Att utveckla och implementera cybersäkerhetspolicy

Lärdomar från den finansiella sektorn

Ulrik Franke

Developing and implementing cybersecurity policy: Lessons from the financial sector

Modern society is increasingly dependent on digital services, making their dependability a top priority. But while there is a consensus that cybersecurity is important, there is no corresponding agreement on the true extent of the problem, the most effective countermeasures, or the proper division of labor and responsibilities. This makes cybersecurity policy very difficult. This article addresses this issue based on observations and experiences from a period of guest research at the Swedish Financial Supervisory Authority *(Finansinspektionen)*, which made it possible to study how cybersecurity policy is developed and implemented in the Swedish financial sector. Observations include policy implementation challenges related to squaring different roles and perspectives mandated by different laws, and to collaboration between independent government authorities, but also policy development challenges: How can the full range of perspectives and tools be included in cybersecurity policy development? As Sweden now revises its cybersecurity policy, this is a key issue.

1. Inledning

Det moderna samhället blir alltmer beroende av digitala tjänster. I mångt och mycket är det en positiv utveckling, där nya tekniska lösningar dels möjliggör arbets- och tidsbesparingar, dels skapar helt nya möjligheter. Få vill tillbaka till att betala räkningar på bankkontor med begränsade öppettider – få vill undvara AI i jakt på nya mediciner eller material. Men ju mer vi använder de digitala verktygen, desto viktigare blir det att de är säkra och pålitliga. Konsekvenserna

Ulrik Franke är verksam vid RISE Research Institutes of Sweden och som adjungerad professor vid KTH. Den aktuella studien är finansierad av Stiftelsen för Strategisk Forskning (avtalsnummer SM22-0057).
E-post: ulrik.franke@ri.se

av avbrott och andra incidenter kan bli stora – det räcker att läsa de senaste årens medierapportering om händelser som REvil-angreppet i juli 2021 som i Sverige stängde ner hundratals Coop-butiker (Luks 2021) eller det utpressningsvirus som drabbade Kalix kommun i december samma år (Oscarsson 2021).

Sådana händelser omtalas ofta i tekniska termer – vad som skedde, vilket skydd som kunde eller inte kunde ha hjälpt, vilka åtgärder som nu vidtas. Det är uppenbart att detta är ett rimligt perspektiv. Cybersäkerhet är till stor del en teknisk fråga. Samtidigt är det inte *enbart* en teknisk fråga. Incidenterna sker i sammanhang som också är organisatoriska, ekonomiska, juridiska etc. och effekterna är inte bara tekniska och fysiska utan kan även vara psykologiska, såsom ett förändrat synsätt på en bransch eller tillit till samhället. Om man betraktar de initiativ som på senare år har tagits för att förbättra det svenska samhällets cybersäkerhet så rör det sig i inte så liten omfattning om nationella lagar och förordningar som säkerhetsskyddslagen och den återupptagna totalförsvarsplaneringen samt om EU-lagstiftning som GDPR,[1] NIS och NIS 2,[2] cybersäkerhetsakten och DORA[3] för den finansiella sektorn. Det är tydligt att sådan cybersäkerhetspolicy fruktbart kan studeras ur en mångfald av olika samhällsvetenskapliga perspektiv.

Cybersäkerhetspolicy är intressant att studera inte minst eftersom det å ena sidan närmast råder konsensus om att cybersäkerheten är viktig, men å andra sidan råder stor osäkerhet kring hur stora problemen egentligen är, vad som är de mest effektiva verktygen för att möta dem och inte minst vem som egentligen har – eller borde ha – vilket ansvar (se vidare litteraturöversikten nedan). Området befinner sig just nu i en utvecklingsfas, där man möjligen kan vänta sig konvergens och ökad mognad med tiden, men där mycket just nu flyter. Som ett konkret och aktuellt exempel kan nämnas att det svenska Nationella cybersäkerhetscentret (NCSC) som etablerades 2020 i form av samverkande självständiga myndigheter med bibehållna egna mandat, nyligen kritiserades av Riksrevisionen som en ”åtgärd med svagt resultat” (Riksrevisionen 2023, avsnitt 3.3.1) och nu enligt regeringen ska omorganiseras under FRA:s huvudmannaskap (Kristersson m.fl. 2023; Försvarsdepartementet 2023). Samtidigt aviserades att regeringen under 2023 skulle påbörja arbetet med en ny nationell informations- och cybersäkerhetsstrategi.

Den här artikeln syftar till att belysa en viktig delmängd av detta område: cybersäkerhetspolicy för den finansiella sektorn. Utgångspunkten är en gästforskningsvistelse på Finansinspektionen (FI), som har möjliggjort att på nära håll följa sektorns policyarbete med cybersäkerhet i praktiken. Detta är intressant i sig, eftersom den finansiella sektorn är så viktig för samhället

1 General Data Protection Regulation.

2 Directive on Security of Network and Information Systems.

3 Digital Operational Resilience Act.

(tillgången till finansiella tjänster är ofta helt nödvändig för de vardagliga behoven hos hushåll och företag). Men det är också intressant ur ett mer generellt perspektiv och de konkreta frågeställningar som studeras är valda – åtminstone delvis – i syfte att vara av intresse bortom den finansiella sektorn:

1. Hur förenar FI sina olika roller med bäring på cybersäkerhet?
2. Hur navigerar FI mellan de skilda synsätt på cyberrisk som myndigheten behöver anamma i sina olika roller?
3. Hur hanterar FI målsättningen att göra sin tillsyn inom cybersäkerhet mer datadriven och automatiserad?
4. Hur hanterar FI sin roll som självständig myndighet med specifika mandat i samverkan med andra självständiga myndigheter med egna mandat när cybersäkerheten kräver gemensamt arbete?

Som framgår av litteraturöversikten nedan har dessa frågeställningar motsvarigheter hos andra myndigheter, i andra sektorer och även i andra länder. Eftersom cybersäkerhetspolicy kräver samarbete mellan statlig och privat sektor, mellan olika departement, mellan myndigheter under regeringen och under riksdagen etc. bedöms iakttagelserna från FI vara av bredare intresse.

Efter en kort terminologisk anmärkning ger nästa avsnitt en översikt över befintlig litteratur; internationell och svensk. Därefter följer en kort metodbeskrivning, varpå huvudbidraget görs i form av iakttagelser och identifierade utmaningar. Artikeln avslutas med en diskussion av vad som krävs för att utveckla och implementera god cybersäkerhetspolicy. Denna slutdiskussion kan ses som ett försök att besvara eller åtminstone belysa en fundamental bakomliggande fråga: Varför är det så svårt att utveckla och implementera god cybersäkerhetspolicy?

1.1 KORT OM TERMINOLOGI

Informationssäkerhet är en bred term som handlar om att rätt information (*riktighet*) – oavsett om den finns i digitala system eller ej – ska vara tillgänglig (*tillgänglighet*) för den som ska ha den men inte för andra (*konfidentialitet*). *Cybersäkerhet* var tidigare en smalare term som användes om säkerheten i den sorts styr- och reglersystem som kontrollerar fysiska processer exempelvis i elnätet, fordon eller fabriker. På senare år har användningen av cybersäkerhetsbegreppet dock breddats så att det numera ofta används synonymt med all sorts informationssäkerhet. I EU:s cybersäkerhetsakt avser cybersäkerhet exempelvis de tre egenskaperna ovan tillsammans med *autenticitet* (att ett objekt är vad det utger sig för att vara) och tillämpas brett för certifiering av produkter, tjänster och processer. Ibland, inte minst i officiella dokument från svenska myndigheter, används begreppen tillsammans

– *informations- och cybersäkerhet* – så att den breda betydelsen framgår. I det följande används dock begreppet cybersäkerhet i bred bemärkelse och inkluderar arbete mot incidenter till följd av såväl angrepp som slarv eller olyckor. För en bra begreppsdiskussion, se von Solms & van Niekerk (2013).

2. Tidigare forskning

I takt med att cybersäkerhetsfrågorna har fått alltmer uppmärksamhet har de naturligtvis också rönt ökat akademiskt intresse. Av naturliga skäl är mycket av denna forskning teknikvetenskaplig, men det finns också en stadigt växande samhällsvetenskaplig litteratur som snarare anlägger ett policyperspektiv på cybersäkerhetsfrågorna. I det följande identifieras först fem återkommande temata ur den internationella litteraturen, varpå litteraturen om svenska förhållanden introduceras i relation till dessa.

2.1 DEN INTERNATIONELLA LITTERATUREN

Policy och nationell strategi för cybersäkerhet är ett mångfacetterat område. Vissa forskare, som Bruijn & Janssen (2017), menar att det inte bara är komplext, abstrakt och svårfångat, utan rentav stundtals paradoxalt, exempelvis för att vi alltid inte vet vem som är motståndaren, hur och till vilken kostnad vi borde skydda oss, hur mycket som borde offentliggöras, eller vem som borde göra vad. I samma anda omtalas cybersäkerhetspolicy inte sällan som ett så kallat *wicked problem* (Carr m.fl. 2020; Hauser 2023); alltså ett problem som är svårt att formulera och lösa på något invändningsfritt och heltäckande vis.

Harknett & Stever (2011) konstaterar, i amerikansk kontext, att samhällsutvecklingen kräver en sammanhängande nationell cyberpolicy, men menar – med stöd av granskningar från Government Accountability Office – att vare sig Bush- eller Obama-administrationernas publicerade strategidokument nådde upp till sina målsättningar. En av de stora utmaningarna handlar om vem – centrala statsledningen, myndigheter, privata företag – som egentligen ska göra vad (Bronk & Conklin 2022). Denna splittring av ansvar och beslutsmandat har pekats ut som det främsta problemet på hela cyberområdet (Dunn Cavelty & Wenger 2020). Är cybersäkerheten ett civilt eller militärt problem? Ett nationellt eller internationellt? Ett ekonomiskt eller ett rättsligt? Ska arbetet ledas uppifrån högsta ort eller decentraliserat nerifrån-och-upp? Backman (2023) konstaterar, i EU-kontext, att i takt med att unionens ambitioner på cyberområdet har växt så har ett äldre riskperspektiv – där det gäller att bygga robusta och resilienta system – kommit att samexistera med ett allt oftare använt hotperspektiv – där det gäller att skydda sig mot angripare (så kallad *securitization*), vilket har lett till visst gnissel mellan medlemsstaterna. Oklarheterna kring vem som är med och vilket perspektiv som ska råda har också lett vissa forskare att applicera eller åtminstone överväga den välkända

så kallade *garbage can*-teorin om organiserade anarkier (Cohen m.fl. 1972) på cybersäkerhetspolicyområdet (Patacsil 2021; Valeriano & Jensen 2021).

Kuerbis & Badiei (2017) argumenterar för att den hierarkiska ansatsen har en begränsad roll och att en mer decentraliserad nätverksmodell ofta är effektivare. Att i praktiken få till stånd sådana nätverk, där myndigheter på ett fruktbart sätt samarbetar med företagen i samhällsviktiga sektorer – betalningar, elförsörjning, vatten och avlopp, etc. – för att höja cybersäkerheten är dock inte alltid lätt. Atkins & Lawson (2021) sluter sig, baserat på intervjuer med berörda intressenter, till att de uppnådda resultaten varierar betänkligt mellan de olika (amerikanska) sektorerna. Några framgångsfaktorer tycks vara att ansvarig myndighet har en god och förtroendefull relation till sin sektor, relevant cyberexpertis och tillräckligt med resurser för att faktiskt hjälpa företagen. Något som kan vara såväl otydligt som konfliktskapande i sådana samarbeten är vem som egentligen är ansvarig för vad. Typiskt är det de privata aktörerna själva som är ansvariga och myndigheternas roll snarare att vara stödjande – eller inspekterande.

I linje med tanken att splittrat ansvar är det stora problemet (Dunn Cavelty & Wenger 2020) föreslås det i litteraturen ibland förändrade ansvarsförhållanden – exempelvis att mindre ansvar borde läggas på enskilda individer (Renaud m.fl. 2020) eller att incitamentsskapande juridiskt ansvar borde läggas på den som har möjlighet att faktiskt åtgärda ett problem (Moore 2010). Eftersom cybersäkerhet kräver samarbete mellan många aktörer som var och en kan ha sin egen agenda är sådana incitamentsfrågor ständigt närvarande i litteraturen (se t.ex. Dynes, Goetz & Freeman 2008; Bauer & Eeten 2009; Rodin 2015). Anderson & Moore (2006) hävdar i en välciterad artikel i *Science* att incidenter sker minst lika ofta på grund av dåliga incitament som på grund av dålig design. Att korrigera sådana dåliga incitament är något av ett ledmotiv i litteraturen om cybersäkerhetsekonomi. Ett exempel är den litteratur som jämför dålig cybersäkerhet med negativa externaliteter som miljöfarliga utsläpp – ett resonemang som pekar på risken att enskilda aktörer investerar för lite i säkerhet eftersom de själva inte bär hela kostnaden för de incidenter som kan uppstå (Gordon m.fl. 2014; Sales 2012: 1525–1528).

Några översiktsarbeten som mer systematiskt belyser den växande floran av nationella och multinationella cybersäkerhetsstrategier är Luiijf, Besseling & De Graaf (2013), Sabillon, Cavaller & Cano (2016), Štitilis, Pakutinskas & Malinauskaitė (2017) och Manjikian & Romaniuk (2021).

Utan anspråk på fullständighet så kan den internationella litteraturen sammanfattas i fem gemensamma – delvis överlappande – temata:

1. För det första att området är mångfacetterat och öppet för olika tolkningar, inte minst eftersom tekniska och icke-tekniska aspekter samspelar på ett icke-trivialt sätt (Harknett & Stever 2011; Bruijn & Janssen 2017; Manjikian & Romaniuk 2021: 1–7).

2. För det andra att det ofta råder osäkerhet om vilka myndigheter och politikområden som har eller borde ha (tolknings-)företräde (Bronk & Conklin 2022; Bruijn & Janssen 2017). Exempelvis kan ett hotperspektiv på cyberfrågorna samexistera med ett riskperspektiv (Backman 2023).

3. För det tredje att cybersäkerhet på nationell nivå handlar om ett flertal kritiska infrastrukturer som ägs och sköts av en stor och heterogen uppsättning aktörer, såväl privata som offentliga, och att alla dessa på något vis måste inkluderas (Harknett & Stever 2011; Kuerbis & Badiei 2017; Atkins & Lawson 2021).

4. För det fjärde komplikationer relaterade till incitament och negativa externaliteter (Anderson & Moore 2006; Moore 2010; Sales 2012; Gordon m.fl. 2014).

5. För det femte svårigheter att snabbt och adekvat fånga upp och förstå hela bredden av de snabbt föränderliga cyberhoten (Renaud m.fl. 2020; Atkins & Lawson 2021).

Som framgår i det följande är dessa temata lika närvarande och relevanta i svensk kontext.

2.2 STUDIER AV SVENSKA FÖRHÅLLANDEN

Ett relativt tidigt exempel på en studie av policysvårigheterna på cyberområdet är Nicanders doktorsavhandling (2015) som undersöker processen från att nya hot upptäcks till det att nödvändiga skyddsåtgärder implementerats och specifikt hur detta kan snabbas upp. I ett delarbete studeras svensk politik för skydd av kritisk infrastruktur under perioden 1995–2002 i kontrast mot andra länder (Nicander 2010). Slutsatsen är att den svenska förvaltningsmodellen med regeringens kollektiva beslutsfattande (kontrasterad mot norskt ministerstyre) och många uppgifter fördelade på självständiga myndigheter (kontrasterad mot brittiskt och australiensiskt arbete med så få departement och myndigheter som möjligt inblandade) bromsade den svenska policyimplementationen. Detta ligger väl i linje med temata två och fem ovan.

Några studier som illustrerar kontexten i vilken svensk cybersäkerhetspolicy utformas handlar om hur aktörer i privat sektor ser på hoten och vilka åtgärder de vidtar. Kävrestad & Huskaj (2021) intervjuade fem svenska civila cybersäkerhetsexperter om deras syn på offensiva cyberoperationer från främmande makt och kunde konstatera att informanternas förståelse var begränsad – eller åtminstone att deras uppfattningar var motstridiga. En mer kvantitativ undersökning av cybersäkerheten i svensk tillverkningsindustri gjordes av Franke & Wernberg (2020). Resultaten pekar på att företagen använder grundläggande tekniska säkerhetsåtgärder i ganska stor omfattning, men att användandet av mer organisatoriska åtgärder (som kontinuitetsplaner, utbildningar av de

anställda eller övningar för att förbättra planer och färdigheter) är mycket mindre vanligt. Dessa båda studier illustrerar hur utmaningen i det tredje temat ovan ser ut i svensk kontext. En studie inriktad på cybersäkerheten i den svenska finansiella sektorn är Varga, Brynielsson & Franke (2021). Utifrån enkäter och intervjuer med deltagare i en stor sektorsövergripande övning som omfattade såväl företag som myndigheter görs iakttagelsen att respondenterna sällan är särskilt intresserade av hotinformation om exempelvis angriparnas beteende. Fokus ligger snarare på tekniska aspekter. Åtminstone i den aktuella övningen dominerade alltså riskperspektivet över hotperspektivet (jämför Backman 2023), vilket kan ses som en illustration av temata ett och två ovan. Det framgick också att det fanns en förväntan bland de privata aktörerna om att få information från framförallt MSB,[4] Säpo, Polisen och Finansinspektionen (Varga, Brynielsson & Franke 2021, avsnitt 5.1.7), vilket återigen illustrerar tema tre ovan.

Naarttijärvi (2019) analyserar ur ett juridiskt perspektiv de olika krav på obligatorisk rapportering av incidenter som införts i svensk rätt på senare år genom säkerhetsskyddslagen, krisberedskapsförordningen (nu upphävd), NIS och GDPR. Diskussionen om eventuella målkonflikter i och mellan systemen för incidentrapportering illustrerar framförallt tema två ovan.

Boholm (2021) har studerat hur diskussionen om dator-, IT, informations- och cybersäkerhet har sett ut i den svenska offentliga debatten sedan mitten av 1990-talet. Blotta mångfalden i de tidningstexter som har studerats illustrerar det första temat ovan, men resultaten knyter också an till temata två och tre genom att påvisa hur cybersäkerhet, eller bristen därpå, över tiden alltmer kommit att förknippas med stater, myndigheter och organisationer.

Svan m.fl. (2024) har genom litteraturstudier och intervjuer studerat statsförvaltningens arbete med informations- och cybersäkerhetsarbete. I linje med temata 1 och 2 ovan finner de såväl oklarheter i definitioner som otydlig ansvarsfördelning. I linje med temata 3 och 5 finner de därutöver bristande återrapportering.

Utöver de akademiska studierna har också Riksrevisionen genom en serie granskningar belyst hur svensk cybersäkerhetspolicy formuleras och implementeras, vilket tematiskt är det som ligger närmast den föreliggande studien. En granskning från 2014 av regeringen samt dess stöd- och tillsynsmyndigheter menade att informationssäkerhetsarbetet inte var ändamålsenligt. Specifikt riktades kritik mot regeringens avsaknad av samlad lägesbild av vare sig hot, incidenter eller åtgärder i statsförvaltningen. Bland rekommendationerna återfanns förslaget att inrätta ”en funktion och en process i Regeringskansliet med syfte att samlat hantera informationssäkerheten” (Riksrevisionen 2014: 13). I en granskning av informationssäkerhetsarbetet på nio myndigheter ett par år

4 Myndigheten för samhällsskydd och beredskap.

senare fann Riksrevisionen allvarliga brister både i myndigheternas arbete och i regeringens styrning (Riksrevisionen 2016).

I en ny granskning 2023 menade Riksrevisionen ånyo att regeringens arbete för att stärka Sveriges informations- och cybersäkerhet inte har varit effektivt. Specifikt har samordningen brustit, näringslivet har inte involverats tillräckligt och myndighetsstyrningen har utgått från de enskilda departementens mål och prioriteringar snarare än sammanvägda avvägningar av vad som är bäst för Sverige (Riksrevisionen 2023). Denna kritik ligger väl i linje med temata ett, två, tre och fem från den internationella litteraturen ovan.

Intressant är också att det fjärde temat – incitament, externaliteter och liknande nationalekonomiska perspektiv – för första gången lyfts i revisionsrapporten från 2023. Genom ett långt citat från Franke (2020: 50) lyfter Riksrevisionen möjligheten att effektivt förbättra samhällets cybersäkerhet genom kloka incitamentsjusteringar (Riksrevisionen 2023: 35).

3. Metod

Datainsamlingen till den föreliggande studien har i huvudsak genomförts under en ettårig gästforskningsvistelse på halvtid vid Finansinspektionen (FI) under 2023, även om vissa iakttagelser gjordes redan under 2022, inom ramen för ett stöduppdrag utan forskningsambition. Gästforskningsvistelsen hade två övergripande syften: Dels att ge FI tillgång till forskningskompetens i skärningspunkten mellan cybersäkerhet och ekonomi för att stärka den egna verksamheten, dels att skapa möjlighet till praktiknära forskning av hög relevans. Dessa förutsättningar har å ena sidan skapat möjligheter till unik insyn i pågående arbete, men å andra sidan också medfört begränsningar i vilken sorts forskning som varit möjlig att bedriva.

Konkret har arbetet alltså alltid varit samskapande, närmast att beteckna som aktionsforskning: I enlighet med det första syftet har diskussioner förts, texter eller bildspel tagits fram och återkoppling lämnats på befintliga underlag inom olika projekt och processer nästan som om det inte funnits något forskningssyfte. Samtidigt har, i enlighet med det andra syftet, urvalet av dessa projekt och processer för deltagande delvis skett utifrån deras forskningspotential och anteckningar har löpande förts i syfte att dokumentera iakttagelser för därpå följande analys som i sin tur informerat nästa urval. I detta svarar metoden ganska väl mot en aktionsforskningscykel (Kemmis, McTaggart & Nixon 2014). Forskaren har otvivelaktigt påverkat de processer som studerats, men deltagandet har också gett en helt annan förståelse för dessa än vad ett passivt utifrån-studerande skulle ha gjort (för en djupare diskussion av detta närmast hermeneutiska inslag i aktionsforskning, se Smits 1997). Samskapande ses ofta, begränsningarna till trots, som en viktig del av hur statsvetenskaplig

forskning kan få samhälleligt genomslag, inte minst när den sker tillsammans med myndigheter (Vetenskapsrådet 2021: 42).

De huvudsakliga projekt och processer som har deltagits i och studerats är (i) övergripande cybersäkerhetsstrategiarbete inom ramen för det finansiella stabilitetsrådet[5] (främst under 2022, före gästforskningsvistelsen), (ii) initieringen av ett samverkansforum för aktörer inom det finansiella systemet drivet av Nationellt cybersäkerhetscenter (NCSC), (iii) analysarbete av FI:s uppdrag som sektorsansvarig myndighet för den finansiella sektorn inom totalförsvaret, (iv) analysarbete av FI:s uppdrag som tillsynsmyndighet i enlighet med säkerhetsskyddslagen, (v) utformande av strategi, (vi) arbete med övningsverksamhet med cybersäkerhetsinslag samt (vii) deltagande i referensgruppen för utredningen om en ny funktion för krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur (Finansdepartementet 2024). Urvalet har naturligtvis delvis varit händelsestyrt, men ur ett vetenskapligt perspektiv har det ändå gjorts i syfte att få fram en lämplig uppsättning fallstudier som totalt sett kan möjliggöra ett mått av analytisk generalisering (Yin 2003). Det är värt att notera att även om FI har utgjort kärnan i datainsamlingen så har projekten och processerna inte endast varit myndighetsinterna. Tvärtom har många av dem involverat även andra myndigheter, Regeringskansliet och privata företag i sektorn, vilket har möjliggjort ett bredare perspektiv.

4. Iakttagelser och utmaningar

4.1 DOMARE ELLER COACH?

FI är i grund och botten en tillsynsmyndighet. FI har enligt förordningen (2009:93) med instruktion för Finansinspektionen ansvar för tillsyn, regelgivning och tillståndsprövning som rör finansiella marknader och finansiella företag samt för att motverka finansiella obalanser i syfte att stabilisera kreditmarknaden. I praktiken innebär detta att myndigheten ger tillstånd till aktörerna i den finansiella sektorn att bedriva sin verksamhet (t.ex. inom bank och försäkring) och därefter utövar tillsyn över dessa, alltså granskar att reglerna följs. Framkommer det att någon aktör inte lever upp till de gällande reglerna så kan FI besluta om ingripande eller sanktion mot företaget. Många av de regler som företagen ska leva upp till är naturligtvis av ekonomisk art och handlar om hur de hanterar sina *finansiella* risker. Sådan tillsyn handlar exempelvis

5 Rådet är ett mötesforum för att diskutera frågor om finansiell stabilitet. Deltagarna är Finansdepartementet, Riksbanken, FI och Riksgälden. I februari 2024 fattade regeringen beslut om att avveckla rådet i dess kommittéform (Fi 2013:09) och istället inrätta det som en del av Regeringskansliet.

om att undvika spekulationsbubblor eller bankrusningar – när alla kunder vill ta ut sina pengar på samma gång. Det finns dock också regler som handlar om så kallade *operativa* risker; sådana risker som oundvikligen uppstår bara genom att man agerar på marknaden. Cyberriskerna tillhör de mest påtagliga operativa riskerna: om konton, depåer och handel hanteras datoriserat så löper de oundvikligen samma risker som alla datoriserade system – främst hot mot riktighet, tillgänglighet och konfidentialitet. Cyberriskerna anses rentav ibland vara de allra viktigaste risker som banker utsätts för (Hull 2015: 479–480) och ESRB[6] (2020) har i en rapport argumenterat för att en cyberincident kan leda till en finanskris om förtroendet för systemet urholkas. Även på cyberområdet kan FI vidta åtgärder om det behövs. Ett aktuellt exempel är när Swedbank fick en anmärkning och en sanktionsavgift på 850 miljoner kronor för bristande intern kontroll vid en ändring i ett verksamhetskritiskt IT-system 2022 (Finansinspektionen 2023). Det är värt att understryka att det inte bara var incidenten i sig som var problemet – utan det faktum att systemändringen gjordes i strid med bankens egna rutiner för hur sådana ändringar ska göras. Just bristande kontroll vid ändringar är för övrigt en av de vanligaste orsakerna till IT-driftavbrott (Franke m.fl. 2012).

FI är dock inte enbart en tillsynsmyndighet. Enligt förordningen (2022:524) om statliga myndigheters beredskap (beredskapsförordningen) är Finansinspektionen, sedan 1 oktober 2022, också så kallad sektorsansvarig myndighet för den finansiella sektorn. De sektorsansvariga myndigheterna leder arbetet med att samordna åtgärder både inför och vid fredstida krissituationer och höjd beredskap (se övergripande beskrivning hos MSB 2023a). Därmed ska FI samverka med hela sektorn, såväl andra myndigheter som företag, för att se till att samhällsviktiga finansiella tjänster fungerar även under kris eller krig. Som sektorsansvarig myndighet ska FI stödja andra aktörer, tydliggöra roller och uppgifter och se till att de åtgärder som vidtas är samordnade. I dagens digitaliserade samhälle är det tydligt att den finansiella sektorns motståndskraft i kris eller krig till inte så liten del är en cybersäkerhetsfråga. Erfarenheterna från Ukraina visar tydligt att cyberangrepp mot den finansiella sektorn är ett vapen i krig – men också att det genom adekvata förberedelser går att hålla digitala finansiella tjänster igång även i krigstid (MSB 2023b: 25–40). Det ska för fullständighets skull också påpekas att även om FI inte utövar tillsyn inom beredskapsarbete i beredskapsförordningens mening, så utövar myndigheten viss tillsyn med beredskapsrelevans i vidare mening (till exempel av beredskapsplaner enligt Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker, FFFS 2014: 4).

Sedan den 1 december 2021 är FI också, enligt säkerhetsskyddsförordningen (2021: 955), tillsynsmyndighet enligt säkerhetsskyddslagen (2018:585) inom

6 European Systemic Risk Board

området finansiella företag. Säkerhetsskyddslagstiftningen har på senare år, i takt med ett försämrat säkerhetspolitiskt läge, skärpts och ställer numera krav på att alla verksamheter – privata som offentliga – som bedriver verksamhet av betydelse för Sveriges säkerhet ska vidta åtgärder för ett fullgott säkerhetsskydd. Syftet är att skydda säkerhetskänslig verksamhet mot bland annat spionerі, sabotage och terroristbrott samt att skydda säkerhetsskyddsklassificerade uppgifter. Precis som i den ordinarie tillsynen är cybersäkerheten en avgörande del i detta – i alla sektorer, men inte minst i den finansiella. FI utövar alltså tillsyn över säkerhetsskyddsarbetet på företag i den finansiella sektorn och kan vid brister vidta åtgärder i form av föreläggande, föreläggande med vite och sanktionsavgift (se sammanfattande information hos Säkerhetspolisen 2023b). Det ska för fullständighets skull också påpekas att tillsynsmyndigheterna inom säkerhetsskydd också har ett ansvar för rådgivning och är den huvudsakliga kontakten vid frågor om säkerhetsskydd och tillämpning av bestämmelser (Säkerhetspolisen 2019).

I korthet är FI alltså med avseende på cyberrisker (i) traditionell finansiell tillsynsmyndighet med fokus på finansiell stabilitet och välfungerande marknader, (ii) sektorsansvarig myndighet enligt beredskapsförordningen med fokus på att samordna och stärka sektorn samt med viss tillsyn med beredskapsrelevans i vidare mening och (iii) tillsynsmyndighet för säkerhetsskydd med fokus på tillsyn men även med den rådgivande roll som tillsynsansvaret innebär.

Den fråga som inställer sig är hur lätta rollerna inom vägledning respektive tillsyn är att förena. Tillspetsat kan man ur företagens perspektiv fråga sig: Är FI en domare som dömer ut sanktionsavgifter på hundratals miljoner kronor när fel uppdagas, eller en coach som fördomsfritt och framåtblickande ska hitta områden i sektorn som behöver förbättras för att klara kris, krig och Sveriges säkerhet? Formellt är FI bådadera. Även om myndigheten själv ser en synergi mellan rollerna så kvarstår risken att det ur andras perspektiv ser svårt ut att sitta på båda stolarna samtidigt. Framförallt sektorsansvaret kräver förtroendefulla relationer till alla andra parter, men frågan om hur FI ska förmå bygga upp och förvalta det förtroendet samtidigt som man är tillsynsmyndighet har under gästforskningen återkommit gång efter annan, i diskussioner såväl inom som utom myndigheten. Naarttijärvi (2019: 430–431) diskuterar samma fråga i incidentrapporteringskontext: MSB motsatte sig starkt skyldigheten att vidarebefordra incidentrapporter enligt (den gamla) krisberedskapsförordningen (2015:1052) till polisen just i syfte att odla tillit och inte avskräcka från rapportering. Vikten av förtroende mellan myndigheter och företag lyfts gång på gång fram i den internationella litteraturen (Brechbühl m.fl. 2010; Clark m.fl. 2014; Atkins & Lawson 2021). Omvänt lyfter Riksrevisionen (2023: 44) fram förtroendebyggandet, såväl mellan myndigheter som mellan individer, som ett exempel på sådant arbete som kantats av svårigheter i den svenska NCSC-kontexten.

En nyckel till att framgångsrikt förena de två rollerna är därför att det inte bara måste göras och fungera – det måste också synas utåt att det fungerar.[7] Ju tydligare FI kan förmedla hur rollerna kan fungera ihop och kanske rentav stärka varandra, desto större blir förtroendet och desto bättre går uppgifterna att lösa.

4.2 RISK- ELLER KONSEKVENSBASERAD TILLSYN?

FI:s tillsyn är vanligtvis *riskbaserad*. Det betyder att myndigheten lägger sina resurser där risken – alltså sannolikheten för och/eller konsekvensen av en oönskad händelse – är som störst. Utifrån att budgetar alltid är begränsade och medlen behöver läggas där de gör som mest nytta är detta också en resursprioriteringsfråga. Att frångå den riskbaserade tillsynen innebär ur detta perspektiv att ta resurser från tillsyn av stora risker och istället lägga dem på tillsyn av små risker. På samma sätt är företagens förebyggande arbete – det som FI utövar tillsyn över – riskbaserat. Företagen förväntas prioritera sitt arbete och sina begränsade resurser efter var riskerna är störst. Detsamma gäller också staten i bred bemärkelse – Riksrevisionen (2023, avsnitt 2.2) riktar exempelvis kritik mot regeringen för att *inte* ha tagit fram den nationella informations- och cybersäkerhetsstrategin utifrån ett riskbaserat tillvägagångssätt. (Det kan dock noteras att det riskbaserade arbetssättet inte är perfekt. En uppenbar komplikation är att bedömningarna av såväl konsekvens som sannolikhet kan vara felaktiga, vilket i så fall leder till felaktiga prioriteringar. Se Eling & Schnell 2020 samt Peihani 2022 för analyser som tyder på att de etablerade riskbaserade metoderna underskattar cyberriskerna.)

Som nämnts ovan är FI numera också tillsynsmyndighet enligt säkerhetsskyddslagen. Säkerhetsskyddsarbete ska emellertid *inte* vara riskbaserat. Sannolikhet och konsekvens ska *inte* vägas samman. Enbart konsekvenser för Sveriges säkerhet räknas (Säkerhetspolisen 2023a). Huruvida de är sannolika eller osannolika ska inte spela någon roll; det avgörande är att de är möjliga. Medan det är tydligt att de företag som omfattas av säkerhetsskyddslagstiftningen endast ska ta hänsyn till konsekvens i sitt säkerhetsskyddsarbete, har det i flera sammanhang rått osäkerhet om huruvida även själva *tillsynen* ska vara strikt konsekvensbaserad eller om FI kan prioritera sin säkerhetsskyddstillsyn även med beaktande av sannolikheter. Oavsett vilket som rent juridiskt är fallet står det klart att såväl FI som företagen som står under tillsyn sedan tidigare är vana vid ett arbetssätt rörande cybersäkerheten, men nu måste vänja sig vid ytterligare ett som kommer att löpa parallellt.

7 Inom juridiken talar man om att ”justice should not only be done, but should manifestly and undoubtedly be seen to be done” (se exempelvis Jung 2012).

4.3 ANTAGONISTISKA HOT ELLER ALLRISKPERSPEKTIV?

Säkerhetsskyddslagen medför ytterligare en snarlik komplikation. Den traditionella IT-tillsynen har ett allriskperspektiv; såväl antagonistiska angrepp som icke-antagonistiska misstag och olyckor ingår. ”Det ovan nämnda exemplet vad gäller anmärkningen och sanktionsavgiften mot Swedbank (Finansinspektionen 2023) är ett bra exempel. Här handlade det inte alls om något angrepp, utan om interna regler som inte hade följts, vilket fick ödesdigra följder. Återigen skiljer dock säkerhetsskyddstillsynen ut sig: här är det bara antagonistiska angrepp som räknas. För det första medför detta samma konsekvenser som frågan om risk- eller konsekvensbaserad tillsyn – såväl FI som företagen måste hålla två parallella arbetsprocesser i huvudet samtidigt. En svensk studie av krishanteringsövningen NISÖ18[8] visade att de deltagande företagen och myndigheterna, åtminstone i övningsscenariot, inte så noga brydde sig om att skilja på vad som var angrepp respektive oavsiktliga incidenter (Varga, Brynielsson & Franke 2018), vilket antyder att det kommer att krävas en mental omställning.

För det andra så medför det också mer konceptuella svårigheter. De två sorternas incidenter kan vara mycket svåra att skilja i praktiken, eftersom en skicklig angripare gärna vill maskera angrepp som oavsiktliga händelser och även eftersom en oavsiktlig händelse kan misstolkas som ett angrepp. Visst stöd för att det är svårt att skilja de två kategorierna åt ges av Franke & Wernberg (2020), där respondenternas bedömningar av riskerna för avsiktliga angrepp respektive oavsiktliga incidenter är så pass snarlika att man kan misstänka att de speglar just denna svårighet.

4.4 HUR GÖRA TILLSYNEN MER DATADRIVEN OCH AUTOMATISERAD?

En viktig del av tillsynsarbetet avseende cybersäkerhet – den traditionella tillsynen av risker och på sikt också den nya avseende säkerhetsskydd – är det underlag som företagen levererar. Det är detta som granskas, det är här som avvikande mönster kan upptäckas, det är utifrån detta som det till slut fattas beslut om eventuella åtgärder. Även om företagen är juridiskt förpliktigade att leverera detta underlag är formatet inte standardiserat. Inte sällan rör det sig i praktiken om långa presentationer med inklippta diagram och tabeller som kräver en hel del manuellt arbete för att ens kunna behandlas. I princip finns det stora möjligheter att automatisera det grundläggande tillsynsarbetet. Men en sådan vision hindras av att det saknas standardisering av inrapporterade data och att FI inte har något juridiskt mandat att ändra på detta. Det är upplysande att kontrastera detta mot de rekommendationer för att tillgängliggöra information som ges av Myndigheten för digital förvaltning (DIGG 2023, princip 4): ”Verksamheten ska sträva efter att använda format,

8 Nationell informationssäkerhetsövning.

API:er och specifikationer som är öppna, standardiserade och maskinläsbara. Det ökar möjligheterna för att samverka digitalt, kombinera och bearbeta information och lägger inte tekniska begränsningar på hur informationen kan användas."[9] Det underlag som erhålls för tillsyn av cybersäkerhet ligger långt från denna princip, vilket försvårar skalbar och datadriven tillsyn. Därmed blir det också svårare att göra sådana datadrivna justeringar som kan behövas för exempelvis cyberrisker – Eling & Schnell (2020) konstaterar exempelvis att samtliga tre cyberriskmodeller för tillsyn som de undersöker är "one-size-fits-all" utan särskild kalibrering, vilket gör dem onödigt trubbiga, även om det ska understrykas att detta inte bara handlar om bristande standardisering av dataformat utan även om en mer grundläggande brist på adekvat dataunderlag som sådant.

4.5 SAMVERKAN, MANDAT OCH SJÄLVSTÄNDIGA MYNDIGHETER

Som framgått ovan är det i såväl internationella som svenska sammanhang mycket vanligt att ansvar för cybersäkerhetsfrågor finns fördelat på flera olika myndigheter, med mer eller mindre tydlig konceptuell och juridisk samsyn kring vem som gör vad.

Den finansiella sektorn är inget undantag. I korthet är de finansiella företagen i grund och botten själva ansvariga för att kunna hantera driftstörningar i enlighet med den så kallade ansvarsprincipen; en grundprincip i svensk krishantering. Myndigheternas roll i relation till detta är främst att koordinera och ytterligare utveckla denna förmåga – både FI och Riksgälden ska som beredskapsmyndigheter i sektorn finansiella tjänster verka för detta. FI är som ovan nämnts dessutom sektorsansvarig myndighet, med särskilt ansvar för att driva på detta arbete och stödja övriga aktörer. Därutöver har Riksbanken enligt lagen (2022: 1568) om Sveriges riksbank (riksbankslagen) ett särskilt ansvar för betalningssystemet såväl under kris som vid höjd beredskap och ytterst krig.

Även om ansvarsprincipen lägger det grundläggande ansvaret på de finansiella företagen är det inte svårt att föreställa sig situationer där en cyberkris i den finansiella digitala infrastrukturen – omfattande avbrott, dataläckage eller förvanskad finansiell information – eskalerar och riskerar att hota den finansiella stabiliteten på ett sådant sätt att någon form av myndighetsingripande är påkallat. Det gäller inte minst i ett skärpt säkerhetspolitiskt läge av det slag vi nu befinner oss i, där det inte kan uteslutas att främmande makt nyttjar cyberangrepp som ett maktmedel (Regeringen 2020: 63 och Försvarsmakten 2022: 29). Det befintliga finansiella stabilitetsrådet – ett organ för att diskutera frågor om finansiell stabilitet och koordinera Finansdepartementet, Riksbanken, FI och Riksgälden – formaliserades i spåren av finanskrisen 2008/09 – och

9 API uttyds Application Programming Interface.

har sedan dess utvecklat och övat upp en god förmåga att koordinerat möta *finansiella* kriser som hotar den finansiella stabiliteten (se även Magnusson 2021, särskilt s. 383–385, för en diskussion av svenska lärdomar och spårbundenheten i dessa utifrån ekonomiska kriser). Men rådet har inte motsvarande förmåga att hantera *operativa* kriser såsom ett omfattande driftavbrott i sektorn. De verktyg som myndigheterna i rådet har till sitt förfogande, främst olika former av ekonomiska garantier för att upprätthålla förtroendet för drabbade aktörer, är snarare symptom- än sjukdomsavhjälpande om grundorsaken är en svår cyberincident. För att på bästa sätt kunna hantera sådana händelser är det möjligt att ytterligare myndigheter, exempelvis försvars- och säkerhetsmyndigheter eller andra tillsynsmyndigheter som Post- och Telestyrelsen skulle behöva involveras. (Det finns också tänkbara händelser där inte heller detta hjälper – rätt kompetens finns bara hos den drabbade själv.) Men medan de tre myndigheterna i stabilitetsrådet – och deras departement – under halvtannat decennium har arbetat och övat ihop på att hantera finansiella kriser har det inte övats på motsvarande sätt med andra relevanta myndigheter eller deras departement. Ett sådant samarbete skulle då behöva improviseras ihop – kanske under ledning av den nationella säkerhetsrådgivarens organisation som i skrivande stund håller på att upprättas. Ytterligare en komplicerande faktor är emellertid att Riksbanken är en myndighet under riksdagen, inte under regeringen, vilket innebär att regeringen inte kan utöva någon styrning över dess verksamhet.

Iakttagelserna ovan är inte nya. De finns exempelvis redovisade i FI:s svar till regeringen i maj 2022 (Finansinspektionen 2022: 22–25), i uppdragsbeskrivningen till utredningen om krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur (Finansdepartementet 2023), liksom i själva utredningen (Finansdepartementet 2024, se särskilt avsnitt 4.5), vilken – åtminstone till del – syftade till att lösa problematiken.

Problematiken är ändå värd att uppmärksamma på nytt, eftersom läget är snarlikt – med undantag för Riksbankens särskilda ställning – även i andra sektorer. Riksrevisionen (2023) bedömer att den nationella informations- och cybersäkerhetsstrategin saknar en tydlig lednings- och styrningsstruktur (avsnitt 2.4) och att även om styrningen av enskilda myndigheter har varit tydlig så leder bristen på sammanhållen styrning till arbete i stuprör utan överblick (avsnitt 5.2). Höjer man blicken ännu mer så återfinns samma frågor också i den generella debatten om hur svensk civil krisberedskap och civilt försvar ska styras. ”Vem ska egentligen leda samordningen när flera centrala myndigheter deltar enligt ansvarsprincipen, vem ska säkerställa resurserna och hur ska kunskapsöverföringen inom nätverket se ut för att man ska kunna åstadkomma en effektiv samordning?” frågar sig Brommesson (2021) i slutsatserna av sin studie av den offentliga styrningen under pandemin. Frågan har lika stor bäring på styrningen av cybersäkerhetsarbetet.

Åtminstone konturerna av denna problematik har kunnat observeras under gästforskningsvistelsen. Ett glapp mellan förväntningar och upplevt utfall är något som exempelvis karakteriserade starten på det samverkansforum för aktörer inom det finansiella systemet som drivs av NCSC. Här kan också göras en iakttagelse relaterad till personalrotation. Det är relativt vanligt att personal byter arbetsplats inom den familj av myndigheter som utgör det finansiella stabilitetsrådet – Finansdepartementet, Riksbanken, FI och Riksgälden. Ett flertal sådana övergångar har observerats under gästforskningsvistelsen när nära kolleger har gjort sådana förflyttningar. Detta är ett osynligt band som stärker dessa myndigheters förmåga att samarbeta snabbt och effektivt när det behövs. Men det har historiskt varit mycket ovanligare att personal från denna myndighetsfamilj byter arbete till eller från de fyra myndigheter som utgör kärnan i NCSC – MSB, Försvarsmakten, Säkerhetspolisen och FRA – eller deras departement, Försvars- respektive Justitiedepartementet. Det är svårt att kvantifiera hur viktig denna förklaring är. Men när FI nu till följd av sina nya uppgifter i ökad omfattning har börjat rekrytera personal med bakgrund från försvars- och säkerhetsmyndigheter är det ingen vågad hypotes att förståelsen för varandra kommer att växa, samarbetet fungera bättre och styrningsproblematiken bli mindre även om den – med ledning av Riksrevisionens kritik av NCSC – knappast helt kommer att försvinna.

5. Vad krävs för att utveckla och implementera god cybersäkerhetspolicy?

Iakttagelserna och utmaningarna ovan pekar huvudsakligen på svårigheterna med att *implementera* cybersäkerhetspolicy. Om man abstraherar dem så kan de sammanfattas tämligen kortfattat och får dessutom en bedräglig självklarhet: För att lyckas med cybersäkerhetspolicy är det bra om varje myndighet har uppgifter som inte står i motsatsförhållande till varandra, om snarlika verksamheter bedrivs enligt samma filosofi, om den moderna teknikens möjligheter till automation och avancerad analys utnyttjas och om olika myndigheters roller och mandat är tydliga i relation till varandra. Självklarheten är som sagt bedräglig: det är en sak att göra observationerna och formulera råden; en helt annan att omsätta dem i praktiken. Riksrevisionen beskriver exempelvis hur man på Regeringskansliet under perioden 2017–2022 försökte samordna cyberfrågorna genom att inrätta interdepartementala arbetsgrupper med olika sammansättning, men att det inte räckte för att ”lösa ut centrala målkonflikter eller styra strategiskt på området” Riksrevisionen (2014: 60). Forskningslitteraturen (temata ett, två och tre) visar också tydligt att Sverige inte är ensamt om dessa problem och antyder att det inte finns några enkla lösningar.

Arbete med cybersäkerhetspolicy är alltså *praktiskt* svårt av en mängd skäl. Emellertid är det också *teoretiskt* svårt. Detta eftersom det är mångfacetterat och öppet för olika tolkningar, där tekniska och icke-tekniska aspekter samspelar på ett icke-trivialt sätt (litteraturens första tema). Annorlunda uttryckt betyder det att problemen kan formuleras och lösas på en mängd olika sätt. Anderson & Moore (2006) menar att incidenter sker minst lika ofta på grund av dåliga incitament som på grund av dålig design – då kan de också förebyggas med goda incitament likväl som med god design.

En pessimistisk tolkning av detta är att cybersäkerhetspolicyarbetet blir *ännu svårare*, eftersom ännu fler kompetenser måste till. Något ligger det naturligtvis i detta. Men en optimistisk tolkning är istället att cybersäkerhetspolicyarbetet blir *lättare*, eftersom det finns så många potentiella verktyg att använda. Svårigheten blir snarast att hitta dessa verktyg.

Riksrevisionen menar att RK:s förmåga på cyberområdet inte räcker till och att ”en förklaring till bristerna är att det saknas tillräcklig operativ och taktisk kunskap om hur cybersäkerhetsarbetet bedrivs på myndigheterna och inom den privata sektorn såväl som specifik domänkunskap såsom internets funktionalitet, kryptokunskap, tekniska säkerhetslösningar och andra centrala komponenter inom cybersäkerhetsområdet. Utan egen kunskap i dessa frågor är risken stor att bedömningar av vad som behöver ske avseende styrning och förmågehöjning blir felaktiga.” Riksrevisionen (2014: 66) Problemet accentueras ytterligare av att det sedan länge råder global brist på utbildad cybersäkerhetspersonal (se t.ex. Caldwell 2013; Blažič 2021).

Riksrevisionen fokuserar här på en uppsättning kompetenser som främst handlar om teknisk design. Det är på intet sätt fel. Men utifrån Anderson & Moore (2006) förefaller det rimligt att komplettera denna kompetensmässiga önskelista med en motsvarande lista fokuserad på incitament. Handläggare som arbetar med cybersäkerhet borde ur detta perspektiv inte *bara* behärska internets funktionalitet, krypton och tekniska säkerhetslösningar utan *också* (exempelvis) asymmetrisk information, externaliteter och beteendeekonomi. Cybersäkerhet är inte *bara* en teknisk fråga och det är viktigt att den inte – av tradition och oförmåga att tänka utanför givna ramar – reduceras till det. Särskilt viktigt är detta i RK, för just där ”ska samtliga perspektiv brytas och samordnas, till skillnad från förvaltningsmyndigheter och andra mer specialiserade organisationer” (Niemann 2013: 72).

Kanske finns det en bias-problematik här: att *implementera* policy är så svårt att den svårigheten skymmer sikten för hur svårt det kan vara att *utveckla* policy – framförallt om svårigheterna består i att vissa perspektiv som skulle möjliggöra vissa verktygslådor helt enkelt saknas. Hur hittar man sådana *unknown unknowns*? Hur kan RK å ena sidan byta perspektiv, undvika gamla hjulspår och hitta kreativa lösningar på problem men å andra sidan upprätthålla den nollfelskultur (Niemann 2013: 86) som präglar – och måste prägla

– stödet till rikets ledning? Det är en fråga av både teoretiskt och praktiskt intresse som det borde forskas (mer) på.[10]

Hur viktiga svårigheterna med att utveckla respektive implementera cybersäkerhetspolicy är, relativt varandra, framstår som mycket svårt att belysa på ett systematiskt sätt. En gästforskningsvistelse av det slag som ligger till grund för den här artikeln är bara en enskild pusselbit – idealt skulle det behövas mycket mer evidens. Men med ledning av bias-problematiken framstår det som rimligt att varna för att underskatta eller förbise svårigheterna med att utveckla cybersäkerhetspolicy som på ett klokt vis nyttjar alla de verktyg som står till buds. Moore (2010) argumenterar exempelvis för att ganska små interventioner som justerar incitament och korrigerar uppenbara marknadsmisslyckanden kan få stor positiv effekt på cybersäkerheten i ett land och i många fall vara mer kostnadseffektivt än stora teknikprojekt. Om det stämmer – vilket verkar rimligt – så blir det angeläget att inte bara fokusera på att avhjälpa svårigheterna med att implementera cybersäkerhetspolicy utan också aktivt arbeta för att förbättra förmågan att utveckla densamma.

Dessa iakttagelser blir särskilt viktiga i ljuset av det nu pågående arbetet med en ny nationell informations- och cybersäkerhetsstrategi (Kristersson m.fl. 2023).

Referenser

Anderson, Ross & Moore, Tyler, 2006. ”The economics of information security”, *Science* 314(5799), s. 610–613. doi: 10.1126/science.1130992.

Atkins, Sean & Lawson, Chappell, 2021. ”An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure”, *Public Administration Review* 81(5), s. 847–861. doi: 10.1111/puar.13322.

Backman, Sarah, 2023. ”Risk vs. threat-based cybersecurity: the case of the EU”, *European Security* 32(1), s. 85–103. doi: 10.1080/09662839.2022.2069464.

Bauer, Johannes M & Eeten, Michel JG van, 2009. ”Cybersecurity: Stakeholder incentives, externalities, and policy options”, *Telecommunications Policy* 33(10–11), s. 706–719. doi: 10.1016/j.telpol.2009.09.001.

Blažič, Borka Jerman, 2021. ”The cybersecurity labour shortage in Europe: Moving to a new concept for education and training”, *Technology in Society* 67, s. 101769. issn: 0160-791X. doi: 10.1016/j.techsoc.2021.101769.

Boholm, Max, 2021. ”Twenty-five years of cyber threats in the news: a study of Swedish newspaper coverage (1995–2019)”, *Journal of Cybersecurity* 7(1), tyab016. doi: 10.1093/cybsec/tyab016.

10 Ett intressant initiativ i sammanhanget är tävlingen *Cyber Challenge* som årligen arrangeras av Försvarshögskolan med domare från ett stort antal relevanta myndigheter och företag. Deltagarna är studentlag från landets lärosäten som ställs inför ett fiktivt scenario där de ska ta fram policysvar. Tävlingen brukar väcka relativt stor uppmärksamhet och 2023 besöktes prisutdelningen av statssekreteraren hos ministern för civilt försvar. Det är särskilt värt att notera att deltagarna rekommenderas ”att bygga laget över institutionsgränser och med olika studieinriktningar” för att bli framgångsrika (https://www.fhs.se/om-forsvarshogskolan/omoss/cyber-challenge.html, läst 2023-08-17).

Brechbühl, Hans m.fl., 2010. ”Protecting critical information infrastructure: Developing cybersecurity policy”, *Information Technology for Development* 16(1), s. 83–91. doi: 10.1002/itdj.20096.

Brommesson, Douglas, 2021. ”Civil beredskap och offentlig styrning under pandemin 2020–2021”, *Statsvetenskaplig tidskrift* 123(5), s. 141–158.

Bronk, Chris & Conklin, Wm Arthur, 2022. ”Who’s in charge and how does it work? US cybersecurity of critical infrastructure”, *Journal of Cyber Policy* 7(2), s. 155–174. doi: 10.1080/23738871.2022.2116346.

Bruijn, Hans de & Janssen, Marijn, 2017. ”Building cybersecurity awareness: The need for evidence-based framing strategies”, *Government Information Quarterly* 34(1), s. 1–7. doi: 10.1016/j.giq.2017.02.007.

Caldwell, Tracey, 2013. ”Plugging the cyber-security skills gap”, *Computer Fraud & Security* 2013(7), s. 5–10. issn: 1361-3723. doi: 10.1016/S1361-3723(13)70062-9.

Carr, Madeline & Lesniewska, Feja, 2020. ”Internet of Things, cybersecurity and governing wicked problems: Learning from climate change governance”, *International Relations* 34(3), s. 391–412. doi: 10.1177/0047117820948247

Clark, Kas m.fl., 2014. ”A Dutch approach to cybersecurity through participation”, *IEEE Security & Privacy* 12(5), s. 27–34. doi: 10.1109/MSP.2014.83.

DIGG, 2023. *Vägledning för att tillgängliggöra information*. Tillgänglig på https://www.digg.se/kunskap-och-stod/oppna-och-deladedata/offentliga-aktorer/vagledning-for-att-tillgangliggorainformation, läst 2023-08-14.

Cohen, Michael D., March, James G. & Olsen, Johan P., 1972. ”A garbage can model of organizational choice”, *Administrative Science Quarterly* 17(1), s. 1–25. Tillgänglig på https://www.jstor.org/stable/2392088.

Dunn Cavelty, Myriam & Wenger, Andreas, 2020. ”Cyber security meets security politics: Complex technology, fragmented politics, and networked science”, *Contemporary Security Policy* 41(1), s. 5–32. doi: 10.1080/13523260.2019.1678855.

Dynes, Scott, Goetz, Eric & Freeman, Michael, 2008. ”Cyber security: Are economic incentives adequate?”, *Critical Infrastructure Protection 1*. Springer, s. 15–27. doi: 10.1007/978-0-387-75462-8_2.

Eling, Martin & Schnell, Werner, 2020. ”Capital requirements for cyber risk and cyber risk insurance: An analysis of Solvency II, the US risk-based capital standards, and the Swiss Solvency Test”, *North American Actuarial Journal* 24(3), s. 370–392. doi: 10.1080/10920277.2019.1641416.

ESRB European Systemic Risk Board, 2020. *Systemic cyber risk*. isbn: 9789294721310. doi: 10.2849/566567.

Finansdepartementet, 2023. *Operativ krisledning vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur*. Fi2023/01842. Stockholm.

Finansdepartementet, 2024. *En ny funktion för krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur*. Fi2024/00185. Stockholm.

Finansinspektionen, 2022. *Förstärkt digital motståndskraft hos företag i den finansiella sektorn*. FI dnr 22-10015. Tillgänglig på https://www.fi.se/sv/publicerat/rapporter/rapporter/2022/forstarkt-digital-motstandskrafthos-foretag-i-den-finansiella-sektorn/.

Finansinspektionen, 2023. *Swedbank får anmärkning och sanktionsavgift*. FI dnr 22-18430. Tillgänglig på https://www.fi.se/sv/publicerat/sanktioner/finansiellaforetag/2023/swedbank-far-anmarkning-och-sanktionsavgift/.

Franke, Ulrik, 2020. *Cybersäkerhet för en uppkopplad ekonomi*. Entreprenörskapsforum.

Franke, Ulrik, m.fl., 2012. ”Availability of enterprise IT systems: an expert-based Bayesian framework”, *Software Quality Journal* 20, s. 369– 394. doi: 10.1007/s11219-011-9141-z.

Franke, Ulrik & Wernberg, Joakim, 2020. ”A survey of cyber security in the Swedish manufacturing industry”, *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)*. IEEE. doi: 10.1109/CyberSA49311.2020.9139673.

Försvarsdepartementet, 2023. Riksrevisionens rapport om regeringens styrning av *samhällets informations- och cybersäkerhet*. Skr. 2023/24:26. Stockholm.

Försvarsmakten, 2022. *Militärstrategisk doktrin – MSD 22*. FM2022-14281:1. Tillgänglig på https://www.forsvarsmakten.se/siteassets/2-om-forsvarsmakten/dokument/doktriner/msd-22.pdf.

Gordon, Lawrence A., m.fl., 2014. ”Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model”, *Journal of Information Security* 6(01), s. 24–30. doi: 10.4236/jis.2015.61003.

Harknett, Richard J & Stever, James A, 2011. ”The new policy world of cybersecurity”, *Public Administration Review* 71(3), s. 455–460. doi: 10.1111/j.1540-6210.2011.02366.x.

Hauser, William E. *Super Wicked Problems: The Shared Challenges of Climate Change and Cyber and the Viability of Shared Solutions*. Diss. Harvard University, 2023.

Hull, John, 2015. *Risk management and financial institutions*. 4. utg. John Wiley & Sons.

Jung, Heike, 2012. ”’Justice must be seen to be done’”, *Nordisk Tidsskrift for Kriminalvidenskab* 99(1).

Kemmis, Stephen, McTaggart, Robin & Nixon, Rhonda, 2014. *The action research planner: Doing critical participatory action research*. Springer. doi: doi.org/10.1007/978-981-4560-67-2.

Kristersson, Ulf m.fl., 2023. ”’FRA får ta över ansvaret för Sveriges cybersäkerhet’”, *Dagens Nyheter* (27 april), s. 5.

Kuerbis, Brenden & Badiei, Farzaneh, 2017. ”Mapping the cybersecurity institutional landscape”, *Digital Policy, Regulation and Governance* 19(6), s. 466– 492. doi: 10.1108/DPRG-05-2017-0024.

Kävrestad, Joakim & Huskaj, Gazmend, 2021. ”How the Civilian Sector in Sweden Perceive Threats from Offensive Cyberspace Operations”, *20th European Conference on Cyber Warfare and Security:* Proceedings of the 20th European Conference on Cyber Warfare and Security, s. 499–506. doi: 10.34190/EWS.21.106.

Luiijf, Eric, Besseling, Kim & De Graaf, Patrick, 2013. ”Nineteen national cyber security strategies”, *International Journal of Critical Infrastructures* 6 9(12), s. 3–31. doi: 10.1504/IJCIS.2013.051608.

Luks, Therese, 2021. ”Miljoner på spel – Coops kassor nere i fyra dagar”, *Svenska Dagbladet Näringsliv* (6 juli), s. 5.

Magnusson, Lars, 2021. ”Lärande och krisbekämpning under tre ekonomiska kriser i Sverige”, *Statsvetenskaplig tidskrift* 123(5), s. 379–390.

Manjikian, Mary & Romaniuk, Scott N., 2021. *Routledge Companion to Global Cyber-Security Strategy*. Routlege companions. London: Routledge. isbn: 0429-39971-5.

Moore, Tyler, 2010. ”The economics of cybersecurity: Principles and policy options”, *International Journal of Critical Infrastructure Protection* 3(3–4), s. 103–117. doi: 10.1016/j.ijcip.2010.10.002.

MSB, 2023a. *Det svenska civila beredskapssystemet*. Tillgänglig på https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/det-svenska-civila-beredskapssystemet/.

MSB, 2023b. *När kriget kom nära – Årsrapport it-incidenter 2022*. MSB2179. Tillgänglig på https://rib.msb.se/Filer/pdf/30339.pdf.

Naarttijärvi, Markus, 2019. ”Rapporteringskrav vid incidenter i myndigheters informationssystem: i spänningsfältet mellan krisberedskap och rättighetsskydd”, *Juridisk Tidskrift* (2), s. 405–431.

Nicander, Lars, 2010. ”Shielding the net–understanding the issue of vulnerability and threat to the information society”, *Policy Studies* 31(3), s. 283–300. doi: 10.1080/01442871003615935.

Nicander, Lars, 2015. ”New threats-old routines: bureaucratic adaptability in the security policy environment”. Diss. Åbo Akademi. Tillgänglig på https://urn. kb.se/resolve?urn=urn:nbn:se:fhs:diva-5630.

Niemann, Cajsa, 2013. ”Villkorat förtroende: Normer och rollförväntningar i relationen mellan politiker och tjänstemän i Regeringskansliet”. Diss. Statsvetenskapliga institutionen, Stockholms universitet. Tillgänglig på https://urn.kb. se/resolve?urn=urn:nbn:se:su:diva-94771.

Oscarsson, Tea, 2021. ”Dröjer månader innan Kalix fungerar normalt”, *Svenska Dagbladet* (22 december), s. 23.

Patacsil, Peter K., 2021. ”The Design and Evolution of the United States Cyber Command.” Diss. George Mason University.

Peihani, Maziar, 2022. ”Regulation of Cyber Risk in the Banking System: A Canadian Case Study”, *Journal of Financial Regulation* 8(2), s. 139–161. doi: 10.1093/jfr/fjac006.

Regeringen, 2020. *Totalförsvaret 2021–2025*. Prop. 2020/21:30. Tillgänglig på https://www.regeringen.se/rattsliga-dokument/proposition/2020/10/ prop.-20202130.

Renaud, Karen, m.fl., 2020. ”Cyber security responsibilization: an evaluation of the intervention approaches adopted by the Five Eyes countries and China”, *Public Administration Review* 80(4), s. 577–589. doi: 10.1111/puar.13210.

Riksrevisionen, 2014. *Informationssäkerheten i den civila statsförvaltningen*. Publikationsnummer RiR 2014:23. Stockholm.

Riksrevisionen, 2016. *Informationssäkerhetsarbete på nio myndigheter*. Publikationsnummer RiR 2016:8. Stockholm.

Riksrevisionen, 2023. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig*. Publikationsnummer RiR 2023:8. Stockholm.

Rodin, Deborah Norris, 2015. ”The Cybersecurity Partnership: A Proposal for Cyberthreat Information Sharing Between Contractors and the Federal Government”, *Public Contract Law Journal* 44(3), s. 505–528. Tillgänglig på https://www.jstor.org/stable/26419479.

Sabillon, Regner, Cavaller, Victor & Cano, Jeimy, 2016. ”National cyber security strategies: global trends in cyberspace”, *International Journal of Computer Science and Software Engineering* 5(5), s. 67.

Sales, Nathan Alexander, 2012. ”Regulating cyber-security”, *Northwestern University Law Review* 107(4), s. 1503–1568.

Smits, Hans, 1997. ”Living within the space of practice: Action research inspired by hermeneutics”, *Counterpoints* 67, s. 281–297. Tillgänglig på https://www.jstor. org/stable/42975254.

Štitilis, Darius, Pakutinskas, Paulius & Malinauskaitė, Inga, 2017. ”EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis”, *Security Journal* 30, s. 1151–1168. doi: 10.1057/s41284-016-0083-9.

Svahn, Mattias, Jarlsbo, Mathilde, Michélsen Forsgren, Miranda & Lindahl, David, 2024. *Delat ansvar är ingens ansvar? En analys av den svenska statsförvaltningens ansvar och styrning vad gäller svenskt informations- och cybersäkerhetsarbete*, Totalförsvarets forskningsinstitut, FOI-R--5546--SE.

Säkerhetspolisen, 2019. *Vägledning i säkerhetsskydd – Introduktion till säkerhetsskydd*. Tillgänglig på https://www.sakerhetspolisen.se/download/18.310a187117da376c6603305/1636446528576/Vagledning-Introduktiontill-sakerhetsskydd.pdf.

Säkerhetspolisen, 2023a. *Säkerhetskyddsanalys – Vägledning i säkerhetsskydd*. Version Januari 2023. Tillgänglig på https://www.sakerhetspolisen.se/download/18.3baf70bf187108c7cf04b7/1681802201089/Sa%CC%88kerhetskyddsanalys_anpassad.pdf.

Säkerhetspolisen, 2023b. *Verksamheten Säkerhetsskydd Tillsyn*. Läst 2023-08-10. Tillgänglig på https://www.sakerhetspolisen.se/verksamheten/sakerhetsskydd/tillsyn.html.

Valeriano, Brandon, & Jensen, Benjamin, 2021. ”Building a national cyber strategy: the process and implications of the cyberspace solarium commission report”, *13th International Conference on Cyber Conflict (CyCon)*, s. 189-214. doi: 10.23919/CyCon51939.2021.9467806

Varga, Stefan, Brynielsson, Joel & Franke, Ulrik, 2018. ”Information Requirements for National Level Cyber Situational Awareness”, *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, s. 774–781. doi: 10.1109/ASONAM.2018.8508410.

Varga, Stefan, Brynielsson, Joel & Franke, Ulrik, 2021. ”Cyber-threat perception and risk management in the Swedish financial sector”, *Computers & Security* 105(102239). doi: 10.1016/j.cose.2021.102239.

Vetenskapsrådet, 2021. *Quality and impact of research in political science in Sweden*. VR2108, Dnr 3.2-2018-00113. Stockholm. isbn: 978-91-88943-46-0.

von Solms, Rossouw & van Niekerk, Johan, 2013. ”From information security to cyber security”, *Computers & Security* 38, s. 97–102. doi: 10.1016/j. cose.2013.04.004.

Yin, Robert K, 2003. *Case Study Research: Design and Methods*. Applied Social Research Methods, Vol. 5. SAGE Publications, Inc.