



Cybersäkerhet

**En kartläggning av Sveriges nuläge 2020
och framtidsutsikter för branschen**



SECURITY LINK
RESEARCH • EDUCATION • INNOVATION

**LINKÖPING
SCIENCE
PARK**

RAPPORTEN ÄR PRODUCERAD
AV UNITALENT AB PÅ UPPDRAG AV
SECURITY LINK, LINKÖPING SCIENCE PARK OCH TILLVÄXTVERKET.

Juni 2020

Rapportförfattare:
Emmy Englund
Linnéa Tullin

Grafisk produktion:
Emmy Englund

Sammanfattning	4
Inledning	6
Studiens genomförande	9
Resultat	11
Nuläge för cybersäkerhetsbranschen	11
Cyberhot och cyberangrepp	13
Tekniker	14
Samhällsfrågor, digitalisering och kompetensutveckling	19
Utbildning, forskning och innovation	24
Framtidsutsikter	30
Organisationer och projekt	33
Sammanfattande slutsatser	38
Förslag på vidare studier	43
Referenser	44

Sammanfattning

Det höga internationella tonläget och Sveriges omfattande och snabba digitalisering driver utvecklingen av cybersäkerhetsmarknaden framåt. Det finns ett stort behov av kompetens på området, både vad gäller utbildningar inom området men också den interna kompetensen hos anställda på företag och myndigheter. Kompetensmässigt saknas det dels teknisk kompetens i form av ingenjörer men också inom andra yrken såsom statsvetare och jurister. Cybersäkerhet är ett brett område som sträcker sig utanför IT-avdelningar och rena teknikbolag och därför krävs också olika kompetenser i kombination med cybersäkerhet.

Det svenska samhällets allt högre grad av digitalisering skapar också en utmaning; behovet av att öka medvetenheten om cybersäkerhet hos befolkningen. Respondenterna i denna kartläggning lyfter genomgående människan som den största risken när det kommer till cybersäkerhet, liksom bristfälliga riskanalyser och bristande, kontinuerligt säkerhetsarbete. Därtill lyfts att utvecklingen av nya tekniker såsom AI och IoT skapar nya risker såväl som möjligheter. Kartläggningen visar att det finns en mängd utvecklingsområden liksom möjliga insatser inom området. Den höga grad av digitalisering som finns i Sverige ställer å ena sidan krav på att företag och individer är medvetna om cybersäkerhetsaspekter, men vår starka digitaliseringsförmåga skapar å andra sidan också förutsättningar för Sverige att bli en ledande cybersäkerhetsnation.

Kartläggningen är baserad på aktuell litteratur, rapporter från myndigheter, mediareportering samt semi-strukturerade intervjuer med erfarna personer med kunskaper inom olika områden kopplat till cybersäkerhet. Kartläggningen utfördes av Unitalent på uppdrag av Linköpings Science Park, Tillväxtverket och Security Link, en centrumbildning vid Linköpings universitet, KTH, Chalmers och FOI.



Inledning

Kartläggningen har genomförts av Unitalent på uppdrag av Linköping Science Park, Tillväxtverket och Security Link, en centrumbildning vid Linköpings universitet, KTH, Chalmers och FOI. Syftet med kartläggningen har varit att ge en bild av cybersäkerhetsområdet i Sverige. Vi har kartlagt befintliga företag, men också fördjupat oss i vilka förutsättningar de verkar under, hur marknaden förutspås växa samt vad det finns för befintlig kompetens samt existerande utbildningsprogram. Utifrån resultatet lyfter vi fram utmaningar och möjligheter för branschen, beskriver framtida marknadsutsikter samt ger förslag till kommande forskningsområden.

Cybersäkerhet är ett brett begrepp som kan innefatta många olika delar. En svårighet i att definiera marknaden för cybersäkerhet är att produkter som inte klassas som säkerhetsprodukter ändå har ett behov av cybersäkerhetslösningar. Det blir därmed svårt att till exempel avgränsa vilken typ av produkter som ska ingå i marknaden för cybersäkerhet.⁷ I den här kartläggningen kan cybersäkerhet sammanfattas som en del i informationssäkerhet som rör säkra processer och att skydda digital information från antagonistiska hot. Det handlar om att säkerställa att rätt information finns tillgänglig för rätt person vid rätt tillfälle, och att ingen annan har tillgång till informationen.

I och med den pågående digitaliseringen och teknikutvecklingen får cybersäkerhetsfrågor ett allt större fokus. Internationella såväl som nationella skandaler och cyberattacker där stora mängder data läcker ut eller stjäls bidrar också till att området får ökad uppmärksamhet. Respondenterna i kartläggningen lyfter att Sverige ligger långt fram vad gäller det digitala samhället, men att cybersäkerhetsfrågor ofta får för lite uppmärksamhet. Därtill finns det en naivitet på individnivå, bland annat kring vilken information vi väljer att dela med oss av när vi använder olika webbplatser, sociala medier och smarta produkter. Den höga graden av digitalisering gör vårt samhälle mer sårbart, men enligt respondenterna skapar detta också förutsättningar för Sverige att bli ledande inom cybersäkerhet på internationell nivå.

Inledning

År 2017 satte Sverige upp en digitaliseringsstrategi med målet att landet ska bli bäst i världen på att ta vara på digitaliseringens möjligheter. Målet består av fem områden, varav ett av delmålen handlar om digital trygghet; ”I Sverige ska det finnas de bästa förutsättningarna för alla att på ett säkert sätt ta del av, ta ansvar för samt ha tillit till det digitala samhället.”¹ Sverige ligger i framkant i flera mätningar vad gäller graden av digitalisering, och hamnar i toppskiktet i EU:s Digital Economy and Society Index² och på en första plats i Network Readiness Index.³ Sverige presterar dock desto sämre när det kommer till cybersäkerhet. Där hamnar landet på plats 32 i Global Cybersecurity Index (GCI), vilket kan jämföras mot Norge på plats 9, och Finland och Danmark på plats 19 respektive 21.⁴ I en rapport från PwC konstateras också att Sverige utsätts för flest cyberattacker i Norden där 8 av 10 företag i undersökningen uppger att de blivit utsatta för en attack.⁵ Som en möjlig förklaring till att Finland och Danmark är mindre utsatta lyfts att det finns ett mer väletablerat samarbete mellan näringsliv och myndigheter vad gäller cybersäkerhet i dessa länder. Rapporten lyfter också att Danmark redan har ett nationellt cybersäkerhetscenter på plats, något som ska inrättas i Sverige under 2020.⁶

Syfte och frågeställningar

Syftet med studien har varit att kartlägga nuläget och framtidsutsikter för cybersäkerhetsbranschen vad gäller utbildning, företag och kompetens inom området. Frågeställningar för att besvara syftet listas nedan.

► *Hur ser nuläget och framtidsutsikterna ut för cybersäkerhetsmarknaden?*

Cybersäkerhet är ett brett begrepp, kartläggningen syftar därför till att identifiera vilka områden som anses vara viktiga just nu och framöver. Därtill undersöks drivkrafter för cybersäkerhetsmarknaden, hur marknaden utvecklats historiskt samt hur den förutspås växa framöver.

► *Vilka utmaningar och möjligheter finns inom cybersäkerhetsbranschen kopplat till teknikområden, människans roll, nationell kompetens och samhällets digitalisering?*

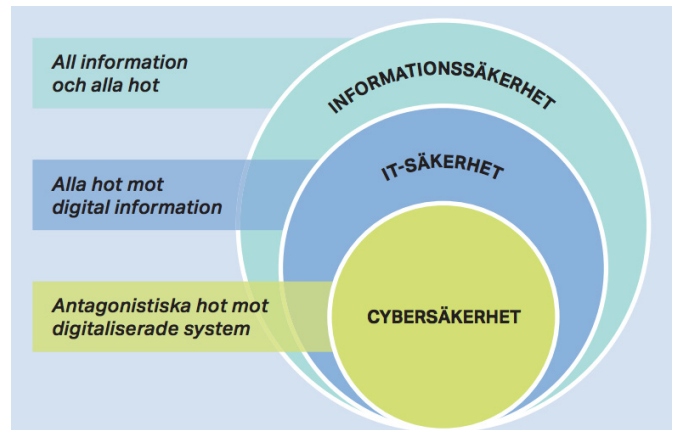
Den ökade digitaliseringsgraden i samhället skapar både utmaningar och möjligheter – dels här och nu, men även framöver. Frågeställningen syftar till att undersöka dessa kopplat till teknik, människa, kompetens och samhälle och om det finns några regionala skillnader.

► *Vilka företag, organisationer, utbildningar och aktörer finns inom cybersäkerhetsområdet i Sverige idag?*

I kartläggningen sammanfattas en mängd antal olika aktörer, företag, organisationer, myndigheter, utbildningar, projekt och initiativ på nationell såväl som regional nivå, med relevans för cybersäkerhetsområdet.

Avgränsningar

Kartläggningen är avgränsad till att undersöka den svenska marknaden för cybersäkerhet. Detta görs främst ur ett nationellt perspektiv, i viss mån sker även en internationell utblick. Begreppet cybersäkerhet är i vissa sammanhang synonymt med IT-säkerhet och informationssäkerhet, i den här rapporten särskiljs dock begreppen. Cybersäkerhet definieras som en delmängd av IT-säkerhet och informationssäkerhet, där det finns ett fokus på att skydda den digitala informationen i system och processer mot ett antagonistiskt hot.



Källa: Teknikföretagen 2020, <https://www.teknikforetagen.se/globalassets/i-debatten/publikationer/cybersakerhet/cyberhoten-mot-svenska-teknikforetag.pdf#page=Cyberhoten%20mot%20svenska%20teknik%C3%B6retag>

Vidare är cybersäkerhet något som berör många olika typer av verksamheter, med cybersäkerhetsmarknaden respektive cybersäkerhetsbranschen avses i det här fallet de företag och organisationer som arbetar direkt med frågor, produkter eller tjänster gällande cybersäkerhet.

Definitionslista

Myndigheter, institut och organisationer

- FMV - Försvarets materielverk
- FOI - Totalförsvarets forskningsinstitut
- FRA - Försvarets radioanstalt
- MSB - Myndigheten för samhällsskydd och beredskap
- PTS - Post- och telestyrelsen
- RISE - Research Institutes of Sweden
- SCB - Statistiska centralbyrån
- SOFF - Säkerhets- och försvarsföretagen
- Säpo - Säkerhetspolisen

Studiens genomförande

A hand holding a pen over a notepad, with a green overlay. The background is a blurred image of a desk with a notepad and a pen. The text "Studiens genomförande" is written in white, bold, sans-serif font, centered on the image.

Studiens genomförande

Studien har genomförts genom att intervjua personer i olika roller och organisationer med stor kunskap och i många fall lång erfarenhet av cybersäkerhet. Intervjuerna har kompletterats med tidigare rapporter och undersökningar på området cybersäkerhet.

Totalt intervjuades 18 personer och intervjuerna var mellan 30 och 60 minuter långa. Intervjuerna följde en semi-strukturerad form, där frågorna utgick från en gemensam intervjuguide men även anpassades beroende på respondentens roll och kunskaper. Respondenterna tillhör flera olika typer av företag, organisationer och myndigheter med koppling till cybersäkerhet och samtliga har lång erfarenhet inom området. Nedan redogörs för de som intervjuats för kartläggningen.

Metoddiskussion

Då syftet med studien har varit att kartlägga nuläget och framtidsutsikter för cybersäkerhet har stort fokus lagts på att intervjua personer med aktuell kunskap inom området. Det händer mycket vad gäller cybersäkerhet och material som tidigare publicerats blir utdaterat på bara några år, vilket gjorde intervjuerna viktiga för att fånga den aktuella bilden. För att intervjuerna skulle ge ett så omfattande och heltäckande underlag som möjligt har stor vikt lagts vid att få ett brett urval av personer för intervjuerna. Samtliga respondenter har omfattande kunskaper inom cybersäkerhetsområdet och många har arbetat med cybersäkerhetsfrågor i flera olika roller och sammanhang. Respondenterna kommer från olika organisationer, exempelvis myndigheter, universitet, cybersäkerhetsföretag eller projekt och andra initiativ rörande cybersäkerhet.

Namn	Roll och företag/organisation
Annika Avén	Ansvarig för Cyberförsvar på SOFF
Martin Bergling	Koordinator på RISE för den nationella innovationsnoden för cybersäkerhet
Rolf Blom	Senior forskare på RISE enhet för Cybersäkerhet
Simone Fischer-Hübner	Professor i datavetenskap på Karlstads universitet
Eva Fogelström	Head of Security Research på Ericsson
Jonas Hallberg	Enhetschef för informationssäkerhet och IT-arkitektur på FOI
Martin Hell	Universitetslektor vid Nätverk och säkerhet på Lunds tekniska högskola
Mårten Holmberg	Business Developer Digital på Blue Science Park
Åke Holmgren	Chef över avdelningen för Cybersäkerhet och säkra kommunikationer på MSB
Jonathan Jogenfors	Senior IT-säkerhetskonsult på Atea
Tore Johnsson	VD på Luleå Science Park
Christian Jonsson	Senior Director på Saab Cybersecurity
Andreas Karström	CTO på Link22
Torbjörn Kronander	VD på Sectra
Fredrik Landberg	VD på Sylog Öst
Lena Miranda	VD på Linköpings Science Park
Richard Oehme	Ordförande för SOFF:s cybergrupp
Andrei Sabelfeld	Professor i webb- och mjukvarusäkerhet på Chalmers
Ola Stensby	Programansvarig Security Arena vid Lindholmen Science Park

Resultat



Resultat

I följande avsnitt beskrivs nuläget för cybersäkerhetsbranschen, aktuella cyberhot, relevanta tekniker samt utbildning och forskning inom området. Avslutningsvis lyfts framtidsutsikter och faktorer som driver marknaden. Resultatet är sammanställt utifrån den litteratur som inhämtats och de intervjuer som genomförts.

Nuläge cybersäkerhetsbranschen

I följande avsnitt beskrivs nuläget för cybersäkerhetsbranschen globalt, nationellt samt regionalt.

Nuläge för cybersäkerhet globalt

Då cybersäkerhet är ett brett begrepp varierar marknadsstorleken beroende på vilka sektorer som inkluderas. Under 2018 estimerade *Markets and Markets* den globala cybersäkerhetsmarknaden till cirka 153 miljarder USD under 2018, och att detta skulle öka till nära 249 miljarder under 2023. Detta motsvarar en årlig tillväxt på 10,2%.⁸ Detta kan jämföras med siffror från Fortune Business Insight som estimerade den globala cybersäkerhetsmarknaden till ungefär 112 miljarder USD under 2019, och att detta skulle öka till närmare 282 miljarder USD till 2027, vilket motsvarar en årlig tillväxt på 12,6%.⁹

I takt med att världen blir alltmer digitaliserad och uppkopplad får också frågor som rör cybersäkerhet ett allt större fokus. Flera respondenter lyfter att det höga internationella tonläget, pågående handelskrig och andra internationella spänningar gör det ännu viktigare att företag investerar i cybersäkerhet. De cyberattacker som utförs blir allt mer riktade och metoderna mer sofistikerade. Även pandemin i och med Covid-19 har gjort att cybersäkerhet fått ett ökat fokus internationellt. Andrei Sabelfeld, professor i webb- och mjukvarusäkerhet på Chalmers, lyfter bland annat att antalet nätattacker ökat i spåren av pandemin. KPMG rapporterar om en ökning av antalet phishing-mail till bankkunder¹⁰ och MSB anser att det finns ett förhöjt hot i att sjukhus blir utsatta för cyberangrepp.¹¹ Mårten Holmberg, Business Developer Digital på Blue Science Park, beskriver hur digitaliseringen har accelererat till följd av Covid-19 och att detta även öppnar för nya säkerhetshål, till exempel när serveråtkomst flyttas ut till en hemmiljö.

FN konstaterade under 2018 att det fanns ett problem i hur organisationen ska arbeta med frågor relaterat till cybersäkerhet. Bland annat lyfts problematiken i att skapa en gemensam syn mellan stater i hur frågan ska hanteras.¹² Samtidigt listas cyberattacker som en av de största, globala riskerna, där både konsekvens och sannolikhet för att det skulle inträffa anses vara hög. Det finns många olika typer av cyberattacker, från spridning av desinformation till intrång i känslig infrastruktur. Cyberattacker där målet är att stjäla data eller pengar eller att på något sätt störa olika typer av infrastruktur var problemområden som förutsågs växa under 2019.¹³ Under 2018 uppskattades kostnaden globalt för cyberattacker till så mycket som 600 miljarder USD. Banker och andra finansiella institutioner lyftes som den mest attraktiva sektorn att angripa. Länder som pekas ut som huvudaktörer för dessa attacker är Ryssland, Iran och Nordkorea. Kina står också för en stor del cyberattacker, men är mer inriktat på olika typer av spionageverksamhet.¹⁴ FBI uppskattade kostnaden för cyberattacker i USA till 3,5 miljarder USD under 2019. Länder som lyfts fram som utsatta för cyberattacker, oavsett art, är bland annat Storbritannien, Kanada och Indien.¹⁵

Nuläge för cybersäkerhet i Sverige

Sverige upprättade en digitaliseringsstrategi och ett digitaliseringsråd redan 2017, men det var först under 2019 som det beslutades att det skulle inrättas ett nationellt cybersäkerhetscenter. Centret ska vara på plats under 2020 och ansvariga myndigheter för centret är Försvarets Radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap och Säkerhetspolisen. Syftet med cybersäkerhetscentret är att stärka Sveriges förmåga vad gäller cybersäkerhet och att förhindra och hantera antagonistiska hot. Centret ska också kunna erbjuda stöd och rådgivning till både offentlig och privat sektor.¹⁶ Åke Holmgren, Chef för avdelningen för cybersäkerhet och säkra kommunikationer på MSB, lyfter att det finns ett behov av arbeta närmare mellan myndigheter för att kunna vara väl förberedda om det skulle inträffa ett större cyberangrepp. Han menar vidare att det finns ett värde av att det är många myndigheter som är delaktiga i ett cybersäkerhetscenter. Cybersäkerhet innefattar många områden och berör därför flertalet olika myndigheters verksamhet, både

grundläggande säkerhetsfunktioner som militär och polis, men även viktig infrastruktur som till exempel svenska kraftnät. Genom en ökad samverkan istället för att centralisera frågan under en myndighet ser Åke fördelar i dels en bredare kompetens ute hos myndigheter och även möjligheter att samordna resurser och kompetens.

Sverige ligger långt framme vad gäller digitalisering enligt respondenterna, något som skapar möjligheter men också utmaningar kopplat till cybersäkerhet. Under senare år har det skett flera stora skandaler, bland annat informationsläckorna från Transportstyrelsen 2017¹⁷ och 1177 Vårdguiden under 2019¹⁸, vilket gett cybersäkerhetsfrågor större uppmärksamhet. Christian Jonsson, Senior Director på Saab Cybersecurity, lyfter också att det är enkelt att exportera kompetens kopplat till cybersäkerhet, samt att den svenska kronan är låg och företag väljer därför att sälja sina lösningar utanför Sveriges gränser. Jonas Hallberg, enhetschef för informationssäkerhet och IT-arkitektur på FOI, poängterar också att flera av de största aktörerna som är duktiga på cybersäkerhet i Sverige inte är rena cybersäkerhetsbolag, till exempel Google och Microsoft. Martin Hell, universitetslektor vid Nätverk och säkerhet på Lunds tekniska högskola, lyfter också detta och konstaterar att mycket kompetens finns inom företag där det finns höga krav på säkerhet, och att det kan vara i dessa icke-cybersäkerhetsföretag som den bästa kompetensen finns.

Det pågår flera nationella satsningar, utöver cybersäkerhetscentret. Bland annat upprättar RISE en cyber range i Kista som ska användas för utbildning och tester inom cybersäkerhet¹⁹, och FOI har sedan tidigare en cyber range i Linköping med samma syfte.²⁰ Det finns också flera branschorganisationer som arbetar aktivt med att driva cybersäkerhetsfrågor framåt, såsom SOFF och Teknikföretagen, genom att bland annat publicera rapporter och undersökningar inom området cybersäkerhet.^{21,22} Mårten Holmberg lyfter att arbetet med cybersäkerhet tidigare har varit en reaktiv process, men att trenden går mot att cybersäkerhet inkluderas i arbetet från början. Han liknar det vid kvalité, som gått från att vara en separat del till att vara en faktor som genomsyrar hela verksamheten, och menar att samma sak kommer att ske för cybersäkerhet.

Regionala skillnader i Sverige

De regionala skillnaderna vad gäller kompetens och fokusområden inom cybersäkerhet beror till stor del på vilket universitet och vilka stora företag som finns i regionen. Nedan redogörs för viktiga aktörer, initiativ och forskningsområden för de olika regioner som ingår i Sweden ICT, ett samarbete mellan sex Science Parks runtom i Sverige.

Göteborg, Västra Götaland - Lindholmen Science Park

Göteborg och Västsverige är generellt sett industri- och fordonstungt, vilket också innebär att det sker mycket arbete på cybersäkerhet inom dessa sektorer. Stora aktörer inkluderar Volvo, SKF, Ericsson, AstraZeneca och även Chalmers och RISE.

Karlskrona, Blekinge - Blue Science park

Blekinge tekniska högskola är det enda universitet i Sverige som har en civilingenjörsutbildning inom datorsäkerhet. Det finns också en nisch inom AI, IoT och cybersäkerhet enligt Mårten Holmberg, och därför bör ett kommande fokusområde bli att se hur dessa områden korsar varandra. Stora aktörer inkluderar Försvarmaktens marinbas, Ericsson och Saab Kockums. I regionen finns därmed såväl stora behovsägare såsom Försvaret och Saab, och även lösningsägare som exempelvis Ericsson, där vissa av dessa aktörer är både behovs- och lösningsägare.

Kista, Stockholm - Kista Science City

Det finns ett kluster och en bredd av företag som arbetar med cybersäkerhet i Kista, bland annat Ericsson, Tele2, IBM, Atea och FOI. RISE har också ett pågående arbete med att upprätta en cyberanläggning i Kista där det ska bedrivas forskning, utbildning och tester kopplat till cybersäkerhetsfrågor. På Stockholms Universitet och Kungliga Tekniska Högskolan finns också en bredd vad gäller cybersäkerhet, både tekniska utbildningar men också inom tvärvetenskapliga områden.

Linköping, Östergötland - Linköpings Science Park

Historiskt sett har Linköping varit starka inom olika områden inom cybersäkerhet och Linköpings Universitet har länge haft en spets inom området. Exempelvis finns en kompetensspets inom kryptografi i Linköping, enligt Fredrik Landberg,

VD på Sylog Öst. Stora företag som Sectra, Saab och Ericsson har länge funnits i regionen och idag finns det också flera andra stora företag som arbetar med cybersäkerhet, bland annat Cybercom, Atea och Combitech. Flera myndigheter är placerade i regionen, bland annat Transportstyrelsen, Sjöfartsverket, Luftfartsverket och VTI. FOI har en forskargrupp och sin cyberanläggning, CRATE, placerad i Linköping.

Luleå, Norrbotten - Luleå Science Park

Facebook är en stor aktör i Luleå där de har sina serverhallar. Flera myndigheter har även sina IT-avdelningar i Luleå, bland annat Försäkringskassan och Tullverket. Vid Luleå tekniska universitet finns kompetens inom cybersäkerhet och det finns också flera små företag i regionen som jobbar inom området, enligt Tore Johnsson, VD på Luleå Science Park. Han lyfter vidare att Luleå Science Park även bedriver, tillsammans med andra Science Parks i Sverige, ett arbete för att försöka skapa ett ekosystem mellan universitet, näringsliv och offentlig sektor.

Lund, Skåne - Ideon Science Park

Stora aktörer inkluderar Axis Communications, Alfa Laval, Tetra Pak och Sony, som även har sitt globala forsknings- och utvecklingscentrum i Lund. På Lunds tekniska högskola bedrivs också forskning kopplat till cybersäkerhet, bland annat inom kryptoteknik och mjukvarusäkerhet.

Cyberhot och cyberangrepp

I och med den breda definitionen av cybersäkerhet innebär begreppet många olika typer av hot. Dessa är delvis tekniska, men angreppen riktas också mot människan. I en internationell rapport från Accenture med över 350 deltagande företag lyfts informationsstöld som det vanligaste cyberhotet under 2019. I rapporten konstaterades också ett växande hot i att data ändras eller förstörs vid ett intrång, där målet inte alltid behövde vara att stjäla något. Den årliga kostnaden per företag till följd av cyberattacker uppskattades i genomsnitt till cirka 13 miljoner USD under 2018, vilket motsvarade en ökning på 72% sedan 2013.²³ Teknikföretagen uppskattade i en rapport från 2019 kostnaden för svenska företag till 16 miljarder SEK om året, och att det främst är forskningsintensiva företag som drabbas.²⁴

Globala trender inom cyberhot under 2020 förutspås bland annat vara att cyberattacker mot kritisk infrastruktur ökar och att cyberkriminella utnyttjar leveranskedjor i större utsträckning, till exempel genom att placera skadlig kod hos en underleverantör. Cyberhoten ökar också i och med ett ökat distansarbete, vilket ställer nya krav på organisationer. Här finns risker kopplade till bland annat vilka nätverk som anställda använder sig av utanför arbetsplatsen, och att cyberkriminella utnyttjar säkerhetsbrister i dessa nätverk för att därefter kunna ta sig in i företagssystem. Förekomsten av deep fake förutspås också bli vanligare och det uppstår även andra typer av cyberhot i samband med utvecklingen av existerande och nya tekniker, såsom AI, 5G och IoT.²⁵

I takt med att världen digitaliseras och kopplas upp ökar antalet cyberkriminella såväl som deras förmåga. Andrei Sabelfeld säger att den ökade uppkopplingen har höjt incitamenten för cyberkriminella, och att det därför har utvecklats en svart marknad under de senaste 10 åren. Enligt Jonas Hallberg blir attackerna alltmer riktade och företag förstår inte alltid hur sårbara de är. PwC skriver i en rapport att andelen svenska företag som ser den organiserade brottsligheten som det största cyberhotet ökade från 40% under 2019 till 51% år 2020.²⁶ Fredrik Landberg säger också att det finns en problematik i att alla IT-incidenter inte rapporteras, utan att företag väljer att lösa problemen i tysthet. Detta beskrivs även i en rapport från FOI, och anledningen till mörkertalet uppges vara en oro för att det skulle skada företagets rykte och verksamhet. Rapporten lyfter också problemet avseende att många företag förblir ovetandes om att de har utsatts för ett angrepp.²⁷

Polismyndigheten anser att en allt större mängd av den allvarliga, organiserade brottsligheten kan kopplas till IT-aspekter. Crime-as-a-service, vilket innebär att kriminella säljer olika typer av cyberangreppsverktyg och liknande, är något som anses vara en bidragande faktor till den här ökningen eftersom kriminella inte längre själva behöver ha kompetensen för att genomföra ett cyberangrepp.²⁸ Under 2019 uppgavs olika typer av skadlig programkod, till exempel virus, vara det vanligaste cyberangreppet på svenska teknikföretag och nära hälften av alla teknikföretag uppgav att de blivit utsatta för ett cyberangrepp. För resterande sektorer var siffran 25%.²⁹

Ransomware är ett typ av säkerhetsangrepp som har ökat de senaste åren. Ransomware innebär ett cyberintrång i ett IT-system där angriparna på något sätt har låst systemet eller kommit över känslig information och kräver en lösensumma för att låsa upp eller återlämna informationen. Även om volymen av attacker uppges ha minskat något har den ekonomiska lönsamheten för ransomware gått upp och anses vara en enkel inkomst för cyberkriminella.³⁰ Ransomware drabbar såväl den privata sektorn som den offentliga. MSB ser en ökad risk för angrepp på bland annat sjukhus i spåren av Covid-19, något som redan skett runt om i Europa. Detta beror bland annat på att medicinska data är värdefull i utpressningssyfte.³¹ Andrei Sabelfeld ser att ransomware kommer att bli ett växande problem framöver, bland annat i och med utvecklingen av AI, då detta öppnar upp nya möjligheter för antagonist.

Spionage

Enligt en rapport av de myndigheter som ska ansvara för cybersäkerhetscentret är cyberhoten som riktas mot Sverige mångfacetterade, och angriparna är både kriminella och statliga aktörer.³² Säkerhetspolisen lyfter i sin årsbok att spionage från andra länder mot Sverige har ökat, och den information som inhämtas olovligt kan värderas till miljardbelopp. Bland annat lyfts att intresset från Kina har ökat eftersom Kina vill åt kunskap, teknologier och innovation som finns i Sverige, något som det används både lagliga och olagliga metoder för att uppnå. Det kan vara genom strategiska uppköp, där uppköpta företag måste dela med sig av företagsinformation till den kinesiska militären, eller genom spionageverksamhet.³³ I en rapport från FOI om Kinas industriella cyberspionage konstateras att svenska myndigheter och företag är attraktiva måltavlor, vilket på sikt kan innebära utmaningar för svensk konkurrenskraft.³⁴

Människan som riskfaktor

I en rapport bland Teknikföretagens medlemmar uppgav 25% av företagen återkommande problem med att anställda kringgår cybersäkerhetsföreskrifter i arbetet, såsom att dela lösenord eller använda egen IT-utrustning.³⁵ Phishing, även kallat lösenordsfiske, är även det vanligast förekommande cyberangreppet mot svenska företag, enligt en rapport från PwC.³⁶ Flera respondenter lyfter också människan som den största risken när det handlar om cybersäkerhet.

Tekniker

Cybersäkerhet berör en mängd olika teknikområden. Nedan beskrivs hur cybersäkerhet kopplar till några av dessa tekniker samt vilka möjligheter och utmaningar dessa områden innebär. Teknikerna som lyfts är de som respondenterna har lyft fram som särskilt viktiga för cybersäkerhetsområdet.

Kryptering

Tack vare en hög kompetens hos företag och myndigheter är Sverige idag en ledande kryptonation. Den nationella kompetensen bidrar till ett säkerhetspolitiskt mervärde och gör att Sverige inte är beroende av utländska aktörer inom området. I och med utvecklingen i omvärlden finns idag ett ökat behov av denna typ av skydd. För att kunna fortsätta utvecklas inom området är det viktigt att tillväxtfrämjande åtgärder beaktas.³⁷ *Utgiftsområde 6 – Försvar och samhällets krisberedskap* i 2018 års budgetproposition belyser vikten av att ha tillgång till inhemsk teknisk kompetens. Framför allt i en konflikt med en kvalificerad motståndare. Vid höjd beredskap kan det vara problematiskt med tillgång till relevant kompetens från utländska aktörer och det är därför av stor vikt att säkerställa att denna kompetens finns i Sverige. Att vara självständig inom vissa områden i förhållande till andra stater är väsentligt och krypto bedöms av regeringen som ett av dessa områden.³⁸

Andreas Karström, CTO på Link22, beskriver att Sverige ligger långt framme när det gäller krypto och att det finns en spets som är viktig att bevara. Även Christian Jonsson lyfter att Sverige har en kompetens inom krypto som är viktig att behålla inom landet. Åke Holmgren beskriver att Sverige är unika i att ha en så avancerad kryptoindustri i relation till landets storlek.

Regeringen har angett att tillgången till nationellt godkända kryptosystem kan vara ett centralt säkerhetsintresse, något som även SOFF lyfter. De ser också att företagen i Sverige här spelar en viktig roll och bör ingå som sakkunniga, utöver centrala myndigheter. Enligt SOFF finns ett behov av forskning, utveckling, innovationsprogram och marknadsfrämjande åtgärder för att utvecklas på området, men också ett behov av att utveckla den svenska industrin inom säkerhet i stort. Arbetet med

kryptografiska funktioner är en del i att skapa ett samlat totalförsvaret. Enligt SOFF prioriteras budget, resurser och ansvar olika i den militära och civila sektorn, där den militära får större del. För att lyckas skapa ett starkt totalförsvaret behövs ett större fokus på den civila sidan.³⁹

I den samlade informations- och cybersäkerhets-handlingsplanen för åren 2019–2022 som publicerats av MSB anges ett antal strategiska prioriteringar inom ramen för den nationella strategin. De innefattar olika typer av målsättningar för informations- och cybersäkerhet i samhället. En av målsättningarna är att tillgången till säkra kryptosystem för IT- och kommunikationslösningar ska motsvara behoven i samhället. Inom denna målsättning ryms en rad åtgärder, vilket är ytterligare ett belegg för vikten av att vi i Sverige kan säkerställa tillgång till kompetens och företag som är framstående inom området.⁴⁰ Sectra är exempel på ett företag som levererar några av de mest hemliga och säkra krypteringarna som Sverige har. Torbjörn Kronander, VD för Sectra, nämner bland annat forskning inom krypto som särskilt viktig framöver. Det finns ett behov av att kryptering utvecklas som forskningsområde. Även Andrei Sabelfeld nämner kompetens inom krypto som särskilt viktigt. Han talar också om möjligheterna han ser inom cybersäkerhet och lyfter tillämpad kryptoteknik (applied crypto) som ett intressant område under utveckling. Denna typ av teknik har bland annat använts under coronapandemin för att ta reda på var personer befinner sig. Det finns mycket som pekar på att krypto är ett viktigt område där det framöver kommer krävas mycket kompetens, nya innovationer, mer forskning och likaså företag som kan utveckla tekniken.

Internet of Things

Ett annat teknikområde som är tätt sammankopplat med cybersäkerhet och som skapar såväl nya möjligheter som utmaningar är IoT, Internet of Things. Begreppet används för att beskriva, både privata och industriella, föremål som utrustas med möjligheten att anslutas till internet. Exempel på IoT-produkter är självkörande bilar, tillämpningar inom sjukvården eller kommunicerande kylskåp. Det verkar knappt finnas några gränser för sammanhang och områden där IoT kan appliceras och ett samlingsnamn för föremålen är "smarta föremål". Säkerheten för IoT-föremål är generellt sett låg och har sällan tillräckligt skydd mot åtkomst och användande av obehöriga. Dessutom

finns drivkrafter på marknaden som stimulerar stora försäljningsvolymerna av IoT-enheter med låga anskaffningskostnader, vilket bidrar till ytterligare svårigheter att skapa säkra produkter.⁴¹ Martin Bergling, koordinator på RISE för den nationella innovationsnoden för cybersäkerhet, beskriver också dessa problem och säger att tillverkarna av IoT-enheter inte i första hand tänker på säkerhet, utan på att snabbt få ut produkter på marknaden, ibland med enklast möjliga kod. Något som skapar en stor angreppsytta för de som vill göra skada.

Säkerhetsutmaningarna kopplade till IoT är många och det kommer behövas stora resurser i framtiden enligt Martin Bergling. Han anser att det idag finns en stor oförståelse kring alla de risker som kan uppstå när allt fler enheter kopplas upp. Antalet uppkopplade enheter är redan stort och förväntas växa snabbt de kommande åren, något som också innebär fler och större risker. Ett annat säkerhetsproblem inom IoT är att många enheter drivs på batteri, vilket innebär en begränsad tillgång på ström. Det i sin tur bidrar till svårigheter att tillämpa bra säkerhetslösningar som också är integritetsskyddande. Ofta finns det bara utrymme att använda enkla algoritmer för att få en förbättrad säkerhet eftersom elförbrukning och beräkningskraft behöver balanseras. Det krävs således en utveckling av dagens IoT-produkter för att de ska hålla en tillräckligt hög säkerhetsnivå.⁴²

Hur denna utveckling ska ske är en naturlig följdfråga. Andrei Sabelfeld säger att den största utmaningen är att lyckas skapa en långsiktig syn på säkerhet, där säkerhet inkluderas redan vid designstadiet, även kallat *security by design* eller *security by construction*. Amerikanska Department of Homeland Security har tagit fram ett antal grundläggande principer för säkerhetsarbete inom IoT, där *security by design* ingår som en av dessa.⁴³ Det är dock en utmaning för många tillverkare att inkludera ett gediget säkerhetsarbete, då många företag är små och inte har samma resurser att lägga på kvalitetssäkring som stora företag. Ett exempel på en säkerhetsåtgärd som en leverantör ibland hoppar över på grund av begränsade resurser är att felsöka mjukvara innan den lanseras på marknaden.⁴⁴

Inom IoT finns också utmaningar när det gäller att skydda människors integritet. Den mängd data som samlas in är stor och växer ständigt. Många personer anser sig inte ha någon känslig information om sig själva men när stora mängder data finns att tillgå från en stor mängd människor, exempelvis

ett helt samhälle, kan det leda till problem på en samhällsövergripande nivå. Detta drabbar också mer eller mindre alla personer i ett samhälle. Det finns alltså höga risker när stora mängder data kan analyseras och kombineras på olika vis. Skyddandet av människors integritet är också problematiskt när det kommer till IoT-enheter som kan användas för avlyssning, exempelvis smartphones, datorer, smarta klockor och trådlösa headsets. Det är inte enbart information om individer som kan hamna i fel händer, även företag och myndigheter kan utsättas för spionage eftersom verksamheter idag i stor utsträckning använder sig av olika typer av IoT-enheter.⁴⁵ Simone Fischer-Hübner, professor i datavetenskap vid Karlstads universitet, ser ett behov av forskning inom dessa utmaningar för IoT. Hon nämner att det finns känsliga data, att det ofta är enkelt att hacka enheterna och att det finns problem med avlyssning. De etiska aspekterna går inte heller att blunda för enligt Simone som ser att även diskrimineringsproblem kan uppkomma som följd. Det är därför av stor vikt att vi lyckas hänga med i den tekniska utvecklingen och att säkerheten inom IoT inte hamnar på efterkälken, anser hon.

Idag bedrivs forskning inom IoT för att ta reda på hur sårbara olika typer av enheter är. Exempelvis har forskare lyckats ta sig in i en app som kommunicerar med en bil, för att sedan lokalisera den och slutligen låsa upp och fjärrstarta bilen. Vid försök på just bilar har forskare även kunnat installera skadlig kod på en enhet kopplad till en bils interna nätverk för att senare kunna stänga av bilens motor under körning. Det kan orsaka förödande konsekvenser och det finns fler exempel på hur vi människor kan drabbas på sätt som hotar liv på individnivå, bland annat inom sjukvården. Pacemakers och pumpar för att dosera medicin är två typer av sjukvårdsutrustning som visat sig vara sårbara för angrepp.⁴⁶ Andrei Sabelfeld betonar vikten av forskning inom detta område och ser ett fortsatt stort behov i framtiden eftersom vi litar allt mer på IoT-enheter. Mårten Holmberg lyfter att framtida forskning inom cybersäkerhet behöver korsas med olika teknikområden och ser just korsningen mellan cybersäkerhet och IoT som ett viktigt område framöver.

Som nämndes ovan kan problemen även uppstå på samhällsnivå. En attack mot ett hushålls kylskåp drabbar specifikt det hushållet hårt, men märks inte av på samhällsnivå. Om däremot en attack kan genomföras mot alla kylskåp i ett helt samhälle, exempelvis mitt i sommaren, kan konsekvenserna

snabbt bli allvarliga och omfattande.⁴⁷ Det finns följaktligen stora risker kopplade till samhällsviktiga funktioner. I Linköping bedrivs klustret IoT World, som valt att fokusera på lösningar för samhällslogistik av olika slag, berättar Lena Miranda, VD för Linköping Science Park. Det kan handla om hur vi optimerar produktion av fjärrvärme i våra nät, hur vi optimerar kollektivtrafiken för att få bäst resurseffektivitet – eller hur vi säkerställer bevisföring från brottsplats till domstol med hjälp av digitala teknologier. I samtliga fall är säkerhetsaspekterna oerhört viktiga, och kommer öka i takt med att vi kopplar på AI i nästa steg. Rolf Blom, Senior forskare på RISE enhet för Cybersäkerhet, berättar att de har stort fokus på IoT och arbetar med att hjälpa svensk industri på att bli duktiga på säkerhet inom området. Det är givetvis viktigt att innovationerna inom IoT går framåt, men vi får inte missa att ta hänsyn till säkerhet när tekniken utvecklas, enligt Rolf Blom.

FOI har på uppdrag av MSB tagit fram ett antal strategier för att hantera olika IoT-relaterade risker och uppmärksamma säkerhetsarbetet. En stor del av säkerhetsproblematiken kring IoT idag ligger i att det är oklart vem som ska ta ansvar för säkerhetsåtgärder när en ny produkt tas fram. Ofta är flera olika företag inblandade vid en sådan process, ett företag står för mjukvaran, ett annat för utformningen av produkten, ett tredje hanterar nätverket enheten ska kopplas in i och ett sista företag sätter produkten i drift. Eftersom industrin inom IoT ofta ser ut på detta sätt kan vägledande strategier vara en stor hjälp för företag för att lyckas få med säkerhetsarbete i utvecklingsprocessen. Även amerikanska Department of Homeland Security vill bygga upp en medvetenhet kring riskerna med IoT hos olika aktörer och ser dessutom ett behov av internationella standarder. De vill arbeta ihop med andra myndigheter och aktörer inom industrin för att förbättra säkerheten inom området, det är då viktigt att vi ser till att Sverige är en del av detta.⁴⁸

Artificiell intelligens

AI, eller artificiell intelligens innebär användningen av digital teknik för att skapa system som klarar av att utföra uppgifter som vanligtvis kräver intelligens. ML, machine learning, är ett närliggande begrepp som ibland definieras som ett område inom AI och ibland som ett helt eget teknikområde. Som eget teknikområde innebär ML att utveckla digitala system som förbättrar utförandet på en specifik uppgift över tid, genom att systemen skaffar sig

erfarenhet. AI och ML har utvecklats snabbt de senaste åren och utvecklingen har möjliggjort att vi idag har tillgång till fördelaktiga applikationer och digitala funktioner. Bland annat självkörande bilar, digitala assistenter för personal inom sjukvård, samt olika typer av användningsområden för drönare såsom snabbare hjälp till katastrofdrabbade områden. I framtiden tros AI vara något som dessutom kan påskynda vetenskaplig forskning och bidra till bättre styrning av världens länder.

Den snabba utvecklingen gör också att det är viktigt att uppmärksamma de utmaningar som AI innebär och de sammanhang där AI kan användas på ett skadligt sätt. I februari 2018 samlades 26 forskare från flera ledande universitet i Oxford för att titta djupare på de risker som finns om AI hamnar i fel händer. I deras rapport beskriver de hur illvillig användning av AI innebär risker för både medborgare, organisationer och stater och hur denna användning kan hota både digital, fysisk och politisk säkerhet. Åtgärder som behövs inom digital säkerhet kan exempelvis handla om att hindra personer från att lära maskiner att hacka olika typer av system. Inom fysisk säkerhet kan det istället handla om att förhindra att personer lyckas göra om vanliga drönare till vapen. Ett exempel inom politisk säkerhet är att se till att inga automatiserade och riktade kampanjer förekommer.⁴⁹

I rapporten föreslår forskarna bättre metoder för att förutse, förebygga och hantera den typ av säkerhetshot som kan uppkomma när illvilliga aktörer använder sig av AI-teknik för att skada andra. Forskarna presenterar fyra övergripande rekommendationer för att möta de hot som kan uppstå av oreglerad AI⁵⁰:

- Lagstiftare och tekniska forskare bör ha ett nära samarbete för att kunna undersöka, förebygga och mildra potentiella skadliga användningar av AI.
- Forskare och ingenjörer inom AI ska ta hänsyn till att deras arbete kan användas på både goda och onda sätt och vid risk för det sistnämnda vidta förebyggande åtgärder genom att ta kontakt med relevanta aktörer när skadliga tillämpningar kan förutses, samt låta identifierade risker vägleda forskningsprioriteringar.
- Använd "best practice"-metoder från exempelvis datasäkerhet eller annat välbeprövat forskningsområde och applicera på forskning inom AI där detta är möjligt.

- Försök att aktivt utöka antalet experter och intressenter som deltar i diskussioner kring de säkerhetsutmaningar som finns inom AI.

Den andra rekommendationen är något som Rolf Blom återkopplar till, vilket är att det finns en stor utmaning i att AI kan användas både på gott och ont. Han berättar hur det går att lura algoritmer genom att träna dem med felaktiga data och att de bland annat kan klara av att upptäcka saker de inte ska upptäcka. Vidare beskriver Martin Bergling hur en framtida självförbättrande AI-enhet på bara några timmar kan bli så smart att den blir farlig. Tore Johnsson anser att AI-kompetensen är en typ av kompetens som kommer vara särskilt viktig framöver och också en kunskap som ska bevaras inom Sverige, där vi behöver sticka ut och ha spetskompetens. Tore och hans kollegor på Luleå Science Park tror att en viktig del i att lyckas med detta är att driva långsiktiga projekt inom AI och de agerar idag som katalysator och projektledare i flera AI-projekt. Även Eva Fogelström säger att AI-kompetens är av stor vikt och ser användning av AI och ML samt skyddandet av AI-modeller som viktiga framtida forskningsområden.

I Sverige arbetar just nu SCB på uppdrag av regeringen med att kartlägga och definiera användningen av artificiell intelligens, samt kartlägga hur stora datamängder analyseras i företag och offentlig förvaltning, inklusive universitets- och högskolesektorn i Sverige. Kartläggningen ska generera ett brett statistiskt underlag och belysa variation i användning av AI mellan olika branscher och sektorer samt de faktorer som påverkar användningen. Idag finns ingen sådan statistik vilket gör att kunskap saknas om var insatser kan behövas för att stärka användningen av AI och därmed också den svenska konkurrenskraften.

Regeringen har som mål att Sverige ska vara ledande i att tillvarata de möjligheter som användning av AI kan ge och på så sätt stärka den svenska konkurrenskraften och välfärdssamhället i Sverige. Den 9 maj 2018 beslutade regeringen en nationell inriktning för AI i Sverige. Inom denna inriktning sammanfattas det gemensamma arbete som behöver ske i Sverige för att förverkliga den potential som AI erbjuder, både inom näringsliv och offentlig sektor. För att AI ska kunna skapa värde krävs det att tekniken kommer till bred användning och då behöver det i alla branscher finnas möjlighet att utveckla sin konkurrenskraft med hjälp av AI. Det

ligger i Sveriges intresse att stimulera användning av AI och säkerställa en god innovationsförmåga där nya innovationer tillämpas av företag och andra aktörer.⁵¹ En åtgärd som redan gjorts är att starta noden AI Innovation of Sweden som koordineras av Lindholmen Science Park på uppdrag av Vinnova. Ett flertal regionala noder har också bildats och noderna i Luleå, Kista och Linköping koordineras av respektive stads Science Park. Det ger dessa noder en god regional förankring, säger Lena Miranda, liksom en bra överhörning vad gäller korsbefruktning med andra innovationsinitiativ inom bland annat IoT, samt visualisering och bildanalys, framhåller hon.

AI kan också användas som ett hjälpmedel för att skapa säkerhet, exempelvis för att stoppa attacker och intrångsförsök, genom att säkerhetssystem lär sig att själva känna igen dessa typer av aktiviteter. Det är betydligt mer effektivt än att människor ska lyckas förutspå alla tänkbara risker.⁵² AI kommer troligtvis vara viktigt i framtidens säkerhetssystem och klara av att upptäcka avvikelser från normalt beteende och kunna agera vid undantag.⁵³

Tekniker under utveckling

Det finns tekniker som idag är under utveckling som på flera sätt kan förändra hur vi människor lever och vad vi klarar av att utföra framöver, bland annat kvantinformatik och 5G. Som med de andra områdena finns inte bara möjligheter utan också utmaningar och det finns en tydlig koppling till cybersäkerhet. Nedan beskrivs dessa två teknikområden och deras utmaningar närmare.

Kvantdatorer

Kvantinformatik är ett tvärvetenskapligt ämne där kvantfysik möter informationsteori. Inom kvantinformatik finns olika delar, de relevanta i detta sammanhang är kvantdatorn och kvantkryptografi. Dessa kan i framtiden påverka vårt samhälle, försvar och vår säkerhet. Kvantdatorn är en dator som klarar av att lösa problem genom att utnyttja nya typer av beräkningsmöjligheter, som inte går att göra med en klassisk datorarkitektur. Med hjälp av en kvantdator förväntas vi bland annat kunna göra avancerade sökningar i stora databaser och försvaga eller helt bryta dagens populära krypteringsmetoder. Det sistnämnda är något som är mycket omtalat eftersom det skulle innebära en stor påverkan på internetsäkerheten.⁵⁴ Om kvantdatorer börjar komma i bruk kommer de datorer vi använder idag att knäckas, vilket innebär en rad nya utmaningar,

berättar Rolf Blom. Även Jonas Hallberg ser utmaningar som användning av kvantdatorer på bred front kommer att skapa och nämner kryptering som en av de största utmaningarna. Attacker från kvantdatorer kommer kunna förstöra mycket och när det gäller just kryptering är det viktigt att vi klarar av att skydda oss mot den typen av hot, menar Jonathan Jogenfors, senior IT-säkerhetskonsult på Atea. För att klara av att möta utmaningarna är forskning en viktig del. SOFF ser att forskning inom kvantdatorer behöver påbörjas tidigt för att kunna arbeta med metodutveckling och ha tillgång till kompetens inom kvantsäkra metoder. Genom att tidigt bli duktiga på området kan vi exempelvis hindra främmande statsmakter från att dekryptera skyddsvärd information.⁵⁵ Även Torbjörn Kronander nämner just kvantdatorer som ett centralt forskningsområde framöver och arbetet i Sverige har redan påbörjats.

Under ledning av Chalmers inleds nu en svensk forskningssatsning inom kvantteknologi, Wallenberg Centre for Quantum Technology. Det är en satsning med en total budget på närmare en miljard kronor och mål att göra Sverige världsledande inom kvantteknologi. Det är ett tioårigt forskningsprogram där runt 40 forskare kommer att delta. Att vara ledande inom ett område som kvantteknologi bidrar till att Sverige kan fortsätta vara den toppnation inom teknik som vi är idag. I forskningsprogrammet ligger fokus på att attrahera de bästa unga forskarna och främja långsiktig kompetensbyggnad. Genom att jobba på detta sätt är förhoppningen att Sverige ska hamna på kvantteknologikartan.⁵⁶

5G

Även 5G är en teknik under utveckling som har potential att på ett omfattande sätt förändra våra samhällen och hur vi lever idag. Ericsson har varit en av de viktigaste större aktörerna för utvecklingen av 5G sedan starten och ser att tekniken har potential att helt förändra världen. Enligt Ericsson kan den nya kommunikationsteknologin skapa möjligheter på både individ-, företags-, och samhällsnivå. 5G kan möjliggöra en ny våg av innovation och vara grunden för flera tekniktrender, bland annat IoT, AI och AR (augmented reality). Genom användning av 5G har Ericsson tillsammans med sina kunder och partners hittills utvecklat bland annat automatiserade fabriker, distansstyrd sjukvård och självstyrande bilar. Detta är endast några exempel på vad användningen av 5G kan ge för möjligheter och vi har bara sett början av denna utveckling.

Många industrier tittar idag på hur de kan använda sig av 5G för att skapa nya innovationer som bidrar till ökad effektivitet och högre kapacitet.⁵⁷

Vad gäller utmaningar kopplat till 5G kommer vi kunna se bredare "attacktytor", fler uppkopplade enheter och ökade trafikbelastningar. Nätverken måste därför vara pålitliga, följsamma och säkra redan från början, något som behöver finnas med i grundutformningen och vara integrerat i designen.⁵⁸ Christian Jonsson säger att 5G på ett storskaligt sätt kommer att förändra hur vi lever i dag, i och med det stora antalet uppkopplade enheter vi kommer ha framöver. Att kunna göra saker säkert på en större och bredare skala kommer därför vara oerhört viktigt och Christian ser detta som en av våra största utmaningar när det gäller 5G. Erik G. Larsson, professor i kommunikationssystem vid Linköpings universitet, beskriver att trådlösa kommunikationslänkar, som 5G baseras på, är till sin natur öppna och därmed känsliga för avsiktliga störsändningar. Denna problematik är välkänd inom militära system, men accentueras för civila kommunikationsnätverk av att avancerad utrustning för störsändning under senare decennier blivit mer och mer lättillgänglig.

Regeringar världen över kämpar idag med frågor om hur de på bästa sätt ska kunna skydda de nya 5G-nätverken, då dessa i vissa fall kan klassas som kritisk infrastruktur. En pågående diskussion är hur olika länder ska hantera förekomsten av kinesisk teknologi när 5G börjar användas storskaligt. Detta skiljer sig mellan olika länder enligt en rapport om cybersäkerhet och 5G publicerad i februari 2020 av RUSI, Royal United Services Institute for Defence and Security Studies i Storbritannien. Vissa länder hänvisar till nationella säkerhetsfrågor och förespråkar därför ett förbud mot kinesiska teknikföretag, medan andra länder inte alls vill utelämnas dessa företag. Oavsett hur världens länder väljer att agera i frågan är det uppenbart att det kommer krävas en stark strategi för cybersäkerhetspolitik som en grundläggande komponent i skyddet av 5G-nätverk.⁵⁹

Samhällsfrågor, digitalisering och kompetensutveckling

I följande avsnitt behandlas frågor som rör cybersäkerhet kopplat till samhälle, digitalisering, människans roll, säkerhetsmedvetande och kompetensutveckling både hos privatpersoner och

på arbetsplatser. Därutöver lyfts uppmärksammade händelser kopplat till cybersäkerhet och hur arbetet med riskanalys ser ut idag.

Samhällets digitalisering

2017 presenterades den svenska digitaliseringsstrategin av regeringen som anger inriktningen för regeringens digitaliseringspolitik. Visionen är ett hållbart digitaliserat Sverige, där hela landets befolkning har förtroende för och tar del av det digitaliserade samhället. Digitaliseringen hjälper till att förenkla vardagen, leder till nya jobb och skapar konkurrenskraft. Den bidrar också till att utveckla Sverige att bli ännu bättre på det vi redan är framstående inom idag - en väl fungerande offentlig sektor, en stabil och pålitlig infrastruktur och en teknikkunnig befolkning.

Riksdagens beslutade mål om att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter ska bland annat uppnås genom regeringens digitaliseringsstrategi, vilken brutits ned i fem delmål. Ett av dessa delmål är digital trygghet som beskriver att det i Sverige ska finnas de bästa förutsättningarna för alla att på ett säkert sätt ta del av, ta ansvar för samt ha tillit till det digitala samhället. Delmålet innebär att individer, organisationer och företag ska ha förtroende för användningen av digitala tjänster och enkelt kunna använda och dra nytta av dem. Viktiga frågor inom detta delmål är integritet, informationssäkerhet och synen på hur samhället klarar av att hantera de risker som digitaliseringen innebär. Men inom delmålet ryms också att vi i Sverige ska ha säkra digitala system där identifierade sårbarheter hanteras på ett bra sätt.⁶⁰

För att lyckas med ovanstående krävs ett systematiskt och löpande säkerhetsarbete för att tidigt identifiera och förebygga säkerhetsbrister och även klara av att hantera incidenter när de inträffar. Det behöver finnas en säkerhetsmedvetenhet hos både privata och offentliga verksamheter, där exempelvis kunskap om hur organisationer skyddar sina nätverk och informationssystem är grundläggande, bland annat för att skydda immateriella tillgångar och personlig integritet. Vårt samhälle behöver klara av att skydda sig både mot små incidenter som inträffar ofta och större incidenter och angrepp. Beroenden och kopplingar mellan olika tekniska system är en sårbarhet i dagens samhälle, eftersom störningar kan ge omfattande konsekvenser som dessutom är svåra att förutse och därmed kan bli svåra att hantera.

Viktiga samhällsfunktioner som vattenförsörjning, eldistribution, transporter och sjukhusutrustning bygger idag på digitala informationssystem, vilket innebär att stora mängder känslig information finns tillgänglig digitalt och därmed skapas en ökad sårbarhet. Därför behövs en balansgång mellan säkerhet och användarvänlighet, så att säkerheten är tillräckligt hög, men att systemen och funktionerna samtidigt är lätta för oss människor att förstå och använda, så att risken för felaktigt användande minskar. Inom delmålet digital trygghet är även genomförandet av EU:s direktiv om åtgärder för en höggemensam nivå på säkerhet i informationssystem och nätverk i hela unionen av stor vikt.⁶¹

Att Sverige är ett av världens mest digitaliserade länder ger oss fördelar men det innebär också fler risker jämfört med ett land som är mindre digitaliserat eftersom Sverige blir en måltavla för digitala angrepp. Detta är något som samtliga respondenter är överens om. Annika Avén, Ansvarig för Cyberförsvar på SOFF, berättar att Sverige idag är mest utsatt för hot jämfört med våra nordiska grannländer och att Sverige är en attraktiv måltavla just på grund av nivån av digitalisering.

Torbjörn Kronander menar att vi i Sverige har byggt upp ett känsligt samhälle i och med digitaliseringen, där det går att komma åt mycket data. Dock anser Torbjörn att just på grund av att vi har kommit så långt har vi också en utvecklad syn på digitalisering och det finns en medvetenhet. Jonathan Jogenfors säger att den utvecklade synen på digitalisering och en generellt stor teknikkunskap hos befolkningen bidrar till att företag kan göra produkter som används av många och att det finns många som kan testa nya produkter, vilket är en fördel. Även Märten Holmberg nämner att Sverige har en stor digital mognad på grund av vår utbredda digitalisering och att vi därför ligger före i vissa avseenden, vilket kan vara en fördel. Han ser dock utmaningarna som det innebär att vi levt med digitalisering så pass länge, vi delar gärna med oss av information vilket skapar vanemönster hos oss som vi kanske inte reflekterar över i så stor grad. Andrei Sabelfeld berättar att svenskar generellt är öppna med det mesta och därför får Sverige en utsatt position exempelvis kopplat till integritet. Vidare förklarar Andrei att vi även är vana vid digitala betalningar och användning av Bank-ID, vilket gör att vi blir väldigt beroende av att det ska fungera och inte innehålla några säkerhetsbrister.

Fredrik Landberg beskriver att ett land som Sverige, som ligger så långt fram, också får gå på många nitar, någon måste göra misstagen först. Men även han anser att Sverige klarar mycket, just på grund av samhällets digitala mognad. Däremot är landet mer beroende av att den digitala infrastrukturen fungerar och Fredrik nämner coronapandemin som ett exempel. Hade inte internet fungerat på ett bra sätt hade vi inte klarat perioden lika bra. Det har varit en större utmaning för andra länder med mindre välfungerande internet att hålla jobb och arbeten igång genom distansarbete, berättar Fredrik.

Samhällsviktiga funktioner behöver dock inte bara fungera utan också vara säkra och här ser Richard Oehme, ordförande för SOFF:s cybergrupp, en stor utmaning. När det handlar om kravställning och upphandling i Sverige sker de ofta enligt principen att lägsta pris vinner men när det handlar om säkerhet innebär det för det mesta att kvaliteten också blir lägre. Det krävs djup kunskap för att kunna beställa rätt kvalitet i upphandlingen. Eftersom olika kommuner använder olika krav i upphandlingen ökar komplexiteten ytterligare, då leverantörerna måste anpassa unika lösningar för varje kund, vilket inte blir kostnadseffektivt, säger Richard. Annika Avén påpekar att alla aktörer dessutom ofta behöver vara sammanlänkade på olika vis och därför räcker det ofta att en aktör brister i sin cybersäkerhet för att många ska drabbas.

Jonas Hallberg ser dock att cybersäkerhet i samhället har fått ett lyft under de senaste fem åren och idag får den uppmärksamhet som ämnet förtjänar. Det finns ett intresse för att få fram resultat inom området. På FOI märker han att de kan arbeta med fler aktörer och att fler verksamheter idag hör av sig och är intresserade av utbildning inom området. Tidigare var det en inre cirkel som var intresserade av cybersäkerhet, idag finns det en mer utbredd kunskap och medvetenhet än för fem år sedan. Christian Jonsson säger att cybersäkerhet ska vara lika självklart i dagens samhälle som att vi har brandsläckare i våra byggnader. Han gör jämförelsen med att läkarna på 1800-talet började inse att bakterier bidrog till att många dog men att det kunde förhindras i stor omfattning endast genom en bra grundhygien. På samma sätt behöver vi tänka om vårt digitaliserade samhälle, det behöver finnas en grundläggande cyberhygien, menar Christian.

Under de senaste åren har det skett flera, större händelser och skandaler kopplat till cybersäkerhet, där stora mängder information har läckt ut. Annika Avén menar att en skandal ofta blir ett uppvaknande. Givetvis vill ingen att de ska inträffa men hon tror att det blir lättare för oss människor när vi har något konkret att förhålla oss till, när vi får exempel på vad som kan inträffa om vi inte prioriterar säkerhet och nämner Transportstyrelsen som ett sådant exempel. Lena Miranda lyfter fram att skandaler som exempelvis den för Transportstyrelsen kan skapa en rädsla bland chefer att våga fatta beslut, då det är komplexa frågor med hög risk. Samtidigt betonar hon att dessa är avgörande för att ta våra verksamheter vidare i utvecklingen. Lena lyfter också att hon tror att det finns en stor potential av att lära oss mer om de kriser som skett i syfte att kunna förebygga framtida kriser.

Även Andrei Sabelfeld menar att skandalerna bidrar till att uppmärksamma cybersäkerhet. Martin Hell anser att skandaler bidrar till att göra folk mer säkerhetsmedvetna och att de fungerar som katalysatorer. När både personer och verksamheter ser konkreta exempel på vad som kan inträffa väljer fler att investera i säkerhet. Den ekonomiska aspekten är viktig eftersom företag bland annat börjar se över vad en attack skulle kosta dem om den inträffade. Då blir det naturligt att lägga pengar på säkerhet, när en konkret ekonomisk förlust kan orsakas av säkerhetsbrister, menar Martin.

Människans roll, säkerhetsmedvetenhet och kompetensutveckling

I ovanstående avsnitt bekräftas det av flertalet respondenter att Sverige har en hög digital mognad och ett tekniskt kunnande hos en stor del av befolkningen och att det, på grund av digitaliseringen, finns en högre säkerhetsmedvetenhet än i många andra länder. Även om vi kommit långt finns det mycket som pekar på att säkerhetsmedvetenheten, både hos privatpersoner och i yrkesroller, är för låg. Experter inom cybersäkerhet och personer som jobbar med området dagligen är av stor vikt men den breda och allmänna kunskapen i samhället är också viktig. Eftersom en stor del av befolkningen i Sverige tar del av samhällets digitalisering behövs kunskapen hela vägen ner på individnivå. Alla kan inte bli experter men genom att bara lära sig grunder och öka säkerhetsmedvetenheten hos befolkningen

kan många incidenter förhindras vilket skapar ett helt annat grundskydd, det menar samtliga respondenter som deltagit i denna kartläggning. Många av dem ser denna typ av kompetensutveckling som det allra viktigaste inom cybersäkerhetsområdet just nu eftersom människan ofta är den svagaste länken och orsaken till att incidenter inträffar.

SOFF ser allvarligt på frågan och har bland annat som förslag att införa cybersäkerhet som ämne i grundskolan för att öka den grundläggande cybersäkerhetsmedvetenheten i samhället. Genom denna åtgärd tror de att såväl kunskapen som intresset för området kan öka, något som är viktigt för att i framtiden få fler personer att utbilda sig och arbeta inom området.⁶² Lena Miranda lyfter fram behovet av att höja kompetensnivån på individnivå, och efterlyser en grundläggande utbildning inom cybersäkerhet som riktar sig till en bred målgrupp av svenskarna – likt Elements of AI, som ges vid Linköpings universitet, som är en grundläggande introduktion till AI.

Den samlade informations- och cybersäkerhets-handlingsplanen för 2019–2022 som MSB, FRA, FMV, PTS, Försvarmakten, Polismyndigheten och Säpo tagit fram, innehåller åtgärder som dessa aktörer enskilt, eller tillsammans med andra aktörer, avser att vidta för att höja informations- och cybersäkerheten i samhället. En av de strategiska prioriteringar som omfattas av handlingsplanen är att öka kunskapen och främja kompetensutvecklingen. Prioriteringen rymmer ett antal målsättningar, där den första handlar om att öka kunskapen i samhället som helhet om de mest angelägna sårbarheterna och behoven av säkerhetsåtgärder. Det ska etableras ett strategiskt arbetssätt för värdering och bevakning av samhällets förmåga inom cybersäkerhetsområdet.

Den andra målsättningen handlar om att öka kunskapen hos enskilda användare av digital teknik om de mest angelägna sårbarheterna och behoven av säkerhetsåtgärder. Detta ska bland annat ske genom den riktade informationskampanj som Försvarmakten lanserade i maj 2019. Kampanjen är främst riktad mot Försvarmakten och andra myndigheter, men även externa målgrupper som exempelvis kommuner och privatpersoner har nåtts av kampanjen. Kampanjen har bland annat innefattat korta informationsfilmer som spridits via sociala medier. Under 2020 utökas kampanjen och omfattas av fler säkerhetsaspekter än de som var i

fokus under 2019, vilka var att öka kunskapen om underrättelsehotet samt peka på beteenden som innebär risker, möjliga konsekvenser av bristande säkerhet och hur dessa risker kan minskas. En annan åtgärd som hör till den andra målsättningen och är ny för 2020, är att genomföra riktade utbildningsinsatser på informations-säkerhetsområdet till offentlig sektor, vilket ska ske på uppdrag av MSB. En sista åtgärd inom ramen för den andra målsättningen är kampanjen ”Tänk säkert”, som handlar om att få individer och företag att vidta åtgärder för att skydda sin viktigaste information. Kampanjen är ett EU-initiativ och äger rum varje år i oktober månad.⁶³

Eva Fogelström säger att det finns ett grundläggande behov av kompetens och förståelse för säkerhet hos människor. Hon anser att alla borde få en grundutbildning i säkerhet, både som privatpersoner och i sina yrkesroller. Det går att bygga in mycket säkerhet i system, men en människa kan orsaka skada ändå, därför är området människa-teknik både intressant och viktigt. Kompetens inom cybersäkerhet idag handlar inte bara om säkerhetsexperten utan det är den breda förståelse hos befolkningen som är den stora utmaningen, enligt Eva. Åke Holmgren anser att medvetenhet är viktigt, men att få människor att agera utifrån dessa kunskaper och skapa en verklig beteendeförändring är en ännu större utmaning. Enligt Andrei Sabelfeld tar det inte lång tid att sätta sig in i det grundläggande. Han vill se ett förändrat tankesätt kring cybersäkerhet och gör jämförelsen med hur coronapandemin drabbat oss och vilket ansvar alla medborgare behövt ta för att klara av situationen. Många kan idag ställa sig frågan varför de ska skydda sin dator när de inte själva anser att de har något värdefullt innehåll. Men det är precis som med Covid-19, det handlar inte enbart om att inte själv bli smittad, utan se till att inte andra blir smittade, menar Andrei.

Systemen som byggs behöver väga upp för mänskliga svagheter, enligt Torbjörn Kronander. Den största utmaningen är att människan i grund och botten är bekväm, menar Tore Johnsson. Det är bekvämt att skriva upp ett lösenord och lägga under tangentbordet och obekvämt att exempelvis sätta upp ett skärmskydd på datorn som hindrar andra från att läsa vad som står på skärmen. Människan i organisationen är därför den stora utmaningen även om majoriteten är godhjärtade, anser Tore. Mårten Holmberg tror att det måste vara enkelt att göra rätt.

Lösenord som ska bytas ofta och består av många olika tecken gör att personer hittar vägar runt det. Vi måste underlätta för den enskilde individen, så det är lätt att agera på ett säkerhetsmedvetet sätt, säger Mårten. Men även om systemen blir säkrare och grundförutsättningarna för att använda dem lättare, krävs det fortfarande att användarna är säkerhetsmedvetna och besitter grundläggande kunskaper.

Annika Avén anser att det borde finnas fler lättillgängliga grundutbildningar och fler utbildningar som kan komplettera för de personer som redan har grundkunskaper. Hon tror även att det är viktigt att lyfta fram förebilder inom branschen. Martin Bergling håller med och menar att vi inte ska stirra oss blinda på tekniken och de tekniska lösningarna utan se till att ta fram utbildningsformer som kan göra alla samhällets medborgare mer säkerhetsmedvetna.

Inom företag finns ett stort behov av att öka medarbetares säkerhetsmedvetenhet. Jonathan Jogenfors berättar att många företag använder IT i verksamheten varje dag och inte förstår hur sårbara de är i och med det. Attackerna som företag kan utsättas för blir mer effektiva och riktade och det är inte bara de stora företagen som drabbas, utan även mindre företag. Därför är det enligt Jonathan viktigt att få både små och medelstora företag att förstå hur beroende de är av säkerhet. Han tar upp ett exempel med de konsekvenser det skulle få för ett mindre företag om deras lagersaldo försvann.

Åke Holmgren beskriver att en stor del av arbetet MSB utför är just råd och stöd till organisationer i förebyggande syfte. Mycket fokus ligger på att stötta offentliga organisationer, men Åke lyfter att det är viktigt att de även når ut till mindre organisationer för att hjälpa dem utveckla sitt cybersäkerhetsarbete. Fredrik Landberg vill att företagen ska inse att de behöver ta hjälp. Han ser att nätverksbyggande mellan företag inom cybersäkerhet kommer vara viktigt framöver. På sått sätt kan företagen diskutera saker gemensamt, utbyta erfarenheter och ha kontakt med personer innan någonting inträffar, för då har de kontakter när något väl händer. Vidare tror Fredrik att det är viktigt att expertkompetensen inom cybersäkerhet inte i alltför stor utsträckning låses in i specifika företag, utan att expertkompetens ska kunna utnyttjas av många samtidigt och på flera ställen genom samarbeten och sedan tidigare etablerade kanaler.

Christian Jonsson lyfter att ledning är en viktig fråga som glöms bort kopplat till cybersäkerhet. Han tror att vi idag är duktiga på och vet hur cyberingenjörer utbildas, men när det kommer till projektledning, management och cybersäkerhetsarbete på strategisk nivå ser Christian att det finns mer att göra och att det krävs att dagens chefer och ledare är mer insatta i ämnet. Det är viktigt att de, utöver sina ledarkunskaper, även besitter kunskaper inom säkerhet. Jonas Hallberg lyfter kultur kring informationssäkerhet på företag som ett intressant framtida forskningsområde, det vill säga hur kulturen på en arbetsplats påverkar informationssäkerheten. Det behöver bland annat forskas på frågor som hur intresse för säkerhet skapas och hur företag ska agera för att engagera medarbetare i säkerhetsarbetet. Överlag ser Jonas att större fokus behöver läggas på frågor som rör just kopplingen mellan människa och teknik och hur människan agerar i en cybermiljö.

Riskanalys

Flera av respondenterna anser att den expertkompetens som finns inom cybersäkerhet i landet är hög, att de som jobbar med cybersäkerhet på avancerad nivå är mycket duktiga inom området. Däremot påpekar nästan alla att kompetensen inom riskanalysarbete, som är en viktig och grundläggande del i arbetet med cybersäkerhet, inte håller samma höga nivå. Jonas Hallberg ser att det är en stor utmaning för branschen, eftersom riskerna är grunden för hela cybersäkerhetsarbetet. Riskerna baseras ofta på okvalificerade gissningar utifrån ett arbete som genomförs snabbt och inte alltid grundligt. Något som inte ger en bra grund, menar Jonas. Det behövs mer innovation och området behöver få mer uppmärksamhet. Jonas ser att det finns för lite forskning inom området idag och att det behövs mer av det framöver för att kunna ta fram bättre modeller än de som finns idag.

Martin Bergling ser utförandet av riskanalyser som ett utvecklingsområde för IT-branschen och tror att riskanalyserna också skulle behöva vara kvantitativa istället för bara kvalitativa vilket många är idag. Han ser inte att åtgärderna från kvalitativa riskanalyser blir tillräckliga. Genom att få ut tydliga värden, som det både går att räkna på och simulera med, blir det lättare att identifiera risker och på så sätt också förebygga eller åtgärda dessa. Det är mer effektivt än att tala om risknivåer som visar låg, medel eller

hög, menar Martin. Jonas Hallberg anser däremot att siffror inte nödvändigtvis innebär att analyserna blir bättre och betonar vikten av att de kvantitativa verktyg som används är genomtänkta. Ola Stensby, programansvarig för Security Arena vid Lindholmen Science Park, tycker inte att han under sina år i branschen har stött på något verktyg som fungerat hela vägen ut. Han tror att vi skulle se bättre resultat av riskanalyser om två eller tre metoder användes parallellt.

Riskanalysarbete är svårt och det krävs en bred kompetens för att kunna utföra bra riskanalyser, menar Andrei Sabelfeld. Han menar att det inte bara är teknisk expertis som krävs, utan också kompetens som kan bedöma vad en organisation har för värdefulla resurser samt hur exempelvis kulturella och sociala aspekter ser ut inom organisationen. Tore Johnsson anser, precis som Andrei Sabelfeld, att riskanalysarbete är svårt och att det blir ännu svårare när verksamheter inte besitter kunskapen som krävs för att avgöra vilka risker som finns eller vet vilka lösningar som kan erbjudas. Som exempel nämner han icke-tekniska företag, där många har svårt att veta vilka risker som kan finnas och hur de ska hanteras. Dessa företag behöver hjälp att genomföra riskanalyser, menar Tore. Det är också viktigt att företag gör riskanalyser från början och inte låter riskanalysarbetet vara något som görs i efterhand, enligt Annika Avén. Hon anser att alla företag bör definiera vad som är viktigast för dem att skydda på ett cybersäkert sätt och hur länge de klarar sig utan resursen vid en eventuell incident. Givetvis måste det för företag finnas en balans mellan kostnad och säkerhet, vilket är en utmaning när det kommer till riskanalysarbete, säger Simone Fischer-Hübner.

MSB tar upp systematiskt riskbaserat arbete som en av deras främsta rekommendationer i deras årsrapport av it-incidentrapporteringar för 2019. MSB har tagit fram ett metodstöd som hjälper verksamheter att bedriva ett systematiskt informationssäkerhetsarbete. Metodstödet bygger på de internationella standarderna i ISO/IEC 27000-serien. Genom ett systematiskt riskbaserat arbete kan verksamheter höja lägstanivån bland medarbetare, öka rapporteringsgraden och dessutom minska konsekvenserna av de incidenter som rapporteras in.⁶⁴

Utbildning, forskning och innovation

Enligt respondenterna finns ett stort behov av utbildning, forskning och innovation på området för cybersäkerhet. Säkerhetsaspekternas ökade vikt leder till en större efterfrågan på såväl forskning som kompetens hos företagen. Det finns flera problemområden när det kommer till kompetensförsörjning inom området för cybersäkerhet, bland annat i att det finns få utbildningar och en ojämn könsfördelning. Det kan också konstateras att det krävs samverkan mellan flera aktörer utöver de som arbetar med utbildningsfrågor för att lösa problemet, från företag såväl som myndigheter.⁶⁵

Det finns flera aktuella forskningsprojekt och nationella initiativ inom, eller med anknytning till, cybersäkerhet. Nedan redogörs för några av dessa.

AI Innovation of Sweden

Ett nationellt center för forskning och innovation kopplat till AI, samarbete mellan aktörer inom privat och offentlig sektor samt akademien.⁶⁶

Nationellt cybersäkerhetscenter

Ett cybersäkerhetscenter som FRA, Försvarmakten, MSB och Säpo fått i uppdrag av regeringen att upprätta under 2020. Centret ska samordna det nationella arbetet med cybersäkerhetsfrågor.⁶⁷

Innovationsnod för cybersäkerhet

En samarbetsplattform som ska upprättas under januari 2020 till juni 2021 för att underlätta och främja forskning inom cybersäkerhet, samt samla nationella aktörer. RISE är projektkoordinator för innovationsnoden.⁶⁸

FOI cyber range - CRATE

CRATE - Cyber Range and Training Environment. En cyberanläggning i Linköping som började utvecklas 2008, är en del av FOI och används för utbildning, träning, övning, utvärdering och experiment. CRATE är ett verktyg till stöd för att utveckla totalförsvarets förmåga i cybermiljön.⁶⁹

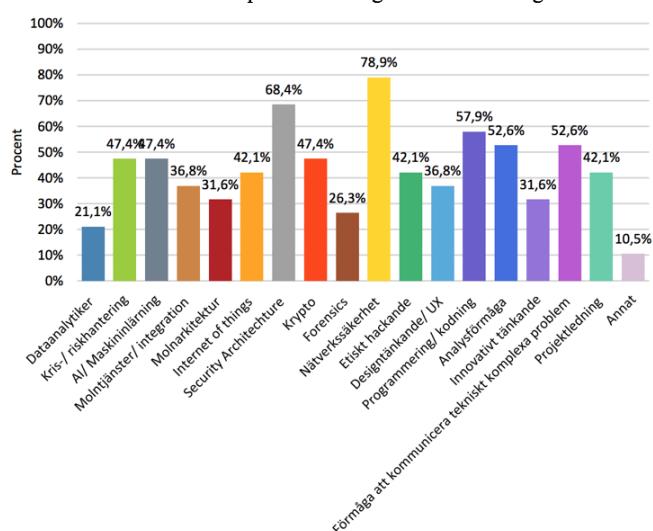
RISE cyber range

En cyberanläggning som är tänkt att användas för att utbilda aktörer inom privat och offentlig sektor i cybersäkerhetsfrågor. Ska upprättas på RISE i september 2019 till augusti 2022 i Kista.⁷⁰

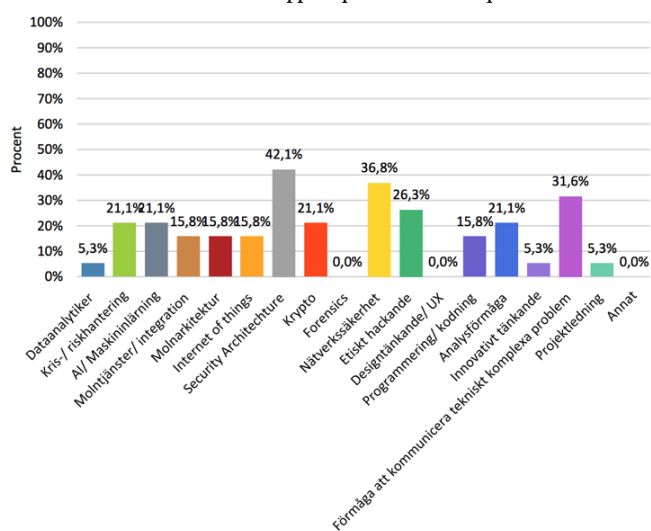
Utbildning och kompetensförsörjning inom branschen

I en undersökning från SOFF från 2018 bland organisationens medlemsföretag uppgav 40% att behovet av medarbetare med cybersäkerhetskompetens ökat och 60% att det ökat avsevärt.⁷¹ Enligt en ny undersökning från SOFF under 2020 identifieras att det fortfarande råder ett stort behov av cyberkompetens nu och kommande fem år, och att det främst är specialistkunskaper som efterfrågas.⁷²

Vilken/ vilka av dessa kompetenser/ färdigheter söker ni idag och framöver?



Vilka av dessa ser ni som topp tre prioriterade kompetenser framöver?



Det finns en stor efterfrågan på kompetens även bland respondenterna, däribland teknisk kompetens för att förstå komplexa system, kunna genomföra riskanalyser och bedriva ett bra säkerhetsarbete. Andreas Karström anser att det är en utmaning att hitta tekniskt kompetent personal som också har ledarkompetens. Även inom de mindre tekniska områdena anser respondenterna att det finns en kompetensbrist vad gäller cybersäkerhet, exempelvis kognitionsvetare, jurister och statsvetare. Att det behövs mer än teknisk kompetens är något som också lyfts av SOFF, som konstaterar att cybersäkerhetsbranschen hade gynnats av att synliggöra den bredd som efterfrågas även inom andra professioner.⁷³ MSB har listat ett antal initiativ i en handlingsplan för informations- och cybersäkerhet under åren 2019–2022. Målsättning 5.3 i handlingsplanen handlar specifikt om kompetensförsörjning, "Det ska bedrivas högre utbildning, forskning och utveckling av hög kvalitet rörande informations- och cybersäkerhet och säkerhet på IT- och telekomområdet i Sverige". Här ingår bland annat att under 2020 utföra en förstudie för att undersöka kompetensförsörjningen inom informationssäkerhet- och cybersäkerhet och stärka de utbildningar som finns inom området.⁷⁴

Respondenterna efterfrågar fler utbildningar inom cybersäkerhet och med mer fokus på praktisk erfarenhet. Christian Jonsson ser gärna någon typ av case-baserad utbildning. Fredrik Landberg menar att det är en hög tröskel för att börja jobba inom IT-säkerhet eftersom säkerhetsarbetet kräver kompetens från start, och lyfter traineeprogram som en bra lösning på problemet.

Nedan listas de utbildningar och kurser, inklusive sommarkurser och hacking-tävlingar, som finns inom cybersäkerhet i Sverige idag.⁷⁵

Under rubrikerna *Utbildningar* och *Kurser* listas endast de som går att söka via antagning.se. Många universitet erbjuder även kurser inom cybersäkerhet på olika utbildningsprogram inom exempelvis datavetenskap, informations- och kommunikationsteknologi och elektroteknik. För kurser som ingår i sådana utbildningsprogram hänvisas till respektive universitets hemsida.

Utbildningar

Nivå	Namn	Högskolepoäng	Skola	Studieort
Kandidatexamen	IT-säkerhet och mjukvarutestning	180	Högskolan Dalarna	Borlänge
Kandidatexamen	IT-forensik och informationssäkerhet	180	Högskolan i Halmstad	Halmstad
Kandidatexamen	Nätverkssäkerhet	180	Linnéuniversitetet	Växjö
Högskoleexamen	Nätverksteknik med IT-säkerhet	120	Högskolan Väst	Trollhättan
Högskoleingenjör	Högskoleingenjör i IT-säkerhet	180	Blekinge tekniska högskola	Karlskrona
Magister	Magisterprogram i nätverksforensik	60	Högskolan i Halmstad	Halmstad
Magister	Folkhälsovetenskap: Digital hälsa och kommunikation - magisterprogram	60	Högskolan i Skövde	Skövde/ Distans
Magister	Integritet, informationssäkerhet och cybersäkerhet - magisterprogram	60	Högskolan i Skövde	Skövde/ Distans
Master	Masterprogram i informationssäkerhet	120	Stockholms universitet	Stockholm
Master	Informationssäkerhet, master	120	Luleå tekniska universitet	Luleå/Distans
Master	Masterprogram i informatik- ledning och styrning av informationssäkerhet	120	Örebro universitet	Örebro
Master	Integritet, informationssäkerhet och cybersäkerhet - masterprogram	120	Högskolan i Skövde	Skövde/ Distans
Master	Masterprogram i informatik – ledning och styrning av informationssäkerhet	120	Högskolan i Skövde	Skövde
Civilingenjör	Civilingenjör i datorsäkerhet	300	Blekinge tekniska högskola	Karlskrona

Kurser

Kursnamn	Högskolepoäng	Skola	Studieort
Cyberoperationer i antagonistisk miljö	7,5	Försvarshögskolan i Stockholm	Stockholm
Datakommunikation och IT-säkerhet	7,5	Högskolan i Gävle	Gävle
Cybersäkerhet – utmaningar med distribuerade arbetsplatser	7,5	Högskolan i Halmstad	Distans
Informationssäkerhet – riskhantering	7,5	Högskolan i Skövde	Skövde
Ledning och styrning av informationssäkerhet A1N	7,5	Högskolan i Skövde	Skövde
Principer för integritet, informations-säkerhet och cybersäkerhet A1N	7,5	Högskolan i Skövde	Skövde/Distans
Datasäkerhet I	7,5	Karlstads universitet	Karlstad
Grundläggande datasäkerhet	5	Linköpings Universitet	Linköping/Distans
Mobil och trådlös säkerhet	7,5	Linnéuniversitetet	Växjö
Internetsäkerhet	7,5	Linnéuniversitetet	Växjö
Strategisk informationssäkerhetshantering	7,5	Linnéuniversitetet	Växjö/Distans
Dator- och nätverkssäkerhet	7,5	Luleå tekniska universitet	Luleå
Informationssäkerhet	7,5	Luleå tekniska universitet	Luleå
Internetsäkerhet	7,5	Luleå tekniska universitet	Luleå
Riskhantering för informationssäkerhet	7,5	Luleå tekniska universitet	Luleå
Säkerhet för IT-infrastruktur	7,5	Luleå tekniska universitet	Luleå
Säkerhet i infrastruktur	7,5	Luleå tekniska universitet	Luleå
Säkerhet och IT-management	7,5	Luleå tekniska universitet	Luleå
Säkerhetsarkitektur	7,5	Luleå tekniska universitet	Luleå/Distans
Informatik: Säkerhet i informationssystem	7,5	Lunds universitet	Lund
Datavetenskap GR (A), Introduktion till IT-rätt och datasäkerhet	7,5	Mittuniversitetet	Distans
Praktisk cybersäkerhet	5	Mälardalens högskola	Distans
Säkerhet i datornätverk, distanskurs	7,5	Mälardalens högskola	Distans

Cybersäkerhet i ett samhällsperspektiv	5	Uppsala universitet	Uppsala
IT-säkerhet	7,5	Uppsala universitet	Gotland
Informatik, Introduktion till IT-säkerhet, avancerad nivå	7,5	Örebro universitet	Örebro
Informatik, Kravställande för informationssäkerhet, avancerad nivå	7,5	Örebro universitet	Örebro
Informatik, Ledning och styrning av informationssäkerhet - tillämpningsområden, avancerad nivå	10,5	Örebro universitet	Örebro
Informatik, Regulativa aspekter av informationssäkerhet, avancerad nivå	7,5	Örebro universitet	Örebro
Informatik, Sociala aspekter av informationssäkerhet, avancerad nivå	7,5	Örebro universitet	Örebro
Informatik, Tillämpad styrning av informationssäkerhet, avancerad nivå	12	Örebro universitet	Örebro

Sommarkurser och tävlingar

Kursnamn	Högskolepoäng	Skola	Studieort
Introduktion till cybersäkerhet G1N	15	Högskolan i Skövde	Skövde
CyberSecurity and Privacy (CySeP)	3,5	Kungliga tekniska högskolan	Stockholm
Midnight Sun Capture the Flag Hacking Competition	N/A	Kungliga tekniska högskolan	Stockholm

YH-utbildningar

Kursnamn	Omfattning	Skola	Studieort
IT-säkerhetstekniker	400 YH-poäng	Campus i12	Eksjö
IT-säkerhetstekniker – Etisk hackare	440 YH-poäng	Edugrade	Hudiksvall
IT-säkerhetstekniker	410 YH-poäng	TUC	Jönköping
IT-säkerhetsspecialist	400 YH-poäng	Stockholms Internationella Handelsskola	Malmö, Stockholm
IT-säkerhetstekniker	400 YH-poäng	Newton	Stockholm, Göteborg
IT-säkerhetstekniker	400 YH-poäng	Frans Schartaus Handelsinstitut	Stockholm
Informationssäkerhets-samordnare	3 terminer	Företagsuniversitetet	Stockholm
IT-säkerhetsspecialist	400 YH-poäng	Xenter	Tumba

Forskning och innovation

Det sker mycket forskning inom cybersäkerhet och eftersom begreppet är brett är även forskningen spridd över flera områden. Jonas Hallberg menar att det generellt sker mycket forskning på tekniska metoder, vilket kommer att fortsätta framöver. Han ser också kommande forskningsområden inom bland annat riskanalys och människans roll i cybersäkerhetsarbetet. MSB har sedan tidigare finansierat forskning inom informationssäkerhet och utmaningar kopplat till digitalisering och cybersäkerhet. Under 2020–2021 kommer det upprättas ett forskningsstöd för "framtidens autonoma och automatiserade cybersäkerhet".⁷⁶ Det finns även ett behov av annat än teknisk forskning, till exempel humanistisk och samhällsvetenskaplig forskning kopplat till utvecklingen av AI.⁷⁷

Fredrik Landberg menar att den kompetensbrist som råder inom cybersäkerhet gör att det blir viktigare att bygga nätverk för att på så sätt kunna utnyttja resurser på ett effektivt sätt. Mårten Holmberg anser att det, förutom att stötta startups, också är viktigt att stötta företag som vill skala upp sina verksamheter. Ola Stensby lyfter också att små- och medelstora företag behöver stöd i cybersäkerhetsarbetet och att mindre företag inte inser att de kan vara måltavlor för cyberangrepp.

Sweden ICT är ett samarbete för innovation mellan sex av Sveriges Science Parks: Ideon Science Park i Lund; Blue Science Park i Blekinge; Kista Science City; Lindholmen Science Park i Göteborg; Luleå Science Park och Linköping Science Park. Totalt består samarbetet av 2400 företag och närmare 60 000 anställda och innefattar såväl startups som tillväxtföretag, forskningsintensiva företag och konsultbolag. Inom ramen för samarbetet finns en mängd tekniska bolag inom bland annat mjuk- och hårdvaruutveckling, IoT och inbyggda system, som är viktiga för Sverige i och med den ökande digitaliseringsgraden. Syftet med samarbetet är att stötta teknikbolag i Sverige och skapa en innovations- och samverkansplattform för dessa, samt att kunna attrahera kompetens. På sikt är målet att genom dessa teknikbolag kunna stärka och främja Sverige som ett digitaliserat samhälle.⁷⁸ Då tekniska, innovativa bolag är utsatta för större cybersäkerhetshot är det av särskild vikt för dessa att arbeta aktivt med cybersäkerhet.

Vidare finns en branschorganisation för samtliga av Sveriges Science Parks och inkubatorer, Swedish Incubators and Science Parks, SISP. SISP omfattar fler än 6000 företag och närmare 100 000 sysselsatta.⁷⁹ Organisationen arbetar för att utveckla branschen för inkubatorer och Science Parks och erbjuder sina medlemmar att vara del i den utvecklingen genom exempelvis utbildning, påverkansmöjligheter och nyheter. Organisationens medlemmar har som syfte att främja kunskapsföretag med tillväxtambitioner genom att erbjuda olika typer av stöd och skapa gemensamma mötesplatser och nätverk. Dessa miljöer utgör en stark infrastruktur för innovation- och förnyelseaktiviteter och fungerar även som samlingspunkt för internationella etableringar.

Martin Bergling lyfter den nya svenska innovationsnoden för cybersäkerhet som ytterligare ett initiativ på området. RISE driver denna nationella kraftsamling kring cybersäkerhet för att accelerera forskning och innovation inom industri och offentlig sektor, där Vinnova svarar för finansieringen medan RISE har rollen som koordinator för arbetet. Projektet startade våren 2020 och ska pågå till 2027.

Framtidsutsikter

I följande avsnitt redogörs för framtidsutsikterna för cybersäkerhet utifrån existerande litteratur och respondenternas åsikter.

Drivkrafter för cybersäkerhetsmarknaden

Det finns flera faktorer som driver utvecklingen av cybersäkerhetsmarknaden. Tore Johnsson sammanfattar de drivande faktorerna som möjligheten att tjäna pengar och olika hot. Han menar att större företag ser en risk i att förlora värdefull information, något som på sikt kommer att börja gälla även privatpersoner i allt större utsträckning, medan andra företag och entreprenörer ser en möjlighet att tjäna pengar med utgångspunkt i detta. Även tekniska aspekter driver utvecklingen framåt, dels handlar det om en allt större e-handel och om uppkomsten av nya, disruptiva teknologier som AI, IoT och Blockchain. Dessutom spås efterfrågan på olika cybersäkerhetslösningar öka framöver inom vissa branscher som bank och finans, sjukvård, produktion och försvarsindustri.⁸⁰

Enligt respondenterna drivs utvecklingen främst av ökande cyberhot, bland annat i ett hårdare internationellt tonläge, omfattande spionageverksamhet från andra länder och fler cyberkriminella. I de årliga rapporterna från FRA och Säpo ges exempel på sådant som driver på utvecklingen. I dessa varnas för både omfattande och ständigt pågående aktiviteter riktade mot Sverige från olika statsaktörer. Andreas Karström anser även att existerande och kommande ramverk och regelverk driver cybersäkerhetsmarknaden framåt. Fredrik Landberg tror att privatpersoner kommer att ställa högre krav på säkerhet och att de kommer vara beredda att betala mer för en säker produkt framöver. Mårten Holmberg menar att cybersäkerhet kommer gå från att vara en reaktiv process till att vara ett förebyggande arbete, och att detta kommer vara en drivande faktor de kommande två åren.

I och med den tekniska utveckling som sker där allt blir mer uppkopplat ökar mängden cyberattacker. När företag och stater utsätts för fler cyberattacker ställs också högre krav på ett bra cyberförsvar.⁸¹ Torbjörn Kronander menar att vi har byggt ett känsligt samhälle till följd av digitaliseringen, och att det är en drivkraft för cybersäkerhetsmarknaden. Respondenterna lyfter att det finns en svårighet i att marknadsföra cybersäkerhetslösningar, eftersom det är svårt att synliggöra resultatet från ett bra cybersäkerhetsarbete. Det är en av anledningarna till att flera respondenter ser större skandaler kopplat till ett bristfälligt cybersäkerhetsarbete som en katalysator för att utvecklingen av cybersäkerhetsmarknaden ska gå framåt.

A low-angle, upward-looking perspective of several modern skyscrapers with glass facades, creating a sense of height and architectural scale. The entire image is overlaid with a semi-transparent purple filter. The text is centered in the middle of the frame.

Organisationer och projekt

Organisationer och projekt

Företag i Sverige

Nedan listas företag med kontor i Sverige som är verksamma inom cybersäkerhet. Företagen är både nationella och internationella. Flera företag erbjuder flera typer av tjänster och produkter, i denna tabell listas de som är kopplade specifikt till cybersäkerhet. Primärt anges huvudkontoret, om det finns fler kontor anges dessa inom parentes. Listan gör inte anspråk på att vara komplett och relevanta företag kan saknas.

Företag	Tjänster och produkter inom cybersäkerhet	Kontor i Sverige
2Secure	Konsulttjänster inom IT-säkerhet, t.ex. riskanalys, utbildning m.m.	Stockholm (Göteborg, Lund, Västerås, Karlstad)
4C Strategies	Konsulttjänster inom IT-säkerhet, t.ex. Riskanalys, utbildning m.m.	Stockholm (Malmö)
Advenica	Nätverkskryptering, riskanalys, riskhantering, utbildning, m.m.	Malmö
Afry	Konsulttjänster inom IT-säkerhet, t.ex. kravställning, systemdesign m.m.	Stockholm m.fl.
Atea	Konsulttjänster inom IT-säkerhet, t.ex. moln, riskhantering, riskanalyser	Stockholm m.fl.
Basalt	Konsulttjänster inom IT-säkerhet, t.ex. Säkra IT-system, teknisk projektledning m.m.	Enköping (Stockholm)
Bosch security systems	IoT, videodatasäkerhet	Stockholm
Centipede	Riskhantering, utbildning m.m.	Vaxholm
Certezza	Riskanalys, informationsklassning, utbildning m.m.	Stockholm
Check Point	Moln, nätverk, riskhantering, mobilsäkerhet	Stockholm
CGI	Konsulttjänster inom IT-säkerhet, t.ex. Testning, riskhantering m.m.	Stockholm (Linköping m.fl.)
Clavister	Biometrisk autentisering, nätverk, moln m.m.	Örnsköldsvik (Stockholm, Nacka)
CISCO	Nätverk, IoT, moln	Stockholm
Combitech	Konsulttjänster inom cybersäkerhet, t.ex. Cybersäkerhet för fordon, riskhantering, utbildning, cyberförsvar m.m.	Linköping
Comex electronics	Brandväggar, kryptering	Stockholm
Crypto	Kryptering m.m.	Lund
Cybercom	Konsulttjänster inom IT-säkerhet, t.ex. riskhantering	Stockholm

Cygate	Konsulttjänster inom riskanalys, autentisering m.m.	Solna (Borlänge, Gävle, Göteborg m.fl.)
DataProtect	Systemdesign, säkerhetstestning, säkerhetsrådgivning m.m.	Borås
Deloitte	Konsulttjänster inom cybersäkerhet, t.ex. riskhantering	Stockholm (Göteborg, Malmö m.fl.)
Detectify	Webbsäkerhet, ethical hacking	Stockholm
Deville IT-konsultbyrå	Konsulttjänster inom IT-infrastruktur och system engineering	Stockholm
Ericsson	Telekom, 5G, IoT, nätverk m.m.	Stockholm (Göteborg, Karlskrona, Linköping, Luleå, Lund, m.fl.)
Expisoft	Nätverk, säker autentisering m.m.	Stockholm
FCG	Konsulttjänster inom IT-säkerhet, t.ex. riskhantering	Stockholm (Malmö)
Fogel Consulting	Konsulttjänster inom cybersäkerhet, t.ex. riskhantering, riskanalys, utbildning, moln, kravställning m.m.	Stockholm
Foreseeti	Automatiserad hotmodellering och attacksimuleringar	Stockholm
Fortinet	Säkerhetslösningar för nätverk	Stockholm
Giesecke+Devrient Mobile Security	Fordon, mobilsäkerhet m.m.	Stockholm
Halon	Säkerhetslösningar för mail	Göteborg
HiQ	IT-konsultföretag med tjänster inom bl.a. cybersäkerhet	Stockholm (Göteborg, Karlskrona, Linköping, Västerås)
Holm Security	Nätverksscanning, webbapp-scanning, riskanalys	Stockholm
Hyker Security	Molnsäkerhetslösningar m.m.	Linköping (Göteborg, Malmö)
IBM	Riskhantering, integrerade säkerhetstjänster m.m.	Stockholm (Göteborg, Malmö, Sundsvall)
IT-Total	Konsulttjänster inom cybersäkerhet, t.ex. riskanalys, utbildning m.m.	Stockholm
Knowit	Konsulttjänster inom cybersäkerhet, t.ex. riskhantering, incidentutredning, moln m.m.	Stockholm (Göteborg, Linköping m.fl.)
Link22	Kritisk infrastruktur, ackreditering, kodgranskning och säkerhetsanalys m.m.	Linköping (Stockholm, Östersund)
Modio	IoT, inbyggda system	Linköping
Mullvad VPN	VPN	Göteborg
Nixu AB	Konsulter inom cybersäkerhet, t.ex. cyberförsvar, moln m.m.	Uppsala (Stockholm)
NTT Security	Riskanalys, säkerhetslösningar för nätverk och moln, m.m.	Solna (Göteborg m.fl.)

Orange Cyberdefense	Säker infrastruktur, datacentrisk säkerhet, moln m.m.	Malmö (Stockholm, Göteborg m.fl.)
Outpost24	Nätverkssäkerhet, moln, penetrationstester m.m.	Karlskrona (Stockholm m.fl.)
Palo Alto Networks	Cybersäkerhetslösningar för nätverk	Stockholm
PrimeKey	Autentisering, moln, IoT m.m.	Solna
PwC	Konsulttjänster inom cybersäkerhet, t.ex. riskhantering, utbildning m.m.	Stockholm
QinetiQ	Riskhantering, test, utbildning m.m.	Linköping (Stockholm)
Recorded Future	Riskhantering, hotövervakning	Göteborg
Rote	Konsulttjänster inom IT-säkerhet, t.ex. riskhantering	Stockholm (Boden, Göteborg)
SAAB	Kritisk infrastruktur, moln, nätverk, militär m.m.	Stockholm (Linköping)
Scandinavian Risk Solutions (SAS)	Riskhantering, krishantering, utbildning m.m.	Stockholm
Secana	Konsulttjänster inom cybersäkerhet, t.ex. riskhantering, sårbarhetsanalyser, utbildning m.m.	Stockholm
Sectra	Kritisk infrastruktur, militär, nätverk, mobil m.m.	Linköping (Stockholm, Örebro)
Secure State Cyber	Säkerhetsgranskning, incidenthantering, utbildning m.m.	Norrköping (Malmö, Stockholm)
Sentor	Risikanalys, incidenthantering, penetrationstester m.m.	Stockholm (Malmö, Gävle m.fl.)
Siemens (Cybersecurity)	Industri, helhetslösningar för cybersäkerhet	Solna
Simovits	IT-säkerhet, t.ex. IT-forensik, kravställning, risikanalys m.m.	Stockholm
SNG	Riskhantering, risikanalys, utbildning m.m.	Stockholm
Säkerhetskontoret	Källkodsanalys, kryptoanalys, penetrationstester och nätverksinspelning	Stockholm
Syntell	Konsulttjänster inom IT-säkerhet, t.ex. kravställning och utbildning	Stockholm (Lund)
Truesec	Risikanalys, incidenthantering, autentisering m.m.	Stockholm (Malmö, Karlskrona m.fl.)
Tutus	Nätverkssäkerhet, säkra mobiler, filkryptering	Stockholm
Weop	Konsulttjänster inom IT-säkerhet, t.ex. projektledning m.m.	Stockholm
West Code Solutions	Konsulttjänster inom riskhantering, isolerade system m.m.	Stockholm
Zebware	Moln	Stockholm

Svenska myndigheter, forskningsinstitut och branschorganisationer

Nedan listas organisationer, myndigheter och institut och hur de arbetar med frågor relaterade till cybersäkerhet.

Organisation	Beskrivning av verksamhet inom cybersäkerhet	Kontor i Sverige
FMV	Försvarets materielverk. Sveriges nationella certifieringsorgan för IT-säkerhet.	Stockholm
FOI	Totalförsvarets forskningsinstitut, bedriver forskning inom bl.a. Cybersäkerhet. Har en cyber range i Linköping, CRATE, för utbildning, forskning och utvärdering inom cybersäkerhet.	Stockholm (Linköping, Umeå)
FRA	Försvarets radioanstalt. En del av Sveriges cyberförsvar.	Stockholm
MSB	Myndigheten för samhällsskydd och beredskap. Samordningsansvar för cybersäkerhet i Sverige.	Karlstad (Kristinehamn, Stockholm)
NFC	Nationellt Forensiskt Centrum. Avdelning inom polismyndigheten som arbetar med forensiskt arbete, bland annat inom IT-forensik.	Linköping m.fl.
PTS	Post- och Telestyrelsen. Myndighet som bevakar områdena elektronisk kommunikation och post i Sverige.	Stockholm
RISE	Forskningsinstitut, forskning inom bl.a. Cybersäkerhet. Ska upprätta en cyber range för utbildning, forskning och testning i Kista.	Göteborg m.fl.
SOFF	Branschorganisation för företag inom säkerhets- och försvarsområdet med verksamhet i Sverige.	Stockholm
Säpo	Säkerhetspolisen. Bedriver arbete med att öka Sveriges cybersäkerhet och motverkar spionage.	Stockholm
Teknikföretagen	Arbetsgivarorganisation. Publicerar rapporter och undersökningar på bl.a. cybersäkerhet.	Stockholm
Vinnova	Sveriges innovationsmyndighet. Finansierar olika typer av forskningsprojekt, bland annat inom cybersäkerhet.	Stockholm



Sammanfattande slutsatser

Sammanfattande slutsatser

Av resultatet från kartläggningen kan ett antal styrkor, svagheter, möjligheter och utmaningar identifieras inom de områden som tagits upp i rapporten. Utifrån nedanstående SWOT-analyser går det att konstatera att det finns flera uppslag till forskningsprojekt, insatser och utvecklingsområden inom cybersäkerhetsområdet. Det handlar dels om olika tekniker, men också avseende mer kvalitativa aspekter, exempelvis kring människans roll kopplat till cybersäkerhet.

SWOT - Tekniker

S

Styrkor

- Den teknikkompetens som finns i Sverige håller en mycket hög nivå.
- Ett omfattande innovationsekosystem.
- Många forskningsprojekt pågår inom flera olika teknikområden.
- Sverige har många framstående företag inom branschen som arbetar både på en nationell nivå och globalt.

W

Svagheter

- Företag har svårt att hitta expertkompetens, det är hård konkurrens om den kompetens som finns i Sverige.
- Det finns en stor drivkraft från företag att snabbt få ut nya tekniska innovationer på marknaden, vilket kan bidra till en lägre säkerhetsnivå på dessa produkter.
- Många tekniker kan användas i syfte att skada människor, företag, myndigheter och infrastruktur.

O

Möjligheter

- Teknikerna utvecklas i snabb takt och kommer bidra till att människor får en enklare vardag. Bland annat genom snabbare nätverk och uppkopplade föremål.
- Verksamheter, både inom privat och offentlig sektor, får med hjälp av olika tekniker mer effektiva och automatiserade processer, säkrare system och avancerad datainsamling som ger nya affärsmöjligheter.

T

Hot

- Många tekniker innebär stora risker kopplat till integritet.
- Illasinnat utnyttjande av teknikerna kan ge förödande konsekvenser för både enskilda individer, verksamheter och samhället i stort, ett exempel på detta är när stora mängder lagrade data används av illvilliga aktörer.
- Attackerna blir allt mer sofistikerade och långsiktiga, för att kunna hantera detta krävs kontinuerligt ökade resurser.

S

Styrkor

- Sverige vill vara bäst i världen på att använda digitaliseringens möjligheter och har därför tagit fram en digitaliseringsstrategi som ska bidra till att hela landets befolkning har förtroende för och tar del av det digitaliserade samhället.
- Sverige är idag ett av världens mest digitaliserade länder med en befolkning som har en stor digital mognad och teknikkunskap.
- Cybersäkerhet kopplat till samhällets digitalisering har fått ett lyft och större uppmärksamhet de senaste åren.

O

Möjligheter

- Befolkningens utvecklade syn på digitalisering bidrar till att det finns många personer som kan testa nya produkter, en öppenhet för ny teknik skapar många möjligheter för företag verksamma inom området.
- Att Sverige är ett digitaliserat land ger oss ett försprång och möjligheter att klara av svåra situationer som kan uppstå, vilket coronapandemin varit ett exempel på, där övergång till distansarbete fungerat väl.

W

Svagheter

- Som ett av världens mest digitaliserade länder blir Sverige också en måltavla för cyberangrepp.
- Eftersom Sverige levt med digitalisering under en lång tid har vi skapat vanemönster som bland annat innebär att vi delar med oss av mycket personlig information utan att fundera över säkerhetsaspekter.
- Det räcker ofta att endast en aktör har säkerhetsbrister för att flera andra aktörer eller individer i samhället ska drabbas.
- Att lägga pengar på säkerhet kan ibland vara svårt att motivera, då konsekvenser synliggörs först när pengar inte investerats i säkerhet.

T

Hot

- Det finns mycket på samhällsnivå som är skyddsvärt och kan utsättas för angrepp, Sverige behöver därför klara av att skydda sig mot både vardagliga incidenter och större angrepp.
- Många av samhällets små och medelstora företag är inte medvetna om vad ett angrepp skulle innebära och inte heller hur de kan skydda sig mot angrepp.
- Idag bygger många samhällsviktiga funktioner på digitala informationssystem, vilket innebär säkerhetsrisker eftersom stora mängder känslig information finns tillgängligt digitalt.

SWOT - Människans roll och kompetensutveckling

S

Styrkor

- Många åtgärder genomförs idag för att höja individers säkerhetsmedvetenhet, både på nationell nivå som når ut till många, men också på företag och genom olika myndigheter.
- Insikten om individens roll har ökat under de senaste åren.

O

Möjligheter

- Utöka befolkningens säkerhetsmedvetenhet genom att exempelvis börja utbilda redan i grundskolan, erbjuda fler kurser som alla Sveriges invånare kan ta del av och fler utbildningstillfällen på svenska arbetsplatser.
- Genom att mer uppmärksamhet läggs på säkerhet kan också intresset för området öka och bidra till att fler personer vill utbilda sig eller arbeta inom området.

W

Svagheter

- Säkerhetsmedvetenheten i Sverige är generellt sett låg och behöver höjas.
- Människan är ofta den svagaste länken och orsaken till att incidenter inträffar.
- Människan är bekväm av sig, vilket skapar säkerhetsrisker, exempelvis genom att en person lägger sitt lösenord under tangentbordet eller inte använder skärmskydd.

T

Hot

- Låg säkerhetsmedvetenhet hos individer kan leda till att incidenter inträffar som drabbar både enskilda individer, men också verksamheter.
- Säkerhetsmedvetenhet och kompetensutveckling på individnivå ses just nu som en av de största utmaningarna inom cybersäkerhetsområdet och det kan innebära stora risker framöver om inte säkerhetsmedvetenheten hos befolkningen höjs.

S

Styrkor

- ▶ Många högt rankade universitet i Sverige med möjlighet och kompetens för att kunna forska inom cybersäkerhet.
- ▶ Existerande starka nationella och regionala nätverk med hög innovationsförmåga.
- ▶ Innovationsmiljöerna inom ramen för SISP, som kan stötta startups och scaleups.

W

Svagheter

- ▶ Få utbildningar inom cybersäkerhet.
- ▶ Hög tröskel för att börja arbeta med IT-säkerhet då det ofta kräver erfarenhet.
- ▶ Cybersäkerhet upplevs som svårt och tekniskt, bredden inom området synliggörs inte.

O

Möjligheter

- ▶ Växande antal nationella och regionala projekt och initiativ inom cybersäkerhet.
- ▶ Utökad samverkan mellan näringsliv, utbildning och offentlig sektor för att minska kompetensbristen.
- ▶ Ökade forskningsanslag till cybersäkerhetsområdet.

T

Hot

- ▶ Internationell konkurrens om kompetens inom cybersäkerhet.
- ▶ Behovet av kompetens inom cybersäkerhet ökar snabbare än ny kompetens tillkommer på marknaden.
- ▶ Hög konkurrens om forskningsanslag inom cybersäkerhet.
- ▶ Bristande cybersäkerhetsarbete bland små- och medelstora företag.



Förslag på vidare studier

Förslag på vidare studier

Genomgående för den kartläggning som utförts är att det finns en enorm bredd i vad som ingår i cybersäkerhet, vilket också innebär att det finns flera förslag på vidare områden att undersöka. Dels hade det varit av intresse att avgränsa ytterligare och undersöka vissa aspekter inom cybersäkerhet närmare, till exempel kopplat till vissa tekniker och integritetsfrågor. Det skulle exempelvis kunna handla om säkerhet och integritetsfrågor i trådlösa system, såsom uppkopplade fordon, eller hur information i applikationer för välmående och hälsa ska behandlas på ett säkert sätt. Ett annat intressant område är att studera cybersäkerhet inom ett begränsat antal olika branscher. Vidare kan det vara av intresse att undersöka hur cybersäkerhet kan lyftas på en samhällsnivå och höja medvetenheten hos varje individ, och hur en sådan informationsinsats skulle kunna genomföras.

Respondenterna lyfter genomgående människan som den största risken, eftersom en människa med tillgång till ett system kan göra skada oavsett hur säkert systemet är. Här anser flera respondenter att det krävs insatser och att det finns mycket forskning att bedriva. Att designa cybersäkra system handlar om mer än tekniken, det är minst lika viktigt att de är användarvänliga för att det ska bli svårt att göra fel. Hur den tekniska säkerheten ska fånga upp den mänskliga faktorn blir därmed ett intressant område för vidare studier.

Avslutningsvis nämns också riskanalys som en grundförutsättning för ett bra cybersäkerhetsarbete av respondenterna. Hur en sådan riskanalys genomförs på bästa sätt är ett område där det finns ett stort behov av utökade studier. Det kan handla om att undersöka om det går att skapa en generell standard för riskanalys, vilka kvantitativa mått som kan användas eller hur cybersäkerhetsrisker kan prissättas.

Referenser

Respondenter

Avén, Annika; Ansvarig för Cyberförsvar på SOFF. Intervju 19 maj 2020.

Bergling, Martin; Koordinator på RISE för den nationella innovationsnoden för cybersäkerhet. Intervju 18 maj 2020.

Blom, Rolf, Senior forskare på RISE enhet för Cybersäkerhet. Intervju 18 maj 2020.

Fischer-Hübner, Simone; Professor i datavetenskap på Karlstads universitet. Intervju 22 maj 2020.

Fogelström Eva; Head of Security Research på Ericsson. Intervju 10 juni 2020.

Hallberg, Jonas; Enhetschef för informationssäkerhet och IT-arkitektur på FOI. Intervju 19 maj 2020.

Hell, Martin; Universitetslektor vid Nätverk och säkerhet på Lunds tekniska högskola. Intervju 19 maj 2020.

Holmberg, Mårten; Business Developer Digital på Blue Science Park. Intervju 10 juni 2020.

Holmgren, Åke; Chef över avdelningen för Cybersäkerhet och säkra kommunikationer på MSB

Jogenfors, Jonathan; Senior IT-säkerhetskonsult på Atea. Intervju 18 maj 2020.

Johnsson, Tore; VD på Luleå Science Park. Intervju 4 juni 2020.

Jonsson, Christian; Senior Director på Saab Cybersecurity. Intervju 10 juni 2020

Karström, Andreas; CTO på Link22. Intervju 10 juni 2020

Kronander, Torbjörn; VD på Sectra. Intervju 26 maj 2020.

Landberg, Fredrik; VD på Sylog Öst. Intervju 11 juni 2020.

Larsson, Erik G.; Professor i kommunikationssystem vid Linköpings universitet. E-mail 23 juni 2020.

Miranda, Lena; VD på Linköping Science Park. Intervju 22 juni 2020.

Oehme, Richard; Ordförande för SOFF:s cybergrupp. Intervju 19 maj 2020.

Sabelfeld, Andrei; Professor i webb- och mjukvarusäkerhet på Chalmers. Intervju 26 maj 2020.

Stensby, Ola; Programansvarig Security Arena vid Lindholmen Science Park. Intervju 26 maj 2020.

Litteratur

1. Digitaliseringsrådet 2018, *En lägesbild av digital trygghet*, dnr: 18-323, Oktober, 2018. [Tillgänglig: <https://digitaliseringsradet.se/media/1131/laegesrapport-digital-trygghet-klar-20.pdf>]
2. European Commission 2020, *Digital Economy and Society Index (DESI) 2020*.
3. D. Soumitra och B. Lanvin, *The Network Readiness Index 2019: Towards a Future-Ready Society*, Portulans Institute and WITSA, mars 2020. [Tillgänglig: <https://networkreadinessindex.org/wp-content/uploads/2020/03/The-Network-Readiness-Index-2019-New-version-March-2020.pdf>]
4. International Telecommunication Union, *Global Cybersecurity Index (GCI) 2018, 2019*. [Tillgänglig: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf]
5. PwC, *Nordic Cyber Crime Survey 2020: Det digitaliserade Sverige – så in i Norden säkert?*, 2020. [Tillgänglig: https://info.pwc.se/hubfs/CybSec_Nordic_CyberCrime-Survey_2020_A4L_FINAL.pdf?utm_campaign=Cyber%20%7C%20Nordic%20Cyber%20Crime&utm_medium=e-mail&_hsmi=82780300&_hsenc=p2ANqtz-UrsDHCKI6gNMCxosk5M5QxXL-2WvrHfdtuT_8LD0xKzWsRT6vtYjl4fpv-loJi0hbdMuA4u3ynbD20XT8b5mMfKRh-VMSQ&utm_content=82780300&utm_source=hs_automation]

6. Regeringskansliet, *Regeringen inleder arbetet med att inrätta nationellt cybersäkerhetscenter*, <https://www.regeringen.se/pressmeddelanden/2019/09/regeringen-inleder-arbetet-med-att-inratta-nationellt-cy-bersakerhetscenter/>, hämtad 21 juni 2020.
7. Teknikföretagen, Swedish ICT Research, IF metall m.fl. *Nationell forsknings- och innovationsagenda: Civil säkerhet*, 2011. [Tillgänglig: <http://www.security-link.se/wp-content/uploads/2014/10/sakerhet-sagenda2011.pdf>]
8. Markets and Markets. *Cybersecurity Market by Solution (IAM, Encryption, UTM, Antivirus/Antimalware, Firewall, IDS/IPS, Disaster Recovery, and DDOS Mitigation), Service, Security Type, Deployment Mode, Organization Size, Industry Vertical, and Region - Global Forecast to 2023*, <https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html>, hämtad 21 juni 2020.
9. Fortune Business Insight, *Cyber Security Market Size, Share & Industry Analysis, By Solution (Network Security, Cloud Application Security, End-point Security, Secure Web Gateway, Internet Security), By Deployment Type (Cloud and On Premise), By Enterprise Size (Small & Medium Enterprise and Large Enterprise), By End-Use (BFSI, IT and Telecommunications, Retail, Healthcare, Government, Manufacturing) and Region Forecast, 2020-2027*, <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165>, hämtad 21 juni 2020.
10. KPMG, *Key cyber risks for banks during COVID-19*, <https://home.kpmg/xx/en/home/insights/2020/05/key-cyber-risks-for-banks-during-covid-19.html>, hämtad 21 juni 2020.
11. Avdelningen för cybersäkerhet och säkra kommunikationer, *Öka motståndskraften mot ransomware: Rekommendationer rikta- de till it-personal, beslutsfattare respektive användare inom hälso- och sjukvårdssektorn*, Myndigheten för samhällsskydd och beredskap, ärendenr: MSB2020-08976-1, 9 juni 2020. [Tillgänglig: <https://www.msb.se/contentassets/310347bfa8424522a-7d96e79156faa2a/pdf-rekommendation-er-oka-motstandskraften-mot-ransom-ware-juni2020.pdf.pdf>]
12. S. Walker, *CYBER-INSECURITIES? A guide to the UN cybercrime debate*, Global Initiative Against Transnational Organized Crime, mars 2019. [Tillgänglig: <https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cyber-crime-in-the-UN-01Mar1510-Web.pdf>]
13. World Economic Forum, *The Global Risks Report 2019*, 14th Edition, 2019. [Tillgänglig: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf]
14. McAfee och CSIS, *Economic Impact of Cybercrime - No Slowing Down*, februari 2018. [Tillgänglig: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cyber-crime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAM-PAIGN_2018_02_21&utm_medium=email]
15. IC3, *2019 INTERNET CRIME REPORT*, FBI, 2019 [Tillgänglig: https://pdf.ic3.gov/2019_IC3Report.pdf]
16. Regeringskansliet, *Regeringen inleder arbetet med att inrätta nationellt cybersäkerhetscenter*, <https://www.regeringen.se/pressmeddelanden/2019/09/regeringen-inleder-arbetet-med-att-inratta-nationellt-cy-bersakerhetscenter/>, hämtad 21 juni 2020.
17. SVT, *Transportstyrelsens it-affär: Detta har hänt*, <https://www.svt.se/nyheter/inrikes/transportstyrelsens-sakerhetsskan-dal-detta-har-hant>, hämtad 21 juni 2020.
18. SVT, *2,7 miljoner inspelade samtal till 1177 Vårdguiden helt oskyddade på internet*, <https://www.svt.se/nyheter/inrikes/2-7-miljoner-inspelade-samtal-till-1177-varldguiden-helt-oskyddade-pa-internet>, hämtad 21 juni 2020.
19. Vinnova, *RISE Cyber Range*, <https://www.vinnova.se/en/p/rise-cyber-range/#:~:text=RISE%20Cyber%20Range%20will%20be.and%20environments%20for%20practical%20exercises>, hämtad 21 juni 2020.
20. FOI, *CRATE - Cyber Range And Training Environment*, <https://www.foi.se/en/foi/resources/crate---cyber-range-and-training-environment.html>, hämtad 21 juni 2020.

21. Säkerhets- och försvarsföretagen, *Cyberförsvar - åtta förslag ur ett marknadsperspektiv*, <https://soff.se/vara-fragor/cyberforsvar/>, hämtad 21 juni 2020.
22. Teknikföretagen, *Cybersäkerhet*, <https://www.teknikforetagen.se/branschfragor/digitalisering/cybersakerhet/>, hämtad 21 juni 2020.
23. Accenture security och Ponemon Institute, *The cost of cybercrime: Ninth annual cost of cybercrime study*, 2019. [Tillgänglig: <https://www.accenture.com/acnmedia/PDF-96/Accenture-2019-Cost-of-Cyber-crime-Study-Final.pdf#zoom=50>]
24. Teknikföretagen, *Cyberhoten: Så ser hotbilden och attackerna ut mot svenska teknikföretag*, 2020. [Tillgänglig: <https://www.teknikforetagen.se/globalassets/i-debatten/publikationer/cybersakerhet/cyberhoten-mot-svenska-teknikforetag.pdf>]
25. Trend Micro, *The New Norm: Trend Micro Security Predictions for 2020*, 2019. [Tillgänglig: <https://documents.trendmicro.com/assets/rpt/rpt-the-new-norm-trend-micro-security-predictions-for-2020.pdf>]
26. PwC, *Nordic Cyber Crime Survey 2020: Det digitaliserade Sverige – så in i Norden säkert?*.
27. FOI, *Kinas industriella cyberspionage*, memonr: FOI Memo 6698, 2019-03-22.
28. Arbetsförmedlingen, Ekobrottsmyndigheten, Försäkringskassan, Polismyndigheten m.fl., *Myndighetsgemensam lägesbild om organiserad brottslighet*, dnr: A457.772/2019, 2019-09-27.
29. Teknikföretagen, *Cyberhoten: Så ser hotbilden och attackerna ut mot svenska teknikföretag*.
30. Björk, Mikael, *Europol varnar: "Bedrägerierna har blivit allt mer aggressiva"*, Dagens Industri, 2019-02-17.
31. Avdelningen för cybersäkerhet och säkra kommunikationer, *Öka motståndskraften mot ransomware: Rekommendationer rikta- de till it-personal, beslutsfattare respektive användare inom hälso- och sjukvårdssektorn*.
32. FRA, FMV, MSB, Polisen och Säpo, *Cybersäkerhet i Sverige - Hot, metoder, brister och beroenden*, 2020 [Tillgänglig: https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/nyhetsdokument/rapport_cybersakerhet_hot-metoderbrister---kopia.pdf]
33. Säkerhetspolisen, Årsbok, 2019. [Tillgänglig: <https://www.sakerhetspolis-en.se/download/18.a5cd4be16df-d84e1716a5/1585209341505/Arsbok2019.pdf>]
34. FOI, *Kinas industriella cyberspionage*.
35. Teknikföretagen, *Cyberhoten: Så ser hotbilden och attackerna ut mot svenska teknikföretag*.
36. PwC, *Nordic Cyber Crime Survey 2020: Det digitaliserade Sverige – så in i Norden säkert?*.
37. Säkerhets- och försvarsföretagen, *Policy PM: Kryptosystem – ett för Sverige väsentligt säkerhetsintresse*, juni 2018. [Tillgänglig: <https://soff.se/wp-content/uploads/2018/06/Policy-PM-Krypto.pdf>]
38. Prop. 2017/18:1 *Utgiftsområde 6: Försvar och samhällets krisberedskap*, Stockholm: Regeringen. [Tillgänglig: <https://www.regeringen.se/4a65d0/contentassets/79f6d-27416794f0bb146c792e02b65fc/utgiftsomrade-6-forsvar-och-samhallets-krisberedskap.pdf>]
39. Säkerhets- och försvarsföretagen, *Policy PM: Kryptosystem – ett för Sverige väsentligt säkerhetsintresse*.
40. MSB, *Samlad informations- och cybersäkerhetshandlingsplan 2019–2022*, mars 2020. [Tillgänglig: <https://rib.msb.se/filer/pdf/29020.pdf>]
41. V. Hedtjärn Swaling och J. Johansson, *NCS3 Studie – IoT-relaterade risker och strategier*, rapportnr: 4591, april 2018. [Tillgänglig: <https://www.msb.se/RibData/Filer/pdf/28550.pdf>]
42. Ibid.
43. Department of Homeland Security 2016. *Strategic principles for securing the Internet of Things (IoT)*. Version 1.0 November 15, 2016.

44. V. Hedtjärn Swaling och J. Johansson, *NCS3 Studie – IoT-relaterade risker och strategier*.
45. Ibid.
46. Ibid.
47. Ibid.
48. Ibid
49. M. Brundage, S. Avin, J. Clark m.fl., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, Future of Humanity Institute, University of Oxford m.fl., februari 2018. [Tillgänglig: <https://img1.wsimg.com/blobby/go/3d-82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217>]
50. Ibid.
51. Infrastrukturdepartementet, *Uppdrag att kartlägga användningen av artificiell intelligens respektive analys av stora datamängder i Sverige*, Stockholm: Regeringen, 27 jun 2019. [Tillgänglig: <https://www.regeringen.se/4adadd/contentassets/d6db8d21a2e14a20ae8fff715a996217/uppdrag-att-kartlagga-anvandningen-av-artificiell-intelligens-respektive-analys-av-stora-datamangder-i-sverige.pdf>]
52. RISE, *Så kan AI och cybersäkerhet stärka varandra*, <https://www.ri.se/sv/berattelser/sa-kan-ai-och-cybersakerhet-starka-varandra>, hämtad 21 juni 2020.
53. RISE, *Så kan AI och cybersäkerhet stärka varandra*, <https://www.ri.se/sv/berattelser/samarbete-okad-cybersakerhet>, hämtad 21 juni 2020.
54. E. Amselem, P. Svenson och L. Gisslén, *Kvantinformatik - teknisk prognos*, FOI, rapportnr: FOI-R--3920--SE.
55. Säkerhets- och försvarsföretagen, *Policy PM: Kryptosystem – ett för Sverige väsentligt säkerhetsintresse*.
56. Chalmers, *Nu startar bygget av en svensk kvantdator*, <https://www.chalmers.se/sv/nyheter/Sidor/Nu-startar-bygget-av-en-svensk-kvantdator.aspx>, 27 januari 2020, hämtad 21 juni 2020.
57. Ericsson, *This is 5G*, 2018. [Tillgänglig: https://www.ericsson.com/4a3114/assets/local/newsroom/media-kits/5g/doc/ericsson_this-is-5g_pdf_v4.pdf].
58. Ericsson, *5G network security is national security*, <https://www.ericsson.com/en/blog/2020/4/5g-network-security-is-national-security>, hämtad 21 juni 2020.
59. J. Sullivan och R. Lucas, *5G Cyber Security: A Risk-Management Approach*, London: Royal United Services Institute (RUSI), februari 2020 [Tillgänglig: https://rusi.org/sites/default/files/20200602_5g_cyber_security_final_web_copy.pdf]
60. Regeringskansliet, *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi*, dnr: N2017/03643/D, 2017 [Tillgänglig: https://www.regeringen.se/49adea/contentassets/5429e024be6847fc907b786ab954228f/digitaliseringsstrategin_slutlig_170518-2.pdf]
61. Ibid.
62. Säkerhets- och försvarsföretagen, *Så kan vi säkra Hur kan vi säkra Kompetensförsörjningen inom cybersäkerhet*, 2018. [Tillgänglig: <https://soff.se/wp-content/uploads/2018/12/Cyberkompetens.pdf>]
63. MSB, *Samlad informations- och cybersäkerhetsbehandlingsplan 2019–2022*.
64. MSB, *Årsrapport itincidentrapportering 2019 - Vad har hänt, varför har det hänt, och vad ska göras för att undvika att det händer igen?*, april 2020. [Tillgänglig: <https://www.msb.se/siteassets/dokument/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/it-incidentrapportering/arsrapport-it-incidentrapportering-2019.pdf>]
65. Säkerhets- och försvarsföretagen, *Så kan vi säkra Hur kan vi säkra Kompetensförsörjningen inom cybersäkerhet*.
66. AI Innovation Sweden, *About AI Innovation of Sweden*, <https://www.ai.se/en/about>, hämtad 21 juni 2020.
67. Regeringskansliet, *Regeringen inleder arbetet med att inrätta nationellt cybersäkerhetscenter*.

68. Vinnova, *Svensk Nod för att Accelerera Innovation & Forskning inom Cybersäkerhet*, <https://www.vinnova.se/p/svensk-nod-for-att-accelerera-innovation-forskning-inom-cybersakerhet/>, dnr: 2019-05214, hämtad 21 juni 2020.
69. FOI, *CRATE - Cyber Range And Training Environment*.
70. Vinnova, *RISE Cyber Range*, dnr: 2019-05214, <https://www.vinnova.se/en/p/rise-cyber-range/>, hämtad 21 juni 2020.
71. Säkerhets- och försvarsföretagen, *Så kan vi säkra ~~Hur kan vi säkra~~ Kompetensförsörjningen inom cybersäkerhet*.
72. Säkerhets- och försvarsföretagen, *"Vilka kompetenser söker Sveriges säkerhets- och försvarsföretag?"*, juni 2020. [Tillgänglig: https://soff.se/wp-content/uploads/2020/06/Cyberkompetens_rapport-200602.pdf]
73. Säkerhets- och försvarsföretagen, *Så kan vi säkra ~~Hur kan vi säkra~~ Kompetensförsörjningen inom cybersäkerhet*.
74. MSB, *Samlad informations- och cybersäkerhetshandlingsplan 2019–2022*.
75. Säkerhets- och försvarsföretagen, *Så kan vi säkra ~~Hur kan vi säkra~~ Kompetensförsörjningen inom cybersäkerhet*, s. 8.
76. MSB, *Samlad informations- och cybersäkerhetshandlingsplan 2019–2022*.
77. J. Ingemarsdotter, D. Eidenskog och V. Hedtjärn Swaling, *Vilse i Lasagnen? - En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur*, FOI, rapportnr: FOI-R--4814--SE, 2020.
78. Sweden ICT, *About Us*, <https://www.swedenict.se/about-us/>, hämtad 21 juni 2020.
79. Swedish Incubator and Science Parks, *Om swedish incubators science parks*, <https://www.sisp.se/om-swedish-incubators-science-parks>, hämtad 21 juni 2020.
80. Fortune Business Insight, *Cyber Security Market Size, Share & Industry Analysis, By Solution (Network Security, Cloud Application Security, End-point Security, Secure Web Gateway, Internet Security), By Deployment Type (Cloud and On Premise), By Enterprise Size (Small & Medium Enterprise and Large Enterprise), By End-Use (BFSI, IT and Telecommunications, Retail, Healthcare, Government, Manufacturing) and Region Forecast, 2020-2027*
81. Nasdaq, *Cybersecurity: Industry Report & Investment Case - HUR*, 2020. [Tillgänglig: https://indexes.nasdaqomx.com/docs/HUR_Research.pdf]