda förmågor, utan som förutsättningar för varandra. Det innebär att i de fall organisationen negligerat, och således misslyckats med att identifiera informationsspridning, misslyckas den även med att acceptera den som ett problem.

I respondenternas utsagor framgår att bristfällig eller avsaknad av omvärldsbevakning bidragit till utmaningar med att förstå och acceptera spridningen som ett problem, vilket medfört att spridningen eskalerade innan organisationen agerat. Vidare blir acceptans en förutsättning för att organisationen ska vidta lämpliga åtgärder, eftersom ett problem som inte accepteras kommer medföra frånvarande eller otillräckliga åtgärder. I de fallen har organisationen uppfattat den illasinnade informationspåverkan som oväntad, vilket gjort den passiv i att acceptera spridningen som ett problem. Då har istället expertmyndigheter fått göra en bedömning av situationen som allvarlig innan den utsatta myndigheten agerat.

Det här resultatet kan förstås utifrån tidigare forskning om organisationers förmåga att identifiera tidiga tecken på kris påverkar hur snabbt man agerar för att undvika eskalering (Duchek, 2020). För att kunna implementera lämplig hanteringsstrategi krävs även förmågan att acceptera ett problem (Duchek, 2020), samt att bedöma situationens allvar (MSB, 2019). Därefter kan organisationen utveckla och implementera lämpliga planer för att hantera situationen.

Att negligera illasinnad informationspåverkan har ingen direkt påverkan på polarisering av samhället, vilket flera av de andra utmaningarna kan konstateras ha. Således gynnas inte Ryssland direkt av att en organisation misslyckas med att identifiera och acceptera spridningen. När en organisation negligerar den illasinnade informationspåverkan så ökar däremot risken för att omfattningen av konsekvenserna blir större, vilket kan leda till en regelrätt kris.

Inom de myndigheter som arbetar med en förväntning om att utsättas för illasinnad informationspåverkan, är organisationerna mer känsliga för tidiga tecken vid omvärldsbevakningen, vilket bidrar till att informationsspridning accepteras som ett problem innan det blivit ett problem. Det medför att organisationen implementerar hanteringsstrategier i ett väldigt tidigt skede och kan således motverka en eskalering på ett effektivt sätt. Bland de organisationer som negligerat tidiga tecken på illasinnad informationspåverkan eller spridning av desinformation, har identifiering, acceptans och vidtagande av lämpliga åtgärder fördröjts. Då identifiering och acceptans inte sker effektivt leder det till stora utmaningar vad gäller att vidta lämpliga åtgärder, eftersom situationen har eskalerat till en grad där det blir svårt att bibehålla kontroll över situationen.

I resultatet framgår att främst beredskapsmyndigheterna förväntar sig att illasinnad informationspåverkan kommer att inträffa. Anledningen till det skulle kunna vara att deras uppdrag som relaterat till krishantering, säkerhet och försvar, medför att risker och hot medvetandegörs för individer inom organisationen i större utsträckning. Medvetenheten kan bidra till förväntningar som bidrar till att de anställda söker efter tidigare tecken på kris. Organisationernas uppdrag kan således tänkas forma hela den organisatoriska kulturen till att bli mer riskmedveten. När en organisations uppdrag inte direkt kan relateras till krishantering

och beredskap finns inte samma medvetenhet om de hot och risker som organisationen kan ställas inför. Istället behöver medvetenheten byggas upp och bibehållas genom exempelvis samverkan eller utbildningar. Sverige och svenska intressen har regelbundet varit måltavla för riktade aktiviteter och illasinnad informationspåverkan som del av Rysslands informationskrigföring väntas fortgå även under kommande år (Wagnsson, 2023; Giles, 2023). Givet den ökade hotbilden är det viktigt att fler myndigheter och organisationer ställer om och blir mer uppmärksamma.

Sett till tidigare forskning kan man dra paralleller till hanteringsstrategier för illasinnad informationspåverkan, vilka beskrivs i de fyra nivåerna: bedöma, informera, förespråka eller försvara. Den första nivån handlar om att bedöma och tillkännage en medvetenhet om situationen (MSB, 2019), vilken kan relateras till förmågan att identifiera och acceptera illasinnad informationspåverkan. Det skulle kunna förstås utifrån tidigare forskning om att det krävs en förståelse för hur desinformationen får spridning för att kunna motverka den (Dowse & Bachmann, 2022). Resultatet i den här studien visar däremot på en ytterligare dimension, där förväntningar visat sig spela en avgörande roll för att identifieringen och acceptansen ska vara framgångsrika.

Isolera eller samverka

Förevarande studie presenterar även att samverkan mellan myndigheter påverkas av deras relation till krishanteringssystemet. Samverkan mellan beredskapsmyndigheter och myndigheter som vanligtvis står utanför det svenska krishanteringssystemet beskrivs i flera fall som utmanande. Det resultatet skulle kunna förstås utifrån tidigare forskning om att traditionellt kvinnligt kodade institutioner generellt uppfattas ha lägre status i relation till

traditionellt maskulint kodade organisationer. Maskulint kodade organisationer relateras främst till operationella beredskapsmyndigheter (Deverell et al., 2019a).

Fortsättningsvis framkommer att avsaknad av samverkansstrukturer tenderar att bidra till att organisationen intuitivt isolerar sig när den utsätts för illasinnad informationspåverkan. Frånvaron av samverkansstrukturer medför att myndigheterna har svårt att förstå den egna organisationens roll i relation till andra myndigheter i situationer då man utsätts för illasinnad informationspåverkan. Det leder också till utmaningar i att förstå varför samverkan behövs. När illasinnad informationspåverkan väl har eskalerat till den grad att situationen definieras som en kris, tenderar organisationen initialt att navigera sig i situationen genom att korrigera falsk information med korrekt information. Det kräver mycket resurser och leder till att uppgiften att förstå och etablera samverkansstrukturer nedprioriteras, vilket gör att det tar tid innan samverkan blir systematiserad i de fallen. Organisationen isolerar sig då instinktivt för att hantera den akuta situationen själva, vilket försvårar samverkan ytterligare. Isoleringen kan dessutom bidra till ytterligare polarisering och splittring, vilket även gynnar Rysslands intressen.

Ser man till samverkan mellan beredskapsmyndigheterna så är den systematiserad och tydligt strukturerad. Den framgångsrika samverkan bygger på att samverkan inträffar med jämna mellanrum, att samverkansstrukturerna regelbundet utvärderas och omstruktureras, och att det finns en god kunskap om de andra myndigheternas roller. Dessutom används samverkansstrukturerna för att dela information som framkommer genom omvärldsbevakning samt för att dela lärdomar efter att olika krissituationer har inträffat, vilket bidrar till ytterligare kunskap och förståelse för varandras organisationer. Det medför att maktrelationerna mellan beredskapsmyndigheterna ter sig symmetriska. Resultatet kan

förstås utifrån tidigare forskning där tillit accentueras som möjliggörare för framgångsrik samverkan. Tilliten kopplas både till individer och organisationer, men även deras status, resurser, kapacitet, strukturer och kunskap om organisatoriska skillnader (Deverell et al., 2019b). Det innebär att utmaningarna kopplat till att organisationen isolerar sig hanteras med mer samverkan, vilket faller väl i linje med resultatet i den här studien.

Slutsatser

Syftet med studien var att bidra till kunskapen om rysk informationskrigföring i den svenska kontexten, genom att undersöka vilka utmaningar som rysk informationskrigföring ställer på myndigheter, samt vilka strategier som upplevs gynnsamma för att motverka dessa. Resultaten visar att utmaningar och gynnsamma hanteringsstrategier kan sammanfattas i följande fyra teman: "restriktivitet eller transparens", "misstro eller tillit", "negligera eller förvänta" samt "isolering eller samverkan". Utmaningarna relateras till restriktivitet, misstro, negligering samt isolering, medan hanteringsstrategier kan kopplas till transparens, tillit, förväntan och samverkan.

Studiens slutsats är att myndigheter som negligerar illasinnad informationspåverkan och som upplever misstro från allmänheten, initialt tenderar att sluta sig och reagera med restriktivitet gentemot allmänheten och isolering från andra myndigheter. Således kan konstateras att den intuitiva reaktionen paradoxalt gynnar ryska intressen. Ökad restriktivitet och isolering kan tolkas som intuitiva reaktioner när organisationen utsätts för hotet och att man negligerar spridning, medan misstro till myndigheter som utmaningar som direkt följer hotet. Organisationer som istället förväntar sig att utsättas för illasinnad informationspåverkan och

som har hög tilltro från allmänheten, kan framgångsrikt bibehålla transparens och god interorganisatorisk samverkan.

Metoddiskussion

Studien visar exempel på vilka utmaningar som respondenter från olika myndigheter upplever att rysk informationskrigföring medför, samt vilka strategier som upplevs krävas för att motverka dessa utmaningar. Kvalitativa studier handlar generellt om tolkningar och meningar, vilket medför utmaningar sett till att generalisera resultatet på en population (Jacobsen, 2017). Eftersom resultaten i förevarande studie enbart visar på upplevda utmaningar och strategier, snarare än faktiska utmaningar och strategier, blir resultatet således inte möjligt att generalisera. Det bör också beaktas att studien är tidsbunden och kontextbaserad, relaterat till de metoder och strategier som rysk informationskrigföring inkluderar just nu. Däremot bidrar resultatet till en fördjupad förståelse för de utmaningar som rysk informationskrigföring kan ställa myndigheter inför, samt vilka strategier som kan vara lämpliga att använda då man utsätts för illasinnad informationspåverkan. Vidare har studien haft en induktiv ansats med ett explorativt förhållningssätt där centrala begrepp konkretiserats för att skapa en förståelse för fenomenet. Det kan jämföras med en deduktiv ansats, där empirin analyseras utifrån teoretiska perspektiv (Ryan & Bernard, 2003). Beroende på vilken teoretisk utgångspunkt som används, kan genererade resultat bli väldigt olika. Eftersom forskningen om fenomenet i en svensk kontext är relativt begränsad, ansågs en induktiv ansats bättre lämpat för att undvika risken för snedvridet resultat.

Insamlingen av kvalitativa data skedde med hjälp av en semistrukturerad intervjuguide. Den semistrukturerade intervjuguiden tillåter öppna reflektioner baserat på respondentens egen

tolkning av fenomenet, samtidigt som den säkerställer att samtliga ämnesområden avhandlas vid respektive intervjutillfälle (Justesen & Mik-Meyer, 2013). Vid explorativa undersökningar kan däremot ostrukturerade intervjuer vara fördelaktiga, eftersom respondenten primärt får styra samtalsstrukturen och definiera innehållet (Justesen & Mik-Meyer, 2013). På grund av den aktuella studiens kraftiga avgränsningar ansågs däremot en semistrukturerad intervjuguide vara bättre lämpad. Ytterligare ett alternativ hade varit strukturerade intervjuer, där exakta frågor och samtalsstruktur är bestämda på förhand (Justesen & Mik-Meyer, 2013). Den modellen hade däremot eliminerat alla explorativa inslag och valdes därför bort som alternativ för den här studien.

Därutöver är även valet av respondenter av metodologisk betydelse. Generellt anses ett slumpmässigt urval vara fördelaktigt för att tillgodose studien med en god representation av urvalet (Jacobsen, 2017). Eftersom antalet respondenter i den aktuella studien var få ansågs däremot det slumpmässiga urvalet riskera att generera skevhet i resultatet. I förevarande studie användes istället en kombination av strategiskt- och bekvämlighetsurval. Det strategiska urvalet anses fördelaktigt då respondenterna behöver erhålla en viss kunskap eller erfarenhet (Jacobsen, 2017). I den här studien har respondenterna arbetat på beredskapsmyndigheter som har en koppling till Sveriges psykologiska försvar, samt på myndigheter som utsatts för illasinnad informationspåverkan. Syftet var att undersöka huruvida det finns någon skillnad i uppfattningar av utmaningar och de hanteringsstrategier som ansågs gynnsamma.

Bekvämlighetsurvalet innebär att respondenter väljs utifrån tillgänglighet, vilket kan leda till snedvridet resultat och brist på variation (Jacobsen, 2017). Eftersom respondenterna kontaktades genom kontaktpersoner på myndigheterna, finns det även en risk för att de valts

ut internt för att de tros ge en positiv bild av organisationen (Eriksson-Zetterquist & Ahrne, 2015). För att få kontakt med respondenter som besitter rätt kunskaper och erfarenheter så fort som möjligt, ansågs strategiskt- och bekvämlighetsurval däremot vara de bästa alternativen.

För att stärka studiens validitet och representation av fenomenet hade antalet respondenter kunnat vara fler. I kvalitativa studier eftersträvas vanligtvis mättnad av information, vilket innebär att man slutar samla in information när ytterligare intervjuer inte tillför någonting nytt (Jacobsen, 2017). Av de respondenter som arbetar på organisationer som utsatts för illasinnad informationspåverkan framhölls väldigt skilda perspektiv, vilket vore önskvärt att undersöka ytterligare genom fler respondenter för att uppnå mättnad. Däremot har relevansen i respondenternas erfarenhet större betydelse än antalet deltagare (David & Sutton, 2016). Bland de respondenter som arbetar på beredskapsmyndigheter var informationen ungefär densamma från samtliga respondenter, vilket tyder på att mättnad har uppnåtts utifrån det perspektivet. För att fördjupa resultatet ytterligare hade det varit intressant att även inkludera respondenter från myndigheter som inte hör till beredskapsmyndigheterna och som inte utsatts för informationspåverkan. Det hade kunnat bidra till fler perspektiv om utmaningar och gynnsamma hanteringsstrategier.

Praktiska implikationer

Resultatet indikerar att chefer behöver vara uppmärksamma på hur organisationer tenderar att initialt reagera med restriktivitet och isolering då man utsätts för illasinnad informationspåverkan. Medan isolering försvårar den interorganisatoriska samverkan och således gör det utmanande att hantera illasinnad informationspåverkan effektivt, medför

restriktivitet att man utmanar det demokratiska och transparenta samhället. En medvetenhet om intuitiva reaktioner som reaktivitet, isolering och tendensen att negligera spridningen gör det möjligt att planera för hanteringsstrategier som motverkar dessa tendenser.

Framtida forskningsförslag

Informationsmiljön har blivit en integrerad del i förståelsen av modern krigföring, och alltfler aktörer riktar in sig på att öka makten och kontrollera den digitala informationsmiljön. För att stärka samhällets resiliens mot rysk informationskrigföring behövs mer forskning inom området, förslagsvis kopplat till hur individens förmåga till källkritik kan stärkas för att begränsa spridningen av desinformation. Det hade även varit intressant med fler studier som behandlar ett bredare spektrum av påverkansoperationer och som inte enbart tar hänsyn till illasinnad informationspåverkan och spridning av desinformation.

Referenser

Alvinius, A., Hede, S. & Helenius, J. (2022). *Ledarskapets kontext - en lärobok för militärer och krishanteringsaktörer*. Studentlitteratur.

Andersson, A. (2023). *Rättsligt ramverk för bemötande av informationspåverkan - En studie av det rättsliga ramverket för bemötande av informationspåverkan genom informationsåtgärder*. Totalförsvarets forskningsinstitut, FOI. https://www.foi.se/rest-api/report/FOI-R--5443--SE

Arce, D. (2024). Disinformation strategies. *Defence and Peace Economics*, https://doi.org/10.1080/10242694.2024.2302236

Appelgren, J., Bay, S., Malminen, J., & Zouave, E. (2020). *Strategisk verktygslåda mot hybridhot: Ett ramverk för gemensam problemförståelse.* Stockholm: Totalförsvarets forskningsinstitut, FOI. https://www.foi.se/rest-api/report/FOI-R--4816--SE

David, M. & Sutton, C.D. (2016). *Samhällsvetenskaplig metod* (S-E. Torhell, övers.). Studentlitteratur.

Degerman, H. (2021). Barriers towards resilient performance among public critical infrastructure organizations: the refugee influx case of 2015 in Sweden. *Infrastructures, 6*(8), 106. https://doi.org/10.3390/infrastructures6080106

Deverell, E., Alvinius, A., & Hede, S. (2019a). Horizontal collaboration in crisis management: an experimental study of the duty officer function in three public agencies. *Risks, Hazards & Crisis in Public Policy, 10*(4), 484-508. https://doi.org/10.1002/rhc3.12179

Deverell, E., Alvinius, A., & Hede, S. (2019b). Maktförskjutning och maktutjämning i myndighetssamverkan: en kvalitativ studie om tjänstemän i beredskap på regional nivå. *Statsvetenskaplig Tidskrift, 121*(4), 549-567.

Dowse, A., & Dov Bachmann, S. (2022). Information warfare: methods to counter disinformation. *Defense & Security Analysis 38*(2), 453-469. https://doi.org/10.1080/14751798.2022.2117285

Duchek, S. (2020). Organizational resilience: a capability-based conceptualization. *Bus Res, 13*, 215-246. https://doi.org/10.1007/s40685-019-0085-7

Ekengren, M., Engström, A., & Rhinard, M. (2021). Coronapandemin - en smygande kris vintern 2020. *Statsvetenskaplig Tidskrift 123*(5), 33.

Eriksson-Zetterquist, U. & Ahrne, G. (2015). Intervjuer. I G. Ahrne & O. Svensson (red), *Handbok i kvalitativa metoder* (2:4 uppl., s. 34-54). Liber.

Frostling-Henningsson, M. (2017). *Kvalitativa metoder: introspektion, poesi, netnografi, collage och skuggning*. Studentlitteratur AB.

Giles, K. (2016). *Handbook of Russian information warfare*. (NDC fellowship monograph series, Vol. 9). NATO Defence College Research Division. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf

Giles, K. (2023). Russian cyber and information warfare in practice; Lessons observed from the war on Ukraine. *Chatham house*. https://doi.org/10.55317/9781784135898

Graziano, A. M. & Raulin, M. L. (2012). *Research methods: a process of inquiry: international edition.* Pearson Education Limited.

Hellman, M. (2021). Infodemin under pandemin: Rysk informationspåverkan mot Sverige. *Statsvetenskaplig Tidskrift, 123*(5), 451-474.

Hellman, M. & Wagnsson, C. (2017). How can European states respond to Russian information warfare? An analytical framework. *European security, 26*(2), 153-170. https://doi.org/10.1080/09662839.2017.1294162

Jacobsen, D. I. (2017). *Hur genomför man undersökningar? Introduktion till samhällsvetenskapliga metoder.* Studentlitteratur AB.

Jonsson, O. (2019). *The Russian understanding of war: blurring the lines between war and peace*. Georgetown University Press. https://doi.org/10.2307/j.ctvr697c8

Kragh, M., & Åsberg, S. (2017). Russia's strategy for influence through public diplomacy and active measures: the Swedish case. *Journal of Strategic Studies, 40*(6), 773-816. https://doi.org/10.1080/01402390.2016.1273830

Kvale, S., & Brinkmann, S. (2014). *Den kvalitativa forskningsintervjun.* Studentlitteratur AB.

Larsen, A. (2009). *Metod helt enkelt - en introduktion till samhällsvetenskaplig metod.* Gleerups Utbildning AB.

Lei, H. (2019). Modern information warfare: analysis and policy recommendations. *Foresight: the Journal of Future Studies, Strategic Thinking and Policy, 21*(4), 508-522. https://doi.org/10.1108/FS-06-2018-0064

Medieakademin. (2023). *Fortroendebarometern 2023*. https://medieakademin.se/wp-content/uploads/2023/03/Presentation_fortroendebarometern_2023-WEBB-Final.pdf

Myndigheten för samhällsskydd och beredskap (MSB). (2019). *Att möta informationspåverkan - handbok för kommunikatörer.* https://rib.msb.se/bib/Search/Document?id=28778

Nilsson, P. E., Olsson, S., & Ekman, I. (2022). *Den nya informationsmiljöns topografi - teknik, människa och strategi i osäkerhetens tidevarv* (FOI-R--5342--SE). Totalförsvaret Forskningsinstitut (FOI), Avdelningen för försvarsanalys. https://www.foi.se/rest-api/report/FOI-R--5342--SE

Palmertz, B. (2021). Influence operations and the modern information environment. I Weissman, M., Nilsson, N., Thunholm, P., & Palmertz, B. (Eds.), *Hybrid Warfare: Security and Asymmetric conflict in International Relations* (s. 113-131). I.B. Tauris.

Pamment, J., Nothhaft, H., Agardh-Twetman, H., & Fjällhed, A. (2018). *Countering information influence activities: the state of the art*. Myndigheten för samhällsskydd och beredskap, MSB. https://rib.msb.se/filer/pdf/28697.pdf

Porche III, I. R. (2020). *Cyberwarfare: An Introduction to Information-Age Conflict*. Artech House.

Ryan, G.W. & Bernard, H.R. (2003). Techniques to identify themes. *Field Methods, 15*(1), 85-109. https://doi.org/10.1177/1525822X02239569

Säkerhetspolisen (2024). *Säkerhetspolisen 2024/2024*. https://sakerhetspolisen.se/download/18.5cb30b118d1e95affec37/1708502268494/L%C3%A4gesbild%202023-2024.pdf

Wagnsson, C. (2023). Rysk informationspåverkan som varaktigt hot. *Statsvetenskaplig Tidskrift, 125*(3), 649-667

Weick, K. E. (1993). The collapse of sensemaking in organizations: the mann gulch disaster. *Administrative Science Quarterly*, *38*(4), 628–652. https://doi.org/10.2307/2393339

Bilagor

Bilaga 1: Intervjuguide för organisationer som utsatts för informationspåverkan

Bakgrund

- Skulle du kunna börja med att berätta lite om din arbetsplats och din befattning i den?
- Kan du berätta om hur den organisation du arbetar på har utsatts för illasinnad informationspåverkan?

Innan händelsen

- Pratade man om potentiell informationspåverkan inom organisationen innan man utsattes? Hur, vad pratade man om?
- Hur förberedda upplevde du att organisationen/medarbetare/chefer var?
- Innan informationspåverkan började, hade ni några utbildningar om illasinnad informationspåverkan eller spridning av desinformation?
- Hade ni några utbildningar kopplat till Ryssland som ett hot mot Sverige?
- Hade ni några arbetsmetoder för att motverka illasinnad informationspåverkan eller ryktesspridning?
- Hade ni några arbetsmetoder eller funktioner för att förutse eller identifiera risker? Hur såg de ut?
- Upplevdes spridning av desinformation som en risk/ett hot?
- Hade ni några arbetsmetoder eller processer för att rapportera eventuella hot/risker?
- Fick ni något stöd eller utbildning av andra myndigheter eller organisationer innan ryktesspridningen startade/för att motverka att ryktesspridning skulle inträffa?

Under händelsen

- När insåg ni att informationspåverkan/spridningen av desinformation kunde innebära en risk för organisationen?

- Hur såg processen ut då ni identifierade informationspåverkan/spridningen av desinformation som ett hot?
- Hur tolkades informationspåverkan/spridningen av desinformation? Såg man det som ett hot mot organisationens verksamhet, eller antog man att det var något som skulle blåsa förbi?
- På vilket sätt upplevdes informationspåverkan/spridningen av desinformation som ett hot, varför? Mot vem? Hur påverkades medarbetare, chefer, organisationer, uppgiften?
- Hur valde ni att hantera informationspåverkan/spridningen av desinformation?
- Fick ni något stöd från andra myndigheter/organisationer för att hantera informationspåverkan/spridningen av desinformation? Hur såg det stödet ut?
- Hur upplevdes de myndigheterna/organisationerna tolka situationen?
- Upplevde ni att ni fick det stöd ni behövde? Vad hade ni behövt istället?

Efter händelsen

- Upplevde du att organisationen försökte lära av informationspåverkan/spridningen av desinformation?
- Har ni några arbetsmetoder för att motverka att en liknande situation inträffar igen?
- Fick ni något stöd av andra myndigheter/organisationer för att bearbeta och lära av händelsen?
- Upplevde du att andra myndigheter/organisationer tog kontakt med er för att lära sig om händelsen?

Bilaga 2: Intervjuguide för operationella organisationer

Bakgrund

- Kan du börja med att berätta om din arbetsplats och dina arbetsuppgifter?

Organisatorisk resiliens

- Hur anser man att Sverige är utsatt?
- Vilka utmaningar upplever du att Sverige ställs inför kopplat till rysk informationskrigföring?
- Hur pratar man om Ryssland som ett hot inom organisationen? Hur tolkar man hotet?
- Hur ser arbetsprocessen ut för att motverka informationspåverkan - arbetar ni med informationspåverkan i generella termer, eller skiljer man rysk informationspåverkan från andra typer?
- Utbildar man medarbetare (inom organisationen) i rysk informationskrigföring? Utbildar man andra organisationer/myndigheter?
- Vilka strategier anses gynnsamma för att motverka utmaningarna?
- Vilken roll har organisationen i arbetet att motverka utmaningarna?
- Vilka hanteringsstrategier anses gynnsamma när en situation, t.ex. ryktesspridning, inträffar? Kanske fråga om chefer har någon specifik roll i hanteringen?
- Hur bör svenska organisationer och myndigheter förbereda sig, vilket stöd kan ni erbjuda/har ni erbjudit i specifika situationer? Finns det något ni inte har förmåga att stödja i sammanhanget, som ni önskar att ni kunde?

Organisationens relation till andra operationella organisationer

- Vad för organisationer samverkar ni mer?
- Sett till myndigheter/organisationer som arbetar aktivt med hotet om informationspåverkan, vilka prioriterar ni att samverka med?

- Finns det några myndigheter/organisationer som arbetar mer med hotet om informationspåverkan vid jämförelse med andra? Vad beror det på?
- Hur ser samverkan ut med de myndigheterna/organisationerna?
- Hur upplever du att förtroendet för din organisation ser ut hos andra organisationer som ni samverkar med?

Organisationens samverkan med icke-operationella organisationer?

- Vilka icke-operationella organisationer prioriterar ni att ge stöd åt?
- Hur arbetar ni med att stärka organisationernas resiliens?
- Hur samverkar ni med organisationer som inte arbetar aktivt med hot mot Sverige?
- Vilka utmaningar upplever du finns med att utbilda och samverka med icke-operationella organisationer?

Lärdomar

- Hur arbetar ni med lärdomar efter att olika händelser inträffat?
- Samverkar ni med organisationer efter att en händelse, t.ex. större ryktesspridning, inträffat?
- Bidrar ni med något stöd för att utsatta organisationer ska förbättra sina processer för att motverka att det händer igen?

Bilaga 3: Informations- och samtyckesblankett

Informations- och samtyckesblankett vid behandling av personuppgifter i samband med studentarbete

För att behandla personuppgifter måste det inhämtas ett samtycke som på ett tydligt och klart sätt talar om vilka uppgifter som kommer samlas in och vad de ska användas till. Denna informations- och samtyckesblankett förklarar hur personuppgifterna kommer att behandlas samt innehåller kontaktuppgifter.

Personuppgifterna behandlas med ditt uttryckliga samtycke. Deltagande i studien är helt frivillig. Du kan när som helst återkalla ditt samtycke utan att ange orsak. Om du inte samtycker till personuppgiftsbehandlingen kan du göra det utan att drabbas av negativa konsekvenser.

Hur kommer personuppgifterna användas?

Syftet med studien är att bidra till fördjupad kunskap om rysk informationskrigföring i en svensk kontext, genom att undersöka vilka hot och utmaningar som svenska myndigheter ställs inför relaterat till rysk informationskrigföring, samt vilka strategier som anses krävas för att motverka dessa hot och utmaningar. För att uppnå syftet utförs kvalitativa intervjuer med en explorativ ansats. Arbetet inkluderar deltagare både från myndigheter som utsatts för informationspåverkan, samt myndigheter som arbetar aktivt med att motverka den.

För att genomföra studien behöver intervjuer genomföras inom området för informationspåverkan, resiliens och interorganisatorisk samverkan för att uppnå resultat. Intervjun beräknas ta omkring 45-60 minuter.

Studien genomförs inom ramen för masteruppsatsen på programmet Ledarskap och ledning för försvar, krishantering och säkerhet på Försvarshögskolan. Studien är en examinationsuppgift och kommer redovisas som en uppsats som utgör ett självständigt vetenskapligt arbete. Resultatet kommer att presenteras i sammanslagen form, med intervjucitat som illustrationer eller förtydliganden. Data kommer att skrivas om till skriftspråk och presenteras på ett sätt som gör att de inte kommer att kunna härledas till en enskild person.

Vilka personuppgifter kommer att behandlas?

Namn, e-postadress och röstinspelning.

Hur skyddas och lagras dina personuppgifter?

Personuppgifterna kommer att lagras elektroniskt på lösenordsskyddad dator tills att arbetet är examinerat och betygsatt. När personuppgifterna inte längre behövs för ändamålet kommer de

att raderas. Det gäller inspelad ljudfil, intervjuutskrift, det underskrivna samtyckesformuläret samt kontaktuppgifter.

Dina rättigheter

Behöver du få felaktiga uppgifter rättade, komplettera med saknade uppgifter (rättelse) eller ångrar du ditt samtycke (återkallelse) kan du i första hand kontakta ansvarig student och/eller dennes handledare (se kontaktuppgifter nedan). Du kan även vända dig till FHS dataskyddsombud på dataskyddsombud@fhs.se.

Kontaktuppgifter till ansvarig student och handledare

Försvarshögskolan, institutionen för ledarskap och ledning.

Handledare: Sofia Nilsson, sofia.nilsson@fhs.se
Student: Amanda Rönnkvist, a.ronnkvist@gmail.com (alternativt stu220528@student.fhs.se)

Personuppgiftsansvarig är Försvarshögskolan, tel. 08-553 425 00 vx. E-post registrator@fhs.se

Vill du veta mer om hur FHS som myndighet hanterar personuppgifter, se.
https://www.fhs.se/om-forsvarshogskolan/kontakta-oss/om-webbplatsen/personuppgifter-pa-forsvarshogskolan.html

Om du inte är nöjd med hur Försvarshögskolan hanterar dina personuppgifter har du alltid rätt att lämna klagomål till integritetsskyddsmyndigheten (IMY) via e-post imy@imy.se eller telefon 08-657 61 00.

Genom mitt undertecknande nedan bekräftar jag att jag har tagit del av ovanstående information och är införstådd med hur mina personuppgifter kan komma att behandlas. Jag är medveten om att mitt deltagande är helt frivilligt och att jag kan avbryta mitt deltagande i studien utan att ange någon orsak.

Ort och datum

Namnförtydligande

Underskrift