REDAKTÖRER
JOAKIM LILJEBERG OCH PATRIK OKSANEN

SVEKET MOT CYBERSÄKERHETEN

FORES

REDAKTÖRER
JOAKIM LILJEBERG OCH PATRIK OKSANEN

SVEKET MOT CYBERSÄKERHETEN

FORES

Sveket mot cybersäkerheten

Redaktörer: Joakim Liljeberg och Patrik Oksanen

Fores
Sveavägen 59, 113 59 Stockholm
info@fores.se · www.fores.se

1:a upplagan, 1:a tryckningen
Grafisk form: Epique studio
Tryck: Spektar Bulgaria 2022

ISBN: 978-91-87379-87-1

FORES

Innehållsförteckning

Förord

Natten till den 24 februari 2022 förnyade Ryssland sitt anfall på grannlandet Ukraina med full styrka. I skrivande stund pågår kriget fortfarande. Det som det inte skrivs lika mycket om i rapporteringen av kriget är den strid som utspelas på internet. Enligt en nyligen publicerad rapport från Microsoft så ingick även kraftfulla cyberattacker från rysk sida vid offensivens inledning. Ukraina klarade av denna attack genom att sprida ut sin digitala infrastruktur runt i Europa. Det digitala cyberkriget mellan de stridande parterna pågår i skrivande stund.

Natten till torsdagen den 16 december 2021 gjorde en främmande person intrång i Kalix kommuns server och krypterade all data. Det medförde allvarliga konsekvenser för hela verksamheten och en kostnad på över två miljoner kronor. Det handlade om en så kallad ransomware-attack och i stället för att betala lösensumman valde Kalix kommun att släcka servrarna och genomföra ett stort återställningsarbete. Detta är ett av flera exempel på de senaste årens IT-relaterade brott som har drabbat organisationer, företag och myndigheter i Sverige.

Det visar att ju mer digitaliserat vårt samhälle blir desto större sårbarheter bygger vi och därmed ökar behovet av ett nationellt gediget cybersäkerhetsarbete. Tyvärr visade Fores egna undersökning att missnöjet med statens insatser för cybersäkerheten är omfattande, med genomgående låga betyg. Allra lägst betyg får myndighetsstödet samt tillgången till utbildad personal. Det nya nationella Cybersäkerhetscentret har ännu inte levererat en mätbar effekt bland verksamhetsledarna enligt undersökningen. Allt som staten är inblandad i får låga betyg, det gäller tillgång på utbildad personal, myndighetsstöd, lagstiftning och koordinering.

Staten sviker cybersäkerheten är en bok för dig som vill läsa om hur det svenska cyberförsvaret ser ut idag och hur det borde se ut, samt vad man ska vara uppmärksam på som verksamhetsledare. Kapitlen är skrivna av cybersäkerhetsexperter tillsammans med säkerhetsanalytiker, flera har erfarenheter från den svenska underrättelsetjänsten.

Jag vill härmed önska er en god läsning och en önskan om att hålla ett vaksamt öga även på den digitala sidan i er vardag. Alla har lås på dörrarna hemma, vissa har larm och några har ett säkerhetsskåp i källaren, ditt digitala hem borde innehålla minst lika många lås och larm. Tänk

igenom vad du gör på internet och fundera på om du inte ska börja byta lösenord lite oftare, du också.

Med vänliga hälsningar,

Ulrica Schenström, vd tankesmedjan Fores, Stockholm, Augusti 2022

Staten sviker cybersäkerheten

av Joakim Liljeberg och Patrik Oksanen

Inledning

Att löner kan betalas ut, att betalkortet fungerar på Coop och att elektricitet och internet fungerar är något människor idag förväntar sig. Liksom att vår data ska vara trygg och skyddad och att företagets hemligheter inte ska kunna stjälas.

Sverige rankas som EU:s tredje mest digitaliserade land enligt EU-kommissionen.[1] Men EU använder sig av en definition av digitalisering som inte stämmer med andra internationella mätningar. Det finns en skillnad mellan att mäta datorisering och digitalisering. Olika mätningar mäter olika saker och enligt en mätning från OECD[2], som mäter digitalisering, hamnar Sverige sist. Enligt NRI-indexet är Sverige det land som är bäst på att ta tillvara på digitaliseringens möjligheter både 2019 och 2020.

1 https://www.regeringen.se/pressmeddelanden/2021/11/sverige-i-toppen-i-ny-ranking-over-eus-mest-digitaliserade-lander/

2 OECD (2020), "Digital Government Index: 2019 results", OECD Public Governance Policy Papers, No. 03, OECD Publishing, Paris, https://doi.org/10.1787/4de9f5bb-en

Network Readiness Index är sammanställt av tankesmedjan Portulans Institute, 2020 gjordes det i samverkan med FN-organet med UNESCO.[3]

Kontrasten till var Sverige hamnar när det gäller cybersäkerhet är närmast brutal. Sverige är sämre än grannländerna och hamnar i National Cyber Security Index 2021 på plats 43 av 160 länder.[4]

Samtidigt ökar hotbildernas komplexitet mot samhället. Främmande makter och kriminella grupperingar försöker på olika sätt exploatera våra svagheter för sina syften. Och attacker är inte hypoteser, utan en vardag. Redan 2018 uttryckte sig dåvarande SAAB-vd:n Håkan Bushke sig dramatiskt: *”Jag anser att vi är ockuperade. Jag anser att det är naivt att inte förstå att utländska organisationer försöker influera vår livsstil i denna stund.”*

Varje dag sker angreppen från främmande makter, många gånger misslyckas de, andra gånger blir konsekvenserna omfattande. Ibland kommer effekterna för att någon annan i IT-kedjan drabbas. När den amerikanska Kaseya drabbades av en ransomware-attack från ryska hackare fick åtta hundra COOP-butiker i Sverige stänga på grund av att kassasystemet slogs ut. Senare samma år drabba-

3 https://www.regeringen.se/pressmeddelanden/2020/10/sverige-etta-i-varlden-pa-digital-samhallsomvandling/

4 https://www.svd.se/a/nAk1Jx/sakerhetsexpert-bra-att-it-attacken-hande#:~:text=Varningarna%20om%20Sveriges%20bristande%20cybers%C3%A4kerhet,i%20National%20cyber%20security%20index

des Kalix kommun av ett angrepp som lamslog kommunens verksamhet och stoppade utbetalningen av den så viktiga decemberlönen.

Kinas omfattande datastölder beräknas kosta enbart den amerikanska ekonomin någonstans mellan 250 miljarder dollar och uppemot 600 miljarder dollar enligt en studie från amerikanska justitiedepartementet. Financial Times beskriver utvecklingen efter studien som accelererande, teknikrivaliteten mellan Kina och USA ökar och i takt med den ökar Kina intensiteten att komma över amerikanska immateriella tillgångar. Även Ryssland genomför aktiviteter riktade mot svenska intressen.[5] Detta förtydligas ytterligare av SÄPO som skriver i deras årsrapport 2021[6] att Ryssland bedriver säkerhetshotande verksamhet mot Sverige bland annat genom cyberspionage.

Cyberangrepp kan användas också för påverkansoperationer, som stölden av Demokraternas e-post som banade vägen för den debatt som ledde Donald Trump till Vita Huset.

Sverige kliver nu in i en extra känslig period, skör regeringsbildningsperiod efter ett val. Detta sammanfaller med Sveriges ansökan om Natomedlemskap vilket gör att Sverige kommande månader

5 Årsöversikt 2020, MUST
6 Säkerhetspolisen Årsbok, 2021

riskerar att vara extra utsatt.

Cyberangrepp är också numera en integrerad del av krigföringen. I en rapport från Microsoft om kriget i Ukraina från i april 2022 pekas 37 destruktiva cyberangrepp mot Ukraina ut under krigets inledning.[7]

En annan fråga är suveränitet över data och hur kan man garantera att känslig personlig data inte hamnar i auktoritära staters händer, exempelvis hur olika medborgare rör sig i samhället. Här finns omfattande risker med att överlämna information frivilligt till kinesiska och ryska appar som sedan i sin tur förmedlar informationen vidare till respektive lands myndigheter.[8]

Ett system är inte starkare än människan bakom det, och det är ytterligare en säkerhetsrisk. Både att få tag på kvalificerad arbetskraft, men också att undvika att arbetsplatsen inte drabbas av medarbetare som direkt eller indirekt tvingas arbeta för främmande makt. Det här har säkerhetspolis i olika länder varnat för vid olika tillfällen.

Den svenska cybersäkerheten har varit omdiskuterad i stora kretsar. Den cyberförmåga och kompetensbrist som Sverige har mäts av internationella institut och organisationer. Vi är inte ensamma om att konstatera att det råder en stor kompetensbrist

7 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
8 https://www.ft.com/content/c02083b5-8a0a-48e5-b850-831a3e6406bb

inom cybersäkerhet, framförallt inom de offentliga verksamheterna. Sverige inrättade ett nationellt cybersäkerhetscenter under slutet av 2020, för att utvecklas fram till 2023.

Jämförelsevis inrättade USA sitt Cyber Command 2010 och under 2008 inrättade NATO sitt Cooperative Cyber Defence Centre of Excellence i Estland (CCD COE). Sverige är sedan några år tillbaka en bidragande partner av detta försvarscentrum. En av CCD COEs nyckelfunktioner är att bedriva övningen ”Locked Shields” som är en av världens främsta och största övningar inom cybersäkerhet. Här placerar sig Sverige väldigt bra internationellt sett då Sverige var det vinnande laget under övningen 2021.

Under den senare delen av 2000-talet har behovet av en kraftfull cyberförmåga ökat också i Sverige. Främmande makt har kraftigt utökat sina möjligheter till både försvar och möjligheter till skada. För att vi själva ska kunna avgöra hur den svenska förmågan placerar sig internationellt får vi vända oss till internationella undersökningar för att se vår placering. Enligt Internationella Teleunionens Global Cybersecurity Index (2020)[9] hamnar Sverige på plats 26, precis efter Egypten, Indonesien och Vietnam. Men enligt Comparitechs undersökning från 2021[10] ham-

9 https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
10 https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

nar Sverige på andra plats, efter Danmark, som det cybersäkraste landet att bo i.

För att Sverige och våra allierade ska kunna möta ett framtida digitalt hot mot våra intressen kommer vi behöva utbildad personal. Det råder en kollektiv kompetensbrist på cybersäkerhetsområdet inom Europa. Detta visar EU:s cybersäkerhetsbyrå The European Union Agency for Cybersecuritys (ENISA) rapport, Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education[11], som publicerades i slutet av 2021. Noterbart är att ENISA konstaterar i rapporten att kompetensbristen är bestående över kommande år trots en fördubbling av antalet nyexaminerade under de kommande två till tre åren. Könsbalansen är också ett fortsatt problem, då endast 20 procent av de inskrivna studenterna är kvinnor. Bristen på personal gör att den offentliga sektorn har svårt att konkurrera i det löneläge som råder på arbetsmarknaden för cybersäkerhetsexperter.

Cybersäkerhetsområdet är stort, snabbt förändrligt och mycket krävande när det gäller både bevakning och kompetens. För att vi ska lyckas att försvara våra intressen även digitalt krävs det att vi ständigt utvärderar och förbättrar oss. Denna förstudie hoppas vi är ett led i den utvecklingen.

11 https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

Bakgrund

Detta arbete startade årskiftet 2021-2022 när ett samarbete inleddes mellan Microsoft Sverige och tankesmedjan Fores. Båda parter, från varsitt håll, var intresserade av cybersäkerhetsfrågan ur ett brett perspektiv men framförallt hur det ser ut i Sverige. Fores har en lång historia av att arbeta med digitaliseringens möjligheter och hot mot densamma. Redan under 2008 hade Fores ett uppmärksammat seminarium med tidigare FRA-anställda i panelen. Microsofts arbete med cybersäkerhet har varit en bärande och viktig del sedan bolaget startades och ser cybersäkerhet som sitt ansvar som globalt techföretag med sin verksamhet inom samhällets flesta sektorer.

Fores och Microsoft var intresserade av att närmare förstå det aktuella läget inom den svenska cybersäkerheten ute i verkamheter för att kunna bidra till utvecklingen. Microsoft har inte ingått bland de skribenter som tagit fram förstudie och denna bok, utan har bidragit finansiellt för att möjliggöra resurser till samarbetet. Fores har haft full frihet att formulera rapporten utifrån egna utgångspunkter, observationer och slutsatser. Detta arbete inleddes med en förstudie och aktuell nulägesanalys av verksamhetsledande personers bedömningar av läget. Det resulterade i produkten du läser i just nu,

en antologi där förstudien är ett delkapitel och där fem experter inom sitt fält skriver om den svenska cybersäkerheten och aspekter på densamma.

Undersökningen

Undersökningen har genomförts av den gröna och liberala tankesmedjan Fores. Syftet med undersökningen är att låta personer i ledande ställning inom olika branscher ge sin syn på både den egna verksamhetens cybersäkerhet och hela Sveriges cybersäkerhet.

Undersökningen har bestått av ett antal utskick via e-post med uppföljande telefonsamtal för att samla in svar från kvalificerade och verksamhetsledande personer. Sammanlagt har totalt hundra verksamhetsledare, inom både offentlig och privat regi, under anonymitet, svarat på enkäten.

Dessa personer svar har passerat genom ett insamlingsverktyg för att sedan sammanställas och analyseras. Vi valde att låta personerna placera sig och sin verksamhet inom en mängd olika fält för att enklare kunna jämföra samhällssektorer bland annat; offentlig förvaltning, energiförsörjning, hälso- och sjukvård samt omsorg, handel och industri, finansiella tjänster, information och kommunikation, livsmedel, skydd och säkerhet, socialförsäkringar, transport, försvar, kommunalteknisk

Fråga för fråga:

1

Totalbetyg för cybersäkerhet inom din samhällssektor	**3,3**

Den första frågan besvarades av samtliga respondenter. Det genomsnittliga svaret faller på 3,3. Noterbart är också att ingen har gett högsta betyg under denna fråga. Däremot har en respondent gett lägsta betyget 1. Sju respondenter har gett en 4.

2

Totalbetyg för cybersäkerheten i hela svenska samhället	**2,6**

Genomsnittet är 2,6 på denna fråga. Det måste ses som ett rejält underbetyg för svensk cybersäkerhet. Hälften av respondenterna ger betyget 2. Bara tre ger en 4. Ingen respondent har delat ut ett högsta eller lägsta betyg.

3

Tycker du att du som verksamhetsansvarig kan arbeta tillräckligt effektivt med cybersäkerhet?

3,1

Frågan besvarades med ett snitt på 3,1, med den största spridningen. En gav högsta betyg 5, en gav lägsta betyg 1, övriga fördelade sig mellan 2-4. Upplevelsen att inte kunna arbeta tillräckligt effektivt med cybersäkerhet illustrerar gapet mellan utmaningarna och de faktiska förutsättningarna.

4

Tycker du som verksamhetsansvarig att koordinering med andra aktörer kring cybersäkerhet fungerar?

2,8

Frågan besvarades med 2,8 i snitt vilket illustrerar cyberfrågornas ledningsproblem i Sverige. Ansvaret är fördelat på olika departement och myndigheter. Vilket gör att koordineringen blir svårare och det är ibland svårt att förstå vem som ansvarar för vad.

5

Tycker du som verksamhetsansvarig att nuvarande gällande lagstiftning täcker det nuvarande behovet?

2,7

Frågan besvarades med 2,7 i snitt, vilket illustrerar att lagstiftningen har svårt att följa med teknikutvecklingen.

6

Tycker du som verksamhetsansvarig att myndighetsstödet är tillfredsställande?

1,7

Enkätens lägsta betyg, 1,7. Myndighetsstödet i en komplicerad IT-djungel med splittrat ansvar upplevs som otillfredsställande av respondenterna. Läget är för många verksamhetsansvariga så frustrerande att hälften av respondenterna gav det absolut lägsta betyget 1. Ingen gav högre än 3.

7

Tycker du som verksamhetsansvarig att tillgång till utbildad personal är tillräcklig?

2,4

Här besvarade respondenterna med ett snitt på 2,4. Personalbristen var påtaglig fyra respondenter som

gav 1, nästan hälften gav 2 i betyg. Dock ska det noteras att tre respondenter gav 4 i betyg och en respondent 5. Det här kan indikera att personalbristen är värre i vissa sektorer än för andra. Lägst tillgång har offentlig förvaltning tätt följt av transporter.

8

Tycker du som verksamhetsansvarig att era egna säkerhetskontroller av personal är tillräckliga?

3,5

På sista frågan är snittet högst i undersökningen som landar på 3,5. Ens egna säkerhetskontroller litar de verksamhetsledande personerna på i ganska stor utsträckning. Men det finns betydande undantag. Fyra svarande gav 2 och en det lägsta betyget 1, medan hälften gav 4 eller 5 i betyg. Den bransch som tycker att de har till störst del otillräckliga säkerhetskontroller är transporter tätt följt av handel och industri.

9

Vad är viktigast att åtgärda för att stärka cybersäkerheten?

För kommentarer skrivna av respondenter se tabellverket i slutet av boken.

försörjning.

Totalt tio frågor ställdes i enkäten varav två inte handlade om betygsättning. Dessa två var den första och den sista. Den första frågan efterfrågade vilken sektor man tillhörde och den sista frågan (fråga 10) var frivillig och öppnade upp för egenformulerade svar i text. I betygsättningen har skalan varit mellan 1 och 5, där 1 är det lägsta och 5 är det högsta.

Samtliga respondenter har svarat på samtliga frågor, förutom fråga tio där endast åtta valde att besvara frågan.

Slutsatser

I svaren från de verksamhetsansvariga så blir Sveriges cybersäkerhetskris tydlig.

Av totalt åtta frågor riktar sig fyra till den egna organisationen och fyra till statens ansvar. Det är tydligt hur svaren skiljer sig. Snittet för de fyra frågor där staten bär ansvar ligger på 2,3 och där verksamhetsledaren själv kan påverka ligger snittet på 3,1.

Det är betyg som i sammanhanget får anses vara illavarslande låga, särskilt sett till den ökande och allt mer komplexa hotbilden. Betyget myndighetsstöd från staten som landar på 1,7 visar att Cybersäkerhetscentret hittills inte har gett någon effekt på verksamhetsledarnas upplevelser. Centrets har till

uppgift att:

- Koordinera arbetet för att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter.
- Förmedla råd och stöd avseende hot, sårbarheter och risker.
- Utgöra en nationell plattform för samverkan och informationsutbyte med privata och offentliga aktörer inom cybersäkerhetsområdet.

Cybersäkerhetscentret är under uppbyggnad, en uppbyggnad som genomförs under åren 2021-2023. Uppenbarligen går dock arbetet alldeles för långsamt för att leverera en mätbar effekt bland tillfrågade verksamhetsledare.

Den statliga delen av samhällets cyberförsvar levererar alltså inte i den utsträckning som verksamhetsledande personer förväntar sig. Frustrationen är också påtaglig över den för låga nivån.

Det finns en rad förslag som radas upp bland de som har besvarat undersökningen och som också har påtalats förut. Sverige bör bland annat:

- Förenkla, harmonisera och modernisera lagar och regler.
- Stärka myndigheternas informationsgivning till företagen

- Öka medvetandegraden och kunskapen hos anställda
- Ökade satsningar på utbildning samt en nationell cybersäkerhetsstrategi
- Aktiv stöttning från myndigheter

Vi vill vänligast och ödmjukast också påminna om att svarsfrekvensen är låg på enkäten med endast hundra svaranden. Därmed anser vi att den statistiska analysen för iakttas med försiktighet och måttfullhet. Vi ser detta som en trendmätning för vidare analys och diskussion än ett statistiskt underlag.

Försvaret av den svagaste länken

av Stefan Kristiansson

Informationssäkerhet, som omfattar konfidentialitet, tillgänglighet och korrekthet, kan inte hanteras isolerat utan måste ses i ett större sammanhang. Den säkerhetspolitiska utvecklingen i omvärlden och utvecklingen av vårt totalförsvar; inte minst behovet av att stärka det civila försvaret, vårt låga säkerhetsmedvetande, behovet av balans i säkerhetsarbetet samt principerna för vår krishantering är exempel på detta.

Vilka faktorer bör beaktas?

För det första; Sveriges säkerhetspolitiska läge har förändrats och försämrats under en längre period. Rysslands försök att påtvinga andra länder sin politiska vilja i strid med internationella konventioner och den europeiska säkerhetsordningen har fått omfattande konsekvenser. Ryssland använder både militära och icke-militära metoder för att nå sina mål.

Kinas ambitioner att utvecklas till en global stor-

makt påverkar också oss. Även om det geografiska avståndet är stort så är vi grannar i den digitala världen och Kina har under en lång period visat ett alltför närgånget intresse bland annat för vårt tekniska kunnande innovationer.

De svenska underrättelse- och säkerhetstjänsterna har under flera år varnat för att underrättelseverksamheten ökat mot vårt land. Enligt Säkerhetspolisen bedriver ett femtontal länder spionerи mot landet. Ryssland, Kina och Iran pekas ut[1]. Det är bra att man är så konkret när det gäller dessa tre aktörer och att man inte använder uttrycket ”främmande makt”. Risken är dock att fokus hamnar helt på de utpekade tre och att vi inte i tillräcklig grad skyddar oss mot de andra tolv.

Intrång i våra informationssystem torde vara det största, mest akuta och ökande underrättelsehotet. Det är flera aktörer som bedriver spionerи mot oss och man är till exempel ute efter information om våra säkerhetspolitiska överväganden, styrkor och framför allt svagheter i totalförsvaret, flyktingar som anses vara ett hot mot regimer samt vår tekniska kompetens. Underrättelsehotet har således, under de senaste åren, breddats både avseende antalet aktörer och vilken information som man är intresserad av.

1 Se Säkerhetspolisens årsböcker, exempelvis 2021.

Informationssäkerheten är naturligtvis av central betydelse för vårt totalförsvar. Utan internet och tillgång till vår samlade information så skadas landet svårt. Det kommer att drabba kritisk infrastruktur som hälso- och sjukvård, livsmedels-, drivmedels-, elförsörjning, kommunikationer, transporter mm. Medborgarna kommer att drabbas och Försvarsmakten kommer inte att kunna lösa sina uppgifter. I de två senaste försvarsbesluten har det gjorts stora och nödvändiga satsningar på det militära försvaret. Det är emellertid viktigt att dessa satsningar motsvaras av upprustning av det civila försvaret. Det finns idag en uppenbar risk att det uppstår en obalans i utvecklingen av totalförsvaret.

Risken för obalans i försvarsplaneringen har uppmärksammats även inom försvarsalliansen Nato och Generalsekreterare Jens Stoltenberg har i ett tal i Bratislava i oktober 2020 uttryckt sig på följande sätt:

> *”Having a strong military is fundamental to our security. But our military cannot be strong if our societies are weak. So our first line of defence must be strong societies. Able to prevent, endure, adapt and bounce back from whatever happens.”*[2]

2 Keynote speech by NATO Secretary General Jens Stoltenberg at the Global Security 2020 (GLOBSEC) Bratislava

För det andra; trots att de flesta medborgare i landet är medvetna om att det säkerhetspolitiska läget försämrats så har vi svenskar ett förhållandevis lågt säkerhetsmedvetande. Alltför få tänker på säkerhetsaspekter när man hanterar information som kan vara av betydelse för totalförsvaret eller för annan samhällsviktig verksamhet. Svenskar tenderar att vara naiva, överdrivet optimistiska och ha förhoppningar om att ingenting obehagligt kommer att inträffa. Krismedvetenhet är ingen stark känsla hos befolkningen i allmänhet och inte heller viljan att planera för det värsta.

En orsak till denna naivitet är att vi tycks leva i en tillvaro där man resonerar och agerar utifrån att antingen är det fred, höjd beredskap eller krig. Och eftersom det varken är höjd beredskap eller krig så är det fred. Alltså behöver vi inte tänka på säkerhetsfrågor. Vi är idag långt ifrån den säkerhetsmedvetenhet som fanns under andra världskriget och under det kalla kriget. Medvetenheten om att vi lever i en gråzon mellan fred och krig saknas hos många. Därmed är vi illa rustade för att möta hot i gråzonen.

Kombinationen av ett ökande säkerhetshot och spionerи mot landet och ett lågt säkerhetsmedvetande är illavarslande och borde hanteras med hög prioritet.

För det tredje; säkerhetsskydd består av informationssäkerhet, personalsäkerhet och fysisk säkerhet. Ett gott säkerhetsskydd uppnås först när det är balans mellan de tre områdena. När det diskuteras informationssäkerhet eller cybersäkerhet tycks man ofta koncentrera sig på de tekniska lösningarna och negligera det som rör de mänskliga aspekterna. Möjligen beror detta på att informationssäkerhet ofta hanteras av tekniker.

Personalsäkerhet handlar inledningsvis om en seriös rekryteringsprocess med ordentliga bakgrundskontroller för att förhindra att man anställer medarbetare som inte är pålitliga från säkerhetsskyddssynpunkt. Vidare handlar det om att informera och utbilda personal i säkerhetsrutiner, följa upp och kontrollera att dessa rutiner följs samt att vidta åtgärder om man upptäcker risker. Fysisk säkerhet handlar naturligtvis om att förhindra obehöriga att få tillgång till känslig information eller viktiga anläggningar och annan infrastruktur.

Obalans i säkerhetsskyddet uppstår till exempel när man i en hamn prioriterar byggande av stängsel och försummar informationssäkerhet och personalsäkerhet.

För det fjärde; Det är rimligt att anta att en aktör som vill påtvinga oss sin politiska vilja inriktar sig

mot den svagaste länken eller den kritiska sårbarheten i vårt totalförsvar. Det kan till exempel handla om att angripa viktiga samhällsfunktioner eller företag som sköter transporter eller levererar el, vatten, livsmedel och drivmedel. Men det kan också handla om att attackera kommuner eller infrastruktur såsom hamnar, flygplatser och förbindelser.

Den svagaste länken i totalförsvaret utgör i praktiken landets försvarsförmåga.

Den svenska krishanteringen styrs och genomsyras sedan många år tillbaka av ansvarsprincipen, likhetsprincipen och närhetsprincipen. I korthet innebär dess principer att den som har ett ansvar för verksamhet i fred också har ett ansvar vid kris. Under en kris ska verksamheten fungera på liknande sätt som i vardagen. Vidare ska en kris hanteras där den inträffar till exempel i en kommun eller region. Om man inte klarar av att hantera krisen så kan man få stöd av länsstyrelse eller av staten.

Vad innebär då detta för cybersäkerhetsarbetet? Risken är uppenbar att ansvaret för denna omfattande och komplexa fråga skjuts ner till nivåer som dels saknar insikt om problemet dels har bristande kompetens och resurser. Det finns naturligtvis också en risk att cybersäkerhetfrågan kommer långt ner på dagordningen medan upprätthållandet av äldrevård, skola, socialtjänst och annan samhälls-

service anses ha högre prioritet. Detta trots att dessa verksamheter till stor del är beroende av fungerande informationssystem.

Sveriges kommuner och regioner (SKR) gjorde under 2019 en omfattande kartläggning av kommunernas informationssäkerhetsarbete.[3] Samtliga Sveriges 290 kommuner tillfrågades om hur långt man kommit i sitt systematiska informationssäkerhetsarbete. Svarsfrekvensen var mycket god. Enkäten gav tydligt besked om att det finns en bred och djup förståelse av betydelsen av ett systematiskt informationssäkerhetsarbete. Samtidigt konstaterades betydande brister avseende styrning, ledning, avsatta medel och resurser för arbetets planering och genomförande samt en tydlig uppföljning av informationssäkerhetsarbetet.

Det framgår av rapporten att

> *”SKR ser sammantaget att informationssäkerhetsarbetet endast ges tillräckligt med uppmärksamhet vid en incident eller när risken för en incident blir uppenbar. Detta medför att kommunens ledning inte ser behovet och nyttan av ett proaktivt, systematiskt arbete med informationssäkerhet, vilket i sig innebär att resurser inte avsätts förrän olyckan redan inträffat.”* (sidan 5)

3 Kommunernas informationssäkerhetsarbete. En övergripande kartläggning av kommunernas systematiska informationssäkerhetsarbete.

En ny lag om säkerhetsskydd trädde i kraft i april 2019 och en ytterligare skärpning infördes 2021. Lagen ställer bland annat krav på att det ska göras en risk- och sårbarhetsanalys samt att analysen ska omsättas i säkerhetsskyddsåtgärder om det finns information eller verksamhet som ska skyddas. Möjligheten finns naturligtvis att läget när det gäller informationssäkerhetsarbetet, som en följd av den nya lagstiftningen, förbättrats. Samtidigt som den nya lagen ökar kraven på exempelvis kommuner så har också belastningen ökat med GDPR (skydd av personuppgifter), EUs NIS-direktiv (säkerhet i nätverk och informationssystem) och CLOUD Act (molntjänster) även om dessa inte har någon direkt koppling till säkerhetskyddsfrågor. Kraven ökar sannolikt mer än resurser och kompetenser så är det tveksamt om situationen förändrats på något avgörande sätt. SKR har inte gjort någon uppföljning av enkäten.

Av regeringens totalförsvarsproposition[4] framgår vidare att:

4 Proposition 2020/21:30 Totalförsvaret 2021 -2025 sidan 62

> *”Effekterna av ett antagonistiskt cyberangrepp* ***kan få lika stora konsekvenser för samhällsviktiga funktioner och kritiska IT-system som ett konventionellt väpnat angrepp****. Ett cyberangrepp kan inför eller under hela eller delar av en konflikt komplettera politiska, diplomatiska, ekonomiska eller militära medel. Sådana angrepp kan hota en stats handlingsfrihet och ytterst dess suveränitet.”* (Författarens markering i fet stil).

Med detta sagt råder det ingen tvekan om att de som har det politiska ansvaret för totalförsvaret inser både att hoten mot våra informationssystem är betydande samt att ett ökat fokus på informationssäkerhet är nödvändigt. Det är också väl känt att vårt land är ett av de mest digitaliserade i världen samtidigt som informationssäkerheten har omfattande brister. I och med att våra försörjningssystem är beroende av internet innebär försvaret av Sverige i ökande grad att försvara internet.

Gapet mellan å ena sidan hotet mot våra informationssystem och andra sidan informationssystemens sårbarhet har ökat under många år som ett resultat av att digitaliseringen fortsatt medan informationssäkerhetsarbetet har eftersatts. Att vända den trenden kräver ett tydligt ledarskap och radikala åtgärder.

Vad behöver då göras för att öka informationssäkerheten?

Det tycks råda en bred enighet på den politiska nivån om att vårt säkerhetsläge försämrats och att gråzonshotet med en blandning av icke-militära och militära hot är allvarligt. Vidare att cyberattacker kan få samma förödande konsekvenser som ett väpnat angrepp. Problemet är att denna insikt ofta saknas i övriga samhället. Därför borde gråzonsproblematiken och de icke-militära hoten ges större utrymme i debatten. När landets gränser kränks av flyg och fartyg från andra länder blir det stora rubriker medan desinformation, påverkansoperationer och intrång i informationssystem, som pågår dagligen, sällan nämns och det leder naturligtvis till att säkerhetsmedvetandet förblir lågt.

För att möta den breda hotbilden i gråzonen borde organiserandet av vårt försvar, på den politiska nivån, samordnas och styras av en minister och ett departement, i stället för som idag delas mellan Justitiedepartementet och Försvarsdepartementet. Detta för att skapa nödvändig balans mellan det militära och civila försvaret. Med en återgång till ett system med *en* försvarsminister, som vi hade under kalla kriget, skulle också myndighetsstyrningen förenklas.

Inom informationssäkerhet arbetar flera olika myndigheter parallellt, Post- och Telestyrelsen, MSB, FRA, Säkerhetspolisen, Försvarsmakten och det nationella cybersäkerhetscentrat (NCSC) som är under uppbyggnad. Kommuner och regioner uppfattar styrningen som spretig och otydlig. En myndighet borde få ansvaret att formulera en tydlig målbild för informationssäkerhetsarbetet. En distinkt politisk inriktning och tydlig styrning från myndighetshåll krävs om vi ska kunna åtgärda det IT-säkerhetsmässiga gapet. Vidare borde det bedrivas forskning om framtida hotbilder så att vi ökar möjligheten att ligga steget före och rusta oss inför nästa incident.

Det talas ibland om bristen på teknisk kompetens för informationssäkerhetsarbetet. Ett annat område där det uppenbarligen saknas kompetens gäller chefer samt ledamöter i styrelser och ledningar. Ofta saknas engagemang och ansvarstagande på högsta nivå till följd av att personer i ledande ställning är osäkra på hur säkerhetsarbetet ska ledas. Allt pekar på att det krävs ett tydligt och fast ledarskap för att få till ett kontinuerligt och systematiskt säkerhetsarbete där resurser i form av tid för information och utbildning av personalen samt anskaffning av teknik är i balans. Det borde säkerställas att chefer både inser att deras roll i detta avseende är av avgö-

rande betydelse och att de har relevant kunskap om säkerhetsfrågor så att kraven i säkerhetsskyddslagstiftningen kan uppnås. Dessutom borde personer i ansvarig ställning ta ansvar för vad som läggs ut på hemsidor och i andra informationskanaler. Den information som offentliggörs, till exempel på hemsidor, måste naturligtvis harmonisera med den risk- och sårbarhetsanalys som gjorts.

De principer som styr krishanteringen lär vi få leva med eftersom de har vissa fördelar inom andra områden än informationssäkerhet. Men det är inte rimligt att alla våra kommuner, regioner och företag som bedriver samhällsviktig verksamhet var och en ska utveckla lösningar för informationssäkerhet. Här borde staten ta ett tydligare samlat ansvar för att säkerställa att alla aktörer lever upp till säkerhetsskyddslagens krav. Man borde kunna ge anvisningar för informationssäkerhetsarbetet, stödja under processen, följa upp och kontrollera resultatet. Man skulle dessutom ha beredskap att bistå i samband med cyberattacker.

Försvaret mot väpnat angrepp övas ofta både i form av nationella övningar och med internationellt deltagande. På samma sätt borde också övningar för det civila försvaret genomföras. Särskilda övningar inom informationssäkerhetsområdet skulle med all säkerhet leda till att brister i olika delar av samhället

kan klarläggas och åtgärdas.

Med en ansvarig myndighet skulle också information om hotbilder och angrepp kunna samlas in och delges på stor bredd. Det skulle leda till en gemensam nationell lägesbild av IT-hotet, omfattande både de statliga och privata delarna av samhället. Vem vet om en attack mot en avlägsen kommun är en isolerad händelse eller inledningen på ett större angrepp på landet? På så sätt skulle samtidigt säkerhetsmedvetandet ökas och beredskapen att möta attacker bli mer effektivt. Ett ytterligare sätt att öka säkerhetsmedvetandet är att tydliggöra vem eller vilka som utfört att attacken samt med vilket syfte. Kommunikation bygger motståndskraft.

Cyberattacker drabbar samhället på hela dess bredd; både det statliga området och det privata. Eftersom det privata näringslivet levererar en stor del av den samhällskritiska verksamheten så borde den också få stöd av den statliga sektorn. FRA borde inte bara ha uppgiften att stödja företag som har ansvar för samhällsviktig verksamhet utan också nödvändiga resurser för att utföra detta viktiga arbete. En annan aspekt är att statliga aktörer förefaller vara tveksamma till att anlita industrin för att höja informationssäkerheten. Det är en självklarhet att militära system utvecklas i industrin medan det tycks råda en annan syn när det gäller IT-säkerhets-

lösningar. Denna inställning borde förändras så att den statliga sektorn kan dra nytta av industrins kompetens både avseende teknik och metoder. IT-industrin borde med självklarhet vara en del av svensk försvarsindustri.

Slutligen borde vi avhålla oss från att använda olika former av ordet robust. När vi talar om robusta lösningar och robusthet är det en chimär som invaggar folk i en falsk föreställning om att problemet är löst och att vi inte behöver oroa oss längre.

Den deprimerande verkligheten är emellertid att oavsett om det bedrivits ett systematiskt och kontinuerligt säkerhetsarbete, så kan systemen hackas, manipuleras, saboteras eller rent av förstöras. Därför borde vi ständigt utveckla alternativa planer för hur ska vi göra om systemen blir utslagna.

Säkerhetsarbetet tar aldrig slut utan är en pågående process som måste takta antagonistens förmågeutveckling.

Moln - en nödvändighet för cybersäkerhet

av Patrik Fältström

Cyberrelaterade hot mot samhället

Bara för 20 år sedan kunde de flesta funktioner i samhället fungera väl utan datorer. Så är det inte längre. Datorer används överallt, för allt. I vissa fall är det bara en ersättning för papper och penna, i andra fall är datorer en absolut nödvändighet. De senaste 20-30 åren handlar inte bara om datorer, utan kommunikation till och mellan datorer. Detta både för funktion och för att uppfylla de lagar och regler som vi följer. Vi behöver alltså väl fungerande system för att hela vårt samhälle ska fungera. Tillgänglighet och riktighet är minst lika viktigt som integritet i det informationssamhälle vi lever i, men tyvärr diskuteras nästan enbart konfidentialitet.

Under kriget i Ukraina har vi sett exempel på hur angrepp från Ryssland förstört kommunikation genom att artillerield träffat fiberförbindelser.

Likaså har datorer som hanterar information (lagring och/eller beräkningar) förstörts eller hotats att tas över av Ryssland under dess avancemang in i Ukraina. En åtgärd mot denna typ av hot inkluderar att flytta beräkning och/eller lagring geografiskt från en plats till en annan med lägre hotbild. Detta kan man hantera genom att antingen ha två eller flera driftplatser eller ha en primär plats och sedan sekundära platser som kan tas i drift vid behov.

Att flytta beräkningskapacitet och lagring kan naturligtvis göras genom att flytta datorer och lagringsenheter, men det finns idag mycket enklare metoder, att ha flera möjliga datorer att göra sina beräkningar, eller lagra information på, och att använda det som för tillfället fungerar bäst. Detta är möjligt genom en allt mer utvecklad abstraktion gällande lagring och beräkningar från de första datorer som byggdes till dagens molnarkitektur.

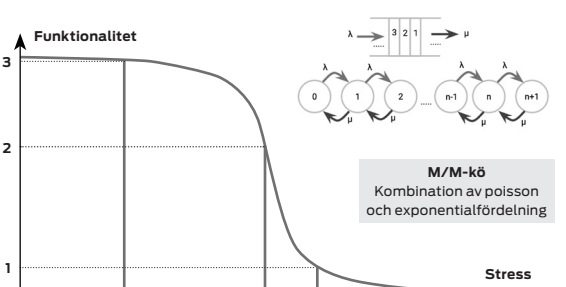
Hur går IT sönder?

Förenklat bygger ett IT-system på att information hämtas, behandlas och lagras eller presenteras. En dator har idag möjlighet att hantera mycket stor mängd sådana operationer varje sekund, och de förbindelser som används för kommunikation mellan datorer kan hantera enorma mängder information.

Men fortfarande är det ”en sak i taget” och ”på begäran” som gäller. Detta sätt att hantera begäran om arbete kallas M/M/1-kö och gör det blir det en kombination av poisson[1]- och exponentialfördelning som visar hur långa svarstider och antal operationer som kan hanteras på en viss tidsenhet vilket visas i Figur 1 nedan.

I sin tur ger detta att vid ökad påverkan är det inte linjärt avtagande funktionalitet utan allt fungerar som det ska tills man når en gräns då allt går sönder. Man kan se det som att man har en nöjespark som det kommer besökare till. Så länge fler besökare lämnar parken än de som kommer så kan parken

Figur 1: Funktionalitet avtar inte linjärt när påverkan (stress) mot ett system ökar



1 **Poissonfördelning** beskriver företeelser som inträffar oberoende av varandra inom ett visst intervall, som samtal till en telefonväxel, och är en ”diskret sannolikhetsfördelning” (red. anm.)

hantera dem. Men om det kommer fler personer per tidsenhet än det lämnar så blir till slut parken full och problem uppstår.

Två olika problem att lösa

Eftersom funktionalitet avtar mycket snabbt vid en viss nivå av påverkan gäller det att se till att denna nivå av påverkan inte är ”en vanlig måndag” utan att det verkligen är vid en exceptionell situation som nivån av påverkan uppnås som gör att system börjar falla sönder. Åtgärder för att inte hamna i denna situation ska alltså höja ett systems förmåga så att brytpunkten nås vid en högre nivå av påverkan.

Ett helt annat problem att hantera är situationen att mängd påverkan är över brytpunkten. Då system inte fungerar, och det kanske inte ens går att få reda på vad som källan till problemet, för symtomen kan vara att tex många olika system är obrukbara men detta beroende på att en fiberförbindelse gått sönder.

Det är därför mycket bättre att höja ett systems förmåga än att lägga krut och energi på reservplaner. Javisst, man måste ha sådana också, men det kanske man bara behöver för det absolut nödvändigaste. Och förhoppningsvis ska man inte heller behöva använda dem.

Cyber och krig

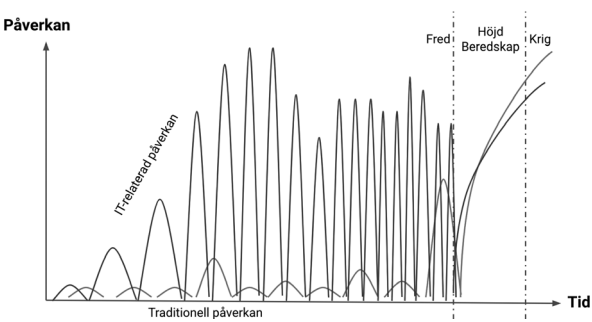
Traditionellt har vi enligt Clausewitz teorier sett krig som en förlängning av politiken, men med andra medel, speciellt önskemålet för en stat att kontrollera en annan. Detta innebär att vi har regler och lagstiftning som bygger på att vi antingen är i fred eller också är vi i höjd beredskap och slutligen krig. Att vi hamnar i krig efter en eskalering av attacker som dessutom är fysiska. När det finns hög risk samhället kommer brytas ner av dessa attacker kan regering och riksdag ta beslut om att övergå i just höjd beredskap eller krig. För att ta dessa mycket svåra beslut är det lättast om underlag är tydliga och så att alla förstår dem.

Idag är teorierna annorlunda. Man har återgått till teorier som Sun Tzu skrev om, att man genom att förstå sin fiende kan man bedra, förleda och på andra sätt än fysiska uppnå sitt mål, att kontrollera motståndaren. Det bästa är om man kan få kontroll utan att förlora egna styrkor, och därmed är även andra medel än traditionella där två krigshärar möts på ett slagfält. Efter de enormt kostsamma kriget i Vietnam har krigskonstens teorier förändrats via Wardens cirklar[2] och Gerasimovs principer[3] till att

2 En attack mot ett samhälle är mest effektiv om de olika delarna angrips samtidigt.
3 Hybridkrigsföringens effektivitet, att de sociala, ekonomiska och politiska konsekvenserna är väl i paritet med ett konventionellt krig och att dessa fenomen ska tas in i det militära tänkandet.

attacker mot ett samhälle sker via andra metoder än militärt krig, och att dessa attacker sker långt tidigare i ett eskalerande angrepp än tidigare vilket visas i Figur 2 nedan.

Figur 2: IT-relaterad påverkan sker tidigt, förmåga måste därför alltid finnas



Speciellt ser vi cyberangrepp som något som redan idag sker och dessutom är antagligen trasiga och övertagna it-system just den anledning som regering och riksdag behöver för att ta beslut om höjd beredskap eller krig. Därför måste åtgärder för höjd förmåga i IT-system utföras långt tidigare i en hotskala än andra åtgärder och dessutom ska de ha effekt utan att vi har de juridiska hjälpmedlen och verktygen som beslut om höjd beredskap eller krig ger.

IT-system måste helt enkelt vara stabila och väl

fungerande alla dagar i veckan, oavsett om det finns hot och åtgärder från statsaktörer eller inte. Åtgärderna måste vara på plats innan något sker. Cyberattacker går snabbt och är effektiva. När något går sönder är det för sent.

Datorn och digitalisering

Kärt barn har många namn. Det vi tidigare gjorde med papper och penna görs idag med hjälp av datorer. Genom åren har möjligheterna tack vare utvecklingen av minnes-, lagrings- och beräkningskapacitet exploderat. Detta kallas ofta digitalisering även om alldeles för många lägger en egen värdering i vad digitalisering egentligen innebär. För mig är digitalisering inte så mycket att använda datorer, utan att förändra processer på det sätt som är möjligt tack vare användning av datorer. Omedelbar tillgång till information gör det möjligt att direkt göra beräkningar och dra slutatser istället för att vänta tills önskad information finns tillgänglig. Autentisering och säkerhet har gjort att kunder själva kan göra de transaktioner som tidigare anställda på företag gjorde. Internet slutligen har gjort att dessa kunder kan göra det på distans. De behöver inte ens ta sig till det ställe där informationen finns eller behandlas.

Abstraktionens triumf

Utveckling av datorer och dess kapacitet började som matematiska och fysiska problem. Reläer och dioder kopplades på ett sinnrikt sätt tillsammans med en klocka som stegade fram pulser som styrdes olika vägar beroende på hur ett program bestämde signalerna skulle gå. De första datorerna var därför mycket stora, innehöll många komponenter och hade därför även problem med sin funktion. Inga komponenter håller för evigt och kontinuerligt underhåll krävdes för att funktion skulle uppnås.

Mycket tidigt byggdes därför delar med förbestämda funktioner som i sin tur kunde kombineras för en mer avancerad funktion. De som byggde dessa mer avancerade funktioner behövde inte förstå hur de olika delarna var konstruerade, utan bara hur de skulle kopplas ihop. När den integrerade kretsen uppfanns blev detta extra tydligt. Varje krets har ett antal anslutningar via vilka olika instruktioner kunde ges. Minne gjorde att program kunde laddas och sedan exekveras.

Även dessa program började med hjälp av allt mer avancerade programspråk bestå av olika funktioner. En allt mer abstrakt beskrivning av vad man ville skulle utföras kunde skapas, och exakt hur alla dioder och elektriska strömmar skulle ledas behövde man inte bry sig om. Ett av många bevis på abstraktion

var 1980-talets skillnad mellan *computer science* och *computing science* som i varje fall de som studerade det senare, som jag själv, anser är en viktig skillnad. *Computer science* ser på hur en dator fungerar, och hur den kan bli effektivare. *Computing science* handlar om hur man gör så effektiva beräkningar och behandling av information givet en viss dator.

Det senare, dvs hur man använder en dator, har utvecklats extremt snabbt de senaste tio åren, inte minst för att utveckling av en ny datorarkitektur eller lagringsmodell för information, tar många år och är mycket kostsam. Hur man använder en dator kan ändras genom att en ny funktion i operativsystemet eller applikationen skrivs och börjar användas. Även på redan installerade datorer och utan att någon del av datorn behöver bytas ut.

Geografisk plats

Men även om vi ökar abstraktionen allt mer måste till slut information finnas på ett ställe, och beräkningar måste göras även det på ett ställe. Avstånd mellan information och beräkning vill man inte heller ska vara för stort för även om överföring av signaler går med (lite slarvigt uttryckt) ljusets hastighet så är det ändå i storleksordningen en miljarddels sekund per

30 cm. Vill man göra många beräkningar per sekund blir därför avståndet mellan information och beräkning viktigt. För att klara sig från att lagringen går sönder och inte kan användas kan man kopiera den information man har lagrad och spara den på en annan plats också, men denna replikering görs av praktiska skäl på ett antal ställen som är praktiskt möjligt, men samtidigt tillräckligt för att risk att alla lagring på alla dessa ställen ska förstöras är minimal.

Virtualisering av datorer

Ett program som skapats för en typ av dator kräver just denna dator för att kunna fungera. Det gör att om man har flera program man vill använda, och dessa inte är gjorda för samma typ av dator, då måste man ha flera olika typer av datorer för att hantera alla dessa program. Att använda alla dessa program på alla dessa datorer blir därför komplicerat. Delning av information mellan programmen kan även det vara en huvudvärk, allt beroende på hur lätt eller svårt det är att föra över information inte bara mellan programmen utan även mellan datorerna som är inblandade.

När beräkningskapaciteten blev tillräcklig i slutet av 1980-talet började därför vissa skriva program för en dator som simulerade andra datorer. Då kunde

man på en dator använda ett program för en annan dator, även om det gick mycket långsammare att köra programmet. Det var ändå värt det för det var trots allt lättare än att ha flera datorer.

Tekniker för virtualisering och de funktioner som man fick tillgång till ökade i samband med att datorer blev snabbare både gällande beräknings- och lagringskapacitet. Överföringskapacitet mellan datorer, och inom en dator (mellan långtidslagring och CPU t.ex.) blev även det kortare, vilket gjorde det enklare för program som kördes på olika datorer att arbeta med samma information samtidigt.

Container som abstraktion av applikationer

I början av 2000-talet vidareutvecklades virtualiseringen från att vara virtualisering av en dator till att vara en virtualisering av ett program. Dvs när ett program skulle köras skapades en temporär omgivning i vilken programmet exekveras, och när programmet var klart så raderades denna. Detta gjordes av säkerhetsskäl, men också för att man på ett enkelt sätt skulle kunna starta program på den dator (av flera) som just då hade tillgängliga resurser. Istället för att hantera (virtualiserade) datorer hanterar

man det som kallas containrar.

En begäran om att något ska utföras resulterar i att utgående från en (eller flera) containrar skapas en så kallad pod på den dator som för tillfället har bäst resurser i vilken exekvering av det som är beskrivet i containrarna. Man kan se en pod som en instantifiering av relaterade containrar. Information hämtas, behandling görs, resultatet levereras, och slutligen stängs den av. För att inte hanteringen, vilket kallas orkestrering, i sig ska ta för mycket resurser kan en pod som startats och använts behållas i ett viloläge och återanvändas om behov uppstår. Denna orkestrering av resurser innebär att man har ett visst antal pod:ar igång som är beredda att ta emot begäran om arbete. Genom att hålla reda på hur många pod:ar som arbetar och hur många som är vilande kan man anpassa antal sådana man har. Om antal vilande pod:ar är för låg kan nya startas, och om det är för många kan de stängas av.

Orkestrering som förmågehöjande åtgärd

Den dynamiska allokering som man kan göra genom att starta och stoppa pod:ar behöver inte vara något som görs på en viss dator (som därmed står på en

geografisk plats) utan detta kan göras på olika datorer på olika platser. Man pratar om att ha en eller flera noder tillgängliga på vilka pod:ar kan startas baserat på beskrivningen i en eller flera containrar.

En tjänst som man vill ska fungera väl är på detta sätt inte beroende av en dator och ett program som körs på denna dator, eller att information ska vara lagrad på dess diskar. Istället är tjänsten beroende av att det finns en ledig pod som kan hantera önskemål från tjänsten, och därmed en väl fungerande orkestrering. Det måste därför finnas tillräckligt många pod:ar (och därmed noder och datorresurser) som är nåbara för att vid varje tillfälle totalt ha så många pod:ar igång som tjänsten kräver. Om antal användare (tex) är för tillfället högt krävs många pod:ar, om antalet är lågt behövs färre.

Vi ser fel i denna typ av dynamisk resursallokering allt som oftast, som när det gavs möjlighet att boka tid för vaccinering mot covid och systemet blev överbelastat. Kanske kunde inte allokeringen göras snabbt nog, kanske fanns inte tillräcklig mängd underliggande datorresurser för alla pod:ar som skulle skapas, kanske användes inte dynamisk allokering?

Men det fina i kråksången är att vi inte bara kan bygga orkestreringen som en virtuell tjänst i sig som dynamiskt allokeras. Vi kan också snurra upp pod:ar på olika geografiska platser allt efter vilket behov

vi har. Det kan röra sig om att ha noder nära användarna för att ge snabbare resultat, eller i ett geografiskt område där risk för destruktion av datorresurser är mindre.

Vi ser det senare ske i Ukraina där som exempel backend för toppdomänen .UA inte bara är virtualiserad utan har flyttats från Kyiv till Prag i Tjeckien. Men egentligen spelar det ingen roll vart den flyttas. Den kan flyttas, och hur den flyttas beror på alla möjliga saker. Kostnad och avtal gällande kapaciteten som används, men allra viktigast är naturligtvis krigets situation i Ukraina. Användarna av tjänsterna märker inget. För det är svårt att märka att något inte är trasigt, förutom genom att funktionalitet finns.

Ett annat exempel är den policy Estland har infört, att genom ett *Government Cloud* se till att landets viktiga tjänster alltid fungerar, och detta genom att inte bara tillåta utan designa för och testa att de flyttas sömlöst till olika tillhandahållare utanför Estland.

Moln är ett nödvändigt teknikval

Att dynamiskt kunna påverka den mängd datorresurser som används och var dessa finns geografiskt är något som idag behövs av många olika anled-

ningar. De vanligaste problemen som uppstår i IT-system är för hög belastning (tjänsten var populär) eller att system går sönder eller slutar fungera för att stödsystem som elektricitet eller kommunikation försvinner.

Den mest effektiva åtgärden mot dessa typer av problem är att kunna dynamiskt allokera resurser för att minska mängd investering i datorer som inte användas, och dessutom att kunna göra det på flera olika platser. Att dessa är populära och effektiva ser vi på de olika standardiserade sätt för orkestrering som utvecklats och inte minst på antalet produkter och tillhandahållare av molntjänster som uppstått.

Man behöver inte köpa moln som tjänst av någon annan, eller snarare, man ska alltid se det som att man köper det som tjänst av någon annan, även om tillhandahållaren är intern. Vi har med moln fått ytterligare en abstraktionsnivå i värdekedjan, förutom det transparenta kommunikationslager som IP-protokollet tillfört i form av internetarkitekturen.

Använder man inte molnteknologi, då kan man i dagens läge inte klara sig länge i den allt grymmare värld vi lever i gällande krigföring där hybridkrig och attacker mot information och informationssystem redan är här.

Några råd på vägen

- Moln är något bra, se till programvara och tjänster du behöver levereras av experter som arbetar med dem hela dagarna. Oavsett om de är inom din organisation eller hos någon annan.
- Börja dock med att göra en analys gällande tillgänglighet, riktighet och konfidentialitet på ett sådant sätt att de blir en korrekt kravställning på den leverantör du väljer.
- Se lagstiftning och dess krav på information och tillhandahållare av tjänster som ytterligare krav i kravställningen på leverantören.
- När du ser på kostnader för tjänsten, glöm inte kostnader för att börja och sluta använda leverantören (dvs migrering till någon annan) och inte bara den återkommande kostnaden.

Kampen om suveränitet i en digital tid

av Carl Heath

Digital suveränitet är ett begrepp som på senare år kommit att få framträdande position i debatten om vårt allt mer digitaliserade samhälle. Användningen av begreppet digital suveränitet innebär i sig en förflyttning i synen på förhållandet mellan nationella intressen och på internet. Begreppets användning har inte sett en lika utbredd spridning i en svenska debatten, men i EU är användandet betydande. Där knyts begreppet i hög grad till ett mer aktivt förhållningssätt till behovet av kontroll av den teknologi som idag utgör grunden för samhällets funktion. Suveränitet är i sig ett begrepp som i flera avseenden handlar om kontroll. Och just frågan om kontroll av teknologi och dess användning är av avgörande betydelse för frågor kopplade till cybersäkerhet. Hur säkerhet ska utformas, av vem, under vilka omständigheter och inom vilket lagrum är centrala utgångspunkter.

Detta kapitel sätter initialt begreppet digital suveränitet i en samtida bredare kontext, där trender som globalisering och digitalisering är viktiga. Vidare beskrivs begreppets mångbottnade innebörd och dess mer politiska komplexitet. Exempel på detta syns genom en beskrivning av hur begreppet digital suveränitet kommit att användas på många olika sätt, beroende på vilken aktör som använder det, och deras politiska intressen.

Digitalisering och globalisering

För att sätta begreppet digital suveränitet i ett sammanhang, så är dess relation till globalisering intressant. Globaliseringen har om man generaliserar betraktats från i huvudsak två olika kontrasterande perspektiv, vilka kommit att stå i motsats till varandra och ses i konflikter om exempelvis globala handelsavtal, om klimatet och andra frågor.

Å ena sidan går det att betrakta globaliseringen som en utjämnare, som Thomas Friedman uttryckte det i sin bok ”The World is Flat”. De som tillskriver sig detta perspektiv beskriver ofta värdet av framväxten av ett globalt regelverk för att driva nationell policy och för att harmonisera regelverk mellan länder. I väldigt grova drag mynnar detta synsätt på

globalisering ut i att den globala marknadsekonomin kan samverka tillsammans med demokratier för att forma gemensamma regler som möjliggör för frihandel, rörlighet för varor och tjänster och så vidare, globalt. En förlängning av detta perspektiv är att denna utveckling skapar möjligheter över tid för att organisera världen bättre på global nivå, snarare än på nationell nivå, och att förflyttningen av regulatoriska strukturer och marknadssystem kan leda till en starkare politisk organisering på global nivå.

Å andra sidan kan man se ett annat perspektiv, som handlar om att betrakta de problem och utmaningar som globaliseringen kan leda till. Väldigt förenklat innebär detta synsätt att peka på hur globaliseringen leder till en urholkning av demokratin, med en minskad förmåga för demokratier att kontrollera sin egen policy och nationella ekonomi. Detta mera kritiska perspektiv till hur globaliseringens processer påverkar demokratin innebär som en konsekvens ett ökat intresse för att se på och vitalisera kopplingen mellan demokrati och kontroll.

Dessa två perspektiv har kolliderat med varandra i en rad områden, och inte minst när det gäller digitala policyfrågor. Digitala policyfrågor har över de senare åren kommit att bli en allt viktigare dimension av internationella ekonomiska och politiska frågor i allmänhet. Under ett par decennier har man

kunnat se hur techföretag kommit att utgöra en allt viktigare del av den ekonomiska tillväxten, och hur de bidrar till den globala ekonomiska utvecklingen. Denna utveckling har också resulterat i en slags dragkamp där dessa företags inflytande och påverkan kommit att växa inom områden som stater tidigare såg som självklara delar av dess egen verksamhet. Denna dragkamp har i sin tur resulterat i allt fler diskussioner, inte minst inom EU, vad gäller ett ökat behov av att återta kontroll från en global nivå.

Det handlar också om att säkerställa så att inte stora länder kan använda sin lagstiftning för att komma åt data som det finns ett nationellt eller europeiskt intresse att skydda. Det här gäller framför allt de länder där de stora techbolagen har sitt huvudkontor.

Ett tydligt exempel är den Europeiska unionens kommissionär Thierry Breton som i ett tal i juli 2020 uttryckte

> *”i ljuset av de växande spänningarna mellan USA och Kina, kommer EU inte att stå vid sidan av, eller bli ett slagfält. Det är dags att ta vårt öde i våra egna händer. Men det betyder också att vi måste identifiera och investera i de digital teknologier som utgör en utgångspunkt för vår suveränitet och industris framtid.”*

Begreppet digital suveränitet i detta europeiska sammanhang återspeglas alltså i de samtida komplexa globala processer, framför allt digitalisering och globalisering, som är två starka och påverkande skeenden. Men vad är digital suveränitet? På många sätt har det kommit att bli ett politiskt begrepp, som används i syfte att möjliggöra för institutioner att fastställa och framhäva dess strategiska intressen, men också för att projicera dem mot resten av världen.

Det finns idag en livaktig akademisk diskurs kring begreppet digital suveränitet och dess natur. På ett plan är begreppet digital suveränitet självmotsägande, på det sättet att det inbegriper två dimensioner som står i motsatsförhållande till varandra. Digital - som på många sätt kan ses som en gränslös företeelse, möter begreppet suveränitet, som i mångt och mycket handlar om kontroll över ett geografiskt territorium.

Tre perspektiv på digital suveränitet

Digital suveränitet är också ett begrepp som kan tolkas och förstås på flera olika sätt.

Ett första sätt att förstå digital suveränitet är uti-

från föreställningen att det finns en särskild slags suveränitet på internet. Under internets första tid, när antalet användare kunde räknas i tiotals miljoner, alltså en bråkdel av idag, förekom en aktiv rörelse vars tankar var att internet, eller cyberspace, hade en alldeles egen suveränitet. Denna digitala suveränitet var fri från den fysiska världens logik, som i många avseenden formats från den westfaliska fredens tydliggörande av vad som kan sägas definiera suveräna stater. Den digitala suveränitet som syns här, är en suveränitet fri från den fysiska världens gränser och regleringar.

Denna tidiga rörelse, som verkade för en egen digital suveränitet på internet, manifesteras bäst i John Perry Barlows manifest ”*A declaration of the independence of cyberspace*”. I manifestet ser Barlow det koloniala och frihetsbegränsande regelverken av traditionella stater som begränsningar för utvecklingen av det han kallar cyberspace. Han förespråkar en digital suveränitet för cyberspace som ska vara likvärdigt tillgänglig för alla, utan privilegier för någon, oberoende av härkomst, ekonomi eller militär makt. Även om Barlows föreställningar om digital suveränitet inte fick en större bärkraft i sin tid, så är hans föreställningsvärld om ett internet eller cyberspace med egen suveränitet en idé som lever kvar idag, på olika sätt och i olika sammanhang.

Ett sammanhang där en form av digital suveränitet beskrivs, som tar spjärn ur Barlows tankar, är bland flera av de olika internationella organisationer som på olika sätt bidrar till att upprätthålla och utveckla internet. En sådan organisation är Internet Society, som menar på att den beslutsprocess som på många sätt format internet till vad den är idag, multi-stakeholder governance-modellen, är avgörande för att skapa och upprätthålla de möjligheter som internet erbjuder. Multi-stakeholder governance innebär att flera olika aktörer, såsom myndigheter, företag, frivilligorganisationer och akademiker, arbetar tillsammans för att styra och utveckla det globala internet. Detta görs genom olika typer av forum och samarbetsorganisationer, där aktörerna kan diskutera och utarbeta gemensamma lösningar på olika frågor som rör internet. Genom dessa beslutsprocesser menar Internet Society att internet och dess grundläggande principer värnas. De ser hur ett växande antal regeringar runt om i världen vill ha mer makt eller inflytande över hur Internet, och de tjänster det möjliggör, fungerar inom deras nationella gränser. Vissa regeringar antar policyer som begränsar rörelsen av data eller reglerar teknikföretag. Syftet med dessa regleringar menar Internet Society kan mena väl och ha goda avsikter, och ha medborgarens bästa i centrum. Men samtidigt

med detta ser de att om varje land tar fram sina egna lagar över det globala internet, riskeras utvecklingen av ett internet som inte är varken öppet, säkert eller pålitligt.

Ett annat exempel på där digital suveränitet handlar om ett tillstånd fri från nationalstater, går att finna i rörelser engagerade i kryptoteknologi, web3, öppen mjukvara med flera sammanhang. Dessa aktörer är en brokig skara som i sig rymmer många olika perspektiv och dimensioner. Gemensamt med många av dem är att de bygger vidare på Barlows idéer om ett suveränt cyberspace, och nyttjar nya teknologier, ofta byggda på öppna, federerade och decentraliserade tjänster med god kryptering, för att skapa tekniska förutsättningar för gemenskaper med en hög grad av autonomi på internet.

Ett andra sätt att betrakta digital suveränitet är att se det i närmare sammanhang av ett par andra begrepp - datasuveränitet, och i dess förlängning också datasäkerhet. Om vi börjar med datasäkerhet, så kan det för stater handla om att upprätthålla en säkerhet som i förlängningen handlar om att säkra statens suveränitet i sin helhet. För företag kan det handla om att säkra sina affärsintressen, och för individer om att säkra den data som finns inom ens privatliv. Här ses ofta en komplexitet, i det att det stundtals upplevs finnas ett motsatsförhållande

mellan individens säkerhet och rätt till privatliv, och statens säkerhet, som ser ett behov av att kunna ta del av invånares data för att beivra brott.

Vidare till det närliggande begreppet datasuveränitet. Ett sätt att beskriva datasuveränitet på är att ta utgångspunkt från ett aktörsperspektiv. I detta perspektiv har individen kontroll över sin egen data och hur den används. Du har rätt att välja hur och när din data samlas in, används, delas och lagras, och du har också rätt att ta bort eller återkalla samtycke till dataanvändning när som helst. Datasuveränitet är också ett sätt för organisationer och företag att säkerställa att de har kontroll över sina egna data och att de inte är beroende av andra för att få tillgång till data eller för att kunna använda data på ett effektivt sätt. Det finns i detta sammanhang en koppling mellan en individs egna data, och samhällets behov av datasäkerhet, som i sin tur är en förutsättning för att kunna sägas ha en datasuveränitet. Ett exempel på en koppling mellan individens data, organisationers data och samhällets data, är när data sätts samman till större helheter. I ett sådant fall, med exempelvis medicinska data, kan den enskilda data vara skyddsvärd primärt för den enskilde. Men när datan sätts samman i en större mängd datapunkter, så kan datans helhet komma att få nya och andra skyddsvärden än enskilda data. En databas kan på så

sätt ha ett organisatoriskt eller nationellt säkerhetsintresse, även om en enskild datapunkt inte har det i samma grad. En enskild persons medicinska data behöver inte självklart utgöra en säkerhetsrisk för samhället, men tillgången till all medicinska data från alla individer ger helt andra möjligheter för den som får tillgång till den, vilket i sig kan sägas vara skyddsvärt för samhället.

Att säkerställa individens skydd för data, är alltså viktigt också för att säkerställa såväl företags som staters data, vilket i sin tur är en förutsättning för datasuveränitet. Såväl individens data, som samhällets data, är också kontinuerligt föränderliga. Datasuveränitet förutsätter alltså en skyddsförmåga över tid. En komplexitet ur ett datasuveränitetsperspektiv är att data inte sällan återfinns i andra länder än där den används. Data nyttjas över internet och med hjälp av tjänster som inte självklart har en tydlig nationell gräns. En e-post kan hinna passera många länder innan det når sin slutdestination. Servern som användaren läser mejlet på kan också den finnas i ett annat land. Lika komplext, eller kanske ännu mer, blir det med molntjänster, som kan ha virtuella servrar vars fysiska lokalisering kan finnas i många olika länder, på flera kontinenter. Det kan i praktiken vara omöjligt att riktigt veta var en viss data befinner sig vid ett specifikt tillfälle. Denna

komplexa väv av digitala tjänster och infrastruktur som internet, och de tjänster som vilar ovanpå internet, erbjuder, betyder att föreställningen om datasuveränitet, och i dess förlängning digital suveränitet, kan komma att stå i konflikt med ett lands tankar om nationell suveränitet.

Ett tredje sätt att se på digital suveränitet är att se de i ljuset av det närliggande begreppet teknologisk suveränitet. I detta sammanhang belyses vikten av ägarskap eller makt över de centrala möjliggörande teknologier som krävs för att en stat eller annan organisering ska kunna upprätthålla sin funktion. Här finns ett antal perspektiv att beakta. En första handlar om synen på kommersiella tjänster i relation till öppen mjukvara och öppen källkod. Frågan om hur starkt ett samhälles beroende är, eller bör vara till ett fåtal stora tekniska tjänsteleverantörer har väckts i flera olika sammanhang och är en pågående diskussion. Ett annat perspektiv är att säkerställa att samhällets data inte är inlåst och oanvändbar, utan går att få tillgång till som öppen och delad data, oavsett om den tekniska lösning datan lagras i är privat eller öppen. I detta sammanhang har EU och även Sverige sedan en tid en aktiv strategi för att säkerställa mer öppen och delad data. Offentlig sektor samlar in, framställer, reproducerar och sprider en mängd information inom en stor flora av områden,

i princip alla de områden där det offentliga är verksamt. Det kan handla om information såsom social, politisk, ekonomisk, rättslig, geografisk information, miljöinformation och så vidare. Information som skapas av en offentlig aktör kan ses som en omfattande och värdefull resurs som kan gynna hela samhället. Ytterligare ett perspektiv till teknologisk suveränitet handlar om förhållandet mellan organisationens behov av att upprätthålla sin funktion, i relation till behovet av att upprätthålla internet som helhet. Här uppstår brytpunkter, där en enskild stat eller organisations behov kan stå i konflikt med behov för att tillgodose ett öppet, fritt och säkert internet som helhet.

Ett politiskt begrepp

Som går att se är alltså digital suveränitet är alltså ett komplext begrepp, som inbegriper olika dimensioner beroende från vilket perspektiv de förstås. Begreppet färgas också av den kontext i vilket det nyttjas. I kontexter av exempelvis säkerhet, ekonomi eller kommunikation kan digital suveränitet nyttjas på olika sätt. Digital suveränitet är alltså ett begrepp i vilket en specifik och avgränsad definition i dagsläget inte enkelt låter sig tecknas. Digital suveränitet

är alltså i någon mening idag i större utsträckning ett komplext politiskt begrepp än ett mera juridiskt eller teknologiskt definierat sådant.

Digital suveränitet och digitala platser

Ett maktperspektiv som knyter an till frågor om digital suveränitet handlar om hur man kan betrakta vilken makt, ideologi, politik och policy påverkar exempelvis en digital, plats eller tjänst, i relation till i vilken grad det är utformningen av platsen, den informations- och systemdesign som finns av samhällets digitala infrastruktur. För att förstå vilken makt en viss reglering exempelvis kan ha, kan det vara värdefullt att förstå den informations- och systemarkitektur som formar den digitala infrastruktur som regleringen är tänkt att påverka.

Det finns alltså ett förhållande mellan policy och systemdesign när det kommer till makt eller inflytande över en digital plats. Statens makt kan vara ”absolut”, men om den digitala platsens design inte stöder den reglering som skapats, är statens effektiva makt ganska liten. Å andra sidan kan statens makt vara begränsad, men om systemdesign av en digital plats är skapad för att vara mycket effektiv,

kan denna i teorin mer begränsade makt vara utomordentligt omfattande i praktiken.

Det går alltså att se att den som äger, eller har det reella inflytandet över en digital plats är den som svarar för denna plats utformning. Den digitala platsens design och de vägval som görs i utveckling och upprätthållande av den avgör i hög grad på vilket sätt det går att engagera sig och delta i denna digitala plats. Avvägningarna för hur en digital plats designas är komplicerad och spelar roll.

Hur designas och driftas digitala platser? Och hur hänger det ihop med demokratin? I en demokrati, är makten legitim när den utövas utifrån rådande demokratiskt beslutade lagar, och i förlängningen den praxis och anda i vilken lagstiftning är utformad. Men i de digitala platserna, hur kan man säkerställa att dessa kommer till uttryck utifrån samma principer, om inte demokratins grundläggande värden tas i beaktande?

Våra digitala platser är generellt sett inte designade och driftade med demokrati som ett huvudsakligt värde. I stället bygger merparten av de digitala platser som nyttjas på principen om äganderätt och marknadskrafter. Den som äger en plats är också den som utövar makt över den digitala platsen. Samtidigt betyder inte det att de som besöker en digital plats eller använder en digital tjänst saknar

inflytande. Utgångspunkten för denna interaktion är marknaden, där relationen utgörs av en kund och den som tillhandahåller tjänsten. Är jag inte nöjd med en tjänst behöver jag inte med självklarhet nyttja den. Samtidigt är detta en sanning med modifikation när nätverkseffekter uppstår i vilket merparten av en grupp finns i samma digitala miljö, kan det vara mycket svårt att i praktiken lämna den, då det också innebär att lämna ett antal samhälleliga eller relationella förpliktelser.

Den fysiska och digitala platsen

I en tid där geografin var avgörande för min möjlighet till inflytande, där informationshastigheten i samhället var den av en häst och vagn, fanns en mycket tydlig koppling mellan makt, medborgare och den fysiska platsen. I en svensk kontext har den så kallade subsidiaritetsprincipen, eller närhetsprincipen, varit viktig. Subsidiaritetsprincipen innebär kortfattat att beslut ska fattas på lägsta ändamålsenliga nivå. Beslut ska fattas så nära medborgaren som möjligt, och där beslut för att lösa olika problem bör fattas på den nivå där man har den bästa kunskapen över beslutets kontext. Men vad innebär nära

i en digital tid? Är nära en fråga om antalet meter mellan medborgaren och beslutsfattaren? Eller är närhetsprincip i en digital tid något nytt och annat? Digitaliseringen har kommit att komplicera detta förhållande om subsidiaritet.

Att delta sammanhang på digitala platser eller att använda digitala tjänster innebär i praktiken att välja ett deltagande utan att lämna ditt eget hem. Du har möjlighet att ta del av och engagera dig i sociala medier, forum, mötesplatser och andra ställen digitalt, och i någon mening befinna dig på två platser samtidigt. Den fysiska och den digitala platsen har inte alltid samma spelregler. Den digitala platsen kan vara en plats som drivs av ett företag, som sätter upp spelreglerna för den platsen. Samtidigt kan företaget vara bundet av lagstiftning i den plats där företaget i sig självt har sin hemvist. På så sätt påverkas deltagandet av en form av digital suveränitet som kommer till uttryck i en kommersiell avtalsrelation, som i sin tur förhåller sig till ett lands regelverk, där den digitala platsen har sin fysiska hemvist.

Utöver de genuint komplexa frågor som väcks rörande hur internet i sig självt upprätthålls i en internationell miljö av överenskommelser, lagar och förordningar, uppstår också frågor om de digitala platser och tjänster som byggs ovanpå internet. Dessa digitala platser är ofta i sig genuint interna-

tionella, vilket komplicerar frågan om makt, ansvar och befogenheter. Hur dessa platser förhåller sig till olika lagstiftning och andra regelverk, och hur lagstiftning påverkar användningen av den digitala platsen eller tjänsten, påverkar också vilka beteenden användaren har.

Internet är en slags miljö som består av många olika digitala platser, där människor lever och verkar. Dessa digitala platser har många likheter med våra fysiska motsvarigheter. Vi upplever, möts, delar, köper, säljer, skapar och utforskar. På internet blir vi arga, ledsna, glada och kära. Vi möter sådana vi träffat tidigare, och främlingar som vi kommer att forma nya band till. Vi formar grupper, gemenskaper och mötesplatser.

Precis som i den fysiska världen behöver vi regler och normer för hur vi möts och är i gemenskap med varandra på våra digitala platser. Dessa regler och normer utvecklas utifrån de lagar och regler som omgärdar den digitala platsens fysiska utgångspunkter, från platsägarens önskan och intentioner, och användarnas behov och förutsättningar.

Digitala platser spelar en stor roll i våra liv eftersom det som händer på den har konsekvenser för våra liv, också utanför de digitala miljöerna. Ett perspektiv i detta sammanhang handlar om hur medborgares rättigheter skyddas i ett sammanhang

där digitala platser vilar på andra lagar och normer. Det har funnits och finns många exempel på där olika länders respektive lagstiftning möter varandra och skapar utmaningar. Men det digitaliserade samhället innebär en allt större förekomst av dessa utmaningar och hinder, då de uppstår utan den fysiska världens behov av förflyttning och resande. I takt med att internet utvecklas uppstår allt fler komplexa situationer där olika lagar och normer möter varandra. Hur våra samhällens förmåga är att adressera dessa situationer blir viktigt för att ta vara på digitaliseringens möjligheter.

Digital suveränitet, säkerhet och samverkan

Ett exempel på ett område där digital suveränitet kommit att bli en aktuell diskussion rör utveckling, drift och säkerhet för kritisk infrastruktur. Med kritisk infrastruktur avses i detta sammanhang den som berör sektorer som är kritiska för ett samhälles funktion, såsom infrastruktur knuten till energi, vatten- och livsmedelsförsörjning, finansiella system, transportinfrastruktur och så vidare. I takt med digitaliseringen har kritisk infrastruktur kommit att bli en digital sårbarhet, vilket har kunnat ses över

de senare åren, i exempel som omfattande cyberangrepp mot länder som Estland eller Georgien, attacken mot en iransk atomanläggning och angrepp som Solar Winds. Ett närtida svenskt exempel är ransomwareattacken mot Kalix kommun. I dessa exempel så har privat och offentlig infrastruktur angripits, vilket i sin tur har resulterat i påtagliga skador och kostnader. Hackerattacker och andra angrepp på kritisk infrastruktur aktualiserar och förstärker behoven av cybersäkerhet och en önskan om att säkra kontrollen över infrastrukturen, för att säkra att vitala samhällsfunktioner inte påverkas.

När det kommer till hanteringen av utveckling, drift och säkerhet kopplat till digital kritisk infrastruktur ses ett ökat behov av samverkan mellan privata och offentliga aktörer. Då digitaliseringen har inneburit att allt fler, inte sällan globala eller transnationella, företag svarar för tjänster med stora värden för offentliga aktörer, blir frågan om digital suveränitet viktig. Frågor om hur en stat kan säkra dess kritiska infrastruktur och centrala tjänster i ett ekosystem där privata och offentliga aktörer samverkar kommer att behöva hanteras i allt ökad omfattning. Här uppstår en viktig diskussion om hur företagens behov av att kunna erbjuda tjänster i en global kontext, och hur de gör för att med sina tjänster möjliggöra för ett globalt sammanhållet

internet, går att säkerställa samtidigt som enskilda länder vidtar åtgärder för att säkra deras digitala suveränitet. Ett exempel på ett område där detta redan idag spelar en viktig roll är inom hälso- och sjukvårdsområdet, där datadelning över nationella gränser är viktig för att kunna forska och utveckla nya behandlingar, metoder och mediciner. Olika länders enskilda behov av att säkra data kan här stå i konflikt med ländernas samtidiga behov av att tillhandahålla bättre hälso- och sjukvård.

Här ser vi exempel på hur de idag uppluckrade gränserna mellan det privata och det offentliga, och det fysiska och det digitala, möter varandra på ett utmanande sätt. Internet har inte samma tydliga gränser som nationalstater har. Det får till konsekvens att de i den fysiska världen förhållandevis tydliga möjligheter som står till buds för att säkra territoriell suveränitet inte går att finna i den digitala miljön. Vid den Westfaliska freden 1648 och senare i FN-stadgan framgår att suveränitet inbegriper att ett land inte agerar inom ett annat lands territorium, utan överenskommelser om motsatsen. Alla stater har en absolut kontroll över vad som sker i dess lands fysiska territorium. Även om denna princip inte alltid så är det den princip som underbygger tankegodset kring suveränitet. Ett exempel på hur dessa principer möter en komplex verklighet är EU,

som i praktiken har överlappande suveräniteter som är omsorgsfullt förhandlade i ett antal överenskommelser på politisk och juridisk nivå.

När det kommer till digital suveränitet återfinns inte samma politiska och juridiska förutsättningar. Idag finns inte motsvarande regelverk på plats för hur en aktörs digitala resurser säkras, även om det går att se begynnelsen till en sådan utveckling. Ett exempel på denna utveckling återfinns i Budapestkonventionen, eller konventionen för cyberkriminalitet, som inbegriper bindande internationella överenskommelser för olaglig verksamhet i den digitala arenan.

Budapestkonventionens huvudsakliga syfte är att harmonisera den nationella lagstiftningen rörande IT-relaterad brottslighet samt att förenkla det internationella samarbetet kring dessa frågor. Det pågår också arbeten inom FN och i andra internationella fora om att än mer utveckla konsensus kring globala normer för de digitala miljöerna. Merparten av detta arbete sker genom den beslutsprocess som tidigare beskrivits - multi-stakeholder governance. Dessa processer bjuder in offentliga aktörer, näringsliv och i många fall civilsamhället för deltagande. Eftersom de digitala miljöerna består av en mix av dessa aktörer i olika former av samverkan, eller kundförhållanden, återfinns ett behov av att reglera och

hantera data på ett sätt som förhåller sig till denna komplexitet.

En tanke med multi-stakeholderprocesser är att åstadkomma en slags balansgång mellan effektivitet och legitimitet i frågor som handlar om överenskommelser som överbryggar nationella gränser och som inbegriper ett behov av aktörer från olika delar av samhällen att samverka. Processerna sker som en konsekvens av att nationalstater erkänner behovet av att också inkludera näringsliv och civilsamhälle i dessa processer. Med detta sagt så saknas inte kritik för denna modell. Den ifrågasätts inte minst av aktörer i civilsamhället, som menar på att de ofta inte har likvärdiga förutsättningar för deltagande som nationalstater eller näringslivet har. Detta riskerar i sin tur att undergräva den legitimitet multi-stakeholderprocesser är i behov av för att upplevas som legitima. Forskare vid Brussels School of Governance har genomfört forskningsprojekt för att bringa klarhet i den logik som multi-stakeholderprocesser utgörs av. Forskningen visar på brister i rådande system. Bland annat har den påvisat att ett slags mer slutna gemenskaper kan bildas i vilket endast aktörer som delar perspektiv deltar. Detta i sin tur kan leda till att resultaten från en process kan ge sken av att ha bred förankring, men i praktiken sakna viktiga dimensioner.

I forskning om handelsavtal för digital handel har deltagande från civilsamhället analyserats. Den pekar på att processernas design är viktig. Multi-stakeholderprocesser kan se väldigt olika ut och beroende på designen kan processerna i sin tur bringa olika utfall. Forskningen visar bland annat att multi-stakeholderprocesser som har fått någon form av tyngre mandat, tenderar att bli mer uppstyrda i sina processer, medan processer med ett mer begränsat mandat, eller som har väldigt öppna processer, kan upplevas som otydliga i sina utfall.

En annan identifierad utmaning i multi-stakeholderprocesser är att många av dem förefaller bestå av etablerade intressen som inte alltid representerar bredare sociala eller samhälleliga perspektiv. Detta riskerar leda till att processerna kan uppfattas som mindre demokratiska, än i de fall en bredare inkludering återfinns. Det går alltså att påvisa ett flertal strukturella problem som behöver hanteras, för att multi-stakeholderprocesser ska kunna uppbära både legitimitet och effektivitet. Samtidigt som dessa problem bör uppmärksammas, finns det idag få andra processer som skulle kunna ersätta multi-stakeholder governancemodellen, då de strukturella förutsättningarna i det internationella samfundet saknas för det.

En konsekvens av det ökade intresset för mul-

ti-stakeholderprocesser och behovet av att öka legitimitet och effektivitet i internationella överenskommelser har inneburit att ett antal stater och andra offentliga aktörer agerar för att driva igenom deras egen linje på den internationella arenan, så som exempelvis behovet av att värna och skydda landets demokratiska värden. Under 2018 beskrev den franska presidenten Emmanuel Macron hur han såg framväxten av två olika internet i världen - det kinesiska och det kaliforniska. Han presenterade ett perspektiv där han menade på att Europa behöver skapa sitt eget förhållningssätt till de policys som omgärdar utvecklingen av globala teknologier. Detta politiska perspektiv har slagit rot i den EU-kommissionen, som pratar om ”Europas digitala decennium”.

Staters förhållningssätt till digital suveränitet

Med utgångspunkten att digital suveränitet är att förhålla sig till som ett komplext politiskt begrepp, är det intressant att se på begreppets tillämpning i olika länder och i en europeisk kontext, då denna i hög grad påverkar en svensk politisk diskurs.

Idag finns där olika visioner i olika länder runt

om i världen av vad ett utpräglat digitalt samhälle kan vara. Dessa visioner färgar också synen på begreppet digital suveränitet och vad man laddar begreppet med. Dessa olika strategier och policys innebär också att olika länder bedriver sin digitala utveckling på mycket olika sätt. Begrepp såsom digital suveränitet har använts runt om i världen i samband med att länder utvecklar förutsättningar för en digital transformation, där länderna förstärker dess förutsättningar att dra nytta av digitaliseringens möjligheter, samtidigt som de försöker undvika dess negativa konsekvenser.

Den pågående förändring av det globala internet, där framväxten av amerikanska och kinesiska teknosfärer syns, med sina egna uppsättningar av standarder, kan som det ser ut idag riskera omkonfigurera Internets nuvarande form. Historiskt har internet kommit att utvecklas genom en stegvis förändring inom kommunikationsteknik, med öppna protokoll som gjort det möjligt för separat utformade nätverk att sammankoppla och leverera tjänster till sina användare under en enhetlig arkitektur. Internetpionjärernas vision var ett globalt nätverk där styrningsmetoder utifrån både ett ”nedifrån och upp” och ”uppifrån och ned”- perspektiv existerar samtidigt. Den geopolitiska utveckling som synts under ett antal år riskerar förstärka klyftan mellan

dessa styrningssätt, polarisera de globala diskussionerna och ytterligare dela upp och splittra det internet som används idag.

Sommaren 2013 förvärrades den politiska dispyten om internets globala infrastruktur efter det att Edward Snowdens läckte interna dokument från amerikanska National Security Agency (NSA). Snowden avslöjade i vilken omfattning amerikanska myndigheter och underrättelsetjänster övervakade och analyserade internetdatatrafik över hela världen. Snowden avslöjade en väletablerad praxis för den amerikanska regeringen att använda data som samlats in av stora amerikanska teknikföretag om deras användare. Många av de företag som ingick i denna praxis kritiserade det sätt på vilket regeringen hade instrumentaliserat detta. Samtidigt blottlade läckan också likheterna mellan underrättelsetjänsternas övervakningsmetoder och ett antal av de stora teknikföretagens affärsmodeller, den så kallade uppmärksamhetsekonomin, i vilket användarens data är den primära råvaran som förädlas till tjänster och produkter för annonsörer. Denna jämförelse bidrog också på detta sätt att förklara varför dessa företags data är så attraktiv, inte minst för olika staters underrättelseverksamhet.

Den ryska statens ansträngningar för att utöva inflytande över internet och dess tjänster är särskilt

långtgående. I slutet av 2019 tillkännagav Putins regering ett åtgärdspaket som syftade till att etablera ett ”suveränt internet”, inklusive tekniska åtgärder utformade för att territorialisera informationsflöden samt tvinga ryska internetleverantörer att skapa den tekniska infrastrukturen för att tillåta all internettrafik till dirigeras lokalt, om regeringen anser det nödvändigt. Det uttalade målet är att utöka den ryska regeringens makt över och inom det ryska undernätverket av Internet. Vidare söker den ryska regeringen också kontroll över DNS. Domännamnssystemet DNS är ett slags översättningssystem som kopplar ihop rätt domännamn med rätt IP-adress, så att man när man surfar hamnar på det ställe man vill. Lite på samma sätt som telefonkatalogen tidigare i historien hjälpt oss att länka rätt telefonnummer med rätt person. Ryssland eftersträvar mer kontroll över DNS för att inte längre vara beroende av ICANN, Internet Corporation for Assigned Names and Numbers. Det är en icke-vinstdrivande organisation som gemensamt drivs av olika intressenter med fokus på internet. Dessa intressenter är främst de företag och organisationer som direkt arbetar med domännamn, IP-adresser och teknisk standardisering av internet, men även världens länder och den intresserade allmänheten deltar i arbetet. ICANN är också den organisation som genom en

särskild funktion tillhandahåller den så kallade rotzonen för DNS-systemet. Rotzonen är startpunkten för all uppslagning av domännamn på internet. Rotzonen finns på de så kallade rotnamnservrarna som är spridda över hela världen. Rotzonen och rotnamnservrarna är nödvändiga för att kunna slå upp ett domännamn så att man sedan kan nå webbplatser och andra tjänster på internet. Rysslands intressen i DNS, och deras önskan om ett mindre beroende från internationella strukturer så som ICANN representerar ett tydligt exempel på en stat som söker makt över ”sitt” nätverk på ett sätt som effektivt påverkar det globala nätverkets konfiguration. Detta extrema fall av makt över ett subnätverk inkluderar således också ett element av makt över det globala Internet.

Kinas regering har redan uppnått målet att säkra sig en position i vilken de utövar i det närmaste full kontroll över det kinesiska Internet. Belägen i ett auktoritärt nätverk beskrivs den resulterande nätverkskonfigurationen som ”ett nätverksanslutet auktoritärt politiskt system”. Förutom sina inhemska ansträngningar är Kina, bredvid Ryssland, ett av få länder i världen som proaktivt försöker omforma den globala digitala ordningen. Det kinesiska politiska ledarskapet ser internet, och digitala tekniker i ett bredare sammanhang, som en möjlighet att kraftigt påskynda landets ekonomiska utveckling och att

utöka den kinesiska regeringens inflytande utanför landets gränser. Dess uttalade ambition är att bli en ”cybersupermakt” i global skala, som avser etablera sig som en central aktör med inflytande över många delar av det globala Internet. Det strategiska förhållningssättet är en förlängning av detta förhållningssätt, där Kina strävar efter att uppnå politisk och ekonomisk överlägsenhet genom teknologisk överlägsenhet. Denna strategi genomförs rent operativt genom många olika ansträngningar. Exempelvis verkar Kina för att utveckla och sprida tekniska standarder och initiera ett stort antal digitala infrastrukturprojekt i såväl asiatiska som afrikanska länder som en del av Kinas ”Belt and Road Initiative” (BRI). Kina, liksom Ryssland, försöker också aktivt påverka relevanta diskussioner om digitala styrelsefrågor inom ramen för FN och i andra miljöer där multi-stakeholderprocesser äger rum.

Europeiska unionen beskriver sitt förhållningssätt som att man strävar efter att röra sig mot ett internet som tar utgångspunkt för de värden som EU framhåller. Med detta menar de att de avser fokusera på att främja en digital transformation som stödjer unionens kärnvärden. Ett exempel på hur detta kommer till uttryck är i kontexten av förhållningssättet till individers data genom lagstiftningen kring GDPR, som är utformade för att ge individer

rättigheter att säkerställa om data om dem själva skyddas. Det pågår idag fler lagstiftningsprocesser i linje med detta, så som Digital Services Act och Digital Markets Act. Gemensamma större initiativ ser dagens ljus, så som en gemensam molninfrastruktur genom projekt som GAIA-X, utveckling av strategier för artificiell intelligens och en stärkt industri för halvledare, för att nämna några områden.

Ett av de primära initiativen som startade EU:s arbete med en digital transformation var initiativet ”e-Europe”, som initierades 1999 av den Europeiska Kommissionen. Initiativet kom under It-bubblans crescendo när IT-undrens tid stod på allas läppar. Man hade sett att USA flera år tidigare hade etablerat policyn ”National Information Superhighway” och såg ett behov av att driva policyutveckling inom EU. Trots att detta initiativ på flera sätt la grunden till att möjliggöra andra initiativ i EU såsom GDPR, var arbetet under denna tid ändå mer begränsat, och fokus låg på att ge näringslivet förutsättningar för att bidra till en digital transformation och kunskapsbaserad ekonomi.

Idag har EU uttryckt en betydligt starkare vision av vad ett digitalt samhälle kan vara. Bakgrunden till detta står till delar att finna i den över tid förändrade geopolitiska situationen med ökade spänningar mellan Kina och USA.

Här har EU valt att röra sig i en egen riktning och inte låta sig definieras av övriga aktörers positioner. Denna egna riktning har kommit att ta spjärn från EU:s upplevda egna behov och värden, med mänskliga rättigheter och datasäkerhet som viktiga element. EU försöker i detta sammanhang uttrycka ett mer nyanserat förhållningssätt till digital suveränitet genom att föra en slags balansakt mellan att värna EU:s kärnvärden, samtidigt som man erkänner att EU är beroende av en global infrastruktur, handel och samverkan med näringsliv som är en förutsättning för att ett globalt informationssamhälle kan finnas. EU vill alltså inte upprätta en helt och hållet autonom digital infrastruktur som förstärker fragmenteringen av det globala internet. Men samtidigt vill EU också skydda sina medborgare.

I en EU-kontext förknippas begreppet i högre grad till frågor om att värna medborgares rättigheter, EU:s säkerhet, samt viljan att en digital transformation för institutioner och aktörer i offentlig sektor, näringsliv och civilsamhälle i EU. I den internationella politiska kontexten strävar EU efter att främja sin syn på vad de digitala miljöerna kan vara, hur de kan se ut och bör regleras, på ett sätt som balanserar värdet av global samverkan med EU:s intressen.

Samtidigt som EU och dess medlemsländer arbetar för att europeiska värderingar är en del av

en digital transformation på global nivå, så har detta arbete också en stor påverkan på nationella offentliga förvaltningar.

I detta sammanhang är det värt att reflektera över ett tidigare resonemang kring den idag nära samverkan mellan det privata och det offentliga i en digital tid. För hur ser en offentlig förvaltning egentligen ut idag, i den digitala miljön? Offentliga förvaltningar har blivit mer och mer beroende av privata aktörer för att förse dem med infrastruktur och tjänster för att stödja staten. Dessa aktörer bidrar i hög grad med att stödja offentliga förvaltningar med deras skyldigheter gentemot andra offentliga verksamheter och medborgare.

I detta sammanhang blir diskursen om innebörd och tolkning av digital suveränitet viktig. Det går att se digital suveränitet i en EU-kontext som ett absolut politiskt mål, som skulle kunna genomföras av en europeisk politik, som kan leda till kontraproduktiva situationer där europeiska samhällen inte kan skörda frukterna av den globala tekniska utvecklingen.

Å andra sidan, utan någon form av skydd för europeiska intressen, regler och värderingar på den globala digitala arenan, riskerar EU att gå miste om det som gör den vill värna - skyddet av individuella rättigheter och demokratiska värden.

I juli 2022 presenterade den svenska regeringen ett ställningstagande för dess syn på tillämpningen av internationell rätt i cyberrymden - Position Paper on the Application of International Law in Cyberspace. Den tar sin utgångspunkt i rådande internationell rätt för att beskriva Sveriges syn på cyberområdet, och däribland också begreppet suveränitet. I denna kontext anses alltså statens suveränitet också inbegripa dess digitala dimensioner. I det svenska ställningstagandet beskrivs att tillämpligheten av befintlig internationell rätt, inklusive FN-stadgan, i cyberrymden har bekräftats av FN:s grupp av regeringsexperter (UN GGE) och av FN:s öppna arbetsgrupp (OEWG). Vidare beskriver man att en bättre förståelse för hur internationell rätt gäller i cyberrymden bidrar till att stärka en öppen, säker, stabil, tillgänglig och fredlig cybermiljö. Den svenska utgångspunkten i detta ställningstagande är att principen om staters suveräna jämlikhet också är tillämplig på cyberrymden. Inom sina territorier har stater jurisdiktion och rätt att utöva myndighet inom ramen för internationell rätt. På internationell nivå är stater oberoende och åtnjuter suverän jämlikhet i förhållande till andra stater. Generellt sett anser Sverige att suveränitetskränkningar kan uppstå från cyberoperationer som leder till skada eller funktionsbortfall. Att ändra och störa data utan

att orsaka fysisk skada kan också kränka suveräniteten. Sådana handlingar inkluderar de som är riktade mot cyberinfrastruktur som tillhör privatpersoner eller enheter. Inblandning i en stats inneboende statliga funktioner kan också utgöra en kränkning av statens suveränitet, inklusive när det utförs med cybermedel. Vidare ser ställningstagandet att tekniska svårigheter ställer till nya utmaningar när det gäller att identifiera ansvariga för cyberoperationer, jämfört med kinetiska operationer, men reglerna om tilldelning enligt lagen om statligt ansvar gäller även i ett cybersammanhang. Ställningstagandet förhåller sig också till cyberkrigföring och internationell rätt. Sverige anser att internationell humanitär rätt (IHL) gäller för cyberoperationer som genomförs i samband med väpnade konflikter. I ställningstagandet konstateras också att mänskliga rättigheter gäller online som de gör offline. Det är en väletablerad princip, som först uttrycktes i FNs råd för mänskliga rättigheters resolution för mänskliga rättigheter från 2012 om främjande, skydd och åtnjutande av mänskliga rättigheter på Internet. Samma mänskliga rättigheter och skyldigheter som stater har i den fysiska världen gäller även i den digitala världen. Även om mänskliga rättigheter är universella och odelbara, är vissa särskilt relevanta för användningen av internet, inklusive (men inte

begränsat till) åsiktsfrihet, yttrandefrihet och informationsfrihet, förenings- och mötesfrihet och integritet. För att möjliggöra fullt åtnjutande av mänskliga rättigheter online menar Sveriges regering i sitt ställningstagande att det är det avgörande att internet förblir öppet, fritt och säkert med lika tillgång och inkludering för alla. De digitala klyftorna, inklusive den digitala klyftan mellan könen, måste stängas. Internet bör styras genom principerna om multi-stakeholder governance.

Det som framgår av det svenska positionsarbetet är att den vidare och djupare komplexitet som tidigare återgivits kopplade till begreppet digital suveränitet inte fullt ut ges utrymme. Frågorna kring cyberrymdens relation till territorium beskrivs inte. Konsekvensen av det är att det svenska förhållningssättet i ställningstagandet i många avseenden kan vara svårt att operationalisera i praktiken. En vidare diskurs rörande digital suveränitet ur ett svenskt perspektiv, och inte minst i ljuset av pågående processer i EU, förefaller vara ett viktigt bidrag för att skapa tydlighet.

Så, vad är då digital suveränitet? Det går alltså att se begreppet digital suveränitet är ett politiskt begrepp, som får olika innebörd beroende på den kontext i vilket begreppet återfinns. Betydelsen av begreppet skiftar också beroende på vilken stat som är föremål för begreppet, men har också olika

kontextuell innebörd beroende på om begreppet nyttjas i en säkerhetspolitisk, ekonomisk eller teknologisk kontext. Med denna vidare utläggning om begreppet är det förhoppningsvis möjligt att se begreppet med något högre upplösning och nyans, vilket blir viktigt i en fortsatt diskussion om samhällets digitalisering i Sverige och i världen, och ett fortsatt välfungerande globalt internet.

Hotet från insidan - den mänskliga faktorn

av Carolina Angelis

Inledning

Att utnyttja människan för att inhämta svåråtkomlig eller till och med hemlig information är inte en ny företeelse, tvärtom. Personbaserad inhämtning, det vill säga att bedriva spionage genom att värva agenter eller spioner, är en metod som har använts sedan urminnes tider – och det är inte för inte som det brukar benämnas världens näst äldsta yrke.

Under sjuttio- och åttiotalet, när datorer och Internet användes i mindre utsträckning än idag, var insiderproblematiken av förklarliga skäl ett större hot än risken att drabbas av en cyberattack. Men i takt med den allt snabbare tekniska utvecklingen och den omfattande digitaliseringen har risker och sårbarheter ökat, något som lett till att fokus för organisationers säkerhetsarbete i större utsträckning har kommit att flyttas från människan till tekniken.

Media rapporterar i princip dagligen om nya

cyberattacker, mindre omfattande så väl som betydligt allvarligare, och flera studier lyfter fram det faktum att Sverige ligger långt fram i digitaliseringsprocessen, men är betydligt sämre när det kommer till cybersäkerhet. Även om vi inte alltid besitter kompetensen eller har tillräckliga resurser för att skydda oss finns trots allt insikten om att vi kan drabbas.

Förståelsen för att någon i vår organisation, eller ännu mindre vi själva, skulle kunna råka ut för ett värvningsförsök från främmande makt verkar vi däremot ha svårare att ta till oss. Enligt Säkerhetspolisen är många anställda inom svenska företag, myndigheter och andra organisationer naiva. Vi verkar tro att den här sortens spionage inte förekommer längre, att det var en metod som försvann när det kalla kriget tog slut. Men i rapporteringen från våra svenska underrättelse- och säkerhetstjänster tydliggörs att den personbaserade inhämtningen ökar.[1] Med det breddade säkerhetshotet menas också att fler verksamheter än vi kanske förväntar oss är av intresse för olika hotaktörer. Vi riskerar alltså inte bara att drabbas av cyberattacker och andra tekniska hot utan även av informationsförlust på grund av spioner som värvats av främmande makt.

Enligt en rapport publicerad av FOI i maj 2022[2] har mer än fyrtio personer dömts för spionage i

1 Se Säkerhetspolisens årsböcker
2 FOI-R--5312—SE, Spionage i Europa 2010-2021, Jonsson & Gustafsson

Europa under de senaste dryga tio åren och ytterligare ett antal ärenden inväntar i skrivande stund domslut. De avslöjade spionerna är antagligen bara toppen av isberget då alla ärenden sannolikt inte når offentlighetens ljus. Av diplomatiska eller säkerhetspolitiska skäl kan ett land välja att inte offentliggöra informationen. Det bör rimligen även finnas ett stort mörkertal där flera nu aktiva spioner ännu inte har avslöjats.

Så kallad teknisk inhämtning är idag ett viktigt och självklart verktyg i de flesta underrättelsetjänsters verktygslåda och cyberattacker är definitivt ett reellt hot mot vår informationssäkerhet. Våra system är i större utsträckning uppkopplade och sammanlänkade samtidigt som det är förhållandevis riskfritt för en angripare att genomföra en cyberattack då man kan befinna sig på tryggt avstånd i någon annan del av världen. Teknisk inhämtning har utan tvekan varit det snabbaste och mest kostnadseffektiva sättet för statliga aktörer att bedriva informationsinhämtning under många år, för att inte säga flera decennier. Även kriminella aktörer har insett värdet av att verka på den digitala arenan, men det finns en tydlig skillnad mellan en kriminell aktör och ett annat lands underrättelsetjänst. Där den kriminella aktören kan tänkas att genomföra en ransomware-attack mot vilken organisation som helst, bara man kan betala

en lösensumma, har underrättelsetjänsten oftast ett specifikt uppdrag att inhämta specifik information för att kunna svara på det sedan tidigare identifierade underrättelsebehovet.

Även när en statlig aktör lyckas att via en cyberattack bereda sig access till ett specifikt mål finns potentiella hinder kvar. Man är sällan eller aldrig intresserad av all data som man nu har tillgång till och måste därför sålla för att hitta den specifika information som var målet med själva attacken. Informationen i systemen kanske dessutom är på svenska vilket kräver att angriparen besitter rätt språkkunskaper alternativt har tillgång till omfattande översättningskapacitet. Har man däremot någon på insidan som kan tala om exakt var informationen finns eller som till och med kan ladda ner den på en USB-sticka och lämna över den till angriparen underlättar det naturligtvis. Ytterligare en anledning till att man inte bara genomför teknisk inhämtning utan även värvar agenter tros vara att det faktiskt har blivit svårare för hotaktörer att bereda sig access rent tekniskt – även om det, som nämnts tidigare, fortfarande finns stora brister i vårt cybersäkerhetsarbete. Och i takt med att vi trots allt blir bättre på att skydda oss rent tekniskt ökar behovet av att rekrytera någon på insidan.

Cybersäkerhet och informationssäkerhet hand-

lar inte bara om IT och teknik. Brandväggar, virusskydd, separata IT-system, krypton och så vidare är förvisso nödvändiga och säkerhetshöjande åtgärder men hjälper inte mycket om någon på insidan så att säga öppnar dörren för angriparen. Människan är och förblir den största sårbarheten, den svagaste länken. Det är vi som hanterar informationen och säkerhetslösningarna, det är vi som ibland råkar göra fel eller till och med väljer att göra det.

Personbaserad inhämtning

Klockan 19.06 den 26 februari 2019 griper Säkerhetspolisen en fyrtiofemårig man på restaurang Kristall på Kungsgatan i Stockholm. Brottet som han misstänks för är olovlig underrättelseverksamhet och i hans jackficka påträffas bland annat ett kuvert med 27 800 kronor.

Mannen, som är IT-konsult och egenföretagare, har via en av de större svenska konsultförmedlingsfirmorna ett uppdrag för Scania i Södertälje. Dessförinnan har han även jobbat på Volvo Cars i Göteborg. Området som han arbetat med är autonoma, dvs självkörande, fordon. Något som även inkluderar utveckling av verktyg för att importera data om det svenska vägnätet från kartdatabaser.

När han grips är han inte ensam. Vid samma bord sitter Jevgenij Umerenko. Umerenko är en rysk underrättelseofficer, närmare bestämt Sverigechef för SVR, utrikesunderrättelsetjänsten.

Men genom att Umerenko har diplomatisk immunitet kan han inte gripas, utan tillåts lämna platsen. Däremot förklaras han *persona non grata* och tvingas lämna Sverige, som en fri man.

IT-konsulten däremot hade ingen sådan ”fallskärm” och i september 2021 dömdes han till tre års fängelse för spionerі. Domen är, enligt Mats Ljungqvist åklagare vid riksenheten för säkerhetsmål, tämligen unik då svensk domstol inte har dömt någon för spionerі sedan 2003.

Säkerhetspolisen beskriver att man sett en allvarlig utveckling när det gäller underrättelsehotet mot Sverige som både breddats och fördjupats. I en intervju från november 2021 säger Daniel Stenling, chef för Säkerhetspolisens kontraspionage, att det redan för tio år sedan fanns hundratals underrättelseofficerare i Sverige med kapacitet att driva uppemot tusen agenter. Sedan dess har aktiviteterna mot Sverige ökat vilket innebär att antalet rekryterade agenter bör vara högre.

Så värvas en agent

Underrättelsetjänsternas process för att rekrytera en agent är universell och består av ett antal steg. Den första fasen, analysfasen, handlar om att identifiera inhämtningsbehovet. Därefter tar man reda på var informationen finns och vem eller vilka som har tillgång till den, något som kallas för målsökning.

Det är information som man många gånger kan hitta via branschtidningar, hemsidor, nyhetsrapportering eller LinkedIn. När man har identifierat en eller flera personer genomför man en kartläggning, bland annat via sociala medier. Man vill ta reda på så mycket som möjligt, alltifrån intressen, livsstil, personlighet, familjesituation och ekonomi.

Finns det några sårbarheter som man skulle kunna utnyttja? Tror man att någon av dem man identifierat i målsökningen är rekryteringsbar? I så fall planerar man noga den första kontakten som sker i närmandefasen. Målet är att det första mötet ska kännas slumpmässigt och spontant, gärna trevligt och angeläget och framför allt helt ofarligt. Om man har gjort en bra kartläggning ökar chanserna till att mötet ska bli bra eftersom man då kan spegla målpersonen med gemensamma intressen, personlighet och värderingar. Om den första kontakten faller väl ut påbörjas det som kallas vänskapsfasen eller kultivering. Den syftar till att utveckla relationen

och lära känna målpersonen bättre.

Tillvänjningsfasen går ut på att vänja målpersonen vid att få små presenter eller pengar för mindre och oskyldiga uppdrag och sakta men säkert höja tröskeln. Efter hand, när målpersonen börjar bli van vid att lämna uppgifter till underrättelseofficeren, kommer det kritiska ögonblicket när man börjar beröra känslig och hemlig information. Om målpersonen är beredd att lämna ut sådan information kan personen anses vara värvad.

Underrättelseoperationer som involverar personbaserad inhämtning är ofta mycket långsiktiga. Det kan ta månader eller år från den första kontakten till dess att personen är fullt ut rekryterad och levererar riktigt värdefull information. Men de är också långsiktiga på så sätt att man inte bara rekryterar personer som redan har access utan även de som man tror kan skapa det, till exempel via sina nätverk. Dessutom närmar man sig även personer som studerar, för främmande makt, intressanta ämnen på universitet, högskolor, medan andra kan vara aktiva i politiska ungdomsförbund. Baserat på vad de studerar kan man anta att de kommer att arbeta på intressanta platser efter studierna. Underrättelseverksamhet bedrivs även mot svenska högskolor och universitet för att inhämta information om forskning och utveckling.

Vem blir spion?

Vad är det som gör att vissa personer låter sig värvas? Vad är det som gör att de, trots uppenbara risker och moraliska aspekter, förråder sin arbetsgivare eller till och med sitt land? Det finns naturligtvis inget enkelt svar på den frågan men det finns ändå några slutsatser som man har kunnat dra genom att studera moderna och historiska case, bland annat när det gäller personligheter och sårbarheter. Rekryterade spioner kan dessutom delas in i två kategorier; de som gjort det mer eller mindre frivilligt och de som på ett eller annat sätt tvingats in i samarbete.

Identifierade personligheter som är mer vanligt förekommande är bland annat grandiosa, narcissistiska och manipulativa, impulsiva, spänningssökande och lättledda samt personer med ett stort behov av att känna sig värdefulla och med en extrem men missriktad lojalitet. Brottet är ofta förenat med bristande inre kontroll, i kombination med en ineffektiv yttre kontroll och någon form av motiv, en sårbarhet[3].

Klassiska sårbarheter är bland annat missnöje, dubbla lojaliteter eller behov av pengar. I merparten av de publika spionfall som omnämns i FOI:s rapport[4] har någon form av ekonomisk ersättning förekommit. Samtidigt har det sällan rört sig om enbart

3 SOU 2012:95, Spioneri och annan olovlig underrättelseverksamhet
4 FOI-R--5312—SE, Spionage i Europa 2010-2021, Jonsson & Gustafsson

ekonomiska motiv, utan snarare en kombination av flera olika drivkrafter. Drivkrafter som främmande makt har lyckats identifiera och utnyttja.

Stig Wennerström, den svenske översten i flygvapnet som spionerade för Sovjetunionen i femton år (mellan 1948 och 1963) fick betalt, men framför allt hade han väldigt höga tankar om sin egen förmåga och betydelse. I förhören som genomfördes med honom motiverar han sitt agerande med att det var tack vare honom som terrorbalansen i världen hade upprätthållits och att han alltså hade verkat för fred. Vad han i själva verket hade gjort var att sälja ut mer eller mindre hela det svenska försvarsplaneringen.

Vissa gör det av egen fri vilja, som Wennerström, andra upplever sig inte ha något val. År 2007 dömdes Denniss Metsavas för spionage. Metsavas, som var en ung estnisk arméofficer i början av sin karriär, hade rest till Ryssland för att hälsa på sina släktingar. Under en trevlig utekväll träffade han en kvinna som han sedan följde med till hennes hotellrum. Dagen därpå blev han uppsökt av två män som bad honom att följa med till polisstationen. Väl där informerades han om att han anmälts för våldtäkt och nu riskerade femton år i ryskt fängelse. Som ”bevisning” visade man honom en film som hade spelats in dolt på hotellrummet. Metsavas förstod att han hade

lurats i en fälla men upplevde inte att han hade något annat val än att samarbeta. Under åren som följde steg han i graderna inom den estniska armén och informationen som han kunde leverera till sin ryske källdrivare blev bättre och bättre och kom att inkludera information om Nato-samarbeten och -system. Upptakten till det grova spionaget var en klassisk honungsfälla och när Deniss Metsavas slutligen greps hade han spionerat för Ryssland under mer än ett decennium.

Att skapa sårbarheter genom att försätta någon i en dålig situation och sedan hota eller tvinga in personen i samarbete kallas *kompromat* eller kompromitterande material (på ryska компрометирующий материал).

Vladmir Putin själv spelade en avgörande roll i en liknande skandal så sent som 1997. Han var då chef för FSB, den ryska säkerhetstjänsten, och hjälpte vid den här tiden dåvarande president Jeltsin att kompromettera överåklagare Yury Skuratov. Skuratov hade just inlett en omfattande utredning om korruption I Kreml, något som naturligtvis inte uppskattades av landets ledande skikt, eftersom många av dem var djupt involverade i korruptionen. Putin lät publicera en film som spelats in dolt av FSB, en film som visade chefsåklagaren i säng med två unga kvinnor. Skura-

tov förnedrades offentligt och tvingades lämna sitt uppdrag varpå utredningen mot Kreml bekvämt nog lades ner. En tacksam Jeltsin utnämnde Putin till premiärminister, något som banade väg för Putin och två år senare, 1999, blev han som bekant Rysslands president.

Honungsfällor används fortfarande av det enkla skälet att det fungerar. Människor som till varje pris vill undvika att information om något man gjort, eller ser ut att ha gjort, når ens partner eller arbetsgivare, är sårbara och riskerar att utnyttjas. Att försöka hemlighålla händelser är sällan en klok strategi för den som blivit måltavla.

Före och efter 24 februari 2022

Sedan Ryssland inledde anfallskriget mot Ukraina har närmare 500 ryska diplomater utvisats från mer än tjugo länder med hänvisning till att de egentligen är underrättelseofficerare som bedriver underrättelseinhämtning, det vill säga spionage, och därmed bryter mot Wienkonventionen om diplomatiska förbindelser. Senast väst massutvisade ryska diplomater var efter mordförsöket på den före detta ryske underrättelseofficeren Skripal och hans dot-

ter i Storbritannien. Även om antalet då ansågs vara omfattande var siffran betydligt lägre då än nu.

Att massutvisa ryska diplomater är ett sätt att protestera mot det ryska agerandet och visa solidaritet med Ukraina, men det är också en fråga om vår nationella säkerhet. Förutom att spionera är de ryska underrättelseofficerarna mycket aktiva när det kommer till andra för oss skadliga verksamheter, som exempelvis påverkansoperationer och desinformationskampanjer. Verksamheter som brukar gå under benämningen gråzonsaktiviteter och som bland annat syftar till att påverka befolkningen och destabilisera samhället.

Antalet ryska diplomater i Sverige har över tid legat på ca 35 personer. Enligt Säkerhetspolisen är var tredje rysk diplomat i själva verket underrättelseofficer, vilket skulle innebära att 10 – 12 ryssar har haft möjlighet att genomföra påverkansoperationer och desinformationskampanjer samt bedriva underrättelseinhämtning mot svenska intressen under diplomatiskt skydd. Den 13 april 2022 utvisade också Sverige tre ryska diplomater. Det betyder att det i skrivande stund (juni 2022) fortfarande bör finnas närmare tio ryska underrättelseofficerare med diplomatisk status i Sverige. Beslutet att inte utvisa samtliga eller åtminstone fler förklaras bland annat med att man vägt in Sveriges intressen av bibehållen

diplomatisk representation i Ryssland.

Att närmare 500 ryska diplomater har skickats hem innebär naturligtvis att Rysslands möjligheter att bedriva spionage och på andra sätt skada väst har minskat avsevärt. De ryska beskickningarna, det vill säga ambassader, handelsrepresentationer och konsulat, som tidigare varit en *fristad* för ryska underrättelseofficerare har dränerats. Vem ska nu fortsätta att driva redan värvade agenter och vem ska rekrytera nya?

Troligtvis har man haft en plan B för varje värvad agent med tydliga rutiner för vad som sker om deras kontaktperson av någon anledning får förhinder. Men många länder har utvisat ett mycket stort antal underrättelseofficerare vilket skulle kunna innebära att även ersättaren har skickats hem och att plan B därför inte längre är möjlig. De som inte utvisats får också räkna med ökad övervakning från ländernas säkerhetstjänster, vilket gör det svårt att utan upptäckt träffa de rekryterade agenterna. I normala fall ansöker man om att få skicka nya diplomater för att ersätta den som tvingats lämna, men det är något som Ryssland nu kan förväntas få svårigheter att få igenom då ny personal ska godkännas av värdlandet.

De ryska underrättelseofficerare som är stationerade på en ambassad eller ett konsulat utomlands har en så kallad täckbefattning, som kulturattaché,

översättare eller ambassadråd. De har diplomatisk immunitet vilket betyder att de inte kan straffas om de blir avslöjade. Däremot kan de förklaras persona non grata och tvingas lämna landet. Men det finns även andra upplägg för att dölja spionaget som exempelvis NOC-operatörer och illegalister. NOC står för *non-official cover* och det är underrättelseofficerare med någon form av täckmantel eller *cover*, där man utger sig för att vara till exempel journalist eller programmerare, eller som påstår sig representera en tankesmedja eller humanitär organisation. En täckmantel som syftar till att man inte ska kopplas till i det här fallet den ryska staten. Många gånger är man förankrad i riktiga företag eller organisationer för att skapa trovärdighet och i vissa fall har verksamheten satts upp just för att ge den *cover* som personen behöver för att lyckas övertyga sin omgivning. De här personerna har ingen diplomatisk status vilket innebär att om de grips kommer de att kunna dömas för spioneri.

Ytterligare en kategori är illegalister. 2010 avslöjades en rysk spionring i USA. Av de tio personer som greps av FBI fanns fyra gifta par och åtminstone två av paren hade dessutom barn, som antagligen inte hade en aning om att deras föräldrar i själva verket var ryska underrättelseofficerare. Illegalisterna i spionringen hade under många år levt helt vanliga

amerikanska liv under tagna namn och påhittade identiteter, vissa av dem i flera decennier. Ett av paren, Vladimir och Lidija Gurjev, kom till USA redan på nittiotalet där de sedan levde som Richard och Cynthia Murphy tills de alltså greps 2010. I juni 2022 greps ytterligare en illegalist, denna gång i Nederländerna. Den nederländska underrättelsetjänsten AIVD avslöjade en rysk GRU-officer som försökte infiltrera den internationella brottsdomstolen i Haag där ryska krigsbrott från så väl Georgien som Ukraina utreds. Enligt uppgift skulle han, om han lyckats få den praktikplats han sökte, få tillgång till mycket känslig information. GRU-officeren levde och uppträdde som Victor Muller Ferreira från Brasilien, i själva verket hette han Sergej Vladimirovitj Tjerkasov och kom från Kaliningrad.

Massutvisningarna av ryska underrättelseofficerare är ett allvarligt avbräck för ryskt spionage, men de som nu skickats hem är underrättelseofficerare som värdländerna trots allt har haft möjlighet att ha koll på. Kvar finns ytterligare diplomater med täckbefattningar och med all säkerhet personer med djupare förankring i vårt samhälle. Förutom att använda sig av redan etablerade NOC-operatörer och illegalister kan vi förvänta oss kontakttagningar via rekryteringsfirmor, tankesmedjor, arrangerade event och konferenser, undersökningsföretag och

nyetablerade start-ups – verksamheter som, åtminstone inte officiellt, kommer att verka under rysk flagg.

Utöver det kan vi räkna med mer offensiva metoder för att komma åt personer med access, där exempelvis ryssar på intressanta positioner utomlands riskerar att avkrävas samarbete samt att man, i än större utsträckning än tidigare, kommer att kombinera teknisk och personbaserad inhämtning.

Med all säkerhet kommer Ryssland fortsätta bedriva spionage mot våra företag, myndigheter eller på annat sätt samhällsviktiga verksamheter. Det kommer kanske att ta tid innan den ryska underrättelseinhämtningen är uppe på samma nivåer som tidigare men man kommer definitivt att göra vad som krävs för att komma tillbaka.

Fokus i det här kapitlet om personbaserad inhämtning ligger av förklarliga skäl på Ryssland, då merparten av de avslöjade och dömda spionerna i Europa under det senaste decenniet har drivits av den ryska underrättelsetjänsten.[5] Dock bör ytterligare hotaktörer lyftas fram och då i första hand Kina och Iran som, enligt Säkerhetspolisen, är de länder som tillsammans med Ryssland utgör det största underrättelsehotet mot Sverige.

5 FOI-R--5312—SE, Spionage i Europa 2010-2021, Jonsson & Gustafsson

Kina

2017 antog Kina en ny underrättelselag som ålägger alla kinesiska medborgare och organisationer att samarbeta med den kinesiska underrättelsetjänsten om så begärs. Det innebär enorma möjligheter att genom medborgare som studerar, forskar eller arbetar utomlands, alternativt som arbetar för utländska företag verksamma i Kina, bedriva personbaserad inhämtning. Den kinesiska civila underrättelsetjänsten MSS (ministeriet för statssäkerhet) och PLA (folkets befrielsearmé) värvar även agenter utomlands, något som framför allt synts i den amerikanska rapporteringen där ett stort antal avslöjanden har gjorts under de senaste decennierna.

2010 och 2018 dömdes två personer i svensk domstol för att ha spionerat på uppdrag av Kina. I båda fallen rörde det sig om flyktingspionage mot tibetaner och uigurer, bosatta i Sverige. Trots att spionaget inte riktat sig mot svenska ekonomiska intressen eller andra klassiska mål som exempelvis politiska beslut eller Försvarsmaktens kapacitet är brotten att betrakta som mycket allvarliga då det underminerar våra demokratiska rättigheter och utgör ett hot mot vårt samhälle.[6]

Den kinesiska staten strävar efter att bli teknologiskt självförsörjande samt uppnå en världsledande

6 Säkerhet för personer som flytt till Sverige Svar på skriftlig fråga 2020/21:734 Justitie- och migrationsminister Morgan Johansson (S) - Riksdagen

position inom flertalet avancerade teknologier, bland annat robotik, flyg- och rymdindustri och nästa generations informationsteknologi. För att nå sina mål använder man sig av både lagliga och olagliga metoder så som forskningssamarbeten, företagsförvärv och spionage.[7] Svenska företag och industrier samt forskning och utveckling är utan tvekan av intresse för Kina och riskerar därmed att utsättas för olika former av spionage. 2017 rapporterade den tyska säkerhetstjänsten BfV om ett stort antal falska LinkedIn-konton som hade skapats av den kinesiska underrättelsetjänsten med syfte att ta kontakt med tyska medborgare av intresse, bland annat högt uppsatta politiker. Målet med kontakttagningarna var att försöka värva dem som kinesiska agenter. Man kan anta att samma metodik används även mot andra länder, inklusive Sverige.

Iran

Enligt Säkerhetspolisen bedriver den iranska staten, förutom flyktingspionage mot iranska minoritetsgrupper och oppositionella exiliranier som befinner sig i Sverige, också industrispionage.[8] 2010 definie-

7 FOIMEMO6698.pdf
8 Säpo Årsbok 2021 (sakerhetspolisen.se)

rade Iran ett antal forsknings- och teknologiområden som skulle prioriteras fram till år 2035, bland annat kärnteknik, bioteknik, rymd- och flygteknik samt miljöteknik. För att nå sina mål använder man sig av metoder som direktinvesteringar i utländska verksamheter genom bulvanföretag, cyberspionage och personbaserad inhämtning. Det finns även exempel på hur man har försökt sätta press på iranska medborgare eller personer med dubbla medborgarskap och tvinga fram ett samarbete. En iransk ingenjör som arbetar på Facebook och numera är bosatt i Kanada, hävdar att han vid ett besök i hemlandet 2020 greps och informerades om att hans familjemedlemmar skulle komma att skadas om han inte accepterade att spionera för Iran. Väl tillbaka i Kanada valde ingenjören att i stället offentliggöra händelsen.[9] Enligt den norska säkerhetstjänsten PST är det här en metod som även den ryska underrättelsetjänsten använder sig av och man får utgå ifrån att det många gånger är ett effektivt tillvägagångssätt, särskilt om personen har nära anhöriga kvar i landet i fråga.[10]

9 FOIR5069 (1).pdf
10 PST (Police Security Service) warns about pressure from Russian agents - Norway Today

Andra nationer

Att Säkerhetspolisen, liksom säkerhetstjänsterna i våra närmsta grannländer och övriga Europa, nämner Ryssland, Kina och Iran som de största underrättelsehoten betyder inte att det är de enda nationerna som bedriver olovlig underrättelseverksamhet mot oss. Även så kallade vänligt sinnade länder och samarbetspartners spionerar.

Exempelvis har USA, precis som Ryssland, betydande inhämtningsresurser och i mångt och mycket använder man sig av samma eller liknande metoder: teknisk inhämtning i form av cyberattacker, personbaserad inhämtning där man rekryterar någon på insidan, signalspaning och så vidare. Efter terrorattackerna i USA den elfte september 2001 infördes också *The Patriot Act,* lagändringar som gav de amerikanska underrättelsetjänsterna mycket stora friheter att på laglig väg samla in data från privata företag som exempelvis Google, Facebook, Verizon och Amazon.

Under senare år har ett antal avslöjanden gjorts som visar att USA har bedrivit underrättelseinhämtning mot länder som Frankrike, Tyskland och Brasilien. I färskt minne har vi också avslöjandet om hur den amerikanska underrättelsetjänsten NSA spionerade på dansk och svensk försvarsindustri[11]

11 Danish Radio reports: the US spied on Saab - Radio Sweden | Sveriges Radio

och även på flera svenska politiker. Den olovliga underrättelseinhämtningen skedde samtidigt som den danska staten upphandlade nya stridsflyg, en upphandling värd många miljarder. Att man spionerar på så kallade vänner må vara upprörande och allvarligt, men samtidigt inte förvånande. Många gånger står mycket stora ekonomiska alternativt säkerhetspolitiska värden på spel och i de här sammanhangen finns inga vänner, däremot finns det samarbetspartners och allierade.

Det finns goda skäl till att Säkerhetspolisen lyfter fram just Ryssland, Kina och Iran som de största underrättelsehoten då de är mycket aktiva och aggressiva i sin underrättelseinhämtning. Utöver det genomför de flyktingspionage, utövar hot och påtryckningar mot före detta medborgare samt genomför desinformationskampanjer och påverkansoperationer. Aktiviteter som på olika sätt riskerar att allvarligt skada svensk ekonomi och demokrati. Det breddade och utökade underrättelsehotet mot Sverige innebär att vi måste fortsätta att arbeta proaktivt, med tekniska säkerhetslösningar men också med ett fokus på människan. Vem vi anställer eller anlitar spelar roll och att ha koll på vem vi samverkar med kommer att bli än viktigare i framtiden.

Motåtgärder

Insiderproblematiken är ett växande problem och ett allvarligt hot som är både svårt att upptäcka och skydda sig emot, men det finns trots allt åtgärder som vi kan vidta för att minska risken att drabbas. Att adressera problematiken börjar egentligen redan när vi anställer nya medarbetare, anlitar konsulter eller underentreprenörer.

En säker rekryteringsprocess och kontinuerlig utbildning av personalen är två av grundpelarna i det säkerhetsarbetet. Förutom rätt kompetens och erfarenhet behöver vi också, så långt det är möjligt, säkerställa att kandidaten är lojal och pålitlig ur säkerhetshänseende och att det inte finns några allvarliga sårbarheter eller beteenden som skulle kunna utnyttjas av någon annan. Det arbetet behöver dessutom löpande följas upp eftersom livet förändras och därmed även förutsättningar och värderingar, något som i slutänden skulle kunna komma att påverka våra lojaliteter. Att genom utbildning skapa säkerhetsmedvetande är en viktig del eftersom en organisation som förstår hur hotbilden mot verksamheten ser ut, vilka hotaktörerna är och vilka metoder man använder sig av är mindre sårbar.

Medarbetare är sällan illojala vid anställning. Det är något som kommer senare, på grund av privata eller arbetsrelaterade stressorer, och det är därför

de uppföljande säkerhetssamtalen är så viktiga. Enligt organisationen Search Security finns det varningstecken som kan indikera att något är fel; som uttryck för missnöje, ilska och negativa attityder.

Konkreta varningssignaler att ta fasta på:

- Att man försöker kringgå behörighetssystem.
- Slår av säkerhetsfunktioner som krypton.
- Undviker nödvändiga säkerhetsuppdateringar
- Frekvent arbetar utanför ordinarie arbetstid när få medarbetare befinner sig på kontoret. Brott mot företagets policy.
- Skapar access till eller laddar ner stora mängder data, som inte ingår i yrkesrollen.
- Försök att föra ut data utanför organisationen.
- Sökningar efter sårbarheter.

Vad som gör det hela så svårt är inte bara vår naivitet utan också vår önskan att tro gott om alla. Vi vill inte misstro våra kollegor och tänka tanken att någon skulle kunna utgöra en risk eller medvetet agera på ett sätt som skulle kunna skada verksamheten.

I grunden är det bra att vi tror gott om andra och litar på varandra. Men verkligheten visar tyvärr att människor ibland gör dåliga saker och i de flesta fallen har varningssignalerna funnits där, vi har

bara inte velat se dem eller agera på dem. Samtidigt är det ju så att om man faktiskt hade vågat lyfta ett förändrat beteende eller berätta att man är orolig för en kollega så hade personen kanske kunnat få hjälp i tid. Det handlar alltså inte om att ”sätta dit folk”, det handlar om att avvärja hot och risker mot verksamheten men även individen. Den som pressas till att begå förräderi är också ett offer, och kan den personen hjälpas innan brott begås eller säkerhetsskada görs är det att föredra.

Verksamheter som lyder under säkerhetsskyddslagen har en skyldighet att genomföra både säkerhetsprövning och kontinuerlig uppföljning av befintlig personal samt att se till att medarbetarna förstår hur hotbilden ser ut och vilket ansvar man har. Men betydligt fler svenska myndigheter, företag och organisationer skulle må bra av att göra samma sak eftersom utländskt spionage inte begränsas till vad vi har säkerhetsklassat.

Svagheter i krav och genomförande

Säkerhetsprövningsintervjun är en synnerligen viktig del i säkerhetsprövningen och för att den ska kunna genomföras på ett kvalitativt sätt krävs

att intervjuaren förstår *varför* frågorna ställs, kan tolka svaren som ges (eller inte ges) och inser vilka följdfrågor som är relevanta att ställa. För att ha möjlighet att identifiera allvarliga sårbarheter samt bedöma lojalitet och pålitlighet behöver intervjuaren förstå så väl hotbild som hotaktörer och vilka metoder dessa använder sig av.

När det gäller säkerhetsprövning av konsulter och underentreprenörer som ska in på kortare eller längre uppdrag i verksamheter som kräver säkerhetsprövning är det inte ovanligt att det åläggs VD eller annan person i det externa bolaget att genomföra själva säkerhetsprövningsintervjun av den egna personalen. En VD/motsvarande för en firma som ska genomföra ett säkerhetsklassat uppdrag har sällan eller aldrig den kompetensen. Utöver bristande erfarenhet på området saknar vederbörande incitament att identifiera sårbarheter som riskerar att hindra medarbetaren från att genomföra uppdraget för kunden. Den verksamhet som lyder under säkerhetsskyddslagen och som behöver anlita externa bolag invaggas här i en falsk trygghet där man snarare sett till att bocka av lagkravet än att verkligen göra vad man kan för att säkra information, system eller anläggningar.

Det finns aldrig någon hundraprocentig garanti för att ens myndigheter eller företag med hög kompetens och stor erfarenhet inom säkerhetsprövning

verkligen klarar av att identifiera sårbarheter eller illojalitet, men då har man åtminstone gjort vad man kan för att minska risken.

Slutsats

Metoderna som används av hotaktörer idag är inte enbart tekniska *eller* personbaserade utan snarare en hybrid av båda och för att kunna skydda oss mot den förändrade hotbilden behöver vi förändra vårt sätt att jobba, vårt försvar.

På grund av det allvarligt försämrade säkerhetspolitiska läget kommer vi med all sannolikhet att uppleva fler cyberattacker mot olika samhällskritiska system men vi kommer också att se fler exempel på rekryterade spioner eller personer som agerar på eget initiativ på grund av exempelvis missnöje eller dubbla lojaliteter.

Vi kommer aldrig att kunna uppnå ett hundraprocentigt skydd. Det finns alldeles för många rörliga delar som vi inte kan kontrollera. Allt ifrån tekniska sårbarheter till individer. Men det betyder inte att vi inte ska försöka. Tvärtom - vi måste göra det så svårt och dyrt som möjligt för en angripare att lyckas och då är den mänskliga faktorn avgörande. Dessutom, varje stoppad incident är trots allt en stoppad incident.

Politik för en cyberrymd som är på riktigt

av Patrik Oksanen

Det som händer på internet och i våra datasystem kan inte ses med blotta ögat. Vår fantasi räcker inte till för att helt förstå detta och göra det verkligt. Därigenom blir vi också i våra reaktioner vid cyberangrepp kognitivt bedövade. Det är som att cyberrymden inte är på riktigt. Vi uppbådar inte kraft, engagemang eller utkräver ansvar som om det vore en händelse i den verkliga fysiska världen. För angriparen blir det här ett budskap om att det är bara att fortsätta med den brottsliga och säkerhetshotande verksamheten. Kostnaden för angreppet är låg, risken i att utföra det är obefintligt medan vinsten kan potentiellt bli enorm. Vem skulle då inte fortsätta att bedriva attacker i cyberrymden?

Tänk om det hände i den verkliga världen?

Hur absurt det egentligen är blir tydligt när vi gör tankeexperiment på att cyberangreppet var en faktisk fysisk händelse. Låt oss här leka med tanken kring tre uppmärksammade cyberangrepp och vad som hade hänt om motsvarande hade skett i den så kallade IRL[1]-världen.

Kalix kommun

Tänker er att motorcykelgänget ”Hell Knutters” rullar mitt i natten 16:e december 2021 in i huvudorten Kalix. De slår till mot kommunhuset och tar genast kontroll över servrar och alla utbetalningssystem. De lägger beslag på tjänstgöringslistor, patientjournaler och all annan information som man behöver för att utföra service och tjänster i en kommun. Ingen anställd kan längre komma åt ens sin e-post hemifrån. Angreppet lamslår Kalix, 1600 anställda blir ställda på backen och kan inte jobba. För att släppa tillbaka Kalix kommunanställda in på sina digitaliserade arbetsplatser vill ”Hell Knutters” ha pengar, mycket pengar, i en lösensumma.

När Kalix kommun ringer polisen i Luleå om härjningarna får man svaret att det får Kalix lösa själva,

1 Irl = In real life, alltså verkliga världen, bortanför datorn.

kanske går det lura in MC-gänget in i isladan och låsa dörren?

I verkligheten drabbades Kalix av ett cyberangrepp som lamslog all verksamhet. Anställda fick bege sig fysiskt till banken för att få sin jullön. Hackarna begärde en lösensumma som de aldrig fick. Det tog över en månad för Kalix att återställa verksamheten helt och kostnaden beräknades till 2,5 miljoner kronor, produktionsbortfall inte medräknat.[2] Vem eller vilka, eller vad som var syftet bakom attacken är inte officiellt klarlagt. Chefen för Säkerhetspolisen Charlotte von Essen kommenterade händelsen för SR med att IT-attacken mot Kalix kommun är ett exempel på hur hotbilden har ökat. [3]

Det som borde ha gjorts från staten sida är precis vad som hade hänt om ”Hell Knutters” hade härjat i den verkliga världen. Polisen hade mobiliserats för att ta hand om hotet, och andra myndigheter - som länsstyrelsen och MSB hade gått in och stöttat Kalix handgripligt för att hantera krisen och dess konsekvenser. Så skedde inte nu. I cyberattacken borde ett nationellt team trätt in och hjälpa kommunen redan 16 december samtidigt som MSB flugit in ledningsstöd och krishjälp för att hantera konsekvenserna av cyberattackerna.

2 Cyberattacken mot Kalix kommun. https://pulse.microsoft.com/sv-se/work-productivity-sv-se/na/fa1-cyberattacken-mot-kalix-kommun/

3 Säpochefen i SR. https://sverigesradio.se/artikel/sapo-om-it-attacken-mot-kalix-kommun-skyddet-behover-starkas

GRU stormar Stortinget - Sverige tiger

Tänk er att det uppför Kar Johans gate i Oslo stormar operatörer från den ryska militära underrättelsetjänsten GRU. Deras mål är nummer 22, Stortinget. I den överraskande attacken som överrumplar vakterna får GRU-operatörerna med sig en stor mängd dokument och brev som de sedan försvinner med. Hur mycket och vilka stortingsledamöters kontor som blev drabbade av räden vill norska myndigheter inte berätta. Först i oktober går norska regeringen ut och berättar vem som ligger bakom attacken - Ryssland och GRU.

Men sedan blir det tyst, märkligt tyst. Inget extra Natomöte, ingen artikel 4-konsultation, inga sympatiyttringar från Natoländer eller uttalande från Sverige eller Finland i nordisk solidarisk anda. Ett enda land uttrycker sitt stöd - Ukraina.

Det som skedde i augusti 2020 var förstås inte ett fysiskt angrepp, utan ett cyberangrepp. Det genomfördes av avdelningen 26165, ökänd för inblandning i bland annat hackningen av Demokraternas e-post i det amerikanska presidentvalet 2016.[4]

Ett riktigt fysiskt angrepp hade lett till omedelbara politiska stöduttalanden och gemensamma fördömanden av skarpaste art. Norges allierade hade

4 https://frivarld.se/rapporter/den-ryska-cyberattacken-mot-stortinget/

sammankallats och det minsta som skulle ha skett är en rad diplomatutvisningar och kanske sanktioner.

Tystnaden kan bara förklaras med att cyberangrepp inte ses som händelser i den verkliga världen trots att de sker mot demokratins och suveränitetens hjärta och att vi vet att följdverkningarna kan bli omfattande. Det som borde ha skett hösten 2020 är åtminstone stöduttalanden och ”name and shame” från en rad huvudstäder tillsammans med gemensamma beslut om straffåtgärder. Att Stockholm var tyst och inte uttalade stöd för ett av sina närmaste grannländer kan inte ses som något annat än självmål för den solidariska säkerhetspolitiken och nordisk sammanhållning.

Riksidrottsförbundet under attack och medierna spelar med

Tänk er att från december 2017 till maj 2018 så smyger sig GRU in och ut på nätterna hos Riksidrottsförbundet i Stockholm. De söker igenom lådor och arkiv och kopierar mängder av det som har att göra med dopningsarbetet. Ingen på RF märker att det finns ovälkomna besökare och att inbrott skett kontinuerligt. I maj 2018 basunerar ryska ”aktivister” och medier ut nyheter om påstådda ”skumma saker”

(som egentligen inte är skumt, men bildsättning är allt) kring svensk dopning och svenska idrottare. Svensk press hakar på.

SR berättar att uppgifterna publicerades på ”en tidigare omdebatterad rysk sida”. Sporten hos Expressen är inne på samma linje och benämner det som en rysk grupp ”som tidigare har fått uppmärksamhet” och får RF:s ansvariga i en märklig försvarsställning: ”Illa – men vi har ingenting att dölja”. Och ”det är inte okej att släppa den här typen av uppgifter”.

Till Ekot säger RF:s ordförande Björn Eriksson att det är ”väl finansierade krafter” och att syftet är att skapa bilden att alla fuskar: ”Det är så man jobbar med ”falska nyheter”, man slänger ur sig påståenden och försöker säga att i mörkret är alla katter grå”. Men vilka krafterna är säger aldrig Eriksson, utan lämnar det till allmänhetens fantasiförmåga.

Polisen gör en utredning och tre år senare säger man att man vet vem som bröt sig in och stal uppgifterna och varför.

I verkligheten var det ingen fysisk inbrottstjuv utan hackare från GRU som låg bakom attacken. Säpos utredning kunde knyta angreppet till den ryska militära underrättelsetjänsten och att det *”skedde genom upprepade fullbordade dataintrång av den ryska militära underrättelsetjänsten GRU:s 85:e*

center. Dataintrånget var en del i en större rysk påverkanskampanj".

Kontraspionagechefen Daniel Stenling kommenterade syftet så här i ett pressmeddelande 2021:

> *"Den säkerhetshotande verksamheten kan ha flera syften samtidigt och vara både direkt och indirekt. Målet kan vara både regimstabilitet, att stärka det egna landets status som stormakt och att påverka beslutsfattande. Det är i detta sammanhang som det misstänkta dataintrånget mot Riksidrottsförbundet ska ses".*

Men utredningen läggs ned eftersom utsikten att ställa rysk underrättelsepersonal inför rätta är för låg. Några andra konsekvenser får inte de nattliga stölderna. Däremot konstaterar åklagaren Mats Ljungqvist i ett pressmeddelande att GRU kommit över medicinska journaler för svenska idrottare:

> *"Informationen har publicerats offentligt och baserat på dessa uppgifter har även svensk media skrivit artiklar som överensstämmer med GRU:s narrativ att svartmåla idrottare och idrottsorganisationer i väst."*[5]

En för GRU lyckad operation. Målbilden uppnådd.

5 Åklagarens pressmeddelande 2021. https://www.aklagare.se/nyheter-press/pressmeddelanden/2021/april/forundersokning-om-grovt-dataintrang-utfort-av-rysk-underrattelsetjanst-nedlagd/

Det som borde ha skett, skrev jag i en artikel hos Frivärld är: ”*att* åklagaren (borde) ha gått till Interpol och efterlyst de misstänkta operatörerna vid GRU:s 85:e center och Sveriges regering borde ha uppmanat ryska myndigheter att utelämna dessa (visst, Ryssland skulle inte göra det, men vi borde inte undvika att göra markeringen). Om det varit omöjligt att namnge inblandade GRU-officerare genom utbytet av underrättelseinformation skulle ett åtal kunna rikta sig högre upp i kedjan till den öppna delen av GRU.”[6]

Dessutom borde Sverige skickat hem ryska diplomater och gjort markeringar i idrottsvärlden. Som att bojkotta flernationsturneringar i Ryssland. Förhoppningsvis med solidarisk uppslutning från våra grannländer.

Cybersäkerhet kräver en politik med konsekvenser

Dagens sätt att se på cyberangrepp som något som inte finns, eller att man får skylla sig själv, kommer inte att avskräcka länder som Ryssland och Kina att fortsätta att angripa våra IT-system. Inte heller sover brottslingar som opererar under skydd från statsaktörer särskilt dåligt om nätterna, oroliga för att bli lagförda.

6 Inlägget hos Frivärld https://frivarld.se/sakerhetsradet/sverige-skickar-fel-signaler-efter-grus-angrepp-pa-rf/

Diskussionen om en avskräckande cyberpolitik pågått i flera i år. Nato beslutade redan 2014 att en omfattande cyberattack skulle kunna trigga artikel 5, den som brukar kallas för ”en för alla, alla för en”-musketörklausulen om kollektivt försvar.[7] Nivån på cyberattacken är alltså ett par steg högre än de fall som finns beskrivna tidigare i kapitlet.

På EU-nivå beslutades det 2017 om ett ramverk för ”Joint EU Diplomatic Response to Malicious Cyber Activities”. Detta tillåter EU och dess medlemsstater att använda alla verktyg som EU:s gemensamma utrikes- och säkerhetspolitik erbjuder. Det här har använts blygsamt, först 2020 fattade EU ett första beslut om sanktioner mot sex personer och tre organisationer från Kina och Ryssland som pekats ut som ansvariga för olika cyberattacker, som den mot OPCW (Organisationen för förbud mot kemiska vapen) och de attacker som är kända som WannaCry, NotPetya och Operation Cloud Hopper. Beslutet innebar reseförbud och frysta tillgångar, däremot gav man sig inte på uppdragsgivarna - staterna Ryssland och Kina.

Ämnet har också diskuterats i Nordiska rådet. I rapporten ”Nordic Foreign and Security Policy 2020” adresserar rapportören Björn Bjarnason hybridhot och cybersäkerhet med uppdraget att också komma med förslag om hur ”*strengthening and*

7 CCDCOE om artikel 5. https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/

reforming multilateralism and the rules-based international order" skulle kunna göras. Behovet att sätta ljus på angriparen lyfts i rapporten:

> *"However, closer collaboration between the Nordics should also entail standing together when Nordic countries or companies are threatened or attacked. This requires the willingness to expose malign and coercive information activities of states or other actors as well as safeguarding and publicly supporting both Nordic research communities and independent media."*

När det Nordiska rådets digitala temasession hölls 2021 gick Bjarnasson längre och uttryckte behov av avskräckning: *"Cyberförsvarets avskräckande kraft ökar om man kan räkna med solidaritet mellan grannländer. Det har effekt om man möter kritik från fem länder i stället för från ett land."*[8]

Vi kommer inte att kunna dämpa angriparens vilja att ge sig på våra system om det fortsätter att vara gratis, förutom investerad tid, att angripa oss. Därför måste kostnadskalkylerna i framför allt Moskva och Beijing förändras.

I vår strategiska kultur tycker vi ofta att begreppet avskräckning är otäckt, men det är vad vi behöver

8 https://kkrva.se/solidaritet-som-avskrackning-mot-cyber-och-paverkansoperationer/

implementera i cyberarenan. Här finns en verktygslåda som används alldeles för lite, som offentliga uttalanden från regeringsföreträdare och internationellt solidariskt stöd. Ord behöver backas upp av handling, som utvisningar av underrättelseofficerare från ambassaderna, personliga sanktioner mot ansvariga och egna offensiva motåtgärder, både i cyberarenan och asymmetriska svar, behöver läggas till verktygslådan tillsammans med det viktigaste av allt - det går inte att stå ensam.

Det behövs en cybersolidaritetspakt mellan demokratier för att ändra logiken som gör angreppen allt för lönsamma. Det här kan handla dels om utveckling av Natos kollektiva respons, och EU:s solidaritetsmekanismer och genom Nordiska rådet. Men cybersolidariteten bör också utsträckas till andra likasinnade länder som Australien, Nya Zeeland, Japan, Sydkorea och Taiwan. Det är högteknologiska demokratier som alla är utsatta för angrepp. I väntan på större överenskommelser finns det ingenting som hindrar de nordiska länderna att gå före, exempelvis tillsammans med våra baltiska grannar i det så kallade NB8-formatet (Nordens fem länder samt de tre baltiska staterna). Här finns ett utrymme att visa ledarskap genom handling, att gå före och visa vägen.

När det gäller kriminella grupperingar så är inter-

nationella sanktioner mot individer ett sätt för att minska deras rörlighet och möjlighet att kunna njuta av sina stölder, precis som EU har infört. Men verktyget måste användas i mycket större utsträckning. Till det behöver straffen för dataintrång höjas, och när det gäller angrepp mot demokratins och svenska statens suveränitet bör de vara utan preskriptionstid. Dessutom bör det införas stränga straff mot de som skyddar och möjliggör cyberbrottslighet.

De flesta av oss skulle minnas dagen då norska stortinget stormades av GRU om det hade skett i den verkliga fysiska världen, precis som vi minns var vi var när vi hörde nyheten om terrordådet i Oslo och på Utöya den 22 juli 2011.

Konsekvenserna av sådan rysk stormning av norsk demokratis hjärta skulle bli omfattande och svåröverskådliga, det i sig är en anledning att GRU inte fysiskt stövlar in i Stortinget med automatvapen. Priset är för högt för att göra ett sådant våghalsigt anfall och vinsten är alldeles för liten.

Det är därför vi måste sluta rycka på axlarna när det handlar om cyberangrepp. Det gynnar bara de som inte vill oss väl. Handlingar i cybervärlden är precis som handlingar i den fysiska världen, de är verkliga och får verkliga konsekvenser. Det är hög tid att vi agerar utifrån den insikten.

FRIA SVAR PÅ FORES ENKÄT

Här listar vi de svar och kommentarer vi fick på enkäten

Vilken sektor tillhör du?	Vad är viktigast att åtgärda för att stärka cybersäkerheten?
x och industri	Enkla direktiv och tips.
Hälso- och sjukvård samt omsorg	Harmonisera, modernisera och förenkla lagar och regleringar. Låt NIS2 ersätta säkerhetsskyddslag för samhällsviktig verksamhet utan överlapp. Verksamhetsområdet är för komplext för en reglering, utan bör styras genom krav på riskbaserade ledningsystem och säker-hetsåtgärder.
Finansiella tjänster	Att stärka myndigheternas egen cybersäkerhet och informationsgivning till oss företag.
Hälso- och sjukvård samt omsorg	Öka medvetandegraden och kunskapen hos alla anställda
Handel och industri	Information till anställda om hot och åtgärder.
Energiförsörjning	- En fungerande CERT-SE. - Myndighetskrav som är effektiva och förankrade i verkligheten för verksamheter som inte är myndigheter. - Större satsning på utbildning nationellt och inom EU samt en nationell strategi.
Livsmedel	Security Operation
Energiförsörjning	- En fungerande CERT-SE. - Myndighetskrav som är effektiva och förankrade i verkligheten för verksamheter som inte är myndigheter. - Större satsning på utbildning nationellt och inom EU samt en nationell strategi.
Livsmedel	Security Operation

Finansiella tjänster	Att myndigheter lyssnar på offentliga OCH privata organisationers problem, samt bygger upp en stark förmåga att stötta med att bedöma hotbild (i nära realtid) relaterad till såväl staters som internationella och nationella kriminella organisationers aktiviteter. T.ex.: a) kommunicera aktuellt nuläge (i nära realtid) - hotbild, scenarios med tänkta utfall, rekommendationer. b) kommunicera trender, exempel, och hur de påverkar olika delar av samhället, rekommendationer. c) ställa krav och följa upp säkerhet och stabilitet hos kritiska organisationer för samhället (IT tjänsteleverantörer, BankID, nationell infrastruktur etc.) för att säkerställa att de fungerar även under påverkningar från omvärlden - internationella eller nationella aktörer och händelser.
Information och kommunikation	Allmän kompetens bland hela befolkningen samt fler med spetskompetens
Energiförsörjning	Mer aktiv stöttning från sektorsspecifika myndigheter. I synnerhet vad gäller samhällsviktig verksamhetsutövning såväl som nationellt samhällsviktig verksamhetsutövning
Finansiella tjänster	Awareness då den sociala/mänskliga delen är svårast att kontrollera och hitta lämpliga skydd för
Transporter	Möjligheten att rekrytera kompetens

Om Fores

På den gröna och liberala tankesmedjan Fores arbetar vi varje dag för att söka de lösningar och reformer som Sverige behöver, för att försvara den liberala demokratin så som vi känner den. Vi står med den ena foten i akademin och forskningen och med den andra i samhällsdebatten. Genom våra temagrupper Tillväxt, Trygghet och Tillit söker vi forskningsbaserade, framtidsoptimistiska reformförslag. Vi publicerar studier, böcker och rapporter samt arrangerar och medverkar i seminarier, samtal, debatter och projekt. Fores är hubben för den liberala demokratins vänner och driver därför bland annat Foresakademin och Reformpuben för nätverkande och idéutveckling. Besök gärna www.fores.se för mer information.

Om författarna

Carl Heath

Carl Heath är senior forskare i RISE, Research Institutes of Sweden. Carl har tidigare haft regeringsuppdrag som särskild utredare att värna det demokratiska samtalet och leda en nationell satsning på medie- och informationskunnighet. Han är verksam i gränslandet mellan frågor kopplade till samhällets digitalisering, demokrati, innovation och livslångt lärande.

Joakim Liljeberg

Chefsanalytiker på Tankesmedjan Fores. Tidigare politisk tjänsteman.

Patrik Oksanen

Patrik Oksanen är ledamot i Kungliga Krigsvetenskapsakademien och Kungliga Örlogsmannasällskapet. Han är säkerhetspolitisk rådgivare åt Fores, senior fellow Frivärld och verksam vid CTSS på Försvarshögskolan. Oksanen är också kolumnist, föreläsare och författare.

Carolina Angelis

Senior rådgivare vid Truesec Human Threat Intelligence, med närmare tjugo års erfarenhet från svensk underrättelsetjänst. Carolina Angelis är också författare till en serie spionromaner och är högaktuell med Dominoeffekten (Saga Egmont förlag 2022).

Patrik Fältström

Patrik Fältström, ledamot av Kungliga Ingenjörsvetenskapsakademien samt belönats med Terra Mariana-korsets orden av Estlands president, är teknik- och säkerhetsskyddschef på Netnod som tillhandahåller grossisttjänster relaterat till internet, som till exempel distribution av tid och frekvens i Sverige. Patrik är dessutom på uppdrag av Försvarsmakten lagledare för det svenska laget i tävlingen Locked Shields som Nato forskningscenter CCDCOE i Tallinn anordnar.

Stefan Kristiansson

Generalmajor, före detta chef för MUST, den militära underrättelse- och säkerhetstjänsten, och sedan flera år verksam som rådgivare vid ett flertal företag.

Referenser

Corballis, T., & Soar, M. (2022). Utopia of abstraction: Digital organizations and the promise of sovereignty. *Big Data & Society*, *9*(1), 205395172210845. https://doi.org/10.1177/20539517221084587

De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of Internet governance. *International Journal of Law and Information Technology*, *30*(1), 68–87. https://doi.org/10.1093/ijlit/eaac004

Digital Sovereignty 2.0. (n.d.). Retrieved June 1, 2022, from https://www.youtube.com/watch?v=MOYM5nP7T-fk&t=648s

Filippi, P. D., & McCarthy, S. (n.d.). *Cloud Computing: Centralization and Data Sovereignty*. 21.

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, *33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1), 205395172098201. https://doi.org/10.1177/2053951720982012

Kaloudis, M. (2021). Digital sovereignty–European Union's action plan needs a common understanding to succeed. *History Compass*, *19*(12). https://doi.org/10.1111/hic3.12698

Lessig, L., & Lessig, L. (2006). *Code* (Version 2.0). Basic Books.

Martin, A., Sharma, G., Peter de Souza, S., Taylor, L., van Eerd, B., McDonald, S. M., Marelli, M., Cheesman, M., Scheel, S., & Dijstelbloem, H. (2022). Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions. *Geopolitics*, 1–36. https://doi.org/10.1080/14650045.2022.2047468

Moerel, E. M. L., & Timmers, P. (2021). *Reflections on Digital Sovereignty*. https://ssrn.com/abstract=3772777

Nugraha, Y., Kautsarina, & Sastrosubroto, A. S. (2015). Towards data sovereignty in cyberspace. *2015 3rd International Conference on Information and Communication Technology (ICoICT)*, 465–471. https://doi.org/10.1109/ICoICT.2015.7231469

Pohle, J., & Voelsen, D. (2022). Centrality and power. The struggle over the techno- political configuration of the Internet and the global digital order. *Policy & Internet*, *14*(1), 13–27. https://doi.org/10.1002/poi3.296

Position Paper on the Application of International Law in Cyberspace. (2022). Swedish Government. https://www.regeringen.se/4a1ce0/contentassets/2bf3882c23bb4fdfb935310b03d562a1/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf

Prasad, R. (2022). People as data, data as oil: The digital sovereignty of the Indian state. *Information, Communication & Society*, *25*(6), 801–815. https://doi.org/10.1080/1369118X.2022.2056498

Roberts, Huw, Cowls, Josh, Casolari, Federico, Morley, Jessica, Taddeo, Mariarosaria, Floridi, & Luciano. (2021). Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies. *Internet Policy Review*. https://ssrn.com/abstract=3937345

T. Kukutai & John Taylor. (2016). *Indigenous Data Sovereignty: Toward an agenda*. https://doi.org/10.22459/caepr38.11.2016

Thompson, G. (2021). Democracy, citizenship, and corporate governance reform: How to deal with the internationalization of corporate activity. *Thesis Eleven*, *167*(1), 42–57. https://doi.org/10.1177/07255136211058481

Werthner, H., & van Harmelen, F. (Eds.). (2017). *Informatics in the Future: Proceedings of the 11th European Computer Science Summit (ECSS 2015), Vienna, October 2015*. Springer International Publishing. https://doi.org/10.1007/978-3-319-55735-9

REDAKTÖRER
JOAKIM LILJEBERG OCH PATRIK OKSANEN

SVEKET MOT CYBERSÄKERHETEN

I Staten sviker cybersäkerheten skriver sex författare om hur den svenska digitala säkerheten mår.

Vi har kunnat läsa och följa hur ransomware-attacker och främmande makts cybersoldater försöker slå ut vitala delar av den digitala infrastrukturen vi använder dagligen. Tyvärr blir vissa attacker lyckosamma och lönesystem släcks ned samtidigt som affärers kassasystem tvingas stänga.

Enligt EU-kommissionens rankning Digital Economy and Society Index (DESI) hamnar Sverige på plats 4 år 2022 över mest digitaliserade länder inom EU. Det uppkopplade och digitala samhället har tyvärr en baksida, det gör oss mycket mer känsliga för cyberattacker. För att skydda oss behövs en genomtänkt strategi och vilja som genomsyrar hela samhället, från det privata näringslivet till det kommunala lönesystemet.

Författarna berättar om varför vi ska skydda vårt digitala samhälle och hur vi ska göra det så effektivt som möjligt, vilken är egentligen den svagaste länken vid ett kraftfullt cybersäkerhetsförsvar och hur mår detsamma idag?

Den här antologin är årets viktigaste läsning om cybersäkerhet.

FORES

FSC www.fsc.org MIX Från ansvarsfulla källor FSC® C112370

ISBN: 978-91-87379-87-1