Myndigheten för samhällsskydd och beredskap

FORSKNING/STUDIE

# Is IT safe? En studie av den publika diskursen av informationssäkerhet i Sverige

Populärvetenskaplig sammanfattning av ett postdok-projekt

**Is IT safe? En studie av den publika diskursen av informationssäkerhet i Sverige: Populärvetenskaplig sammanfattning av ett postdok-projekt**

Tidsperiod: 2017 – 2021
Utförare: Göteborgs universitet
Ansvarig: forskare/författare Max Boholm

Kort sammanfattning Projektet har undersökt hur tidningar och riksdagsdokument framställer problemet med informations- och cybersäkerhet. Undersökningen har visat vilka riskfrågor som väcks, dvs. vad som hotar vad, vilka lösningar som presenteras, hur problemformuleringen skiljer sig mellan tidningar och riksdag och hur framställningen förändrats över tid.

© Myndigheten för samhällsskydd och beredskap (MSB)
MSB:s Kontaktpersoner: Erik Sundström, 010-240 5371

Foto omslag: Thomas Henriksson

Publ. nr: MSB1802 – juli 2021

MSB har beställt och finansierat genomförandet av denna forskningsrapport (alt. studierapport). Författarna är ensamma ansvariga för rapportens innehåll.

# Innehåll

**SAMMANFATTNING** ..... **4**

**INLEDNING** ..... **5**
Om begreppen informationssäkerhet och cybersäkerhet ..... 5

**DATAINSAMLING OCH METOD** ..... **6**
Sökord och datainsamling ..... 6
Det empiriska materialet ..... 6
Analysram ..... 6

**RESULTAT** ..... **8**
Ett flerdimensionellt problem ..... 8
Likheter ..... 9
Fokus ..... 10
Skillnader ..... 11
Förändring över tid ..... 12
Tematisk förändring i media ..... 12
Tematisk utveckling i riksdagsdokument ..... 12

**RELEVANS OCH ANVÄNDNING** ..... **13**

**FÖRDJUPAD LÄSNING** ..... **14**

# Sammanfattning

Den offentliga bilden av cybersäkerhetsproblem i exempelvis nyhetsmedia och riksdagen bidrar sannolikt till att forma allmänhetens och beslutfattares uppfattningar och attityder på området. Kunskap om hur cybersäkerhet framställs i tidningar och riksdagsdokument ger därför möjligheter för aktörer, såväl offentliga som privata, att förbättra sina analyser och det stöd och den samordningen av cybersäkerhetsfrågor i samhället de kan erbjuda. För att bättre förstå vilka cybersäkerhetsrisker som uppmärksammas i det svenska samhället så har forskningsprojektet undersökt tidningar och riksdagsdokument. Projektet har fyra huvudresultat. För det första visar projektet på *cybersäkerhetsproblematikens spännvidd* i det offentliga rummet. Exempelvis framställs ett problem *för* och *från* information och informationssystem på makro-, meso- och mikronivå (med hot *för* och *från* stater, organisationer och individer). För det andra har projektet visat på stora *likheter* mellan tidningar och riksdagsdokument. Nästan alla teman för risker finns i både tidningar och riksdagsdokument. I många fall, uppmärksammas problemets delar i samma utsträckning, till exempel, sabotage, spionage, spam, bedrägerier, intrång och överbelastningsattacker. För det tredje har projektet pekat på ett antal *skillnader*. Exempelvis, politiska storskaliga hot som krig och terrorism är vanligare i riksdagsdokumenten, medan ”hackare” är vanligare i tidningarna. För det fjärde har projektet visat på *förändringar över tid*. Tidningsmaterialet uppvisar tre trender: en militarisering med ökat fokus på relationen mellan stater, ett ökat fokus på organisationer som hot, och hajper av illasinnade innovationer som till exempel spam, bedrägerier, virus och överbelastningsattacker. I riskdagsdokumenten har intresset för nästan alla teman tilltagit dramatiskt under senare år. Nästan inga teman har minskat med tiden.

# Inledning

I det moderna digitala samhället är informations- och cybersäkerhet ett växande problem. Hur tongivande samhällsaktörer framställer problemet kan tänkas vara av avgörande betydelse för hur problemet i förlängningen hanteras. För att förstå hur den publika diskursen om denna problemformulering ser ut undersöks tidningar och riksdagsdokument, som är särskilt intressanta i detta avseende.

Forskningsprojektets syfte har varit *att analysera den publika diskursen om informations- och cybersäkerhet i Sverige, mer precist tidningar och riksdagsdokument*. Med diskurs avses här den enhet av språkliga uttryck och begrepp som tillsammans bidrar till framställningen av något som varandes på ett visst (eller flera olika) sätt och som sammantaget reflekterar ett eller flera förhållningssätt till detta fenomen.

Projektet har sökt svaren på följande forskningsfrågor:

1. I vilken omfattning uppmärksammas informations- och cybersäkerhet i press och riksdagsdokument?
2. Vilka riskfrågor väcks? (Vad hotar vad?)
3. Vilka lösningar på problem presenteras?
4. Hur har framställningen av informationssäkerhet förändrats över tid?
5. Hur skiljer sig framställningen mellan tidningar och riksdag?

## Om begreppen informationssäkerhet och cybersäkerhet

Den klassiska definitionen av informationssäkerhet är skyddandet av information med avseende på dess *konfidentialitet*, *riktighet* och *tillgänglighet*.[1] I korthet, menas med definitionen att information är säker givet att man kan undvika obehörig åtkomst till den (konfidentialitet), undvika oönskad förändring av den (riktighet), och garantera att den är tillgänglig när den behövs (tillgänlighet). Begreppet cybersäkerhet är både vidare och snävare än informationssäkerhet. Under begreppet cybersäkerhet avses vanligtvis digital eller elektronisk information, inte information i allmänhet. Vidare avses ofta med cybersäkerhet skyddandet av system och användare av dessa system, såväl som användarnas intressen, inte endast informationen självt.[2] Givet den centrala roll som information har i det

[1] För en kritisk översikt av denna definition av informationssäkerhet, se Lundgren, Björn, and Niklas Möller. "Defining information security." *Science and Engineering Ethics 25* (2019): 419-441.
[2] Rossouw Von Solms och Johan Van Niekerk ("From information security to cyber security." *Computers & Security* 38 (2013): 97-102) föreslår följande definition av cybersäkerhet (min emfas): “the protection of

moderna digitala samhället, så är informationssäkerhet och cybersäkerhet i praktiken mycket nära relaterade begrepp. I en studie som denna är det därför knappast meningsfullt att försöka upprätthålla en strikt empirisk skiljelinje mellan hur det ena eller det andra framställs. Projektet undersöker således framställningen av informations- *och* cybersäkerhet, så som det fångas av ett antal nyckelord och begrepp, exempelvis *informationssäkerhet*, *dataskydd* och *cyberbrott* (se nedan).

# Datainsamling och metod

## Sökord och datainsamling

En viktig metodologisk uppgift för projektet har varit att identifiera ett relevant och noga avgränsat empiriskt material. För att lyckas med det har projektet empiriskt undersökt vilka termer som används i vardagsspråket för att beskriva cybersäkerhetsfrågor. Den empiriska undersökning finns beskriven i appendix till projektets enskilda studier och har resulterat i ett sammansatt sökuttryck, bestående av termer som till exempel (där * används för att fånga varierande ändelser för ord):

> botnet*, cyberattack*, cyberbrott*, cyberhot*, cyberkrig*, cybersäkerhet*, cyberspion*, cyberterror*, dataskydd*, datavirus*, datorintrång*, hackare*, informationsoperation*, internetattack*, internetsäkerhet*, nätbedr*, spam, virushot*, virusmask*

Det sammansatta sökuttrycket har används i Mediearkivet Retriver för att identifiera tidningsartiklar och i Riksdagens öppna data för att identifiera riksdagsdokument. Ett dokument har inkluderats i det empiriska materialet om det innehåller åtminstone tre förekomster av sökorden.

## Det empiriska materialet

Det empiriska materialet består av:

- 1269 tidningsartiklar publicerade under 1995–2019 (25 år) i *Svenska Dagbladet* ($n$ = 596), *Göteborgs Posten* ($n$ = 407) och *Aftonbladet* ($n$ = 266).
- 443 riksdagsdokument från 1979 till 2020 (42 år), närmare bestämt propositioner ($n$ = 162), betänkanden ($n$ = 96), motioner ($n$ = 75) protokoll från kammaren ($n$ = 73), svar på skriftliga frågor ($n$ = 19), interpellationer och frågor ($n$ = 18).

## Analysram

Varje dokument i det empiriska materialet har analyserats utifrån en övergripande analysram som utgår ifrån den relationella naturen hos begreppen risk och

---

*cyberspace itself*, the *electronic information*, the *ICTs* [=information and communication technologies] that support cyberspace, and the *users* of cyberspace in their personal, societal and national capacity, including any of their *interests*, either tangible or intangible, that are vulnerable to attacks originating in cyberspace".

säkerhet.[3] Den övergripande analysramen, med fyra övergripande variabler (*P*, *X*, *K* och *Y*) är:

*P* skyddar mot: *X* kan ha negativa konsekvenser *K* för värdet *Y*

Variablerna *X* och *Y* kan preciseras, med snävare begrepp som följd. Exempelvis, *hot* kan definieras som *X*, där *X* är en *avsiktlig* handling eller agenten eller instrumentet för handlingen. Tabell 1 definierar 9 analytiska kategorier i relation till variablerna *P*, *X*, *K* och *Y*.

**Tabell 1**. Analysram

| Kategori | Definition |
|---|---|
| Hot | *X* = avsiktlig |
| Misstag | *X* oavsiktlig avs. *K* |
| Olycka | *X* ≠ handling |
| Konsekvens | *K* |
| Offer | *Y* = person, organisation |
| Tillgång | *Y* = objekt |
| Svaghet | *X* = tillstånd |
| Sårbarhet | *X* = svaghet hos *Y* |
| Skydd | *S* |

**Kommentar**: Kategorierna definieras i relation till relationen: *P* skyddar mot: *X* kan ha negativa konsekvenser *K* för värdet *Y*

Dokumenten i det empiriska materialet har tolkats genom dessa analytiska kategorier (Tabell 1). Exempelvis, betrakta följande sats från *Svenska Dagbladet* (6 augusti, 2011):

> Under fem års tid har en okänd aktör brutit sig in i datasystemen på bland annat FN, Olympiska kommittén (IOC), flera länders regeringar, samt en mängd bolag.

I exemplet, ser vi till exempel att kategorin *hot* uttrycks genom ”en okänd aktör” och ”brutit sig in”. Vidare finner vi *tillgången* ”datasystemen” och ett antal *offer*, som till exempel, ”FN” och ”Olympiska kommittén”.

För varje kategori kan på detta sätt en lång rad av förekomster av varje kategori i Tabell 1 identifieras. Nästa steg i analysen har varit att identifiera teman hos förekomsterna. För hot, finns exempelvis en lång rad teman som *Attacker*, *Brottslighet*, *Intrång* och *Terrorism*. Dessa teman utgör i sin tur grunden för vidare analys: deskriptiv statistik av hur vanliga teman är och hur de är relaterade, jämförelse mellan tidningar och riksdagsdokument på basis av $\chi^2$-test (chitvå-test) och förändring över tid (relationen mellan tid och frekvens i termer av Pearsons korrelationskoefficient).

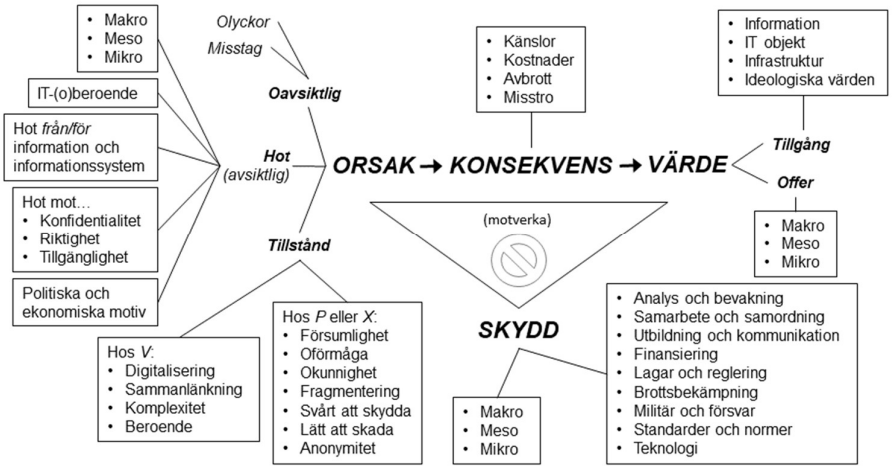
[3] Se, t.ex., Fillmore, Charles J. och Beryl T. Atkins "Toward a Frame-Based Lexicon: The Semantics of RISK and its Neighbors" i *Frames, Fields, and Contrasts* (Adrienne Lehrer, Eva Feder Kittay, Richard Lehrer, red.), Hillsdale N.J., Lawrence Erlbaum: 75-102; Baldwin, David A. "The concept of security.*" Review of International Studies* 23 (1997): 5-26; Boholm, Åsa, and Hervé Corvellec. "A relational theory of risk." *Journal of Risk Research* 14 (2011): 175-190.

# Resultat

## Ett flerdimensionellt problem

Den publika diskursen om cybersäkerhet i Sverige är mångfacetterad och realiserar en lång rad dimensioner (Figur 1). Exempelvis:

- Teman för hot, offer och skydd sträcker sig från makronivå till mikronivå. I materialet, finns risker för och från stater, organisationer och individer. Samma nivåer av samhället finns för skyddande aktörer.
- Hoten är både IT-beroende och IT-oberoende. Exempel på det senare är datorvirus, överbelastningsattacker och spam. Dessa hot finns inte utan Internet och modern IT. Exempel på IT-oberoende hot är bedrägerier och utpressning, som fanns för internet, men som i och med Internet har fått en ny utformning och omfattning.
- Problembeskrivningen inbegriper risker för konfidentialitet (t.ex. dataintrång), riktighet (t.ex. manipulation), och tillgänglighet (t.ex. överbelastningsattacker). Därmed omfattar problemformuleringen de klassiska dimensioner som uppmärksammats i samband med informationssäkerhet.
- Värden på spel är informationsbaserade (t.ex. information), materiella (t.ex. datorer och infrastruktur), ”virtuella” (t.ex. hemsidor), ideologiska (t.ex. demokrati) och ekonomiska (t.ex. pengar och kreditkort).
- Problembeskrivningen innefattar både risker *mot* information och system och risker *genom* information och system (t.ex. kriminell handel på ”mörka nätverk” och desinformationskampanjer).
- Problembeskrivningen innefattar hot med politiska (t.ex. terrorism och krig) och ekonomiska (t.ex. kriminalitet) motiv.
- Problembeskrivningen innefattar polisära, militära, legala, ”mjukt” normativa (t.ex. strategier), informerande och utbildande, kooperativa, finansiella, och tekniska lösningar på problemet.




Figur 1. En flerdimensionell diskurs (dimensioner och underkategorier).

Spännvidden av problembeskrivningen är intressant i jämförelse med forskningslitteraturen om cybersäkerhet.[4] I den framhävs ofta en likande bredd av risker. Med andra ord speglar den publika diskursen i Sverige de problem som uppmärksammats i forskningen och således är denna diskurs en möjlig källa för allmänheten att uppmärksamma relevanta cybersäkerhetsproblem.

# Likheter

Trots den omfattande variationen av teman i tidningar och riksdagsdokument, så finns det stora likheter mellan hur cybersäkerhetsfrågor framställs. Det är i stort sätt samma typer av teman som väcks i tidningsartiklarna som i riksdagsdokumenten. Den huvudsakliga avvikelsen i detta avseende är att dåvarande Folkpartiet (FP) beskrivs som en illasinnad aktör (d.v.s. ett hot) i tidningsartiklarna, i samband med dataintrånget 2006, då medlemmar av FP tog sig in i Socialdemokraternas intranät. FP som hot förekommer inte i riksdagsdokumenten.

I tillägg till de omfattande kvalitativa likheter som identifierats gäller även att många teman uppmärksammas i samma utsträckning i tidningar och riksdag. Framförallt gäller detta teman för hot, tillgångar och offer. Tabell 2, sammanfattar resultaten i detta avseende.

I jämförelse med tidigare forskning av andra länder (fr.a. USA), så kan man sluta sig till stora likheter med de teman som uppmärksammas i den svenska diskursen. Sammantaget, ger detta upphov till de generella slutsatserna att den svenska diskursen om cybersäkerhet är relativt enhetlig (avseende media och riksdag) och del av en global relativt enhetlig diskurs om cybersäkerhet.

[4] Se t.ex. Singer, Peter Warren och Allan A. Friedman *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2014.

**Tabell 2**. Exempel på hot, tillgångar och offer där det inte finns några signifikanta eller endast marginella skillnader mellan tidningar och riksdag

| Kategori | Hot | Tillgång, offer |
|---|---|---|
| Ingen signifikant skillnad | botnät, sabotage, spionage, utpressning, bedrägerier, intrång, överbelastningsattacker, barnpornografibrott, spam, och övervakning | databaser, nätverk, regeringen, kommuner, militären, och media |
| Marginell skillnad | attacker, kriminell handel, företag, brottslighet, och stölder | banker, myndigheter, information, nationer, användare, filer, och hemligheter |

**Kommentar**: *Ingen signifikant skillnad* definieras av ett icke-signifikant $\chi^2$-test. En *marginell skillnad* är en där effektstorleken ($\phi$) är mindre än 0,10 (se publikationer under *Fördjupad läsning* för detaljer).

# Fokus

Vissa teman är vanligare än andra. Särskilt, kan man notera följande fokus i det empiriska materialet:

- Det är större fokus på avsiktliga risker (hot) än oavsiktliga (misstag, olyckor). Medan nästan alla tidningsartiklar och riksdagsdokument uttrycker hot av olika slag, så är andelen andel artiklar och dokument som uttrycker misstag och olyckor betydligt mindre.
- Det är större fokus på orsaker än konsekvenser. Nästan alla tidningsartiklar och riksdagsdokument uttrycker orsaker till oönskade händelser, men en betydligt mindre andel diskuterar konsekvenserna själva.
- Särskilt kan man notera ett begränsat fokus på ekonomiska konsekvenser: kostnader. I endast 9% av både tidningsartiklarna och riksdagsdokumenten framställs kostnader som en oönskad konsekvens.
- Det är större fokus på risker *för* information (t.ex. intrång och manipulering av data) och system än risker *genom* information och system (t.ex. barnpornografibrott och kriminell handel på ”mörka” nätverk).
- Det är nästan uteslutande fokus på externa hot, medan intresset för insider-brott är marginellt (4% respektive 3% av tidningar och riksdag).

I relation till tidigare forskning kan en mer allmän slutsats framhävas. I tidigare forskning har storskaliga hot med förödande konsekvenser visat sig vara en central del i hur cybersäkerhetsproblemet definierats av politiker och regeringar (fr.a. med fokus på USA).[5] Den svenska diskursen som undersökts i detta projekt har tydliga inslag av sådana teman, men är långt ifrån begränsad till denna problematik. I jämförelse med tidigare forskning om cybersäkerhetsdiskursen i USA, förefaller den problemformulering i svenska nyheter och riksdag mer moderat.

[5] Se t.ex. Dunn Cavelty, Myriam *Cyber-Security and Threat Politics: Us Efforts to Secure the Information Age*. London: Routledge, 2008.Lawson, Sean *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. New York: Routledge, 2020.

## Skillnader

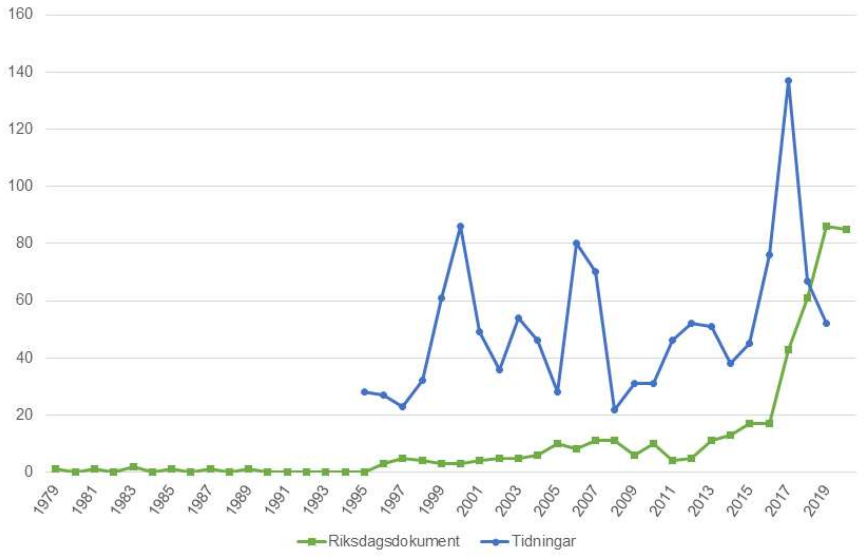
Trots stora likheter, så finns vissa skillnader mellan tidningar och riksdag. Framförallt, kan följande skillnader noteras:

- Det är större fokus på de politiskt motiverade hoten krig, terrorism och desinformation i riksdagsdokumenten än i tidningsartiklar.
- Även förödande konsekvenser (”kriser”, ”katastrofer” m.m.) är vanligare i riksdagsdokument än tidningsartiklar (notera dock att temat är relativt ovanligt även i riksdag: 9%, jämfört med 2% i tidningar).
- Den skyddande dimensionen (t.ex. lagar, militär, underrättelse, utbildning, och samarbeten) är vanligare och mer differentierad med högre frekvens för fler teman, i riksdag än i tidningar. Exempel på teman där det finns större skillnader är samarbeten och samverkan, lagar och reglering, statlig styrning och militär och försvar.
- I tidningarna finns ett stort fokus på ”hackare”, då nära hälften av tidningsartiklarna uttrycker detta hot, men detta tema är marginellt i riksdagsdokumenten (knappt en tiondel). Tolkningen av det flertydiga ordet hackare, med positiva och negativa betydelser, har således i nyhetsrapporteringen växt fram som en av de huvudsakliga hoten, men denna stereotyp har inte haft samma betydelse för det mer formella språkbruket i riksdagens dokument.
- I tidningarna finns ett större fokus på individer som hot än i riksdagsdokumenten.
- Det är i riksdagsdokumenten större fokus på abstrakta ideologiska värden som frihet, demokrati, rättigheter och individens integritet än i tidningsartiklar.
- Riksdagens dokument framhäver infrastruktur och ”samhällets funktionalitet” som hotade tillgångar i större utsträckning än tidningsartiklar. Riksdagsdokumenten uttrycker även ”samhället” som en hotad tillgång i större utsträckning än tidningsartiklar.
- I tidningarna finns ett större fokus på de vardagliga IT-objekten datorer, lösenord och hemsidor än i riksdagsdokumenten.

Sammantaget kan dessa skillnader sammanfattas under två övergripande dimensioner: *abstraktion* och *skala*. Riksdagsdokumenten tenderar att betona storskaliga politiska hot, abstrakta tillgångar och offer på makronivå i större utsträckning än tidningsartiklarna. Tidningarna tenderar att fokusera individuella hot och vardagliga tillgångar i större utsträckning än riksdagsdokumenten.

# Förändring över tid

I både tidningar och riksdag har intresset för cybersäkerhet ökat över tid, men utvecklingen ser olika ut (Figur 2). Riksdagsdokumenten uppvisar ett svagt tilltagande intresse för cybersäkerhet fram till 2016, men en kraftig ökning från 2017. I mediematerialet finns ett fluktuerande intresse för cybersäkerhet med flera toppar och dalar.




Figur 2. Förändring över tid.

## Tematisk förändring i media

I pressen har tre trender identifierats. För det första, finns i mediematerialet en ökande *"statifiering"* och *militarisering*, med ett ökat fokus på nationer, krigsföring, informationsoperationer, spionage, och underrättelsetjänster som hot.

För det andra finns en process med ökad *"organisation-ifiering"* med ökat fokus på organisationer, företag, och myndigheter som hot. Omvänt, finns ett avtagande intresse för individer som hot.

För det tredje finns i mediematerialet flera *hajper*, med stort intresse, under begränsad tid för virus, spam, bedrägerier, överbelastningsattacker, och utpressning. T.ex. problematiken med datorvirus är som mest framträdande under 1999 till 2005, med rapporter om de globala virusen Melissa, I love you och Sobig, men även under senare år i och med det globala utpressningsviruset Wannacry. Andra exempel är spam (skräp-epost) och nätbedrägerier, som båda är mest framträdande under 2000-talets första decennium. .

## Tematisk utveckling i riksdagsdokument

Alla teman i uppvisar riksdagsmaterialet en ökande trend för perioden 1979-2020. För snävare tidsperioder (2001-2020 och 2011-2020), så har inte alla teman en

signifikant ökande trend, men endast spam (hot) minskar över tid (nämligen under 2011-2020). En slutsats om riksdagsmaterialet är således att teman för problemformuleringen av cybersäkerhet har ackumulerat över tid, snarare än att huvudintresset för teman har bytts ut mot andra.

# Relevans och användning

Informations- och cybersäkerhet inbegriper många olika aspekter. För att förbättra informations- och cybersäkerheten i samhället krävs därför en helhetssyn som inte enbart fokuserar på utveckling av de tekniska aspekterna av informationssystem, utan även avser öka förståelsen av sociala och psykologiska aspekter. Den mänskliga faktorn har alltmer framhävts som en nyckelkomponent i cybersäkerhetsarbete. Många gånger är användaren den svagaste länken i informationssäkerhet. I slutändan är användarens beslut avgörande för systemets säkerhet. Givet ett helhetsperspektiv är kunskap om användares medvetenhet och uppfattning om informationssäkerhet viktig för att uppnå säkra informationssystem. Flera faktorer kan i sin tur påverka användares medvetenhet och uppfattning om informations- och cybersäkerhet. En sådan faktor är i vilken utsträckning informationssäkerhet uppmärksammas i samhället, samt på vilket sätt som informationssäkerhet framställs av olika samhällsaktörer. Nyhetsmedia kan tänkas vara en särskilt viktig aktör för den allmänna framställningen av informationssäkerhet i samhället. Trots det har nyhetsmedias roll sällan undersökts. En annan viktig aktör i denna framställning är den politiska sfär som utgörs av Riksdagen, Sveriges högsta beslutande organ. Hur problemet framställs i riksdagen kan tänkas ha avgörande betydelse för hur problemet uppfattas och hanteras i andra delar av samhället.

Detta projekt har varit ett första steg mot att bättre förstå cybersäkerhetsdiskursen i Sverige, vilket i förlängningen kan bidra till att förstå hur nyhetsmedia och politisk kommunikation bidrar till cybersäkerhet.

Att besvara empiriska frågor om orsakerna till och konsekvenserna av diskursen är bortom syftet för detta projekt, men projektets resultat är relevanta för fortsatt arbete med dessa frågor. För det första, givet ett *kritiskt perspektiv* är det relevant att fråga hur den publika framställningen av cybersäkerhet överensstämmer med objektiva riskbedömningar av cyber-faror. Ett sådant upplägg skulle kunna identifiera över- och underdrifter i den publika diskursen, vilka sin tur skulle kunna adresseras i särskilda informationsinsatser för att förbättra kunskapen om cybersäkerhet i samhället. Resultat från projektet med särskilt intresse i detta avseende är:

- Den publika diskursen om informations- och cybersäkerhet domineras av ett fokus på *avsiktliga* risker (här definierade under termen *hot*).
- Denna diskurs uppvisar fr.a. fokus på *externa* hot, men det är minimalt intresse insider-problematik.

- Det är betydligt mycket större fokus på möjliga *orsaker* till negativa konsekvenser än på konsekvenserna själva. Särskilt kan ett begränsat fokus på kostnader konstateras.
- Diskursen innehåller i stor utsträckning *dramatiska ordval* som ”krig”, ”attacker” och ”terrorism”.

I samtliga dessa avseenden är det långt ifrån självklart att diskursen motsvarar de verkliga problemen på området.

För det andra är projektets resultat relevanta för vidare kunskapsinhämtning om diskursens möjliga *konsekvenser för allmänhetens och beslutfattares förståelse av cybersäkerhetsproblem*. I detta avseende kan särskilt tre resultat uppmärksammas.

- Tidningsmaterialet uppvisar en tilltagande ”statifiering” och militarisering. En relevant fråga att ställa är vilka konsekvenser dessa processer har för allmänhetens uppfattningar av problemen med cybersäkerhet. Psykologisk forskning visar på betydelsen av närhet för beslutsfattande.[6] När personer upplever ett psykologiskt, socialt eller geografiskt avstånd till problemet är de mindre motiverade att lösa problemet. Möjligen finns det en risk att det ökade intresset på storskaliga hot och konflikter mellan stater, ökar individers upplevda avstånd till problemet och därmed deras benägenhet till skyddande åtgärder.
- I riksdagsdokumenten och i tilltagande omfattning i tidningar finns ett fokus på andra stater, krig, och spionage som hot. En relevant fråga att ställa är hur denna ”konfliktifiering” påverkar de lösningar man ser och prioriterar på området, särskilt då hanteringen av många cybersäkerhetshot kräver internationella samarbeten.
- Cybersäkerhetsdiskursen i Sverige är mångfasetterad och spretig. Givet denna variation är det relevant att fråga vilka konsekvenser den breda variation har för förståelsen av problemet och dess lösningar. Den innehåller många olika dimensioner, som inte självklart kan hanteras på ett och samma sätt. Möjligen ger bredden i diskursen upphov till en oprecis problemformulering. Denna utmaning bör tas i särskilt beaktande vid informationsarbete där mottagarens bakgrundsförståelse är av avgörande betydelse eller i samverkan där olika aktörers gemensamma förståelse för problemet bör säkerställas.

# Fördjupad läsning

Boholm, Max. ”Twenty-five years of cyber-threats in the news: a study of Swedish newspaper coverage (1995–2019)”. Under granskning.

[6] T.ex. Kostyuk, Nadiya och Carly Wayne "The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public." *Journal of Global Security Studies* 6 (2021): ogz077.

Boholm, Max. ”The multidimensional problem of cybersecurity in politics: A text analysis of Swedish Government documents (1979-2020)”. Under granskning.

Boholm, Max.”A shared agenda? Cybersecurity representations in Swedish newspaper and government documents”. Under granskning.

**Myndigheten för samhällsskydd och beredskap (MSB)**
651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1802 – juli 2021 ISBN ISBN