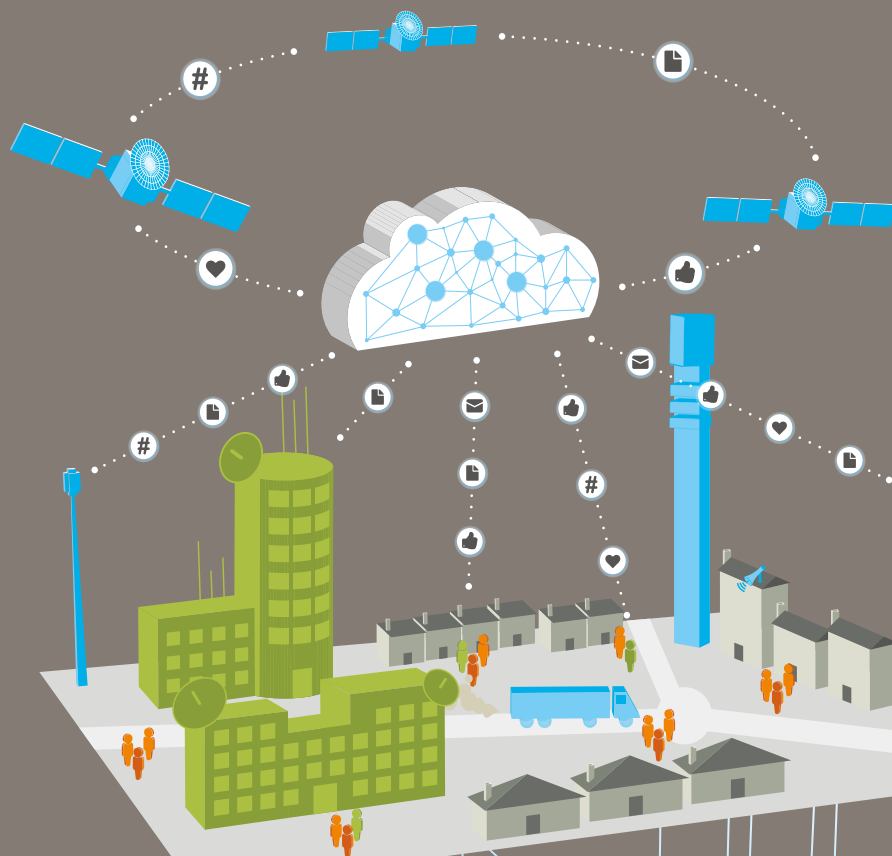




Myndigheten för  
samhällsskydd  
och beredskap

# Mediebranschen 2016

– hot, risker och sårbarheter





# Mediebranschen 2016

– hot, risker och sårbarheter

Mediebranschen 2016 – hot, risker och sårbarheter

Myndigheten för samhällsskydd och beredskap (MSB)

Redaktör: Christina Goede 010-240 43 05

Författare: Erik Ryd och Johan Turell

Produktion: Advant Produktionsbyrå

Tryck: DanagårdLiTHO

Publikationsnummer: MSB1086 - mars 2017

ISBN: 978-91-7383-738-5

## Förord

Det är sex år sedan MSB senast tog fram en analys av hot, risker och sårbarheter i mediebranschen, och under den tiden har förutsättningarna för medierna genomgått stora förändringar, samtidigt som det säkerhetspolitiska klimatet har försämrats.

Bara de senaste två åren har en rad antagonistiska händelser inträffat, som ytterst hotar grundläggande demokratiska värden. Terrorattacken mot redaktionen på Charlie Hebdo 2015, överbelastningsattacker mot flera mediehus i mars 2016 och sabotaget mot Häglaredsmasten i maj 2016 är några sådana exempel. Hot- och hatkampanjer riktade mot enskilda journalister eller redaktioner, försök att plantera falsk information och aggressiv användning av sociala medier som del i påverkanskampanjer, utgör också en del av hotbilden mot mediebranschen.

Mediebolagen är beroende av komplexa informationsinfrastrukturer som kan bli otillgängliga genom oavsiktliga störningar och avbrott. Detta är idag en ständig risk för både distribution och produktion av medialt innehåll. Därutöver har det tuffa ekonomiska läget för flera nyhetstidningar, en snabb teknologisk utveckling och ändrade användarvanor hos konsumenter skapat ytterligare utmaningar.

Fungerande medier är samhällsviktiga som förmedlare av nyheter, samhällsgranskande journalistik och samhällsviktig information. Medierna utgör även en central del i den kedja av system som förmedlar varningar och larm samt viktiga meddelanden från myndigheter under tider av kris, katastrofer och ytterst krig.

Självständig rapportering och ostörda möjligheter att förmedla nyheter är vitala beståndsdelar i en demokrati. Om förutsättningarna rubbas riskerar samhällets funktionalitet att undermineras och demokratin att urholkas. Och om en akut samhällskris inträffar samtidigt som mediekanaler drabbas av avbrott eller på annat påverkas, riskerar det att få allvarliga konsekvenser.

Syftet med denna rapport är att ge en övergripande bild av mediebolagens verksamhetsnära risker och sårbarheter, samt några samhällsrisker där mediebolagen spelar en särskild roll. Rapporten presenterar även utvecklingstrender som kan ha betydelse för mediebolagen och samhällets säkerhets- och beredskapsarbete. Slutligen finns i rapporten förslag till åtgärder.

Stockholm den 20 mars 2017

Nils Svartz  
Tillförordnad generaldirektör

# Innehåll

<b>Sammanfattning</b> .....	<b>11</b>
<b>1. Inledning</b> .....	<b>15</b>
1.1 Mediebolagen – uppgifter och funktion i samhället.....	15
1.2 Om rapporten.....	17
1.3 Syfte och målgrupp .....	19
1.4 Metod .....	19
1.4.1 Materialinsamling .....	19
1.4.2 Avgränsningar.....	21
<b>2. Utveckling och trender</b> .....	<b>23</b>
2.1 Distribution .....	24
2.1.1 Teknikutvecklingen bidrar till förändrade medievanor.....	25
2.1.2 Generell mediekonsumtion .....	27
2.1.3 Ekonomiska trender.....	29
2.2 Produktion .....	31
2.2.1 Att samla in och komma åt information .....	32
2.2.2 Att välja ut och rapportera nyheter .....	34
2.2.3 Mediers journalistiska nyhetsinnehåll .....	35
2.3 Hot och trakasserier mot medier .....	37
2.4 Mediebranschen och påverkanskampanjer .....	40
2.4.1 Förändrade förutsättningar och olika typer av påverkan .....	41
2.4.2 Hot som del av påverkanskampanjer .....	44
2.4.3 Cyberattacker som del av påverkanskampanjer .....	45
2.5 Mediebranschen och några allvarliga incidenter .....	47
2.5.1 Terrorattacken mot Charlie Hebdo den 7 januari 2015.....	47
2.5.2 Teracoms masthaveri i Häglared den 15 maj 2016.....	49
2.5.3 Överbelastningsattackerna mot svenska mediehus den 19 mars 2016.....	51
2.5.4 Överbelastningsattackerna mot Dyn DNS den 21 oktober 2016 .....	53

<b>3.</b>	<b>Samhällsviktig verksamhet inom mediebranschen.....</b>	<b>57</b>
3.1	Inledning.....	57
3.2	Enkätundersökning riktad till mediebranschen.....	58
3.3	Övergripande om samhällsviktig verksamhet i mediebranschen.....	58
3.4	Identifierade samhällsviktiga verksamheter inom mediebranschen.....	62
3.4.1	Krishantering.....	62
3.4.2	Granskning.....	65
3.4.3	Trygghet.....	65
<b>4.</b>	<b>Risker och sårbarheter i mediebranschen.....</b>	<b>67</b>
4.1	Inledning.....	67
4.2	Metod för riskanalysen.....	67
4.2.1	Sammanställning av de verksamhetsnära riskerna.....	69
4.2.2	Sammanställning av samhällsriskerna.....	70
4.3	Beroenden och sårbarheter.....	71
4.4	Verksamhetsnära risker och sårbarheter.....	73
4.4.1	Personal kommer att skadas fysiskt eller psykiskt.....	73
4.4.2	Verksamhetskritisk information kommer att bli otillgänglig.....	76
4.4.3	Egendom kommer att drabbas av skada.....	78
4.4.4	Verksamhetskritisk information kommer att bli röjd.....	80
4.4.5	Allmänhetens förtroende för organisationen kommer att minska.....	82
4.4.6	Verksamhetskritisk information kommer att bli felaktigt ändrad.....	84
4.4.7	Verksamhetskritisk information kommer att bli felaktigt raderad.....	87
4.5	Samhällsrisker och sårbarheter.....	88
4.5.1	Påverkanskampanjer bedrivs mot allmänheten och beslutsfattare genom medier.....	88
4.5.2	Sveriges informationsinfrastruktur är otillräckligt skyddade mot angrepp.....	91
4.5.3	Mediekonsumtionen ger inte redundans till krisberedskapen.....	94
4.5.4	Samhället har en otillräcklig beredskap för att hantera storskaliga och plötsliga kontroverser...	97
4.5.5	Vissa områden och samhällsgrupper hamnar i medieskugga.....	100
4.6	Syntes.....	102
4.6.1	Påverkan och samhällets krisberedskap.....	103
4.6.2	Påverkan och angrepp mot informationsinfrastruktur.....	103
4.6.3	Storskaliga kontroverser och angrepp.....	104
4.6.4	Övergripande slutsatser.....	105

<b>5. Mediebranschen och det civila försvaret.....</b>	<b>107</b>
5.1 Höjd beredskap – identifierade risker och sårbarheter .....	108
5.2 Lärdomar från omvärldsbevakning .....	110
<b>6. Åtgärdsförslag .....</b>	<b>113</b>
6.1 Åtgärdsförslag till mediebolagen.....	113
6.1.1 Ta fram skyddsstrategier för journalister i digitala miljöer .....	113
6.1.2 Utveckla ett systematiskt arbete med informationssäkerhet inom mediebolagen.....	113
6.2 Åtgärdsförslag till myndigheter .....	115
6.2.1 Stöd insatser för ökad medie- och informationskunnighet .....	115
6.2.2 Satsa på medvetandehöjande insatser om olika kriskommunikationskanaler vid kris.....	116
6.2.3 Utredda ett interaktivt kriskommunikationssystem .....	117
6.2.4 Se över hot och trakasserier mot medier.....	118
6.2.5 Se över konsekvenserna av medieskugga.....	119
6.3 Gemensamma insatser för ett stärkt civilt försvar .....	119
<b>Bibliografi .....</b>	<b>124</b>





# Sammanfattning

## Sammanfattning

År 2010 genomförde MSB en kartläggning av risker och sårbarheter i mediebranschen. Under de senaste åren har medielandskapet förändrats och fortsätter att ändras i snabb takt. Medieföretagens villkor och verksamhet utvecklas ständigt. Så även arbetet med säkerhet och beredskap i och med nya arbetsformer, ändrade ekonomiska förutsättningar och nya riskbilder som uppstår.

I denna rapport ger MSB en uppdaterad bild över de hot, risker och sårbarheter som identifierats för svenska mediebranschen under 2016. Riskerna har analyserats, dels utifrån fredstida förhållanden, dels utifrån höjd beredskap. Kontinuitet i mediebolagens verksamhet har stått i fokus.

Resultatet är tänkt att fungera som underlag för det fortsatta arbetet med medieberedskap samt för att sprida ytterligare kunskap om ämnesområdet. I rapporten presenteras även åtgärdsförslag som, om de vidtas, förhoppningsvis kan leda till att riskerna begränsas, eller att sårbarheter hanteras.

Underlaget för rapporten har inhämtats genom en enkätundersökning riktad till branschaktörer, workshops tillsammans med Mediernas beredskapsråd, litteraturstudier samt omvärldsbevakning och intervjuer med branschaktörer.

I rapporten har två typer av risk analyserats; verksamhetsnära risker och samhällsrisker. Verksamhetsnära risker avser risker som har en nära koppling till mediebolagen respektive deras verksamhet. Den andra typen av risk avser risker för samhället i stort som har en tydlig bäring på, eller tar sina avstamp i, mediebranschen.

MSB bedömer att de verksamhetsnära riskerna för mediebranschen (i fallande ordning efter störst risk) är att:

- personal kommer att skadas fysiskt eller psykiskt
- verksamhetskritisk information kommer att bli otillgänglig
- egendom kommer att drabbas av skada
- verksamhetskritisk information kommer att bli röjd
- allmänhetens förtroende för organisationen kommer att minska
- verksamhetskritisk information kommer att bli felaktigt ändrad
- verksamhetskritisk information kommer att bli felaktigt raderad.

MSB bedömer därutöver att samhällsriskerna för mediebranschen (i fallande ordning efter störst risk) är att:

- påverkanskampanjer bedrivs mot allmänheten och beslutsfattare genom medier
- sveriges informationsinfrastrukturer är otillräckligt skyddade mot angrepp
- mediekonsumtionen inte ger redundans till krisberedskapen
- samhället har en otillräcklig beredskap för att hantera storskaliga och plötsliga kontroverser
- vissa områden och samhällsgrupper hamnar i medieskugga.

MSB föreslår åtta åtgärder för att bemöta de risker som identifierats i analysen:

- ta fram skyddsstrategier för journalister i digitala miljöer.
- stödja utvecklandet av ett systematiskt arbete med informationssäkerhet inom mediebolagen
- stödja insatser för ökad media- och informationskunnighet (MIK) hos befolkningen
- satsa på medvetandehöjande insatser om olika kriskommunikationskanaler vid kris
- utreda ett interaktivt kriskommunikationssystem
- se över hot och trakasserier mot medier
- se över konsekvenserna av medieskugga
- stärka det civila försvaret genom att öka mediernas robusthet.

MSB har översiktligt analyserat mediebranschens förutsättningar till kontinuitet vid krigsfara och krig under höjd beredskap. MSB bedömer att mediebolagen behöver fortsätta, och i många fall utöka, sitt arbete med planering för hela hotskalan inklusive civilt försvar. En del i det är att stärka sin generella krisberedskapsförmåga.



# Inledning

# 1. Inledning

## 1.1 Mediebolagen – uppgifter och funktion i samhället

*”Människors lika värde samt invånarnas jämlika och jämställda möjligheter till inflytande och aktivt deltagande i samhällslivet är ett nationellt intresse. Yttrandefrihet, informationsfrihet, rätten till utbildning, mötesfrihet, demonstrationsfrihet, föreningsfrihet samt religions- och övertygelsefrihet är några av de mänskliga rättigheter som ska skyddas genom arbetet för Sveriges säkerhet. Demokrati, mänskliga fri- och rättigheter, samt Sveriges säkerhet stärks av fria, självständiga medier.*

*Robusta samhällskommunikationer, i synnerhet mellan myndigheter, är av central betydelse. Hur myndigheter, allmänhet och medier kommunicerar kan även vara avgörande för hur en kris eller händelse utvecklar sig.”*

Våra nationella intressen  
Nationell säkerhetsstrategi  
Regeringen, 2017

Utöver att göra nytta i alla de bemärkelser som bolag på den svenska marknaden gör för Sverige bedömer MSB att mediebranschen bedriver samhällsviktig verksamhet ur flera perspektiv. Under normala förhållanden har svenska medier en viktig roll i sitt uppdrag att granska och rapportera om maktutövningen i Sverige på lokal, regional, nationell och EU-nivå, samt Sveriges och svenska aktörers förhållanden utomlands. På detta sätt kan människor få en inblick i förtroendevaldas och andra beslutsfattares arbete och ges förutsättningar att följa och påverka samhällsutvecklingen.

Vid extraordinära händelser förblir de ovan nämnda uppgifterna fortsatt relevanta, samtidigt som mediebranschen också får en viktig roll i att tillhandahålla och upprätthålla samhällets varnings, larm- och informationssystem. Delar av mediebranschen är central för den svenska krishanteringen i fråga om när det gäller såväl informationsspridning som beslutsfattande. Viktigt meddelande till allmänheten (VMA)<sup>1</sup> och kärnkraftslarm är exempel på larmsystem som är beroende av den informationsinfrastruktur som mediebranschen tillhandahåller.

---

1. Se kapitel 3 Samhällsviktig verksamhet inom mediebranschen nedan.

Under perioder av ökad oro och säkerhetspolitisk instabilitet i omvärlden har medierna ett stort ansvar att rapportera till allmänheten, oavsett förekomsten av allvarliga samhällstörningar. Det öppna och demokratiska samhället ska fortsatt bevaras även om Sverige skulle dras in i ett krig eller om krigsliknande förhållanden skulle uppstå inom eller i anslutning till Sveriges gränser. Åsiktsfrihet och fria medier ska vidmakthållas.

Public service, som består av Sveriges Radio (SR), Sveriges Television (SVT) och Sveriges Utbildningsradio (UR), har via sina statliga uppdrag och regleringar ett särskilt ansvar att förmedla information från myndigheter till allmänheten. De har även en särskilt angiven roll och ett ansvar i totalförsvaret, vilket är den verksamhet som förbereder Sverige för krig.

Mediebranschen genomgår stora förändringar på grund av den snabba teknikutvecklingen, ökad konkurrens på den globala mediemarknaden och förändrad medieanvändning hos enskilda individer och samhällsinstitutioner. Antalet befintliga redaktioner och journalister minskar i det som bland annat kallats tidningskrisen, samtidigt som de kvarvarande aktörerna anpassar sig till nya digitala plattformar, såsom webb-tv och sociala medier, för att nå konsumenterna. Kravet på snabbhet och omedelbar nyhetsförmedling har varit ständigt närvarande inom branschen ända sedan direktsänd tv via satellit introducerades på 1990-talet. Den digitala tekniken kan sägas ha ytterligare skruvat upp kraven på snabbhet, inte minst i fråga om kris- och konfliktrapportering.

Den enskilde individen har tillgång till en allt större mängd information och därtill har möjligheterna att styra informationsflödet utifrån eget intresse ökat. Via sociala medier skapas informella grupperingar som i kraft av gemensamma intressen, värden eller ideologier delar ett urval av nyheter och annan information med varandra, och där förtroenderelationer inom gruppen styr vilken grad av trovärdighet som tillskrivs både den information som delas och den som inte delas. Prenumerationer på nyhetsmedier och andra sociala medieplattformar gör också att enskilda individer snabbt kan delta i och ta del av nyhetshändelser, när de händer.

Dagens omfattande informations- och medieflöde karaktäriseras av lättillgänglighet och låga trösklar för att både skapa och sprida information. I det ständiga flödet har många möjligheter uppstått och fördelarna är många för både ekonomisk och samhälllig utveckling. Parallellt med de positiva effekterna uppstår också utmaningar med att para ihop kraven på lättillgänglighet och snabbhet i rapporteringen med journalistiska värden som vali-



dering, verifiering och källkritik. Problematiken kan göra det svårt för den enskilde att avgöra vad som är sant och falskt. I begränsad utsträckning kan också en trend skönjas där det viktigaste inte längre är att kunna avgöra vad som är sant och vad som inte är sant, utan snarare att få informationen att ge stöd åt en viss attityd eller ett visst perspektiv.

Sett från ett strategiskt kommunikationsperspektiv skapar detta en säkerhetsproblematik. Medierna är idag ett verktyg för såväl de som vill sprida välgrundad information som de som vill bedriva påverkanskampanjer. Liksom andra liberala demokratier är Sverige utsatt för påverkanskampanjer. Sverige har också, i kraft av fria och oberoende medier, resurser för att motverka och bemöta sådan påverkan.

Den försvarspolitiska inriktningen för 2016–2020 betonar att Sverige ska kunna identifiera och möta påverkanskampanjer som hotar det öppna samhället eller som syftar till att påverka Sveriges säkerhetspolitik. Hotet mot mediebranschen begränsas dock inte till olika påverkansförsök genom exempelvis planterade falska nyheter, vilseledning och trakasserier av journalister – även distributionsinfrastrukturen står under hot från olika former av cyberattacker och sabotage.

## 1.2 Om rapporten

MSB följer och analyserar utvecklingen inom medieområdet utifrån ett beredskapsperspektiv. Arbetet sker i nära samarbete med säkerhets- och beredskapschefer samt tekniskt ansvariga inom branschen inom ramen för Mediernas beredskapsråd. MSB:s roll i detta sammanhang är att fungera som kunskapsförmedlare och samtalspartner till mediebolag och andra aktörer som myndigheter och departement. Mer information om detta arbete finns i den externa bilagan 3.

Risk- och sårbarhetsanalyser om mediebranschen har tidigare gjorts av Styrelsen för psykologiskt försvar 2006, 2007 och 2008. MSB tog därefter vid och tog fram rapporten *Mediebranschen 2011 – Hot, risker och sårbarheter*. För att behålla en kontinuerlig analys och bedömning av mediebranschens förutsättningar att fortsätta uppfylla sin viktiga samhällsroll har MSB nu tagit fram denna rapport. Syftet är att ge en övergripande bild av för mediebolagen verksamhetsnära risker och sårbarheter, samt några samhällsrisker där mediebolagen spelar en särskild roll. Rapporten<sup>2</sup> presenterar även

---

2. *Mediebranschen 2016 – Hot, risker och sårbarheter* benämns inte som en risk- och sårbarhetsanalys eftersom begreppet har en formell betydelse som är reglerad i föreskrift.

utvecklingstrender som kan ha betydelse för mediebolagen och samhällets säkerhets- och beredskapsarbete.

Rapportens övergripande upplägg från och med kapitel 2 är att först beskriva utveckling och trender inom mediebranschen. Kapitlet är initialt uppdelat på branschens två traditionella ben: produktion och distribution. Det omfattar också ett särskilt avsnitt om hot och våld mot personer verksamma inom branschen. Syftet är att ge en kontextuell inramning, det vill säga ett sammanhang, för det som sedan beskrivs.

I de tre följande avsnitten redogörs för aspekter som har betydelse för hotbilden mot medierna. I avsnitt 3 presenteras utveckling och trender i fråga om hot och trakasserier riktade mot medierna. I avsnitt 4 presenteras en fördjupad redogörelse för den påverkan som riktas mot mediebranschen och påverkan som bedrivs genom olika mediekanaler mot allmänheten och beslutsfattare. I avsnitt 5 presenteras några för mediebranschen avgörande incidenter som på olika sätt illustrerar den mer extrema delen av hotbilden mot medier.

I kapitel 3 presenteras tre typer av samhällsviktig verksamhet inom mediebranschen. Syftet är att ge en bild av vad som är särskilt skyddsvärt inom branschen, utifrån ett samhällsperspektiv. I kapitel 4 redovisas en riskanalys utifrån utveckling och trender, hotbilden, och den samhällsviktiga verksamheten. Redovisningen är uppdelad i för mediebolagen verksamhetsnära risker respektive samhällsrisker.

Fram till och med riskanalysen har alla redogörelser och analyser utgått från ett läge av fred i Sverige och dess närområde. I kapitel 5 varieras den grundpremisen. I kapitlet analyseras mediebolagens roll inom det civila försvaret, vilka omständigheter de kommer att verka inom under höjd beredskap samt hur den i kapitel 4 presenterade riskbilden förändras under höjd beredskap.

Rapporten avslutas med kapitel 7, där en uppsättning åtgärdsförslag och rekommendationer presenteras.

I bilagorna, som är separerade från rapporten till ett externt dokument, finns bland annat en fördjupning av kapitel 2: Utveckling och trender där de två avsnitten om distribution respektive produktion som presenteras nedan utökas.

## 1.3 Syfte och målgrupp

Syftet med rapporten är att ge svenska medier, politiker och myndigheter samt den intresserade allmänheten en helhetsbild över hot, risker och sårbarheter för mediebranschen, dels utifrån ett tillstånd av fred, dels utifrån höjd beredskap. Syftet är också att presentera en uppsättning åtgärdsförslag som, om de genomförs, kan leda till att riskernas sannolikhet eller konsekvenser begränsas, eller att sårbarheter hanteras.

Den primära målgruppen för rapporten är medierna och sekundära målgrupper är politiker och berörda myndigheter. Rapporten presenterar två typer av risker, verksamhetsnära risker och samhällsrisker. Den första kategorin är avsedd att vara ett stöd för medierna i det egna säkerhetsarbetet. Den avser risker med en direkt bäring på mediernas verksamhet i vardagen.

De nedan presenterade samhällsriskerna är avsedda att utgöra ett kunskapsunderlag för såväl den primära som den sekundära målgruppen. Åtgärdsförslag presenteras för båda målgrupperna. En tertiär målgrupp är den intresserade allmänheten.

Redogörelserna som presenteras inom respektive kapitel nedan har tagits fram med målsättningen att de ska vara så utförliga som intresserar sig för frågorna ska kunna skaffa sig en egen uppfattning utan att i särskilt stor grad behöva konsultera andra källor.

## 1.4 Metod

### 1.4.1 Materialinsamling

Enkätundersökning riktad till mediebranschen

Under hösten 2016 har MSB genomfört en enkätundersökning om hot, risker och sårbarheter inom mediebranschen. Undersökningen var helt frivillig och totalt kontaktades 111 verkamma inom den svenska mediebranschen. 49 respondenter besvarade enkäten i sin helhet. Urvalet gjordes utifrån offentliga register över bolag med registrerad medierelaterad verksamhet och huvudkontor i Sverige. Respondenterna fördelades över små (1–199 anställda) och stora (200+ anställda) bolag, huruvida de är distribuerande eller producerande, samt utifrån den spridning över landet som de har (lokal,

regional, nationell, ej geografiskt avgränsad). Det låga antalet svar gör att viss försiktighet bör beaktas i fråga om hur säkra resultaten är.<sup>3</sup>

Däremot kan representativiteten för den svenska mediebranschen anses god. Sammantaget leder det till att enkätundersökningens resultat möjliggör förhållandevis detaljerade problembeskrivningar vad gäller hot, risker och sårbarheter för branschen. Dessa problembeskrivningar gör det i sin tur möjligt att formulera åtgärdsförslag. Det är dock oklart om de problembeskrivningar och åtgärdsförslag som undersökningen resulterar i skulle framstå som lika väl motiverade om antalet respondenter hade varit högre. MSB bedömer dock att bilden som ges är viktig att förmedla – under förutsättning att osäkerheten i resultaten betonas.

#### Workshopar med Mediernas beredskapsråd

I oktober och december 2016 höll MSB särskilda workshoppar med Mediernas beredskapsråd. Där diskuterades riskbilden mot medierna, samhällsrisker med bäring på medierna samt frågor med koppling till civilt försvar och höjd beredskap. Syftet var att ta in information om hur medierna anpassat sitt säkerhetsarbete med anledning av det förändrade säkerhetspolitiska läget. Mer ingående information om den privat-offentliga samverkan som tar plats inom Mediernas beredskapsråd finns iden externa bilagan 3: MSB och medieberedskap.

#### Intervjustudie med medieföreträdare

För att ytterligare fördjupa kunskapen om riskbilden och frågor med koppling till den återupptagna planeringen för det civila försvaret, och för att grunda frågeställningarna i några medieorganisationers egna omständigheter så genomfördes en intervjustudie med merparten av medlemmarna i Mediernas beredskapsråd och ytterligare företrädare för bolag i branschen.

#### Litteraturstudie och omvärldsbevakning

I arbetet med den föreliggande rapporten har en omfattande omvärldsbevakning bedrivits. Dessutom har en särskild litteraturstudie genomförts. Studien behandlade trender och utveckling inom, eller med bäring på mediebranschen, samt frågeställningar med koppling till påverkanskampanjer och mediebranschen.

---

3. Med 49 svarande av totalt 111 kontaktade respondenter och en konfidensnivå (statistisk säkerhet) om 95 procent blir inte alla de redovisade resultaten i rapporten statistiskt signifikanta.

## Analys

MSB har analyserat och kontinuerligt bedömt allt insamlat material utifrån dess relevans för framställningen. Särskilda analyser har genomförts med avseende på bolagens beroenden, mediebranschens samhällsviktiga verksamhet, risker och sårbarheter, samt mediebranschen och det civila försvaret.

Mer ingående beskrivningar av vissa delar av analysen, vars metodik MSB har bedömts vara särskilt värd att framhäva, presenteras i kapitel 3: Samhällsviktig verksamhet inom mediebranschen, avsnitt 3.2 Enkätundersökning riktad till mediebranschen nedan.

### 1.4.2 Avgränsningar

Rapporten avgränsas till att primärt analysera de så kallade traditionella *mediebolagen* – radio, tv, nyhetsbyråer, dagstidningar, webbmedier samt leverantörer av informationsinfrastruktur för mediedistribution. I det nya medielandskapet har såväl nya kanaler som aktörer tillkommit i och runt mediebranschen – dessa tas också upp i de fall där det påverkar den roll och funktion som traditionella medier har i samhället, men utelämnas i övrigt.

Redogörelser för trender och utveckling inom mediebranschen är uppdelad på branschens två traditionella ben: distribution och produktion. Distribution ska i rapporten förstås som förmedling av information i stor skala, till en potentiellt stor publik. Samhälleliga larmsystem har därför även inkluderats i det. Till produktion har räknats nyhetsbyråer och andra aktörer som producerar det material som enskilda individer i slutändan konsumerar. Fokus inom branschen har legat på traditionella mediebolag såsom tidningar, tv, radio och bolag som möjliggör distribution av information för respektive medium. Nyare medieaktörer, som sociala medier och bolag som Google berörs också, fast i begränsad utsträckning.

Medierna verkar inom en bransch som använder många och avancerade teknologier. För att behålla läsbarheten har fördjupningen i tekniska detaljer hållits begränsad. Det har i sin tur inneburit att vissa nischer inom branschen har belysts mer än andra. Ett exempel på en nisch inom mediebranschen som därmed inte har prioriterats närmare är tryckeribranschen.

**Utveckling och trender**

## 2. Utveckling och trender

Mediebranschen förändras snabbt och den teknologiska utvecklingen och mediernas ekonomiska situation har stor betydelse för branschens utveckling. Den teknologiska utvecklingen har möjliggjort effektiviseringar för både det redaktionella arbetet och distributionen av nyheter.

Digitalisering är ett nyckelord i det nya medielandskapet. Med digitalisering avses den teknologiskt drivna processen att förändra tidigare tekniker, exempelvis analog teknik, till digital teknik – inom alla aspekter av samhället. Förutom att stärka och förbättra redan existerande metoder tillåter digitalisering även nya innovationer och kreativitet. Mediebranschen, liksom det övriga samhället, deltar i och påverkas av processen. Digitaliseringen har i sig lett till ett större beroende av uppkoppling vilket i sig medför större risker genom exponering av egna it-system mot internet.

Genom digitaliseringen och användandet av ny teknik har mediekonsumtionen ändrats vilket ytterligare utmanat de traditionella mediebolagens ekonomi, finansiella modeller och verksamhet. Jättar inom digitaliseringen som Facebook, Twitter, Amazon och Google har under de senaste åren fått en allt större roll i det svenska medielandskapet, främst som konkurrenter om annonsintäkter och inflytelserika distributionskanaler för medialt material.

Utvecklingen inom mediebranschen tycks gå mot att allt färre kan eller vill producera den journalistik som allt fler vill tjäna pengar på att distribuera. Gränsdragningen mellan den professionella medieproducenten, exempelvis journalisten eller nyhetsbolaget, och den icke-professionella producenten har blivit svår att upprätthålla. Detta har framförallt inneburit en stor utmaning för nyhetsjournalistiken som genre och profession. Journalistiken har lämnat det tidigare tillvägagångssättet av att ”gå ut”, leta upp och samla in information för att skapa en nyhetsberättelse. Idag handlar journalistik mer om att sälla i och värdera ett nästan oändligt informations- och bildflöde och skapa nyhetsberättelser utifrån det.

Detta kapitel har inledningsvis delats in i två för branschen traditionella pelare: produktion och distribution. Exempel på producerande verksamhet inom branschen är framtagande av nyheter, nöjesprogram, och annat innehåll som sedan förekommer i tidningar och tidskrifter, tv, radio, på sociala medier och i övrigt på internet. Exempel på distribuerande verksamhet inom branschen är operatörer av informationsinfrastruktur som möjliggör telefoni (mobil och fast), internetåtkomst, tv- och radioutsändningar.

Uppdelningen är användbar för att redogöra för och diskutera utvecklingstrender, men det är viktigt att komma ihåg att den numera enbart delvis speglar verkligheten. Många av branschens aktörer sysslar i någon mån med både produktion och distribution, och vid en internationell utblick finns indikationer på att det i framtiden kan bli vanligt att uppköp leder till att distribution och infrastruktur tillsammans med produktion och medieinnehåll ägs av en och samma storkoncern.

I den här rapporten avses med distribution de olika metoder och tekniker som används för att leverera medieinnehållet från producent till konsument. Här ingår de distributionsplattformar genom vilka befolkningen tar del av materialet. De mer traditionella plattformarna består av utdelning av tryckta tidskrifter och tidningar, samt av radio- och tv-sändningar. Under de senaste decennierna har dessa mediekkanaler fått sällskap av nya plattformar som vuxit fram genom den teknologiska utvecklingen, framför allt genom internet.

Eftersom viss teknologisk och ekonomisk utveckling som har skett inom distribution också har lett till förändringar inom produktion presenteras distributionen först.

Produktion omfattar i denna rapport insamlandet av underlag till, samt framställandet och bearbetandet av medieinnehåll, och då främst nyheter.

Utöver utvecklingen inom distribution och produktion finns också en särskild hotbild mot mediebranschen. Hot och trakasserier kopplat till arbetet är vardag för många journalister. Påverkanskampanjer bedrivs i dag genom flera mediekkanaler – mediebranschen utsätts för desinformation, hot, och cyberattacker i syfte att påverka allmänheten och beslutsfattare. Under de senaste två åren har mediebranschen dessutom utsatts för allvarliga incidenter som på olika sätt illustrerar den mer extrema delen av hotbilden mot medier. Allt detta redogörs för i avsnitt tre till fem nedan.

## 2.1 Distribution

Utvecklingen av distributionsdelen inom mediebranschen har under de senaste åren karaktäriserats av skiftet från traditionell mediers (etermedias) tablåstyrda utbud till den större valfriheten och interaktiviteten på uppkopplade plattformar. Denna process har till stor del formats av det nya medielandskapets distributionsteknik. Här har även mediekonsumtionen hos användare spelat en stor roll.



### 2.1.1 Teknikutvecklingen bidrar till förändrade medievanor

Utvecklingen inom mediebranschens distributionsdel styrs genom ett samspel mellan bolagen och mediekonsumenterna. Bolagen gör nysatsningar inom teknik och plattformar där de tror att användningen kommer att öka och uppfattningen om var användningen kommer att öka grundar sig i stor utsträckning på användarstatistik. Ju fler som konsumerar medieinnehåll genom en viss plattform eller med hjälp av en viss teknologi, desto mer satsar bolagen på att utveckla den plattformen eller teknologin, eller liknande teknologier med ännu bättre funktionalitet.

Att mediebranschen därför försöker optimera nyttan av sociala medier är alltså inte konstigt. Användningen av sociala medier är väl utbredd i Sverige och under de senaste sex åren har användningen mer än fördubblats hos alla internetanvändare över 12 år. Under 2010 svarade 28 procent att de använde sociala medier dagligen och 2016 hade siffran stigit till 58 procent. Facebook är fortfarande det mest populära sociala mediet.

Nyhetskonsumtion och teknisk utveckling

Många vänder sig i dag till tidning, radio och tv för att ta del av nyheter. Men till skillnad från för tio år sedan vänder sig konsumenterna nu även till de olika nyhetskällorna på nya sätt – den som förr läste tidningen i pappersformat läser den nu ofta via dator och mobila enheter, antingen via pappersupplagan i PDF-format, via tidningens nätupplaga eller via dess sociala medieplattformar.

En tydlig trend är att fler människor väljer plattformar såsom webb-tv, nyhetswebbsidor och sociala medier för nyhetsinhämtning. Nästan hälften av alla svenskar läser nyheter genom sociala medier såsom Facebook och många ser det som ett bra komplement till nyhetswebbsidor för att få information om aktuella händelser. Beroende på vad som intresserar användaren och vilka andra personer och aktörer som användaren interagerar med, påverkas utbudet av nyheter i den enskilde användarens flöde. Detta hänger samman med att en snabbt växande andel av den svenska befolkningen använder smarta mobiler, och att dessa och andra mobila enheter blir allt viktigare i människors liv.

Nyhetsredaktionerna upplever i dag att deras möjligheter att påverka i vilken utsträckning de når ut till användarna har minskat. Men enligt Facebooks egna undersökningar värderar många användare ändå traditionella nyhetsaktörer högt i sina flöden.

Utbyggnad av bredbandsnätet

Medialt innehåll som ska förmedlas måste i dag generellt passera genom betydligt fler infrastrukturer än tidigare och infrastrukturerna är ofta kopplade mot internet. I och med det alltmer digitaliserade samhället och den snabba utvecklingen av nya digitala plattformar har det skett en stor satsning för att utöka tillgängligheten till bredband, framför allt på landsbygden.

I regeringens bredbandsstrategi från 2009 sattes som mål att 90 procent av alla hushåll och fasta verksamhetsställen ska ha tillgång till 100 Mbit/s senast 2020. Enligt Post- och telestyrelsen (PTS), som ansvarar för uppföljning och analys av bredbandsmålen, är förutsättningarna för att nå målet goda. I oktober 2015 hade 61 procent av Sveriges hushåll och bolag tillgång till bredband på minst 100 Mbit/s. Regeringen ökade även satsningen på bredbandsutbyggnad på landsbygden med 3,25 miljarder kronor mellan 2014 och 2020 och föreslår ytterligare utökningar i budgetpropositionen för 2017.<sup>4</sup>

De närmaste åren väntar lanseringen av 5G där Telia och Ericsson planerar ett pilotprojekt under 2018 med tester i Stockholm och Tallinn. 5G är nästa generations standard för mobil datatrafik och är fortfarande under utveckling.

Mindre traditionellt tv-tittande och mer digitala alternativ

Under 2014 svarade svenskägda kanaler för över 80 procent av den totala tittartiden (främst SVT). Det senaste decenniet har marknaden för tv-kanaler dominerats av public service, Bonnier, MTG och SBS Discovery. De yngre delarna av befolkningen vänder sig dock alltmer till de flexibla lösningar som digitala tv-tjänster erbjuder. Så kallade play-tjänster utgör ett av dessa alternativ och drivs vanligtvis av de traditionella tv-kanalerna. Tjänsterna tillgängliggör delar av kanalernas ordinarie utbud för kunden ”on demand”, vilket innebär att konsumenten inte är bunden av fasta sändningstider för respektive program.

Digitaliseringen av mediedistributionskanaler och kriskommunikation

I takt med att allt fler mediekanaler utvecklats till, eller vuxit fram som, helt digitala lösningar har en särskild problematik uppkommit. Med digital utsändning och mottagning krävs en viss nivå av signalkvalitet (ofta kopplat till signalstyrka) för att sändningen alls ska kunna generera exempelvis bild eller ljud. En mottagare av en analog signal kan få fram viss information även när signal-

4. Budgetpropositionen för 2017 föreslår en tillförsel av ytterligare 4,1 miljarder till bredbandsutbyggnaden under 2017–2020.

kvaliteten är låg. Ett illustrerande exempel på det är radiomottagare – för en analog radio som mottar en dålig signal uppstår brus men ljud kommer fortfarande fram. I motsvarande fall för ett digitalt system blir det tyst när signalkvalitet inte möts. Sårbarheten i digitala system ligger i att en viss signalkvalitet alltid måste nås för att information ska kunna avkodas på ett korrekt sätt så att information kan förmedlas. För kriskommunikationsförmågan är denna utveckling potentiellt sett problematisk eftersom personer som enbart förlitar sig på digitala mottagare blir mer sårbara.

### 2.1.2 Generell mediekonsumtion

Ny teknik och nya former av distribution för medieinnehåll ställer dagligen den enskilde individen inför en stor mängd val. Människor använder mobilen över 200 gånger per dag och få minns vilka typer av distributionskanaler som tv, radio eller dagstidningar de väljer.

Internetanvändning ökar och användandet av traditionella medier minskar. Den genomsnittliga medieanvändaren ägnar 6,33 timmar per dag åt olika medier. Den största användartiden hos befolkningen i åldrarna 9–79 år ägnas åt internet med 122 minuter per dag. Internetanvändningen ökar för varje år men inte i samma omfattning sedan 2013.

Medan internetanvändningen ökar minskar användningen av traditionell tv, radio och dagstidningar. Konsumtionen av linjär tv har minskat med cirka nio minuter sedan 2011.<sup>5</sup> Den minskade tv-konsumtionen kan delvis vara en följd av den kraftiga expansionen av tv-liknande tjänster online, såsom play-tjänster. Även konsumtionen av radio har minskat de senaste åren och enligt rapporten *Medieutveckling 2015* minskar användartiden för radio år för år. Men radio kan trots detta anses vara en populär distributionskanal.

Även användandet av dagstidningar har minskat. 2015 var användartiden för tryckt dagstidning en genomsnittlig dag 20 minuter vilket är en minskning med 9 minuter sedan 2007. Av de personer som läser dagstidningar läser fortfarande majoriteten dagstidningen i tryckt form, men flera dagstidningar finns nu tillgängliga via internet eller applikationer<sup>6</sup> vilket har resulterat i att många konsumenter i stället väljer dessa distributionskanaler.

5. 2011 var tittartiden en genomsnittlig dag 162 minuter och 2014 var tittartiden en genomsnittlig dag 152,7 minuter för befolkningen i åldrarna 3-99 år.

6. 67 procent läser dagstidningar totalt, 54 procent på papper och 24 procent via internet eller applikation.

Skillnader i ålder och mellan kön

Det går även att hitta skillnader mellan könen i mediekonsumtion. Skillnaderna märks främst vid internetanvändning och ökar mellan könen med stigande ålder. Även vid mobilanvändning märks skillnader. Flickor använder mobiler i större utsträckning än vad pojkar gör från 10 års ålder. Flickor använder även sociala medier längre tid än vad pojkar gör och skillnaden ökar snabbt ju äldre de blir. De största användarna av sociala medier är unga kvinnor mellan 16 och 25 år. Det går dock inte att identifiera någon skillnad mellan mäns och kvinnors konsumtion av de traditionella medierna som radio, tv, och läsning av tryckta dagstidningar och tidskrifter.

Medieinnehåll konsumeras i dag på olika sätt i olika åldersgrupper, och det förefaller finnas ett betydande glapp mellan de olika gruppernas mediekonsumtion. Enligt rapporten *Svenskarna och internet 2016* från Internetstiftelsen i Sverige (IIS) är internet betydligt viktigare som allmän informationskälla än traditionell radio, dagstidningar i pappersformat, tv och sociala medier för åldersgrupperna 16–25, 26–35 och 36–45 år.

Bland den äldre generationen är internetanvändandet fortfarande lågt. Enligt rapporten använder 73 procent av männen och 64 procent av kvinnorna i åldersgruppen 66–75 år internet dagligen i hemmet, bland de som är äldre är användningen 40 procent bland män och 24 procent bland kvinnor. I samma åldersgrupper rankas internet lägre, och sociala medier avsevärt lägre, än tv, dagstidningar och radio i fråga om vad som utgör de viktigaste informationskällorna. Den genomsnittliga användningstiden per vecka av smarta mobiler respektive sociala nätverk, samt kunnigheten om datorer är också enligt samma rapport låg inom de åldersgrupperna.

Samtidigt tar internet för första gången förstaplatsen som allmänt informationsmedium för svenskarna, och trenden talar för att ledningen kommer att öka över tid. I och med införandet av "betalväggar" bland flera av de större mediehusen i Sverige uppkommer en möjlig utveckling av att vissa grupper, i brist på "gratis nyhetstjänster", i större utsträckning vänder sig till alternativa nyhetstjänster.

När IIS började sina mätningar år 2000 var dagstidningar det viktigaste mediet som informationskälla, tätt följt av tv och sedan radio. Med undantag för tv som hade en positiv trend fram till 2010, har de tre medierna blivit allt mindre viktiga som informationskällor. Medan tv fortfarande ligger nära den nivå mediet hade när mätningarna började har nivån för dagstidningar och radio minskat betydligt. I 2016 års mätning internet lika viktigt som dagstidningar var när mätningarna började.

Enligt rapporten *Mediekonsumtion 2016* från Myndigheten för press, radio och tv (MFRT) minskar den linjära tv-konsumtionen i en utveckling som verkar accelerera. Precis som bland andra linjära mediekkanaler är tittandet på linjär tv vanligast i den äldre delen av befolkningen. Andelen som lyssnar något på traditionell radio under en vanlig dag har minskat med 6 procentenheter sedan 2010, något som inte fullt ut har kompenseras av webb- eller poddradio. Läsaandet av dagstidningar har också totalt gått ner sedan 2010, från en nivå på strax under 90 procent av alla medborgare i åldrarna 9–79 år, till strax under 80 procent 2015. Under den tiden har läsaandet av papperstidningar gått ned från nästan 70 procent av befolkningen till 50 procent 2015. Samtidigt läser 26 procent tidningen på nätet. Andelen som prenumererar på en tidning sjunker stadigt i en tydlig trend. Medan 64 procent hade en tidningsprenumeration år 2010 hade 53 procent det 2015.

Mediekonsumtion i samband med kris

Resultatet från en MSB-finansierad studie<sup>7</sup> vid Göteborgs universitet om kriskommunikation visar att medieanvändningen ökar vid kriser, och att den enskilde individen söker information i fler medier än den brukar använda till vardags. Särskilt stor var användningen av nyhetsmedier med möjlighet till snabba uppdateringar. Här var användningen av tidningar på webben (84 procent) störst, men också tv (67 procent) och radio (55 procent) användes av många. Strax under hälften av de som svarade uppgav att de använt något socialt medium (45 procent) eller nyheter i mobilen (41 procent), och var fjärde säger sig ha gått in på någon myndighets hemsida (25 procent). Ytterligare ett resultat var att medieanvändningen varierar beroende på kris – sociala medier ökar i betydelse när krisen pågår länge.

### 2.1.3 Ekonomiska trender

När annonsintäkterna från traditionell mediedistribution minskar tvingas branschaktörer att hitta andra lösningar för att konkurrera på marknaden. Det inkluderar exempelvis att utöka distributionskanalerna för att nå ut till fler konsumenter och på så sätt öka annonsintäkterna, samt att koncentrera ägandeskapet av olika mediebolag för att få skalfördelar. Konsekvensen blir att den mediala mångfalden minskar. Det finns även risk att vissa områden (så som

---

7. MSB har finansierat en undersökning inom projektet *Kriskommunikation 2.0* utförd av Institutionen för journalistik, medier och kommunikation (JMG) vid Göteborgs universitet (GU) om hur medieanvändningen såg ut vid fem olika kriser. JMG, med hjälp av Opinionslaboratoriet (LORE) vid GU använde för detta syfte en Medborgarpanel mellan 2012 och 2014.

glesbygd och socioekonomiskt svaga områden) samt vissa grupper (såsom minoriteter och ideologiskt definierade grupper), blir mindre uppmärksammade i nyhetsrapporteringen.

#### Marknadsutvecklingen

Bolag inom den svenska mediebranschen får framför allt sina intäkter från två olika håll. Dels från försäljning av annonsutrymme till annonsörer, dels från försäljning av medieinnehåll till konsumenter. De senaste årens förändringar i människors mediekonsumtion har dock medfört en avsevärd minskning av mediebranschens annonsintäkter. Exempelvis har antalet prenumeranter på morgontidningar minskat vilket har resulterat i att dagspressen tappade en tredjedel av sina annonsintäkter mellan 1990 och 2010, räknat i fasta priser. Annonsbortfallet har haft en stor betydelse för den minskade lönsamheten hos de tryckta medierna. Intäkter från annonsförsäljning som tidigare genererades via papperstidningar kommer numera via andra kanaler, främst internetbaserade tidningar som sedan 2012 är landets största reklambärare.

#### Minskad mediemångfald

Enligt rapporten *Landsbyggd i medieskugga* från 2014 kan ägandekoncentrationen inom flera nyhetsproducerande mediebolag ha negativa effekter på lokalmedia. En effekt av den är att antalet lokalredaktioner och den lokala närvaron har minskat. Strategin satte tydliga spår i det svenska medielandskapet mellan åren 2004 och 2014, då antalet lokalt bemannade tidningsredaktioner minskade från 258 till 164. Nya siffror från Institutet för mediestudier för 2016 visar att 35 kommuner saknar både lokalredaktion, lokal gratistidning och nyhetssida.

Den omfattande minskningen och nedläggningen av just tidningar i Sverige har kommit att kallas "tidningskrisen". Även antalet lokalreportrar har minskat till följd av att mediebevakningen har övergått till centralredaktionerna. Detta har gett upphov till en lägre medial mångfald i landet. En konsekvens av den minskade mediala mångfalden är enligt SOU 2015:94 *Medieborgarna och medierna* att landsbygden hamnar i en politisk och demokratisk skugga. Denna problematik behandlas även i avsnittet 2.2 Produktion nedan.

En annan risk med flerkanalpublicering är att mediehusen publicerar samma nyheter i flera kanaler, vilket innebär att samma innehåll enbart ompaketeras för att passa de olika kanalerna. De flesta dagliga medier tillhör samma mediekoncern och inom koncernen samordnas innehållet. Konsekvenserna är återigen, likt problematiken rörande ägandekoncentration, att den mediala mångfalden i landet minskar.

Utredning om Teracom's ägandeform

Det statligt ägda mediebolaget Teracom AB äger och driver det svenska marknätet för radio och tv. Bolaget erbjuder också utrymme och service åt andra bolag i sina master och byggnader. Marknätet har en viktig funktion för krisberedskapen och ska kunna sända under i stort sett vilka förhållanden som helst.

Marknäten är viktiga inom både mediepolitiken och för krisberedskapen. Den tekniska utvecklingen har medfört att allt fler konsumenter radio och tv via andra distributionsformer än marknäten. Därmed har förutsättningarna för Teracom förändrats och bolaget planerar en strategiförändring där telekomverksamheter utan anknytning till marknäten får större betydelse.

Under 2016 granskade Riksrevisionen Teracom's verksamhet för att se om den var effektiv nog för att uppnå målet att public service-bolagens sändningar säkert ska kunna nå hela befolkningen. Man tittade också bland annat på om bolagets monopol inom marknätet var motiverat. Riksrevisionen kom fram till att beredskapsfunktionen kan motivera ett statligt ägande av marknäten i Sverige.

## 2.2 Produktion

I detta avsnitt beskrivs primärt produktionen av nyhetsjournalistik inom mediebranschen. De följande underavsnitten om produktion i mediebranschen utgår från tre dimensioner. Först redogörs det för nyhetsmediernas möjligheter att samla in och komma åt information som behövs i nyhetsförmedlingen, och hur förutsättningarna för att göra det har förändrats sedan 2011. Därefter redogörs för arbetet med att ta fram det som bedöms vara relevant för publicering, och arbetet med att värdera informationen inför beslut om publicering till allmänheten. De två dimensionerna är i praktiken sammanlänkade då det journalistiska arbetet består i att söka publicerbart material. Uppdelningen här syftar till att belysa respektive dimension för sig. Slutligen redogörs det för hur specifikt nyhetsflödets innehåll har påverkats av det förändrade medielandskapet. Fokus ligger på det redaktionella arbetet med nyhetsjournalistik som granskar makthavare och förmedlar viktig samhällsrapportering. Denna typ av nyhetsjournalistik är nödvändig för att säkerställa att den enskilde individen får tillgång till samhällsgranskande och oberoende nyheter.

### 2.2.1 Att samla in och komma åt information

Att upprätta information i form av text, bild och ljud har aldrig varit enklare. I denna informationsmiljö har den traditionella nyhetsjournalistiken allt svårare att hävda sig som genre – inte minst vad gäller dess roll som den så kallade *tredje statsmakten*.

Andelen orter med ständig medienärvaro och bevakning, *medias geografiska täckning*, i Sverige blir allt mindre. Utbudet av nyhetsjournalistik har försämrats på flera håll och mindre orter är ofta de som förlorar täckning. Den lokala nyhetsrapporteringen minskar i omfång. I synnerhet glesbyggd och resurssvaga områden täcks allt mindre av granskande samhällsjournalistik på lokal nivå. Såväl lokal nyhetsinhämtning (journalister som regelbundet förhör sig om vad som försiggår lokalt) som lokal nyhetsförmedling (medier som lokalt förmedlar vad som försiggår i området) är på tillbakagång. Fenomenet beskrivs ibland som att de aktuella områdena hamnar mer och mer i *medieskugga*. När medieskugga uppstår i området kan de boende komma att sluta uppfatta de större nyhetsmedierna som relevanta.

Den uteblivna rapporteringen och det uteblivna innehållet om vissa områden och grupper i samhället riskerar därför att försvaga räckvidden av annars etablerade kommunikationsvägar. Det kan leda till att de boende exempelvis inte tar till sig viktig information som förmedlas genom de kanalerna under en kris, eller att de går miste om samhällsviktig journalistik. Samtidigt har utvecklingen gjort att samhällsviktiga aktörer själva i viss mån kan informera kunder och allmänhet vid samhällsstörningar. Utanför det aktuella området kan också fördomar växa fram och förstärkas när nyhetsinhämtningen och förmedlingen från området minskar eller blir ensidig.

De för dagstidningarna (ofta lokala) så viktiga annonspengarna har gått till andra aktörer som Google och Facebook, vilka oftast endast bidrar till distributionen av nyheter. Sveriges lokala dagstidningar har haft ett starkt beroende av annonsintäkterna från just tryckta upplagor, varför den generella nedgången i annonseringen i pappers-tidningar slagit hårt mot just dessa tidningar.

När annonsintäkterna försvunnit har olika försök till anpassning genomförts, ofta i form av digitala satsningar. På nätet har det dock visat sig svårt att få betalt för lokala nyheter. Detta har lett till ytterligare anpassning där dagstidningar blivit mediehus inriktade på publicering i många kanaler. År 2014 uppgav tre av fyra journalister att vinstkraven ökat i betydelse över tid. Sex av tio journalister uppgav att hänsyn till annonsmarknaden, samt publikundersökningar



också har ökat i betydelse. Antalet journalister inom dagspressen föll från 7 000 till 5 000 mellan 1992 till 2011. Denna minskning har sedan 2012 förmodligen accelererat vilket en rad olika exempel tyder på. TV4 lade ner sina 13 regionala redaktioner 2014 vilket markerade slutet för deras regionala tv-journalistik. I Skåne tappade redaktionerna cirka 40 procent av den redaktionella personalen mellan 2009 och 2014.

Samtidigt som den professionella journalistiken hotas har den så kallade medborgarjournalistiken vuxit sig starkare, det vill säga journalistik som bedrivs av så kallade *medieborgare*.<sup>8</sup> Vissa bedömare menar dock att denna typ av journalistik inte kan kompensera för bortfall i de traditionella nyhetsmedierna, däremot kan de bidra till en större mångfald och fler perspektiv.

Ett område där nyhetsrapportering kan sägas ha ökat i omfattning är vid samhällskriser där medieborgare i högre grad kunnat fungera som aktörer i kriskommunikationen, exempelvis under skogsbranden i Västmanland 2014. Sammantaget kan det konstatera att den tekniska utvecklingen och de sociala mediernas roll gett journalister tillgång till fler och nya källor för informationsinhämtning vid kriser, men också minskat deras förmåga att agera som grindvakter (engelskans *gate-keepers*). Med ett allt större antal digitala plattformar för informationsspredning utmanas journalisternas möjligheter att styra och forma nyhetsproduktion (och därmed också i många fall samhällsinformation) vid samhällskriser.

Myndigheter och enskilda individer kan nu direkt interagera med varandra, och det blir möjligt för myndigheter att i samspel med stora grupper av människor driva en agenda som inte först filteras och granskas av nyhetsredaktionerna. Det bör dock ändå sägas att det fortfarande verkar vara så att de etablerade nyhetsmedierna med sina breda publikker (inklusive de nyhetsproducerande mediebolagen själva) och stora spridning, har ett stort inflytande på nyhets- och informationsflödena, framförallt i krissituationer.

Vissa bedömare menar att den tekniska utvecklingen och tillkomsten av vissa lagar har medfört att källskyddet är hotat. Information om material och källor finns i dag i hög grad på enheter som kan tappas bort, stjälas, hackas eller tas i beslag av polisen som en del i ett bredare utredningsarbete. Ovana och okunskap vid användandet av olika elektroniska kommunikationer, exempelvis molntjänster, inom journalistkåren tillsammans med situationer där den som ska lämna tips gör så via e-post eller sociala

8. Termen *medieborgare* syftar på en medborgare som själv är aktiv genom att producera och sprida innehåll, som bland annat kan ligga nära journalistikens urval, till andra personer.

medier leder till en ökad risk för spårbarhet och ett hot mot källskyddet. Vid intervjuer med representanter för svenska nyhetsbolag framkommer det att arbetet med det digitala källskyddet är eftersatt hos flera svenska mediebolag inom nyhetsproduktion.

### 2.2.2 Att välja ut och rapportera nyheter

Utmaningen för nyhetsförmedlande aktörer är stor. Stora mängder information måste sällas och kontrolleras, samtidigt som rapporteringen måste gå snabbt och hög tillgänglighet säkerställas. Detta kan kallas att ha en grindvaktsfunktion. Grindvaktsfunktionen har traditionellt varit utspridd på flera redaktioner och fungerat som en sluss som information passerar igenom innan den sätts i cirkulation bland allmänheten som faktiska nyheter. I takt med digitaliseringen och framväxten av sociala medier har grindvaktsfunktionens betydelse för vilken information som når allmänheten minskat. Detta har överlag lett till en stor variation av nyheter och information i samhället.

Eftersom antalet journalister har krympt har påfrestningen på den gamla interna grindvaktsfunktionen hos redaktionerna blivit större. Det har lett till att arbetsinsatsen för respektive möjlig nyhet har tvingats minska. Redaktörsrollen har enligt Pressombudsmannen (PO) skurits ned eller försvunnit på många håll. Från ett individ- eller publikperspektiv kan det antas att mediernas grindvaktande har fått en minskad betydelse för konsumtion av nyheter och samhällsinformation. Det beror dels på att de etablerade nyhetsmedierna bara utgör en av många kanaler för nyhetskonsumtion, dels på att grindvaktsrollen nu har delats upp och innehålls av fler aktörer vilka bådalett till att nyhetskonsumtionen har blivit mer individuell.

Den enskilde nyhetskonsumenten berörs och påverkas i sitt nyhetsurval, förutom av etablerade nyhetsmediers grindvakter, också av en ny slags grindvakter via sina personliga nätverk såsom Facebook och Twitter. Vängrupper konsumerar samma typer av nyheter från samma typer av nyhetsbolag och/eller plattformar. På sociala medier har därför en sorts "sekundär grindvaktsfunktion" uppkommit genom att medieborgare aktivt deltar i nyhetsflödet. Den tydligaste minskningen av grindvaktsfunktionens effekt har skett hos medier inom glesbygd och storstäders förortsområden och utvecklingen har inte vägts upp av nya plattformar och initiativ på lokal medienivå. Ett anslutande fenomen är algoritmernas växande betydelse för vilka nyheter som visas, i synnerhet på sociala medier eller vid sökningar i sökmotorer. Läs mer om detta i underavsnitt 2.4.1 Förändrade förutsättningar och olika typer av påverkan nedan.

Även om nyheter från etablerade aktörer i stor utsträckning når ut till enskilda individer via sociala medier gör de det vid sidan av en ström av annan information. Ofta sprids uppgifter som inte är verifierade och ibland sprids direkta felaktigheter. Risken är att de traditionella grindvakternas minskade betydelse leder till att en lägre andel av de uppgifter som enskilda individer stöter på under en dag grundar sig på kontrollerade fakta.

Aktörer inom mediebranschen upplever själva att sociala medier utgör en utmaning, eftersom ny kunskap och andra verktyg behövs för att kunna bekräfta information därifrån. Beslut att publicera obekräftade uppgifter görs ofta utifrån en bedömd risk för faran i att vänta för länge med att offentliggöra information. Rykten som redan hunnit börja spridas på exempelvis sociala medier, oberoende av mediers rapportering, sänker publiceringströskeln för traditionella medier. I stället anser de att en snabb rapportering från dem kan motverka konsekvenserna av spridandet av felaktig information.

Två områden som identifierats i arbetet med att stävja de negativa effekterna av *digitala löpeldar*<sup>9</sup> är större självkontroll hos enskilda användare och tekniska lösningar som med hjälp av artificiell intelligens och indikatorer identifierar delad information som med hög sannolikhet är falsk eller grovt missvisande. En sådan teknisk lösning skulle antingen minska informationens synlighet eller på olika sätt markera att informationen förmodligen inte är trovärdig.

### 2.2.3 Mediers journalistiska nyhetsinnehåll

Marknadsvillkoren som de traditionella medierna lever under medför att underhållning, lättviktigt nyhetsmaterial och mer granskande journalistik konkurrerar om samma utrymme. Det är ett problem eftersom den granskande journalistiken är dyr och ofta tar lång tid att producera i jämförelse med annat medieinnehåll. Exempelvis visar en studie av det skånska medielandskapet att endast 3 procent av de undersökta dagstidningarnas producerade material kunde klassas som ”kvalitativ granskning”. Detta enligt en definition där materialet både skulle vara undersökande, redovisa fakta, ha två av varandra oberoende förstahandskällor, handla om makt/maktutövning och vara självständigt, innehålla kritiska perspektiv samt redovisa källor och metod.

För att frigöra journalisters tid, tillföra nytt material och utnyttja redaktionella resurser effektivare, har flera svenska nyhetsbolag

9. Med digitala löpeldar avses här rykten, lögner, hat och annan skadlig information som snabbt sprids i digitala miljöer såsom sociala medier.

börjat använda sig av botar för att skriva enklare texter (i en utveckling som följer den inom amerikansk medier, dock ännu i begränsad utsträckning).<sup>10</sup> Det råder delade meningar om hur önskvärd denna utveckling är, en del ser det som ett komplement och andra som ovälkommen konkurrens. Än så länge har reporterbotarna främst införts i sport- och väderrapportering, men även Tidningarnas Telegrambyrå (TT) har en bot under utveckling.

I dag presenterar en del av de traditionella mediebolagen på sina digitala plattformar verifierad nyhetsrapportering i samma flöde som annat material, material som de tagit fram under andra former eller i andra syften. Det kan därför vara svårt att urskilja vad som har tagits fram enligt metoder som grundar sig på metodik där källkritik, nyans och andra analytiska aspekter värderas högt, och vad som inte lever upp till sådana krav. Vissa bedömare menar att en liknande utveckling även har uppstått inom tv-nyheterna, där trivialisering och likriktning har ökat mellan några av de största nyhetsprogrammen. En internationell utblick pekar på att problemet är särskilt utbrett inom lokalmedier, där officiella källor och PR-byråers påståenden ofta får stå oemotsagda.

Förhållandet mellan antalet journalister och antalet kommunikatörer har uppmärksamrats vid ett flertal tillfällen under de senaste åren. Utvecklingen går emot en sjunkande skara journalister jämte en ökning i antalet informatörs- och kommunikatörstjänster inom exempelvis statliga myndigheter, landsting och kommuner. Att fler intresseorganisationer, tankesmedjor och PR-byråer riktar påverkansarbete mot medierna kan vara ett problem för den fria och diversifierade opinionsbildningen. I en undersökning gjord vid Göteborgs universitet 2014 uppgav över hälften av de tillfrågade journalisterna att verksamma inom PR fått ett ökat inflytande över journalistiken. Det ska dock nämnas att 85 procent svarade att påverkan från verksamma inom PR fortfarande hade liten påverkan på journalistiken. Enligt Demokratiutredningen (SOU 2016:5) från 2016 och tidigare Demokratiutredning från 2000 finns det starka skäl för regeringen att vidta åtgärder för att försäkra att ett påverkansarbete från myndigheter, landsting och kommuner inte pågår gentemot allmänheten kring politiska frågor. Som viktigt i detta sammanhang pekar utredningarna också ut nyhetsmediers förutsättningar att själva granska och skapa sig en uppfattning om myndigheters verksamhet.

---

10. Botar används inom sociala medier, kanske främst på Twitter. Ofta används de i påverkanssyfte genom att automatiskt dela och sprida information som deras upphovspersoner vill nå ut med. I redaktionella sammanhang kan botar, som är specialskrivna mjukvara, användas för att ta fram enkla texter för publicering.

## 2.3 Hot och trakasserier mot medier

I detta och de två följande avsnitten redogörs det för aspekter på hotbilden mot medierna. Den första aspekten består av förekomsten av hot och trakasserier riktade mot journalister och andra verkssamma inom branschen. Effekterna av hot och trakasserier blir, förutom det personliga lidandet och ändringarna i livsstil hos de utsatta, utebliven bevakning av vissa frågor, och självzensur. Innehållet i detta avsnitt överlappar en del med det som tas upp i underavsnitt 2.4.2 Hot som del av påverkanskampanjer nedan. Det bör dock betonas att problemet med hot och trakasserier kan ha andra orsaker än viljan att försöka påverka.

Fysiskt våld mot journalister är ovanligt, endast 1 procent av 619 tillfrågade journalister uppgav att de har utsatts för våld till följd av sitt arbete de senaste 12 månaderna i en undersökning från Tidningsutgivarna (TU) 2016. I en europeisk kontext har det dock förekommit incidenter där dödligt våld använts eller planerats gentemot mediebolag. En sådan incident redogörs för i underavsnitt 2.5.1. Terrorattacken mot Charlie Hebdo den 7 januari 2015 nedan. Vid en undersökning 2016 uppgav 12 av 42 redaktioner som utsatts för hot att de har haft medarbetare som tvekat inför publicering eller jobb på grund av allvarliga hot. 11 av de 42 redaktionerna hade haft medarbetare som har undvikit bevakningsområden eller arbetsuppgifter till följd av allvarliga hot.

En annan typ av hot- och förtalsproblematik finns inom de flesta av de interaktiva kanaler som mediebolagen använder för att nå ut till och kommunicera med mediekonsumenter. Det är framförallt i mediernas kommentarsfält som detta visar sig. Eftersom sociala medier gör det möjligt för personer att hota och trakassera har flera nyhetssajter valt att stänga ner sina kommentarsfält. Exempelvis valde Mittmedia 2015 att stänga ner samtliga kommentarsfält på koncernens webbsidor. Även fyra tidningar i Norrköpings Tidningars Media-koncernen (NTM) valde 2016 att stänga ner kommentarsfälten under sina nyhetsartiklar.

Med digitaliseringen har en strid ström av hat, hot, trakasserier och förtal kommit in via e-post och sociala medier till redaktioner och enskilda journalister. Anonymitet för de som skriver, synliggörandet av journalisterna själva och låga trösklar för att ta kontakt, via e-post eller sociala medier, har alla lett till den problembild som i dag finns för aktörer inom mediebranschen.

Det råder delade meningar om huruvida hoten mot mediebranschen har ökat. Antalet hot tycks öka enligt två av de senaste undersökningarna bland mediebranschens aktörer. En tredje undersökning visar däremot att hotsituationen är densamma 2016 som 2013.

Mest utsatta för hot är de med roller som chef och ledarskribent. Bland de olika bevakningsområdena får de journalister som jobbar med nyheter om kriminalitet och rättsfrågor utstå hot i störst utsträckning, hela 72 procent svarade 2013 i en enkät att de blivit hotade. År 2016 svarade 60 procent inom samma grupp att de blivit hotade de senaste 12 månaderna. En relativt stor andel av hoten bedöms av respondenterna komma från organiserad brottslighet. Överlag kommer hot mot medierna till största del från enskilda individer. I utredningar gjorda av Utgivarna och TU under 2016 framkommer det att av olika grupperingar är det högerextremister som hotar och trakasserar journalister i störst utsträckning.

När journalister blev tillfrågade i en enkät från Göteborgs universitets Journalistpanel 2016 om vilka ämnen som utlöste trakasserier var frågor med koppling till främlingsfientlighet det mest framträdande. Bland de vanligaste ämnena som utlöste trakasserier mot journalister fanns frågor om immigration/flyktingar/integration (vilket nämdes av 34 procent av de tillfrågade journalisterna), bevakningen av Sverigedemokraterna (7 procent) och rasism (4 procent). Runt 8 procent nämnde också ämnena kriminalitet samt genusfrågor och feminism som utlösare av trakasserier. Kvinnor inom medier får också i högre grad än män utstå sexistiska kommentarer och hot om sexuellt våld. Brittiska The Guardian granskade 2016 alla kommentarer som publicerats i deras kommentarsfält sedan 2006. Resultatet visade, trots att majoriteten av journalister på The Guardian är män, att kvinnor får flest kränkande kommentarer. Av de 10 journalister som fått flest kränkande kommentarer var 8 kvinnor. I en undersökning bland svenska medier från TU från 2016 svarade dock ungefär lika många män (31 procent) som kvinnor (36 procent) att de blivit utsatta för hot eller trakasserier, i eller till följd av sitt arbete, de senaste 12 månaderna. I en rapport från 2015 av Nordicom utpekades främlings- och kvinnofientliga diskurser som "en form av symboliskt våld på idéer, i detta fall idéer om ett mångkulturellt och jämlikt samhälle". Hotbilden mot journalister har lett till att regeringen nu utvecklar en handlingsplan som de förväntas presentera under 2017.

Journalistförbundet uppmanar journalister att polisanmäla hot, något som nu ofta följs. Det är dock sällan som anmälningarna har lett till fällande dom och oftast har undersökningen lagts ner trots att bevis har funnits. För att kunna fälla någon för hot på internet, måste personen kunna kopplas till verktyget som förmedlade hotet. Exempelvis måste polisen kunna bevisa att personen faktiskt skrev hotet på datorn, trots att IP-adressen kan kopplas till en fysisk person med personnummer. Även vid andra typer av brott som begås via

internet, exempelvis förföljelse (engelskans stalkning) på nätet, är det svårt att knyta en gärningsman till brottet. Brott som olaga förföljelse ses också ofta som ett lågprioritetsbrott vilket gör det svårt för polisen att erhålla tillstånd för husrannsakan i syfte att införskaffa bevis.

Ytterligare en form av påverkan mot medier är de tillfällen när personer eller grupper kräver att få sitt budskap publicerat, något som blivit allt vanligare enligt vissa bedömare.

När en redaktion drabbas av hot kan dess geografiska placering bli avgörande. På mindre redaktioner ute i landet kan effekterna av hot få extra stor påverkan. En redaktion med en liten eller mycket liten personalstyrka är i det perspektivet ytterst sårbar. Situationen kan bli än mer problematisk om tillräcklig uppbackning av övriga samhället saknas i form av exempelvis polisiär närvaro. Det minskade antalet lokalredaktioner på flera orter har förstärkt sårbarheten hos de medieaktörer som fortfarande är verksamma.

En sista problematik kring medier och trakasserier är förtal i syfte att diskreditera verksamma inom branschen. Förtal som metod för att påverka medier behandlas nedan i avsnittet 2.4 Mediebranschen och påverkanskampanjer. I svensk kontext har ett uppmärksammat fall av förtal skett mot en person inom mediebranschen under 2016. Förtalet riktades mot en tidnings ledarskribent och gick ut på att denne skulle ha "suttit inne 6 mån för pedofili för 7 år sedan" vilket spreds på en Facebooksida om Ukrainakonflikten. Enligt åtalet ska spridningen ha varit ämnad att medföra allvarlig skada för ledarskribenten. Personen som spridit det falska påståendet har dömts för grovt förtal.

Mediebranschens aktörer arbetar med hotproblematiken genom bland annat Mediernas säkerhetsgrupp. Säkerhetsgruppen består av bland annat public service-bolagen, Bonnier, Mittmedia och Schibsted – sammankallande för gruppen är TU:s vd. Säkerhetsgruppen träffar polisen en gång i halvåret för att diskutera hot mot medier och hur brott kan förhindras. Polisen har i sin tur tillsatt en beredningsgrupp som aktörer inom mediebranschen kan kontakta för rådgivning och för att anmäla hot. Polisen kan därmed samla in information om hot – hur vanliga de är och om vissa grupperingar eller enskilda individer systematiskt hotar medieaktörer. Polisen ska även kunna kontakta TU:s vd om de anser att risknivån har höjts, vilket sedan vidareförmedlas till medlemmarna i säkerhetsgruppen. Mediehusens säkerhetsansvariga ska i sin tur via TU:s vd kunna meddela om de uppfattar att hotnivån har ökat, vilket i så fall vidareförmedlas till en kontaktperson inom polisen.

## 2.4 Mediebranschen och påverkanskampanjer

I detta, det föregående och det nästkommande avsnitt redogörs för aspekter på hotbilden mot medierna. I den försvarspolitiska inriktningspropositionen för 2016–2020 beskrivs innebörden av begreppet påverkanskampanj som ett förfarande med syfte att påverka en statsledning, befolkning, eller särskilt utpekade målgrupper. Det är ett övergripande och strategiskt begrepp som inrymmer enskilda konkreta aktiviteter i form av påverkansoperationer vilka genomförs för att förmedla en för egna syften fördelaktig bild av olika skeenden.

Regeringen konstaterar att påverkanskampanjer förekommer såväl i fred som under höjd beredskap och i krig samt att flera myndigheter har ansvar och roller förknippade med denna verksamhet. Det framgår att Sverige i dagsläget är utsatt för påverkanskampanjer från främmande makter som bland annat syftar till att påverka Sveriges säkerhetspolitik. Det fastställs att berörda myndigheter och aktörer ska kunna identifiera, möta påverkanskampanjer och neutralisera propagandakampanjer.

Enligt regeringspropositionen är Sverige inte ensamt om att bli föremål för främmande makters påverkanskampanjer. Regeringen menar att de baltiska länderna är föremål för starka påtryckningar som påverkanskampanjer från Ryssland, som syftar till att skada de baltiska ländernas relation till vissa minoritetsgrupper i regionen och undergräva ländernas suveränitet. Påverkansoperationer bedrivs bland annat via medier och genom annan riktad kommunikation.

Desinformation är ett vanligt förekommande samlingsbegrepp för avsiktligt producerad "falsk, inkomplett eller vilseledande information" riktad mot en specifik aktör eller målgrupp. Desinformation syftar ofta till att så tvivel och minska förtroendet för olika institutioner, snarare än att försöka övertyga meningsmotståndare med tydligt urskiljbara budskap. Desinformation syftar till att sprida och blanda motbilder i form av lögner, halvsanningar och inkompleta fakta, göda konspirationsteorier, samt begränsa tilltron till fakta och institutioner som tillhandahåller detsamma. Eftersom nyhetsmedier både återger information om faktiska händelser och är en viktig arena för demokratisk debatt, löper de risk att utnyttjas av främmande makt i dess försök att påverka befolkningen genom desinformation och annan intellektuell påverkan.



### 2.4.1 Förändrade förutsättningar och olika typer av påverkan

Vid en samhällsstörning eller olycka finns det i dag ofta en mängd olika medier och kanaler för enskilda individer att välja mellan för att skaffa sig så mycket information och så många perspektiv på den aktuella situationen som möjligt. Det omfattande informationsflödet leder dock inte nödvändigtvis till att enskilda individer alltid tar till sig mer information än tidigare.

En tydlig trend är att enskilda individer tar del av information genom sociala medier allt oftare och det blir allt vanligare att endast ta del av enskilda artiklar och inlägg i stället för tidningar och nyhetsprogram i dess helhet. Vilka nyheter som exponeras i de individuella sociala flödena styrs i stor grad av algoritmer. Algoritmerna kan skapa så kallade filterbubblor, vilket innebär att endast sådant innehåll som användaren har visat sig ha en preferens för visas. Algoritmerna sluter sig till användarnas preferenser genom deras individuella val på den plattform där algoritmen är aktiv, exempelvis Facebook och Twitter. Filterbubblor kan medföra att individen bygger in sig i ett slutet informationsekosystem där den breda nyhetsorienteringen begränsas. Fenomenet med filterbubblor kompletteras av förekomsten av så kallade ekokammare<sup>11</sup>. Ekokammare uppstår när individer samlas i grupper som definieras av att medlemmarna utgår från samma världsbild, och där motbilder och avvikande uppfattningar antingen inte tas upp alls, eller avfärdas. Individer tenderar därmed att bli mer selektiva i sin informationsinhämtning, både medvetet och utan individens vetskap. I takt med utvecklingen har Facebook alltmer kommit att pressas att ta ett ansvar för innehållet på sin plattform. Bolaget har själv valt att definiera sig som ett ”teknikbolag”, snarare än ett mediebolag, och menar därför att det inte ansvarar för innehållet såsom till exempel en tidning skulle behöva göra.

Det råder delade meningar om huruvida algoritmer, filterbubblor och ekokammare skulle vara skyldiga till det stora genomslaget av falska nyheter. Flera forskare som har deltagit i den omfattande diskussionen om huruvida filterbubblor har påverkat utgången i det amerikanska valet har argumenterat för att filterbubblor som ett stort problem kan vara överdrivet.<sup>12</sup> Den uppfattade inverkan av ekokammare och förstärkandet av egna redan existerande uppfattningar inom filterbubblor skulle kunna vara överdrivna sett till dess effekt på opinion och samhälle. Liknande problem finns även hos flera sökmotorer och deras användande av olika algoritmer för sök-

11. Ett forum där egna åsikter förstärks likt ett eko genom att upprepas från olika aktörer med gemensam ideologisk hemvist och där de deltagande aldrig behöva ta del av ståndpunkter som utmanar den egna existerande världsbilden.

12. Det förnekas dock inte att filterbubblor är ett problem, diskussionen handlar om hur omfattande problemet är.

optimering. Ren desinformation kan enkelt florera bland de högsta sökresultaten till följd av exempelvis flitigt länkande mellan olika oseriösa nyhetssidor till följd av sökalgoritmernas konstruktion, eller genom att pengar investeras i att via Googles annonserings-system associera vissa sidor med vissa sökord eller fraser.

Mediebranschens aktörer har också uttryckt en oro för utvecklingen mot allt snabbare nyhetspubliceringar och dess påverkan på den journalistiska kvaliteten. Nyheter publiceras som utkast och fylls sedan på allt eftersom mer information blir tillgänglig. Under tiden eftersöks information från läsare i form av till exempel bilder, webb-tv och läsarkommentarer. Samtidigt är det en förtroendefråga att vara snabb med nyhetsrapportering.

För att möta det ökade flödet av falska och kraftigt vinklade nyheter har ett antal initiativ inletts på olika håll. Flera applikationer har exempelvis tagits fram för att på automatisk väg markera när en nyhet kommer från en mindre trovärdig källa (hädanefter ”granskande applikationer”). Facebook har också utarbetat en egen plan för att underlätta för användarna att rapportera vissa artiklar som fejkade nyheter, samt genom att ta stöd av oberoende organisationer för att faktagranska nyhetsartiklar som delas av många.

Flera stora nyhetsmedier arbetar också för att på olika sätt kunna påvisa att nyhetsrapportering har skett efter vissa principer, standarder och kvalitetskrav för journalistik. Arbetet sker främst i två spår. Dels genom att omstrukturera det redaktionella arbetet för att inte stämpas som mindre trovärdig av granskande applikationer, dels genom att ta fram en slags kvalitetsmärkning som mediebolagen frivilligt kan ansluta sig till (i stil med sådana som finns inom livsmedelsnäringen). Kvalitetsmärkningen är tänkt att enbart kunna användas när journalistik bedrivs enligt vissa källkritiska, metodologiska och etiska krav. Avsikten är att oberoende faktagranskande organisationer ska upprätthålla märkningen och granska användningen.

De ovan beskrivna utmaningarna inom journalistiken öppnar för större genomslag av påverkanskampanjer. Sociala medier och användarproducerat text- och bildmaterial används alltmer som journalistiska källor och det kan vara svårt att veta vem som ligger bakom informationen. Det finns också ett stort antal falska användare och konton. Till exempel uppskattas att Facebook 2015 hade ungefär 170 miljoner falska användare. Falska användare kan se mycket trovärdiga ut med bakgrund och en IP-adress med rätt geografisk placering.

Den information som förmedlas kan få stor spridning, speciellt när den utger sig för att komma från politiker eller nyhetsaktörer. Det finns svenska exempel på detta där en falsk Dagens Nyheter-webb-sida uppgav att den förre stats- och utrikesministern Carl Bildt ville bilda en organisation som skulle motarbeta EU-motståndare och driva på för ett associationsavtal mellan EU och Ukraina. I februari 2015 florerade det ett förfalskat brev där avsändaren påstods vara nuvarande försvarsminister Peter Hultqvist. I brevet framgick det att Sverige ämnade sälja artilleripjäser till Ukraina.

Det finns alltså stora möjligheter att påverka nyhetsflöden och det sker allt i större omfattning. När en aktör som bedriver påverkansoperationer/kognitiv påverkan använder sociala medier för att nå ut med sina budskap, används ofta botar (se underavsnitt 2.2.3 Mediers journalistiska nyhetsinnehåll ovan). De används för att göra retweets vid vissa nyckelord eller svara med fördefinierade budskap samt att sprida virus och annan skadlig kod. Botar används också för att sprida spam som ska vilseleda och få vissa valda tweets att verka vara populära och omdiskuterade. Men det finns också exempel där det är mänsklig arbetskraft som står för påverkanskampanjer i stor skala. I februari 2015 beskrev Dagens Nyheter ett ryskt bolag i St. Petersburg där hundratals personer jobbade dygnet runt med att producera påhittade blogginlägg och nätkommentarer bestående av desinformation. Uppdraget var att hylla Putin och den ryska linjen i världspolitiken och håna västerländska ståndpunkter och politiker.

Ett annat exempel på spridandet av desinformation är det uppmärksammade fallet då en amerikansk hedgefondanalytiker under orkanen Sandy 2012 spred falska nyheter om läget, ett antal incidenter och stormens utveckling i New York via sitt twitterkonto – rykten som retweetades i stor omfattning och till sist återrapporterades i etablerade medier. Desinformation som spreds verkade vara ämnad att skapa förvirring och rädsla och ledde till att viktiga resurser fick läggas på att utreda och dementera falsk information, samt hantera att människor började agera utifrån den falska informationen.

Det kan också finnas ekonomiska incitament bakom spridande av falska nyheter – ett exempel på det är den grupp unga make-donier som lyckades tjäna stora pengar genom nyhetssajter med falska nyheter riktade till den amerikanska befolkningen under presidentvalet 2016. Före valet postade de och andra flera nyheter med medvetet uppseendeväckande innehåll för att generera stora mängder läsare och därmed annonsintäkter. Mest lönsamt ska spridning via Facebook ha varit och innehållet som slog igenom bäst var

bland annat falska uppgifter skapade för att locka till sig supportrar av den dåvarande presidentkandidaten Donald Trump. Som dessa exempel illustrerar kan motiven och aktörerna bakom spridandet av falska nyheter i olika medieflöden se ytterst olika ut.

En påverkanskampanj mot Sverige och dess mediebransch kan ske genom kognitiva, fysiska, diplomatiska, ekonomiska och militära medel. Nedan lyfts två särskilda metoder fram: hot mot journalister och cyberattacker.

#### 2.4.2 Hot som del av påverkanskampanjer

Hot som en del i påverkansförsök från olika aktörer såsom extremistgrupper och främmande makt utgör en särskild problematik för mediebranschen och samhället i stort. Se avsnitt 2.3 Hot och trakasserier mot medier ovan för en mer ingående redogörelse om hot och trakasserier mot verksamma inom mediebranschen i allmänhet (och i synnerhet journalister). Det bör betonas att hot som påverkansmedel inte bör behandlas som vilka hot som helst. Medan hot i andra sammanhang kan utgöra självändamål så används hoten i det här sammanhanget för att uppnå något ytterligare. Hot kombineras också ofta med andra strategier för att samlat uppnå ett mål. Påverkan kan leda till stor skada på såväl enskilda individer som samhället.

Utebliven rapportering till följd av rädsla för eller på grund av hot är en ytterst reell påverkansproblematik för den svenska mediebranschen. När högkapacitetsaktörer (aktörer med koppling till grov organiserad brottslighet eller de politiska extremistmiljöerna) hotar journalister är det vanligt att syftet bedöms vara att påverka journalistens rapportering. Efter att ha rapporterat om proryska nättroll blev exempelvis en journalist på det finska tv-bolaget YLE måltavla för en omfattande kampanj av smutskastning, hot och trakasserier. Efter att ha deltagit i en uppmärksammas granskning av det nedskjutna planet Malaysia Airlines Flight nr. 17 över Ukraina den 17 juli 2014 där bevisen starkt indikerade rysk inblandning fick de granskande medborgarjournalisterna i Bellingcat-gruppen sina datorer utsatta för hackning och upprepade *spearphishing*<sup>13</sup>-försök. De fick också sin hemsida förvanskad. Målet tycks ha varit att svartmåla gruppen och avskräcka från ytterligare publiceringar om Rysslands roll i nedskjutningen av planet.

---

13. Spearphishing är en angreppsmetod som går ut på att skicka mejl som härmar utseendet hos utskick från aktörer som mottagaren litar på, i syfte att användaren ska klicka på en länk i mejlet och därigenom ladda ner skadlig kod som ger en extern angripare en väg in i systemet.

Aktörer inom politisk eller religiös extremism eller organiserad brottslighet har olika motivbilder till att hota journalister. Bland aktörer inom organiserad brottslighet finns det, enligt Säkerhetspolisens rapport Otillåten påverkan mot medier från 2009, en medvetenhet om att medier kan användas på ett strategiskt sätt. Medieexponering av dessa aktörer/kriminella kan leda till att de får lättare att rekrytera ungdomar i riskzonen. Aktörerna kan även använda medierna för att bidra till eller förstärka sitt skrämsekapital. Ju större skrämsekapital en aktör har desto mindre behöver aktören faktiskt göra i praktiken för att uppnå effekt.

Motiven inom olika extremistgrupper för att hota journalister är mer komplexa än för aktörer inom organiserad brottslighet. Dessa motiv är mer baserade på ideologiska grunder. Till exempel dömdes fyra män varav tre var bosatta i Sverige för terroristbrott mot den danska tidningen Jyllands-Posten 2010. Enligt den danska säkerhetspolisen var gärningsmännen militanta extremister. Motivet till attentatet var en kontroversiell teckning av profeten Mohammed som tidningen hade publicerat. Incidenten behandlas i underavsnittet 2.5.1 Terrorattacken mot Charlie Hebdo den 7 januari 2015 nedan.

### 2.4.3 Cyberattacker som del av påverkanskampanjer

Cyberattacker som en del av en påverkanskampanj mot och genom journalister och medier förekommer, och väntas växa som fenomen. Tre typer av attacker och den roll inom påverkanskampanjer de kan användas till redovisas här, men betydligt fler möjliga varianter finns.

Överbelastningsattacker kan användas för att hota eller tysta fri opinionsbildning. Det självklara fallet att nämna i den svenska kontexten är DDoS-attackerna<sup>14</sup> mot de svenska mediehusen i mars 2016. De behandlas i underavsnitt 2.5.3 Överbelastningsattacker mot svenska mediehus den 19 mars 2016 nedan. Ett annat uppmärksammat fall inträffade i september 2016 när journalisten och cybersäkerhetsexperten Brian Krebs webbsida utsattes för en DDoS-attack motsvarande 620 gigabits per sekund, då ett världsrekord. Rekordet slogs sedan under cyberattacken mot Dyn DNS som redogörs för i underavsnitt 2.5.4 Överbelastningsattacker mot Dyn DNS den 21 oktober 2016 nedan. Angreppet var så kraftigt att bolaget Akamai, som till dess erbjudit gratis överbelastningsskydd till Krebs webbsida, av hänsyn till sina betalande kunder såg sig tvingat att sluta ge webbsidan skydd eftersom tjänsten belastades så hårt att de övriga

14. DDoS står för Distributed Denial of Service och avser ett angrepp där många enheter samverkar för att tillsammans överbelasta en server eller en uppsättning servrar genom att samtidigt och med hög hastighet skicka stora mängder data.

kunderna riskerade att lida skada. Enligt en undersökning som Krebs sedan genomförde visade det sig att ett adekvat skydd mot sådana angrepp kostar mellan 150 000 och 200 000 dollar, summor som är helt omöjliga att betala för de flesta enskilda journalister och mindre mediebolag. Samtidigt är det möjligt att få en DDoS-attack utförd mot ett utpekad mål för en mindre summa, vilket visar att det råder en assymmetrisk kostnadsbild för försvar relativt attack. Kombinationen av att så många har råd att angripa journalister och andra som publicerar information som andra vill förhindra från att sprida, och att skyddet mot sådana angrepp är så dyrt, gör att överbelastningsattacker som påverkansmedel är effektivt. Angreppet mot Krebs var förmodligen ett svar på deras granskning av, och publiceringar om, några av personerna bakom DDoS-tjänsten vDOS bara dagar före attacken.

Intrång i it-system genom angrepp som spearphishing kan användas för att komma åt information som journalister har, för att stjäla den, radera den eller för att manipulera den. Stulen information kan användas för att svartmåla journalisten personligen eller dennes arbete. Men personliga uppgifter om journalisten kan också publiceras och användas för att hota denne. Journalistgruppen Bellingcat utsattes för en sådan kampanj av attacker efter att dragit slutsatsen att Ryssland låg bakom nedskjutningen av Malaysia Airlines Flight nr. 17 över Ukraina under 2014. En av gruppens ryska journalister fick sina online-konton och mobila enheter hackade, varpå personliga detaljer och foton publicerades online. Journalisten fick kort därefter dödshot med hänvisning till det arbete denne hade deltagit i.

Två större intrång, förmodligen med hjälp av samma angreppsteknik, drabbade 2013 tidningarna The New York Times och The Wall Street Journal efter att de hade granskat den dåvarande kinesiske premiärministern Wen Jiabao och dennes familj. The New York Times hade i sin granskning funnit att Wen och hans familj hade tjänat flera miljarder dollar på tveksamma affärer. Angreppet bedömdes vara en del av en större kampanj av intrångsförsök mot amerikanska medier för deras granskningar av kinesiska ledare och bolag. På grund av dessa granskningar fick The New York Times motta hot om att fortsatta granskningar skulle leda till "konsekvenser". Syftet med kampanjen ska ha varit att komma över känslig information som medierna hade tillgång till, men också för att försöka kontrollera Kinas image utomlands.

Ett tredje sätt att med cybermedel skada medier är att kapa deras sändningar, konton eller webbsidor för att därefter ändra deras

utseende eller informationen i eller på dem. I samband med spear-phishing-kampanjen mot Bellingcat fick gruppen också sin sida kapad och förvanskad. Ett annat framstående mediebolag som drabbats av samma sak är Forbes som den 13 februari 2014 fick sin webbsida kapad av en hackergrupp med nära kopplingar till den syriska regimen. Efter att ha fått sina system infiltrerade tidigare under dagen började det vid 10-tiden lokal tid dyka upp nyheter på sidan som inte hade skrivits av anställda på bolaget. Efter att bolaget hade vidtagit vissa åtgärder mot intrånget bytte angräparna metod och började ersätta sidans innehåll med så kallade tags (en slags graffiti för cyberdomänen) och bilder på den syriska flaggan. Attackerna fortsatte, trots Forbes motåtgärder, i nästan två dygn. Efter nästan ett dygn av attacker vände sig hackergruppen till Twitter och erbjöd sig sälja Forbes-anställdas kontouppgifter till högstbjudande. Attacken tvingade Forbes att göra omfattande nyinvesteringar i säkerhet, och att göra sig av med system som komprometterats. Målet med attackerna var att ge igen för de reportage Forbes publicerat om kriget i landet, och för att visa vad som skulle hända om Forbes eller andra tidningar försökte sig på något liknande igen.

## 2.5 Mediebranschen och några allvarliga incidenter

I detta och de två föregående avsnitten redogörs det för aspekter av hotbilden mot medierna. Utöver de hot och utmaningar som beskrivits hittills finns några tongivande incidenter av det mer extrema slaget som bidrar till att dimensionera hotbilden mot medier. Gemensamt för incidenterna är att de på ett eller ett annat sätt blottlagt en risk och potentiell sårbarhet i mediebranschen och/eller i samhället i stort.

### 2.5.1 Terrorattacken mot Charlie Hebdo den 7 januari 2015

Den 7 januari 2015 angreps den franska satirtidningen Charlie Hebdo av beväpnade män. Attacken resulterade i att elva personer miste livet. Motivet ska ha varit att hämnas för publiceringen av teckningar som föreställde profeten Mohammed. Bland de döda fanns nio av tidningens anställda, däribland fyra kända satirtecknare. Attacken fick stor medial uppmärksamhet och aktualiserade återigen terrorhotet och risken för dödligt våld mot mediebranschen.

Klockan 11.20 på onsdagen klev två beväpnade män in på satirtidningen Charlie Hebdos redaktion i Paris. De öppnade eld mot de som befann sig i lokalerna och ska under attacken ha ropat ”Vi har

hämns profeten”. Vid attacken ska ett redaktionsmöte pågått inne på tidningen. Elva personer skjuts till döds i attacken, två av dem var poliser och resten var anställda på tidningen – fyra av dem kända satirtecknare. Attacken pågick i fem minuter, varpå de två gärningsmännen flydde i en bil. Omedelbart efter attentatet höjdes säkerhetsläget i hela Parisregionen (Île de France). På fredagseftermiddagen två dagar senare dödades gärningsmännen vid en polisiär och militär insats mot deras förskansning inuti ett tryckeri i Dammartin-en-Goële, några kilometer nordost om Paris. En man som tagits som gisslan kunde också fritas vid insatsen. Gärningsmännen visade sig vara två bröder härrörande från Paris och motivbilden ska ha varit att utkräva hämnd för publiceringen av bilder som föreställde den islamske profeten Mohammed. En av bröderna ska ha varit välkänd hos fransk säkerhetspolis. Båda bröderna fanns med på en ”no fly”-lista över misstänkta terrorister, enligt uppgifter från USA. Bägge var identifierade som säkerhetshot. Efter attacken tog terrororganisationen al-Qaidas gren i Yemen på sig terrordådet.

Attacken mot tidningsredaktionen uppmärksammades globalt och väckte starka känslor mot terrorismen och dess hot mot det öppna demokratiska samhällets grundvärden, som yttrande- och tryckfrihet. För svensk del fanns resonans med den planerade terrorattacken mot danska Jyllands-Posten 2010 vilken avväjdes samma dag som den skulle genomföras. Den avstyrda attacken mot Jyllands-Posten föranledde en ökad säkerhet hos flera svenska mediebolag och ledde till krav på förstärkt skydd från myndigheternas sida. I ett öppet brev menade Utgivarna 2013 att Säkerhetspolisen inte gör tillräckligt för att skydda medierna från hot. I brevet lyfte Utgivarna den bredare hotbilden mot svenska medier och uppmanade Säkerhetspolisen att leva upp till författningsskyddet som anger att den ska motverka brott som syftar till att påverka bland annat journalisternas yrkesutövning. Den 8 januari 2014 träffades Säkerhetspolisen och den dåvarande Rikskriminalpolisen Utgivarnas vd och andra representanter inom intresseorganisationen för att samtala kring hotbilden mot medier och utveckla samarbetet kring frågan.

I Sverige återuppväckte dådet mot Charlie Hebdo en diskussion om det skydd som den svenska staten genom de rättsvårdande myndigheterna (i synnerhet Säkerhetspolisen) är förbundna att ge mediebolagen, samt det säkerhetsarbete som medierna själva bedriver.

Efter attacken mot Charlie Hebdo höll Säkerhetspolisen och dåvarande Rikskriminalpolisen även ett möte med flera mediebolag om säkerheten på redaktionerna. För mediebranschen i Sverige utgör terrorhot ett problem som säkerhetsarbetet nu ständigt



(men med varierande intensitet) har att förhålla sig till. För enskilda mediebolag medför terrorhotet exempelvis ökade investeringar i skyskydd och personalsäkerhet. För samhället kan det i stället handla om ett ökat behov av resurser i form av bland annat polisiär närvaro och underrättelseverksamhet från rättsvårdande myndigheter.

Terrorincidenterna illustrerar hur hotbilden mot personer verk samma inom mediebranschen i extremfallet dimensioneras av gränsöverskridande hot. Medierna utgör därmed, i vissa fall, mål som vissa grupper är beredda att korsa nationsgränser, och genomföra omfattande planering, för att angripa.

### 2.5.2 Teracoms masthaveri i Häglared den 15 maj 2016

En annan typ av hot är det som riktas mot informationsinfrastrukturen. En sådan incident var Teracoms masthaveri i Häglared 2016. Klockan 22.45 söndagen den 15 maj 2016 bröts cirka 200 meter av på den 322 meter höga Dalsjöforsmasten vid Häglared utanför Borås och föll till marken. Polisen misstänkte tidigt sabotage eftersom muttrar till stålvajrar lossnat från flera betongfundament. De gick under måndagen den 16 maj ut med informationen att misstanken hade bekräftats.

Mastens betydelse för medieutsändningar

Incidenten innebar att sändningarna på radiokanalerna P1, P2, P3, P4 Sjuhärad och Rix FM omedelbart avbröts i närområdet. Teracom beräknade att cirka 190 000 boende i närområdet drabbades av avbrottet. Sveriges radio P4 Sjuhärad fick avbrott i sina utsändningar på grund av incidenten och fick gå via relä under det första dygnet. Hade detta inte varit möjligt hade den lokala informationen inte gått att få ut i tid. En Rakelsändare drabbades också, men detta system påverkades inte tack vare redundans<sup>15</sup> i nätet i form av andra master.

Trots att masten gått av kunde VMA sändas ut. Teracom uppgav att det under den akuta fasen gick att nå 88 procent av de drabbade med VMA-meddelanden, men då på andra frekvenser än de vanliga. VMA kunde sändas via P4 Riks som efter haveriet hade nära 90 procent täckning i området runt masten. P4 Riks sändningar kunde också utökas så att de kunde nå alla i området inom ett dygn. Detta trots att masten var avbruten.

---

15. Begreppet redundans används i den här rapporten på ett sätt som motsvarar hur begreppet används inom ingenjörsvetenskapen. Redundans kan därmed stå för dubbla uppsättningar av kritiska komponenter eller funktioner i ett system för att göra systemet mer motståndskraftigt mot påfrestningar.

Med de mobila master som sattes upp direkt efter incidenten<sup>16</sup>, samt med hjälp från några närliggande, överlappande master, nådde tv-signalerna för SVT, TV4 och TV6 fullgod täckning. Teracom uppgav att det genom dessa insatser tog mindre än två dygn efter haveriet att få upp samtliga tjänster, inklusive radio och cirka en vecka att få samtliga tjänster att fungera fullt ut genom provisoriska lösningar. Det tog dock tid att få en permanent lösning till stånd. Under hösten 2016 uppgav Teracom att de återetablerat 95 procent av områdets ursprungliga radio- och tv-tjänster.

Vidtagna åtgärder och efterspel

Teracom uppger att incidenten vid Häglaredsmasten var första gången som bolaget upplevt omfattande sabotage mot ett av sina skyddsobjekt. Cirka tio dagar efter incidenten så hade Teracom en 90-metersmast i drift med ungefär samma täckning som den ursprungliga masten. Även ett antal andra aktörer vidtog åtgärder, bland annat hade MSB dagliga samverkanskonferenser med berörda aktörer och tog fram lägesbilder.

Två dagar efter sabotaget mot masten inträffade ytterligare händelser och det uppstod spekulationer i bland annat nyhetsmedier om att det skulle finnas ett samband mellan dessa händelser och mastbrottet. Ett nätfel hos Luftfartsverkets flygledning ledde till stopp för ordinarie kommunikations- och radarsystem. En systemuppdatering orsakade problem i SOS Alarms kommunikation med räddningstjänst och ambulanser och SJ:s biljettbokning låg nere under ett antal timmar, vilket påverkade biljettbokningen. Efter dialog med berörda aktörer gick MSB ut till allmänheten och dementerade ett samband mellan mastbrottet, flygstoppet, och de övriga incidenterna.

Direkt efter sabotaget av Häglaredsmasten uppstod spekulationer kring möjliga gärningsmän. I dessa spekulationer figurerade framför allt tre ungdomar som bara någon vecka tidigare lagt ut en video på internet där de ses klättra i Häglaredsmasten. Ungdomarna valde att själva gå till polisen och är inte längre misstänkta för sabotaget. De dömdes dock för olaga intrång.

Vad gäller Teracom's övriga installationer uppger bolaget att de omedelbart satte ut väktare vid alla de 54 storstationer de driver. Teracom säger också att de vidtagit ett flertal åtgärder för att undvika liknande händelser, bland annat har de satt in mer övervakning. Teracom uppger att en ny högmast i Häglared kommer att finnas på plats sommaren 2017.

---

16. Direkt efter incidenten ersattes masten tillfälligt av två mobila radiosändare, mastbilar, dock med mindre kapacitet, cirka 57 procent av själva masten.

Ett fåtal av de aktörer som intervjuades för denna rapport drabbades av incidenten med lägre sändningsförmåga, dock främst lokalt. Ett tv-bolag uppger att deras sändningar låg nere i tre dagar till följd av incidenten och att de inte hade full sändningsförmåga förrän tio dagar senare. Enbart en aktör som inte drabbades valde att göra en översyn av sitt skydd. Denna aktör såg då främst över det fysiska skyddet i form av väktarrutiner, rutiner för intrång samt beslutsrutiner. De såg däremot inte över säkerheten för sändning eftersom de inte drabbats.

Incidenten visar hur sårbara delar av den svenska informationsinfrastrukturen är, att det går att orsaka stor skada med förhållandevis primitiva metoder och att sådan skada i sin tur kan leda till oro och ryktesspridning bland allmänheten.

### 2.5.3 Överbelastningsattackerna mot svenska mediehus den 19 mars 2016

Under några timmar på lördagskvällen den 19 mars 2016 genomfördes två distribuerade överbelastningsattacker (DDoS-attacker) mot Aftonbladet och Expressens nätutrustningar som gjorde att inkommande trafik blockerades. Innan tekniska åtgärder hann sättas in, drabbades även flera andra tidningar, däribland Dagens Nyheter och Svenska Dagbladet. Utöver mediehus drabbades även en del andra typer av bolag, bland annat banken SBAB, färjebolaget Destination Gotland och Hitta.se. TV4:s internetjänst TV4Play på TV4.se drabbades också.

Några dagar senare, den 24 mars, inträffade en ny våg av liknande DDoS-attacker. Flera nyhetssajter, däribland Dagens Nyheter, Aftonbladet, Dagens Industri, Sydsvenskan, Helsingborgs dagblad samt Svenska Dagbladet låg då nere eller var svåra att komma in på. Dessa attacker var dock inte lika omfattande i trafikvolym som de som inträffade den 19 mars.

#### Konsekvenser och effekter

Attacken innebar att tidningarnas webbsidor inte gick att nå. Den första vågen av angrepp var mycket omfattande i trafikvolym. De flesta mediehus fick sina sajter att fungera under söndagen, men flera av dem drogs fortsatt med stora problem som bland annat innebar svårigheter att publicera artiklar på nätet. Den andra attackvågen, som kom den 24 mars, var även den inriktad på ett fåtal webbplatser, men även mot en operatörs egna adresser.

Huvudattacken var inriktad på ett fåtal mediehus. Att flera tidningar drabbades var sannolikt en effekt av att dessa fanns hos samma driftleverantör alternativt använde samma infrastruktur.

Vidtagna åtgärder och efterspel

Attackerna polisanmäldes och polisen inledde en förundersökning om grovt dataintrång. Attackerna diskuterades i regeringens kris-  
hanteringsråd och på det säkerhetspolitiska rådets ordinarie möte i  
mars 2016.

Överbelastningsattackerna mot mediehusen fick stor medial upp-  
märksamhet. Kombinationen av att medier hade attackerats, att  
experter bedömde DDoS-attackerna som samordnade, samt att  
datatrafiken från ryska internetoperatörer ökade kraftigt på kvällen  
den 19 mars<sup>17</sup> gjorde att incidenten ledde till stor ryktesspridning.  
Spekulationer förekom om att attackerna planerats och utförts i  
Ryssland, något som polisen snabbt tonade ner. Information före-  
kom också om ett Twitter-konto där ett anonymt hot mot Sveriges  
regering och svenska medier lagts ut strax före attackerna den  
19 mars. Som orsak angavs att Sverige spridit falsk propaganda.  
Attackerna föranledde en diskussion om mediernas roll i att säkra  
demokratin och de möjliga konsekvenserna av omfattande attacker  
mot medier. Statsminister Stefan Löfvén uttalade sig i Dagens  
Nyheter om vikten av fungerande medier: ”Det är en viktig del av  
säkerheten och en viktig del av demokratin att nyhetsförmedling  
fungerar i tider av oro.”

De intervjuade aktörernas åtgärder

Flertalet av de aktörer som intervjuats för denna rapport såg efter  
överbelastningsattackerna över sitt skydd och den förmåga de bedömt  
sig ha för att klara överbelastningsattacker. Detta gjorde de oavsett  
om de hade varit drabbade eller inte. Exempel på åtgärder som vidtogs  
var bland annat att skaffa ytterligare internetleverantörer respektive  
redundanta kabelanslutningar. En aktör nämnde särskilt att de ökat  
sitt samarbete med leverantörerna, vilket aktören såg som en viktig  
faktor för att klara av incidenter av denna typ.

PTS genomförde i slutet av maj samma år ett seminarium om  
överbelastningsattacker. På seminariet deltog både mediebolag och  
teleoperatörer. Syftet var att sprida erfarenheter från de aktuella  
attackerna, hur man kan möta dessa hot, och att diskutera hur  
teknikutveckling och affärsmodeller kan bidra till lösningar, samt  
att öka förståelsen mellan mediebolag och telekombranschen.

Incidenten visar hur överbelastningsattacker kan användas mot  
svenska medier för att störa deras verksamhet i form av förmedling  
av information, granskning och opinionsbildning. Den visar också  
att det med fjärrmedel är förhållandevis enkelt att slå mot tjänster

---

17. Det behöver inte betyda att attacken har sitt ursprung i Ryssland, den eller de som ligger bakom på olika sätt  
kan ha dirigerat attacken genom landet, eller utnyttjat virusinfekterade ryska datorer.

som används av flera medier, och därmed orsaka skada på flera medietjänster samtidigt.

#### 2.5.4 Överbelastningsattackerna mot Dyn DNS den 21 oktober 2016

Fredagen den 21 oktober 2016 drabbades tre av DNS-operatören Dyns datacenter i nordöstra USA av två omfattande, och flera mindre, DDoS-attacker.<sup>18</sup> Attackerna begränsade stundtals tillgången till tjänsten helt och hållet, men Dyn lyckades begränsa skadeeffekterna av de senare attackerna så att merparten av bolagets tjänster gick att nå med vissa dröjsmål. Då DNS-operatörer tillhandahåller katalogtjänster med adressuppgifter till webbsidor och nättjänster innebar angreppet att alla de webbsidor som inte samtidigt var listade i någon annan katalogtjänst inte längre gick att nå. Attacken misstänks ha genomförts med stöd av ett eller flera så kallade botnets, vilket innebär att internetanslutna enheter (digitala videospelare, skrivare, kameror, mobiler, routers etc.) hade kapats med den skadliga koden Mirai. Med en uppskattad överföringshastighet på 1,2 terabit per sekund uppskattades attacken ha varit den största av sitt slag någonsin, mer än dubbelt så stor som den ditintills största observerade attacken.

Den första attacken mot Dyn påbörjades cirka klockan 10.10 svensk tid. Den inleddes med ett mindre angrepp på bolagets DNS-plattform för Östasien, Sydamerika och Östeuropa. När Dyn utförde sina skydds- och incidenthanteringsrutiner skiftade angriparen snabbt mål mot DNS-plattformen för östra USA. Dyn svarade då med att tillsätta ytterligare skyddsåtgärder och hade klockan 12.20 fullt ut implementerat dem. Angreppet avslutades kort därefter. Den första attacken ledde till att Dyns katalogtjänst var helt otillgänglig under merparten av tiden det pågick. En ny attack inleddes cirka klockan 14.50. Den likande till karaktären den första attacken, men den här gången kom anropen från enheter som var mer jämnt fördelade globalt.

Vid tidpunkten för den andra attacken hade dock Dyn full incidentberedskap och kunde därför begränsa skadeeffekterna. Attacken ledde därför endast till att tjänsten var sporadiskt otillgänglig. Däremot gick det inte att förhindra att tjänsternas svarstider även fortsättningsvis var långa då ”köbildningen” till tjänsten blev allt längre under angreppets förlopp.<sup>19</sup> En mindre, men ändå betydelsefull, attack initierades därefter klockan 20.00 och pågick till cirka 22.10, med i stort sett samma resultat som den andra attacken.

18. DNS står för Domain Name System, en slags katalogtjänst för att kunna navigera på internet. Systemet över-sätter domännamn i e-postadresser och webbadresser, som användare skriver i t.ex. webbläsarens adressfält, till en numerisk adress som möjliggör för webbläsaren att hitta den eftersökta sidan.

19. Problemet förvärrades genom att automatiska funktioner i den programvara vanliga användare använder gör förnyade anrop när den sökta tjänsten inte svarar inom ett bestämt tidsintervall.

Några av bolagen och aktörerna vars sidor och tjänster drabbades var The Guardian, The New York Times, Amazon, CNN, The Wall Street Journal, Spotify, Netflix och PayPal. Något som gjorde attacken särskilt allvarlig i Sverige var att de samhällsviktiga informationstjänsterna Krisinformation.se och Regeringen.se båda blev otillgängliga. Även MSB.se och Informationssäkerhet.se drabbades.

Ingen tog direkt på sig ansvaret för att ha genomfört attackerna, men några dagar senare påstod sig hackerkollektiven SpainSquad, Anonymous och New World Hackers ha stått bakom attacken. Motivet ska ha varit att de önskade ge igen för vad de ansåg var en orimlig behandling av WikiLeaks-grundaren Julian Assange som då uppehöll sig på Ecuadors ambassad i London och där hade fått sin internetåtkomst indragen inför det amerikanska valet. Andra aktörer pekades också ut. Bolag och myndigheter som utrett incidenten har dock varit skeptiska till flera av de hackerkollektiv och enskilda alias som föreslagits stå bakom attackerna. En analys pekar dock på att hackers som velat demonstrera sin egen kapacitet och orsaka störningar kan ha legat bakom attackerna. Enligt den analysen fanns det förmodligen inte några ekonomiska eller politiska motiv till attackerna.

Dessa attacker är ett exempel på hur så kallade Internet of Things-an slutna enheter (IoT-enheter) kapas i mycket stor skala för att sedan användas som botnets för att angripa mål och bedriva brottslig verksamhet. Attackerna bedömdes av Dyn som ovanligt sofistikerade, och ska ha skapats av att hundratusentals enheter anropade Dyns tjänst samtidigt. En expert har uppskattat att cirka 10 procent av de enheter som globalt infekterades av Mirai användes för att angripa Dyns servrar.

I efterspelet av attackerna gick det kinesiska bolaget Hangzhou Xiongmai Technology ut och bekräftade att bolagets produkter, såsom digitala videospelare och kameror, hade kapats i stor skala för att bygga upp den infrastruktur som sedan hade använts för att genomföra attackerna.<sup>20</sup>

Bolagets förslag till lösning visar hur svårt det är att hantera problemet. Först måste ägare av sådana enheter upplysas om att de har enheter som kan ha kapats. Sedan måste de antingen installera ny så kallad firmware, vilket är tekniskt avancerat och tidskrävande samtidigt som det inte ger några fördelar för användaren. Alternativt kan användarna koppla loss enheten från sin internetanslutning,

---

20. Företaget föreslog att de som köpt deras produkter före september 2015 kunde installera en ny firmware (programvara som styr och kontrollerar elektronisk utrustning) på sina enheter, eller koppla bort enheterna från internet, för att undvika att enheterna som köpts skulle kunna användas för liknande attacker i framtiden.

med minskad funktionalitet som möjlig följd. Eftersom få känner till problemen och incitamenten att åtgärda dem är låga, lär problemen kvarstå så länge oskyddade enheter säljs och används.

Många bedömare anser att antalet DDoS-attacker, mängden data som skickas för att överbelasta målet och förfiningen i hur attackerna genomförs alla har ökat, samt att den trenden kommer att fortsätta 2015 och 2016 har använts för att testa nyckelpunkter i internetinfrastrukturen för att klargöra hur sårbara de är.

Överbelastningsattackerna mot Dyn visar hur mediernas verksamhet kan störas ut genom brottslig verksamhet som inte riktar sig specifikt mot dem. Incidenten förstärker också slutsatsen från underavsnitt 2.5.3 Överbelastningsattackerna mot svenska mediehus den 19 mars 2016 ovan om att attacker på tjänster som används av flera medier utgör ett naturligt mål för de som önskar skada medierna.

**Samhällsviktig  
verksamhet inom  
mediebranschen**



## 3. Samhällsviktig verksamhet inom mediebranschen

### 3.1 Inledning

För att säkerställa att de resurser samhället investerar i, att samhällsskyddet är ändamålsenliga och att satsningar görs på rätt saker, behöver det vara klarlagt vad som är samhällsviktigt. Detta kapitel underbygger i synnerhet bedömningarna av de samhällsrisker som presenteras i avsnitt 4.5 Samhällsrisker och sårbarheter nedan.

MSB har i föreskrift definierat vad som avses med samhällsviktig verksamhet för offentliga aktörer (se nedan). Arbetet med att identifiera samhällsviktig verksamhet inom mediebranschen, som redovisas nedan, har resulterat i att tre teman för sådan verksamhet har identifierats. Ett tema, som berör mediebranschens samhällsgranskande roll, visar sig omfattas av den definition av samhällsviktig verksamhet som MSB tillämpar i föreskrifterna om statliga myndigheters risk- och sårbarhetsanalyser.

I MSB:s föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2016:7) definieras samhällsviktig verksamhet som en verksamhet som uppfyller minst ett av följande villkor:

1. Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället.
2. Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.
3. Det första villkoret relaterar alltså till samhällets funktionalitet på olika sätt. Genom att vissa flöden, processer, tjänster eller annat upprätthålls kan samhället fungera som vanligt.

### 3.2 Enkätundersökning riktad till mediebranschen

För att skapa en övergripande bild av den samhällsviktiga verksamheten inom mediebranschen har MSB brutit ned definitionen av samhällsviktig verksamhet i tre frågor, och inkluderat dem i enkätundersökningen. Frågorna var:

1. Enligt er bedömning, skulle det kunna uppstå en allvarlig kris i samhället om din organisation drabbades av ett avbrott i kärnverksamheten som varade i upp till...
2. Enligt er bedömning, skulle det kunna uppstå en allvarlig kris i samhället om 10 procent av alla organisationer i Sverige med en kärnverksamhet som liknar er drabbades av ett avbrott som varade i upp till...
3. Enligt er bedömning, är er organisations verksamhet nödvändig eller mycket väsentlig för att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt?

Båda de två första frågorna bröts ned i tre tidsintervall, 24 timmar, 48 timmar respektive en vecka och hade fem svarsalternativ avseende nivå (lokal, regional, nationell nivå samt alternativet Nej respektive Kan inte bedöma). Den sista frågan bröts inte ned i tidsintervall, men hade samma svarsalternativ.

### 3.3 Övergripande om samhällsviktig verksamhet i mediebranschen

MSB har i arbetet med den här rapporten identifierat tre huvudsakliga teman som ligger till grund för hur aktörer inom mediebranschen resonerar kring om de bedriver samhällsviktig verksamhet.

Det första temat (hädanefter: *krishanteringstemat*) avser mediebolagens bidrag till samhällets krishanteringsförmåga i rollen som förmedlare av viktig samhällsinformation, kommunikation mellan olika delar av allmänheten och myndigheter och andra viktiga aspekter i samband med en kris.

Det andra temat (hädanefter: *granskningstemat*) avser mediebolagens roll som den tredje statsmakten. Med det avses mediebolagens roll som granskare av samhällets maktavare och den upplysning om samhällets missförhållanden som de förmedlar till allmänheten. Denna typ av journalistik har ibland kallats samhällsviktig journalistik.

Det tredje temat (hädanefter: *trygghetstemat*) avser den stora roll som medier spelar för den enskilde individen i vardagen. Mediekonsumtion utgör en betydande del av det som stora delar av befolkningen förknippar med en trygg och normal tillvaro. Försvinner möjligheten att ta del av medieinnehåll, såsom nyheter, fakta eller underhållning, kan oro uppstå, vilket i sin tur kan anstränga samhällets resurser. Medieföreträdare anser att risken för att oro skapas bland allmänheten är särskilt stor om ett sådant avbrott skulle verka orsakat av bero på en extern antagonists handlingar. Temat faller delvis utanför den ovan angivna definitionen av samhällsviktig verksamhet eftersom det inte avser att något särskilt tv- eller radioprogram eller någon särskild webbsida, utan snarare handlar om helheten i medieutbudet, och att det överhuvudtaget finns ett medieutbud.

Det bör noteras att de tre temana ibland samverkar. Ett exempel på det är användningen av väl etablerade och förtroendeingivande programledare som leder nyhetsrapporteringen i samband med samhällskriser, vilket utöver själva krisrapporteringen också skapar en upplevelse av kontinuitet och trygghet.

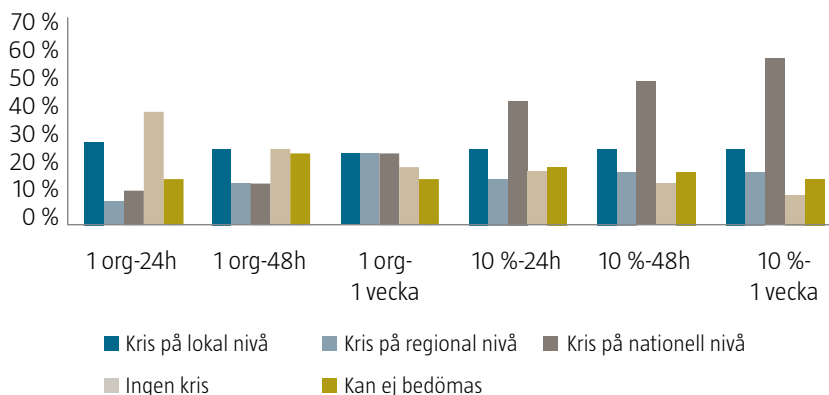
Enkätundersökningen utgick från definitionen av samhällsviktig verksamhet som finns i MSB:s föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser, och de två aspekter på samhällsviktighet som den definitionen handlar om. De sammanfaller ganska väl med de två första temana ovan. Det tredje temat, om mediebolagens roll som tredje statsmakt, täcks inte av definitionen men utgör ändå en för samhället avgörande verksamhet.<sup>21</sup> Enkätresultat om det temat saknas därför.

De två första frågorna i metodavsnittet ovan relaterar alltså till föreskriftens första villkor för vad som kan räknas som samhällsviktig verksamhet. Diagrammet nedan sammanfattar svaren för de två första frågorna. Det visar därmed de svarande branschaktörernas bedömningar av hur fort, och på vilken nivå, som en kris i samhället kan uppstå vid avbrott hos först enskilda aktörer, och sedan hos 10 procent av alla aktörer som har samma sorts kärnverksamhet som respondenten.

---

21. Avslöjanden av skandaler och missförhållanden inom exempelvis statlig verksamhet eller näringslivet, eller granskning av samhällets missförhållanden är avgörande för att enskilda individer ska kunna göra informerade val av sina makthavare, och utkräva ansvar. Definitionen av samhällsviktig verksamhet ovan är inriktad mot att identifiera ur vilka källor en kris kan uppstå, och vilka verksamheter som kan bidra till att minimera risken. Rollen som tredje statsmakt är samhällsviktig, men avslöjanden som exempelvis leder till politiska skandaler kan snarast *medföra att en kris uppstår*.

### Huruvida en kris kan uppstå i samhället vid avbrott hos bolag i mediebranschen



**Figur 1:** De första tre stapelgrupperna återger svaren till fråga 1 ovan, de tre senare stapelgrupperna återger svaren till fråga 2.

Resultaten stämmer i delar överens med vad MSB har observerat i samband med en liknande undersökning mot transportsektorn, med några få skillnader.<sup>22</sup> Den samlade bilden, som följer ur definitionen av samhällsviktig verksamhet och aktörernas svar, är att det finns en uppfattning bland mediebranschens aktörer att det finns en förhållandevis hög grad av samhällsviktighet i mediebranschens verksamhet.<sup>23</sup>

En annan skillnad som är genomgående är de svarande branschaktörernas betoning av hur fort en samhällelig kris kan uppstå på den lokala nivån, och därmed hur samhällsviktig deras verksamhet är på lokal nivå. En hypotes för att förklara det är att frågorna handlade om huruvida en samhällelig kris kan uppstå om verksamheten drabbas av ett avbrott. Om en sådan verksamhet drabbas av ett avbrott och det i nära anslutning till det också uppstår ett lokalt krisläge där det finns ett stort behov av att nå ut med information kan det sammantaget uppstå en samhällelig kris.

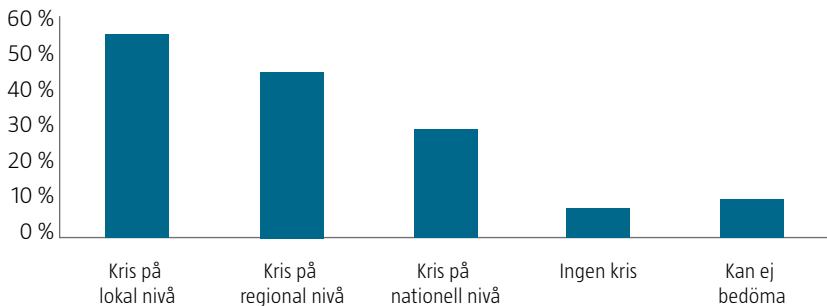
22. De dubbla trenderna att stapeln Ingen kris går ned medan stapeln Kris på nationell nivå går upp återfinns inom den andra undersökningen. En skillnad från transportsektorn är att Ingen kris-stapeln är klart mindre och Kris på nationell nivå-stapeln är klart större inom mediebranschen vid utgångsläget (stapelgruppen längst till vänster) än inom t.ex. transportbranschen. Samtidigt är Ingen kris-stapeln tydligt lägre och Kris på nationell nivå-stapeln högre i slutläget (stapelgruppen längst till höger).

23. Det ska inte tolkas som att mediebranschens aktörer därmed anser att andra sektorer verksamhet inte också är samhällsviktig, eller att de sektorernas verksamheter är mindre samhällsviktiga. Resultaten pekar enbart på att mediebranschens aktörer skattar branschens verksamhet som lite mer samhällsviktig än vad andra aktörer gör när de skattar verksamheten inom sin egen bransch.

Den statistik som redovisas i avsnitt 2.1 Distribution ovan pekar på att i synnerhet äldre personer använder internetbaserade medietjänster i begränsad utsträckning och därför saknar det stora utbud och de möjligheter till interaktivt informationsutbyte som sådana tjänster erbjuder, och av den anledningen skulle de kunna bli särskilt drabbade. Om det är en riktig hypotes är det ett tecken på att den pågående neddragningen av lokalmedier kan vara särskilt allvarlig. Den trenden redovisas mer i detalj i de två första avsnitten i kapitel 2: Utveckling och trender ovan.

Hur viktiga lokalt baserade och förankrade medier är betonats ytterligare av svaren på den tredje frågan ovan (som i sin tur relaterar till det andra villkoret i definitionen av samhällsviktig verksamhet ovan).

Huruvida den egna verksamheten är nödvändig eller mycket väsentlig för att skadeverkningarna av en kris i samhället ska kunna minimeras



**Figur 2:** Staplarna återger svaren på fråga 3 ovan om självskattad samhällsviktighet på olika samhällsnivåer.

Det är anmärkningsvärt att andelen branschaktörer som menar att de har en uppgift inom krishanteringen på lokal, regional och nationell nivå är betydligt högre i mediebranschen än i transportsektorn, sett till de svar MSB har fått i respektive undersökning. Digitaliseringen har medfört att enskilda individer kan inhämta och sprida information utan att använda traditionella medier, och det är troligt att samhällsaktörer, exempelvis myndigheter, kommer att kunna nå betydande delar av befolkningen under en samhällskris även om traditionella medier inte kan agera med full funktionalitet. Däremot är det möjligt att hanteringen av en samhällskris begränsas och tar

längre tid om lokala medier inte fungerar. Vissa grupper (i synnerhet äldre) kan också ha mycket stor nytta av, eller till och med vara beroende av, traditionella medier för att på ett optimalt vis klara av en samhällskris.

### **3.4 Identifierade samhällsviktiga verksamheter inom mediebranschen**

Utifrån de tre samhällsviktiga temana presenteras nedan några särskilda funktioner och verksamheter inom mediebranschen som utgör samhällsviktiga verksamheter. Verksamheterna presenteras i ordning av det tema de främst hör till.

#### **3.4.1 Krishantering**

Krishanteringstemat omfattar ett flertal samhällsviktiga verksamheter och funktioner. Utöver ordinarie nyhetsrapportering vid kriser och förmedling av samhällsinformation i allmänhet bör de följande företeelserna särskilt omnämnas.

Public service (under höjd beredskap)

I Sverige finns det två nivåer av höjd beredskap: skärpt beredskap och högsta beredskap. Regeringen får besluta om skärpt eller högsta beredskap om Sverige är i krigsfara eller om det råder utomordentliga förhållanden som är förorsakade av att det förekommer krig utanför Sveriges gränser alternativt att Sverige har varit i krig eller krigsfara. Om Sverige befinner sig i krig så råder högsta beredskap per automatik.

Vid beredskapshöjning ingår SR, SVT och UR i totalförsvaret. Totalförsvaret är den verksamhet som är nödvändig för att förbereda Sverige för krig. I sändningstillstånden mellan staten och public service-bolagen anges att om högsta beredskap råder ska SR och SVT utgöra självständiga organisationer med totalförsvarsuppgifter och lyda direkt under regeringen. Vid högsta beredskap ställs UR:s resurser till SR:s och SVT:s förfogande. Även vid skärpt beredskap kan regeringen besluta om att public service ska fungera på samma sätt som om det vore högsta beredskap. Public service-bolagen ska dock vägledas av de bestämmelser om programverksamhet som finns i tillstånds- och anslagsvillkor även vid höjd beredskap och svåra påfrestningar på samhället i fred.

MSB har tidigare bedömt att delar av SVT:s (och, i förlängningen, public services) krishanterings- och stödfunktioner utgör viktiga

samhällsintressen. Se den externa bilagan 2: MSB:s särskilda uttalande med anledning av strejkvarslet hos SVT i april 2016.

Viktigt meddelande till allmänheten (VMA)

VMA används vid olyckor och samhällsstörningar för att omedelbart varna och informera allmänheten. Sändningsledningen hos Sveriges Radio (SR) ser till att meddelandet sänds i radio- och tv-sändningar (inklusive text-tv). SR ansvarar för innehåll och utformning, och ser till att meddelandet har en lämplig utformning samt att det genom sin omfattning eller på annat sätt inte negativt påverkar programverksamheten. Sändningsledningen förser även privat lokalradio och vissa kommersiella tv-kanaler med underlag för vidareändring av VMA.

Utöver SVT sänder även tv-kanalerna TV4, Kanal 5 och Kanal 9 VMA enligt avtal. Polisen, kommunal räddningsledare och statlig räddningsledare samt Strålsäkerhetsmyndigheten, SOS Alarm, smittskyddsläkare och anläggning med farlig verksamhet kan begära ett VMA.

VMA kan även vid behov meddelas med hjälp av landets utomhusvarningssystem som består av cirka 4 500 varningsanläggningar med ljudsändare. Det pågår ett arbete för att vidareutveckla VMAs funktionen så att hörselskadade lättare ska kunna ta del av samhällsviktig information. SOS Alarms SMS-tjänst (se nedan) är ett steg i denna utveckling.

”Viktigt meddelande” är en av fyra signalkaraktärer som kan utlösas i det existerande utomhusvarningssystemet. De övriga är ”Faran över”, ”Beredskapslarm”, och ”Flyglarm”. Efter att signalen ”Viktigt Meddelande” utlösts läses ett meddelande upp i SR som beskriver händelsen och vad allmänheten behöver göra för att undgå de eventuella faror som finns. Detta blir det viktiga meddelandet till allmänheten.

Sedan 2013 har ett arbete pågått med att ta fram ett kompletterande system till VMA inom SOS Alarm. Sedan 2014 kan utskick av meddelanden i form av talmeddelande göras till fasta telefonlinjer. I februari 2015 tillkom även möjligheten att skicka ut meddelanden till adressregistrerade mobiler<sup>24</sup> via sms.

---

24. Användaren har ett mobiltelefonabonnemang registrerat hos en mobiloperatör med en tillhörande gatuadress.

#### Myndighetsmeddelanden

Myndighetsmeddelanden är avsedda för händelser som ur ett tidsperspektiv inte bedöms utgöra akut fara för liv. De har karaktären av servicemeddelanden men kan ha ett innehåll som gränsar mot det som skulle falla under VMA. Myndigheterna kontaktar SR P4 lokalt när de önskar sända ett myndighetsmeddelande till allmänheten. Ett myndighetsmeddelande ska sändas utan skäligen dröjsmål. SR ska kostnadsfritt sända de meddelanden som är av vikt för allmänheten. Om en myndighet begär det ska SR också säkerställa att meddelandet utformas på ett lämpligt sätt.

#### Utökad varningssystem vid kärnkraftverk

Ett särskilt varningssystem finns för kärnkraftsolyckor. Inom den inre beredskapszonen kring kärnkraftverken ska allmänheten kunna varnas både utomhus och inomhus. Utomhus används samma system som för övrig utomhusvarning, men för inomhusvarning används RDS-systemet (Radio Data System). För att kunna få denna varning har alla hushåll inom den inre beredskapszonen mottagit särskilda radiomottagare som är avsedda för varningsmeddelande. Länsstyrelserna i de län där kärnkraftverk finns i dag, det vill säga Halland, Kalmar och Uppsala, ansvarar för information till allmänheten i fråga om kärnkraftsvarningar.

#### Krisinformation.se

MSB driver webbsidan Krisinformation.se och via den förmedlas information från myndigheter och andra ansvariga till allmänheten före, under och efter en stor händelse eller kris. All information som finns på sidan är bekräftad information från myndigheter och övriga ansvariga. Före en kris förmedlar Krisinformation.se nyheter om allvarliga händelser i Sverige och utomlands, varav vissa kan utvecklas till kriser. På sajten finns också information om hur myndigheter arbetar för att förebygga och hantera kriser. Sidan beskriver också vad enskilda individer själva har för ansvar och vad de kan göra för att skydda sig före och under en kris.

Under en kris ger Krisinformation.se allmänheten en översiktlig bild av vad som har hänt genom att sammanställa och sprida information från myndigheter, kommuner och andra aktörer. Det går också att ställa frågor till redaktionen via Facebook och Twitter om händelsen.

Efter krisen fortsätter redaktionen att beskriva vilken hjälp och vilket stöd för den som har drabbats som finns hos myndigheter och andra aktörer.



### 3.4.2 Granskning

Granskningstemat omfattar all fördjupad samhällsgranskning som på ett väsentligt sätt informerar allmänheten om missförhållanden, vanskötsel, korruption, brottslighet och andra aspekter som är av synnerligt värde för att enskilda individer ska kunna utöva sina demokratiska rättigheter på ett informerat sätt.

Exempel på samhällsgranskning inom medier

Samhällsgranskning inom medier underlättar för befolkningen att fatta egna beslut som bygger på ett bra och riktigt underlag när de till exempel ska rösta fram förtroendevalda eller göra val mellan olika produkter och tjänster i rollen som konsument.

Ett exempel på samhällsgranskande journalistik och dess inverkan är DN:s avslöjanden om missförhållanden inom Riksrevisionen under sommaren 2016. Riksrevisionen – med uppgift att själva genomföra oberoende revision i syfte att stärka den demokratiska insynen och säkerställa en god resursanvändning och en effektiv förvaltning i staten – blev granskade av journalister och det avslöjades att de agerat olämpligt, begått allvarliga fel och brutit mot regler. Ett annat exempel är SVT:s program Uppdrag granskning avslöjanden om Telia Soneras affärer i Uzbekistan där bolaget anklagats för att ha släppt in den uzbekiska säkerhetstjänsten i sina egna telefonväxlar och mutat sig till 3G-licenser och telefonnummerserier från personer med koppling till regimen.

### 3.4.3 Trygghet

Det är svårt att peka ut några särskilda verksamheter som faller inom temat. Snarare handlar det om att helheten och mångfalden av utbudet inte får försvinna. Om det mediala utbudet skulle begränsas – exempelvis genom att en aktör blir utsatt för angrepp eller att delar av informationsinfrastrukturen slås ut – kan detta väntas ge effekt hos befolkningen genom det symboliska i att vardagsflödets normalitet brutits. Tryggheten ska alltså inte begränsas till att enbart förstås som den dagliga nyhetsrapporteringen utan omfattar i någon utsträckning all produktion och distribution av medialt innehåll.

# **Risker och sårbarheter i mediebranschen**

## 4. Risker och sårbarheter i mediebranschen

### 4.1 Inledning

I detta kapitel presenteras resultatet av MBS:s riskanalys av verksamhetsnära risker och samhällsrisker. Analysen grundar sig på den redogörelse som presenterats i de ovanstående kapitlen. Den utgår från ett tillstånd av fred, det vill säga ett läge där det varken råder krig eller krigsrisk i Sverige eller i Sveriges närområde. En analys av hur förutsättningarna och riskerna förändras vid ett säkerhetspolitiskt försämrat läge presenteras i kapitel 5: Mediebranschen och det civila försvaret nedan.

MSB har i analysen behandlat fler risker än de som redovisas här. Endast risker som efter analysen har befunnits välgrundade och tillräckligt allvarliga redovisas.

I redovisningen av riskerna hänvisas till ett antal incidenter. Vissa av de incidenterna refereras fler än en gång. Meningen med det är att illustrera att incidenter ofta realiserar fler än en risk.

De identifierade riskerna har delats upp i verksamhetsnära risker och samhällsrisker. De verksamhetsnära riskerna grundar sig primärt på den enkät som har skickats till den svenska mediebranschen. Samhällsriskerna baseras primärt på omvärldsbevakning, litteraturstudie samt intervjuer och workshop. De två risktyperna kan ha stor inverkan på varandra. Det som händer på verksamhetsnivå hos en eller flera aktörer inom branschen kan få direkta effekter på samhällsnivå. Fenomen och utveckling på samhällsnivå kan i sin tur ha direkta konsekvenser på den enskilda verksamheten och effekter på all form av medieverksamhet. Eftersom mediebolagen utgör den här rapportens primära målgrupp presenteras för de bolagen verksamhetsnära risker först.

### 4.2 Metod för riskanalysen

I arbetet med riskanalysen har vissa metodval gjorts. Riskerna och deras benämningar är *tematiska*, och med det avses att de är neutrala i termer av hur de realiserar. Riskerna beskrivs och analyseras alltså inte i termer av till exempel antagonism eller särskilda sätt som de hade kunnat uppstå på.<sup>25</sup> Ett exempel på detta är risken ”Egendom

---

25. Det finns dock två undantag i avsnittet om samhällsrisker nedan.

kommer att drabbas av skada” som redovisas nedan. Skada på egendom kan orsakas av antagonistiska handlingar<sup>26</sup> som sabotage eller annan skada, men även genom icke-antagonism som handhavandefel, eller naturfenomen som bränder och på andra sätt. I stället för att behandla risken för brand separat samlas sätten som egendom kan drabbas av skada under en och samma tematiska risk. Några av sätten som risken kan realiseras på redovisas som exempel.

Riskerna bedöms utifrån sannolikhet (hur ofta de inträffar), incidenten i sig och dess konsekvenser<sup>27</sup> (hur mycket skada de medför) samt konfidens (hur goda grunder det finns för bedömningen). Sannolikhetsbedömningarna, incident- och konsekvensbedömningarna och konfidensbedömningarna görs alla enligt skalan: mycket låg, låg, medelhög, hög, mycket hög.

Varje risk presenteras enligt det följande upplägget:

1. **Riskbenämning:** Riskens namn i form av den skadliga händelsen som risken kan utlösa om den realiseras.
2. **Bedömning:** En box med sannolikhetsbedömning, incident- och konsekvensbedömning (kort: konsekvensbedömning), en samlad riskvärdering utifrån sannolikhets- och incident- och konsekvensbedömningen samt en konfidensbedömning.
3. **Riskbeskrivning:** Beskrivning av risken i form av relevant statistik, påverkade beroenden och/eller samhällsviktig verksamhet, typiska scenarier för risken (om risken handlar om att verksamhetskritisk information blir otillgänglig så kanske ett scenario som skulle kunna leda till det vore brand i verksamhetens lokaler eller gisslanprogramvaruinfektion i it-systemen).
4. **Orsaksbeskrivning:** Beskrivning av möjliga orsaker till risken.
5. **Sårbarhetsbeskrivning:** Om det finns en identifierad sårbarhet som påverkar risken redovisas det.
6. **Skyddsbeskrivning:** Om det finns ett identifierat skydd som påverkar risken redovisas det.
7. **Konsekvensbeskrivning:** Möjliga konsekvenser av risken beskrivs för enskilda individer, mediebolag och samhället.

26. Handlingar som medvetet genomförs i syfte att skada.

27. Det talas ofta om sannolikhets- respektive konsekvensbedömning. I den här analysen betonas dock att den önskade händelse som risken i sig är medför skada, och att den skadan kan förvärras genom att den oönskade händelsen i sin tur kan ha ytterligare negativa konsekvenser.

Riskanalysen är indelad i två avsnitt, utifrån de två fokusområden som den föreliggande riskanalysen omfattar. Det första fokusområdet är verksamhetsnära risker, det vill säga risker för mediebolagen själva. Det andra fokusområdet är samhällsrisker, alltså risker för samhället i stort som har en tydlig bäring på eller tar sina avstamp i mediebranschen.

Mer information om den metod som använts i rapporten finns i den externa bilagan 7.

#### 4.2.1 Sammanställning av de verksamhetsnära riskerna

Här presenteras en sammanställning av de verksamhetsnära risker som presenteras i detalj i avsnitt 4.4 Verksamhetsnära risker och sårbarheter nedan.

RISKBENÄMNING	SANNOLIKHET	KONSEKVENS	KONFIDENS	RISK-BEDÖMNING
Personal kommer att skadas fysiskt eller psykiskt	Medelhög	Hög	Hög	Hög
Verksamhetskritisk information kommer att bli otillgänglig	Medelhög	Hög	Medelhög	Hög
Egendom kommer att drabbas av skada	Medelhög	Hög	Låg	Hög
Verksamhetskritisk information kommer att bli röjd	Mycket låg	Hög	Medelhög	Låg
Allmänhetens förtroende för organisationen kommer att minska	Låg	Medelhög	Medelhög	Låg
Verksamhetskritisk information kommer att bli felaktigt ändrad	Mycket låg	Medelhög	Låg	Låg
Verksamhetskritisk information kommer att bli felaktigt raderad	Mycket låg	Medelhög	Låg	Låg

De redovisade verksamhetsnära riskerna är händelseorienterade. Det betyder att de handlar om enstaka oönskade händelser. Mer långsiktiga utvecklingar har inte behandlats, även om de naturligtvis kan utgöra risker. Därför behandlas inte den pressade ekonomiska situationen för många medier som en egen risk i detta avsnitt. I stället bör riskerna och mediernas förmåga att stå emot dem ses mot bakgrund av den ekonomiska situationen.

#### 4.2.2 Sammanställning av samhällsriskerna

Här presenteras en sammanställning av de samhällsriskerna som presenteras i detalj i avsnitt 4.5 Samhällsrisker och sårbarheter nedan.

RISKBENÄMNING	SANNOLIKHET	KONSEKVENS	KONFIDENS	RISK-BEDÖMNING
Påverkanskampanjer bedrivs mot allmänheten och beslutsfattare genom medier	Hög	Hög	Hög	Hög
Sveriges informationsinfrastrukturer är otillräckligt skyddade mot angrepp	Hög	Hög	Medelhög	Hög
Mediekonsumtionen ger inte redundans till krisberedskapen	Medelhög	Hög	Hög	Hög
Samhället har en otillräcklig beredskap för att hantera storskaliga och plötsliga kontroverser	Hög	Medelhög	Medelhög	Hög
Vissa områden och samhällsgrupper hamnar i medieskugga	Låg	Medelhög	Låg	Låg

### 4.3 Beroenden och sårbarheter

Resultaten om mediebolagens beroenden och sårbarheter, som redovisas nedan, har utgjort underlag för bedömningen av de risker som har identifierats. De företagsen som ingått i respektive riskbedömning nämns uttryckligen i respektive risks text i avsnitt 4.4 Verksamhetsnära risker och sårbarheter nedan.

De flesta branscher har i dag ett antal tvärsäktoriella beroenden. Vissa typer av beroenden är genomgående för i stort sett alla branscher, medan andra är mer specialiserade. Ett beroende av något måste inte i sig göra ett bolag särskilt sårbart, utan det beror på i vilken utsträckning bolaget har säkerställt försörjningen av det som bolaget är beroende av. Utifrån det resonemanget valde MSB ut 14 företagsen (el, elektroniska kommunikationer, etc.) och ställde följande frågor för respektive företagsen:

1. Har ni (bolaget) analyserat om ni är beroende av företagsen, och i vilken utsträckning (om någon) som ni är beroende av företagsen?
2. Har ni (bolaget) vidtagit åtgärder för att säkerställa försörjningen av företagsen, och i vilken utsträckning bedömer ni att försörjningen av företagsen är säkerställd?
3. Har ni (bolaget) planer på att vidta åtgärder för att säkerställa försörjningen av företagsen, och i vilken utsträckning anser ni er vara i behov av att vidta sådana åtgärder?

MSB matade sedan in svaren i en modell där den sammanlagda och för branschen övergripande sårbarheten kortsiktigt och långsiktigt beräknades, samt vilken grad av osäkerhet som präglar beräkningen. Skalan som användes för bedömning är: mycket hög, hög, medelhög, låg, mycket låg. Den bakomliggande tanken är att om en aktör bedömer sig vara i hög grad beroende av någon företagsen, samtidigt som aktören inte har gjort tillräckligt för att säkerställa tillgången, är aktören sårbar i förhållande till den företagsen. Om en konsekvens av en inträffad risk är att tillgången eller försörjningen av en sådan företagsen avbryts förvärras skadan i proportion till hur sårbar den drabbade aktören är i förhållande till företagsen.

En översikt av resultaten presenteras i ordning av den företeelse som sammantaget har visats utgöra det största beroendet och sedan i fallande ordning:

<b>FÖRETEELSE</b>	<b>GRAD AV BEROENDE</b>	<b>BEDÖMNING AV SÅRBARHET</b>	<b>OSÄKERHET I BEDÖMNING</b>
It-system	Mycket högt beroende	Medelhög sårbarhet	Låg osäkerhet
Elektroniska kommunikationer	Mycket högt beroende	Medelhög sårbarhet	Låg osäkerhet
It-tjänster	Mycket högt beroende	Medelhög sårbarhet	Låg osäkerhet
EI	Mycket högt beroende	Medelhög sårbarhet	Medelhög osäkerhet
Allmänhetens förtroende	Mycket högt beroende	Medelhög sårbarhet	Låg osäkerhet
Personal med specialkompetens	Högt beroende	Medelhög sårbarhet	Låg osäkerhet
Verksamhetsrelevant information	Högt beroende	Medelhög sårbarhet	Låg osäkerhet
Korrekt tid	Högt beroende	Låg sårbarhet	Medelhög osäkerhet
Andra aktörer i samma sektor	Högt beroende	Låg sårbarhet	Medelhög osäkerhet
Behovsanpassade lokaler	Högt beroende	Låg sårbarhet	Låg osäkerhet
Aktörer i andra sektorer	Högt beroende	Låg sårbarhet	Medelhög osäkerhet
Outsourcade tjänster	Visst beroende	Låg sårbarhet	Låg osäkerhet
Myndighetstjänster	Visst beroende	Låg sårbarhet	Låg osäkerhet
Positionssystem	Visst beroende	Låg sårbarhet	Medelhög osäkerhet



## 4.4 Verksamhetsnära risker och sårbarheter

Nedan presenteras sju verksamhetsnära risker och tillhörande aspekter. Varje rubrik ska läsas som Risken att [namnet på risken]. Riskerna presenteras utifrån bedömningen högst till lägst riskgrad.

### 4.4.1 Personal kommer att skadas fysiskt eller psykiskt

Den samlade bedömningen för risken att personal inom mediebranschen skadas fysiskt eller psykiskt är **hög**. Sannolikheten för att sådana incidenter ska ske bedöms som medelhög, och skulle det inträffa blir konsekvensen hög. Bedömningen av risken baseras på ett varierat underlag med relativt hög samstämmighet bland de olika källorna. Ett undantag i samstämmigheten är MSB:s enkätsvar om antagonistiskt orsakad fysisk skada mot personal och den övriga tillgängliga statistiken. Konfidensen bedöms som **hög**.

I MSB:s enkät anger nio respektive 14 respondenter (18 procent och 29 procent) att de under det närmaste året har haft minst en antagonistisk incident där personal drabbats fysiskt respektive psykiskt. För icke-antagonistiska incidenter angav fem respektive fyra respondenter (10 procent och 8 procent) att de under det närmaste året hade drabbats av fysisk respektive psykisk skada. Detta kan jämföras med en undersökning från Tidningsutgivarna (TU) 2016 där endast två av respondenterna (1 procent) angav att de utsatts för våld de senaste 12 månaderna. I en annan undersökning, gjord av Utgivarna 2016, svarade 2 av 94 redaktioner att de haft medarbetare som utsatts för våld. Hot och trakasserier är däremot vanligare. I samma undersökning svarade 42 av de 94 redaktionerna som deltog att de hotats under de senaste tolv månaderna, en ökning från 2015 då 33 av 101 svarade det samma. 41 av de 94 redaktionerna svarade att de haft medarbetare som utsatts för trakasserier under de senaste 12 månaderna.

I en annan undersökning av TU från 2016 svarade 20 procent (av 619 respondenter) att de hotats, och 27 procent att de trakasserats, under de senaste 12 månaderna. När Journalistpanelen vid Göteborgs universitet frågade 2241 journalister om de drabbats av hot och trakasserier uppgav 30 procent att de hotats och 66 procent att de fått motta nedsättande kommentarer under de senaste 12 månaderna. Situationen har lett till att Sverige har sjunkit från en femte plats

2015 till åttonde plats i Reportrar utan gränsers ranking World Press Freedom Index.

Den övergripande bilden är att även om hot och trakasserier är vanliga omsätts sällan hoten i faktisk fysisk handling mot den enskilde journalisten.

Riskens orsaker

Orsakerna, och motiven, till hot och trakasserier mot medier är flera. Hat, vrede och ilska över en enskild publicering kan generera hot. En vilja att pacificera journalister förekommer också. Enskilda personer utgör den största källan till hot och trakasserier mot journalister. Även ideologiska skäl kan ligga bakom och bland extrema grupperingar är de högerextrema rörelserna de som oftast hotar och trakasserar medier. Det finns indikationer på att trösklarna för hot och trakasserier sänkts samt att hatet enklare når fram till journalister i och med digitaliseringen och de många och lättillgängliga kontaktvägar som uppkommit med den. Icke-antagonistiska incidenter kan orsakas av olika olyckor men även sjukdom, till följd av exempelvis epidemi och pandemi. 40 procent av mediebolagen bedömde i *Mediebranschen 2011 – Hot, risker och sårbarheter* att det var troligt att en epidemi eller pandemi skulle inträffa.

Sårbarheter och skydd

Mediebolagen har i denna analys befunnits ha en hög grad av beroende av personal med specialkompetens, och det beroendet utgör en medelhög sårbarhet för mediebolagen. Skadan för bolaget kan därmed variera ganska kraftigt beroende på om den eller de drabbade har specialkompetenser som ingen annan på bolaget har – och som det kan vara svårt att ersätta.

De ekonomiska omständigheterna och kravet på att följa med i digitaliseringen för att överleva har medfört att många lokalredaktioner lägger ned sina redaktioner. Det har eventuellt lett till att de få redaktioner som finns kvar blir desto mer sårbara. Skulle hot och allvarliga trakasserier riktas mot en redaktion där ett mindre antal personer jobbar, kan verksamheten snabbt sättas ur spel. Samhället har en central roll att spela som stöd för dessa sårbara aktörer, särskilt i form av polisiär närvaro och omhändertagande av anmälningar.

31 procent respektive 35 procent av respondenterna i enkätundersökningen anger att de inte vet hur fort de kan vidta åtgärder för att hantera en incident där personal har lidit fysisk respektive psykisk skada. 55 procent anger att de kan agera inom två timmar när personalen har drabbats av fysisk skada och 39 procent anger att de

kan agera inom två timmar om personalen har drabbats av psykisk skada. Bortsett från de som svarar att de inte vet hur fort de skulle kunna agera så finns det ingen som svarar att det skulle ta mer än 24 timmar att agera för vare sig incidenter där personalen har drabbats av fysisk skada eller incidenter där personalen har drabbats av psykisk skada. Mediebranschens aktörer har under ledning av TU upprättat Mediernas säkerhetsgrupp. Ordförande för gruppen är TU:s vd, och medlemmarna utgörs av public service-bolagen, Bonnier, Mittmedia, Schibsted och några andra. Gruppen har ett nära samarbete med polisen, med vilken hotinformation återkommande utbyts. För att stödja arbetet har polisen även tillsatt en särskild beredningsgrupp.

Konsekvenser om risken realiserar

Hot och trakasserier utlöser oro och rädsla bland de journalister som drabbas och förändringar i livsvanor kan bli nödvändiga. I vissa fall kan hot och trakasserier medföra självscensur. Många som drabbas börjar tvivla på sitt yrkesval. För andra enskilda individer kan konsekvensen bli att de inte förvärvar nödvändiga eller nyttiga kunskaper om i synnerhet lokala skeenden. För enskilda bolag kan konsekvenserna bli sjukskrivningar, lägre produktivitet och i värsta fall att medarbetare slutar. Mycket beror på hur fort bolaget kan bistå sina anställda med stöd och hjälp, samt vilket stöd den drabbades omgivning kan ge.

För samhället och demokratin kan konsekvenserna bli allvarliga om rapporteringen om vissa ämnen och grupper uteblir till följd av hot. En långsiktig följd av det är att det kan etableras en uppfattning om att hota journalister är ett sätt att undgå granskning på. Det demokratiska ansvarsutkrävandet förutsätter en livskraftig mediebransch som granskar politiker och beslutsfattare, bolag, civilsamhälle och brottslig verksamhet.

#### 4.4.2 Verksamhetskritisk information kommer att bli otillgänglig

Den samlade bedömningen är att risken för att verksamhetskritisk information har blivit otillgänglig är **hög**. Sannolikheten för att sådana incidenter ska ske bedöms som medelhög, och skulle det inträffa blir konsekvensen hög. Ett någorlunda varierat underlag har legat till grund för bedömningen. Konfidensen bedöms som **medelhög**.

I MSB:s enkät svarade nio respondenter (18 procent) att de under den senaste 12 månaderna drabbats av minst en antagonistisk incident där verksamhetskritisk information blev otillgänglig. För icke-antagonistiska incidenter uppgav 13 respondenter (27 procent) detsamma. Digitaliseringen har medfört ökad tillgång till information. Utvecklingen har också inneburit att tillgången är sårbar på nya sätt. Antalet möjliga attacktyper och felkällor har mångdubblats.

En trend av det antagonistiska slaget är spridningen av gisslanprogramvara (engelskans ransomware). Gisslanprogramvara är en typ av skadlig kod som krypterar innehållet på lagringsmedier (som hårddiskar eller USB-minnen) varpå ett krav på betalning görs för att det "kidnappade" innehållet ska släppas för användaren.<sup>28</sup> Givet det snabba informationsflödet och den centrala roll som information har i journalisters och redaktioners dagliga arbete kan dessa verksamheter väntas löpa en relativt stor risk för denna typ av angrepp. Tillgången till information via distributionsplattformar som nätbaserade tidningar, eller webb-tv kan störas genom DDoS-attacker. Att fler respondenter svarar att verksamhetskritisk information gjorts otillgänglig genom en icke-antagonistisk incident kan indikera att exempelvis handhavandefel och driftavbrott utgör en mer aktuell risk för branschens aktörer och tillgängligheten till verksamhetskritisk information.

I Mediebranschen 2011 – Hot, risker och sårbarheter för mediebranschen bedömde mediebolagen i snitt att risken för avbrott i elektroniska kommunikationer var allvarligast sett till sannolikhet (lite över sex på en tiogradig skala). Ibland finns verksamhetskritisk information hos människor själva, och då blir tillgången till informationen beroende av tillgången till personen, varför plötslig frånvaro från arbetsplatsen genom sjukdom eller av andra skäl kan innebära att risken realiserar.

28. I viss mån kan denna typ av händelse likställas med "Verksamhetskritisk information kommer att bli felaktigt raderad" då konsekvenserna kan bli helt lika.

#### Riskens orsaker

Ekonomiska motiv hos en antagonistisk part kan också vara orsak till att verksamhetskritisk information blivit otillgänglig. Här finns risk för utpressning av personer och organisationer. DDoS-attacker mot exempelvis tidningars webbsidor kan initieras utifrån en önskan om att hämnas genom sabotage, men sådana attacker kan också genomföras för att sända ett budskap till tredje part (tidningens läsare), i syfte att skapa oro och rädsla. För icke-antagonistiska incidenter kan orsaker som undermåliga serviceavtal (engelskans Service Level Agreements) med driftleverantörer, kompetensbrist hos personal som leder till handhavandefel och större elavbrott eller avbrott i elektroniska kommunikationer ligga bakom. I de fall verksamhetskritisk information blir otillgänglig till följd av en frånvarande medarbetare kan alltifrån sjukdom till hot och trakasserier vara orsaker.

#### Sårbarheter och skydd

Mediebolagen har i MSB:s analys befunnits ha en hög grad av beroende av verksamhetsrelevant information och det beroendet utgör en medelhög sårbarhet för mediebolagen. De bolag som håller sig med egna it-system och egen drift av dem blir mycket beroende av kompetent it-personal med specialistkunskaper. Eftersom tillgången till sådan kompetens är begränsad kan säkerställandet av en kontinuerlig it-drift vara särskilt sårbart för plötslig frånvaro av sådan personal. Av samma skäl kan det vara svårt att nyrekrytera personal med de rätta kunskaperna.

Bland respondenterna i enkätundersökningen anger 33 procent att de inte vet hur fort de kan vidta åtgärder för att hantera en incident där verksamhetsrelevant information har blivit otillgänglig. 45 procent anger att de kan agera inom två timmar, och endast två procent behöver mer än 12 timmar.

#### Konsekvenser om risken realiserar

För den enskilde individen bedöms konsekvenserna i regel bli begränsade om de alls märks. Driftavbrott i utsändning av radio eller tv, eller avbrott i driften av en webbaserad tidnings hemsida kan innebära att eftersökt innehåll inte kan nås. Bredden i tjänsteutbudet medför dock att mediekonsumenten i regel har andra alternativ att vända sig till. Hur allvarlig en incident kan bli beror på vilken typ av mediebolag det rör sig om, hur mycket och vilken information som har blivit otillgänglig etc.

För mediebolag liksom för samhället är konsekvenserna uppskattningsvis begränsade om det rör sig om en kortare tids otillgänglighet. Drabbas ett bolag av en gisslanprogramvaruinfektion som krypterar stora delar av de interna nätverken kan mycket av den kontinuerliga verksamheten avstanna. För samhället blir konsekvenserna i regel begränsade om avbrottet gäller enstaka mediebolag eller under kortare tidsperioder. Om avbrott sker över längre tidsperioder eller drabbar många, exempelvis om webbplatser har gjorts otillgängliga, kan det orsaka problem för både individer och organisationer och därtill kan oro uppstå.

#### 4.4.3 Egendom kommer att drabbas av skada

Den samlade bedömningen är att risken för att egendom kommer att drabbas av skada är **hög**. Sannolikheten för att sådana incidenter ska ske bedöms som medelhög, och skulle det inträffa blir konsekvensen hög. Underlaget som använts till bedömningen är begränsat och baseras på statistik från enkäten. Då det huvudsakligen finns ett underlag till stöd för risken kan samstämmighet inte bedömas. Konfidensen bedöms som **låg**.

Risken kan realiseras genom allt från skadegörelse i form av sabotage till handhavandefel, bränder eller naturhändelser som översvämningar. I MSB:s enkätundersökning angav nio respondenter (18 procent) att utrustning blivit otillgänglig, fyra respondenter (8 procent) att utrustning förstörts, sex respondenter (12 procent) att organisationens lokal(er) blivit (temporärt) otillgängliga och en respondent (2 procent) att organisationens lokal(er) förstörts i antagonistiska incidenter, allt detta inom ett tidsspänn omfattande det senaste året. På samma fråga avseende icke-antagonistiska incidenter angav 13 respondenter (27 procent) att utrustning blivit otillgänglig, fem respondenter (10 procent) att utrustning förstörts, två respondenter (4 procent) att organisationens lokal(er) (temporärt) blivit otillgängliga under det senaste året. Ingen angav att organisationens lokal(er) förstörts genom en icke-antagonistisk incident under det senaste året.

#### Riskens orsaker

Utifrån respondenternas svar följer det tydligt att antagonism i större utsträckning har varit orsak till att lokaler har skadats, medan utrustning oftare skadas utan att det har funnits något ont uppsåt. En tänkbar orsak till att lokaler utsätts för åverkan oftare än utrustning kan vara att risken för att bli observerad eller påkommen med skadegörelse vid vissa tider under dygnet är låg, medan utrustning i regel antingen är inlåst eller används. Skadegörelse kan orsakas av ilska mot bolagets verksamhet, i syfte att hota, skrämja eller hämnas. Det kan också finnas ideologiska orsaker eller att skadegörelsen sker som ett resultat av annan brottslig verksamhet (såsom exempelvis inbrott). Icke-antagonistiska incidenter som innebär att egendom skadas kan orsakas av slarv och brand i exempelvis elektronisk utrustning etc.

#### Sårbarheter och skydd

Risken påverkas av det höga beroendet av behovsanpassade lokaler och de mycket höga beroendena av it-system, it-tjänster och elektroniska kommunikationer. Incidenter som brand i exempelvis datahallar, master eller sängutrustningar kan utgöra en allvarlig källa till skada på flera verksamhetskritiska resurser och i förlängningen på framförallt den distributiva förmågan. Företeelserna har i MSB:s analys bedömts utgöra en medelhög sårbarhet för mediebolagen och beroende på hur risken realiserats kan skadan för bolaget komma att variera kraftigt.

Mediebolagen bedömer sig snabbt kunna bemöta incidenter där utrustning eller lokaler blir otillgängliga eller förstörda: 28 respektive 25 respondenter (57 procent och 51 procent) anger att de kan vidta åtgärder för att hantera att utrustning har blivit otillgänglig respektive förstörd inom fyra timmar, 27 respektive 23 respondenter (55 procent och 47 procent) säger sig kunna vidta åtgärder inom fyra timmar om organisationens lokaler har blivit otillgängliga respektive förstörda. Eftersom mediebolagens verksamhet i många avseenden förutsätter ett agilt arbetssätt bedömer MSB att de övergripande har en god förmåga att snabbt vidta åtgärder för att kunna bedriva verksamhet under andra former.

#### Konsekvenser om risken realiserats

För enskilda individer inom allmänheten medför risken inga särskilda konsekvenser. För det enskilda bolaget kan konsekvenserna variera kraftigt beroende på hur risken realiserats. Om risken realiserats på ett sätt som negativt påverkar möjligheten att använda behovsanpassade lokaler, it-system, it-tjänster och elektroniska kommunikationer

kan skadan kortsiktigt bli stor för bolaget. För den enskilde journalisten inom bolaget kan en borttappad mobil riskera ett läckage av källuppgifter.

Långsiktigt bör försäkringar kunna dämpa konsekvenserna och möjliggöra en återgång till normalitet. Om risken inträffar på större koncerner och skadorna tar lång tid att reparera eller ersätta kan tjänste- eller produktleveransen minska vilket skulle kunna leda till ett minskat eller uteblivet medieflöde i vissa kanaler eller på vissa orter. I *Mediebranschen 2011 – Hot, risker och sårbarheter* bedömde mediebolagen i snitt att brand utgjorde den allvarligaste risken sett till konsekvensen (nära nio på en tiogradig skala) vilket är talande för allvarligheten av skada och förstörelse av egendom, såsom lokaler och kritisk utrustning, för en verksamhets funktionalitet.<sup>29</sup>

#### 4.4.4 Verksamhetskritisk information kommer att bli röjd

Den samlade bedömningen är att risken för att verksamhetskritisk information ska bli röjd inom mediebranschen är **låg**. Sannolikheten för att sådana incidenter ska ske bedöms som mycket låg, men skulle det ändå inträffa blir konsekvensen hög. Bedömningen av underlaget som ligger till grund för värderingen baseras på statistik från enkäten, intervjuer och underlag om framförallt incidenter och omedvetenheten om sårbarheter kring källskydd i digitala miljöer. Materialet som ligger till grund för bedömningen är varierat, men ger endast svaga indikationer till stöd för riskbedömningen. Konfidensen bedöms som **medelhög**.

I MSB:s enkät uppger två respondenter (4 procent) att de fått verksamhetskritisk information röjd genom en antagonistisk incident. En respondent (2 procent) uppger att information röjts genom en icke-antagonistisk incident. I intervjuer med representanter från mediebranschen framkommer det att arbete med det digitala källskyddet kan stärkas. Om arbetet med digitalt källskydd inte fungerar befaras det att viktiga källor, som visselblåsare, slutar höra av sig varpå viktig samhällsgranskning uteblir.

Riskens orsaker

Röjandet av kritisk information för organisationer inom branschen kan ha olika orsaker beroende på vilken information det rör sig om.

29. I mediebolagens bedömning är det möjligt att även skada mot personal legat till grund för värderingen av riskens konsekvens.



Angrepp och infiltration i syfte att exponera uppgiftslämnare kan vara en orsak, en annan att underminera granskningar eller avslöja affärshemligheter och kontakter.

Icke-antagonistiska orsaker till att verksamhetskritisk information röjs kan vara att information sparas på platser och utrymmen där fler än de som är behöriga att se informationen har tillträde. Bristande behörighetskontroll för skyddade utrymmen (såväl fysiskt som inom it-miljöer) kan också möjliggöra att utomstående kommer över information de inte ska ha. Oklara hanteringsregler för vad som får skickas över mejl och liknande kan också innebära att information hamnar där den inte ska vara. Verksamhetskritisk information kan också röjas medvetet (både genom medarbetare och exempelvis cyberattacker utifrån), på antagonistiska grunder eller för att en medarbetare vill avslöja vad vederbörande ser som missförhållanden. I de fall aktörer, såsom främmande makt, vill kartlägga beslutsfattare och väljer att samla in information genom intrång hos mediebolag kan sannolikheten för röjande av verksamhetskritisk information hos de större svenska mediebolagen sägas vara betydligt högre än den nuvarande totalbedömningen ”mycket låg”.

#### Sårbarheter och skydd

Mediebolagen har i MSB:s analys befunnits ha en hög grad av beroende av verksamhetsrelevant information och, det beroendet utgör en medelhög sårbarhet för mediebolagen. Källskyddet är centralt för villigheten hos enskilda individer att lämna känsliga uppgifter till medierna. Genom digitaliseringen har nya kommunikationsvägar uppstått, och en förväntan finns att även de nya sätten att meddela sig med andra ska kunna omfattas av ett effektivt källskydd. Men verksamhet i digitala miljöer lämnar många spår som kan användas för att identifiera uppgiftslämnare, och det medför i sin tur att källskyddet ofta är sårbart.

Sårbarheten ökar eftersom effektivisering ofta också innebär att mycket data samlas på ett och samma ställe, vilket gör att en angripare kan komma åt mycket mer på en och samma gång än förut. Samtidigt har delar av mediebranschens nyhetsproducenter låg kunskap om hur digitala fotavtryck kan minimeras och hur lämnade uppgifter kan skyddas.

Bland respondenterna i enkätundersökningen anger 41 procent att de inte vet hur fort de kan vidta åtgärder för att hantera en incident där verksamhetsrelevant information har blivit röjd. 41 procent anger att de kan agera inom två timmar, och endast 8 procent behöver mer än tolv timmar.

Konsekvenser om risken realiseras

För den enskilde uppgiftslämnaren kan röjandet av källorna till känsliga reportage eller liknande leda till att uppgiftslämnare drabbas av repressalier. Om källor eller känsliga uppgifter såsom anställdas personuppgifter eller affärshemligheter röjs hos ett bolag inom mediebranschen och det uppmärksammas brett så kan det allmänna förtroendet för bolaget minska och till följd av detta försämrad lönsamhet.

I och med implementerandet av den nya europeiska dataskyddsförordningen GDPR kan mediebolag som misslyckas med att hantera personuppgifter på ett säkert sätt också dra på sig stora kostnader i form av böter. Det ska tilläggas att det för bolag kan vara svårt att upptäcka dataintrång som leder till röjande av verksamhetskritisk information. På en samhällsnivå kan benägenheten att meddela medier om missförhållanden minska när människor upplever att de inte kommer att få ett adekvat skydd trots att de tar en risk. Detta drabbar journalistikens granskande roll negativt och kan få särskilt svåra konsekvenser för den samhällsviktiga verksamheten granskning. Det kan i sin tur medföra att allmänheten går miste om information om missförhållanden, exempelvis inom samhällsviktig verksamhet.

#### 4.4.5 Allmänhetens förtroende för organisationen kommer att minska

Den samlade bedömningen är att risken för att allmänhetens förtroende för organisationer i mediebranschen kommer att minska är **låg**. Sannolikheten för att sådana incidenter ska ske bedöms som låg, och skulle det inträffa blir konsekvensen medelhög. Underlaget som använts till bedömningen är varierat och innehåller statistik från enkäten och expertbedömningar. Konfidensen bedöms som **medelhög**.

För medieproducerande bolag kan medieinnehåll som uppfattas som falskt, missvisande eller vinklat leda till ett minskat förtroende, men underlåtenhet att rapportera eller på annat sätt förmedla information när det finns ett intresse från allmänheten och myndigheter att få information kan också ha den effekten eller konsekvensen. Bland mediedistributörer är förtroendet förmodligen främst kopplat till tillgänglighetsaspekter och driftsäkerhet. Om tillgången till utbudet som distributören erbjuder försvinner, eller om efterfrågade tjänster och informationsförmedling inte levereras så kan förtroendet minska.

Oron som uppstod i samband med att franska TV5 Monde kapades och började sända IS-propaganda illustrerar också hur kapningsförsök och liknande verksamhet kan tänkas ha effekten att allmänhetens förtroende minskar. Gemensamt för distribuerande respektive producerande mediebolag är förmodligen att om delar av allmänheten uppfattar att bolaget bedriver en agenda som bedöms göra det svårt att förhålla sig neutral, oberoende eller objektiv, eller om bolaget uppfattas ha kopplingar till organisationer eller rörelser som bedriver en sådan agenda, kan allmänhetens förtroende också minska.

I enkäten anger tre respondenter (6 procent) att organisationens förtroende hos allmänheten tagit skada genom en antagonistisk incident, fem respondenter (10 procent) uppger detsamma för en icke-antagonistisk incident. Det förefaller alltså vara relativt ovanligt med incidenter som leder till förtroendetapp hos allmänheten, åtminstone utifrån bolagens egna bedömningar. Det bör dock betonas att det är oklart om det minskade förtroendet som uppstår genom en sådan incident har någon längre varaktighet.

#### Riskens orsaker

Plötsliga negativa förändringar i allmänhetens förtroende för bolaget förefaller därför oftare orsakas av handhavandefel som kommer till allmänhetens kännedom, exempelvis i form av felpubliceringar. Däremot kan antagonistiska incidenter potentiellt medföra stor skada när de väl sker. Ett uppmärksammat exempel på detta är det förtal som en ledarskribent på Hudiksvalls tidning utsattes för, vilket ledde till fällande dom under 2017. Ledarskribenten ska ha pekats ut som pedofil vilket var en anklagelse som uppges varit ämnad att orsaka allvarlig skada för ledarskribenten.

Vid en internationell utblick finns även fall där exempelvis svartmålning skett till följd av granskning av säkerhets- och utrikespolitiskt känsliga ämnen. I ett ekonomiskt tuffare klimat kan granskning och verifiering av material före publicering bli lidande. Kravet på snabbhet i rapporteringen, skapad av konkurrens bland traditionella nyhetsmedier men också med sociala medier och ryktesspridningen som kan inträffa där, är ytterligare en felkälla. Samtidigt utgör det omfattande flödet av information i samhället en utmaning i sig att bevaka och kritisk granska för nyhetsrapporterande mediebolag. Utöver detta kan missinformation, desinformation och falska nyhetspubliceringar av andra mer eller mindre seriösa aktörer leda till egna felpubliceringar hos den egna redaktionen.

Sårbarheter och skydd

Mediebolagen har i MSB:s analys befunnits ha en mycket hög grad av beroende av allmänhetens förtroende, och det beroendet utgör en medelhög sårbarhet för mediebolagen.

49 procent av respondenterna i enkätundersökningen anger att de inte vet hur fort de kan vidta åtgärder för att hantera en incident där allmänhetens förtroende för bolaget har påverkats negativt. 29 procent anger att de kan agera inom två timmar, men 14 procent anger att vissa incidenter kan ta mer än 48 timmar.

Konsekvenser om risken realiserar

För den enskilde individen blir konsekvenserna begränsade om denna typ av incidenter inträffar hos enstaka mediebolag. Om det drabbar många bolag kan den enskilde individen få svårt att hitta källor till nyhetsförmedling som vederbörande litar på. I förlängningen kan det leda till en mindre välinformerad allmänhet och en ökad demokratisk sårbarhet. Konsekvensen för de mediebolag som bedriver samhällsviktig verksamhet eller granskande journalistik (och som lever på ett högt allmänt förtroende) kan bli snabbt sinande annonsintäkter.

För samhället kan konsekvensen bli att den journalistiska granskningen av makthavare minskar och får ett mer begränsat genomslag och hos vissa mediekonsumenter eventuellt ersätts av mindre noggranna granskningar i andra forum. På längre sikt kan ett försvagat förtroende för medier leda till att förutsättningarna för ett demokratiskt ansvarsutkrävande grundat på fakta urholkas. Ytterligare en konsekvens kan vara försvårade förutsättningar för att förmedla viktig samhällsinformation i kritiska situationer.

#### 4.4.6 Verksamhetskritisk information kommer att bli felaktigt ändrad

Den samlade bedömningen är att risken för att verksamhetskritisk information raderas är **låg**. Sannolikheten för att sådana incidenter ska ske bedöms som mycket låg, men skulle det ändå inträffa blir konsekvensen medelhög. Underlaget som ligger till grund för bedömningen är begränsat utöver MSB:s enkät. Konfidensen bedöms som **låg**.

På frågan om huruvida verksamhetskritisk information riskerar att ändras svarade två respondenter (4 procent) att de under den senaste 12 månaderna drabbats av minst en antagonistisk incident där verksamhetskritisk information blev ändrad. För icke-antagonistiska incidenter uppgav tre respondenter (6 procent) detsamma.

#### Riskens orsaker

Antagonistiska ändringar i verksamhetskritisk information som finns i it-system kan uppkomma genom skadlig kod, intrång och insiders. Verksamhetskritisk information som kan ändras genom skadlig kod kan till exempel vara konfigurationer för tid och takt, vilket kan leda till att synkronisering mellan system slutar att fungera. Ett exempel på intrång var när den Jönköpings-baserade nättidningen Jmini i september 2016 drabbades av ett dataintrång, varpå innehållet på tidningens hemsida först ändrades – och sedan försvann. Sådana angrepp kan initieras utifrån en vilja att svartmåla bolaget, men också för att oroa allmänheten eller sänka allmänhetens eller partners förtroende för detsamma.

Ytterligare ett exempel på ett verksamhetskritiskt angrepp var kapningen av TV5 Mondes sändning i april 2015. För medieproducenter kan även desinformation leda till att medieinnehåll blir felaktigt, eller missvisande, varpå deras produkter kan svartmålas. Verksamhetskritisk information kan även utgöras av kundregister, avtal, lönelistor och andra för bolaget viktiga informationsmängder. Denna typ av information kan ändras genom intrång eller insiderverksamhet, men också genom rena misstag.

Ett exempel på en icke-antagonistisk incident där verksamhetskritisk information blev ändrad inför sändning var när lokala tv- och radiostationer i New York i september 2016 meddelade att en evakuering av Long Island hade beordrats med anledning av stormen Hermine. Lokala myndigheter hade sökt stöd för att sprida information om att frivillig evakuering från en liten ö med ett fåtal boende utanför Long Island hade beordrats, men någonstans i processen fram till sändning hade delar av meddelandet fallit bort. I stället framstod det som att en evakuering (utan att nämna att den var frivillig) hade beordrats för Long Island, ett område med totalt cirka 3 miljoner invånare.

Sårbarheter och skydd

Mediebolagen har i MSB:s analys befunnits ha en hög grad av beroende av verksamhetsrelevant information och det beroendet utgör en medelhög sårbarhet för mediebolagen.

35 procent av respondenterna i enkätundersökningen anger att de inte vet hur fort de kan vidta åtgärder för att hantera en incident där verksamhetsrelevant information har blivit felaktigt ändrad. 43 procent anger att de kan agera inom två timmar, och endast 8 procent behöver mer än tolv timmar.

Konsekvenser om risken realiserar

För den enskilde individen blir konsekvenserna oftast begränsade (även om mer allvarliga konsekvenser också i förekommande fall kan inträffa – såsom i det ovan nämnda exemplet om stormen utanför Long Island), beroende på vilken typ av mediebolag det rör sig om, hur mycket och vilken typ av information som har blivit ändrad. För det drabbade bolaget kan konsekvenserna bli allt från felaktiga leveranser av tidningar och annat betalmaterial till felaktiga publiceringar. Det kan i sin tur leda till merarbete och minskat förtroende bland kunder och allmänhet.

På en samhällsnivå kan felaktigt ändrad verksamhetskritisk information, hos exempelvis större nyhetredaktioner, leda till att hanteringen av kriser blir betydligt mer resurskrävande när oro uppstår och människor tar beslut på felaktiga grunder. Fler exempel på detta inträffade i samband med att orkanen Sandy drev in över New York, samtidigt som ett oseriöst konto på Twitter började sprida falska uppgifter om de skador orkanen orsakade och hur krishanteringen fortgick. Kontots falska uppgifter spreds och kom att sändas ut i nationell tv, bland annat av tevekanalen CNN. Eftersom det fanns en reell risk för att människor på grund av de falska uppgifterna skulle fatta irrationella beslut tvingades de lokala myndigheterna använda värdefulla krishanteringsresurser för att bemöta de falska uppgifterna.

#### 4.4.7 Verksamhetskritisk information kommer att bli felaktigt raderad

Den samlade bedömningen är att risken för att verksamhetskritisk information raderas är **låg**. Sannolikheten för att sådana incidenter ska ske bedöms som mycket låg, men skulle det ändå inträffa blir konsekvensen medelhög. Underlaget som ligger till grund för bedömningen är begränsat utöver MSB:s enkät. Konfidensen bedöms som **låg**.

I MSB:s enkät svarade två respondenter (4 procent) att de under den senaste 12 månaderna drabbats av minst en antagonistisk incident där verksamhetskritisk information blev otillgänglig. För icke-antagonistiska incidenter uppgav två respondenter respondent (4 procent) det samma.

Riskens orsaker

Att data hos medieproducenter medvetet och olovligen raderas kan exempelvis ske dels för att skada bolaget, dels för att hindra bolaget från att sprida information som andra inte vill ska komma ut. Betydligt vanligare är nog att information raderas på icke-antagonistiska grunder. Ett uppmärksammat exempel på hur fel det kan gå inträffade i april 2016 när en ägare av ett webshotell<sup>30</sup> skulle genomföra uppdateringar av sin it-miljö. Ägaren använde sig av ett kommando som ignorerar eventuella varningar som systemet producerar och raderar allt på en angiven plats. Olyckligtvis hade vederbörande gjort ett misstag när instruktionerna om var i filsystemet kommandot skulle tillämpas skrevs. Det ledde till att allt, inklusive webshotellets säkerhetskopior, raderades. På ett ögonblick försvann merparten av firmans tillgångar, med mycket begränsade möjligheter att återskapa det som gått förlorat.

Sårbarheter och skydd

Mediebolagen har i MSB:s analys befunnits ha en hög grad av beroende av verksamhetsrelevant information och det beroendet utgör en medelhög sårbarhet för mediebolagen.

37 procent av respondenterna i enkätundersökningen anger att de inte vet hur fort de kan vidta åtgärder för att hantera en incident där verksamhetsrelevant information har blivit felaktigt raderad. 39 procent anger att de kan agera inom två timmar, och 10 procent behöver mer än tolv timmar.

30. En tjänst som möjliggör upprätthållandet av en egen offentlig webbserver att publicera sig på.

Konsekvenser om risken realiseras

För den enskilde individen blir konsekvenserna förmodligen i regel begränsade, beroende på vilken typ av mediebolag det rör sig om, hur mycket och vilken typ av information som har blivit raderad. Som konsument kommer effekterna förmodligen främst bestå i minskad tillgång till medialt innehåll antingen för att en producent påverkats eller för att en distributör upplevt störningar. För det drabbade bolaget kan konsekvenserna bli stora. Verksamhetskritisk information kan vara allt från kundregister till kontrakt, lönelistor och arbetsmaterial. Bolaget leverans av tjänster och/eller produkter kan därför i värsta fall störas kraftigt.

På en samhällsnivå kan raderandet av verksamhetskritisk information i ett mediebolag leda till att viktiga nyheter eller annan viktig information inte når ut. På en övergripande nivå kan det konstateras att det med dagens teknik och relativt billiga lagringslösningar finns en generellt hög tröskel av skydd mot radering av information genom olika lösningar för säkerhetskopiering. Detta kan i sin tur mildra konsekvenserna av raderandet av verksamhetskritisk information, även om tiden som krävs för återskapandet av den förlorade informationen i sig kan vara kritisk.

## 4.5 Samhällsrisker och sårbarheter

Nedan presenteras fem samhällsrisker och tillhörande aspekter. Varje rubrik ska läsas som Risken att [namnet på risken]. Riskerna presenteras utifrån bedömningen högst till lägst riskgrad.

### 4.5.1 Påverkanskampanjer bedrivs mot allmänheten och beslutsfattare genom medier

Den samlade bedömningen är att risken för utvecklingen av påverkan mot allmänheten och beslutsfattare genom medier är **hög**. Sannolikheten för denna riskutveckling är hög, och konsekvensen av den bedöms som hög. Underlaget för denna riskbedömning utgörs av statistik, expertbedömningar av enskilda händelser och trender samt en bedömning av regeringen. Konfidensen bedöms som **hög**.



Allmänhetens och/eller beslutfattares världsbild och/ eller beslutsfattande manipuleras via medier i en riktning som stämmer överens med antagonistiska aktörers intressen.

#### Riskens orsaker

Kampanjer för påverkan har intensifierats och ökat i antal på senare år. Digitaliseringen och det förändrade säkerhetspolitiska läget har skapat incitament för påverkansförsöken. I det nya medielandskapet har falska nyheter och liknande desinformation lättare kunnat spridas. Filterbubblor och ekokammare inom sociala medier och internetfora samt alternativa medier har ytterligare öppnat upp för framgångsrik påverkan i det svenska samhället. Trycket på att snabbt rapportera de senaste nyheterna har genom teknik som möjliggör omfattande rapportering i realtid inneburit att mediebolagen i brist på lika snabba tekniker för källkritik nu är mer sårbara för planterade falska nyheter. Det uppdrivna tempot kan därför leda till felrapportering.

Antagonister utnyttjar de nyhetsproducerande mediebolagens vilja att rapportera om sådant som ligger i allmänhetens intresse och skapar falska nyheter, vinklar befintliga nyheter på ett missvisande sätt och förstärker sensationella inslag för att skapa ilska, oro och missstro. Ett uppmärksammat exempel på detta var när det i januari 2016 rapporterades om att en 13-årig flicka, med ryska rötter, i Tyskland skulle ha blivit kidnappad och våldtagen av migranter. Historien var uppdiktad, men fångades ändå upp av ryska medier och höga företrädare för den ryska staten kritiserade tyska myndigheter för deras hantering av fallet. När fallet började tas upp på diplomatisk nivå blev det en världsnvyhet och vid det laget var reaktionerna på sociala medier och i andra sammanhang mycket upprörda. Först i efterhand kunde det klargöras att hela historien var påhittad, men vid det laget hade den redan hunnit orsaka stor skada.

#### Sårbarheter och skydd

Mediebranschen och samhället är beroende av den verksamhet och funktion som nyhetsmedier utgör i form av kritisk granskning av information. Kompetens och tid är resurser som krävs hos redaktionerna ute i landet för att tolka, verifiera och validera nyheter före publicering. Ytterligare en beroendedimension i sammanhanget är mängden verksamheter med kapacitet att bedriva denna kvalitativa granskning – både för nyansering, meningsutbyte och förmågan att skydda sig mot försök till planterande och spridande av falska nyheter.

Den allt vanligare flerkanalpubliceringen där samma medieinnehåll, exempelvis nyheter, publiceras i flera kanaler från ett och samma mediehus är en sårbarhet för samhället. Om planterad desinformation skulle snappas upp och passera de redaktionella interna kontrollfunktionerna på mediehuset riskerar distributionen av denna information att gå ut genom fler kanaler till fler konsumenter. En annan sårbarhet är den minskade redaktörsrollen som enligt Pressombudsmannen (PO) skurits ned eller försvunnit på många håll. I valtider ökar det demokratiska samhällets sårbarhet för påverkanskampanjer och spridning av desinformation, vilket inte minst kontroverserna kring den ryska inblandningen i det amerikanska presidentvalet är ett tydligt exempel på.

Mediebolagens skydd mot påverkan i form av desinformation utgörs av den traditionella redaktörsrollen samt det journalistiska hantverket att verifiera underlaget till nyhetspubliceringar. Den stora mängden lättillgänglig information som digitaliseringen medfört utgör i sig ett skydd, eller möjlighet, i sammanhanget då verifiering och faktakoll genom sökande på publicerade källor eller kontaktuppgifter till relevanta experter förenklats. Ytterligare skydd mot påverkan är initiativ som gratistidningen Metros "Viralgranskaren". Detta initiativ har löpande bemött virala falska nyheter<sup>31</sup>. Medvetande-höjande insatser, som Källkritikens dag, om värdet av källkritik vid läsandet och delande av nyheter i sociala medier har också genomförts. Det har också lanserats en applikation till webbläsare som varnar när användaren besöker en sida, eller när en artikel dyker upp i Facebook-flödet från en webbsida, som hamnat på Viralgranskarens varningslista. Användaren får vid besök på sådana sidor via varningsapplikationen relevant information om sidan.

Slutligen ska MSB:s arbete med psykologiskt försvar nämnas. Myndigheten står bland annat för samordning av information till allmänheten vid kriser via Krisinformation.se och analysverksamhet vid särskilda händelser – så kallad påverkansanalys vilket syftar till att öka kunskapen om försök att påverka svenska myndigheter eller opinion vid i första hand säkerhetspolitiska kriser. MSB bedriver i nuläget "18-årsuppdraget" tillsammans med Försvarsmakten och Rekryteringsmyndigheten, där det ingår delar som syftar till att höja medvetenheten om vikten av källkritik. Myndigheten tillhandahåller också ett test där ungdomar kan träna sin källkritiska förmåga. MSB samverkar också med Statens medieråd kring pedagogiskt material om källkritik.

---

31. Med viral information avses här information som på kort tid och snabbt sprids mellan många människor över en eller flera plattformar (såsom sociala medier).

Konsekvenser om risken realiseras

Konsekvensen för den enskilde medborgaren är en ökad exponering för falska nyheter och ökad osäkerhet kring medieflödets trovärdighet. Det kan leda till känsloreaktioner som ilska och oro, men också till att den enskilde individen inhämtar felaktiga uppfattningar, att medborgarnas i högre grad utsätts för falska påståenden och att de får allt svårare att avgöra vad som är falsk information. I och med detta finns en risk att tilltron till påståenden, uttalanden och information generellt minskar och på så sätt också förtroendet mellan människor och mellan medborgare och samhällsinstitutionerna. Påståenden som börjar spridas och diskuteras hos allmänheten över tid kan vara svåra att åtgärda med en vanlig dementi från exempelvis en myndighet eftersom exempelvis rättningar som publiceras i efterhand i regel inte får samma genomslag som den ursprungliga uppgiften.

Om bolag inom mediebranschen används för påverkansoperationer och det framkommer i allmänna sammanhang kan allmänhetens förtroende för bolaget ta skada. Om bolaget är profilerat som en seriös, oberoende aktör kan partners och sponsorer avbryta samarbeten och kontrakt. På samhällsnivå fattas beslut i större utsträckning på felaktiga eller falska grunder, oro sprids, polarisering uppstår, tillit till institutioner minskar. Det leder i sin tur till att samhällets handlingskraft och förmåga att agera samlat minskar, samt att möjligheten att skydda sig mot yttre påfrestningar kan bli lägre.

#### 4.5.2 Sveriges informationsinfrastrukturer är otillräckligt skyddade mot angrepp

Den samlade bedömningen av att risken för att Sveriges informationsinfrastrukturer är otillräckligt skyddade mot angrepp är **hög**. Sannolikheten för att risken ska realiserars bedöms som hög, och skulle den inträffa blir konsekvensen hög. Underlaget som ligger till grund för bedömningen av denna risk utgörs främst av expertbedömningar. Underlaget är därför begränsat i sin variation men bedömningarna är samstämmiga varför konfidensen bedöms som **medelhög**.

Under 2016 har tre incidenter skett med direkt påverkan på mediedistributionen i Sverige. Den första incidenten var DDoS-angreppen mot flera mediebolag den 19 och 24 mars 2016 som ledde till att flera tidningar, TV4 och några andra bolag inte gick att nå. Den andra incidenten var sabotage av Dalsjöförs masten i Häglared den

15 maj samma år som medförde att utsändningen av flera radio-kanaler upphörde och cirka 190 000 personer drabbades. Den tredje var DDoS-attacken mot en katalogtjänst (DNS) som bolaget Dyn tillhandahåller den 21 oktober. Den ledde till att alla webbsidor och tjänster som hade registrerat sig hos Dyn, för att kunna hittas på nätet, (och enbart hos Dyn) inte längre gick att nå.

Incidenterna visar att det finns många sätt att störa distributionen av medier. Enligt statistik om förekomsten av betydande nätsäkerhetshändelser i elektronisk kommunikation från PTS skedde det mellan 2012 och 2016 sju incidenter där nationella störningar och avbrott orsakades av överbelastningsattacker. De störningar och avbrott som orsakades av tillgänglighetsattacker ska vanligtvis ha pågått mellan en och två timmar. I ett av fallen ska störningarna och avbrotten pågått i över tio timmar.

#### Riskens orsaker

Orsakerna till sådana angrepp är ofta svåra att avgöra då det först och främst ofta är svårt att hänföra angreppet till någon särskild aktör, och att det därutöver kan vara svårt att avgöra varför en given aktör genomförde angreppet även om det går att attribuera det. Eftersom det numera går att köpa ett DDoS-angrepp mot ett utpekad mål för ganska små summor ökar mängden aktörer som kan stå bakom ett sådant angrepp, och därmed också de möjliga motiven till varför det utförs. Möjliga exempel på motivbilder kan vara allt från makt-demonstrationer och att hämnas till att bevisa att det går, att testa hur kraftfullt DDoS-vapnet är, att försöka begränsa tillgången till information och att orsaka skada. Nyhetsproducerande medier har specifikt utsatts för DDoS-attacker för att tystas i sin rapportering.

Även om de uppräknade incidenternas efterspel har inneburit att många bolag har börjat satsa mer på säkerhet bedöms sårbarheten mot sabotage och cyberattacker även fortsättningsvis som hög. Problemet förvärras av att innehållet som ska förmedlas i dag måste passera genom betydligt fler infrastrukturer än förut, och att alla infrastrukturer (i varierande mån) är exponerade mot internet och därför kan utsättas för cyberattacker. Bolag som försöker höja säkerheten har svårt att lyckas eftersom det är svårt att ställa krav på hela kedjan som innehållet passerar igenom. Angreppet mot Dyn innebar rekordhög belastning på bolagets servrar. Angreppet genomfördes med hjälp av ett eller flera botnät, alltså internetanslutna enheter som kapas för att skicka trafik mot ett mål (vilket i sin tur

överbelastar mottagaren av trafiken).<sup>32</sup> Att allt fler enheter internetansluts, samtidigt som de ges svaga eller obefintliga skydd mot kapningsförsök som kan genomföras mot många enheter samtidigt, kommer leda till att belastningen i attackerna framöver kommer att bli värre. Enligt vissa bedömare är det enda riktigt kapabla försvaret mot sådana angrepp att ha en mycket hög redundans i alla de system och tjänster som är nödvändiga för att bedriva verksamheten – och det är dyrt. Därutöver gör konkurrenssituationen att det är svårt att dela information om sårbarheter och skydd så att bolagen kan ta lärdom av varandra.

#### Sårbarheter och skydd

En sårbarhetsfaktor i detta sammanhang är den ökade grad av beroende av internetbaserad distribution av medier, såsom tv radio och nyheter, vilket vid en större störning på internetinfrastrukturen skulle kunna få långtgående effekter på mediernas tillgänglighet om något händer med denna infrastruktur. Ytterligare en sårbarhet som har koppling till denna risk är centraliseringen av bland annat it-drift som skett inom mediebolagen de senaste åren. Vid en riktad attack mot en eller flera verksamheters centraliserade it-drift kan effekterna väntas bli värre om attacken lyckas.

För den fysiska infrastrukturen såsom master och andra sändningsanläggningar finns skydd genom statusen av skyddsobjekt där tillträde begränsas genom skalskydd och beivran av överträdelse med stöd av säkerhetsskyddslagen. För nätutrustning finns möjlighet till redundans genom införskaffandet av en extra ISP med egen kabel in samt överbelastningsskydd för den egna nätverksutrustningen.

MSB:s arbete med förebyggande arbete mot IT-incidenter samt informationsspridning och samverkan vid incidenter via funktionen CERT-SE är ytterligare en del av det existerande skyddet gentemot cyberattacker mot den svenska informationsinfrastrukturen. Därutöver sker också erfarenhetsutbyte genom privat-offentlig samverkan inom Mediernas beredskapsråd och det nybildade FIDI-Drift. MSB stödjer även robusthetshöjande åtgärder inom ramen för myndighetens arbete med etermedieberedskap. PTS bedriver förebyggande arbete med krisberedskap samt informationsspridning och samverkan inom ramen för Nationella telesamverkansgruppen (NTSG) vid allvarliga händelser inom elektronisk kommunikation. Detta bidrar till en ökad hanteringsförmåga av incidenter inom elektroniska kommunikationer.

---

32. Botnät ska inte förväxlas med botar. Botar avser mjukvara som på automatisk väg utför enklare uppgifter.

Konsekvenser om risken realiseras

Konsekvenserna av att informationsinfrastruktur slås ut blir att information inte kan förmedlas i stor skala. För enskilda kan det innebära att eftersökt information inte kan nås. För bolag kan det innebära stora kostnader för att reparera skador, investera i ökad säkerhet och återupprätta skadat förtroende. För samhället leder sådana angrepp till det exempelvis kan bli svårt att i stor skala sprida viktig samhällsinformation i samband med en kris. Men det kan också innebära att oro sprids bland allmänheten då en viktig del i många tillvaro plötsligt försvinner sett till trygghet. Infrastrukturen som signalerna passerar igenom är också delvis samma infrastruktur som vanliga internetanvändare använder, varför storskaliga attacker kan leda till att delar av allmänheten får en nedsatt förmåga att informera sig själva, och att meddela sig med omvärlden.

#### 4.5.3 Mediekonsumtionen ger inte redundans till krisberedskapen

Den samlade bedömningen är att risken för att informationsinfrastrukturen inte ger redundans till krisberedskapen är **hög**. Sannolikheten för att en sådan utveckling pågår bedöms som medelhög, och skulle det inträffa blir konsekvensen hög. Underlaget till stöd för analysen är begränsat i sin variation, men ger gedigna kvantitativa data och präglas av en tydlig samstämmighet. Konfidensen bedöms som **hög**.

Effektiv informationsförmedling under en kris i dagsläget förutsätter att både nätbaserade tjänster (som webbtidningar och sociala medier) och traditionell mediedistribution (främst via radio) fungerar, detta för att möta kravbilderna i den framväxande mediekonsumtionen. Ett ekosystem av informationsinfrastrukturer som skulle kunna innebära en tydlig redundans medför på grund av användarmönstren i stället en ökad belastning där flera parallella system behöver fungera för att uppnå samma effekt som tidigare.<sup>33</sup> Givet den nuvarande utvecklingen kommer äldre informationsinfrastrukturer att generera allt mindre nytta utifrån ett krisberedskapsperspektiv då internet som källa till information blir alltmer dominant. Medborgare med kognitiva nedsättningar eller låga kunskaper om hur mobila enheter och datorer kan användas blir därmed särskilda riskgrupper i samband med en kris.

33. Om de som idag konsumerar medier främst över ett medium skulle bredda sin mediekonsumtion till flera mediekanalet så skulle kriskommunicerande organisationer ha en redundans i sin informationsförmedling.

### Riskens orsaker

Risken orsakas av de splittrade mediekonsumtionsvanorna mellan i synnerhet olika åldersgrupper, där de äldre fortfarande i stor utsträckning förlitar sig på traditionell medieförmedling medan unga i allt större grad nästan enbart konsumerar medier genom nätbaserade tjänster som webbsidor och sociala medier.

### Sårbarheter och skydd

En tydlig sårbarhet i kriskommunikatörers förmåga är att kravet på informationsförmedling över flera medier ställer stora krav på samordning. När den misslyckas och olika information sprids i olika kanaler, samtidigt som mistaget inte omedelbart upptäcks, kan det ta lång tid för mediekonsumenter som inriktar sin konsumtion på nästan uteslutande ett medium att upptäcka att olika budskap finns, och att de bör vara extra kritiska. Svenskar har i allmänhet en hög grad av tilltro till nyhetsmedier och myndigheter, varför det är troligt att felaktiga budskap som inte ser uppenbart orimliga ut kommer att bli betrodda.

Men den höga utbildningsgraden hos befolkningen kan göra att felaktigheter som florerar i medieflödet snabbare upptäcks och uppmärksammas vilket är en form av skydd. En i sammanhanget positiv sida med svenskars mediekonsumtion är att många verkar utöka den uppsättning informationskanaler och medier som de vänder sig till under en kris.

MSB tillhandahåller i dagsläget en applikation för krisinformation och utvecklar därutöver ytterligare en applikation som kommer att sammanföra information från ett antal flöden som är relevanta för den enskildes beredskap. Den nya applikationen kommer också att kunna konfigureras så att den levererar lokal information som är av särskild vikt utifrån den enskildes förutsättningar och situation.

MSB är också aktiva på sociala medier, och använder exempelvis sin sida på Facebook för att sprida information och samla uppgifter om VMA-systemets genomslagskraft. De befintliga lösningarna för kriskommunikation kommer dock främst till nytta om den enskilde själv skaffar någon sådan applikation eller väljer att följa MSB:s eller andra kriskommunicerande organisationers sidor på sociala medier.

Inom den privata sektorn finns ytterligare lösningar som kan ha en positiv verkan vid ett krisläge. Ett exempel är Facebooks funktion Säkerhetskoll vilken låter användare av tjänsten inom ett visst geografiskt område (katastrofområde) ”checka in” sig som säkra efter en större incident eller kris. Funktionen kräver enbart att användaren har en fungerande internetanslutning och ett Facebook-konto. Med

hjälp av geografiska data som automatiskt skickas till Facebook från användarens enheter kan företagets algoritmer exempelvis avgöra om användaren befinner sig i ett katastrofområde. När funktionen används meddelar den att användaren befinner sig i säkerhet till alla i användarens Facebook-vänkrets. Google har också en kriskommunikationstjänst, kallad Viktiga meddelanden (engelskans Public Alerts), som i realtid skickar uppdateringar med relevant information till användarens internetanslutna enheter. Googles tjänst saknar i nuläget interaktiva inslag i stil med de som Facebooks funktion har. Internet- och sociala mediebaserade lösningar når inte alla, de är bara en av flera kanaler för kriskommunikation. Viktigt i sammanhanget är dock att internetanvändningen i dag ligger på 93 procent av befolkningen äldre än tolv år 2016 och sociala medier används av 77 procent av den internetanvändande befolkningen äldre än tolv år 2016.

Andra skyddsåtgärder är insatser för medvetandehöjning om vilka mediekanaler som finns, hur de i dag används för att förmedla exempelvis VMA och myndighetsmeddelanden samt vad den enskilde individen behöver göra för att kunna använda och tillgängliggöra sig information från alla existerande informationsmedier. Mer om detta i underavsnitt 6.2.2 Satsa på medvetandehöjande insatser om olika kriskommunikationskanaler vid kris nedan.

Konsekvenser om risken realiserar

Flera konsekvenser av utvecklingen bör uppmärksammas. Under kriser som har en direkt påverkan på informationsinfrastrukturen kan medborgare sakna förmågan att tillgodogöra sig nödvändig samhällsinformation. Bolagen (med undantag för public service) förhåller sig till utvecklingen genom att nedmontera äldre infrastruktur och ställa om sina affärsmodeller och investeringar mot ny teknik.

För samhället kan konsekvenserna innebära att högre krav ställs på att krishanterande organ säkerställer att samordnad, korrekt och relevant kommunikation sprids i alla de medietyper som används. Det ställs också högre krav på att krishanterande organ har en beredskap för att hantera avbrott i de nya informationsdistributionsystemen. Samtidigt kan avbrott i ett givet medium medföra att i synnerhet de yngsta och de äldsta åldersgrupperna ändå inte mottar informationen eftersom de kanske tillgodogör sig information enbart från en sorts medium. De ökade kraven är resurskrävande och avbrottsrisken för det medium respektive åldersgrupp föredrar kan i sin tur innebära att den totala krishanteringsförmågan belastas på ett sådant sätt att den är lägre än vad den kunnat vara.



#### 4.5.4 Samhället har en otillräcklig beredskap för att hantera storskaliga och plötsliga kontroverser

Den samlade bedömningen är att risken för att stora kontroverser kopplade till medier kommer att drabba Sverige är hög. Sannolikheten för att sådana incidenter ska ske bedöms som **hög**, och skulle det inträffa blir konsekvensen medelhög. Underlaget som ligger till bedömning för risken baseras på iakttagelser av ett flertal internationella incidenter. Få exempel finns på sådana incidenter i en svensk kontext men det finns ingen anledning att tro att Sverige inte skulle kunna drabbas av samma incidenttyp – ett flertal kontroverser har förekommit här där medierapporteringen haft en central roll. Konfidensen bedöms som **medelhög**.

Med *kontrovers* avses här när information som av många kan uppfattas som upprörande eller stötande fort sprids till många människor och leder till kraftiga reaktioner som i sin tur kräver att myndigheter och/eller andra samhällsinstitutioner agerar. Det är alltså inte ämnet i sig som är problemet, utan reaktionerna. Kontroverser kan uppstå på många sätt. De kan orsakas av spridning av såväl sann som av falsk information, och genom såväl påverkanskampanjer som av fullt legitima skäl som exempelvis samhällsgranskande journalistik. Samhällelig debatt om svåra frågor är således inte i sig ett problem – överreaktioner, antagonistiska handlingar och oro kan däremot vara det. Kontroverser måste inte uppstå genom medierna, men de kan förstärkas genom medierapportering.

Globaliseringen av medielandskapet är centralt för att förstå moderna kriser. Men kontroverser kan också uppstå i, och utvecklas genom, medielandskapet. Jyllands-Postens publicering av Muhammebilderna 2005 och motreaktionerna som uppstod, främst i Mellanöstern och Nordafrika, genom krav på bojkott av danska varor krävde en omfattande diplomatisk insats. Snowden-läckan om de amerikanska underrättelsetjänsternas omfattande övervakningsprogram 2013 och det politiska efterspelet påverkar fortfarande USA. Den falska rapporteringen om en våldtäkt av en tysk flicka med ryska rötter som skulle utförts av flyktingar i Tyskland i början av 2016 kom att användas av Ryssland i syfte att påverka den tyska opinionen och så split i det tyska samhället.

I Sverige aktualiserades betydelsen av källkritik för medier vid kontroverser i och med upploppen i Husby 2013. Rapporteringen om denna kontrovers kom att spridas utomlands. Frågor som uppstod om upploppen blev enligt journalister snabbt polariserade, varför det blev viktigt att få in alla inblandade aktörers perspektiv i rapporteringen.

#### Riskens orsaker

Med ytterst korta tidsintervall kan nyheter och andra publiceringar snabbt lyftas från det lokala planet till det nationella och ibland internationella planet där kontroversen kan få allvarliga konsekvenser för det lokalområde och land där medierapporteringen började.

Det finns exempel på sådana kontroverser som grundats på såväl antagonistiska som icke-antagonistiska incidenter. Kategorisering av vad som är grundat i antagonism och inte kan vara svår att göra. Det som först kan ha varit ett icke-antagonistiskt reportage kan plockas upp av en annan part som i sin tur förvränger eller vinklar nyheten för andra/egna syften.

Orsakerna till denna risk kan spåras till den teknologiska utvecklingen och digitaliseringen av information och informationsflöden samt till globaliseringen generellt. En förstärkande problematik utgörs av logiken för nyhetsmediers rapportering vid bland annat kriser av kontroversiell karaktär. Nyhetsmedier skapar förtroende genom att rapportera snabbt om händelseutvecklingen vid en samhällshändelse vilket gör att de har relativt lite att förlora vid en kris så länge jämna steg kan hållas med konkurrenternas rapportering. Publiceringsbeslut om huruvida det är läge att lägga ut information om en given incident påverkas också av huruvida information om incidenten redan cirkulerar. När så är fallet sänks tröskeln för vad som anses vara tillräckligt underbyggt för att publicera, bland annat för att det finns en uppfattning om att snabb rapportering kan lindra konsekvenser av att felaktig information sprids.

Mediebolagen menar också att myndigheterna ibland förvärrar situationen genom att hänvisa till en kommande presskonferens, samtidigt som ryktesspridning redan pågår på sociala medier och i andra sammanhang. Myndigheter kan å andra sidan ha uppfattningen att mediers närvaro i samband med en kontrovers ibland kan leda till att den eskalerar, varför de försöker kontrollera informationsflödet genom att hänvisa till presskonferenser och begränsa tillgången till de som är direkt operativt involverade i hanteringen.

På grund av att det kan gå så fort för en nyhet att bli viral och spridas mellan länder kan dess innebörd lyftas från en kontext till en annan på ibland oförutsedda sätt. Desinformation och vilseledning kan

förvrida nyheten och spä på kontroversen. Yttrande- och tryckfrihetens gränser har debatterats när publiceringar blivit föremål för internationella kontroverser och olika syn på vad som ska få skrivas eller illustreras tydliggjorts mellan olika delar av världen.

Sårbarheter och skydd

För att en aktör – exempelvis en nyhetsredaktion eller en stat som representerar ett land – ska kunna hantera en eskalerande kontrovers krävs både förmåga att ta in information för att skapa en lägesbild och förmågan att nå ut med information, exempelvis nya fakta, förtydligande av ståndpunkt eller dementi. Detta skapar ett beroende av tillgång till relevanta mediekanaler (de kanaler där de som berörs av kontroversen kan nås och själva verkar) där nyheter och debatt om kontroversen sker, samtidigt som kanaler med stor räckvidd för det egna budskapet krävs.

Sårbarheten i sammanhanget är det splittrade och globala medielandskap som uppstått. Egna åtgärder för att bemöta och nå ut med egen information under en kontrovers riskerar att drunkna i den stora mängd åsikter och information som flödar både under och efter en pågående storskalig kontrovers. Kontroverser kan också spås på av användandet av braskande nyhetsrubriker (vilka används för att öka säljupplagan) när dessa orsakar kraftiga reaktioner hos mediekonsumenterna.

Skyddet mot storskaliga kontroverser för det svenska samhällets del är i stor utsträckning samma skydd som finns mot risken för att påverkanskampanjer bedrivs mot allmänheten och beslutsfattare genom medier. Etablerade och betrodda mediekanaler, medvetandehöjande insatser om källkritik samt resurser för att verifiera och validera information är skydd som redan finns mot denna risk. De psykologiska försvarsförmågorna kan användas för att minska risken att påverkan bedrivs mot allmänhet och beslutsfattare genom medier.

Kanaler med samordnad och välgrundad information riktad till allmänheten är ett skydd – exempelvis MSB:s webbsida [Krisinformation.se](http://Krisinformation.se). MSB bistår även med informationssamordning samt arbete med att utveckla och vidmakthålla informatörsnätverk för samordnad kriskommunikation. MSB bedriver i nuläget ”18-årsuppdraget” tillsammans med Försvarsmakten och Rekryteringsmyndigheten, där det ingår delar som syftar till att höja medvetenheten om vikten av källkritik. MSB tillhandahåller också ett test där ungdomar kan träna sin källkritiska förmåga. Ytterligare ett skydd består av det höga förtroende som allmänheten har för nyhetsmedierna och svenska myndigheter. Det möjliggör ett stort genomslag för myndigheternas bedömningar och för nyhetsmediers förmedling av information, även efter att en kontrovers har briserat.

Konsekvenser om risken realiseras

Konsekvenserna för enskilda som hamnar mitt i rapporteringen kan vara omedelbart globalt kändisskap och en stor utsatthet. För enskilda som inte är mitt i rapporteringen kan konsekvensen exempelvis bli oro. För bolag som blir en del av kontroversen kan konsekvenserna bli att resurser måste läggas på att stärka säkerheten, att öka och bredda kommunikationen samt att den normala verksamheten avstannar eller måste styras om. I förlängningen har konsekvenserna av incidenter som blivit internationella kontroverser blivit alltifrån våldsdåd och mordhot till trakasserier mot redaktioner. På en samhällsnivå har konsekvenserna varit en bojkott mot ett helt land, resurskrävande insatser av polisiära myndigheter, protester mot ambassader, försämrade diplomatiska relationer, påverkanskampanjer mot hemmaopinionen och kraftigt vinklande av inhemska förhållanden i annat lands nyhetsrapportering med vitt spridda missuppfattningar som följd.

Om kontroversen rör inrikespolitiska frågor såsom flyktingmottagande eller kravaller i förorten kan överdrifter i medierapporteringen ytterligare spä på konflikt, våld och oro. En pågående kontrovers kan också utnyttjas för att spä på osämja i samhället av en antagonist, som en del i en påverkanskampanj. Ytterligare en problematik i sammanhanget är att de omfattande kontroverserna som kan uppstå till följd av en publicering riskerar att leda till själv-censur för att slippa negativa konsekvenser för exempelvis den egna organisationen.

#### 4.5.5 Vissa områden och samhällsgrupper hamnar i medieskugga

Områden och grupper i samhället riskerar att hamna i medieskugga. Den samlade bedömningen är att risken för detta är **låg**. Sannolikheten för att denna utveckling ska ske bedöms som låg, och skulle det inträffa blir konsekvensen medelhög. Underlaget till stöd för analysen är varierat. Statistiken för minskande redaktionell personal och journalister inom dagspressen indikerar att den mediala täckningen på lokal nivå minskar och problemet med att en ökad del av befolkningen inte känner igen sig i den mediala rapporteringen har uppmärksammats i flera sammanhang. Konfidensen bedöm som **låg**.

Individer i vissa områden såsom glesbyggd och i resurssvaga områden, samt i vissa språkgrupper och ideologiska grupperingar, lämnas, eller ställer sig utanför den etablerade, rikstäckande, mediebevakningen. Dessa individer blir inte, eller uppfattar sig inte bli representerade på ett tillräckligt eller korrekt sätt i etablerade medier med större täckning vilket gör att dessa medier inte längre uppfattas som relevanta.

#### Riskens orsaker

Lokalmedier, eller (nyhets)medier inriktade på mindre läsargrupper, får låg ekonomisk avkastning av att täcka områden där det antingen bor få människor, eller där få har råd/är villiga att betala för sådana tidningar och andra nyhetstjänster. Kommersiella nationella nyhetsmedier får huvuddelen av sina annonsinkomster genom att fokusera på nyhetsförmedling som intresserar en stor publik, vilket tenderar att medföra ett fokus på händelser på riksplenet eller i storstäderna.

#### Sårbarheter och skydd

Det demokratiska samhället behöver genom medier kunna nå ut, kommunicera och ta in information – i form av exempelvis perspektiv och åsikter – från alla delar av samhället. Därför finns ett beroende av förtroende och intresse från alla grupper i samhället till väletablerade och fungerande mediekanaler. Detta förtroende och intresse – i form av tillgänglighet, igenkänning och tillit – behöver gå hand i hand med en viss köpkraft. Denna uppfattade eller reella brist på köpkraft och/eller förtroende och intresse är en sårbarhet i sammanhanget eftersom val om vad som ska granskas och rapporteras om kommer vägas mot detta hos de kommersiella aktörerna.

Det skydd mot medieskugga som finns i dag består främst av tillgänglighetshöjande insatser inom redan etablerade medier. Exempel på detta är lokaltidningen Norrans implementerade av en Google-funktion i sin webbupplaga vilken möjliggör ett översatt nyhetsutbud på 91 olika språk. Här ska även nämnas public services uppdrag att sända program riktade till olika målgrupper, från olika geografiska platser i Sverige, samt att ha sändningar på minoritetsspråk och teckenspråk.

Konsekvenser om risken realiseras

Utvecklingen riskerar att skapa ett upplevt och/eller reellt utanförskap för den enskilde medborgaren som därmed inte får sin verklighet, eller intressen, bevakade. Det skulle också kunna leda till att kunskapsnivån i samhället sänks när vissa inte får lika stora kunskaper om dagsaktuella händelser som de annars skulle ha fått, i synnerhet bland samhällsgrupper som har svårt att tillgodogöra sig nyheter och information via exempelvis internet. Även det som tidigare talats om som den samlade gemensamma föreställningen om nationen, vilken upprätthölls och understöddes av nyhetsmedierna, splittras. För mediebolagen, främst de traditionella, blir konsekvensen ett minskat förtroende och/eller ökat ogillande från vissa grupper i samhället som upplever sig osynliggjorda eller felaktigt porträtterade.

På en samhällsnivå kan konsekvensen av att rapportering inte sker från vissa områden och platser bli att fördomar sprids och inte utmanas. I förlängningen kan bristen på en nyanserad rapportering om vissa områden och samhällsgrupper bidra till en ökad segregering. Om inte medier med lokal täckning, eller täckning inom exempelvis en minoritetsgrupp, finns i vissa områden eller bland vissa grupper kan det bli svårare att nå ut med relevant samhällsinformation, krisinformation och viktiga meddelanden samt nyheter i de områdena och grupperna. Det leder i sin tur till en lägre medvetenhet om samhället i stort hos medborgarna i dessa kategorier. De traditionella medierna kan inte heller förväntas fungera lika bra som en kommunikationsväg för viktig information vid exempelvis samhällskriser hos dessa grupper.

## 4.6 Syntes

I detta avsnitt redogörs för hur ett urval av de ovan redovisade riskerna kan komma att samverka. Varje analys innehåller en redogörelse för huruvida den första risken förvärrar den andra och huruvida den andra risken förvärrar den första. Med det menas att den första risken antingen gör att den andra risken har en högre sannolikhet att inträffa, eller att den andra riskens oönskade händelse blir än värre om den skulle inträffa. Varje analys behandlar också huruvida någon syntesrisk<sup>34</sup> uppstår ur en kombination av de två riskerna. Endast de risker som har bedömts ha en stark samverkande effekt redovisas.

---

34. En risk som uppstår genom samverkan mellan minst två andra risker.

#### 4.6.1 Påverkan och samhällets krisberedskap

Risken för att samhället har en otillräcklig beredskap för att hantera storskaliga och plötsliga kontroverser kan förvärra risken för att påverkanskampanjer bedrivs mot allmänheten och beslutsfattare genom medier. En otillräcklig beredskap kan innebära att genomslaget och skadan blir desto större, varför investeringen som en sådan påverkanskampanj innebär kan framstå som mer välmotiverad. Den senare risken förvärrar också risken för att samhället har en otillräcklig beredskap för att hantera storskaliga och plötsliga kontroverser. Dagslägetes säkerhetspolitiska situation medför att krishanterande aktörer med stor sannolikhet inte bara kommer att behöva hantera sådana kontroverser i sig, utan även påverkanskampanjer som bedrivs för att förstärka kontroversens negativa konsekvenser och effekter. Det har inte identifierats någon tydlig syntesrisk utifrån de båda riskerna.

#### 4.6.2 Påverkan och angrepp mot informationsinfrastruktur

Risken för att Sveriges informationsinfrastrukturer är otillräckligt skyddade mot angrepp förvärrar inte risken för påverkan, med några undantag. I de fall någon aktör inte vill att viss förmedling av information ska ske, eller önskar skapa oro genom att stänga ner medierna, kan ett angrepp vara motiverat inom ramen för en påverkanskampanj. I mer extrema lägen kan ett angrepp också användas för att kapa en utsändning av exempelvis tv eller radio för att därigenom bedriva påverkan. Risken för att påverkanskampanjer bedrivs mot allmänheten och beslutsfattare genom medier förvärrar inte i sig risken för påverkan, med några undantag.

Desinformation och vilseledning kan användas för att provocera fram angrepp, men kan även användas före, men i synnerhet efter, ett angrepp för att förleda beslutsfattare och allmänheten om vem som låg bakom, vilka motiven eller vems fel det var, huruvida det var rättfärdigt etc. En tydlig syntesrisk är ett scenario där inte all internettrafik alternativt alla tv- eller radiosändningar blockeras utan där åtkomst till trovärdiga nyhetskällor begränsas, men där andra medier fortsätter att fungera – sociala medier exempelvis. Det i kombination med en påverkanskampanj (som kan, men inte måste, komma från samma aktör) kan leda till att en samverkan mellan riskerna uppstår som medför än större skada.

#### 4.6.3 Storskaliga kontroverser och angrepp

Risken för att Sveriges informationsinfrastrukturer är otillräckligt skyddade mot angrepp förvärrar risken för att samhället har en otillräcklig beredskap för att hantera storskaliga och plötsliga kontroverser. Ett angrepp mot den svenska informationsinfrastrukturen kan både utgöra startskottet för en sådan kontrovers, och genomföras för att förvärra kontroversen medan den pågår. Så länge det är förhållandevis enkelt att angripa informationsinfrastrukturen kommer det finnas en stor mängd aktörer som framgångsrikt kan göra det. Vore det svårare (och känt att det är svårare) att genomföra ett sådant angrepp skulle risken för att ett sådant angrepp förmodligen minska. Detta eftersom färre framgångsrikt skulle kunna genomföra det, och färre samtidigt skulle anse att det är värt investeringen i resurser, tid och pengar som skulle krävas.

Efterspelet av ett sådant angrepp skulle kunna innebära en öppen debatt där spårning av och bevis mot den som angrep sker på mer eller mindre välavvägda grunder, vilket i sin tur skulle kunna utvecklas till diplomatiska kontroverser. Ett exempel på det är de påstådda ryska cyberattacker på det demokratiska partiet i USA och landets valmyndighet. Risken för att samhället har en otillräcklig beredskap för att hantera storskaliga och plötsliga kontroverser förvärrar också risken för att Sveriges informationsinfrastrukturer är otillräckligt skyddade mot angrepp. Om det är känt att Sveriges förmåga att hantera en storskalig kontrovers är bristande kan trösklarna för att initiera en sådan attack vara lägre än de annars skulle vara. En tydlig syntesrisk är att storskaliga och plötsliga kontroverser och angrepp på informationsinfrastrukturen används för att motivera varandra. Ett angrepp kan användas för att initiera en kontrovers, varpå kontroversen används för att motivera flera angrepp. På motsvarande vis kan en storskalig och plötslig kontrovers utgöra ett eget startskott på en sådan ond spiral, varpå angrepp på informationsinfrastrukturen följer.



#### 4.6.4 Övergripande slutsatser

Riskanalysen och analysen av hur riskerna samspelar indikerar att förstärkningseffekter uppstår mellan ”informationsrisker”. Det är risker som handlar om avsaknad av riktig information, tillgång till falsk information och viralitet. Risker som berör svagheter i informationsinfrastrukturen (”infrastrukturrisker”) och hur den används, tycks inte förstärka informationsriskerna. Skälet till att de två kategorierna av risk i de flesta fallen inte verkar förstärka varandra är att informationsriskerna orsakar som mest skada när informationen får flöda fritt, så fort och så brett som möjligt, medan infrastrukturriskerna (huvudsakligen) handlar om vilka sätt det fria informationsflödet är begränsat eller kan begränsas. Det kan dock finnas scenarier där viss informationsinfrastruktur blockeras eller begränsas vid sin källa – huvudsakligen för traditionella medier – genom cyberattacker eller fysiska sabotage. Där skulle det kunna vara problematiskt om exempelvis internetinfrastrukturen var intakt men fylld av desinformation via genomslagskraftiga kanaler som sociala medier.

# **Mediebranschen och det civila försvaret**

## 5. Mediebranschen och det civila försvaret

I den försvarspolitiska inriktningen för 2016–2020 anger regeringen att planeringen för civilt försvar ska återupptas. Civilt försvar är i grunden hela samhällets inneboende robusthet, motståndskraft och förmåga att hantera ett väpnat angrepp. Förmågan att hantera kriser i fred ger grundläggande förmåga att hantera krigsfara och krig.

Civilt försvar är den verksamhet som ansvariga aktörer genomför i syfte att göra det möjligt för samhället att hantera situationer när beredskapen höjs. Det civila försvaret är därmed inte en organisation. Det är statliga myndigheter, kommuner, landsting, privata bolag och frivilligorganisationer som bedriver verksamheten som består av skydd av befolkningen, säkerställande av samhällsviktiga funktioner och övriga samhällets stöd till Försvarsmakten. Arbetet med civilt försvar ska ske hos de aktörer i samhället som bedriver sådan verksamhet som stödjer samhällets funktionalitet – det vill säga samhällsviktig verksamhet.

I Sverige är det privata bolag som driver flera av de samhällsviktiga verksamheterna, det gäller inte minst inom mediebranschen. MSB har i sin vägledning för samhällsviktig verksamhet särskilt pekat ut elva samhällssektorer innehållandes viktiga samhällsfunktioner och samhällsviktig verksamhet. En av dessa sektorer är information och kommunikation. Exempel på viktiga samhällsfunktioner inom sektorn är telefoni (mobil och fast), internet, radiokommunikation, distribution av post, produktion och distribution av dagstidningar, webbaserad information och sociala medier. Av dessa funktioner faller flera inom ramen för det som mediebranschens aktörer upprätthåller i samhället. Om sektorns viktiga samhällsfunktioner skulle avstanna så är risken överhängande att varningsmeddelanden, nyheter och samhällsinformation inte når allmänheten i tillräcklig grad.

Hur höjd beredskap eller en krigssituation skulle påverka mediebranschens aktörer kan variera beroende på vilket läge Sverige befinner sig i innan och under den eskalerande situationen samt många andra omständigheter.

Det ökade trycket på det civila samhället och mediebranschen inför och under höjd beredskap indikerar ett behov av en stark kris- hanteringsförmåga för att ge en robustare grund för hanteringen av en krigssituation.

## 5.1 Höjd beredskap – identifierade risker och sårbarheter

MSB har vid framtagandet av denna rapport fått indikationer på att vissa delar av mediebranschen i stort sett saknar planering eller förberedelser för höjd beredskap. Det redaktionella arbetet inom nyhetsbolag ska i sig vara präglad av ett ”ständigt krisberedskapsläge”, men beredskapen är inte dimensionerad för omständigheter som kan tänkas råda under krigsliknande förhållanden.

Utifrån att förmågan att hantera kriser i fred ger grundläggande förmåga att hantera krigsfara och krig behöver mediebolagens hantering av bland annat fredstida riskhantering uppmärksammas. I MSB:s enkät till mediebranschen som gjordes i anslutning till denna rapport framkommer vissa möjliga svagheter i mediebolagens arbete med riskanalyser och hanterandet av identifierade risker och åtgärder. Få av bolagen verkar identifiera åtgärder i sin riskanalys, och bland riskidentifieringen analyseras risker kopplade till allmänhetens förtroende hos relativt få bolag. Det kan även finnas stödbehov för arbetet med informationssäkerhetsrisker. Få bolag har en särskild funktion som leder arbetet med riskanalys, vilket kan vara ett resultat av den tuffa ekonomiska situationen och/eller mindre storlek på flera bolag.

För att åtgärder ska vidtas eller risker hanteras krävs det nästan alltid att ansvar och mandat tilldelas. Svaren från enkäten indikerar att ansvariga för hanteringen av respektive risk och ansvariga för hanteringen av respektive åtgärd i högre grad behöver pekas ut.

För att säkerställa att åtgärdernas eftersökta effekt verkligen realiserar sig krävs uppföljning. I nuläget är det få bolag som följer upp sina åtgärder inom verksamhetsuppföljningen vilket tyder på att det råder en utbredd okunskap bland mediebolagen om huruvida åtgärder fullföljts och om dessa fått önskad effekt.

MSB bedömer att det inom ramen för arbetet med civilt försvar och höjd beredskap kan finnas skäl för att i samverkan med branschens aktörer utreda hur olika former av stöd skulle kunna utformas för att stärka mediebolagens riskhantering. Utöver mediebolagens fredstida riskhantering är redan identifierade risker och sårbarheter gentemot mediebranschen i fred av fortsatt betydelse under ett läge av höjd beredskap. Riskerna och sårbarheterna som presenterats i denna rapport bedöms ha lika stor eller större inverkan på branschens förmåga att bidra till upprätthållandet av samhällslig funktionalitet och krisberedskap under en krigssituation. Då förmågan att hantera en krigssituation bygger på förmågan att hantera ett krisläge är det MSB:s uppfattning att riskerna som identifierats i denna rapport också utgör ett viktigt första steg för planeringen av åtgärder, i syfte att stärka det civila försvaret.

Inför och vid höjd beredskap hotas sannolikt särskilt mediebranschens distributionsförmåga, eftersom sabotage och attacker kan förväntas ske mot den svenska (informations)infrastrukturen. Detta inverkar på såväl de verksamhetsnära riskerna 4.4.2 Egendom kommer att drabbas av skada och 4.4.7 Verksamhetskritisk information kommer att bli felaktigt raderad (se ovan) som samhällsriskerna 4.5.3 Mediekonsumtionen ger inte redundans till krisberedskapen och 4.5.2 Sveriges informationsinfrastrukturer är otillräckligt skyddade mot angrepp.

Som redovisat i risken 4.5.1 Mediekonsumtionen ger inte redundans till krisberedskapen ovan, finns det tydliga skillnader i vilka medium och plattformar som olika åldersgrupper i samhället använder för att tillägna sig information och nyheter. Den informationsinfrastruktur som byggts upp för public service används främst av den äldre generationen. För att säkerställa informationsspredningen under höjd beredskap har vissa aktörer öppnat för att avtala med svenska staten om ökad redundans och möjlighet till kompletterande sändningsförmåga för prioriterade mediekana-ler från utlandet. Djupare kunskap om hur ett sådant avtal skulle kunna se ut, samt vad det skulle kunna innehålla och omfatta kan behöva undersökas.

I samband med utsändning, i synnerhet i marknätet, finns betydande skillnader i förhållande till hur det var förr i tiden. Två sådana skillnader är av synnerlig betydelse. Den första skillnaden är att signalen måste passera genom fler aktörers informationsinfrastruktur för att nå fram till slutmottagaren i jämförelse med tidigare. Den andra skillnaden är att de aktuella informationsinfrastrukturerna (i varierande grad) är exponerade mot internet och därför kan angripas från fjärran. Möjligheterna för enskilda bolag att krävställa säkerheten i hela kedjan av aktörer vars informationsinfrastruktur signalen passerar igenom bedöms vara låg.

Det är därför MSB:s bedömning att det bör undersökas hur redundansen i kedjan och säkerheten i systemen kan utvecklas (exempelvis genom avtal mellan operatörerna och staten) för att säkerställa förmågan att nå ut med samhällsinformation och nyheter i samband med höjd beredskap. Under krigsliknande förhållanden kommer extra höga behov finnas av exempelvis driftsäkerhet, skalskydd och personskydd hos mediebolagen och deras leverantörer till följd av den förhöjda hotbilden. För att etablera och säkerställa en önskvärd nivå behöver avtal slutas och på dem följande åtgärder vidtas av mediebolagen för att upprätta nödvändiga förmågor. För att kunna säkerställa ändamålsenliga effekter bör avtalen slutas och åtgärderna vidtas långt innan krigsliknande förhållanden uppstår.

## 5.2 Lärdomar från omvärldsbevakning

Vid höjd beredskap kan två typer av hot väntas vara särskilt allvarliga för den svenska mediebranschen och samhället: angrepp mot infrastruktur samt påverkanskampanjer. Sett i ett internationellt perspektiv finns ytterligare aspekter av framförallt informationskrigföring som ger en bredare och djupare förståelse för hur förhållandena kan se ut under ett scenario med höjd beredskap.

Annekteringen av Krim 2014 utgör ett exempel på vinningarna av att störa ut civil telekommunikationsinfrastruktur för att skaffa sig ett informationsövertag. Flera sårbarheter i det moderna medielandskapet aktualiserades då. I nutida krigföring kan stater ha som mål att initialt i en konflikt störa ut civila traditionella medier såsom tv- och radio-sändningar, och online-medier såsom sociala nätverk. Syftet är att hindra en motståndares ”propaganda och desinformation” att nå ut.

Infrastrukturen för internet består bland annat av havskablar förlagda utmed havsbotten, så även i haven runt Sverige. Ökad verksamhet kring havskablar kan indikera att en kartläggning pågår av sådan kritisk infrastruktur och dess status som en möjlig måltavla vid en eskalerande konflikt. Aktivitet runt kablarna har också upptäckts flera gånger de senaste åren. I rymden har vissa manövrer av farkoster i närheten av kommunikationssatelliter och testskjutningar av anti-satellitvapen tolkats som ytterligare indikationer på möjliga prövningar som kan uppstå under ett scenario av höjd beredskap för svensk del.

Sammanfattningsvis kan civil internetanslutning komma att störas ut, vilket är något som bland annat mediebranschens aktörer bör planera inför vid arbete med civilt försvar. I nuläget är en allmän trend att konsumenter av system för internetinfrastruktur, såsom mediebolag, inte betalar för robusta och redundanta lösningar.



# Åtgärdsförslag



## 6. Åtgärdsförslag

MSB har identifierat åtta åtgärdsförslag. En sammanfattning av hur de möter riskerna presenteras i tabellen på nästa uppslag.

Presentationen av åtgärdsförslagen följer upplägget beskrivning av åtgärden, utförare, partner(s), möjligt stöd och målgrupp.

### 6.1 Åtgärdsförslag till mediebolagen

#### 6.1.1 Ta fram skyddsstrategier för journalister i digitala miljöer

Mediebolagen kan utveckla tydliga skyddsstrategier för sina medarbetare och exponeringen av dessa i digitala miljöer för att motverka hot och trakasserier.

**Åtgärdsförslag:** Skyddet kan utvecklas med avseende på hur hantering av öppna kommentarsfält ska ske, användandet av bylines på vissa artiklar, restriktivitet i aktiviteter på sociala medier och dolda telefonnummer. Värt att notera är att sådana åtgärder redan har vidtagits av vissa aktörer inom branschen. MSB bedömer att det finns utrymme för större samordning mellan åtgärder och större kunskapsutbyte om branschstandarder för rutiner och förhållnings-sätt till hot och trakasserier i digitala miljöer.

Samarbetspartners kring åtgärden är mediebolagen själva. Möjliga partners kan vara MSB, JMG, TU och IIS. MSB och mediebolagen själva kan bistå med kunskap och kompetens. Målgruppen för åtgärden är mediebolagen och dess journalistkår.

#### 6.1.2 Utveckla ett systematiskt arbete med informationssäkerhet inom mediebolagen

MSB bedömer att det finns utvecklingspotential i mediebolagens arbete med informationssäkerhet. Detta gäller både för beroende av infrastruktur, intern hantering av verksamhetskritisk information och specifikt hos nyhetsproducerande mediebolag och deras upprätthållande av digitalt källskydd.

	Ta fram skyddsstrategier för journalister i digitala miljöer	Utveckla ett systematiskt arbete med informations säkerhet inom mediebolagen	Stöd insatser för ökad medie- och informationskunnighet	Satsa på medvetandehöjande insatser om olika kriskommunikationskanaler vid kris	Utreda ett interaktivt kriskommunikationssystem	Se över hot och trakasserier mot medier	Se över konsekvenserna av medieskugga	Gemensamma insatser för ett stärkt civilt försvar	Totalt antal åtgärder som riktar sig mot risken:
Personal kommer att skadas fysiskt eller psykiskt	1	0	0	0	0	1	0	1	3
Verksamhetskritisk information kommer att bli otillgänglig	0	1	0	0	0	0	0	1	2
Egendom kommer att drabbas av skada	0	0	0	0	0	0	0	1	1
Verksamhetskritisk information kommer att bli röjd	0	1	0	0	0	0	0	1	2
Allmänhetens förtroende för organisationen kommer att minska	0	1	1	1	0	0	0	1	4
Verksamhetskritisk information kommer att bli felaktigt ändrad	0	1	0	0	0	0	0	0	1
Verksamhetskritisk information kommer att bli felaktigt raderad	0	1	0	0	0	0	0	1	2
Påverkanskampanjer bedrivs mot allmänheten och beslutsfattare genom medier	0	0	1	1	0	0	0	1	3
Sveriges informationsinfrastruktur är otillräckligt skyddade mot angrepp	0	1	0	0	0	0	0	1	2
Mediekonsumtionen ger inte redundans till krisberedskapen	0	0	0	1	1	0	0	0	2
Samhället har en otillräcklig beredskap för att hantera storskaliga och plötsliga kontroverser	0	0	1	1	0	0	0	1	3
Vissa områden och samhällsgrupper hamnar i medieskugga	0	0	0	1	0	0	1	0	2
<b>Totalt antal risker som åtgärden riktar sig mot</b>	<b>1</b>	<b>6</b>	<b>3</b>	<b>5</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>9</b>	

**Åtgärdsförslag:** MSB rekommenderar att ett systematiskt informationssäkerhetsarbete, bland annat genom ett ledningssystem för informationssäkerhet, införs i det bredare arbetet med skydd av verksamhetskritisk information. Detta skulle appliceras på exempelvis branschens innehav och beroende av informationsinfrastruktur och outsourcade it-tjänster samt utnyttjande av molnlösningar. Här behöver ett helhetsgrepp tas kring de beroendekedjor som alla mediebolag i någon mån har kopplade till sin informationshantering.

Initiala steg för arbete med digitalt källskydd är framtagande av policyer och utbildning på området för mediebolagen. Redan existerande arbete på området av Utgivarna och IIS kan ligga till grund för fortsatt arbete med digitalt källskydd. En väg framåt, för att höja nivån på branschens hantering av källskydd i digitala miljöer, skulle vara en branschstandard. Standarden skulle bottna i krav på systematiskt informationssäkerhetsarbete i stil med ISO 27000-seriens krav. På motsvarande sätt kan distribuerande mediebolag se över säkerheten kring konfigurationsdata för sin informationsinfrastruktur.

Samarbetspartners kring åtgärden rekommenderas vara mediebolagen själva, exempelvis med hjälp av centrala branschorgan som Utgivarna. Partners kan vara, förutom centrala branschorgan, IIS (för arbetet med digitalt källskydd) och MSB. MSB kan främst bidra med kunskap och kompetens samt metodstöd för informationssäkerhet. Målgrupp för åtgärden är mediebolagen.

## 6.2 Åtgärdsförslag till myndigheter

### 6.2.1 Stöd insatser för ökad medie- och informationskunnighet

I det alltmer varierade och splittrade medielandskapet ställs högre krav på den enskilde individens förmåga att finna, analysera, kritiskt värdera och själv skapa information i olika medier och sammanhang – även kallat medie- och informationskunnighet (MIK). MSB bedriver i nuläget ”18-årsuppdraget” tillsammans med Försvarsmakten och Rekryteringsmyndigheten, där det ingår delar som syftar till att höja medvetenheten om vikten av källkritik. MSB tillhandahåller också ett test där ungdomar kan träna sin källkritiska förmåga. Vikten av att den enskilde individen ska kunna och vilja tillgodogöra sig kunskap genom medieanvändning lyfts i både Framtidskommissionens och Medieutredningens slutrapporter och vikten av kritiskt tänkande och källkritiskt granskande av information lyfts i Demokratiutredningens slutrapport.

MSB bedömer med utgångspunkt i den ovan redovisade riskanalysen att det finns ett behov av att stärka motståndskraften hos allmänhet och beslutsfattare mot falska eller missvisande påståenden, ryktes-spridning och påverkan genom olika mediekkanaler. Se särskilt under-avsnitten 4.5.1 Påverkanskampanjer bedrivs mot allmänheten och beslutsfattare genom medier och 4.5.4 Samhället har en otillräcklig beredskap för att hantera storskaliga och plötsliga kontroverser ovan.

**Åtgärdsförslag:** Upprätta anpassade utbildningar i MIK för olika åldersgrupper och stärk kravet på källkritik, argumentations-analys och kritiska förhållningssätt i skolornas läroplaner. Kraven bör anpassas så att elever lär sig att tillämpa sådana verktyg i den moderna mediemiljön. Informera också om påverkan, digitala löp-eldar och andra fenomen i den digitala miljön som innebär att den enskilde individen måste vara särskilt försiktig.

MSB avser att fortsätta att vidta åtgärder för att höja kunskaps-nivån inom detta område och kan bistå med stöd till olika kunskaps-höjande projekt utförda av samarbetspartners, såsom skolor och bibliotek. Målgruppen är allmänheten i stort, fokus bör vara på barn och unga vuxna.

### 6.2.2 Satsa på medvetandehöjande insatser om olika kriskommunikationskanaler vid kris

Myndigheter och andra aktörer bör kriskommunicera på de platt-formar där människor finns, men för att göra informationsförmed-lingen effektiv bör också den enskilde individen ha kunskaper om de kanaler för kriskommunikation som finns, och vad denne kan förvänta sig i fråga om dem.

**Åtgärdsförslag:** Det bör genomföras informationsinsatser som betonar varför det är viktigt att använda flera nyhetskällor genom flera mediekkanaler för att säkerställa redundans i informationstillgången och riktighet i uppgifter som inhämtas. Informationen bör utfor-mas utefter kända medievanor under både normala och krisartade förhållanden hos alla åldersgrupper. För ungas medieanvändning som är koncentrerad till sociala medier ska för- och nackdelar med dessa kanaler lyftas tillsammans med råd och instruktioner om andra mindre utnyttjade kriskommunikationskanaler som radio och tv. Det samma skulle göras till de äldre delarna av befolkningen där användarmönstret är det omvända. Den medvetandehöjande informationskampanjen bör göras i de mediekkanaler som respektive åldersgrupp använder.

I nuläget är informationen om kriskommunikation inriktad på att informera om fördelarna med att exempelvis äga en radio med vev. I de föreslagna informationsinsatserna skulle detta budskap kompletteras med information om fördelarna med internet, och plattformar som sociala medier till de grupper i samhället som för närvarande använder dem i liten eller obefintlig utsträckning. Informationsinsatserna skulle också kunna innehålla budskap som stöttar källkritisk förmåga där vikten av använda olika källor (och källors medium) betonas. Kärnan i informationsarbetet skulle alltså vara att betona att alla bör använda flera olika källor, i flera olika medier för att på så sätt säkerställa såväl tillgänglighet som riktighet. Åtgärden skulle på så sätt kunna leda till att den befintliga informationsinfrastrukturens fulla potential för kriskommunikation och -beredskap används.

MSB avser fortsätta att vidta åtgärder för att höja kunskapsnivån inom detta område. Möjliga partners kan vara mediedistributörer, IIS och Myndigheten för radio och tv för underlag om rådande medievanor. MSB kan bistå med kunskap och kompetens kring kriskommunikation. Målgruppen för åtgärden är allmänheten i stort med särskilt fokus på vissa åldersgrupper.

### 6.2.3 Utredda ett interaktivt kriskommunikationssystem

Risken för bristfälligt utnyttjandet av den existerande informationsinfrastrukturen för krisberedskapen, genom främst mediekonsumtionsvanor, begränsar den potential som redan finns i vissa funktioner inom social media. Dessutom kräver utvecklingen av ungas medievanor att sociala medier tar en större plats i planeringen för framtidens kriskommunikation.

Som nämnt i underavsnitt 4.5.3 Mediekonsumtionen ger inte redundans till krisberedskapen ovan tillhandahåller MSB i dagsläget en applikation för krisinformation och utvecklar dessutom ytterligare en applikation som kommer att sammanföra information från ett antal flöden som är relevanta för den enskildes beredskap. Den nya applikationen kommer också att kunna konfigureras så att den levererar lokal information som är extra viktig utifrån den enskildes förutsättningar och situation. Det finns ett mycket stort antal användare på exempelvis Facebook som inte följer MSB och/eller andra kriskommunikationsorganisationer, och som inte heller har någon sådan applikation. Andelen användare som potentiellt skulle kunna nås, om det enda som krävdes för det var ett medlemskap på Facebook, är därmed stort.

**Åtgärdsförslag:** MSB föreslår därför att det bör utredas hur man kan utveckla ett interaktivt kriskommunikationssystem som kompletterar de tjänster som redan finns genom att vara en del av plattformen, snarare än en påbyggnad i ett tillhörande ekosystem av applikationer. Systemet skulle utarbetas i samarbete med företag som tillhandahåller plattformstjänster som används av stora delar av den svenska allmänheten.

Avtal om att kunna ansluta till, utveckla och använda existerande funktionalitet hos privata aktörer, som redogjordes för i underavsnitt 4.5.3 Mediekonsumtionen ger inte redundans till krisberedskapen ovan, skulle kunna slutas med Facebook, Twitter och/eller Google. Utöver att ge information till anhöriga skulle funktionen också kunna användas för att i realtid meddela om och föra statistik över vilka och hur många som tagit del av myndighetsinformation om exempelvis var det finns tillgång till rent vatten eller var evakuering sker samt vilka uppgifter i sociala medier som inte är verifierade än.

Utredningen bör dock ställa fördelarna i form av ökad räckvidd och en stärkt möjlighet till att ha en lägesbild över kriskommunikationens genomslagskraft mot potentiella nackdelar, såsom avbrottsrisker och risken för antagonistisk manipulation. Utredningen bör också se över hur än större nytta kan dras från befintliga tjänster i samband med att ett sådant kriskommunikationssystem etableras. Åtgärden bör ses som ett komplement till andra kanaler för kriskommunikation.

MSB avser påbörja ett arbete med att utreda denna fråga. Partners skulle till exempel kunna vara Facebook, Twitter och/eller Google samt myndigheter med områdes- eller sektorsansvar samt kommunerna vilka redan ansvarar för delar av den existerande VMA-infrastrukturen. MSB kan bidra med stöd i det långsiktiga arbetet med utvecklande av kriskommunikationssystem. Målgruppen för åtgärden är allmänheten och samhällets krisberedskapsfunktion i stort.

#### 6.2.4 Se över hot och trakasserier mot medier

Hot och trakasserier är i dag vardag i mediebranschen, vilket i förlängningen kan vara ett hot mot demokratin. Det finns därför ett behov av att motverka grunderna till hotbilden mot branschen och de som är verksamma inom den.

**Åtgärd:** MSB ser ett behov av att stävja den utveckling av hot och trakasserier som mediebranschen nu utsätts för. Medieutredningen föreslår att en utredning ska ”se över möjligheterna för att stärka det straffrättsliga skyddet för journalister...” – ett skydd som genom lagförande av sådana brott skulle ge ett starkt signalvärde om all-

varet i att hota och trakassera journalister. Medieutredningens lyfte i sitt delbetänkande även fram statens ansvar för att värna det goda samtalsklimatet och beivra hot och kränkningar mot enskilda individer, samt att staten bör se extra allvarligt på hot och kränkningar av journalister eftersom dessa agerar i demokratins tjänst. MSB bedömer att det finns behov av ett bättre straffrättsligt skydd för journalister och stödjer Medieutredningens slutsats om att området bör utredas.

Samarbetspartners kring denna åtgärd kan vara flera aktörer: centrala branschorgan inom mediebranschen, Brottsförebyggande rådet (BRÅ) samt Säkerhetspolisen. MSB kan bidra med kunskap och kompetens.

### 6.2.5 Se över konsekvenserna av medieskugga

Medieskugga över vissa områden och samhällsgrupper riskerar påverka såväl krisberedskapen, motståndskraften mot påverkan och graden av möjlighet till informerat deltagande i de demokratiska samhällsprocesserna.

**Åtgärdsförslag:** MSB rekommenderar att det ses över hur medieskugga över vissa områden och samhällsgrupper påverkar samhällets funktionalitet och förmågan att nå ut med samhällsinformation under en samhällskris. Arbetet bör syfta till att kartlägga hur viktiga meddelanden kan nå individer när få betrodda och etablerade mediekanaler, såsom traditionella medier, finns på plats. Även sårbarhet gentemot påverkan, som en följd av medieskugga, bör vara en parameter i denna undersökning.

Samarbetspartners kring denna undersökande åtgärd kan vara flera, till exempel mediebranschen eller kommunerna. MSB kan bistå med kunskap och kompetens. Målgrupper för åtgärden är mediebranschen och allmänheten i stort.

## 6.3 Gemensamma insatser för ett stärkt civilt försvar

MSB bedömer att arbetet med att åtgärda de risker som är kopplade till civilt försvar förutsätter ett avtalat stöd mellan mediebolagen och den svenska staten. En analys av hur sådana avtal skulle kunna utformas för att fungera effektivt i det nya medielandskapet behöver genomföras. Analysen bör omfatta dels vilka typer av stöd staten kan och bör ge mediebolagen i deras robusthetshöjande arbete, dels vilka stöd mediebolagen kan och bör ge Sverige under höjd beredskap.

Analysen bör vägledas av vikten i att upprätthålla mediebranschens tre samhällsviktiga teman: krishantering, granskning och trygghet. Mediernas oberoende och fria, granskande roll bör i synnerhet betonas. De nedan föreslagna delåtgärderna utgör åtgärder som mediebolagen med stöd av svenska staten skulle kunna vidta för att stärka sin robusthet. Delåtgärderna är förslag på den typ av särskilda åtgärder som behöver vidtas när planeringen inom totalförsvaret kommit längre.

Vissa deltagare inom Mediernas beredskapsråd har redan öppnat för att utveckla beredskapshöjande avtal med staten.

Förslag på delåtgärder som skulle kunna stärka krishanteringsförmågan (mediebolagens egen och samhällets med stöd av medierna) och därmed förmågan att hantera ett krigstillstånd:

- Mediebolagen rekommenderas i högre utsträckning upprätta, pröva och utvärdera sina krishanteringsplaner utifrån aspekten civilt försvar. För att kunna få fungerande krishanteringsplaner krävs återkommande riskanalyser och ett strukturerat riskhanteringsarbete. Mediebolagen rekommenderas lägga större vikt vid riskerna som påverkar allmänhetens förtroende. Krishanteringsplaner behöver också i större utsträckning spridas och övas inom organisationen. Detta behövs för att medvetandegöra och förbereda all berörd personal samt för att utvärdera och utveckla planen i sig.
- Inrätta beredskapsplaner för verksamheten där det planeras såväl för kommunikationsbehov, personalbehov och utrustningsbehov, som för tillhörande skydd.
- Utbilda medarbetare i grundläggande informationssäkerhet samt påverkan, anpassat efter den verksamhet som bedrivs – exempelvis tekniskt orienterat för distributionsbolag och digitalt källskydd för nyhetsproducenter.
- Hitta former för samarbete mellan mediebolagen – exempelvis extra driftsajter, lån av infrastruktur och lokaler etc.
- Upprätta starka skydd för (både tillgång till och drift av) elektroniska kommunikationer inom de egna verksamheterna.
- Skaffa redundans i internetförbindelser respektive katalogtjänster (se avsnitt 2.5.4 Överbelastningsattackerna mot Dyn DNS den 21 oktober 2016 ovan), skaffa säkra backupptjänster och genomför penetrationstester<sup>35</sup> samt se över skydd och rutiner för gisslanprogramvara och annan skadlig kod.

---

35. Tester där den fysiska, it-baserade och övriga säkerheten testas för intrång under ordnade former.



- Skaffa överbelastningsskydd för webbplatser, e-tjänster och telefonitjänster.
- Sätta mål för svarstider (förslagsvis med utgångspunkt i de incidenttyper som har studerats i denna rapport).
- Utveckla särskilda rutiner för validering och verifiering av information som kan tillämpas för särskilt känsliga frågor.

Sammarbetspartners kring delåtgärderna rekommenderas vara mediebolagen själva tillsammans med staten. MSB kan utgöra en partner och bidra med kunskap och kompetens för arbetet med avtal vilket är en förutsättning för delåtgärdernas genomförande. Målgruppen för åtgärderna är mediebolagen.



# **Bibliografi**

## Bibliografi

Albinsson, Pär-Anders m.fl., *Analys och detektion av vilseledning och påverkansoperationer i sociala medier*. Totalförsvarets forskningsinstitut, FOI-R-4142-SE, ISSN 1650-1942, december 2015, webblänk: <https://foi.se/rapportsammanfattning?reportNo=FOI-R--4142--SE> (hämtad 2016-11-09).

Andersson, Sus, Petra Jankov Picha, Fredrik Laurin och Anders Thoresson, *Digitalt källskydd – en introduktion*. Internetstiftelsen i Sverige, Internetguide, nr 35. 2016, webblänk: <https://www.iis.se/docs/digitalt-kallskydd-2.pdf> (hämtad 2017-01-27).

Arkhede, Sofia och Ohlsson, Jonas, *Nyhetsintresse och nyhetskonsumtion*. Göteborgs universitet, SOM-institutet, SOM-rapport nr 2015:33, webblänk: [http://som.gu.se/digitalAssets/1561/1561529\\_nyhetsintresse-och-nyhetskonsumtion-2015.pdf](http://som.gu.se/digitalAssets/1561/1561529_nyhetsintresse-och-nyhetskonsumtion-2015.pdf) (hämtad 2017-02-02).

Asp, Viktoria, Bynander, Fredrik, Daléus, Pär, Deschamps-Berger, Jenny, Sandberg, Daniel och Schyberg, Erik, *Bara skog som brinner? Utvärdering av krishanteringen under skogsbranden i Västmanland 2014*. Försvarshögskolan beteckning 640/2014, FHS/Crismart 11 september, Stockholm, 2014, webblänk: [https://www.fhs.se/Documents/Externwebben/forskning/centrumbildningar/Crismart/Publikationer/Crismart%20\(2015\)%20-%20Bara%20skog%20som%20brinner.pdf](https://www.fhs.se/Documents/Externwebben/forskning/centrumbildningar/Crismart/Publikationer/Crismart%20(2015)%20-%20Bara%20skog%20som%20brinner.pdf) (hämtad 2016-11-09).

Brandtzaeg, Petter Bae m.fl., "Emerging Journalistic Verification Practices Concerning Social Media", *Journalism Practice* Vol. 10 (3) 2016, sidorna 323-342, webblänk: <http://www.tandfonline.com/doi/full/10.1080/17512786.2015.1020331> (hämtad 2016-11-09).

Brangetto, Pascal och Veenendaal, Matthijs A., *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations*. 8th International Conference on Cyber Conflict, Tallinn, 2016, sidorna 113–126, webblänk: <https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2008%20Influence%20Cyber%20Operations%20-%20The%20Use%20of%20Cyberattacks%20in%20Support%20of%20Influence%20Operations.pdf> (hämtad 2016-11-02).

Broberg, Per-Anders, *Hot och hat – så påverkas medierna*. Utgivarna, rapport 2016:1, webblänk: [http://utgivarna.se/images/Filer/Utgivarna\\_Hot\\_och\\_hat\\_juni2016\\_enkelsidor.pdf](http://utgivarna.se/images/Filer/Utgivarna_Hot_och_hat_juni2016_enkelsidor.pdf) (hämtad 2017-01-24).

Brottsförebyggande rådet, *Hot och våld: Om utsatthet i yrkesgrupper som är viktiga i det demokratiska samhället*. Rapport: 2015:12, Stockholm, 2015, webblänk: [http://www.bra.se/download/18.43d343f714ce4faf9081ce/1440752473386/2015-12\\_Hot\\_och\\_v%C3%A5ld.pdf](http://www.bra.se/download/18.43d343f714ce4faf9081ce/1440752473386/2015-12_Hot_och_v%C3%A5ld.pdf) (hämtad 2017-02-03).

Cantor, Lily, "From traditional gatekeeper to professional verifier: how local newspaper journalists are adapting to change", *The Journal of the Association of Journalism Education*, vol. 3 (1), 2014, sidorna 102–119. Webbsida: [http://shura.shu.ac.uk/7991/1/Canter\\_From\\_traditional\\_gatekeeper\\_to\\_professional\\_verifier.pdf](http://shura.shu.ac.uk/7991/1/Canter_From_traditional_gatekeeper_to_professional_verifier.pdf) (hämtad 2016-11-09).

Europaparlamentet och Rådet, *Art. 85 GDPR Processing and freedom of expression and information*. General Data Protection Regulation, webblänk: <https://gdpr-info.eu/art-85-gdpr/> (hämtad 17-01-27).

Datainspektionen, *EU:s dataskyddsreform*. Datainspektionen.se [Webbsida], 2016, webblänk: <http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddsreform/> (hämtad 2017-01-27).

Davidsson, Pamela och Findahl, Olle, *Svenskarna och internet 2016*, Internetstiftelsen i Sverige, Stockholm, 2016, webblänk: [https://www.iis.se/docs/Svenskarna\\_och\\_internet\\_2016.pdf](https://www.iis.se/docs/Svenskarna_och_internet_2016.pdf) (hämtad 2017-01-24).

Davidsson, Pamela, *Svenskarna och sociala medier 2016*. Internetstiftelsen i Sverige, Stockholm, 2016, webblänk: [https://www.iis.se/docs/Svenskarna\\_och\\_sociala\\_medier\\_2016.pdf](https://www.iis.se/docs/Svenskarna_och_sociala_medier_2016.pdf) (hämtad 2017-02-03).

Fackförbundet ST, *Öppenhet på villovägar? En rapport om meddelarfrihet och öppenhet inom stat och myndigheter*. Stockholm, 2014-05-15, webblänk: [https://st.org/sites/st.org/files/attachment/oppnenhet\\_pa\\_villovagar\\_20140515\\_0.pdf](https://st.org/sites/st.org/files/attachment/oppnenhet_pa_villovagar_20140515_0.pdf) (hämtad 2017-01-24).

Framtidskommissionen, *Svenska framtidsutmaningar*. ID-nummer: Ds 2013:19. Stockholm, Kulturdepartementet, 2013, webblänk: <http://www.regeringen.se/49b6cf/contentassets/c709bf195f8a48278ec51d02cdbc82cf/framtidskommissionens-slutrapport-svenska-framtidsutmaningar> (hämtad 2017-01-24).

Försvarsmakten och Myndigheten för samhällsskydd och beredskap, *Sverige kommer att möta utmaningarna: Gemensamma grunder (grundsyn) för en sammanhängande planering för totalförsvaret*. Beteckning: FM2016-13584:3/MSB2016-25, datum 2016-06-10, webblänk: [https://www.msb.se/Upload/Insats\\_och\\_beredskap/160610%20FM2016\\_13584\\_3%20Rapport%20MSB%20och%20FM.pdf](https://www.msb.se/Upload/Insats_och_beredskap/160610%20FM2016_13584_3%20Rapport%20MSB%20och%20FM.pdf) (hämtad 2017-02-02).

Giles, Keir, *Handbook of Russian Information Warfare*. NATO Defense College, Fellowship Monograph 9, Rom, 2016, webblänk: <http://www.ndc.nato.int/news/news.php?icode=995> (hämtad 2017-01-24).

Gustafsdotter, Jeanette och Lindberg, Tobias *Hot mot mediehus och medarbetare*. Utgivarna, rapport 2015:1, webblänk: [http://www.utgivarna.se/images/Utgivarna\\_Hot\\_mot\\_mediehus\\_och\\_medarbetare\\_2015\\_final.pdf](http://www.utgivarna.se/images/Utgivarna_Hot_mot_mediehus_och_medarbetare_2015_final.pdf) (hämtad 2017-02-03).

Jendel, Lena, *Nya kriser möter nya medier – digital krishantering i det nya medielandskapet*. MSB. Publ.nr MSB1059 – December 2016, webblänk: <https://www.msb.se/RibData/Filer/pdf/28208.pdf> (hämtad 2017-01-27).

Journalistpanelen 2016, maj, *Hoten och hatet mot journalister*. Institutionen för journalistik, medier och kommunikation, Göteborgs universitet, webblänk: [http://jmg.gu.se/digitalAssets/1577/1577351\\_jp9-trakasserier-journalister.pdf](http://jmg.gu.se/digitalAssets/1577/1577351_jp9-trakasserier-journalister.pdf) (hämtad 2016-10-27).

Karlsson, Michael, *Nätjournalistik i krissituationer – information eller desinformation*. Karlstads universitet, 2010, webblänk: <http://docplayer.se/4623194-Natjournalistik-i-krissituationer-information-eller-desinformation.html> (hämtad 2016-11-09).

Kleberg, Madeleine, *Underlag till Jämställdhetsutredningen*. U2014:06, Stockholms universitet, webblänk: <http://www.sou.gov.se/wp-content/uploads/2015/03/Media-Madeleine-Kleberg.pdf> (hämtad 2016-11-09).

Krebs, Brian, *The Democratization of Censorship*. KrebsOnSecurity.com (Webbsida), publicerad 2016-09-25, webblänk: <https://krebsonsecurity.com/2016/09/the-democratization-of-censorship/> (hämtad 2017-01-24).

Kulturdepartementet, *Medieborgarna och medierna. En digital värld av rättigheter, skyldigheter – möjligheter och ansvar*. ID-nummer: SOU 2015:94, webblänk: <http://www.regeringen.se/4ab02f/contentassets/aca20d317683426797fc15c0056004f3/medieborgarna--medierna.-en-digital-varld-av-rattigheter-skyldigheter--mojligheter-och-ansvar-sou-201594> (hämtad 2017-01-27).

Kulturdepartementet, *Människorna, medierna och marknaden*. ID-nummer: SOU 2016:30, webblänk: [http://www.regeringen.se/contentassets/a54e03720c7b4b9eb3f227e8ca32d72b/manniskorna\\_medierna\\_marknaden\\_SOU\\_2016\\_30](http://www.regeringen.se/contentassets/a54e03720c7b4b9eb3f227e8ca32d72b/manniskorna_medierna_marknaden_SOU_2016_30) (hämtad 2017-01-27).

Kulturdepartementet, *Låt fler forma framtiden! Del A*. ID-nummer: SOU 2016:5, webblänk: <http://www.regeringen.se/48e909/contentassets/16dfd1fed76e42dd9f40c9229637e44b/lat-fler-forma-framtiden-sou-20165-del-a.pdf> (hämtad 2017-01-27).

Kulturdepartementet, *Låt fler forma framtiden! Del B*. ID-nummer: SOU 2016:5, webblänk: <http://www.regeringen.se/48e909/contentassets/16dfd1fed76e42dd9f40c9229637e44b/lat-fler-forma-framtiden-sou-20165-del-b.pdf> (hämtad 2017-01-27).

Kulturdepartementet, *Slutbetänkande av medietredningen – En gränsöverskridande mediepolitik: För upplysning, engagemang och ansvar*. ID-nummer: SOU 2016:80, webblänk: <http://www.regeringen.se/contentassets/c4f57b68335e491a948185108aa3833f/en-gransoverskridande-mediepolitik.-for-upplysning-engagemang-och-ansvar-sou-201680> (hämtad 2016-11-09).

Lindberg, Tobias, *Därför hotas medier och medarbetare*. Utgivarna, Rapport 2015:2, webblänk: [http://www.utgivarna.se/images/Darfor\\_hotas\\_medier\\_okt2015\\_uppslag.pdf](http://www.utgivarna.se/images/Darfor_hotas_medier_okt2015_uppslag.pdf) (hämtad 2017-02-03).

Löfgren Nilsson, Monica, *Hot och hat mot svenska journalister*, Nordicom-Information 37, 2015, 3–4, sida 51–56, webblänk: [http://www.nordicom.gu.se/sites/default/files/kapitel-pdf/nordicom-information\\_37\\_2015\\_3-4\\_51-56.pdf](http://www.nordicom.gu.se/sites/default/files/kapitel-pdf/nordicom-information_37_2015_3-4_51-56.pdf) (hämtad 2017-01-24).

Myndigheten för radio och tv, *Mediekonsumtion 2016*. Stockholm, 2016, webblänk: [http://www.radioochtv.se/Documents/Publikationer/Medieutveckling/Mediekonsumtion/MU%202016%20-%20Mediekonsumtion\\_sep2016.pdf?epslanguage=sv](http://www.radioochtv.se/Documents/Publikationer/Medieutveckling/Mediekonsumtion/MU%202016%20-%20Mediekonsumtion_sep2016.pdf?epslanguage=sv) (hämtad 2017-01-24).

Myndigheten för samhällsskydd och beredskap, *Gemensamma grunder för samverkan och ledning under samhällsstörningar.*, Publikationsnummer MSB780, 2016-09, webblänk: <https://www.msb.se/RibData/Filer/pdf/27484.pdf> (hämtad 2017-01-24).

Myndigheten för samhällsskydd och beredskap, *Kriskommunikation i det digitala medielandskapet: Rapport från projektet Kriskommunikation 2.0*. Publikationsnummer MSB995, 2016-03, webblänk: <https://www.msb.se/RibData/Filer/pdf/28028.pdf> (hämtad 2017-01-24).

Myndigheten för samhällsskydd och beredskap, *Mediebranschen 2011 – hot, risker och sårbarheter*. Publikationsnummer MSB330 – november 2011, webblänk: <https://www.msb.se/RibData/Filer/pdf/26075.pdf> (hämtad 2016-11-09).

Myndigheten för samhällsskydd och beredskap, *Vägledning för samhällsviktig verksamhet*. Publikationsnummer MSB620, 2014-01, webblänk: <https://www.msb.se/RibData/Filer/pdf/27285.pdf> (hämtad 2017-01-24).

Nygren, Gunnar, och Kajsa Althén, *Landsbygd i medieskugga: nedmonteringen av den lokala journalistiken och bilden av landsbygden i Dagens Nyheter*. Södertörns högskola, 2014, webblänk: [https://www.jordbruksverket.se/download/18.37e9ac46144f41921cd356d8/1412749232104/Landsbygd\\_i\\_medieskugga\\_webversion.pdf](https://www.jordbruksverket.se/download/18.37e9ac46144f41921cd356d8/1412749232104/Landsbygd_i_medieskugga_webversion.pdf) (hämtad 2017-01-24).

Ohlsson, Jonas, *Den svenska mediemarknaden 2016 Ägare – bolag – medier*. Nordicom, Göteborgs universitet, 2016, webblänk: [http://nordicom.gu.se/sites/default/files/publikationer-hela-pdf/den\\_svenska\\_mediemarknaden\\_2016.pdf](http://nordicom.gu.se/sites/default/files/publikationer-hela-pdf/den_svenska_mediemarknaden_2016.pdf) (hämtad 2017-02-03).

Oxford University, *Digital Wildfire: (Mis)information flows, propagation and responsible governance*. Digitalwildfire.org [Webbsida], 2016, webblänk: <http://www.digitalwildfire.org/> (hämtad 2017-01-27).

Post- och telestyrelsen, *2016-års risk- och sårbarhetsanalys för PTS och dess ansvarsområden*. Diariennr 16-4837. 2016-10-28, webblänk: <http://www.pts.se/upload/Rapporter/Om-PTS/PTS%20gemensamma%20RSA%202016.pdf> (hämtad 2017-01-24).

Regeringen, *Försvarspolitisk inriktning – Sveriges försvar 2016–2020*. Regeringsproposition 2014/15:109, Stockholm, 2015, webblänk: <http://www.regeringen.se/contentassets/266e64ec3a254a6087ebe9e413806819/proposition-201415109-forsvarspolitisk-inriktning-sveriges-forsvar-2016-2020> (hämtad 2016-11-09).

Regeringen, *Nationell säkerhetsstrategi*. Stockholm, 2017, webblänk: <http://www.regeringen.se/48e36d/contentassets/a02552ad-9de94efcb84154b0f6ed76f9/nationell-sakerhetsstrategi.pdf> (hämtad 2017-01-24).

Riksrevisionen, *Digitalradio – varför och för vem?* RiR 2015:5, Stockholm, 2015, webblänk: [http://www.riksrevisionen.se/PageFiles/22004/RiR\\_2015\\_05\\_DAB\\_ANPASSAD.pdf](http://www.riksrevisionen.se/PageFiles/22004/RiR_2015_05_DAB_ANPASSAD.pdf) (hämtad 2017-01-27).

Riksrevisionen, *Teracom och marknäten – mediepolitik, monopol och krisberedskap*. RiR 2016:18, webblänk: [http://www.riksrevisionen.se/PageFiles/24952/RiR\\_2016\\_18\\_teracom\\_ANPASSAD.pdf](http://www.riksrevisionen.se/PageFiles/24952/RiR_2016_18_teracom_ANPASSAD.pdf) (hämtad 2017-02-03).



Singer, Jane B. "User-generated visibility: Secondary gate-keeping in a shared media space." *New media & society* 16.1, 2014, sidorna 55–73, webblänk: <http://journals.sagepub.com/doi/abs/10.1177/1461444813477833> (hämtad 2014-01-27).

Statens medieråd, *Ungar & medier 2015 – Fakta om barns och ungas användning och upplevelser av medier*. Stockholm, 2015, webblänk: <http://statensmedierad.se/download/18.7a953dba14fef1148cf3b32/1442841939189/Ungar-och-medier-2015.pdf> (hämtad 2016-11-09).

Strömbäck, Jesper, "Framtidens medielandskap, demokratin och den sociala sammanhållningen" i Delbetänkande av Digitaliseringskommissionen, *Om Sverige i framtiden – en antologi om digitaliseringens möjligheter*, sida 341-367, Stockholm, 2015, webblänk: [https://digitaliseringskommissionen.se/wp-content/uploads/2015/06/SOU-2015\\_65-WEBB-antologi.pdf](https://digitaliseringskommissionen.se/wp-content/uploads/2015/06/SOU-2015_65-WEBB-antologi.pdf) (hämtad 2016-11-09).

Säkerhetspolisen, *Otillåten påverkan mot medier*. Författningsskyddsensheten, 2009, webblänk: [http://www.sakerhetspolisen.se/download/18.635d23c2141933256ea1db2/1381154798498/NH\\_otillaten\\_paverk\\_medier\\_2009.pdf](http://www.sakerhetspolisen.se/download/18.635d23c2141933256ea1db2/1381154798498/NH_otillaten_paverk_medier_2009.pdf) (hämtad 2016-11-09).

ThreatConnect, *Belling the BEAR*. ThreatConnect Blog [Webbsida], publicerad 2016-09-28, webblänk: <https://www.threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/> (hämtad 2017-01-24).

Tidningsutgivarna, *Hot, våld och trakasserier mot medier*. TU, 2016, webblänk: [http://tu.se/wp-content/uploads/2016/06/Hot\\_presentation\\_2016.pdf](http://tu.se/wp-content/uploads/2016/06/Hot_presentation_2016.pdf) (hämtad 2017-01-24).

Totalförsvarets forskningsinstitut, *Hotbildsunderlag i utveckling av civilt försvar*. FOI Memo 5089, 2014, webblänk: <https://www.foi.se/download/18.2bc30cfb157f5e989c3201a/1477565924431/Hotbildsunderlag+i+utvecklingen+av+civilt+f%C3%B6rsvar.pdf> (hämtad 2016-12-07).

Weibull, Lennart, *Medieförtroende i nytt medielandskap* i Annika Bergström & Henrik Oscarsson (red). Göteborgs universitet: SOM-institutet, 2014, webblänk: [http://www.som.gu.se/digitalAssets/1487/1487705\\_119-136-lennart-weibull--medief-rtroende.pdf](http://www.som.gu.se/digitalAssets/1487/1487705_119-136-lennart-weibull--medief-rtroende.pdf) (hämtad 2017-02-03).

Westlund, Oscar, "Mognande mobil multimedia" i Oscarsson, Henrik och Annika Bergström (red.), *Mittfåra & marginal*, sida 189-200, SOM-institutet, Göteborg: Göteborgs universitet, 2014, webblänk: [http://som.gu.se/digitalAssets/1487/1487684\\_189-200-oscar-westlund--mobil.pdf](http://som.gu.se/digitalAssets/1487/1487684_189-200-oscar-westlund--mobil.pdf) (hämtad 2016-11-09).



Myndigheten för samhällsskydd och beredskap (MSB)  
651 81 Karlstad Tel 0771-240 240 [www.msb.se](http://www.msb.se)  
Publ.nr MSB1086 - mars 2017 ISBN 978-91-7383-738-5