Myndigheten för samhällsskydd och beredskap

STUDIE

Mot en palett/karta av styrmedel för informationssäkerhet – förslag till konceptuell styrmodell

Faktaruta

Mot en palett/karta av styrmedel för informationssäkerhet. Förslag till konceptuelll styrmodell

2016-10-05

Louise Yngström Konsult

Louise Yngström

Studien presenterar en kort analys av styrmedel användbara i en styrmodell för informationssäkerhet. Den kompletterar en tidigare genomförd kunskapsöversikt över decentraliserade styrmodeller med fallstudier från informationssäkerhetsområdet. Avsikten är att bidra till ytterligare fördjupade diskussioner relaterade till arbetsdokumentet ’Tankar om styrmodell – Förslaget om styrmodell i NISU’.

MSB:s kontaktpersoner:
Helena Andersson, 010-240 41 33
Andreas Rappe, 010-240 44 91

Diarienr 2017-8991
Publikationsnummer MSB1128 – oktober 2016
ISBN 978-91-7383-769-9

MSB har beställt och finansierat genomförandet av denna studierapport. Författaren är ensamt ansvarig för rapportens innehåll.

Förord

Författaren av denna rapport vill uttrycka sin glädje över att beretts tillfälle att deltaga i den viktiga diskussionen om hur informationssäkerhet på ett helhetligt sätt kan realiseras i Sverige. Diskussionen har hållits levande genom åren och förslagen har varit många. Förhoppningen är att förslaget i NISU om en nationell styrmodell kan få utgöra en start mot samverkan mellan teknik, organisation och människor för att upprätthålla tillitsfulla och säkra tillämpningar i en ständigt föränderlig omvärld.

Innehållsförteckning

Sammanfattning

Studiens syfte är att presentera en kort analys av styrmedel användbara i en delvis decentraliserad modell för informationssäkerhet. Den kompletterar med två fallstudier från informationssäkerhetsområdet en tidigare genomförd kunskapsöversikt över decentraliserade styrmodeller. Avsikten är att bidra till ytterligare fördjupade diskussioner relaterade till arbetsdokumentet ’Tankar om styrmodell – Förslaget om styrmodell i NISU’.
Den tidigare genomförda Kunskapsöversikt över decentraliserade styrmodeller betonar att olika perspektiv fokuserar olika frågeställningar och kontexter samt att ’decentraliserade styrmodeller bör beaktas utifrån den konkreta situationen där de är tänkta att användas’ eftersom ’företeelsen decentraliserade styrmodeller rymmer en så pass stor variation av konkreta styrmodeller och kombinationer av styrmedel att det i varje situation bör konkretiseras vilken aspekt av styrmodellen som avses’ samt att ’det offentligas roll som meta-guvernör…kan kombineras på olika sätt i syfte att nå måluppfyllelse.’
Fallstudierna analyseras och diskuteras huvudsakligen utifrån dimensionen motivationsantagning uttryckt som regelstyrning, incitamentsstyrning, kapacitetsstyrning, lärande och symbolisk styrning, samt explicitgör vilka aktörer som medverkade, vilka möjligheter och hinder som decentraliseringen utgjorde samt vilka omständigheter som gav goda eller mindre goda konsekvenser. I en sammanfattande analys klargörs vilka styrverktyg som kan urskiljas eller efterfrågas, vilken relevans fallstudierna bedöms ha i nuläget samt hur man i en förändrad miljö med globalisering, mindre tydliga gränser och barriärer och starkare marknadsaktörer kan ta tillvara tidigare gjorda erfarenheter från informationssäkerhetsprojekt.
Studien avslutas med ett förslag till en konceptuell styrmodell som ansluter till vad som framställts i arbetsdokumentet ’Tankar om styrmodell – Förslaget om styrmodell i NISU’ och föreslår samtidigt hur styrmodellen – inom ramen för en känd teoretisk modell - kan tillvarata en systematisk blandning av regelstyrning, kapacitetsstyrning och lärande. Styrningen enligt förslaget kan sammanfattningsvis tolkas antingen som att staten fungerar som en meta-governor alternativt genom decentraliserade styrmedel i ett perspektiv av Governance där målgrupper, stakeholders, aktörer, beneficiaries etc genom förhandlingar kan finna gemensamma avgränsningar, mål, krav och utföranden.

1. Inledning

1.1 Uppdragets syfte och utgångspunkt

Uppdragets syfte är att presentera en kort analys av styrmedel användbara i en modell för informationssäkerhet. Utgångspunkten för analysen är dokumenten Kunskapsöversikt över decentraliserade styrmodeller, Tankar om styrmodell och NISU s 211-215. I Kunskapsöversikten diskuteras ett antal fallstudier av decentraliserade styrmodeller och vissa generella slutsatser föreslås. En mycket kortfattad rapportering av ”Styrning på IT-området” görs. Avsikten nu är att komplettera denna del med fallstudier från informationssäkerhetsområdet och därvid fånga in rapportörens egna reflektioner - såväl redan dokumenterade som nya – relaterade till decentraliserad styrning. Det förväntas att olika perspektiv fokuserar olika frågeställningar och kontexter – kan tidigare erfarenheter eller teorier vara behjälpliga i att identifiera viktiga/uppdykande frågeställningar? Hur kan innovation och proaktivitet behandlas i styrningssammanhang?

Flera av de frågor som nämns som förslag till vidare forskning i Kunskapsöversikten berörs i samband med fallstudierna från informationssäkerhetsområdet; tex vilka var de berörda aktörerna och hur uppfattade dessa möjligheter och hinder av decentraliserad styrning. Det bör också vara möjligt att analysera under vilka omständigheter goda eller mindre goda konsekvenser uppfattades.

Resultatet av denna studie skall kunna användas för fördjupade diskussioner relaterade till Hypotes för styrmodell i dokumentet Tankar om styrmodell. I den utökade Figur 1 från Kunskapsöversikten nedan har begreppen som används där sorterats in i figuren. Fallstudierna från informations-säkerhetsområdet nedan diskuteras i första hand utifrån dimensionen motivationsantagning.

	Government	**Governance**	**Meta-governance**
Källa till auktoritet	Staten	Olika aktörer (offentliga i privata)	
Relation	Hierarki	Nätverk	
Typ av förvaltning	Traditionell, regelstyrd, byråkratisk, webersk byråkrati	New Public Management; mål-o-resultat, kontrakt, målstyrning, granskning,	

		konkurrens, marknadsliknande	
Styrmedel	Hårda	Mjuka	kombinationer
	centraliserad	decentraliserad	
Dimension	Vertikal	Horisontell	
Motivationsantagning	Regelstyrd	Incitament; kapacitet; lärande; symbolisk	

Utökad figur 1 Kunskapsöversikten; sammanfattning av styrmodeller/medel

1.2 Moderna systemproblem – wicked problems

Kunskapsöversikten refererar till begreppet wicked problems i fallstudien över hur decentraliserade styrmodeller fungerar när det gäller vattenförsörjningen. ”Vattenfrågan betraktas av författarna som det som brukar benämnas ett wicked problem. Med begreppet avses problem som griper över flera områden, där förutsättningarna ständigt ändras, varför problemet aldrig kan lösas slutgiltigt. Det är dssutom ett område med många inblandade aktörer, alltifrån EU, länsstyrelser, kommuner och privata aktörer.”

Ur systemteoretisk synpunkt omfattar merparten av informationsrelaterade system wicked problems som kan ’lösas’ på olika sätt. Systemteoretiker använder i stället begreppet ’systemiskt’ problem och menar att det inte finns en garanterad bästa ’lösning’ utan olika sätt att ’hantera’ problemet. Ett annat sätt att förstå problematiken med systemiska problem är att omvärlden och systemet självt är ständigt föränderliga och därmed krävs att systemet kan lära sig att anpassa sig till förändringar, såväl kortsiktigt som långsiktigt. Det kan också vara så att systemen i ett längre tidsperspektiv ändrar förutsättningar för omvärlden. Systemen är komplexa och kan vara svåra att avgränsa gentemot omvärlden eller sin miljö. Problem med komplexa system med varierande osäkerhet torde idag snarare benämnas moderna systemproblem; hantering och styrning av dem uppmärksammas på många olika håll. Genomgående teman är att verklighetens system kräver mer holistisk syn för att överbrygga ’silo’ effekter och andra hinder för att kunna fortsätta vara framgångsrika i förändrings-, förnyelse- eller anpassningsarbete. Som en delmängd av systemteorier betraktas cybernetiken; läran om styrning och kontroll, som visar hur system styr mot mål genom negativ återkoppling, men också som styrform – positiv återkoppling - kan välja bland olika mål för att hitta/utvärdera andra/bättre målnivåer.

På senare tid har begreppen ’kreativa förstörelse’ och ’innovation’ fått fokus inom informationssystemuppbyggnad där kreativ förstörelse avser uppkomsten av så stora förändringar att systemen inte utan vidare kan anpassas utan kräver omstrukturering. Innovation torde vara ett liknande begrepp där förändringar sker som kräver omstrukturering av etablerade system. Merparten eller kanske alla system med wicked problems/systemiska

problem torde bäst styras genom decentraliserade styrmedel (incitamentsbaserade, kapacitetsskapande, symboliska, lärande) i ett perspektiv av Governance där målgrupper, stakeholders, aktörer, beneficiaries, etc genom förhandlingar kan finna gemensamma avgränsningar, mål, krav och utföranden.

Den fallstudie som valts för informationssäkerhetsområdet och som redovisas nedan visar klart på att problemen är av typen wicked/systemiska. Karlssons slutsatser i Kunskapsöversikten uppfattar jag som ett annat uttryck för detta: ”Den övergripande slutsatsen av både forskningsöversikten och de empiriska fallstudierna är att decentraliserade styrmodeller bör beaktas utifrån den **konkreta situationen** där de är tänkta att användas……dels rymmer företeelsen decentraliserade styrmodeller en så pass stor **variation** av konkreta styrmedel och **kombinationer** av styrmedel att det i varje situation bör konkretiseras vilken aspekt av styrmodeller som avses… Dels handlar det om vari det problem består som styrmodellerna antas kunna hantera.” Vidare nämner han fördelar såsom att stimulera innovation och kunskapsbyggande där ”det offentligas roll som meta-guvernör…kan kombineras på olika sätt i syfte att nå måluppfyllelse. I denna användning har det offentliga möjligheten att kombinera det mest hierarkiska styrmedlet, regleringar, med styrmedel som vilar på långtgående decentralisering som kapacitetsskapande styrmedel.”

2. Fallstudie Informationssäkerhet

Fallstudie Informationssäkerhet är byggd på två masteruppsatser vid Institutionen för Data- och Systemvetenskap[i].

> *”Under ett par decennier har tanken om en gemensam elektronisk ID-lösning för Sverige funnits. På 1990-talet verkade föreningen Säkrad Elektronisk Information i Samhället, SEIS, för detta syfte. SEIS bestod av flertalet aktörer inom statliga och privata företag och organisationer. Föreningen skulle arbeta fram en lösning för elektronisk identifiering, ett elektroniskt ID-kort, som skulle användas inom såväl offentlig fövaltning, industri som näringsliv. Denna lösning arbetades fram, men den blev inte allmänt använd, utan i dagsläget utnyttjas ett antal olika elektroniska identifieringslösningar. Dessutom var tanken från SEIS sida att det elektroniska ID-kortet skulle få stor spridning, men så har inte skett. SEIS visioner blev aldrig verklighet.”* (ur SEIS uppsatsens sammanfattning)

> *”I detta arbete har vi för avsikt att, med fokus på RSV, redogöra för den process som legat till grund för realiserandet av den elektroniska ID-handlingen och den fortsatta förvaltningen av den tekniska lösning som möjliggör den.”(*ur RSV uppsatsens sammanfattning)

Båda uppsatser berör ett nytt och inte tidigare ’löst’ problem; en innovation som forskningen medgett men som ännu inte fått spridning och användning praktiskt men som av många berörda betraktades som en tillräckligt mogen teknik att införas. Målet för SEIS uppsatsen var ”att kunna bidra allmänt till större förståelse för centrala frågor kring utveckling av stora IT-orienterade infrastrukturer”, för RSV uppsatsen ”att dokumentera den process som drivits för att få den elektroniska ID-handlingen till stånd, med speciell fokusering på RSV:s förehavanden” samt ”utgöra en bakgrundsbeskrivning för andra myndigheter, och även företag, i deras strävan att implementera en PKI-lösning av typen e-ID”. Metoden för SEIS uppsatsen var i huvudsak undersökning, problematisering, diskussion och faktasammanställning baserat på kvalitativa intervjuer av personer som medverkat i det centrala SEIS arbetet. Analysen av intervjuerna var Grounded Theory inspirerade. RSV uppsatsens metod utgick från en organisatoriskt orienterad beslutsstödsmodell som tagits fram av en tidigare masteruppsats (Wall&Joergensen, Masteruppsats 2002, DSV/SU) för implementering och integration av ett PKI-baserat säkerhetssystem, där RSV nu utgjorde en fallstudie. Studenterna använde deltagande observation samt det tidigare utförda arbete inom RSV fångades upp genom intervjer och dokumentationsgranskning.

2.1 Fallstudie ett: Säkrad elektronisk information i samhället, SEIS

Vid tiden för SEIS start i mars 1995 fanns redan tidigare flera initiativ inom e-ID området; inom den oberoende ideella föreningen SEIS skulle dessa kunskaper och erfarenheter tas tillvara på ett helhetligt sätt för att främja användningen för gemensamma metoder i samhället. Tankar om att projekten/produkter/tjänster skulle vara klara för användning allmänt i Internetmiljön sporrade deltagandet; tekniska, administrativa, sociala och juridiskt accepterbara normer skulle främjas och normer för utvärdering och användning av produkter och tjänster för säker elektronisk informationshantering i samhället skulle kunna göras tillgängliga och vid behov även utvecklas. Verksamheten skulle bedrivas i projektform. Siktet var i första hand inställt på Sverige, men även tankar om samverkan och påverkan med andra nordiska länder, europeiska länder och USA fanns. Ur några av rösterna: ”SEIS var en fortlöpande grupp för att få med sig samhällsbyggarna i det här, med bra kontakter i Regerings- och departementsfora.”, ”Nu ska vi ha ett ordentligt system i Sverige, som ska gynna Sverige…, som ska gälla alla, och vi ska även få med oss alla andra länder”, ” Det var även tänkt att det skulle gå rätt fort så att när Internet blev stort skulle allt detta vara på plats”.

Före SEIS fanns ett flertal föreningar och initiativ som utvecklade och undersökte olika aspekter av identifiering inför den kommande internetboomen. De huvudsakliga kraven utöver att användaren skall kunna vara anonym på nätet var att för olika typer av transaktioner, till exempel affärstransaktioner, krävdes en säker användaridentifiering samt att transaktionen i efterhand inte skall kunna nekas till. Ett europeiskt samarbete där Sverige deltog presenterade en rapport om säkra dataflöden och betalningar över gränserna under mitten av 1980-talet vilket ledde till föreningen Teletrust med grenar i flera europeiska länder med uppgift att utbilda, informera, och ordna seminarier om dessa frågor. Inom Teletrust utvecklade Siemens teknik möjlig för ett smartkort, dvs ett kort som svarade mot de uppställda kraven på säker identifiering och signering. Ett annat initiativ, Allterminalen, var ett samarbete mellan myndigheterna Rikspolisstyrelsen, Riksförsäkringsverket, Riksskatteverket och Datainspektionen med snarlikt syfte, men nu med fokus på svensk offentlig förvaltning att få fram en säker lösning för anställda vid myndigheterna. Inom banksektorn drevs projektet Strategisk samverkan med mål att utveckla en öppen lösning, tillgänglig för alla baserad på oberoende teknik med behörighetskrav för ett elektroniskt ID-kort med viss samverkan med Allterminalprojektet. Handelsbanken, Nordbanken, Skandinaviska Enskilda Banken, Sparbanken, Posten, Ikano Finans, Smart och Telia deltog. Det fanns också flera individföreningar inom informationsteknologi och säkerhet som studerade frågorna under denna tid samt givetvis internationella forskningsorienterade sammanslutningar såsom International Federation for Information Processing, IFIP, vars tekniska kommittee om informationssäkerhet med svensk ordförande hade hållit sin första internationella säkerhetskonferensen i Stockholm 1983. SEIS bildades av en styrgrupp från Allterminalprojektet där nationella organisationer och företag

inventerades; bl.a. nämndes Kommunförbundet, Landstingsförbundet, Försvaret, Rikspolisstyrelsen, Posten, bankerna från Strategisk samverkan, Ericsson, Volvo och Microsoft som medlemmar. Totalt omfattade SEIS ett femtiotal företag och organisationer och tanken var att genom dessa skulle en stor del av Sveriges befolkning täckas in. Man hade således förhoppning om en evolutionistisk utveckling. SEIS drevs som en ekonomisk förening finanserad genom medlemsavgifter och bidrag från bland annat ÖCB, Telia och Posten. Merparten av arbetet som utfördes ersattes av de enskilda medlemsföretagen och organisationerna. Ett tidigare förslag att bilda en stiftelse för arbetet hade förkastats. Föreningen existerade 1995-2000; i maj 2000 integrerades SEIS slutligen i föreningen Gemenskapen för Elektroniska Affärer, GEA. Verksamheter med elektroniska id-handlingar har pågått därefter i olika skepnader som Nätverket för Elektroniska Affärrer, NEA, e-nämnden för elektronisk förvaltning, 24-timmarsmyndigheten mfl. samtidigt som europeiska initiativ för att stödja rörlighet och affärer inom unionen ständigt pågår.

SEIS ändamål beskrevs vid konstituerande sammanträde den 24 mars 1995 som”Föreningen är en oberoende, ideell organisation som har till allmännyttigt ändamål att främja användningen av gemensamma metoder för säkrad elektronisk informationshantering i samhället.” Verksamheten skulle främja användningen av tekiska, administrativa, socialt och juridiskt accepterbara normer för säkrad elektronisk informationshantering, främja användningen av normer för utvärdering och användning av produkter och tjänster för säker elektronisk informationshantering, samt vid behov utarbeta sådana normer. 1998 när arbetet materialiserats vidare, beskrevs föreningens syfte som ”SEIS ska, för medlemmarnas räkning förvalta, utveckla och skapa acceptans för den elektroniska lösning för identifikation, signering och kryptering som föreningen tagit fram. Vi ska bevaka och påverka utvecklingen inom området så att företag och organisationer tar fram lösningar i form av tjänster, regelverk, produkter och system som möjliggör att vi i samhället skall kunna kommunicera elektroniskt på ett tryggt och säkert sätt”.

Arbetet organiserades i fyra arbetsgrupper: Elektroniskt identitetskort; framställning av digitala signaturer och elektronisk identifiering, Regler och tjänster; ligga som grund för uppdelning av ansvaret för tjänster och produkter, exempelvis administration av kortförvaltning, katalog och certifikatshantering samt kortutgivning, Tekniska plattformar; att specificera och certifiera produkter och funktioner som använder elektronisk identifikation, Användningsområden; att infoga säkerhetsfunktioner i epost, ehandel, samt terminal och andra användningsområden.

Föreningen styrdes ursprungligen av den initierande styrgruppen från Allterminalprojektet utökad med med representanter från banker och Statskontoret. Bland styrelsemedlemmar fanns ursprungligen både representanter från praktiskt verksamma säkerhetsexperter inom området och ledare inom medlemsorganisationer och företag. Mot slutet av föreningens tid blev styrelsen mer exekutiv och saknade djup teknisk kompetens. En av de intervjuade personerna noterade ”…en blandning är det bästa…man ska ha av

alla sorterna, men jag hade nog gärna sett att det hade varit fler praktiker även i fortsättningen…”

SEIS påverkade och samverkade med Finland och Estland för deras utveckling och användning av id-handlingar för elektroniska system. Finland realiserade ett medborgarkort som hade stora likheter med SEIS förslag, Estlands lösning utvecklades delvis baserat på SEIS arbete. En delegation från SEIS till USA resulterade i visst intresse för den svenska lösningen och företaget RSA utvecklade delvis baserat på SEIS en ny standard. Även inom IETF, Internets standardiseringsorgan, och ETSI, det europeiska standardiseringsorganet har visst arbete från SEIS kunnat användas. Vid tiden för SEIS arbete – före händelserna i USA 9/11 – var användning av personnummer – en form för unik identifiering av personer – starkt ifrågasatt. För att minska risken för felidentifiering innehöll SEIS’ standardspecifikation tre krypteringsnycklar; en för identifiering, en för kryptering och en för signering, vilket inte heller accepterades internationellt.

I den analys som gjordes baserad på intervjuerna av SEIS personer, sammanfattas vilka positiva respektive negativa faktorer som påverkade SEIS utveckling och genomslagskraft. De externa faktorer som ansågs positivt påverka utveckling och genomslagskraft var teknik och samhälle; tekniken fanns men behövde vidareutvecklas och samhället /uppfattades ha/ ett behov av säker identifiering för att kunna utnyttja internet effektivt; det vi idag uppfattar som e-samhället/e-förvaltning. Dessvärre var det fler externa negativa faktorer som påverkade: ekonomi, regering och riksdag, USA, Europa, samhället samt en grupp personer benämnda ’internetgurus’. Interna viktiga faktorer som framkom genom intervjuerna var i huvudsak tre grupper: människorna, Ideerna/visionerna, Företag/organisationer. Att styra och leda dessa visade sig inte helt lätt; en av intervjupersonerna sammanfattade som svar på frågan Vad skulle ni ändra på om ni fick starta om utredningen 1995 med den erfarenheten ni har idag? ” Det hade varit viktigt att förankra projektet hos de som var emot SEIS. Man borde analyserat mer vad alla deltagare ville med SEIS innan arbetet började. Ett närmare och mera aktivt samarbete mellan styrelse och grupper(projekt) hade varit önskvärt. Det borde ha funnits bara en CA-verksamhet. Regeringen eller ett departement borde agerat som beställare till SEIS projektet. Och slutligen, det kunde kanske inte bli annorlunda eftersom ”internethypen” störde en hel del och företagen ville få snabba vinster.” Uppsatsförfattarna dristade sig att säga:”Vi konstaterar att SEIS arbete till viss del utvecklats vidare men funderar över varför inte kunskaperna och erfarenheterna tagits tillvara när det påbörjas nya utredningar.”

2.1.1 Analys fallstudie ett

SEIS är att initialt betrakta som ett **symboliskt projekt** där deltagarorganisationer var innifrån styrda av sin starka uppfattning om behovet av säker elektronisk identifiering med hjälp av ett smartkort som visuellt var ett vanligt ID-kort med foto, namn och personnummer och som elektroniskt innehöll funktioner för identifiering, signering och kryptering.

Man hade också en stark tro på att Sverige, även internationellt , skulle kunna gå i bräschen för detta tänkande och kanske upprepa möjligheten att påverka utvecklingen såsom man gjort i samband med integritetslagstiftningen. Grundarna, med förankring inom statsförvaltningen, såg möjligheter att tillsammans med näringslivet driva utvecklingen helhetligt. Flera av deltagarna – både från offentliga organisationer och näringsliv - hade tidigare erfarenheter av hur arbetet inom Sårbarhetsberedningen och –kommitteen hade givit praktiska och positiva resultat inom informationssäkerhetsområdet i Sverige. Att säkerhetsarbete inom området måste bedrivas med hänsyn taget till lagar och regler, organisatoriska och ekonomiska förutsättningar samt teknik och teknisk utveckling var en utgångspunkt för merparten av informationssäkerhetsarbete. Internationellt var arbetet inom Sårbarhetsberedningen och – kommitteen välkänt och Sverige åtnjöt ett stort anseende. Trots nedläggningen av Sårbarhetsberedningen i mitten av 1980-talet med däravföljande ansvarsuppdelning för styrning och reglering av offentlig verksamhet för sig, fanns de informella nätverken av kompetenta personer kvar – nu många som SEIS grundare men också som deltagare i olika nationella och internationella aktiviteter som redogjorts för ovan.

Mycket talar för SEIS som ett **symboliskt lett** projekt. Deltagarna var kunniga i tekniska, organisatoriska och juridiska frågor och såg framtiden med ”informationshighways” som stora möjligheter både för näringsliv och offentlig förvaltning men uppfattade att politiker inte var tillräckligt kunniga eller hade förstått säkerhetsproblematikens betydelse för den framtida utvecklingen. ”Man kom på att SEIS skulle vara en alldeles utmärkt politisk plattform att påverka säkerhetsfrågor när det gäller regeringen. Och behovet av säkerhetslösningar och påverka införandet av digital signatur.”, ”Man hade tänkt sig att man skulle nyttja standarden och få ett kort för många ställen, det var inte direkt målet, men man drömde om sådana saker. Postens ID-kort kan användas för det mesta så man hade tänkt att det här skulle kunna användas för mycket mer.”, ”Det ena målet var att man skulle få med så många som möjligt av de olika nordiska länderna, och man skulle inte glömma bort att det stora landet var Amerika. Det har alltid varit Amerika, och har man inte med sig dem kan man lika gärna glömma det. Det var inte helt orimligt för Amerika var väldigt intresserade av svensk säkerhetsteknik och köpte ett antal svenska säkerhetsbolag.” Författarna noterar även att många deltagare brann för säkerhetsfrågor och samtidigt var vana vid att säkerhetsarbete inte uppmärksammas annat än vid stora händelser och därför var övertygade om att ”Om vi ger ut ett kort på tillräckligt säkert sätt, så kan bankerna använda sig av detta och alla de som då vill koppla in sitt kort i deras system och då kommer de till sina konton via vanliga personkort.”

SEIS var ett försök- huvudsakligen symboliskt värderingsstyrt - att utan reglering uppifrån, utan governance, påverka hur reglering kan/ska ske. Det fanns vid denna tid många olika och starka uppfattningar om ’bästa’ lösning men avsaknad av politisk vilja eller tilltro till en marknadslösning gjorde i stället att SEIS arbete **blev kapacitetsskapande** och i stället stimulerade till fortsatt experimenterande och innovation i olika fortsättningsprojekt. SEIS

försökte skapa ett lärande styrmedel genom att utveckla standarder men nådde inte ända fram.

Vilka var de berörda aktörerna: uppläggningen av SEIS avsåg att få med så många olika aktörer som möjligt -såväl offentlig förvaltning som näringsliv- i projektet för att på sätt skapa tillräckligt goda produkter, tjänster, system och standarder.

Vilka möjligheter och hinder utgjorde decentraliseringen: konstruktionen som ett symboliskt styrt projekt/förening utan klar beställare utgjorde ett hinder för styrning av verksamheten när produkten tagits fram och pengarna tröt.

Vilka omständigheter gav goda eller mindre goda konsekvenser: det fanns ingen självklar beställare såsom tex regering, riksdag, branschorganisation, sektorsorgan el dyl; snarare var det så att SEIS skapades som förening för att vara en möjlig påtryckare genom att kunna demonstrera hur produkten elektroniskt ID kort skulle kunna lösa säkerhetsproblem på ett ensat sätt för både offentlig och privat verksamhet. Tiden var helt enkelt inte rätt att introducera ett allmängiltigt koncept byggt på unik identifiering av individer.

2.2 Fallstudie två: Kartläggning av RSV:s process att införa e-ID

(eller the devil is in the details)

Arbetet med RSV:s införande av e-ID pågick 2001-2003 men kan ses som ett arbete i tiden. Flera nationella och internationella initiativ påbörjades som tidigare beskrivits under hela 1980-talet. Därutöver hade Tulldatasystemet 1990 visat praktiskt vilka förenklingar företag upplevde med att kunna lämna export- och importdeklarationer elektroniskt via Tullens EDI, Electronic Data Interchange, system. Realisering av systemet hade krävt ändring i tullagen (1987:1065) till att medge begreppet elektroniskt dokument. 1994 initierade regeringen flera initiativ: budgetpropositionen (Prop 1993/94:100) presenterade riktlinjer för utveckling av den elektroniska infrastrukturen för informationsförsörjning, IT-kommissionen som ett samarbete mellan näringsliv och förvaltning för att främja bred användning av informationsteknologin skulle fokusera på användare och applikationer och Toppledarforum, som informell samverkans- och arbetsgrupp mellan myndigheter, däribland RSV, och tunga organisationer ledd av finansministern skulle bidra till att förverkliga målen i budgetpropositionen om en öppen elektronisk infrastruktur. RSV hade också erfarenheter från sina tidigare projekt och ambitioner att använda digital teknik för informationsutbyte med företag, att minska sin pappershantering och förenkla arkivfrågor, till exempel 1992 då standardiserade räkenskapsuppgifter, SRU, kunde lämnas in elektroniskt.

I alla föreslagna fall aktualiserades juridiska, organisatoriska och tekniska frågor aktuella inom infrastruturen såsom identifiering, signering, tidsbestämning mm, vilka beskrevs ingående i utredningen Elektronisk dokumenthantering inom skatteförvaltningen, finansdepartementet 1994(DS 1994:80) och som resulterade i en i stort sett identisk proposition (Prop 1994/95:93). Undantaget var att inget beslut kunde tas om att godta elektroniskt lämnade deklarationer. SEIS arbetet startade 1995 som en förlängning av Allterminalen och Strategisk samverkan som tidigare beskrivits, och pågick 1995 – 2000. RSV var en av de drivande myndigheterna där. Ytterligare hade regeringen 1999 uppdragit till Statskontoret att utreda kraven på säker elektronisk överföring av dokument och meddelande till, från och inom statsförvaltningen. Förarbetet hade gjorts inom ett samråd mellan Arbetsmarknadsstyrelsen, Centrala Studiestödsnämnden, Lantmäteriet, Patent- och Registreringsverket, Riksarkivet, Riksförsäkringsverket och Riksskatteverket. Samma år skapades också begreppet 24-timmarsmyndigheten; 2000 kom Statskontorets rapport ”24-timmarsmyndighet – Förslag till kriterier för statlig elektronisk förvaltning i medborgarens tjänst.”

2000 initierade RSV:s verksledning ett pilotprojekt för att lämna elektroniska skattedeklarationer med syfte att studera krav på den tekniska infrastrukturen och ge underlag för beslut om säkerhetsnivåer. Projektet använde mjuka certifikat, dvs implementerade inte SEIS konceptet med ett smartkort.

Till skillnad från SEIS föreningen hade RSV ett regeringsuppdrag att under ett inledningsskede ha sammanhållande ansvar för administration av cerifikat för elektronisk identifiering och elektroniska signaturer inom statsförvaltningen. (ingen kryptering tv) Uppdraget hanterades av RSV i projektet SAMSET, Samhällets Elektroniska Tjänster, tillsammans med PRV, RFV och Statskontoret och omfattade att utarbeta allmäna riktlinjer och gemensamma rutiner för certifikatshantering inom statsförvaltningen, samodna statsförvaltningens krav och behov inför upphandlingen och avrop av cerifikat och tillhörande tjänster för elektronisk identifiering och elektroniska signaturer, att samordna myndighetsgemensamma tjänster som krävs för väl fungerande infrastruktur för användning av elektroniska signaturer i statlig verksamhet och svara för information och vägledning till myndigheterna i dessa frågor (Ju2000/4939). Samtidigt skulle SAMSET samverka med banker och andra privata aktörer med en samordnad PKI-lösing som slutligt mål. Ett gemensamt medborgarcerifikat med personnummer som del skulle också realiseras. Således kom RSV och SAMSET arbete att systematiskt leda, utveckla, implementera och dokumentera innovationen PKI-lösning för säker kommunikation mellan RSV och samtliga av Sveriges myndiga invånare. Alla beslut kunde i förväg inte förutses och utvecklingen av tekniken som var basen för elektronisk identifiering var också stadd under utveckling; projektet innehöll ett flertal systemiska problem och därmed hörande avvägningar.

Fallstudien redovisar arbetet utifrån beslutsstödets sex steg: Beslut/övervägande om PKI, Förberedelsefas, Kravställning, Beslut om tillvägagångssätt, Införande, Drift och förvaltning. SAMSET bedömdes som ett

strategiskt projekt med flera underliggande mer operativa projekt. Styrningen skedde genom en styrgrupp bestående av RSV:s IT-chef som projektledare, överdirektören på Statskontoret samt representanter för PRV och RSV. Kontakt hölls veckovis mellan projektledaren och överdirektören på RSV och viktiga beslut fattades i samråd med RSVs verksledning. Samordning om avrop skedde mellan ledningspersoner på RSV och RFV för genomförande av avrop, teknik och säkerhet samt verksamhetsfrågor - ”arbetet kom att utvecklas så att rapporterna från teknikgruppen och verksamhetsgruppen fungerade som underlag för den grupp som genomförde avropen” (ur intervju med RSV säkerhetsexpert). RSV-IT ledde arbetet att utveckla en teknisk lösning, för införandet engagerades den ordinarie drift- och supportorganisationen och för förvaltningsansvaret utsågs en person på RSV-IT. RSV hade genom sitt tidigare pilotprojekt (RSV Rapport 2000:15) och engagemang av olika personer i många aktuella utredningar redan en betydande kompetens och erfarenhet som också kompletterades under arbetet med spetskompetens inom säkerhets-, strategi- och juridik områdena. Här var RSV’s nätverk genom deltagande i pågående och tidigare verksamhet av värde. För den tekniska implementeringen styrde existerande applikationer från pilotprojektet som använde mjuka certifikat – således kom avtalet att tecknas med BIDT (bankernas ID lösning) även om RSV förorsakades ytterligare utveckling för en serverlösning, och trots att det uttalat skulle vara önskvärt med hårda certifikat, dvs kort. RSV hade tidigare under utredningarna om säkerhetsnivåer konstaterat att mjuka certifikat skulle vara tillfyllest för säkerhetsnivåerna klass 1-2, medan den högsta säkerhetsnivån, klass 3, skulle förutsätta en kortbaserad lösning. I beslutssituationen resonerade RSV att eftersom det krävdes att skadeståndskrav skulle kunna riktas mot den som utfärdat det kvalificerade certifikatet och samtidigt fri bevisföring och bevisprövning gäller så bedömde RSV inte eventuella tvister som allvarliga. ”Skulle det uppstå tvist gällande en deklaration kan lösningen helt enkelt vara att göra om deklarationen” (intervju med ansvarig på RSV). ”Valet berodde framförallt på försörjningen av e-ID-handlingen, där BIDT:s lösning gav bäst förutsättningar att nå en kritisk massa med den omfattande kundbas och den enkelhet som lösningen medför för kunden ” (ur intervjuer av säkerhetsexpert på RSV/IT och projektledaren för SAMSET), dvs man gjorde avsteg från tidigare tagna beslut om kortimplementering för att försäkra sig om att antalet användare skulle bli tillräckligt många; i Finland hade det visat sig svårt att få en tillräcklig kritisk massa av användare mycket beroende av de administrativa kraven som ställdes på utställningen av korten samt att dess användning krävde tillgång till en kortläsare. Med BIDT:s lösning fanns redan kunder som tog omaket som krävdes att skaffa, implementera och använda en mjuk lösning. Det finns flera exempel i fallstudien på att beslut inte fanns dokumenterade eller tycks ha fattats informellt: ”Besluten är inte heller dokumenterade i alla lägen utan har en tendens att växa fram och med tiden bli allmänt vedertagna.” och ”Straxt efter det att rapport 2000:15 publicerades fattades ett informellt beslut om att tanken på att upprätta en statlig CA skulle överges totalt. I detta senare skede hade man nämligen klarare insett problemen som en statlig CA skulle ha inneburit för myndigheterna.” (i intervju med projektledare).

2.2.1 Analys fallstudie två

RSV:s projekt att införa e-ID kan betraktas delvis ur synpunkten decentraliserad styrning med förankring i governance; i första hand som **kapacitetsskapande** inom SAMSET men också som **lärande styrmedel** för hela statsförvaltningen. Det fanns också initialt ett inslag av **ekonomiskt incitament** men utredningar konstaterade att även om vinster uppstod i form av till exempel mindre handläggningspersonal så uppstod nya utvecklingskostnader; vinsterna skulle i stället ligga i ett framtidsperspektiv. Karlsson anger i Kunskapsöversikten för kapacitetsskapande styrmedel att det skall främja beteende, ge kunskap/information/resurser samt stimulera till innovation, och för lärande styrmedel att ingen självklar lösning finns, målgruppen får själv göra utvärdering, det finns utrymme för experimenterande samt inget tvång föreligger.

Fördelen för RSV var att det fanns en beställare: uppdraget gällde statsförvaltningens administration av certifikat för elektronisk identifiering och elektroniska signaturer även om det också fanns önskemål om involvering av näringslivet som till exempel leverantör av tekniska lösningar. Det fanns ingen självklar lösning – målet var klart men hur man bäst skulle komma dit var inte stipulerat. RSV gjorde själv utvärderingen; till exempel att välja mjuka certifikat trots att säkerhetskraven delvis motsade detta - och det fanns utrymme för experimenterande vilket gjordes både genom pilotprojekt och under lösningens gång.

Troligtvis hade man lärt sig genom sina erfarenheter att ett komplext system som detta behövde krav eller förslag på reglering, men man behövde experimentera med och resonera om olika möjliga utfall. Att man också hade tillgång till RSV's IT avdelning torde haft stor betydelse för experimenterandet som kunde utföras lokalt och snabbt för återkoppling till kunniga beslutsfunktioner. Även det faktum att resultatet i första hand skulle gälla enbart för statsförvaltningen var troligen en fördel eftersom det var ett system som man var väl förtrogen med. Genom SAMSET's medverkan som strategiskt projekt kunde man också överbrygga 'silo' effekter som oftast nämns som återhållande kraft inom statliga organisationer.

Vilka var de berörda aktörerna: I första hand gällde uppdraget statsförvaltningen med RSV tillsammans med SAMSET (RSV, PRV, RFV och Stadskonkoret) som huvudsakliga aktörer även om uppdraget i förlängningen även gällde riktlinjer för utveckling av hela den elektroniska infrastrukturen för informationsförsörjning för att främja en bred användning. Avvikelsen från ursprungliga krav på hårda certifikat för högsta säkerhetsklass möjliggjorde att främja användning av merparten av allmänheten.

Vilka möjligheter och hinder utgjorde decentraliseringen: möjligheten/förmågan att kunna fatta informella men väl underbygda beslut när omständigheter så krävde utgjorde en klar fördel.

Vilka omständigheter gav goda eller mindre goda konsekvenser: RSV hade tillgång till både egen och extern expertkunskap samt en egen IT avdelning som deltog praktiskt i arbetet.

2.3 Sammanfattning analys, styrmodeller och styrverktyg i fallstudierna

Vilka styrverktyg kan urskiljas eller efterfrågas: För RSV fallet framstår kombinationen av kapacitetsskapande och lärande styrverktyg ha utgjort framgångsfaktorer. Hela projektet vilade dock på att det fanns en beställare; vad som i Kunskapsöversikten benämns styrmedel i perspektiv av Governance. SEIS hade ingen beställare, projektet var symboliskt styrt av deltagande organisationer och personer. En tolkning genom Kunskapsöversikten är att det var en horisontell, decentraliserad, frivillig och marknadsorienterad interaktion – ett självstyrande nätverk - mellan offentliga och privata aktörer som ursprungligen hade fastlagt överordnade ramar, men som med tiden blev mindre intresserade av att deltaga med expertis och medel; omvärldsfaktorerna upplevdes som oklara.

Vad i fallstudierna är av relevans idag? Båda fallstudierna hade som utgångspunkt att realisera en innovation och att bidra till en standardisering som tillsammanstagna skulle få en genomgripande påverkan på informationssäkerheten för hela samhällets informationsförsörjning. SEIS mål var att påverka också internationellt medan RSV's mål gällde Sverige. Idag fungerar RSV's lösning i samhället parallellt med många andra elektroniska identitetslösningar, främst för olika ekonomiska kortlösningar och integrerat i hela telecomvärlden. Dagens slutanvändare förväntar sig viss säkerhet för sina tillämpningar – eller snarare uppfattar att det existerar säkerhetsrisker inom I&K tillämpningar men har låga kunskaper om vad de själva kan göra för att minska riskerna och utgår därför ifrån att säkerheten till del är tillgodosedd inom ramen för systemen. Fallstudierna visar hur större innovativa samhällsgenomgripande informationssäkerhetsprojekt framgångsrikt kan bedrivas av myndigheter och organisationer tillsammans i Sverige, givet en beställare som kan ge utrymme för experimenterande och försöksverksamhet. Informationssäkerhetskollektivet är vana vid att arbeta med de begränsningar som utgörs av juridiska, organisatoriska, tekniska och till viss del även sociala frågor, och har genom praktiska erfarenheter mestadels tillräckligt god överblick och kunskap om sitt område för att kunna delta i decentraliserade kapacitetsskapande och lärande styrningsformer.

Globalisering/mindre tydliga gränser och barriärer/starkare marknadsaktörer: betydelsen av fungerande informationssäkerhet är större i dag än vid tiden för de två fallstudierna just pga globalisering, mindre tydliga gränser och starkare marknadsaktörer. Det innebär dock inga hinder för att en styrmodell för informationssäkerhet som föreslås i NISU skulle kunna inspireras av uppbyggnaden av erfarenheter från redan gjorda

informationssäkerhetsprojekt. Att fungera som en kombination av kapacitetsskapande och lärande system med en klar beställare.

Incitamentsstyrd: ekonomisk	**Kapacitetsskapande**	**Symbolisk**	**Lärande**
RSV (delvis)	RSV	SEIS	RSV

Figur 2 Sammanfattning decentraliserade styrmodeller i fallstudierna

Kapacitetsskapande	**Symboliska styrmedel**	**Lärande styrmedel**
Främja beteende, Ge kunskap, information, resurser, Stimulera innovation, Strategisk - långsiktig	Målgrupp följer styrmedel som är i linje med dess värderingar, Värde- och innifrån styrda aktörer	Inget tvång, ingen självklar lösning, Målgruppen gör själv utvärdering, Utrymme för experimenterande, Benchmark, standarder, ranking, Granskande; utvärdering, tillsyn, revision, Aktivitetsfrämjande (mitt tillägg)
RSV: SAMSET som strategiskt organisations-överbryggande grupp med definierat regeringsuppdrag, Egna interna tester och pilotprojekt , Deltagande i externa samverkans- och arbetsgrupper	SEIS: erfarenheter från Allterminalen (statlig organisation) och Strategisk Samverkan (banker i samverkan), Eftersträvade smartkort med personnummer och tre separata kryptonycklar, Informations- och kunskapsskapande för omvärlden	RSV: Ansvar för en central statlig tillämpning med många kopplingar till statliga och ekonomiska organisationer, Ingen självklar lösning, Möjlighet till /inhouse/ experimenterande, Aktiv IT verksamhet

Figur 3 Sammanfattning styrverktyg använda i fallstudierna

3. Tankar om en styrmodell för informationssäkerhet, inspirerad bl.a. av Hypotesen för styrmodell

Jag ser **fyra nivåer** på ett system, men vill sortera de annorlunda än som uttryckts i Hypotesen. I **basen** ligger Juridiska krav/normering som gäller alla som berörs av reglerna. Styrmedel reglerande (i fallstudierna de regleringar och lagar som man utan prut vet gäller för tillämpningarna och som inte direkt diskuteras annat än som begränsningar eller utgångsvärden). Nästa lager utgörs av den **kapacitetsskapande** delen som uppfattas som den därnäst minst föränderliga; ”Geist” eller ”beställare”. Den innehåller mer statisk kunskap dvs ’state-of-the-art’, Best Practise, standarder; den är normativ. Den kan vara ”endast för anslutna, gemensamma informationklasser, skyddsnivåer m.m., möjliggör gemensam kravställning”. Som jag uppfattar SAMFI diskussionsdokumentet Styrmodell för informationssäkerhet är det lagret Kapacitetsskapande som diskuteras i en gemensam styrmodell (beskriven som: sammanhållen helhet, roller och ansvar, gemensamt regelverk, strategiska och operativa regler, riskanalys och nationell riskhantering, informationsklassificering, upphandling, kunskapsförsörjning, kommunikation-terminologi, uppföljning) eventuellt med urskiljande av ”kunskapsförsörjningen”. Jag uppfattar detta lager som det som skall göras av alla parter som är anslutna, dvs statsförvaltningen tillsammans med anslutna privata (nationella och internationella) organisationer. Eventuellt skulle det kunna delas in i sektorer, branscher etc men ses som en helhet tillsammans. Det överordnade syftet med detta lager är att styra genom att möta variation/förändring med variation i enlighet med cybernetikens terminologi och förståelse: vi kan bara hantera osäkerheten dvs variationen genom att möta den med tillräcklig variation. Målet – som aldrig nås i en föränderlig miljö – är att bringa ner osäkerheten i komplexa system utan att ta bort komplexiteten; därmed anpassas systemet kontinuerligt till sina – likaledes föränderliga – förutsättningar. I likhet med Ackoff’s[ii] begrepp ’idealiserad design’ som leder till ideal-sökande system. Till del uppfattar jag att MSB’s existerande verksamhet inom informationsäkerhetsområdet är kapacitetsskapande, enligt Kunskapsöversikten sammanfattas det med att främja beteende och därför ge kapacitet (kunskap, information, resurser) och stimulera innovation. Till det vill jag lägga till uppföljning och återkoppling mot ställda krav[iii]. Jag tolkar ’stimulera till innovation’ som kunskapsskapande – inte direkt aktiviteten att utföra innovation, vilken jag vill hänföra till nästa lager det **lärande**, som jag ser som det lager som ”skapar möjlighet för samverkande aktörer att (ev) bilateralt ensa arbetssätt och konstruera egna modeller/överenskommelser för interoperabilitet…etc” enligt beskrivningen i Hypotesen. Det lärande skiktets huvudsyfte är att styra förändring, utveckling, innovation, och proaktivitet genom experimenterande och aktiviteter; ett laboratorium. I enlighet med

cybernetiken, att öka variationen i verkligheten genom experimenterande för att eventuellt hitta nya styrsätt eller -nivåer. Det lärande lagret har givetvis koppling till det kapacitetsskapande; effekter av deras utveckling och innovation kan innebära krav på förändring av normer och 'state-of-the-art' för det dagliga arbetet, och kopplingen medger evidensbaserat agerande baserat på utförda experiment. För att avgöra när normer eller 'state-of-the-art' skall förändras i det kapacitetsskapande lagret fordras en **övergripande beslutsnivå** – det jag uppfattar SAMFI utgör idag, men som troligen borde utökas med inte bara säkerhetsorienterade myndighetsrepresentanter utan också med representanter från X(näringslivsorienterad, hälso- och sjukvårdsorienterad) som kan bidra med att styra informationssäkerhetsarbetet i Sverige också mot synen som redogörs för i OECD's Recommendation on Digital Security Risk Management for Economic and Social Prosperity 2015[iv], fortsättningsvis kallad SAMFI+.

Två viktiga 'key messages' inleder OECD Rekommendationerna: "First there is a focus on the economic and social objectives of public and private organisations and the need to adopt an approach grounded in risk management. Instead of being treated as a technical problem that calls for technical solutions, digital risk should be approached as an economic risk……Second there is a recognition that through dynamic management, security risk can be reduced to a level deemed acceptable relative to the economic benefits expected from the activities at stake…". Av detta följer att definitionen av säkerhet ("the state of being free from harm or danger") som ett binärt och statiskt tillstånd ersätts med begreppet säkerhetsrisk för sociala och ekonomiska aktiviteter som är beroende av den digitala omgivningen/miljön; säkerhet blir ett adjektiv som karaktäriserar risk, riskfaktorer och riskhantering och relaterar mer till en holistisk syn. Samtidigt behöver man inte använda begreppet cybersecurity som, det påpekas i Rekommendationerna, förstås olika i olika kulturer. (Och, skall tilläggas är relaterat till vetenskapen cybernetik som diskuterar kontroll- och styrtekniker utan relation till någon speciell kultur.)

Rekommendationerna innehåller både övergripande och detaljerad information; dokumentet är indelat I en kortfattad del som beskriver Principer (fyra generella och fyra operationella) och en fylligare förklarande del (Companion Document) som detaljerat beskriver digital security risk management cykliskt med återkopplingar. De generella principerna (Awareness, skills and empowerment; Responsibility; Human rights and fundamental values; Co-operation) fungerar som pelare för de operationella principerna (Risk assessment and treatment cycle; Security measures; Innovation; Preparedness and continuity). Val av explicit säkerhetsfunktionalitet (security measures) värderas mot givna värden i sociala och ekonomiska termer. "It prevents decisions from being made in isolation, from a separate technical or security point of view."

En nationell styrmodell ska enligt NISU sid 211-214 beakta:

Föränderligt sätt att bedriva verksamheten, implicerar myndighetsöverskridande och kunna inkludera privata aktörer; olika aktörer,

Lagstiftning kompletteras med olika former av avtal; lagar, regler, normer, standarder, och

Det offentliga behöver vara kvalificerad beställare med möjlighet att stärka utvecklingen hos enskilda organisationer och gemensam infrastruktur; kunskap, innovation, proaktivitet.

4. Förslag till konceptuell styrmodell

Bas. Styrmedel Reglerande: enligt Hypotesen. Gäller alla som berörs av reglerna – i första hand offentliga organisationer. Utgör just en bas.

Geist/Beställare. Styrmedel Kapacitetsskapande. Mål: att minska variationen och avvikelser, dvs öka säkerheten genom systematiskt arbete och uppföljning : Uppsättning bindande regler och riktlinjer som bygger på externa krav och befintligt existerande kunskapsstöd såsom normer, standarder, informationsklassificering, gemensam terminologi, riskanalyser, etc omfattande minst innehållet i MSBFS 2009:10. Olika varianter av samma typ som MSBFS2009:10 kan upprättas för olika branscher/sektorer/offentliga organisationer/privata organisationer. Uppföljningar görs både internt (inom organisationen)och externt (av Geist) för att garantera följsamhet, höjd kunskap och förståelse samt ökat fokus på informationssäkerhet. Någon form av ackreditering för anslutna organisationer.

Framtidsorienterad anpassning. Styrmedel Lärande. Mål: att experimentera/testa innovationer och nya former/modeller/standarder/tekniker för informationssäkerhet, dvs möjliggöra förändring, utveckling, innovation och proaktivitet. Nya kunskaper avses överföras till Geist efter tillbörliga beslut därom. Utvecklings- och forskningsorienterad think tank inom informationssäkerhet/digital security risk management for economic and social prosperity. Fordrar 'utblick', dvs inte bara ta del av resultat i Geist utan följa utveckling och forskning internationellt och nationellt.

Visionsbaserad och identitetsskapande ledning, SAMFI+, ansvarig för bedömning och beslutsfattande rörande vikten av fokus för hela styrmodellen där Geist kommer att arbeta mot ensad verksamhet – stabilitet - medan Framtidsorienteringen kommer att arbeta mot förändring – instabilitet. SAMFI+ skapar beslutsunderlag och direktiv för förändring i Geist.

Förslaget är inspirerat av Beers modell för Viable Systems (Beer 1972, 1979, 1985); som beskriver fem olika delsystem: det operativa utförande, det biträdande med arbetsformer, standarder mm, det samordnande i nutid, det framtidsorienterade, det identitetsskapande. I förslaget ovan utgörs de av: **organisationernas egna arbete, Basen, Geist, Framtidsorienterad anpassning, Visionsbaserad och identitetsskapande ledning SAMFI+.**

Det existerar många olika beskrivningar i litteraturen över Beers Viable System Model och dess användning; huvudargumentet här för att använda den som inspiration och konceptuell förståelse av de stora och omfattande arbete som

styrmodell för informationssäkerhet utgör är att myndigheter och organisationer själva skall göra arbetet som skall koordineras/styras på ett helhetligt sätt. Det har konstaterats tidigare att informationssäkerhetsproblem är systemiska/wicked problems, dvs det finns inte en slutlig lösning utan det existerar många olika sätt att hantera problemen. Som visats i fallstudierna är det både detaljkunskaper och kunskap om de stora sammanhangen som har betydelse för att kunna vara framgångsrik – det behöver byggas upp kunskaper och erfarenheter som kan användas framöver samtidigt som dagens problem måste lösas på ett tillfredsställande och operativt fungerande sätt. Organisationer behöver både ha kortare målbilder att uppnå (från Geist) men också kunna förändra sitt beende och därmed mål i ett längre perspektiv (från Framtidsorienterad). För beslut om vikt mellan Geist och Framtidsorienterad finns SAMFI+[v].

Decentraliseringen tillgodoses således genom arbetet inom de olika organisationerna som vilar på juridiska krav och normer giltiga för branschen/sektorn/motsvarande stöds av **basen**. Decentraliseringen tillgodoses även inom **Geist**; genom att följa uppställda bindande regler och riktlinjer kan organisationerna själva detaljstyra sitt arbete samt visa genom uppföljningar begärda av respektive ackrediteringsform – myndigheter, offentlig förvaltning, näringsliv etc – att så är fallet. Här finns också möjlighet inom GEIST (eventuellt uppdelat på olika ackrediteringsgrupper) att bedöma krav på förändringar för att nå myndighetsöverskridande/motsvarande effekter. Decentraliseringen kan vidare tillgodoses inom **Framtidsorienterad anpassning och inlärning**, först genom förändring/utveckling/innovation/pro-aktivitet och därnäst som en möjlighet också för GEIST att inkorporera till exempel nya arbetsformer och standarder efter **beslut av SAMFI+.**

Styrningen enligt förslaget kan antingen ses som att staten fungerar som en meta-governor alternativt genom decentraliserade styrmedel i ett perspektiv av Governance där målgrupper, stakeholders, aktörer, beneficiaries etc genom förhandlingar kan finna gemensamma avgränsningar, mål, krav och utföranden.

5. Referenser

Stafford Beer: Brain of the Firm: A Development in Management Cybernetics. New York: Herder and Herder, 1972

Stafford Beer: The Heart of Enterprise, New York: John Wiley, 1979

Stafford Beer: Diagnosing the System for Organizations. New York: John Wiley, 1985

Jan Ytterholm och David Åhs: Kartläggning av RSV:s process att införa e-ID, Masteruppsats rapport 03-67 DSV-SU, Institutionen för Data- och systemvetenskap, Stockholms universitet, 2003

Eva Blix och Ingela Pihlström: Var SEIS mission impossible? – en djupdykning i delar av den svenska IT-historien, Masteruppsats rapport 05-14 DSV-SU, Institutionen för Data- och systemvetenskap, Stockholms universitet, 2005

En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter, MSB740 – Augusti 2014

Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten Betänkande av NISU 2014 SOU 2015:23

Russel L Ackoff et al.: Designing a National and Technological Communication System, University of Pennsylvania Press 1976

Arbetsmaterial:

Tankar om styrmodell med Hypotes om styrmodell

Styrmodell för informationssäkerhet

Lars Karlsson: Kunskapsöversikt över decentralicerade styrmodeller, Förvaltningshögskolan, Göteborgs universitet, Februari 2016

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSBXXX - Månad År ISBN 978-91-7383-XXX-X

[i] Föreningen Säkrad Elektronisk Information I Samhället, SEIS av Blixt&Philström, Masteruppsats 2005, DSV/SU och Kartläggning av RSV;s process att införa e.ID av Ytterholm&Åhs, Masteruppsats 2003, DSV/SU

[ii] Ackoff, Russell L et al: Designing a National Scientific and Technological Communication System, University of Pennsylvania Press 1976. Ur förordet "Decentralization is the most striking characteristic of the scientific and technical information enterprise in the United States. Numerous overlapping and often competitive services are offered by professional societies and other not-for-profit organizations, profit-seeking firms, and federal agencies….we cannot force needed improvements on users, buyers, and sellers of information services. But we can attempt to formulate and encourage the adoption of an ideal system that combines the best of all possible arrangements for providing access to available information. This offers a way to balance our democratic respect for pluralism with our managerial requirements for efficiency and effectiveness."

[iii] I enlighet med MSB's En bild av myndigheternas infromationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter, Publ.nr: MSB740 – augusti 2014

[iv] OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en

[v] En kort beskrivning av modellen finns i Stuart A Umpleby: The Viable System Model, George Washington University, 2006 skriven för The International Encyclopedia of Organizations Studies. Ett kort citat därifrån:" The Viable System Model identifies five management functions within an adaptive system. System one consists of the units that do the basic work of the organization, for example manufacturing products or delivering services. System two consists of units that handle coordination and scheduling among the system ones. System two activities include allocating space and equipment and enforcing rules and procedures. System three is the middle management function, except that its primary activity is to make a "resource bargain" with the system ones. That is, system three makes resources available in exchange for a commitment by the system ones to meet certain objectives that are agreed upon. System four is responsible for long-range planning and the design of new products and services. Whereas system three is responsible for activities "inside and now," system four is responsible for activities "outside and then." System five manages the interaction between systems three and four and embodies the corporate ethos. Hence, system five decides the identity of the firm and its governing principles and norms. This includes decisions about the kinds of businesses to be developed by system four and to be put into operation by systems three, two and one."