Sveriges cybersäkerhet

Uppgifter, ansvar och struktur

av Patrik Sternudd

Résumé

This article describes the key aspects of cyber security and related areas, including a proposed definition of cyber security suitable for the Swedish context, followed by an overview of some of the more prominent laws and regulations that govern cyber security for agencies and other entities in Sweden. The article then proceeds to describe the current challenges regarding the overall cyber security posture in Sweden, together with a number of suggestions to improve the situation. A central theme is that cyber security must be a continuous concern for all parts of the Swedish society.

I INLEDNINGEN AV artikeln ”Sveriges cyberförsvar tar form” gavs följande konstaterande och utfästelse: Även om flera av de aktörer som har direkta eller stödjande uppgifter i Sveriges cyberförsvar i många fall också har ett omfattande ansvar för Sveriges informations- och cybersäkerhet så är cyberförsvar inte synonymt med cybersäkerhet. Regleringar, mandat och ansvar för Sveriges cybersäkerhet kommer istället att behandlas i en framtida skrift.[1]

Denna artikel innehåller den utlovade redogörelsen och består av:

1. En beskrivning av begreppet cybersäkerhet, dess innebörd och dess relation till relaterade begrepp.
2. En översikt över vilka aktörer som enskilt och tillsammans är nödvändiga för att skapa och upprätthålla en tillräcklig nivå av cybersäkerhet i Sverige.
3. En legal grundplatta formad av en handfull särskilt viktiga författningar och föreskrifter som tillsammans definierar den förväntade grundnivån av cybersäkerhet för olika verksamhetsutövare i Sverige.
4. En redogörelse för några myndigheters särskilda uppgifter för samordning och stöd inom ramen för Sveriges samlade cybersäkerhet.
5. En modell som utgör ett komplement till cyberförsvarspyramiden[2] genom att erbjuda en struktur för att vi ska förstå och vidareutveckla befintlig reglering samt att, oavsett reglering, prioritera de aktiviteter som på kort och lång sikt ger bäst effekt för att förbättra Sveriges förmåga att hantera cybersäkerhetsrelaterade hot.
6. Från oönskat till önskat läge; en analys över vilka cybersäkerhetsutmaningar samhället har idag och fortsatt kommer att ha på kort- och medellång sikt, samt förslag på åtgärder för att de inte ska kvarstå också på lång sikt.
7. Några förslag på författningsförändringar som kan genomföras på kort sikt för att stärka Sveriges cybersäkerhet.
8. Avslutande reflektioner.

Artikeln är skriven med totalförsvarets behov och uppgifter som dimensionerande faktorer i syfte att skapa en modell och

struktur som omhändertar de svåraste påfrestningarna som samhället kan ställas inför. För att uppnå detta måste tillräcklig cybersäkerhet genomsyra samhället även i lägre konfliktnivåer.

Cybersäkerhet och relaterade begrepp

Cybersäkerhet som begrepp, liksom prefixet cyber, har ökat markant i användning de senaste åren. Den ökade användningen till trots saknas en gemensam uppfattning om begreppets innebörd, vilket riskerar att försvåra arbetet att komma överens om lösningar på de strukturella problem som föreligger inom området. I syfte att bidra till ökad förståelse och minskad språkförbistring innehåller det här avsnittet dels en beskrivning av relaterade begrepp, dels ett föreslag på definition av cybersäkerhet med tillhörande fördjupning.

Informationssäkerhet

Ett centralt relaterat begrepp är informationssäkerhet, som omfattar skyddet av all information oavsett hur den förmedlas eller lagras. Det spelar således ingen roll om informationen hanteras via elektronik, papper eller i ett samtal mellan två individer. Vidare ska informationen skyddas mot alla typer av hot, vilket inkluderar antagonistiska aktörer såväl som misstag, olyckor och naturhändelser.

Informationssäkerhet delas av tradition upp i ett antal önskade eller nödvändiga egenskaper, där de tre absolut mest centrala är *riktighet*, *tillgänglighet* och *konfidentialitet*. Inte sällan tillkommer dessutom en eller båda av egenskaperna *oavvislighet* och *autenticitet*. Innebörden av samtliga fem egenskaper återges i tabell 1.

Informationssäkerhet kan ses som både som ett kvalitetsattribut som ska uppnås och den verksamhet som bedrivs för att uppå de ingående egenskaperna. En koncis definition, som enbart omfattar de tre första egenskaperna, återfinns i MSB:s föreskrifter för leverantörer av samhällsviktiga tjänster: ”Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.”[3]

Uttryckt som en verksamhet kan informationssäkerhet sägas utgöra de åtgärder som krävs för att säkerställa att rätt information (ej förvanskad) med klarlagd källa är tillgänglig i rätt tid (när den behövs) för rätt individer (men inga andra) och att dessa i efterhand inte kan förneka tillgång till, eller ändring av informationen.

Ibland används ordet sekretess istället för konfidentialitet. Ordet sekretess har dock i svensk lagstiftning en annan, om än relaterad, innebörd: förbud mot att röja en uppgift.[4]

Egenskap	Innebörd	Engelsk term
Riktighet	Informationen är inte förvanskad eller manipulerad	*Integrity*
Tillgänglighet	Informationen är tillgänglig när den behövs	*Availability*
Konfidentialitet	Informationen är endast tillgänglig för den som är behörig till den	*Confidentiality*
Oavvislighet	Tillgång till, eller förändring av, informationen kan inte förnekas i efterhand	*Non-repudiation*
Autenticitet	Informationen har sitt ursprung hos den källa som den anges komma ifrån	*Authenticity*

Tabell 1 – Informationssäkerhetsegenskaper.

Det kan vara värt att notera att information som uppfyller samtliga fem informationssäkerhetsattribut fortfarande kan vara totalt oanvändbar. Källan, vare sig det är en människa eller ett sensorsystem, kan till exempel vara opålitlig. Att informationen uppfyller riktighetskriteriet är således inte detsamma som att den är korrekt för sitt avsedda användningsområde; detta är istället en fråga för informationshanterings- och datakvalitetsprocesser.

Integritet och dataskydd

Ett närbesläktat begrepp är integritet som ibland felaktigt används när riktighet avses. Förväxlingen är inte förvånande eftersom riktighet på engelska heter integrity, men orden har olika innebörd.

Integritetsbegreppet kan exemplifieras genom de upphävda personuppgiftslagarna och deras ersättare i form av EU:s dataskyddsförordning[5] (GDPR) och dess kompletterande svenska författningar. Både de upphävda och ersättande författningarna reglerar och begränsar i huvudsak under vilka förutsättningar det är tillåtet att samla in, ta del av eller på annat sätt behandla information som påverkar individers personliga integritet.

Inom informationssäkerheten är den svenska betydelsen av integritet således snarare ett specialfall av konfidentialitet eftersom det handlar om att begränsa tillgång till information. Genom införandet av GDPR har även begreppet dataskydd börjat användas som ett samlingsnamn för reglering och åtgärder inom integritetsområdet.

It-säkerhet

En delmängd av informationssäkerheten är hur informationen ska skyddas när den behandlas i olika typer av it-system. Denna delmängd benämns it-säkerhet och definieras i en teknisk rapport från SIS som ”it-relaterade tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet”.[6]

En mer utförlig definition finns i *Försvarsmaktens handbok Nomenklatur Ledning 2016:*

> Ett IT-systems förmåga att förhindra den i det egna systemet lagrade eller behandlade informationen obehörigen röjs, förändras eller förstörs.
>
> I IT-säkerhet inkluderas kommunikationssäkerhet. IT-säkerhet ingår som en del i informationssäkerheten.[7]

Båda definitionerna sorterar it-säkerhet som en del av, eller ett medel för att uppnå, informationssäkerhet. Därmed sätts informationen som systemen hanterar i första rummet, medan skydd av själva systemen mot otillåtna funktionsförändringar blir en implicit förutsättning.

Detta kan i sin tur leda till en medveten eller omedveten avgränsning till kontors- eller andra system avsedda för mänsklig bearbetning av information, medan exempelvis styr- och reglersystem hamnar i skymundan.

Det går naturligtvis att föra ett teoretiskt resonemang, att den maskinkod som finns i systemen och därmed styr dess funktionalitet också utgör information, men definitionerna ger inte ett tydligt stöd för en sådan tolkning utan den är i bästa fall implicit. Vidare är definitionerna begränsade till it-tekniska funktioner, vilket exkluderar administrativa säkerhetsåtgärder.

Inom it-säkerheten tillkommer ytterligare ett antal begrepp. Två exempel är *spårbarhet* och *autentisering*. Spårbarhet är en egenskap som innebär att det i efterhand går att avgöra vad som har hänt i ett system eller med en viss informationsmängd. Autentisering är en aktivitet för att säkerställa identiteten hos en aktör i ett system, exempelvis vid inloggning. Autentisering är i de flesta fall en för-

utsättning för spårbarhet och båda skapar förutsättningar för informationssäkerhetsegenskaperna oavvislighet och autenticitet.

Säkerhetsskydd och begreppsapparater

Som tidigare nämnts omfattar informationssäkerheten alla typer av hot. För att upprätthålla informationssäkerheten krävs därför ett stort antal skyddsåtgärder och verksamheter som ligger utanför omfattningen av denna artikel. Några exempel är brandskydd, inpassering till datahallar och fysiska arkiv samt kontroller av att personal inte missbrukar tilldelade behörigheter för att läsa, ändra, skapa eller sprida information på ett otillbörligt sätt. Informationssäkerhetsområdet är med andra ord mycket omfattande.

På samma gång finns det andra områden som är beroende av eller på annat sätt har relationer till informationssäkerheten, vilket skapar parallella begreppsapparater. Ett exempel är säkerhetsskyddsområdet, som genom säkerhetsskyddslagen (2018:585) delas upp i tre olika säkerhetsskyddsåtgärder: informationssäkerhet, fysisk säkerhet och personalsäkerhet.[8] Därmed blir den fysiska säkerheten inom säkerhetsskyddet sidoordnad istället för underordnad informationssäkerheten.

Att olika delar sorteras på olika sätt i olika verksamheter är naturligt utifrån att både omfattning och övergripande målsättningar varierar. De olika begreppsapparaterna samexisterar således och utgör stöd för respektive verksamhet och reglering.

Defekter och sårbarheter

En defekt är en brist eller felaktighet i en produkt som innebär ett beteende eller utseende som inte är vad tillverkaren avsett. Detta gäller för alla typer av produkter, oavsett om de innehåller mjukvara[9] eller inte. När det gäller mjukvara finns ett annat vanligt förekommande ord, nämligen buggar. Författaren anser dock att ordet *defekt* är mer rättvisande då en bugg inte är något som plötsligt uppstår utan är något som skapats till följd av bristande produktions- och kvalitetsprocesser.

Defekter finns i olika former och med olika grad av allvarlighet för den som drabbas. Det finns exempelvis defekter som har minimal säkerhetspåverkan och som framför allt påverkar en produkts övriga användbarhetsaspekter inklusive dess prestanda.

För att särskilja defekter med säkerhetspåverkan används ofta begreppet sårbarhet, som här avser en defekt i hård- eller mjukvara som kan utnyttjas för otillbörlig åtkomst eller förändring av ett system eller dess information. Som alternativ till ordet sårbarhet används även säkerhetsbrist, eller förenklat, bara brist.

Cybersäkerhet

Sedan en tid tillbaka har begreppet cybersäkerhet börjat användas. Sannolikt är det en följd av att cyber security i stor utsträckning används på engelska, där det under det senaste decenniet trängt ut det äldre begreppet computer security som haft en innebörd liknande svenskans it-säkerhet. Även inom svensk författning har ordet cybersäkerhet börjat sitt intåg, exempelvis i myndighetsinstruktionen för MSB.[10]

Ibland förefaller begreppen användas som synonymer men det finns några skillnader:

1. Cybersäkerhet är funktions- och systemcentriskt, med en tydlig tyngdpunkt mot systemens korrekta funktionalitet och tillgänglighet som möjliggörare för den verksamhet de stödjer. Informationen som hanteras i eller passerar genom systemen skyddas som en effekt av att systemen är tillräckligt säkra.

2. Cybersäkerhet omfattar alla typer av system. Förutom styr- och reglersystem och andra funktioner som är av betydelse för samhället omfattas produkter och tjänster som vid första anblicken inte primärt är it-system men som ändå innehåller eller är beroende av informationsteknik.
3. Cybersäkerhetsbegreppet används ofta, explicit eller underförstått, i en kontext av antagonistiska hot. Att ett system slutar fungera på grund av översvämning i en datahall eller en krets som går sönder av ålder är därmed inte typiskt en cybersäkerhetsfråga även om det naturligtvis påverkar systemets tillgänglighet.

Ovanstående aspekter framgår än mer tydligt när de engelska beskrivningarna av cybersäkerhetsbegreppet studeras. Inom Nato och i USA har man bland annat gjort en förflyttning från att fokusera på Information Assurance till att se cybersäkerhet som ett medel för att uppnå Mission Assurance.

En definition för svenska förhållanden

För att underlätta den fortsatta utvecklingen inom området är det önskvärt att etablera en gemensam förståelse för innebörden av cybersäkerhet. Till stöd för detta har ett förslag på definition med tillhörande fördjupning tagits fram, med ingångsvärden att:

- ligga i linje med cybersäkerhetsbegreppets internationella användning,
- vara kompatibel med informationssäkerhetsbegreppet,
- kunna användas både för att beskriva verksamhet och som ett kvalitetsattribut.

Föreslagen definition för cybersäkerhet: Att över tid förhindra och begränsa antagonistiska cyberaktiviteters skadliga inverkan på ett systems korrekta funktionalitet och tillgänglighet, samt skydd mot otillbörlig påverkan eller åtkomst av den information som lagras i, bearbetas eller förmedlas av systemet.

En viktig princip som genomsyrar definitionen är att det inte nödvändigtvis är systemet självt som ska svara för allt skydd eftersom det i många fall är en förutsättning att det finns människor, organisationer och processer utanför systemet som exempelvis omhändertar säkerhetsövervakning och incidenthantering. Definitionen innehåller därutöver ett antal nyckelord och uttryck som beskrivs i efterföljande stycken.

Det första nyckeluttrycket kommer direkt i definitionens inledning. Över tid innebär det att cybersäkerheten måste upprätthållas så länge systemet är i bruk. Även om ett system mot förmodan inte skulle ha några kända eller okända brister när det börjar användas kommer sårbarheter i komponenter och delsystem att uppdagas över tid. Ytterligare andra komponenter kommer att behöva bytas ut för att skyddet ska hålla jämna steg med utvecklingen av attackverktyg. På samma sätt måste personal som ansvarar för säkerhetsövervakning och incidenthantering hålla sina kunskaper och färdigheter aktuella.

Det andra nyckeluttrycket är förhindra och begränsa, med särskilt fokus på att begränsa. Det är naturligtvis önskvärt att helt kunna förhindra antagonistisk inverkan men önskvärt är inte detsamma som praktiskt möjligt. Planeringsantagandet behöver vara att en antagonist förr eller senare lyckas forcera eller kringgå en eller flera säkerhetsfunktioner. Vidare kommer en tillräckligt välplanerad överbelastningsattack sannolikt att få åtminstone initial negativ inverkan. Omfattningen på skadan, liksom antagonistens möjlighet att skapa fotfäste i systemet, kan däremot begränsas genom en

god säkerhetsarkitektur tillsammans med förmågan att i tid upptäcka och hantera de antagonistiska aktiviteterna.

Det tredje nyckeluttrycket är användningen av ordet system i kombination med antagonistiska cyberaktiviteter. Genom att inte låsa definitionen till en ofullständig uppräkning av olika typer eller kategorier av system blir definitionen giltig för alla typer av system som en antagonist genom olika cyberaktiviteter kan påverka.

Ordet system används således avsiktligt i vid bemärkelse och omfattar såväl tekniska, sociotekniska och konceptuella system och inkluderar bland annat

- styr- och reglersystem, inbyggda system i anläggningar, fordon och farkoster,
- system för elektronisk kommunikation inklusive satellitkommunikation,
- informationssystem som används för beslutsstöd och lägesförståelse,
- enskilda enheter som mobiltelefoner[11] och surfplattor, liksom större ekosystem där dessa ingår tillsammans med appbutiker, telefontillverkare och mobiloperatörer,
- en eller flera programvaror som exekveras av en processorenhet, till exempel en dator med dess operativsystem och övriga applikationer,
- hem- och kontorsnätverk bestående av datorer, skrivare, ljudanläggningar, tv-apparater och annan uppkopplad utrustning,
- system-av-system där flera förekomster av exempelvis något av ovanstående nämnda system kopplas ihop för att uppnå ett specifikt syfte.

Att inte i onödan avgränsa definitionen till specifika system gör det dessutom möjligt att definiera funktioner, organisationer och nationer som system för att på så sätt kunna analysera dess samlade cybersäkerhet.

Cybersäkerhet respektive cyberförsvar

Cyberförsvar avhandlades i ”Sveriges cyberförsvar tar form”[12] varför området här endast beskrivs översiktligt i syfte att illustrera skillnader och likheter med cybersäkerhetsområdet.

Den gemensamma faktorn är att motverka antagonisters möjlighet att påverka genomförandet av verksamhet genom cyberaktiviteter riktade mot system inklusive informationen i dessa som verksamheten är beroende av.

Skillnaden består i att cybersäkerhet är något som angår och kräver delaktighet ifrån i princip samtliga samhällsaktörer, medan cyberförsvar framför allt är relaterat till totalförsvaret och med särskilt bäring på det militära försvaret.

För cyberförsvar, men inte cybersäkerhet, gäller därmed följande:

- De system som ligger inom cyberförsvarets intressesfär är i första hand sådana som är av särskilt vikt för totalförsvaret och ytterst det militära försvarets förmåga att möta ett väpnat angrepp och genomföra mobilisering.
- Den dimensionerande antagonisten är kvalificerade statliga och statsunderstödda aktörer oavsett dess formella association till statens väpnade styrkor.
- Den dimensionerande konfliktnivån är höjd beredskap och väpnat angrepp vilket innebär att totalförsvarsplikten inklusive värnplikten utgör en viktig komponent för att planera för och uppnå uthållighet.
- Cyberdomänen är en del av operationsmiljön,[13] där cyberoperationer kan stödja operationer i andra domäner. Cyberoperationer som militärt maktmedel ställer i sin tur krav på officerare med förståelse för hur krigets krav och

folkrätten relaterar till operationer i cyberdomänen.

Till följd av att Försvarsmaktens huvuduppgift är att kunna möta ett väpnat angrepp kommer dock delar av ovanstående kriterier att vara giltiga även för myndighetens cybersäkerhetsarbete. Därmed kan de delar av cybersäkerhetsarbetet som syftar till att säkerställa Försvarsmaktens operativa förmåga konceptuellt sägas ingå som en del i cyberförsvaret.

CERT och CSIRT

CERT och CSIRT är engelska förkortningar, som över åren kommit att ingå i det svenska fackspråket. Både CERT och CIRT avser verksamheter inom it- eller cybersäkerhetsområdet.

CERT står för *Computer Emergency Response Team* och brukar avse en organisation eller funktion vars uppgifter är att koordinera och stödja vid incidenthantering samt sprida information och rekommendationer om sårbarheter och incidenter. En CERT är ofta ett nav på central nivå, med informationsutbyte och samarbete även utanför den egna organisationen.

CSIRT står för *Computer Security Incident Response Team*. CSIRT finns i ett antal språkliga variationer, däribland CIRT och IRT. En CSIRTS uppgift kan vara att genom effektiv incidenthantering begränsa skadan vid en incident samt återställa påverkade system till ett funktionellt och säkert tillstånd.

Även om namnen är vedertagna saknas samsyn kring den exakta innebörden vilket innebär att olika CERT- och CSIRT-funktioner kan skilja sig avseende uppgifter och verksamhet. Uppgiften att arbeta proaktivt för att förhindra framtida incidenter kan till exempel ingå i både CERT och CSIRT. Båda namnen används dessutom ibland som synonymer.

Sammanfattning av begreppen

Utifrån vad som beskrivits ovan kan de olika begreppen något förenklat sammanfattas enligt följande:

Informationssäkerhet omfattar skyddet av information oavsett i vilken form den är representerad och oavsett vilken typ av hot som avses.

- Informationssäkerhet kan vara ett begrepp och verksamhetsområde i sin egen rätt men också ingå i andra områden som exempelvis säkerhetsskydd. I säkerhetsskyddslagen har delar som annars hanteras som en delmängd inom informationssäkerhetsområdet lyfts ut och sidoordnats.
- It-säkerhet är den del av informationssäkerheten som omfattar it-tekniska åtgärder för att skydda information som hanteras i eller av ett it-system.
- Cybersäkerhet omfattar åtgärder för att förhindra att framför allt antagonistiska cyberaktiviteter påverkar ett system (inklusive styr- och reglersystem m m) och i förlängningen den information som systemet hanterar.
- Cyberförsvar omfattar åtgärder för att förhindra att statliga eller statsunderstödda antagonister genom cyberdomänen kan begränsa eller förhindra förmågan att försvara Sverige och svenska intressen. Krigets krav är dimensionerande.

Utifrån ovanstående är begreppet informations- och cybersäkerhet, som används i propositionen *Totalförsvaret 2021–2025*[14] och *Handlingskraft,*[15] inte en tautologi utan ett bra samlingsbegrepp eftersom det sätter fokus på behovet av ökad cybersäkerhet samtidigt som behovet av informationssäkerhet kvarstår.

Läsaren bör avslutningsvis vara uppmärksam på att it-säkerhet och cybersäkerhet i dagsläget används både som synonymer och med liknande eller andra innebörder än vad som beskrivs i denna artikel. Sannolikt kommer viss harmonisering att ske under de kommande åren, där det till exempel inte är otänkbart att cybersäkerhet på sikt tränger ut eller absorberar it-säkerhetsbegreppet på samma sätt som redan har skett i USA.

Aktörer som tillsammans ansvarar för Sveriges cybersäkerhet

Precis som övriga kvaliteter är cybersäkerhet inte något som uppstår av sig självt eller tillhandahålls kostnadsfritt av någon annan. Detta gäller oavsett om det är specialdesignade system för ett specifikt ändamål eller konsumentprodukter tillverkade i stora serier.

Grundförutsättningen för Sveriges cybersäkerhet är därför att varje verksamhetsutövare, oavsett organisationsform, som använder informationsteknik i sin verksamhet också ansvarar för att de produkter och tjänster denne är beroende av har tillräcklig cybersäkerhet för att verksamheten ska kunna bedrivas. Det är verksamhetsutövaren som bestämmer vilka produkter och tjänster denne använder och cybersäkerhet är i det sammanhanget en av många kvaliteter som behöver säkerställas genom egna resurser alternativt med hjälp av leverantörer.

Utöver ansvaret för den egna verksamheten finns det system, tjänster och information som är av betydelse inte bara för verksamhetsutövaren utan också för samhället i stort och ytterst Sveriges säkerhet. För sådan verksamhet finns särskilda författningar liksom myndigheter som inom deras ansvarsområden utfärdar föreskrifter och utövar tillsyn. Därutöver finns reglering som syftar till att skydda information om fysiska personer samt reglering med krav på korrekt funktionalitet i konsumentprodukter och konsumenttjänster.

Sveriges samlade cybersäkerhet bör därför ses som ett sammanhängande system där flera olika aktörer ansvarar för olika delar.

För Sveriges cybersäkerhet ansvarar därmed bland annat:

- varje myndighet, region, kommun, företag eller annan organisation som använder eller anskaffar system innehållande informationsteknik till stöd för verksamheten,
- alla, oavsett organisationsform, som tillhandahåller it-tjänster för annan aktörs räkning,
- alla som utvecklar produkter eller system som innehåller it-komponenter, oavsett organisationsform och oavsett om det är för egen användning eller på uppdrag av någon annan,
- alla som köper och använder konsumentprodukter med it-komponenter, och särskilt sådana som har möjlighet att oavsett överföringsmedia utbyta information med andra enheter,
- alla lärosäten och andra utbildningsanordnare som tillhandahåller kurser och utbildningar om hur it-komponenter i form av hård- eller mjukvara samt av dessa sammansatta system utvecklas och produceras,
- riksdag och regering som utfärdar lagar och förordningar och genom statsbudgeten tilldelar resurser för den offentliga verksamheten samt förutsättningar för forskning och utveckling,
- regeringen och regeringskansliet som inriktar och samordnar myndigheternas verksamhet genom instruktioner, regleringsbrev och regeringsbeslut,

- de myndigheter som under regeringen och utifrån respektive sakområdesansvar inom den svenska förvaltningsmodellen ansvarar för föreskrifter, tillsyn, rekommendationer och stöd,
- polis- och åklagarmyndigheten samt övriga delar av rättsväsendet, som ansvarar för att utreda och lagföra individer som begår it-relaterade brott,
- skolväsendet, för att tidigt ge befolkningen förståelse för hot och gällande lagstiftning, samt också kunskap för att så långt som möjligt inte drabbas av hoten,
- standardiserings- och certifieringsorgan inom alla produktområden som innehåller någon form av informationsteknologi som kan påverka produktens eller omgivningens säkerhet.

Utöver ovanstående finns försäkringsbolagen, som sannolikt kommer att få en större roll på sikt genom att försäkringspremier och möjlighet till ersättning för cybersäkerhetsrelaterade skador kan komma att spegla försäkringstagarens mognad och åtgärder inom området.

Samtliga områden behövs för ett robust samhälle där cybersäkerheten skapar möjlighet för fortsatt digitalisering. Områdena och dess aktörer verkar i olika tidsperspektiv och skapar också förutsättningar för varandra. Även det omvända gäller; en aktör som inte löser sina egna uppgifter försämrar förutsättningarna för övriga aktörer.

En legal grundplatta för Sveriges cybersäkerhet

I det här avsnittet återges exempel från en handfull författningar och föreskrifter som tillsammans definierar den förväntade grundnivån av cybersäkerhet för olika verksamhetsutövare i Sverige. Syftet är att tillhandahålla en översikt med några förtydligande exempel, de flesta förordningarna och inte minst de föreskrifter som kompletterar dem innehåller ytterligare styrning och vägledning.

Utifrån att avsnittet behandlar den rättsliga grunden med kompletterande föreskrifter exkluderas standarder som för vissa branscher utgör förutsättningar för exempelvis produktgodkännande. Det kan dock konstateras att dessa standarder i vissa fall ställer hårdare krav på utvecklingsmetodik och systemens resulterande korrekta funktionalitet än vad lag, förordning och föreskrifter inom cybersäkerhetsområdet gör.

Krav på statliga myndigheter

Förordningen (2022:524) om statliga myndigheters beredskap ställer krav på samtliga myndigheter under regeringen:

> 13 § Varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Därvid ska behovet av säkra ledningssystem särskilt beaktas.[16]

För 13 § har Myndigheten för samhällsskydd och beredskap (MSB), med undantag för Försvarsmakten och kommittéväsendet, föreskriftsrätt. Sådana föreskrifter har utfärdats avseende informationssäkerhet[17] respektive säkerhetsåtgärder i informationssystem.[18]

Sammantaget innebär föreskrifterna att de myndigheter som omfattas ska bedriva ett strukturerat informations- och cybersäkerhetsarbete med förankring i myndighetensledningen, samt att ett antal tekniska krav på myndigheternas informationssystem ska vara uppfyllda. Ett av många relevanta krav återges nedan:

> 11 § Myndigheten ska säkerställa att säkerhetstester och granskningar möjliggör iden-

tifiering av sårbarheter. Myndigheten ska ha interna regler för hur kontroll görs av att

1. informationssystemen är uppdaterade,
2. valda säkerhetsåtgärder är införda på korrekt sätt, och
3. genomförda säkerhetskonfigurationer är tillräckliga.[19]

Ovanstående paragrafs efterlevnad förutsätter kunskap om vilka it-produkter myndigheten använder och är beroende av. Krav på detta finns i andra kapitlet med grundläggande bestämmelser:

4 § Myndigheten ska upprätthålla uppdaterad dokumentation över

1. hård- och mjukvara som används i varje enskilt informationssystem,
2. beroenden mellan olika interna informationssystem respektive beroenden av informationssystem hos externa aktörer,
3. vilka informationssystem som behandlar information som har behov av utökat skydd, och
4. vilka informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag.[20]

Krav på säkerhetskänslig verksamhet

För verksamheter som bedriver säkerhetskänslig verksamhet gäller säkerhetsskyddsförordningen (2021:955) där tredje kapitlet reglerar informationssäkerhet. Informationssystem regleras i 1-5 §§, där exempelvis 4 § ställer krav på förmåga att både upptäcka och hantera incidenter:

4 § En verksamhetsutövare som ansvarar för ett informationssystem som ska användas i säkerhetskänslig verksamhet ska vidta lämpliga skyddsåtgärder för att kunna upptäcka, försvåra och hantera skadlig inverkan på informationssystemet samt obehörig avlyssning av, åtkomst till och nyttjande av informationssystemet.

Verksamhetsutövaren ska också se till att spårbarhet finns för händelser som är av betydelse för säkerheten i systemet.[21]

Säkerhetsskyddslagstiftningen gäller, med några få undantag, samtliga verksamhetsutövare oavsett organisationsform. Ett mindre antal myndigheter samt regeringskansliet får inom sina respektive tillsynsområden utfärda ytterligare föreskrifter. Bland dessa har Säkerhetspolisen och Försvarsmakten överordnade roller inom sina respektive tillsynsområden. Båda myndigheterna har gett ut kompletterande föreskrifter.

Två exempel ur Säkerhetspolisens föreskrifter återges nedan:

2 § Verksamhetsutövaren ska se till att hårdvara och tredjepartsprogramvara i informationssystem som har betydelse för säkerhetskänslig verksamhet granskas för att upptäcka och åtgärda säkerhetsbrister och sårbarheter, eller att hårdvaran och programvaran på annat sätt bedöms vara tillförlitlig från säkerhetsskyddssynpunkt.

[---]

32 § Verksamhetsutövaren ska för informationssystem som är skyddsvärda utifrån perspektiven riktighet eller tillgänglighet ha de rutiner och funktioner som krävs för att upprätthålla kontinuitet i den säkerhetskänsliga verksamheten. Verksamhetsutövaren ska för sådana informationssystem vidta åtgärder som säkerställer att informationssystemet kan återställas.[22]

Vidare ställer säkerhetsskyddsförordningen krav avseende utbyte och förmedling av säkerhetsskyddsklassificerad information, där uppgifter som ska kommuniceras utanför den egna kontrollen ska skyddas med hjälp av godkända kryptografiska funktioner.[23]

Användande av sådana kryptografiska funktioner faller inom vad som traditionellt

benämns signalskyddstjänst, där Försvarsmakten utöver ansvaret att godkänna de kryptografiska funktionerna också har föreskriftsrätt avseende hur dessa får och ska användas. Föreskrifterna[24] återfinns i Försvarsmaktens författningssamling tillsammans med föreskrifterna för säkerhetsskydd[25] inom Försvarsmaktens tillsynsområde.

Krav på elektroniska kommunikationsnät

Lagen (2022:482) om elektronisk kommunikation ställer krav på leverantörer av elektroniska kommunikationsnät och elektroniska kommunikationstjänster. I första paragrafen om lagens syfte framgår att:

> Vid tillämpningen av lagen ska särskilt Sveriges säkerhet liksom elektroniska kommunikationers betydelse för yttrandefrihet och informationsfrihet beaktas.[26]

Lagens åttonde kapitel behandlar säkerhet, där första paragrafen inleds med:

> 1 § Den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att på ett lämpligt sätt hantera risker som hotar säkerheten i nät och tjänster. [---][27]

Lagen ger även tillsynsmyndigheten ett verktyg i form av oberoende granskning:

> 2 § Om det finns särskilda skäl, får tillsynsmyndigheten ålägga den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst att på egen bekostnad låta ett oberoende kvalificerat organ utföra en säkerhetsgranskning av hela eller delar av verksamheten och att redovisa resultatet av granskningen för myndigheten.[28]

Genom den tillhörande förordningen utses Post- och telestyrelsen (PTS) till föreskrifts- och tillsynsmyndighet.[29] PTS föreskrifter och allmänna råd om säkerhet i nät och tjänster omfattar 13 olika kapitel. Ett exempel ur tolfte kapitlet återges nedan:

> 1 § Tillhandahållaren ska kontinuerligt övervaka kommunikationstjänster och aktiva delar i kommunikationsnät för att kunna förebygga, upptäcka och åtgärda säkerhetsincidenter.
>
> Tillhandahållaren ska ha system som skapar larm vid säkerhetsincidenter som innebär störningar eller avbrott.
>
> Tillhandahållaren ska dygnet runt kunna initiera relevanta åtgärder för att hantera säkerhetsincidenter.[30]

Lagen, förordningen och föreskrifterna omfattar slutligen krav på planering och förberedelser för höjd beredskap, där PTS innan föreskrifter lämnas avseende totalförsvarets behov ska samråda med Försvarsmakten och MSB.

Krav på samhällsviktiga tjänster

För verksamhetsutövare som är etablerade i Sverige och som tillhandahåller samhällsviktiga tjänster gäller, med några undantag, lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster där det bland annat framgår att:

> 13 § Leverantörer av samhällsviktiga tjänster ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken.[31]

Lagen omfattar samhällsviktiga tjänster inom sektorerna

- energi,
- transport,
- bankverksamhet,
- finansmarknadsinfrastruktur,
- hälso- och sjukvård,
- leverans och distribution av dricksvatten,
- digital infrastruktur.

Lagen undantar, något förenklat, leverantörer som faller under annan reglering, exempelvis säkerhetsskyddslagen eller lagen om elektronisk kommunikation.

Genom den tillhörande förordningen ges MSB föreskriftsrätt.[32] De gällande föreskrifterna ställer i likhet med MSB:s föreskrifter för statliga myndigheter krav på ett systematiskt informationssäkerhetsarbete som utgår från ledningen.[33] Föreskrifterna innehåller bland mycket annat krav på incidenthantering:

> 11 § En leverantör ska ha interna regler och arbetssätt för att upptäcka och vidta åtgärder för att minimera konsekvenserna av incidenter och avvikelser avseende informationshanteringen i nätverk och informationssystem som används för att tillhandahålla samhällsviktiga tjänster.
>
> Efter avslutad incidenthantering ska leverantören identifiera grundorsaker till att incidenter och avvikelser inträffat samt vidta åtgärder för att förhindra att liknande incidenter och avvikelser inträffar på nytt.[34]

Föreskrifterna gäller även vid utkontraktering till externa aktörer. Den som ansvarar för tjänsten ska i så fall identifiera och hantera risker samt genom avtal reglerna de säkerhetsåtgärder som den externa aktören ska vidta.

Utöver MSB har även Statens energimyndighet, Transportstyrelsen, Finansinspektionen, Livsmedelsverket och PTS föreskriftsrätt avseende lagens 12-14 §§ inom sina tillsynsområden. Socialstyrelsen får dessutom utfärda föreskrifter för Inspektionen för vård och omsorgs tillsynsområde. PTS har som exempel bland annat föreskrivit följande för sektorn digital infrastruktur:

> 13 § Leverantören ska, i den utsträckning som följer av 6 §, säkerställa att
>
> 1. de som utför arbetsuppgifter för att upprätthålla säkerheten i nätverk och informationssystem har tillräcklig kompetens för att utföra sina arbetsuppgifter,
> 2. tillräckliga personella resurser finns tillgängliga för att upprätthålla säkerheten i nätverk och informationssystem, och
> 3. anställda och uppdragstagare känner till och tillämpar framtagna processer och rutiner för upprätthållande av säkerheten i nätverk och informationssystem.[35]

Krav på digitala tjänster och varor med digitala delar

Leverantörer av digitala tjänster som varken används för säkerhetskänslig verksamhet eller är samhällsviktiga regleras genom 15-16 §§ i lagen om informationssäkerhet för samhällsviktiga och digitala tjänster. För innebörden av digitala tjänster hänvisar förordningen till definitionen i EU-direktivet 2015/1535:

> b) *tjänst*: alla informationssamhällets tjänster, det vill säga tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare.[36]

Definitionen och därmed lagen har med andra ord en mycket bred omfattning gällande typer av tjänster. Däremot undantas företag som sysselsätter mindre än 50 personer och

har mindre årlig omsättning eller balansomslutning än 10 miljoner euro.

I den tillhörande förordningen framgår att

> 6 § Vid bedömningen av om säkerhetsåtgärder enligt 15 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster säkerställer en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till risken, ska följande beaktas:
>
> 1. säkerheten i system och anläggningar,
> 2. incidenthantering,
> 3. hantering av driftskontinuitet,
> 4. övervakning, revision och testning, och
> 5. efterlevnad av internationella standarder.
>
> […][37]

Utöver ovanstående författningar ställer också konsumentköplagen (2022:260) krav på leverantörer av digitala tjänster:

> 4 § För en vara med digitala delar ska näringsidkaren se till att konsumenten informeras om och tillhandahålls säkerhetsuppdateringar och andra nödvändiga uppdateringar.
>
> Vid ett enstaka tillhandahållande av ett digitalt innehåll eller en digital tjänst gäller näringsidkarens skyldighet enligt första stycket under den tid som konsumenten med fog kan förutsätta uppdateringar. Vid kontinuerligt tillhandahållande av ett digitalt innehåll eller en digital tjänst under en period gäller skyldigheten under tre år efter det att varan med digitala delar avlämnades eller den längre tid som avtalet löper.[38]

Således är en vara eller tjänst enligt ovan att anse som felaktig i fall näringsidkaren inte tillhandahåller säkerhetsuppdateringar under en tid av tre år efter köptillfället. I en kontext av varor som exempelvis smarta mobiltelefoner, trådlösa accesspunkter, uppkopplade ljudanläggningar, nätverksskrivare och andra konsumentprodukter är det viktigt att notera att treårsgränsen gäller från varans avlämnande och inte tidpunkten från dess tillverkning.

För att ovanstående ska gälla förutsätts även att slutanvändaren tar sitt ansvar:

> 8 § En vara med digitala delar ska inte anses felaktig om den avviker från vad som anges i 1 eller 2 § enbart till följd av att konsumenten inte inom skälig tid har installerat en uppdatering som har tillhandahållits enligt 4 §.
>
> Detta gäller dock endast om näringsidkaren har informerat konsumenten om att uppdateringen finns tillgänglig och om konsekvenserna av bristande installation, och konsumentens bristande installation inte har berott på anvisningarna för installationen.

Krav på alla som omfattas av GDPR

I det inledande avsnittet om begrepp introducerades EU:s dataskyddsförordning (GDPR) från ett integritetsperspektiv. EU-förordningen gäller med undantag för området försvar och säkerhet samtliga aktörer oavsett organisationsform.[39]

Även om den personliga integriteten är starkt förknippad med att begränsa spridning och otillåten behandling av personuppgifter förutsätter upprätthållande av integriteten också att informationen skyddas mot såväl antagonister som olyckshändelser och misstag. Krav på sådan säkerhet ingår som en av de huvudsakliga principerna för behandling av personuppgifter:

> De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller

organisatoriska åtgärder (integritet[40] och konfidentialitet).[41]

Förtydligande krav till principen finns i fjärde kapitlets andra avsnitt.

Krav på incidentrapportering

En förutsättning för att myndigheter med ansvar inom informations- och cybersäkerhetsområdet ska kunna ha en god lägesuppfattning, vidta lämpliga åtgärder samt ge rekommendationer till regeringen är att den som drabbas av en cybersäkerhetsrelaterad incident skyndsamt rapporterar den. Eftersom olika myndigheter har olika ansvar innebär det att det finns olika mottagare beroende på verksamhet och allvarlighetsgrad. Därutöver är det upp till varje verksamhetsutövare att bedöma huruvida en incident också utgör ett brott och i förekommande fall anmäla detta till Polismyndigheten.

De huvudsakliga flödena för incidentrapportering som regleras genom de föregående presenterade författningarna framgår nedan:

Incidenter inom säkerhetskänslig verksamhet rapporteras alltid till Säkerhetspolisen. För verksamheter inom Försvarsmaktens tillsynsområde sker rapportering även till Försvarsmakten.

- Incidenter inom myndigheter exklusive Regeringskansliet, kommittéväsendet, Säkerhetspolisen, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets forskningsinstitut rapporteras till MSB.
- Incidenter som rör elektroniska kommunikationsnät och elektroniska kommunikationstjänster rapporteras till Post- och telestyrelsen.
- Incidenter som rör samhällsviktiga och digitala tjänster rapporteras till MSB, som också vidarebefordrar dessa till respektive tillsynsmyndighet.
- Incidenter som inte rör samhällsviktiga och digitala tjänster kan frivilligt rapporteras till MSB i enlighet med MSB:s föreskrifter.[42]
- Personuppgiftsincidenter inom ramen för dataskyddsförordningen rapporteras till Integritetsskyddsmyndigheten (IMY) samt till de fysiska personer som drabbats av incidenten.

Ett tillkommande och viktigt flöde till följd av den reviderade beredskapslagstiftningen som gäller från den första oktober 2022 är att Försvarsmakten får föreskriva vilken rapportering beredskapsmyndigheterna och de civilområdesansvariga länsstyrelserna ska lämna till Försvarsmakten.

De olika rapporteringsvägarna medger dels separation av skyddsvärden, dels att rapporteringen direkt når den sakområdesansvariga myndighet som har behov av informationen för att lösa sina uppgifter. Dessa myndigheter kan i sin tur ha ansvar för att vidareförmedla informationen till andra, med eller utan bearbetning.

Viten, sanktionsavgifter och skadestånd

Inom områdena elektroniska kommunikationsnät, samhällsviktiga och digitala tjänster, säkerhetskänslig verksamhet samt GDPR har tillsynsmyndigheterna befogenheter att utfärda sanktionsavgifter, viten eller både och. För digitala tjänster och varor med digitala delar inom konsumentköplagens område gäller istället rätt till skadestånd som bland annat omfattar ”annan förlust på grund av dröjsmålet eller felet”[43] vilket torde kunna bli särskilt intressant kopplat till de konsekvenser bristande cybersäkerhet kan resultera i.

Det enda område där underlåtenhet att följa krav på informations- och cybersäkerhet inte kan få några ekonomiska konsekvenser

är således de statliga myndigheternas beredskap. Det ska här dock konsteratas att de krav som ställs på statliga myndigheter över huvud taget inte gäller för kommuner och regioner.

Sammanfattning av grundplattan

Sammanfattningsvis kan det konstateras att följande verksamheter och områden har författningsmässiga regleringar med explicita krav på informations- och cybersäkerhet:

- samtliga myndigheter under regeringen inklusive länsstyrelserna,
- säkerhetskänslig verksamhet, oavsett organisationsform,
- leverantörer som tillhandahåller allmänna eller elektroniska kommunikationsnät,
- leverantörer av samhällsviktiga tjänster,
- leverantörer av digitala tjänster och varor med digitala delar,
- samtliga aktörer vars personuppgiftshantering omfattas av GDPR.

Inom samtliga områden finns reglering avseende incidentrapportering inklusive till vilken myndighet incidenterna ska rapporteras. Eftersom konsumentköplagen inte omfattar incidenter på samma sätt som övriga lagar sker i det fallet ingen rapportering till någon myndighet. Däremot gäller att leverantören ska informera konsumenten om att det finns tillgängliga säkerhetsuppdateringar i produkten eller tjänsten.

Myndigheter med samordnande eller stödjande uppgifter

I det här avsnittet redovisas ett antal myndigheter med särskilda uppdrag från statsmakten att samordna eller stödja i cybersäkerhetsrelaterade frågor. De stödjande uppgifterna är just stödjande och innebär inte att övriga myndigheters, företags och privatpersoners eget ansvar att upprätthålla en adekvat nivå av cybersäkerhet försvinner.

Kriteriet avseende uppdrag från statsmakten innebär att exempelvis nedanstående aktörer exkluderas:

- Företag som erbjuder konsult- eller andra cybersäkerhetstjänster.
- Aktörer som utan uppdrag från svenska staten kostnadsfritt tillhandahåller aktuell information om sårbarheter och andra cybersäkerhetsrelaterade hot.
- Lärosäten och företag inom och utanför Sverige som tillhandahåller utbildning inom cybersäkerhetsområdet.

Även om dessa exkluderas i det här sammanhanget fyller de viktiga funktioner i ekosystemet. Till exempel kan en verksamhetsutövare välja att använda externa tjänster för säkerhetsövervakning istället för att upprätthålla egen kompetens.

Myndigheterna kan delas i två kategorier: de som är samordnande och stödjande samt de som enbart är stödjande. Bland de samordnande myndigheterna återfinns Försvarsmakten, MSB, Myndigheten för digital förvaltning och Säkerhetspolisen.

I sammanhanget kan det vara lämpligt att nämna Nationellt cybersäkerhetscentrum (NCSC), vilket inte är en myndighet utan ett samverkansorgan för myndigheter med specifika uppgifter inom Sveriges cybersäkerhet. En av styrkorna är att genom samlokalisering enklare kunna dela information mellan centrets aktörer. Möjligheterna att använda NCSC som en plattform för att hantera hybridhot beskrivs vidare i avsnittet ”Att möta och hantera hybridaktiviteter med cyberkomponenter” i artikeln om Sveriges cyberförsvar.[44]

Slutligen har samtliga tillsynsmyndigheter inom säkerhetsskyddsförordningen enligt förordningens 8 kap 12 § i uppgift att inom respektive tillsynsområde ge vägledning om säkerhetsskydd vilket inkluderar de delar av informations- och cybersäkerheten som omfattas av lagen. Dessa myndigheter och affärsverk är:

- Försvarsmakten och Säkerhetspolisen (beskrivs fördjupat i eget avsnitt).
- Affärsverket svenska kraftnät.
- Transportstyrelsen.
- Post- och telestyrelsen.
- Försvarets materielverk.
- Finansinspektionen.
- Statens energimyndighet.
- Strålsäkerhetsmyndigheten.
- Länsstyrelserna i Stockholms län, Skåne län, Västra Götalands län samt Norrbottens län.

De myndigheter som därutöver presenteras särskilt återges nedan i kategori- och bokstavsordning.

Försvarsmakten

Försvarsmaktens ansvar utgår från dels huvuduppgiften att kunna möta ett väpnat angrepp, dels dess uppgifter inom säkerhetsskyddslagstiftningen. Eftersom Försvarsmakten och det militära försvaret är beroende av system och tjänster utanför Försvarsmaktens rådighet, blir delar av totalförsvarets cybersäkerhet en angelägenhet för den försvarsplanering som leds och samordnas av Försvarsmakten. I myndighetsinstruktionen ingår uppgifter och ansvar relaterat till försvarsplanering och totalförsvar, inte minst i 3 §:

> [---] Försvarsmakten ska ha en aktuell försvarsplanering. Planeringen ska omfatta alla resurser som är nödvändiga för att genomföra Försvarsmaktens verksamhet. Försvarsmakten ska fortlöpande lämna upplysningar till berörda myndigheter om förhållanden i försvarsplaneringen som har betydelse för deras verksamhet.[45]

I ”Sveriges cyberförsvar tar form” beskrivs Försvarsmaktens möjligheter att lämna stöd till civila aktörer, exempelvis genom stödförordningen. Det framgår av samma avsnitt även att Försvarsmakten fått i uppgift att i fred och krig kunna förstärka skyddet av kritiska samhällsfunktioner.[46]

Indirekt lämnar Försvarsmakten stöd genom att dels involvera totalförsvaret i övningar som SAFE Cyber och Locked Shields, dels genom att tillhandahålla anslutningar till särskilda system samt elektroniska kommunikationsnät som FTN och SGSI. Som kontakt- och samverkansyta mot civila CERT- och CSIRT-enheter samt militära motsvarande inom andra länder och mellanstatliga organisationer upprätthåller Försvarsmakten den militära CERT-funktionen FM CERT.

Försvarsmaktens ansvar som tillsynsmyndighet inom säkerhetsskyddet beskrivs separat i kommande avsnitt. Inom säkerhetsskyddslagstiftningen ansvarar Försvarsmakten dessutom för granskning och godkännande av sådana signalskyddsprodukter och system som i lagstiftningen benämns säkra kryptografiska funktioner. Försvarsmakten försörjer även samhället med de kryptonycklar som regelbundet måste bytas för att upprätthålla säkerheten i de kryptografiska funktionerna.

Myndigheten för digital förvaltning

Myndigheten för digital förvaltning (DIGG) har en central roll för den offentliga sektorns digitalisering. DIGG ska enligt sin myndighetsinstruktion ”[…] samordna och stödja den förvaltningsgemensamma

digitaliseringen i syfte att göra den offentliga förvaltningen mer effektiv och ändamålsenlig".[47]

Uppgiften omfattar informationssäkerhet och personlig integritet:

> 8 § Myndigheten ska bedriva arbetet med digitalisering av den offentliga förvaltningen på ett sätt som säkerställer skyddet av säkerhetskänslig verksamhet och informationssäkerhet i övrigt samt skyddet av den personliga integriteten.[48]

Vidare har DIGG ansvar för vissa tjänster med bäring på informations- och cybersäkerhetsområdet:

> 3 § Myndigheten ska
>
> 1. ansvara för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift,
> 2. främja användningen av elektronisk identifiering och underskrift,
>
> [---]
>
> 4 § Myndigheten ska vidare
>
> 1. främja användningen av den myndighetsgemensamma infrastrukturen för säkra elektroniska försändelser, [---][49]

Avseende den fjärde paragrafen har DIGG genom förordningen om myndighetsgemensam infrastruktur för säkra elektroniska försändelser också uppgiften att tillhandahålla infrastrukturen i fråga.[50]

Det handlar således inte om digitalisering eller säkerhet: Uppgifterna i instruktionen innebär att DIGG ska samordna och stödja *säker digitalisering i hela den offentliga sektorn* med undantag för vissa myndigheter inom exempelvis försvar och säkerhet som exkluderats från uppdraget.

Myndigheten för samhällsskydd och beredskap

MSB har genom dess myndighetsinstruktion en stödjande och samordnande roll för samhällets informationssäkerhet:

> 11 a § Myndigheten ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och regioner samt företag och organisationer.
>
> Myndigheten ska årligen lämna en rapport till regeringen med en sammanställning av de incidenter som rapporterats in till myndigheten enligt 14 § förordningen (2022:524) om statliga myndigheters beredskap.
>
> Inför arbetet med att sammanställa rapporten ska myndigheten inhämta upplysningar från Säkerhetspolisen och Försvarsmakten om de incidenter som rapporterats in till de myndigheterna enligt 2 kap. 4 § första stycket 2 säkerhetsskyddsförordningen (2021:955).
>
> Myndigheten ska även rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder på olika nivåer och områden i samhället.[51]

För incidenter som inte faller inom försvar och säkerhet regleras genom förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster att incidentrapportering ska göras till en utsedd *CSIRT-enhet*, samt att MSB är denna enhet.[52] I förordningen framgår att:

> […] CSIRT-enheten ska
>
> 1. ta emot incidentrapporter som lämnas enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster eller enligt föreskrifter

som har meddelats i anslutning till den lagen,

2. utan dröjsmål tillgängliggöra informationen i incidentrapporter för tillsynsmyndigheterna och Socialstyrelsen, och
3. skyndsamt uppmana leverantörer att till Polismyndigheten anmäla incidenter som kan antas ha sin grund i en brottslig gärning. [---][53]

MSB benämner sedan lång tid tillbaka sin CSIRT-funktion CERT-SE. Som komplement till ovanstående förordning ska MSB utöver att ta emot rapporter också kunna stödja i hanteringen av incidenterna:

11 b § Myndigheten ska ansvara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter. Myndigheten ska

1. agera skyndsamt vid it-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i det arbete som krävs för att avhjälpa eller lindra effekter av det inträffade,
2. återrapportera till berörda aktörer i samband med att en it-incident har rapporterats,
3. samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, och
4. vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa.[54]

MSB ansvarar också för att besluta om vilka myndigheter som utöver de som anges explicit i förordningen om totalförsvar och höjd beredskap ska ha säkra kryptografiska funktioner.[55] Detsamma gäller, efter överenskommelse, för företag.

Säkerhetspolisen och Försvarsmakten

Säkerhetspolisen och Försvarsmakten har ett samordnande och stödjande ansvar avseende sådan cybersäkerhet som faller inom säkerhetsskyddslagstiftningen. I förordningens åttonde kapitel, ”Tillsyn, föreskrifter och stöd”, framgår att:

2 § Säkerhetspolisen och Försvarsmakten ska vara samordningsmyndigheter.

Myndigheterna ska

1. i samverkan följa upp, utvärdera och utveckla arbetet med tillsyn och samråd,
2. i samråd ta fram och tillhandahålla metodstöd för tillsyn och samråd,
3. förmedla relevant hotinformation till tillsynsmyndigheterna, och
4. leda ett samarbetsforum där tillsynsmyndigheterna ingår, i syfte att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.[56]

Vidare, enligt 11 § i samma kapitel ska myndigheterna också på begäran lämna råd till regeringskansliet, riksdagen och dess myndigheter samt till justitiekanslern.

Säkerhetspolisen ger även sig själv en stödjande uppgift genom sina egna föreskrifter:

7 § Säkerhetspolisen tillhandahåller, om Säkerhetspolisen inte bedömer att det i ett enskilt fall är olämpligt, beskrivningar av dimensionerande antagonistiska förmågor till verksamhetsutövare.[---][57]

Försvarets materielverk

Försvarets materielverk driver, i enlighet med sin myndighetsinstruktion ett nationellt certifieringsorgan (CSEC) för it-säkerhet i produkter och system:

> 5 § Vid Försvarets materielverk finns ett nationellt certifieringsorgan för it-säkerhet i produkter och system. Materielverket, certifieringsorganet, ska i sin verksamhet beakta nationella säkerhetsintressen, verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat [---][58]

Av paragrafens fortsättning framgår att certifieringsorganet även ansvarar för certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för kvalificerade elektroniska stämplar.

Förvarets materielverk får också, inom sitt verksamhetsområde, tillhandahålla tjänster till andra än Försvarsmakten, vilket ger möjlighet för andra aktörer att exempelvis lägga uppdrag på robusta ledningsstödssystem och andra produkter som är anpassade för högre konfliktnivåer.[59]

Försvarets radioanstalt

Försvarets radioanstalt (FRA) är en försvarsunderrättelsemyndighet med särskilda uppgifter avseende signalspaning, där lagen (2008:217) om signalspaning i försvarsunderrättelseverksamhet anger att regeringen, regeringskansliet, Försvarsmakten, Säkerhetspolisen och NOA inom Polismyndigheten får inrikta signalspaningen. I FRA:s myndighetsinstruktion regleras vilka verksamheter myndigheten ska stödja, vilket utöver signalspaningsområdet inkluderar stöd till Försvarsmakten avseende utveckling och vidmakthållande av Försvarsmaktens cyberförsvar och cyberförsvarsförmåga.[60]

Enligt instruktionens 4 § ska FRA även ha hög teknisk kompetens inom informationssäkerhetsområdet. Paragrafen reglerar att myndigheten, efter begäran från statliga myndigheter och enskilda verksamhetsutövare, får stödja dessa under förutsättning att de hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende.

Inom ramen för sina uppgifter upprätthåller FRA intrångsdetekteringssystemet TDV, vilket bidrar till kartläggning av antagonistiska aktiviteter som riktas mot särskilt skyddsvärda verksamheter.

Totalförsvarets forskningsinstitut

Totalförsvarets forskningsinstitut (FOI) har till uppgift att ”[…] bedriva forskning, metod- och teknikutveckling samt utredningsarbete för totalförsvaret […]”.[61] Utifrån uppgiften samt uppdrag från Försvarsmakten och MSB utvecklar och tillhandahåller FOI den civila cyberträningsanläggningen Crate där aktörer från totalförsvaret kan öva sin personal på att hantera cyberattacker mot kritisk infrastruktur.

En modell för Sveriges cybersäkerhet

Som framgår i avsnittet om den legala grundplattan finns det ett antal lagar, förordningar och föreskrifter med bäring på cybersäkerhetsområdet. Regleringarna finns både nationellt och inom EU. Därtill kommer ett antal europeiska och internationella standarder som i vissa fall utgör praxis alternativt hänvisas till från myndighetsföreskrifter. Framöver kommer Försvarsmakten och i förlängningen andra myndigheter såväl som försvarsindustrin också att behöva förhålla sig till styrande Natopublikationer.

För att underlätta både förståelse för och fortsatt utveckling av befintlig reglering, samt som stöd för att prioritera de aktiviteter som på kort och lång sikt ger bäst effekt för att förbättra Sveriges samlade motståndskraft inom cybersäkerhetsområdet presenteras nedanstående modell. Modellen har, precis som den föreslagna definitionen

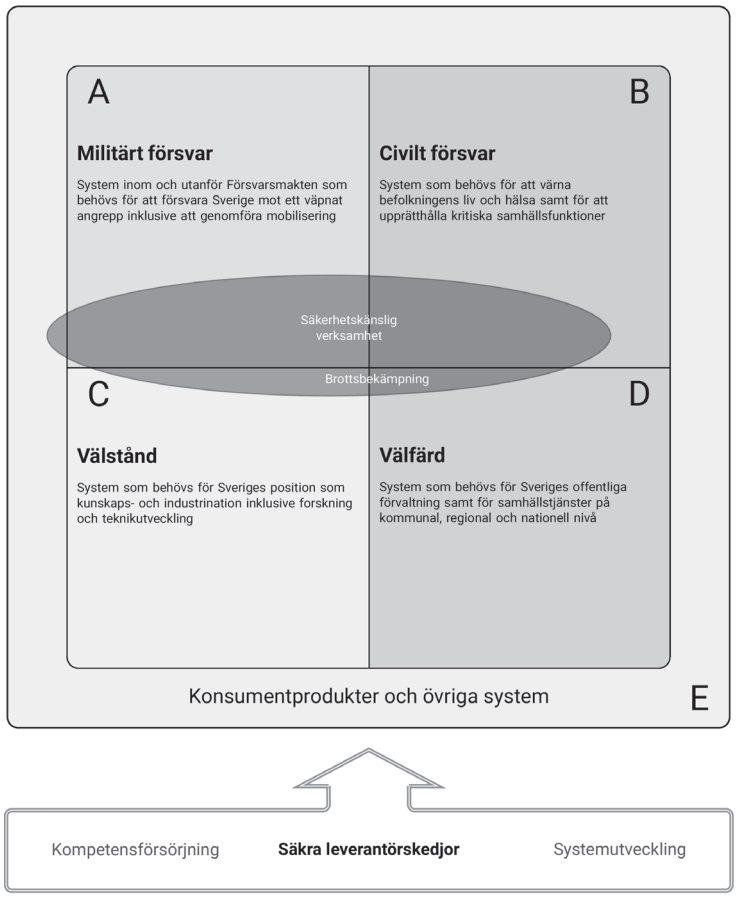
av cybersäkerhet med tillhörande förklaring ett funktions- och systemcentriskt perspektiv. I modellen grupperas olika typer av system samt dess regleringsområde och aktörer i kategorier utifrån dess betydelse för samhället.

Nedanstående förtydliganden bör beaktas vid användning av modellen:

- För att hålla texten kort används ordet system i den vida bemärkelse som beskrivs i det inledande begreppsavsnittet. Ett system kan därmed bestå av flera sammansatta delsystem som tillsammans skapar en specifik funktion eller tjänst hos en verksamhetsutövare.
- Ett specifikt system eller en enskild produkt kan användas av verksamheter inom flera kategorier och därmed omfattas av regleringar och tillsyn från flera områden.
- Kategoriernas storlek i figuren har ingen koppling till antalet system i kategorierna.

Kategori A – Militärt försvar

Kategorin omfattar de system som behövs för att det militära försvaret ska kunna försvara Sverige mot ett väpnat angrepp. Detta inkluderar system som krävs för att upprätthålla ledningsförmågan inklusive ÖB:s kommunikation med statsledningen samt



Figur 1. Modell för Sveriges cybersäkerhet. Illustration: Patrik Sternudd.

system som krävs för att genomföra mobilisering. Många av systemen finns inom Försvarsmakten men det finns också system hos andra myndigheter och privata aktörer. Kategorin och verksamheten för att skydda och försvara systemen har nära kopplingar till Försvarsmaktens cyberförvar.

För Försvarsmaktens egna system och elektroniska kommunikationsnät har Försvarsmakten direkt rådighet och ansvarar därmed för skydd och försvar i egen regi. För system utanför Försvarsmaktens rådighet har Försvarsmakten med stöd av övriga totalförsvarsaktörer ett ansvar att inom totalförsvarsplaneringen identifiera vilka system som är väsentliga för det militära försvaret samt vidta lämpliga förberedelser för skydd och försvar av dessa. Försvarsmakten behöver även säkerställa rapporteringsvägar för att informationsförsörja den militära cyberlägesbilden såväl som regeringen.

Sektorsansvariga myndigheter, beredskapsmyndigheter och civilområdesansvariga länsstyrelser har en indirekt stödjande uppgift att upprätthålla tillräcklig cybersäkerhet inom egen verksamhet såväl som för de områden och sektorer de ansvarar för.

Kategorin regleras framför allt av Försvarsmaktens myndighetsinstruktion och andra författningar som direkt reglerar Försvarsmaktens verksamhet samt de lagar och förordningar som rör Sveriges krigsförberedelser, exempelvis beredskaps- och fullmaktslagar.

Kategori B – Civilt försvar

Kategorin omfattar de system som behövs för att i högre konfliktnivåer värna befolkningens liv och hälsa samt att upprätthålla kritiska samhällsfunktioner. Kategorin har tydliga kopplingar och överlappningar avseende system inom välfärden men är avgränsad till totalförsvarets civila delar inklusive dess stöd till det militära försvaret.

MSB har en samordnande och stödjande roll avseende totalförsvarsplaneringen inom kategorin. Sektorsansvariga myndigheter, beredskapsmyndigheter och civilområdesansvariga länsstyrelser har ett direkt ansvar för att upprätthålla tillräcklig cybersäkerhet inom egen verksamhet såväl som att stödja och samordna inom de områden och sektorer de ansvarar för. Dessa aktörer behöver även säkerställa rapporteringsvägar för att informationsförsörja civila cyberlägesbilder inom de nivåer och områden de ansvariga myndigheterna finner nödvändiga för att lösa sina uppgifter.

Kategorin regleras framför allt av de lagar och förordningar som rör Sveriges krigsförberedelser samt i förekommande fall fullmaktslagstiftningen.

Kategori C – Välstånd

Kategorin omfattar de system som behövs för Sveriges position som kunskaps- och industrination samt för forskning och teknikutveckling. I kategorin har företag och andra aktörer ett behov av att skydda exempelvis forskning och forskningsdata från manipulation eller stöld. Resultatet av forskning och teknikutveckling ligger sedan till grund för system och tjänster inom de övriga kategorierna. Ur ett samhällsperspektiv såväl som för respektive företag är det även angeläget att cybersäkerheten i exempelvis processindustrier och andra anläggningar är tillräcklig för att en antagonist inte ska kunna stoppa eller hota att stoppa verksamheten.

Kategorin regleras bland annat av dataskyddsförordningen (GDPR), lagen (2018:558) om skydd av företagshemligheter, lag och förordning om samhällsviktiga och digitala tjänster samt bransch- och verksamhetsspecifika regleringar och standarder.

Kategori D – Välfärd

Kategorin omfattar de system som behövs för Sveriges offentliga förvaltning samt för samhällstjänster och medborgarservice på kommunal, regional och nationell nivå.

Kategorin omfattar hälso- och sjukvård vilket gör att regioner och kommuner har ett särskilt ansvar för att inom egen verksamhet upprätthålla den nivå av cybersäkerhet som krävs för att exempelvis operationer eller annan vård och omsorg inte ska påverkas negativt. Motsvarande ansvar gäller för övriga verksamhetsområden inom regioner och kommuner.

Kategori E – Konsumentprodukter och övriga system

Kategorin regleras bland annat av dataskyddsförordningen (GDPR), lag och förordning om samhällsviktiga och digitala tjänster, de delar ur beredskapslagstiftningen som rör fredstida kriser samt områdesspecifika regleringar och standarder. Bland de områdesspecifika regleringarna finns exempelvis patientdatalagen (2008:355) och lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation, där Socialstyrelsen och Integritetsskyddsmyndigheten genom patientdataförordningen (2008:360) utses till föreskriftsmyndigheter.

Kategorin *konsumentprodukter och övriga system* omfattar konsumentprodukter samt de system som inte uppenbart tillhör någon av de övriga kategorierna. I kategorin ingår system där säkerhetsbrister kan ge allvarliga konsekvenser för liv, hälsa, egendom och miljö utan att systemen för den sakens skull är samhällskritiska. Som exempel kan nämnas inbyggda system som styr fordon och farkoster.

Kategorin regleras bland annat av dataskyddsförordningen (GDPR), de delar ur lag och förordning om samhällsviktiga och digitala tjänster som inte rör de samhällsviktiga tjänsterna, konsumentskyddslagstiftningen samt branschspecifika regleringar och standarder.

Säkerhetskänslig verksamhet

Den säkerhetskänsliga verksamheten och de system som används för att bedriva denna finns inom alla kategorier. Det är upp till varje verksamhetsutövare oavsett organisationsform att identifiera vilka system som omfattas av lagen och utifrån genomförd analys vidta nödvändiga åtgärder för att upprätthålla informationssäkerheten.

Försvarsmakten[62] utfärdar föreskrifter och genomför tillsyn av säkerhetsskyddet inom myndigheter under Försvarsdepartementet, samt Fortifikationsverket och Försvarshögskolan. Försvarsmakten har också en särställning avseende signalskyddet där bland annat föreskriftsrätten omfattar alla verksamhetsutövare som använder signalskydd.

Säkerhetspolisen utfärdar föreskrifter och genomför tillsyn av säkerhetsskyddet av säkerhetskänslig verksamhet för alla organisationer som inte står under Försvarsmaktens eller riksdagens tillsyn.

Regeringen har vidare utsett ett antal myndigheter som under Försvarsmaktens och Säkerhetspolisens samordning utövar tillsyn samt vid behov utger kompletterande föreskrifter.

Kategorin regleras av säkerhetsskyddslagen med tillhörande förordning, där relevanta paragrafer rörande informations- och cybersäkerhet beskrivits i föregående avsnitt.

Brottskämpning och rättsvård

Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten och Sveriges Domstolar ansvarar för att ta emot anmälan om, utreda samt lagföra it-relaterad brottslighet som

inte faller under Säkerhetspolisens mandat. Säkerhetspolisen ansvarar bland annat för utredning av olovlig underrättelseverksamhet, spionerі samt brott som hotar Sveriges inre säkerhet.

Polismyndigheten och Säkerhetspolisen har inom sina mandat rätt att använda tvångsmedel för att upprätthålla lag och ordning. Utöver Försvarsmaktens och övriga försvarsunderrättelsemyndigheters verksamhet för att kartlägga yttre hot bedriver Säkerhetspolisen underrättelsearbete inom sitt ansvarsområde. Polismyndigheten bedriver underrättelseverksamhet relaterat till övrig it-brottslighet.

Den verksamhet de brottsbekämpande och rättsvårdande myndigheterna bedriver omfattar system i samtliga kategorier, samtidigt som myndigheterna själva ansvarar för de system och produkter som krävs för att lösa sina respektive uppgifter.

Kategorin regleras framför allt av brottsbalken (SFS 1962:700), säkerhetsskyddslagstiftningen, myndighetsinstruktioner samt områdesspecifik lagstiftning.

Säkra leverantörskedjor

För att ett system ska ha tillräcklig cybersäkerhet under hela dess livscykel är det en förutsättning att all mjuk- och hårdvara som ingår i systemet kommer från betrodda leverantörer med förmåga att producera säkra system. Detta gäller vid första leverans såväl som för samtliga därefter följande uppdateringar.

Säkerheten måste upprätthållas under utveckling, överföring och installation så att en antagonist inte kan byta ut hård- eller mjukvara mot en alternativ version med exempelvis bakdörrar eller andra överraskningar som kan aktiveras när antagonisten bestämmer. Detta förutsätter bland annat att autenticitet upprätthålls för all mjukvara och konfiguration samt att processer finns för att löpande följa upp säkerheten i samtliga inkluderade tredjepartsbibliotek.

Även om alla aktörer i kedjan måste göra sitt ligger det slutliga ansvaret alltid på beställarsidan, som utöver att ställa nödvändiga krav också över tid måste följa upp att de efterlevs samt säkerställa att varje leverans är korrekt och tillförlitlig.

Säkra leverantörskedjor inklusive systemutveckling förutsätter slutligen tillgång till välutbildad personal inom ett antal olika deldiscipliner. Att åstadkomma detta är en samhällsangeläget som förutsätter åtgärder på alla nivåer från grundskola till departement och regering tillsammans med engagemang från näringslivet.

Det egna ansvaret

Ett för artikeln genomgående tema, som också gäller i samtliga kategorier, är varje verksamhetsutövares ansvar för de system denne nyttjar, oavsett om dessa är egenutvecklade eller utgörs av externa tjänster. Det egna ansvaret omfattar bland annat att:

- känna till och efterleva de lagar, förordningar och föreskrifter som reglerar informations- och cybersäkerhet för den egna verksamheten,
- skyndsamt åtgärda kända sårbarheter som tillkännages genom säkerhetsuppdateringar och rekommendationer från mjukvaru- och systemleverantörer samt genom publikt tillgängliga sårbarhetsdatabaser,
- ta del av och agera på hotinformation och rekommendationer som publiceras av MSB inklusive dess CSIRT-funktion CERT-SE,
- rapportera incidenter till berörda myndigheter samt polisanmäla misstänkt eller bekräftad brottslig verksamhet,

- avdela tillräckliga ekonomiska och personella resurser för att upprätthålla den nivå av cybersäkerhet som krävs för verksamheten. Dessa behov kan i vissa fall vara större än den författningsreglerade lägsta nivån.

Oavsett reglering kan varje organisation uppnå en god grundnivå genom att följa MSB:s föreskrifter och allmänna råd för statliga myndigheters informationssäkerhet alternativt föreskrifterna för samhällsviktiga tjänster. För mindre företag finns även Stöldskyddsföreningens (SSF) norm *Basnivå – grundläggande it-säkerhet* att tillgå. Normen har tagits fram i ett samarbete mellan SSF, MSB, Polisen och aktörer i näringslivet.[63]

Ovanstående avser framför allt verksamhetsutövare i form av organisationer. Även den enskilda medborgaren har ett ansvar för att hålla sina egna produkter och system uppdaterade med tillgängliga säkerhetsuppdateringar, byta ut produkter som inte längre uppdateras och som har gränsytor mot internet eller andra uppkopplade system, samt där så är möjligt ersätta lösenord med tvåfaktorsautentisering.

Det egna ansvaret, för organisationer såväl som för privatpersoner, inkluderar att inte utsätta andra för fara genom oaktsamhet. Även om den egna verksamheten kan förefalla mindre viktig ur ett samhällsperspektiv kan en angripare utnyttja det som en språngbräda för att komma åt andra, mer kritiska, system.

Från oönskat till önskat läge

De senaste årens cybersäkerhetsdebatt har till stor del handlat om konsekvenserna av de incidenter som inträffat inklusive behovet av att förstärka förmågan att hantera dessa. Den ökade probleminsikten är positiv och en förutsättning för förändring. Samtidigt har diskussionen i stor utsträckning handlat om symptomen medan rotorsakerna inte fått lika stor uppmärksamhet. Även om förmågan till incidenthantering och kontinuitetsplanering är en angelägenhet för alla verksamhetsutövare är det ännu bättre om incidenterna aldrig inträffar; när antagonistiska aktiviteter väl upptäcks kan den värsta skadan redan ha skett eller inte längre gå att förhindra.

Utgångspunkten för den fortsatta diskussionen är ett oönskat nuläge som kan sammanfattas i tre punkter:

1. Alltför många produkter och system levereras från början med mer eller mindre allvarliga sårbarheter.
2. Produkter med kända sårbarheter fortsätter att användas både när säkerhetsuppdateringar saknas och när tillverkaren tillhandahållit sådana. Detta resulterar i ett smörgåsbord av attackvektorer för en antagonist att välja mellan.
3. Lagar, förordningar, föreskrifter, standarder och rekommendationer avseende informations- och cybersäkerhet efterlevs inte. Detsamma gäller sådana rekommendationer som på engelska kallas *best current practice* och som sedan åtminstone början av 2000-talet tillhandahållits gratis av både företag och ideella organisationer.

Inget av ovanstående är nytt. Bristande kvalitet i mjukvara är ett globalt problem med en probleminsikt som går tillbaka till åtminstone 1968, då en Natokonferens arrangerades för att diskutera problem och lösningar kring vad som benämndes vara en uppseglande mjukvarukris.[64] Konferensen resulterade i förlängningen att programvaruteknik[65] etablerades som en egen vetenskaplig disciplin, inklusive akademiska utbildningar i ämnet.

Tjugo år senare, 1988, inträffade det första stora utbrottet av en internetmask som utnyttjade sårbarheter i kända pro-

gram i kombination med dåligt valda användarlösenord för att sprida sig mellan system.[66] Den centrala frågan, drygt 50 år efter Natokonferensen och drygt 30 år efter internetmasken, är varför situationen kvarstår och inte minst vad som kan göras för att ta Sverige ur den. Författarens analys är att det nuvarande tillståndet till stor del beror på fem sammanhängande och ömsesidigt förstärkande faktorer, vilka återges nedan.

För det första: Cybersäkerhet ses som någon annans ansvar snarare än den egna verksamhetsledningens. Det finns även en tradition av att hantera cybersäkerhet som enbart en teknisk fråga som kan omhändertas separat från övrig verksamhet och ännu hellre av en utomstående myndighet eller annan extern aktör.

För det andra: Kostnaderna och konsekvenserna för bristande cybersäkerhet belastar sällan den som skapat produkten eller tjänsten vars sårbarheter orsakat skadorna. Det är inte heller alltid den verksamhetsutövare som beställt produkten eller tjänsten som drabbas hårdast; istället kan det vara enskilda individer, andra organisationer och ytterst nationer som över kortare eller längre tid får försöka hantera konsekvenserna.

För det tredje: Arbetsinsatsen och kompetenskraven för att skapa och distribuera produkter med bristande cybersäkerhet är en bråkdel jämfört med motsatsen. Det finns gott om verktyg som stödjer produktion och tillgängliggörande av osäker programvara. Dessa verktyg går ofta utmärkt att använda utan teoretisk förståelse för programvarukvalitet inklusive cybersäkerhet.

För det fjärde: Att produkter innehållande programvara har defekter är något beställare och konsumenter förväntas acceptera. Innebörden av *time to market* har inom it-branschen en förlängning i form av uttrycket *release now, patch later.* Uttrycket, som finns i olika varianter, illustrerar synen på mjukvarukvalitet generellt men får också särskilda konsekvenser avseende cybersäkerhet eftersom den som investerar tid och resurser för att ta fram en säkrare produkt riskerar att inte få några kunder till följd av att produkten lanseras senare och med en högre prislapp.

För det femte: Ansvaret för att bedöma om en produkt innehållande programvara har tillräcklig säkerhet faller idag på den enskilde konsumenten eller näringsidkaren, samtidigt som denne i dagsläget saknar förutsättningar för att göra ett aktivt val. I den mån säkerhet nämns i produktinformationen är det inte ovanligt med skönmålande formuleringar och hänvisningar till kryptoalgoritmer, som å ena sidan kräver expertkunskaper för att förstå innebörden och å andra sidan saknar nödvändiga detaljer för en expertbedömning avseende produkten i sin helhet.

Att cybersäkerhet inte prioriteras kan illustreras genom en vetenskaplig artikel från 2021 där forskare inom CDIS-samarbetet skickade ut en enkät till offentliga aktörer i Sverige. Av 129 svarande kommuner hade 71 procent färre än en heltidsanställd som arbetade med cybersäkerhet. Av 134 svarande myndigheter var siffran 48 procent med ytterligare 10 procent som svarade att cybersäkerheten var utkontrakterad.[67]

Angående utmaningen att skapa tillräckligt säkra system finns det inom akademien såväl som i specifika branscher ackumulerad kunskap och erfarenhet kring vad som krävs för att ta fram högkvalitativ mjukvara. Däremot är, i de absolut flesta fallen, användandet av dessa metoder och verktyg inget som premieras utan snarare tvärtom leder till förlorare affärer. Detta minskar sannolikt också intresset att finansiera eller bedriva forskning och innovation inom området.

Många organisationer påtalar vidare att det råder brist på individer med utbildning

på avancerad nivå inom området, samtidigt som individer som har ringa eller begränsad utbildning fortsatt anställs för att arbeta som utvecklare. Situationen kan uppfattas som paradoxal men är möjlig, eftersom de kunskaper och färdigheter som lärs ut inom den ingenjörsdisciplin och de utbildningar som uppstod efter Natokonferensen 1968 i många fall inte är nödvändiga utifrån gällande kravnivå i it-branschen.

I förlängningen är det också tveksamt vilka incitament ungdomar har att genom studielån finansiera en tre- till femårig ingenjörsutbildning eller datavetenskaplig utbildning när det går lika bra att få motsvarande befattning och lön genom att införskaffa betydligt ytligare kunskaper på egen hand. Även frånvaro av årlig löneutveckling under studietiden kommer sannolikt att missgynna den som lägger tid och kraft på en längre utbildning. Därför riskerar bristen på personal med rätt kompetens att kvarstå och också förvärras i takt med att fler individer i branschen behövs till följd av den fortsatta tekniska utvecklingen.

Återigen, den situation som beskrivits ovan är inte på något sätt plötsligt uppkommen. Det som har hänt är att medvetenheten om problemen har ökat, vilket till del kan bero på det ökande och fortsatt accelererande beroendet av digitala system kombinerat med ett försämrat omvärldsläge. Till det kommer att kriminella, oavsett om de är statsunderstödda eller ej, i högre grad börjat använda utpressningsprogramvara som inkomstkälla vilket leder till större ekonomisk skada för den drabbade.

Den centrala frågan är hur trenden kan vändas innan större förluster av människoliv eller skador på egendom eller miljö sker. Svaret är att på strategisk nivå måste cybersäkerhet hanteras som en samhällsangelägenhet där alla aktörer behöver vara delaktiga. På teknisk nivå måste hård- och mjukvara oavsett tillämpning börja produceras med säkerhet i åtanke. Först då kan samhället komma ifrån den ständiga kapplöpningen där verksamheten alltid är i efterhand för att täppa till de sårbarheter som alltför ofta uppmärksammas genom att en antagonist utnyttjar dem för sina syften.

Åtgärder på kort sikt – inriktning och uppföljning

För att åstadkomma nödvändiga strukturella förändringar bör följande åtgärder övervägas:

1. Tydlig inriktning med uppföljning från regeringen och regeringskansliet av myndigheternas arbete för att säkerställa efterlevnad av lagar, förordningar och föreskrifter inom informations- och cybersäkerhetsområdet. Uppföljningen bör särskilt inkludera effekterna av tillsynsmyndigheternas arbete.
2. Utökade resurser för tillsynsmyndigheterna, inklusive mandat att utfärda viten och sanktionsavgifter för både offentliga och privata aktörer som inte följer författningar och föreskrifter. Sanktionerna för att prioritera bort nödvändig cybersäkerhet behöver sannolikt vara i paritet med vad det hade kostat att upprätthålla en adekvat säkerhetsnivå från början, möjligen också i kombination med ersättningskrav för de kostnader och skador som drabbar andra till följd av underlåtenheten.
3. En samordnad och gemensam linje avseende cybersäkerhet genom samtliga departement. Sveriges informations- och cybersäkerhet är inte en fråga för enbart försvars- och justitiedepartementet. Genom att man fullt ut nyttjar styrkan med den svenska förvaltningsmodellen kan nödvändiga effekter uppnås på bredden men det kräver en gemensam

bakomliggande strategi som säkerställer att målkonflikter mellan olika intressen undvikas.

Olika departement och sakområden kommer fortsatt att ha skilda behov, vilket framgår av modellen i föregående avsnitt. Däremot bör så långt som möjligt dessa behov harmoniseras, exempelvis i form av den kravtrappa som beskrivs i nästa delavsnitt.

4. Översyn och, vid behov, införande av krav i akademiska yrkesexamina på förståelse av hur bristande informations- och cybersäkerhet kan påverka samhället och den egna professionen.

   Författningsstöd finns redan genom de generella krav högskoleförordningen (1993:100) för flera examina ställer på bland annat värderingsförmåga och förhållningssätt.[68] För önskad effekt är det centralt att bredda perspektivet till mer än de tekniska utbildningarna: En grundläggande förståelse för cybersäkerhet behöver bland annat ingå även i ekonom- och juristutbildningar.

   För att uppnå önskat läge behöver varje enskilt lärosäte ta ansvar för sina egna utbildningar samtidigt som Universitetskanslersämbetet (UKÄ) behöver följa upp att nödvändig effekt uppnås genom den tillsyn myndigheten bedriver. Ett specifikt uppdrag samt resurser för detta till UKÄ kan vara nödvändigt för att komma igång med arbetet. Vid behov kan också mindre justeringar i högskoleförordningen bli aktuella.

5. Utökade och öronmärkta anslag för utbildningsplatser på lärosäten som har relevanta utbildningar inom informations- och cybersäkerhet. Idag finns i vissa fall kapacitet för fler studenter samtidigt som lärosätet slagit i taket för hur många platser som statsmakten finansierar. Sådan styrning kan uppfattas som klåfingrig och detaljreglerande men kan ändå vara nödvändig till dess att systemet stabiliserats.

6. Införande av cybersäkerhetsrelaterad standardisering för konsumentprodukter. Den nya konsumentköplagen är ett utmärkt första steg på vägen men för att konsumenterna ska kunna ta sitt ansvar behövs en tydlig kvalitetsmärkning samt ett kontrollsystem för detta. En sådan märkning bör vara gemensamt inom EU och kan med som alternativ inordnas inom befintliga kvalitetssystem, exempelvis CE-märkningen.

Sammantaget ger ovanstående förändringar förhoppningsvis kaskadeffekter genom hela systemet. Tydliga krav kombinerat med effektiv tillsyn av verksamhetsutövare, oavsett organisationsform, bör till exempel leda till motsvarande krav på leverantörer som utvecklar system eller tillhandahåller tjänster. För att kunna leverera enligt kraven behöver leverantörerna i sin tur anställa individer med rätt kompetens alternativt utbilda dessa efter anställning. Oavsett kommer trycket att öka på tekniska lärosäten och andra utbildningsföretag då det gäller att erbjuda relevanta utbildningar i tillräcklig omfattning. Genom att det ställs högre krav på kompetens kommer också löner och andra förmåner att premierna längre utbildningar vilket ökar attraktionskraften för dessa samtidigt som samhällets sammantagna förmåga ökar. Därmed uppstår en positiv spiral som även bedöms kunna leda till ökad konkurrenskraft för svenska företag.

Sveriges konkurrenskraft kan ökas ytterligare genom olika samarbeten mellan myndigheter och aktörer i näringslivet. Ett exempel är det cybercampus som Försvarsmakten, MSB och RISE tillsammans med andra aktörer arbetar med att etablera, där ambitionen är att knyta samman akademisk forskning

med aktörer som kan skapa produkter och tjänster utifrån forskningsresultaten.

Ett annat exempel kan vara ett samarbete mellan offentliga och privata aktörer för att skapa förmåga till inhemsk produktion av utvalda elektronikkretsar som är av vikt för totalförsvaret och där kraven på säkerhetsskydd i hela leverantörskedjan är särskilt högt. Om samma anläggning också producerar tillförlitliga delar till kritiska industritillämpningar kan kostnaderna delas på flera aktörer samtidigt som nödvändiga volymer för att hålla tillverkningen igång uppnås. Motivet till inhemsk produktion, som alternativt skulle kunna vara ett nordiskt eller europeiskt samarbete är det enkla faktum att det inte spelar någon som helst roll hur säker programvaran är om en antagonist har planterat in bakdörrar i den underliggande hårdvaran. Det hårdvaran döljer kan programvaran aldrig upptäcka. Likaså är det praktiskt omöjligt att fysiskt granska varje levererad hårdvarukrets för att upptäcka eventuella bakdörrar.

Harmoniserad kravtrappa med företräde för nationell säkerhet

I avsnittet om den legala grundplattan beskrivs sex olika regleringsområden med explicita krav på informations- och cybersäkerhet. Eftersom behovet av cybersäkerhet går genom hela samhället är det naturligt att det regleras i flera områden. Nuvarande regler innebär dock vissa utmaningar för den verksamhetsutövare som bedriver verksamhet som omfattas av mer än ett område.

För det första ställer förordningarna och föreskrifterna liknande men inte identiska krav. Detta innebär att verksamhetsutövarna behöver analysera och dokumentera skillnaderna samt vilka åtgärder som är tillräckliga för varje enskilt fall. I nästa steg behöver verksamhetsutövaren uppnå samsyn med respektive tillsynsmyndigheter.

För det andra kan det vara svårt att avgöra vilka lagar och förordningar som gäller i ett specifikt fall. Till exempel innehåller lagen om informationssäkerhet för samhällsviktiga och digitala tjänster utöver specifika undantag följande paragraf:

> 9 § Om det i lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder och incidentrapportering ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt denna lag, med beaktande av bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.[69]

För att underlätta för alla aktörer som ska efterleva de olika regleringarna förordas därför att en nationell harmoniserad kravtrappa för informations- och cybersäkerhet etableras. Trappan kan utformas på olika sätt. Ett exempel kan vara att utgå från modellen i det föregående avsnittet men det finns naturligtvis flera andra möjliga strukturer.

Oavsett struktur bör trappan leda till en gemensam grundplatta som gäller inom samtliga områden och sedan byggs på allt eftersom systemens eller funktionernas betydelse för samhället och Sveriges suveränitet ökar. Ytterligare påbyggnad kan göras inom särskilda funktionsområden, exempelvis inom elektroniska kommunikationsnät samt områdes- och verksamhetsspecifika krav inom de olika beredskapssektorerna.

I utformningen av trappan, vars grund behöver ligga i lagar och förordningar, är det viktigt att fortsatt beakta och säkerställa fortsatt separation mellan unionsrätten och den nationella säkerheten. Bland annat är det angeläget att skydda information om förhållanden kopplade till totalförsvaret och särskilt det militära försvarets behov och för-

mågor. Detta inkluderar incidentrapporter samt reglering för denna.

Här finns det skäl att se över skärningen mellan beredskapsförordningarna respektive regleringen för samhällsviktiga och digitala tjänster, där det i det första fallet kan finnas skäl att utöka vilka verksamheter som anses utgöra samhällskritiska funktioner ur ett totalförsvarsperspektiv. Samtidigt saknar beredskapslagstiftningen i dagsläget föreskrifts- och tillsynsmöjligheter inom cybersäkerhetsområdet gentemot privata aktörer.

Även nationellt är det viktigt att upprätthålla separation så att endast de myndigheter som har ett ansvar för, eller påverkas av incidenterna, får del av informationen. Dessa myndigheter får i sin tur ansvara för att övriga myndigheter eller aktörer som har behov av informationen delges denna. Ytterligare en viktig aspekt i detta är att skapa förutsättningar för att incidentrapporter så snabbt som möjligt, utan omvägar, når de aktörer som behöver agera på informationen.

En avslutande fördel med den trappa som föreslås är att den ökade enkelheten bör kunna öka produktionstakten och minska kostnaderna för de system som kommer att behöva ersätta äldre och osäkrare sådana, samt inte minst det ökade behovet av system inom uppbyggnaden av totalförsvaret.

Harmonisering av tillsynsmyndigheter

Det finns idag en diskrepans mellan vilka myndigheter som har föreskrifts- och tillsynsansvar beroende på om verksamheten faller inom säkerhetsskydd eller totalförsvar, där majoriteten av de civilområdesansvariga länsstyrelserna är tillsynsmyndigheter i säkerhetsskyddsförordningen. De civilområdesansvariga länsstyrelserna i Örebro och Östergötland utgör undantag och ligger istället under andra länsstyrelsers tillsyn.

Ytterligare diskrepanser framträder när samhällsviktiga och digitala tjänster, som är det tredje större regleringsområdet med bäring på informations- och cybersäkerhet, inkluderas. Flera av tillsynsmyndigheterna är sektorsansvariga myndigheter i förordningen om statliga myndigheters beredskap. Affärsverket svenska kraftnät samt Trafikverket utgör undantag, dessa ingår istället som beredskapsmyndigheter inom sina respektive sektorer.

Det finns ibland goda skäl till att ha sådana diskrepanser. Ur ett cybersäkerhetsperspektiv är det dock önskvärt att så långt som möjligt harmonisera strukturerna, inte minst för att möjliggöra effektiv uppföljning och tillsyn i den kravtrappa som föreslås i det föregående avsnittet.

Stöd och incitament för systematisk mognad

Att ta fram högkvalitativa system bestående av hård- och mjukvara kräver ändamålsenliga processer där kvalificerad personal inom olika discipliner samordnas för att uppnå önskat slutresultatet. Detta skiljer sig inte nämnvärt från andra tillverkande högteknologiska branscher. Vad som däremot skiljer sig är att i övriga branscher skulle bristande tillverkningsmetoder sannolikt innebära ett slutresultat som marknaden och konsumentskyddsorganisationer aldrig skulle acceptera, medan det i it-branschen istället resulterar i säkerhetsmässigt undermåliga system som används på bred front i samhället.

Att visa att ett system är osäkert är förhållandevis lätt men att löpande under utveck-

lingsprocessen bygga upp ett förtroende för att systemet är tillräckligt säkert kräver desto mer. Som konstaterats tidigare i artikeln saknas dock ofta ekonomiska incitament att upprätthålla nödvändig kompetens och processmognad. Detta leder till ett moment 22 där myndigheter som är villiga att betala för sådan förmåga ändå inte kan föra in det som krav i upphandlingar eftersom det finns för få företag som kan lämna anbud, varvid samhällets cybersäkerhetsskuld fortsätter att ackumuleras.

Vägen ut ur problemet är därför att skapa en tillräcklig volym av svenska företag med förmåga att producera högkvalitativa och därmed säkrare system. För att åstadkomma detta kan följande åtgärder i kombination övervägas:

1. Ändrad instruktion samt nödvändiga resurser till Upphandlingsmyndigheten att som komplement till befintliga områden[70] stödja det offentliga avseende kravställning och verifiering av krav för informations- och cybersäkerhet.
2. Uppdrag till DIGG alternativt Försvarets materielverk att utveckla förmåga och kapacitet att som oberoende instans utvärdera företag och andra systemutvecklande organisationer i relevanta mognadsmodeller för systemutveckling samt metoder för att utveckla tillförlitliga system.
3. I uppdraget bör det även ingå att kunna stödja utvecklingsorganisationer med att införa systematiska processer och mognadsmodeller, samt att upprätthålla ett register där företag som uppnått och regelbundet kan visa att de upprätthåller en viss mognadsnivå kostnadsfritt kan välja att lista sig.
4. Uppdrag till DIGG alternativt Upphandlingsmyndigheten att stödja den offentliga sektorn så att kommande upphandlingar säkerställer att leverantörerna har tillräcklig mognadsnivå för att uppnå ställda cybersäkerhetskrav.
5. Under en övergångsperiod utforma upphandlingar på ett sådant sätt att projekten inleds med en första fas där leverantören med stöd av DIGG eller FMV höjer sin mognad till en för uppdraget acceptabel nivå. Allt eftersom fler leverantörer uppnår en tillräcklig nivå kan stödet trappas ner samtidigt som kraven på sådan förmåga skärps, med första prioritet för system och tjänster som är samhällsviktiga.

Ett exempel på en mognadsmodell för generell mjukvarukvalitet är CMMI-DEV som togs fram av universitetet Carnegie-Mellon (CMU). En sådan modell bör kompletteras med lämpliga metoder från standarder för säkerhetskritiska tillämpningar, exempelvis standarden för elektronik i vägfordon, SS-ISO 26262, som tillämpar metoden med *Safety Cases*.[71] Förenklat innebär metoden att tillverkaren parallellt med utvecklingen sätter samman en strukturerad argumentation uppbackad av relevanta bevis som tillsammans belägger påståendet att systemet är tillräckligt säkert för sitt ändamål. Metoden har genom den internationella standarden för assuransfall, ISO/IEC/IEEE 15026, även generaliserats för att kunna användas oavsett bransch.

Ytterligare åtgärder att överväga

Om de ovanstående listade förslagen inte ger tillräckligt resultat kan i nästa skede ytterligare åtgärder övervägas:

1. Ett straffrättsligt ansvar för verksamhetsansvariga som grovt åsidosätter sina skyldigheter, på liknande sätt som inom arbetsmiljöområdet alternativt säkerhetsskyddet.
2. Ett konsumentansvar som innebär någon form av konsekvens för den som avsiktligt

använder produkter som saknar vedertagen märkning alternativt inte installerar nödvändiga säkerhetsuppdateringar och därigenom orsakar skada för andra personer eller samhället. Detta kan liknas framförandet av ett trafikfarligt fordon, eller allvarligare, vållandet av en trafikolycka till följd av framförandet.

En utmaning som kräver en djupare analys är dock hur en rimlig balans uppnås så att innovation och konkurrens inte hämmas. En särskild fråga i sammanhanget är om ansvaret ska avgränsas till kompletta produkter eller om det också ska gälla alla typer av applikationer och operativsystem en slutanvändare installerar på sin dator. En reglering som förhindrar nyttjande eller utveckling av öppen källkod, som till stor del också används i kommersiella lösningar skulle sannolikt få allvarliga konsekvenser för fortsatt innovation och digitalisering.

3. Ett system för auktorisation av både företag och individer som har nyckelroller i utveckling eller anskaffning av samhällskritiska system. Inspiration kan hämtas från elsäkerhetsområdet, där tillsynsmyndigheten med stöd av elsäkerhetslagen (2016:732) ställer krav på att installatören har både utbildning och praktisk erfarenhet. För företag ställs krav på fungerande egenkontroll. Auktorisationen för företag respektive individer delas sedan in i olika nivåer. En sådan nivåindelning skulle i cybersäkerhetsområdet kunna spegla systemets vikt för samhället.

   Införande av sådan auktorisation inom it-området är dock långt ifrån lika enkel som inom elsäkerhetsområdet. Det finns ett antal utmaningar som kommer att kräva fördjupad analys liksom samverkan mellan myndigheter, akademi och näringsliv.

Önskat läge

De åtgärder som presenterats ovan förväntas bidra till ett önskat läge som kan sammanfattas enligt följande:

- Cybersäkerhet ses som en samhällsangelägenhet där alla aktörer inklusive den enskilde individen bidrar med sin del och tar sitt ansvar.
- En nationell harmoniserad kravtrappa för informations- och cybersäkerhet som omfattar lagar, förordningar, föreskrifter och vägledningar är etablerad.
- De lagar, förordningar och föreskrifter som rör informations- och cybersäkerhet efterlevs och ses som en lägsta nivå.
- Tillsynsmyndigheter är utsedda för samtliga relevanta områden och är resurssatta för att kunna utföra en effektiv tillsyn som både är stödjande och uppföljande.
- Totalförsvarets aktörer och övriga samhällsviktiga funktioner har säkra leverantörskedjor för samtliga system de är beroende av.
- Svenska högskolor och universitet åtnjuter ett välförtjänt internationellt rykte om att i relevanta vetenskapsområden producera individer med förståelse och förmåga att bidra till samhällets cybersäkerhet.
- Svenska företag och Sverige som nation är en väl ansedd leverantör av hård- och mjukvarukomponenter och system för säkerhetskritiska tillämpningar inom både EU och Nato.

Genomgående för det önskade läget är förståelsen och acceptansen i alla led för att säkerhet aldrig kan granskas in i efterhand utan måste designas in från början och därefter kontinuerligt upprätthållas under hela

systemets livslängd. Denna förståelse kombineras med insikten att målet inte är hundra procent säkra system. Istället gäller att varje system ska vara tillräckligt säkert för sitt syfte, vilket innebär frånvaro av oacceptabel risk. Vad som är oacceptabel risk för ett givet system är inte konstant utan bestäms bland annat av systemets utformning och egenskaper, dess användningsmiljö inklusive exponering samt konsekvenserna för verksamheten vid antagonistisk påverkan.

Förslag på författningsändringar

Som tillägg till det föregående avsnittet har det noterats några fall där existerande författningar skulle kunna justeras i syfte att dels förstärka de befintliga strukturerna för att ge ansvariga myndigheter bättre verktyg att lösa sina uppgifter, dels generellt förtydliga och flytta fram positionerna för cybersäkerhet inom svensk författning. Förslagen presenteras med ett stort mått av ödmjukhet utifrån att de är skrivna för en artikel och inte inom ramen för en offentlig utredning med stöd av juridisk expertis.

Korrigerande av felöversättningen i svenska GDPR

Den svenska versionen av GDPR[72] bör utifrån artikelns begreppsavsnitt korrigeras avseende den felaktiga direktöversättningen av engelskans *integrity*. Ordet *integritet* bör således ersättas med *riktighet* i:

- Kapitel II, artikel 5, punkt 1f.
- Kapitel IV, artikel 32, punkt 1b.

Åtgärden kan ses som trivial, men förvirring och språkförbistring bör så långt som möjligt undvikas.

Införande av cybersäkerhet i beredskapslagstiftningen

Utifrån vad som beskrivits i det inledande begreppsavsnittet kan tiden vara inne att införa cybersäkerhet i beredskapslagstiftningen genom att i förordningen om statliga myndigheters beredskap:

1. införa en definition av cybersäkerhet i förordningens 6 §, förslagsvis med utgångspunkt från artikelns begreppsavsnitt,
2. ändra rubriken före 13 § från Informationssäkerhet till *Informations- och cybersäkerhet*,
3. revidera 13 § för att inkludera den tillförda definitionen av cybersäkerhet, ta bort de nuvarande begränsningarna till informationshanteringssystem och myndighetens egna system samt förtydliga att det är ledningsförmåga snarare än ledningsstödssystem som ska upprätthållas.

   Förslag på ny lydelse: Varje myndighet ansvarar för att de system och tjänster myndigheter nyttjar har en sådan nivå av informations- och cybersäkerhet att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Myndigheten ska särskilt beakta behovet av att i samtliga konfliktnivåer upprätthålla den egna ledningsförmågan.
4. införa en kompletterande paragraf om rapportering efter 14 § som gäller oavsett om det är säkerhetskänslig verksamhet eller ej. Skyndsam rapportering till Försvarsmaktens CERT är nödvändig för att åtgärder för skydd och försvar snabbt ska kunna vidtas. Försvarsmakten bör därför också ges möjlighet att utfärda föreskrifter för sådan rapportering. Förslag på lydelse:

   Cybersäkerhetsrelaterade händelser som kan påverka det militära försvarets förmå-

ga att möta ett väpnat angrepp ska skyndsamt rapporteras till Försvarsmakten.

Ett antagande är att det föreslagna avsnittet om informations- och cybersäkerhet gäller i samtliga konfliktnivåer. Om juridisk expertis gör en annan tolkning utifrån rubrikindelningen i förordningen bör förändringar göras så att det blir tydligt att det gäller både innan och under höjd beredskap samt så långt som möjligt under väpnad konflikt.

Genom att begränsningen till myndighetens egna system tas bort samt att tjänster införs i lydelsen måste myndigheterna också ställa motsvarande krav på sina leverantörer. Detta innebär att privata aktörer indirekt men utan behov av ytterligare lagstiftning träffas genom de avtal myndigheterna behöver upprätta. Sådana avtal behöver utöver att gälla för samtliga konfliktnivåer också omfatta incidentrapportering samt myndigheternas möjlighet att hos leverantören regelbundet kontrollera att kraven är uppfyllda. Konstruktionen innebär slutligen att de privata aktörerna får ersättning för det arbete som krävs för att tillhandahålla produkter och tjänster som uppfyller totalförsvarets behov av robusthet och säkerhet.

Krav på cybersäkerhet även för regioner och kommuner

Det finns för närvarande en lucka i lagstiftningen genom att de krav som gäller för statliga myndigheter inom beredskapslagstiftningen inte omfattar andra offentliga aktörer. Detta är kanske den mest allvarliga bristen i nuvarande reglering, inte minst utifrån det ansvar kommuner och regioner har för att upprätthålla befolkningens liv och hälsa i samtliga konfliktnivåer, samt att kunna lämna stöd i övrigt till det militära försvaret i händelse av höjd beredskap eller krig.

De förslag på krav som ovan föreslås för statliga myndigheters beredskap bör därför införas i motsvarande förordningar för regioner och kommuner. MSB:s föreskriftsrätt bör som konsekvensändring utökas till att även omfatta dessa.

Utökade verktyg för Försvarsmakten inom totalförsvaret

Försvarsmakten har i dagsläget rätt att ta del av andra aktörers totalförsvarsplanering samt en uppgift att delge relevant egen planering till dessa. Däremot saknar myndigheten mandat att kontrollera den faktiska cybersäkerheten hos dessa aktörer liksom möjlighet att ge inriktningar avseende nödvändiga åtgärder för att höja skyddet eller förbereda system för försvar av Försvarsmaktens kvalificerade cyberförsvarsresurser.

Försvarsmakten bör därför avseende cybersäkerhet och cyberförsvar få mandat att avseende system, inklusive elektroniska kommunikationstjänster, som är av betydelse för huvuduppgiften:

1. med Försvarsmaktens egna resurser vid behov genomföra säkerhetsgranskningar inklusive penetrationstestning både inifrån och utanför systemgränsen,
2. ålägga myndigheter, affärsverk, regioner och kommuner att vidta särskilda åtgärder för att öka skyddet i specifika system samt att i vissa fall också förbereda dem för cyberförsvar,
3. inrikta vilka verksamhetsutövare av betydelse för det militära försvaret som ska anslutas till det intrångsdetekteringssystem som Försvarets radioanstalt upprätthåller.

Den första punkten har tydliga likheter med 8 kap 2 § i lagen om elektronisk kommunikation där tillsynsmyndigheten får ålägga genomförandet av oberoende granskningar

som sedan redovisas för myndigheten. För att upprätthålla de skyddsvärden som föreligger avseende försvarsplaneringen föreslås här istället att sådan granskning genomförs av Försvarsmaktens egna resurser.

Den andra punkten är avsiktligt avgränsad till offentliga aktörer för att förenkla ett snabbt införande. Motsvarande behov kan föreligga även för privata aktörer men detta är en mer komplicerad fråga som också gäller utanför cybersäkerhetsområdet.

I den andra punkten ingår möjligheten att uppdra åt en verksamhetsutövare att begära stöd från Försvarets radioanstalt utifrån dess myndighetsinstruktion.[73] För ökad tydlighet avseende detta kan det finnas skäl att uppdatera 4 § i instruktionen för att explicit ange att stöd kan lämnas till totalförsvarsaktörer.

Införande av tillsyn kopplat till beredskapslagstiftningen

Det krav och de föreskrifter för informations- och cybersäkerhet som ställs utifrån förordningen om statliga myndigheters beredskap har gällt under lång tid. Under samma tid har incidenter inträffat hos olika myndigheter där incidenternas natur gör att det finns skäl att misstänka att förordningen inte har efterlevts.

Det är därför lämpligt att utse tillsynsmyndigheter som kan arbeta både proaktivt och på förekommen anledning för att stödja och följa upp efterlevnaden. Dessa tillsynsmyndigheter, som också bör få ge ut kompletterande föreskrifter skulle, med utgångspunkt från hur tillsynen för säkerhetskänslig verksamhet är organiserad, kunna vara:

- Försvarsmakten för myndigheter under försvarsdepartementet samt Försvarshögskolan och Fortifikationsverket.
- MSB för övriga statliga myndigheter under regeringen med undantag för Säkerhetspolisen. MSB föreslås dels för myndighetens roll inom det civila försvaret, dels för att MSB idag är föreskriftsmyndighet avseende informationssäkerheten i förordningen om statliga myndigheters beredskap. Ett alternativ skulle kunna vara att istället ge Säkerhetspolisen tillsynsuppdraget eftersom det då i princip skulle bli samma myndigheter som inom säkerhetsskyddslagstiftningen.
- De civilområdesansvariga länsstyrelserna för länsstyrelser samt för regioner och kommuner inom respektive civilområde.

På samma sätt som att MSB idag har i uppgift att inom lag och förordning för samhällsviktiga och digitala tjänster stödja tillsynsmyndigheterna bör MSB ges ett motsvarande uppdrag även inom detta område. En förutsättning för att förändringen ska ge effekt är att de utsedda myndigheterna också tillförs ekonomiska medel för att kunna utveckla och bedriva tillsynsverksamheten.

Föreskriftsrätt även för digitala tjänster

I förordningen om samhällsviktiga och digitala tjänster utses MSB samt tillsynsmyndigheterna inom respektive ansvarsområde till föreskriftsmyndigheter för samhällsviktiga tjänster. MSB får även utfärda föreskrifter för incidentrapportering avseende samhällsviktiga såväl som digitala tjänster.

Däremot har regeringen inte fördelat föreskriftsrätt avseende digitala tjänster. Även om själva förordningen ställer vissa förtydligande krav avseende säkerheten för dessa så bör samma myndigheter som utfärdar föreskrifter för de samhällsviktiga tjänsterna också ges rätt att göra det för de digitala tjänsterna.

Införande av cybersäkerhet i säkerhetsskyddslagstiftningen

Enligt säkerhetsskyddslagen ska skyddsåtgärden informationssäkerhet:

1. förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och
2. förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet[74]

I författningskommentarerna framgår att den andra punkten särskilt syftar till att tillgodose behov av riktighet och tillgänglighet för information och informationssystem ”som har avgörande betydelse för t ex styrning, reglering och övervakning av för Sverige viktiga samhällsfunktioner […]”[75] Detta innebär en utvidgning av informationssäkerhetsbegreppet genom att omfatta andra system än sådana vars syfte är att hantera information. Samtidigt definierar säkerhetsskyddsförordningen informationssystem som ”[…] ett system av sammansatt mjuk- och hårdvara *som behandlar information*” (egen kursivering),[76] vilket är i linje med informationssäkerhetsbegreppets traditionella betydelse.

För att tydliggöra att cybersäkerhet ingår i säkerhetsskyddet kan man därför överväga att i säkerhetsskyddslagens andra kapitel införa cybersäkerhet som en fjärde säkerhetsskyddsåtgärd, samt döpa om säkerhetsskyddsförordningens tredje kapitel till ”Informations- och cybersäkerhet”.

Viten och sanktionsavgifter för bristande cybersäkerhet

I *Totalförsvaret 2021–2025* konstaterade regeringen att det finns ett problem i att säkerhetsskyddsstiftningens tillsynsmyndigheter saknade sanktionsmöjligheter.[77] Konstaterandet efterföljdes av en lagrådsremiss, proposition och ett betänkande från justitieutskottet inför riksdagsbehandling. Av betänkandet framgår bland annat att:

> Avsaknaden av sedvanliga tillsynsbefogenheter och möjligheter att ingripa medför enligt regeringen att det finns en risk att verksamhetsutövare är mindre benägna att följa tillsynsmyndigheternas anvisningar och säkerhetsskyddslagstiftningens krav, vilket i förlängningen kan leda till skada för Sveriges säkerhet.[78]

Efter behandling i riksdagen reviderades lag och förordning vilket bland annat innebär att tillsynsmyndigheterna kan utdela både viten och sanktionsavgifter. Samtidigt fick tillsynsmyndigheterna ökade befogenheter att begära information från och tillträde till de verksamheter som tillsynen gäller.

De problem som i betänkandet tas upp avseende säkerhetsskyddet kvarstår för den cybersäkerhet som faller utanför säkerhetsskyddslagstiftningen. Nedanstående stycke från betänkandet skulle vara lika aktuellt om ordet *säkerhetsskydd* ersattes med *cybersäkerhet*:

> Flera uppmärksammade händelser de senaste åren har visat att verksamhetsutövare av stor betydelse för Sveriges säkerhet har haft ett eftersatt säkerhetsskydd. Orsaken har bl.a. varit att de har haft otillräcklig kunskap om sina egna skyddsvärden och att säkerhetsskyddsfrågor inte varit tillräckligt prioriterade i den egna organisationen.[79]

Så länge myndigheter, regioner och kommuner utan konsekvenser kan ignorera cybersäkerheten är det tvivelaktigt vilken nytta eventuell tillsyn gör. Därför bör förordningen om statliga myndigheters beredskap, avseende informations- och cybersäkerhetsområdet, kompletteras på liknande sätt som skett inom säkerhetsskyddet.

En förutsättning är att det tidigare förslaget om att faktiskt utse tillsynsmyndigheter införs tillsammans med den utökade omfattningen till att gälla även regioner och kommuner. Det är slutligen angeläget att möjligheten att utfärda viten och sanktionsavgifter gäller för underlåtenhet att skyndsamt rapportera cybersäkerhetsincidenter till berörd myndighet.

Avslutande reflektioner

Tiden då cybersäkerhet kunde ses som en option, alternativt någon annans problem som bör lösas på central nivå, är förbi. Tillräcklig cybersäkerhet är redan i viss utsträckning en förutsättning för att samhället ska fungera och kommer i ännu högre utsträckning att vara det i framtiden. Kostnaden för att ignorera cybersäkerheten kommer snart att vara betydligt större än att investera i nödvändiga resurser för att skapa och upprätthålla den. Det finns också konsekvenser som är svåra att mäta i ekonomiska termer, inte minst ur ett totalförsvarsperspektiv.

Sveriges cybersäkerhet är en angelägenhet och en utmaning som måste lösas på bred front och av hela samhället. Grundproblemet är inte i första hand bristen på regleringar utan snarare okunskap om vilka dessa är, kombinerat med bristen på tilldelade resurser för att efterleva dem. Inte minst saknas i många verksamheter individer med rätt kompetens och tillgänglig tid för att omsätta gällande styrningar i effektiva säkerhetshöjande åtgärder.

Det behövs naturligtvis även fortsatt myndigheter med samordnande ansvar inklusive ansvar för föreskrifter och tillsyn, men det konkreta arbetet med att upprätthålla cybersäkerheten måste ske på daglig basis hos varje enskild aktör. Framför allt måste cybersäkerhet vara en integrerad del i varje verksamhets risk- och kontinuitetsplanering. Inspiration kan med fördel hämtas från Natos princip att cybersäkerhet syftar till att säkerställa verksamhetens förmåga att lösa sina uppgifter, vilket innebär att tillräcklig cybersäkerhet inte bara är den enskilda verksamhetsutövarens ansvar utan också en förutsättning för dess fortsatta verksamhet.

Mycket återstår att göra. Samtidigt innebär den svenska förvaltningsmodellen att när ett problem väl har identifierats som angeläget så finns det goda möjligheter att agera på bred front. Attityden och målsättningen bör därför, med omedelbar verkan, vara att nya system som tillförs inte ytterligare ökar samhällets cybersäkerhetsskuld utan istället reducerar den. Parallellt och i samma andra behöver åtgärder vidtas för att minska exponering och risk i befintliga system.

Sverige bör fortsatt sträva efter att ligga i teknikens framkant. Vägen framåt är således fortsatt digitalisering, men säker sådan och med beaktande av totalförsvarets behov. Genom detta kan svenska företag bli världsledande inom säker digitalisering och därmed säkerställa inte bara vår egen cybersäkerhet utan också vårt framtida välstånd.

Författaren är civilingenjör i informationsteknologi och tjänstgör vid Försvarsstaben.

Noter

1. Sternudd, Patrik: ”Sveriges cyberförsvar tar form”, *KKrVAHT*, 1. häftet 2022, s 80-106.
2. Ibid, s 95-102.
3. *Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8)*, MSB, 2018, 4 §.
4. *Offentlighets- och sekretesslagen (2009:400)*, Regeringen, 3 kap 1 §.
5. *EU:s dataskyddsförordning (GDPR*), Europaparlamentets och rådets förordning (EU) 2016/679, 2016.
6. *Terminologi för informationssäkerhet,* TR 50:2015, SIS, 2015.
7. *Försvarsmaktens handbok Nomenklatur ledning 2016*, FM2016-4705:4, Försvarsmakten, 2016.
8. *Säkerhetsskyddslagen (2018:585)*, Riksdagen, 2 kap 2-4 §§.
9. I artikeln, liksom i svensk författning används orden *mjukvara* och *programvara* synonymt.
10. *Förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap*, Regeringen, 11c §.
11. Ordet mobil*telefon* är något missvisande då det skapar en mental association som inte uppenbart inrymmer att dagens telefoner har betydligt högre beräkningskraft, lagringsutrymme och bandbredd än många datorer hade för 20 år sådan. Lägg till det multipla kameror, mikrofoner och positioneringssystem.
12. Op cit, Sternudd, Patrik, se not 1.
13. *Militärstrategisk doktrin 22 (MSD 22)*, Försvarsmakten, 2022, s 50-59.
14. *Totalförsvaret 2021–2025*, prop 2020/21:30, Regeringen, 2020.
15. *Handlingskraft – Handlingsplan för att främja och utveckla en sammanhängande planering för totalförsvaret 2021–2025*, Försvarsmakten; Myndigheten för samhällsskydd och beredskap, 2021, s 24.
16. *Förordningen (2022:524) om statliga myndigheters beredskap*, Regeringen, 13 §.
17. *Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter*, MSBFS 2020:6, MSB, 2020.
18. *Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter*, MSBFS 2020:7, MSB, 2020.
19. Ibid, 4 kap 11 §.
20. Ibid, 2 kap 4 §.
21. *Säkerhetsskyddsförordningen (2021:955)*, Regeringen, 3 kap 4 §.
22. *Säkerhetspolisens föreskrifter om säkerhetsskydd*, PMFS 2022:1, Säkerhetspolisen, 2022, 2 och 32 §§.
23. Op cit, *Säkerhetsskyddsförordningen*, se not 21, 3 kap 5 §.
24. *Försvarsmaktens föreskrifter om signalskyddstjänsten*, FFS 2021:1, Försvarsmakten, 2021.
25. *Föreskrifter om ändring i Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd*, FFS 2020:3, Försvarsmakten, 2020.
26. *Lagen (2022:482) om elektronisk kommunikation*, Riksdagen, 1 kap 1 §.
27. Ibid, 8 kap 1 §.
28. Ibid, 8 kap 2 §.
29. *Förordningen (2022:511) om elektronisk kommunikation*, Regeringen.
30. *Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster*, PTSFS 2022:11, PTS, 2022, 12 kap 1 §.
31. *Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster*, Riksdagen.
32. *Förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster*, Regeringen, 7 §.
33. *Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster*, MSBFS 2018:8, MSB, 2018, 6-7 §§.
34. Ibid, 11 §.
35. *Post- och telestyrelsens föreskrifter och allmänna råd om säkerhetsåtgärder för samhällsviktiga tjänster inom sektorn digital infrastruktur*, PTSFS 2021:3, PTS, 2021, 13 §.
36. *Europaparlamentets och rådets direktiv (EU) 2015/1535*, 2015, artikel 1.1 b.
37. Op cit, *Förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster*, se not 32, 6 §.
38. *Konsumentköplagen (2022:260)*, Riksdagen, 4 kap 4 §.
39. *Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning*, Riksdagen, 1-4 §§.
40. Det är i sammanhanget något ironiskt att den svenska versionen av GDPR som i stor utsträck-

ning reglerar just integritet samtidigt utgör ett exempel på sådan felaktig direktöversättning av *integrity* som beskrivs i det inledande begreppsavsnittet.

41. Op cit, *EU:s dataskyddsförordning (GDPR)*, se not 5, kap II, artikel 5, punkt f.
42. *Myndigheten för samhällsskydd och beredskaps föreskrifter om frivillig rapportering av tjänster som är viktiga för samhällets funktionalitet*, MSBFS 2018:11, MSB, 2018.
43. Op cit, *Konsumentköplagen*, se not 38, 6 kap 3 §.
44. Op cit, Sternudd, Patrik, se not 1, s 92-93.
45. *Förordningen (2007:1266) med instruktion för Försvarsmakten*, Regeringen, 3 §.
46. Op cit, Sternudd, Patrik, se not 1, s 93-94.
47. *Förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning*, Regeringen, 1 §.
48. Ibid, 8 §.
49. Ibid, 3-4 §§.
50. *Förordningen (2018:357) om myndighetsgemensam infrastruktur för säkra elektroniska försändelser*, Regeringen, 1 §.
51. Op cit, *Förordningen med instruktion för Myndigheten för samhällsskydd och beredskap*, se not 10, § 11 a.
52. Op cit, *Förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster*, se not 32, 11-12 §§.
53. Ibid, 12 §.
54. Op cit, *Förordningen med instruktion för Myndigheten för samhällsskydd och beredskap*, se not 10, 11 b §.
55. *Förordningen (2015:1053) om totalförsvar och höjd beredskap*, Regeringen, 16 §.
56. Op cit, *Säkerhetsskyddsförordningen,* se not 21, 8 kap 2 §.
57. Op cit, *Säkerhetspolisens föreskrifter om säkerhetsskydd*, se not 22, 2 kap 7 §.
58. *Förordningen (2007:854) med instruktion för Försvarets materielverk*, Regeringen, 5 §.
59. Ibid, 6 §.
60. *Förordningen (2007:937) med instruktion för Försvarets radioanstalt*, Regeringen, 3 §.
61. *Förordningen (2007:861) med instruktion för Totalförsvarets forskningsinstitut*, Regeringen, 1 §.
62. Inom Försvarsmakten har uppgiften tilldelats Militära underrättelse- och säkerhetstjänsten (Must).
63. Ytterligare information samt vägledning finns på *https://www.ssfcybersakerhet.se*, (2022-12-10).
64. Naur, Peter och Randell, Brian (red): *Software Engineering: Report on a conference sponsored by the NATO Science Committee, Garmisch, Germany, 7th to 11th October 1968*, Nato, 1969.
65. *Programvaruteknik* är den svenska översättningen till *Software Engineering* som vetenskaplig disciplin.
66. Spafford, Eugene Howard: *The Internet Worm Incident*, CSD TR·933, Purdue University, 1989.
67. Andreasson, Annika; Artman, Hanrik; Brynielsson, Joel och Franke, Ulrik: A census of Swedish public sector employee communication on cybersecurity during the COVID-19 pandemic, 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2021, s 1-8.
68. ”Bilaga 2 EXAMENSORDNING” i *Högskoleförordningen (1993:100)*, Regeringen.
69. Op cit, *Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster*, se not 31, 9 §.
70. *Förordningen (2015:527) med instruktion för Upphandlingsmyndigheten*, Regeringen.
71. Metoden med *Safety Cases* tillkom och började användas i brittisk oljeindustri som en konsekvens av domaren Lord Cullens utredning efter katastrofen på olje- och gasplattformen Piper Alpha 1988.
72. Op cit, *EU:s dataskyddsförordning (GDPR)*, se not 5.
73. Op cit, *Förordningen med instruktion för Försvarets radioanstalt*, se not 60, 4 §.
74. Op cit, *Säkerhetsskyddslagen,* se not 8, 2 kap 2 §.
75. *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag*, prop 2017/18:89, Regeringen, 2018, s 138.
76. Op cit, *Säkerhetsskyddsförordningen*, se not 21, 1 kap 3 §.
77. Op cit, *Totalförsvaret 2021–2025*, se not 14, s 131.
78. *Ett starkare skydd för Sveriges säkerhet*, 2021/22:JuU3, Riksdagen, s 5.
79. Ibid.