SVERIGES RIKSDAG

Motion till riksdagen 2023/24:461

av Hanna Gunnarsson m.fl. (V)

Cybersäkerhet

1 Innehållsförteckning

2 Förslag till riksdagsbeslut

1. Riksdagen ställer sig bakom det som anförs i motionen om att Sverige ska verka för ett internationellt regelverk kring cybersäkerhet och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör ta fram riktlinjer för hur outsourcing av it-verksamhet så långt det är möjligt ska kunna undvikas i den statliga förvaltningen och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör uppdra åt relevanta myndigheter att ta fram tydligare säkerhetskrav och villkor för upphandlingar på it-området samt på oberoende granskning och tillkännager detta för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att en it-haverikommission bör tas fram i samarbete mellan berörda myndigheter och tillkännager detta för regeringen.
5. Riksdagen ställer sig bakom det som anförs i motionen om att det i lagstiftningen bör införas en generell möjlighet att ogiltigförklara en uppsägning eller ett avskedande som utgör en repressalie på grund av att personen har rapporterat information om missförhållanden, och detta tillkännager riksdagen för regeringen.
6. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen snarast bör utreda och återkomma med ett förslag till statliga molntjänster där data och program ska kunna lagras på ett säkert sätt och tillkännager detta för regeringen.
7. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen i kontakter med länder som finansierar trollfabriker, såsom Ryssland, Turkiet och Kina, tydligt bör markera mot sådana metoder och kräva ett stopp på det statliga stödet till dessa aktiviteter och tillkännager detta för regeringen.
8. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör ge relevanta myndigheter i uppdrag att inrätta ett kunskapslyft för lärare i medie- och informationskunskap och tillkännager detta för regeringen.
9. Riksdagen ställer sig bakom det som anförs i motionen om att det ska krävas att AI är utvecklad i enlighet med en nationell policy med etisk kod för att den ska kunna användas av offentlig verksamhet och tillkännager detta för regeringen.

3 Inledning

Sverige och världen står i dag inför större utmaningar än på länge och vi befinner oss i ett i många avseenden nytt säkerhetspolitiskt läge. Utgångspunkten för Sveriges försvars- och säkerhetspolitik ska vara att värna vårt lands säkerhet. Det kräver en modern försvarsmakt som har förmågan att möta de olika former av hot som vårt land kan ställas inför. Ett framgångsrikt totalförsvar kräver dock att samhället i övrigt är robust och upprätthåller en hög nivå av säkerhet inom de samhällsviktiga strukturerna. Där utgör informations- och cybersäkerhet ett särskilt viktigt område.

Sverige utsätts för tusentals aggressiva cyberattacker varje dag, dygnet runt.[1] Våra svagheter utnyttjas av grupper som vill oss illa. Angriparna utgörs både av privata

[1] FRA, Björn Lyrvall, intervju Ny Teknik 20/2-20.

hackare, kriminella nätverk, terrororganisationer och stater. Framför allt Kina och Ryssland utför avancerade angrepp, både på företag och andra stater, men även Iran märks som en antagonist.[2] Även USA agerar aggressivt i cyberrymden.[3]

I dag bygger en stor del av den svenska krisberedskapen på att vi har fungerande it-system för t.ex. logistik och försörjning av el och vatten, men även för information till medborgarna. Vid ett haveri riskerar viktiga samhällsfunktioner att drabbas hårt eller rent av slås ut. Ett tryggt och robust system måste utgå från välgrundade och motiverade riskbedömningar. Det kräver både att det finns tillräcklig kunskap och kompetens och att arbetet sker regelbundet och systematiskt med återkommande uppföljning.

Sverige är ett av de mest digitaliserade länderna i världen. Det är på många sätt en tillgång och öppnar upp för nya möjligheter att bedriva verksamhet både offentligt och i det privata näringslivet. Rätt använt kan digitaliseringen göra våra liv bättre och vårt samhälle mer effektivt. Men den ökade digitaliseringen innebär även ökade digitala risker. Sakernas internet eller det s.k. Internet of Things innebär att allt fler saker är uppkopplade mot internet. Det innebär också att enorma mängder information skickas och delas över nätet. Intelligenta hus, smarta elnät och mätningar av hälsodata kan ge mycket exakt information om privatpersoner såväl som större samhällsförändringar. I fel händer kan även sådan vardaglig information missbrukas.

Enligt Försvarsmakten kan en cyberattack få lika stora konsekvenser för samhällsviktiga funktioner som ett konventionellt väpnat angrepp. Även EU konstaterar att ett cyberangrepp under vissa förutsättningar kan likställas med ett väpnat angrepp.

4 Digital sårbarhet

Både individer och samhällsstrukturen kräver stora mängder av information för att vardagen ska fungera. Dagens informationshantering sker i hög utsträckning med hjälp av olika it-system. En hög it-användning leder ofta till effektivisering och mer välfungerande tjänster och verksamheter, men innebär även digitala säkerhetsrisker. Det har också skett en tydlig ökning av incidenter relaterade till internet och digitalisering, såsom dataintrång, bedrägerier, nedstängningar och spridning av skadlig kod. Vem som ligger bakom kan variera, men det kan handla om privatpersoner, organiserad brottslighet, terrorister och andra statsmakter. Spridning av skyddsvärd information kan ske p.g.a. slarv eller obetänksamhet, eller genom att någon aktivt ser till att skaffa sig den. Därutöver kan ett it-haveri ske p.g.a. naturkatastrofer eller andra olyckor som påverkar systemet.

Informationssäkerhet handlar om att all skyddsvärd information ska vara tillgänglig, riktig, konfidentiell och spårbar. En bristande informationssäkerhet riskerar att få förödande konsekvenser. Incidenter eller störningar som angriper den digitala infrastrukturen kan leda till omfattande problem för t.ex. de finansiella systemen, hälso- och sjukvården, livsmedelsförsörjningen, kommunikationen med medborgarna eller den nationella säkerheten. När hanteringen av viktig information brister riskerar detta också att leda till ett försämrat förtroende för etablerade samhällsstrukturer.

Ett angrepp på svensk infrastruktur kan ha olika syften och utföras på olika sätt. Det kan handla om att försöka komma åt skyddsvärd information, kartlägga system eller

[2] Säpo Lägesbilder 2022/2023.
[3] New York Times 2019, U.S. Escalates Online Attacks on Russia's Power Grid.

nyckelpersoner. Men det kan också handla om överbelastningsattacker för att störa ut specifika tjänster och funktioner, för att försvåra för vårt samhälle att fungera som det ska. Försvarsberedningen skriver i sin rapport Allvarstid (Ds 2023:19) om hur ”även till synes begränsade angrepp kan orsaka svårigheter och skapa oro bland befolkningen”. Det är därför centralt att motverka även mindre angrepp.

Det är i detta sammanhang viktigt att vara medveten om de regionala förutsättningarna och riskerna. Som exempel kan nämnas it-attacken mot Coop den 2 juli 2021. En it-attack mot matvarukedjan fick kassasystemet att haverera och många butiker var tvungna att stänga. För en liten ort med bara en butik får ett sådant haveri stora konsekvenser i enskilda människors vardag och kan leda till rädsla och otrygghet.

Det är av stor vikt att vi ser svensk cybersäkerhet som en helhet. Hela samhället måste ha ett starkt skydd för information och mot cyberangrepp, vi är inte starkare än den svagaste länken. I en enkät till verksamhetsledare gjord av tankesmedjan Fores fick frågan om huruvida myndighetsstöd är tillfredsställande lägst betyg av alla frågor. Vänsterpartiet menar att staten och det offentliga samhället har ett speciellt ansvar att ge stöd och hjälp till andra verksamheter för att hela samhället ska vara tryggt och säkert. Det finns stora behov av koordinering, råd, stöd, informationsutbyte och övningar, så att inte alla verksamheter, kommuner eller företag måste utveckla helt egna lösningar.

Att skyddsvärd information skulle komma obehöriga till del kan innebära en nationell säkerhetsrisk, men också ett enskilt hot mot de individer som eventuellt drabbas. Att hemliga identiteter offentliggörs, att journalisters källor avslöjas eller att uppgifter om vem som arbetar på viktiga nyckeltjänster inom t.ex. polisen blir tillgängliga undergräver i förlängningen det demokratiska samhället. Den offentliga förvaltningen kräver en nödvändig tillit mellan medborgare och stat. Myndigheter som samverkar måste våga göra det utan att uppleva att informationen hanteras på ett otillfredsställande sätt.

4.1 Cyberattacker och hybridkrigföring

Det nya omvärldsläget har gjort att Försvarsmakten behöver ställa om. Det handlar både om ett nytt säkerhetspolitiskt läge och inte minst om ett behov av att öka förmågan att hantera cyber- och hybridkrigföring.

Hybridkrigföring karaktäriseras av en kombination av traditionella militära medel och irreguljära och civila metoder, som t.ex. psykologisk krigföring, politisk påverkan, it-angrepp, elektronisk krigföring osv. Gränsen för vad som är hybridkrigföring är svårare att avgöra än vid ett militärt angrepp. Så kallad gråzonsproblematik kan förstås ses som ett tillstånd mellan krig och fred, där hybridkrigföring ofta utgör en central del.

Syftet med att använda en gråzonsstrategi är att vinna fördelar och uppnå politiska mål utan att behöva möta eskalering och starka motåtgärder.[4] Det ger också en möjlighet att testa eller demonstrera förmågor och studera förmågan att försvara sig mot dessa, utan att det leder till en kraftfull konflikt. Men det kan också övergå i väpnat angrepp. Inför Rysslands fullskaliga attack mot Ukraina märktes t.ex. en hög aktivitet av ryska cyberattacker i syfte att destabilisera landet innan den militära invasionen. Även Ukrainas grannländer har utsatts för ryska cyberangrepp.

Det märks också att fysiskt övertagande och förstörelse av internetinfrastruktur är en viktig del av den mer traditionella krigföringen på marken. Enligt den ukrainska

[4] FOI, Gråzonsproblematik och hybridkrigföring – påverkan på energiförsörjning 2018.

regeringen hade omkring 15 procent av landets internetinfrastruktur förstörts i juni 2022.[5]

Trots att Sverige inte befinner sig i konflikt med något annat land beskriver Björn Lyrvall, generaldirektör på FRA, hur Sverige i någon bemärkelse redan befinner sig i en slags gråzon.[6] Det har på senare år skett en väsentlig ökning vad gäller antalet aggressiva attacker mot svensk kritisk infrastruktur. Det gäller inte minst mot myndigheter och statliga bolag. Även attackerna mot svensk sjukvård tycks ha ökat kraftigt.[7,8] Enligt Europeiska unionens byrå för cybersäkerhet (Enisa) är offentlig förvaltning/regering den sektor som är överlägset mest utsatt för cyberhot.[9]

Internationellt samarbete är helt nödvändigt för en fungerande cybersäkerhet. Oavsett hur stark den nationella säkerheten på cyberområdet är, måste frågan om cybersäkerhet oundvikligen betraktas som en internationell sådan. Det handlar både om hur stater själva agerar mot varandra och hur stater agerar gentemot andra aktörer. Inom EU finns direktiv om nät- och informationssäkerhet (NIS och NIS2) som omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster. Men det saknas fortfarande ett gemensamt internationellt regelverk kring cybersäkerhet.

Sverige ska verka för ett internationellt regelverk kring cybersäkerhet. Detta bör riksdagen ställa sig bakom och ge regeringen till känna.

5 Totalförsvaret

Ett starkt totalförsvar kräver ett robust samhälle i alla delar. Det fordrar ett robust cyberförsvar med en god förmåga till cyberoperationer. Men det innebär också en väl utbyggd välfärd där kommuner och regioner har tillräckliga resurser för att bedriva en god verksamhet både på daglig basis och vid ansträngda lägen. En välfärd, i alla dess delar, som inte fungerar i normalläge kommer ha svårt att hantera större kriser. Det är därför av största vikt att kommuner och regioner förstår sin del i totalförsvaret och hur dagliga beslut och i värsta fall nedskärningar påverkar helheten och totalförsvaret i stort. Fungerande it-system och cybersäkerhet är en del av det arbetet. I propositionen Totalförsvaret 2021–2025 (prop. 2020/21:30) konstateras att förmågan att i fredstid hantera antagonistiska hot behöver förbättras, bl.a. vad gäller cyberattacker.

Vänsterpartiet ser vikten av att stärka det civila försvaret inom samhällets alla områden. Det civila försvaret ska dimensioneras och planeras för både kris och krig. Ett utökat och utvecklat civilt försvar innebär bland mycket annat förbättrad informations- och cybersäkerhet. Där kan Nationellt cybersäkerhetscenter som nu är under uppbyggnad spela en viktig roll.

För att upprätthålla en god cybersäkerhet är det nödvändigt att hela tiden ligga i framkant vad gäller utveckling på området. Därför är forskning, utveckling och internationellt samarbete viktiga komponenter.

[5] Enisa Threat Landscape 2022.
[6] Intervju TT, 20 feb 2020, https://www.nyteknik.se/nyheter/fra-aggressiva-cyberattacker-mot-sverige-varje-dag/599122.
[7] Företaget Check Point Research, https://go.checkpoint.com/2023-cyber-security-report/chapter-01.php.
[8] https://lakartidningen.se/aktuellt/nyheter/2023/02/okade-it-attacker-mot-sjukvard/.
[9] Enisa Threat Landscape 2022.

Frivilligorganisationerna inom det civila försvaret har stor betydelse för totalförsvarets samhällsförankring och fungerar också som ett stöd till Försvarsmakten. Det är en nödvändig del av totalförsvarsplaneringen att öka uthålligheten i verksamheter som angränsar till cyberförsvaret och för att upprätthålla cybersäkerheten på bredden. Försvarsmakten fattade 2022 därför beslut om att ge uppdrag till Frivilliga radioorganisationen (FRO) att utveckla verksamheten inom cyberförsvar och cybersäkerhet. Vänsterpartiet vill understryka vikten av att cybersäkerhet blir en fråga för samhällets alla delar.

5.1 Statligt och offentligt ansvar, ägande och drift

Den offentliga förvaltningen, framför allt på statlig nivå, hanterar dagligen mängder av information. Mycket av det som skapas och lagras är både viktigt och känsligt. Vissa uppgifter klassas som skyddsvärda och en del rör även rikets säkerhet, medan andra uppgifter innehåller mycket information om enskilda individer. Om informationen går förlorad, stjäls, manipuleras eller sprids till obehöriga kan det få allvarliga följder. Konsekvenserna kan t.ex. vara att integritetskänsliga uppgifter sprids, betalningar uteblir, el- eller vattenförsörjningen störs eller att uppgifter om samhällsviktiga funktioner kommer obehöriga till del.

De senaste årens stora privatiseringar och utförsäljningar av offentlig verksamhet har gjort att det offentliga samhället inte längre har rådighet över den samhällsviktiga verksamheten. Detta är inte bara ett demokratiproblem, att verksamhet som vi alla borde ha makten över i stället drivs av privata företag, ofta i vinstintresse, utan också ett säkerhetsproblem. Privatiseringar betyder att det offentliga samhället inte längre har den totala insynen och makten, utan att denna ligger någon annanstans, i värsta fall på ett företag med koppling till en annan stat. Vi har de senaste åren sett hur framför allt kinesiska företag med starka kopplingar till den kinesiska staten investerar strategiskt i, och tar över, samhällsviktig infrastruktur i andra länder.

Denna utveckling gör att privatiserade verksamheter blir svåra att samordna och styra och gör i värsta fall vårt samhälle väldigt sårbart vid kriser. Vänsterpartiet menar att denna utveckling måste brytas och att stora förändringar måste göras.

Vi menar att det är i medborgarnas intresse att verksamheter och infrastruktur som är viktiga för samhällets utveckling ägs av medborgarna gemensamt, genom staten, regionerna eller kommunerna. Detta gäller t.ex. utbyggnaden av 5G-infrastrukturen. Det är bra att regeringen de senaste åren har tagit initiativ till lagstiftning för att öka säkerheten vid uppköp av samhällsviktig verksamhet, men Vänsterpartiet anser att det är av stor betydelse att sådana verksamheter i stället ägs och drivs offentligt.

För att Sverige ska klara av att hålla en hög nivå av kompetens på it-säkerhetsområdet krävs att utbildningsväsendet förmår att tillhandahålla tillräcklig utbildning, både vad gäller kvantitet och kvalitet. Också möjligheterna till vidareutbildning är centrala. Där spelar högskolor, universitet och annan vuxenutbildning en viktig roll. Vänsterpartiet ser positivt på regeringens planer att skapa ett cybercampus i syfte att utbilda fler experter på cybersäkerhet och främja forskning på området.

5.1.1 Myndigheternas ansvar för informationssäkerhetsarbete

Både Riksrevisionen och Säpo har tidigare riktat kritik mot bristande it- och informationssäkerhet hos flera myndigheter. Bland annat har myndigheternas förutsättningar för ett effektivt informationssäkerhetsarbete liksom uppföljningsarbetet varit alltför dåligt.

Nivån på informationssäkerheten hos de granskade myndigheterna är dessvärre inte tillräcklig och förståelsen för vikten av en god informationssäkerhet är överlag alltför liten. Det får i sin tur till följd att arbetet inte prioriteras tillräckligt i förhållande till riskerna. Skydd av it och information måste betraktas som en kärnverksamhet av alla, både offentliga och privata verksamheter, och tilldelas de resurser som krävs. Det krävs såklart också utbildad personal, vilket det i dag är brist på inom detta område. Ytterst är det regeringens ansvar att se till att det finns nödvändiga förutsättningar för myndigheterna. I samband med en ökad digitalisering är det centralt att säkerhetsaspekten finns med från början. En förutsättning för att myndigheterna ska kunna ligga i framkant vad gäller säkerhetsarbetet är rätt kompetens och effektiva beslutsvägar.

Samtidigt som myndigheterna inte klarar av att hantera uppgifterna är det dominerande påbudet att allt fler it-områden ska läggas ut på entreprenad. En politisk vilja till ökad outsourcing av it-tjänster måste sättas i relation till vilka säkerhetsrisker det kan medföra. När kortsiktig vinst blir en drivkraft för att upprätthålla fungerande it-system sätts långsiktigheten på undantag och helheten går förlorad. Outsourcing av skyddsvärda uppgifter bör endast ske i undantagsfall.

Regeringen bör ta fram riktlinjer för hur outsourcing av it-verksamhet ska kunna undvikas i den statliga förvaltningen. Detta bör riksdagen ställa sig bakom och ge regeringen till känna.

Om upphandlingar på it-området ändå sker måste tydliga säkerhetskrav finnas med redan i inledningsskedet. Det är centralt att både beställare och köpare har nödvändig kompetens för att avgöra vilka säkerhetslösningar som krävs. Krav såväl som genomförande bör också så långt det är möjligt granskas av en oberoende aktör.

Regeringen bör uppdra åt relevanta myndigheter att ta fram tydligare säkerhetskrav och villkor för upphandlingar på it-området samt på oberoende granskning. Detta bör riksdagen ställa sig bakom och ge regeringen till känna.

Sammanfattningsvis har informationssäkerhetsarbetet inom staten under lång tid varit alltför dåligt. Att Riksrevisionen konstaterar att arbetet med informationssäkerhet inte når upp till en godtagbar nivå är allvarligt, liksom att regeringen inte har försäkrat sig om att det finns nödvändiga förutsättningar för myndigheterna att upprätthålla en god nivå. Det innebär att problemet är omfattande och att den enskilda myndigheten i sig inte har tillräckliga verktyg för att komma till rätta med de problem som finns.
I stället har man lagt ut en allt större andel av it-verksamheten på externa aktörer, vilket i flera uppmärksammade fall fått stora negativa konsekvenser.

Myndigheten för samhällsskydd och beredskap (MSB) har efterlyst ett bättre samarbete med privata aktörer för att möta det ökade antalet cyberattacker.[10] Ett sådant samarbete är positivt men får inte innebära att statliga myndigheter ersätter sin egen it-kompetens med externa aktörer.

Alla statliga myndigheter ska i dag rapportera allvarliga it-incidenter till MSB. Syftet är bl.a. att skapa förutsättningar för att vidta rätt skyddsåtgärder och utveckla förmågan att förebygga och hantera framtida incidenter. Det är bra och viktigt. Vänsterpartiet menar att omfattande it-incidenter i högre grad behöver rapporteras, följas upp och granskas i en sammanhållen process. Det gäller alla större incidenter med en samhällelig påverkan, även lokalt. Obligatoriet omfattar myndigheter, men även andra organisationer kan välja att rapportera frivilligt. Här finns utrymme för att öka privata aktörers vilja att delta i rapporteringen. Det kräver ett system som möjliggör att företag

[10] https://sverigesradio.se/artikel/msb-kravs-mer-samarbete-om-it-sakerhet.

och organisationer kan lämna ifrån sig tillräcklig information utan att det i sig utgör en säkerhetsrisk.

En it-haverikommission bör tas fram i samarbete mellan berörda myndigheter. Detta bör riksdagen ställa sig bakom och ge regeringen till känna.

Att teknik som möjliggör övervakning används på rätt sätt är avgörande för förtroendet för statsförvaltningen. Det måste alltid finnas möjlighet till granskning även av känsliga förfaranden. Arbetstagare som slår larm om missförhållanden på sin arbetsplats, s.k. visselblåsare, ska ha ett starkt skydd mot repressalier. Det är en förutsättning för att arbetstagare ska våga larma om missförhållanden och en grundläggande del av ett fritt och demokratiskt samhälle.

Det bör i lagstiftningen införas en generell möjlighet att ogiltigförklara en uppsägning eller ett avskedande som utgör en repressalie p.g.a. att personen har rapporterat information om missförhållanden. Detta bör riksdagen ställa sig bakom och ge regeringen till känna.

Läs mer om skydd för visselblåsare i vår motion (2020/21:4086) med anledning av prop. 2020/21:193 Genomförandet av visselblåsardirektivet.

Regeringen och Sverigedemokraterna har i Tidöavtalet kommit överens om att tjänstemannaansvar ska införas. För oss är det grundläggande att ansvariga chefer och politiker tar sitt ansvar för att strukturerna och personalförsörjningen på myndigheterna är välfungerande och bra och att det finns en tillräcklig kompetensnivå för att i så stor utsträckning som möjligt undvika att fel begås. Det gäller inte minst på it-säkerhetsområdet. Vänsterpartiet vill därför inte återinföra tjänstemannaansvaret i samma form som det såg ut förut.

5.1.2 Statlig molntjänst

Att lagra data digitalt över internet via ett s.k. moln blir allt vanligare och tillämpas i stor utsträckning i offentlig sektor. Men det finns stora säkerhetsutmaningar med detta. Statens servicecenter har redan 2017 i rapporten En gemensam statlig molntjänst för myndigheternas it-drift, föreslagit en säker hantering av data genom en statlig molntjänst i form av statligt ägda serverhallar för lagring åt offentlig sektor. Statens servicecenter konstaterar också att en molntjänst bör ha sitt säte utanför storstadsområdena för att stärka säkerheten och öka effektiviseringen för att sänka kostnaderna. Vänsterpartiet anser vidare att ett statligt moln också skulle kunna hantera lagringen åt privata företag, och verksamheten skulle på sikt kunna bli lönsam för staten. Det gäller i synnerhet samhällsviktiga företag vars verksamhet är av särskild vikt att skydda. Dessvärre har regeringen agerat saktfärdigt och inkonsekvent, och någon statlig molnlösning har ännu inte sett dagens ljus.

Vänsterpartiet anser därför att regeringen snarast ska återkomma med ett förslag till en eller flera statliga molntjänster där data och program ska kunna lagras på ett säkert sätt. Molntjänsterna ska också, mot rimlig avgift, kunna hantera lagring åt andra aktörer än staten, om så önskas.

Regeringen bör snarast utreda och återkomma med ett förslag till statliga molntjänster där data och program ska kunna lagras på ett säkert sätt. Detta bör riksdagen ställa sig bakom och ge regeringen till känna.

5.2 Strategiska uppköp

Försvarsberedningen konstaterar i sin rapport Allvarstid (Ds 2023:19) hur ”Ny teknik ses av såväl Kina som USA som nyckeln till framtida konkurrenskraft inom både det militära och det civila området, och det pågår en teknikkapprustning länderna emellan”. Man skriver vidare hur ”Kinas strategiska uppköp av och investeringar i digital och fysisk infrastruktur kan fylla såväl civila som militära syften”. Det påverkar allt från produktionen av halvledare till olika former av antagonistiskt agerande i rymden.

Riksdagen har nyligen tagit beslut om ett granskningssystem för utländska direktinvesteringar till skydd för svenska säkerhetsintressen (prop. 2022/23:116) som innebär en ny lag som ger en granskningsmyndighet möjlighet att granska utländska direktinvesteringar och, om det är nödvändig, förbjuda dem. Vänsterpartiet menar att ett sådant granskningssystem är bra och nödvändigt. Strategiska uppköp är en stor utmaning mot ett robust och säkert samhälle då det riskerar att ge andra stater makt över samhällsviktiga företag, verksamheter och infrastruktur i Sverige, samt tillgång till känslig information om invånare i Sverige. Det är speciellt problematiskt när dessa uppköp eller investeringar görs av odemokratiska eller auktoritära stater som inte delar Sveriges syn på demokrati och mänskliga rättigheter. Vi menar dock att det finns ett behov av att gå längre än den föreslagna lagstiftningen. Även upphandlingar och investeringar i offentlig verksamhet som infrastruktur, skola, vård och omsorg bör omfattas av granskningssystemet. Detta är samhällsviktig verksamhet som är kritisk för vårt samhälles funktionalitet, och det får stora konsekvenser för det civila försvaret under större kriser om sådana företag exempelvis inte vill samarbeta om resurser och lösningar eller arbetar med andra mål än övriga samhället. Offentligt ägande och drift av samhällsviktiga verksamheter är att föredra framför privat, då det ger direkt demokratisk kontroll över verksamheten och möjlighet att planera samhällets samlade resurser utifrån en helhet.

6 Demokratiska aspekter

Det finns en stark koppling mellan fred, demokrati och vår gemensamma säkerhet. Dessvärre kan vi se att demokratin är under attack i vår omvärld. Hotet mot demokratin handlar i dag främst om att regeringar urholkar de demokratiska rättigheterna som fria och rättvisa val, tryck- och yttrandefrihet och likhet inför lagen. Demokratins tillbakagång måste alltså förstås bredare än att det enbart handlar om rena diktaturer.

6.1 Integritet

Digitaliseringen gör att skyddet för den personliga integriteten ställs inför nya utmaningar. Stora mängder persondata samlas in när vi använder oss av sociala medieplattformar, appar, elektroniska enheter, banktjänster och välfärdssystem. Det ger möjligheten att urskilja övergripande mönster som kan hjälpa oss som samhälle att analysera och förutsäga nuvarande och framtida beteenden för att samordna och optimera resurser och kompetenser. Men samma data kan också användas för att övervaka oss och för att övervaka våra beteenden. Persondata, ”big data”, säljs och används bl.a. av företag för att rikta reklam till tänkbara konsumenter.

Vänsterpartiet ser med stor oro på den utveckling som skett sedan början av 2000-talet och som i dag lett till att vi börjar närma oss ett övervakningssamhälle. Frågor om personlig integritet och mänskliga rättigheter får gång på gång stå tillbaka. Varje inskränkning har motiverats utifrån skenbart goda syften som effektivare brottsbekämpning och ett generellt ökat skydd för invånarna. Sammantaget framstår dock helheten av två decenniers skärpta lagar när det gäller t.ex. kamerabevakning, hemliga tvångsmedel, signalspaning, utlänningskontroll och åtgärder i syfte att hindra terrorism, som illavarslande. Varje inskränkning som godtas tenderar att bereda väg för ännu fler och mer ingripande åtgärder. Argument i stil med att den som har rent samvete inte har något att frukta riskerar att bli urvattnade floskler ju fler inskränkningar av den personliga integriteten som accepteras. Konsekvenserna för samhällsklimatet och demokratin på lång sikt är svåra att överblicka. Sverige befinner sig i en svår situation som i sig innebär ett hot mot vår demokrati om vi inte vänder utvecklingen tillsammans.

En ökad cyberförmåga måste hanteras varsamt. När de tekniska kunskaperna för massövervakning utvecklas måste regelverket vara tydligt. Brottsbekämpning och ett försvar av Sveriges gränser är naturligtvis av högsta prioritet. Samtidigt måste lagar och regler utformas för att undvika massövervakning och kontroll över de egna medborgarna. En förmåga att övervaka samtliga medborgares digitala kommunikation såsom t.ex. EU:s förslag om chat control innebär ett stort politiskt ansvar. Också utvecklingen av allt mer avancerad AI för med sig risker. Vänsterpartiet säger nej till chat control eftersom förslaget är alldeles för långtgående. Det är ett enormt intrång i rätten till privatliv och innebär massövervakning. Läs mer i vår motion Demokrati, integritet och transparens (2023/24:V627).

6.2 Propaganda och trollfabriker

Spridning av desinformation och ”fake news” leder till populism, politikerförakt och en försvagad demokrati och tillit till samhället och dess företrädare. Många gånger leder denna typ av desinformation också till ökad rasism, hat och risk för våld mot utsatta grupper i samhället. Propaganda är en central beståndsdel i psykologisk krigföring och inte minst i hybridkrigföring. Genom att försöka påverka sin egen befolkning, invånare i andra länder, makthavare eller andra kan man få igenom sin agenda utan att behöva sätta in militära medel. Eller så kan propagandan vara ett sätt att kratta manegen inför ett angrepp.

I sina försök att sprida den ryska världsbilden till andra länder och legitimera angreppet på Ukraina har Ryssland etablerat flera statliga medier – exempelvis Sputnik och RT (tidigare Russia Today) – som sänder nyheter till utlandet på flera språk. Dessa medier försöker sprida den ryska regimens officiella syn på händelserna i världen. Den ryska regimen har även upprepade gånger anklagats för försök att påverka opinion och valresultat i flera västländer. Man använder sig också av desinformation för att sprida osäkerhet och för att undergräva förtroendet för demokratiska samhällsstrukturer. Ett exempel är hur rysk desinformation och konspirationsteorier spreds om coronapandemin och covid-19-vaccinet. Ett annat är krigspropagandan i samband med Rysslands folkrättsvidriga krig mot Ukraina.

Trollfabriker är ett propagandaverktyg med syfte att påverka samhällsdebatten. Det kan t.ex. ske genom desinformation eller polariserande budskap på falska nyhetssidor och sociala medier. Tidigare har det framför allt handlat om människor som får betalt

för sina trollaktiviteter, men utvecklingen har gått mot att det i högre utsträckning handlar om AI-styrd spridning. Både statliga och privat finansierade trollfabriker förekommer, framför allt i auktoritära och icke-demokratiska stater.

I Sverige är det framför allt de ryska trollfabrikerna som har uppmärksammats. Där använder sig regimen av en trollfabrik under namnet Internet Research Agency (IRA). IRA sprider information med budskap som gynnar den ryska ledningen i sociala medier. Mueller-rapporten konstaterade 2019 att den ryska regeringen genom hackerattacker och påverkansoperationer försökte lägga sig i det amerikanska presidentvalet 2016. Sommaren 2018 rapporterade Dagens Nyheter om hur ryska trollfabriker sprider lögner och propaganda om Sverige. Majoriteten av inläggen handlar om brottslighet, invandring och muslimer. Under coronapandemin slogs ryska trollfabriker för att undergräva förtroendet för västerländska covid-19-vaccin. Kriget mot Ukraina har föranlett en omfattande krigspropaganda där falska nyheter blandas med AI-genererade klipp och vilseledande bilder. I mars 2022 dök t.ex. ett fejkat klipp på Ukrainas president Volodymyr Zelenskyj upp där han uppmanade sina landsmän att lägga ner vapnen.

Men även andra länder ägnar sig åt liknande aktiviteter. I Turkiet kan nämnas hur det styrande partiet AKP finansierar trollfabriken AK Trolls för att bl.a. öka stödet för Turkiets attacker i Syrien och för att undergräva förtroendet för oppositionspartier som HDP. I Kina betalas hundratusentals människor för att bedriva propaganda för det kinesiska kommunistpartiets räkning, populärt kallad 50 centsarmén, eftersom man får betalt per inlägg. Här i Sverige har tidningen ETC uppmärksammat hur Sverigedemokraterna betalat personer för att publicera propaganda helt i linje med hur trollfabrikerna agerar.

Även Sverige har blivit utsatt för liknande typer av påverkanskampanjer, där kampanjen mot den svenska socialtjänsten är ett aktuellt och tydligt exempel. I sådana situationer är det viktigt att hela samhället, inklusive vårt stora föreningsliv, hjälps åt att sprida korrekt information för att motverka felaktigheter.

Vänsterpartiet menar att utvecklingen med trollfabriker, propaganda och desinformation måste motarbetas. Användningen av dessa metoder behöver fördömas och lyftas i Sveriges diplomatiska kontakter med andra länder.

Regeringen bör i kontakter med länder som finansierar trollfabriker, såsom t.ex. Ryssland, Turkiet och Kina, tydligt markera mot sådana metoder och kräva ett stopp på det statliga stödet till dessa aktiviteter. Detta bör riksdagen ställa sig bakom och ge regeringen till känna.

6.2.1 Kunskapslyft för lärare

För att lärare ska ha möjlighet att bemöta faktaresistens och argumentera med elever vars åsikter influeras av framför allt alternativa medier och fake news krävs kompetenshöjande åtgärder. Det arbetet handlar om mer än vanlig källkritik. Rasistiska och sexistiska budskap har en stor spridning på nätet och för många unga är hat via nätet vardag i dag. De utsätts, ser andra utsättas och utsätter själva andra. De möter kränkningar, hot och trakasserier i bloggar, kommentarsfält och sociala medier.

Det är generellt svårt för människor att se skillnad på falska och sanna påståenden. De falska nyheter som sprids mest på nätet ser ofta trovärdiga ut. Så pass trovärdiga att de kan lura rutinerade journalister, politiker och experter. Stora delar av radikaliseringsprocesserna av enskilda personer och grupper sker via olika chattforum och dolda

webbplatser. Darknet och deep web används flitigt för att sprida antidemokratiska och våldsamma budskap.

Enligt Medieutredningen behövs en nationell MIK-reform (media- och informationskunskap) för att utveckla medborgarnas medvetenhet och förståelse för medieteknik, medielogik och hur deras egen medieanvändning i livets mikropauser har potentialen att påverka såväl dem själva som andra. Vänsterpartiet menar att det i nuläget endast är genom skolan som alla barn och unga kan nås av en fullgod MIK-undervisning. Det finns goda exempel på lokal och regional nivå, men dessa saknar resurser att nå alla på en nationell nivå. Vi vill därför börja med att ge lärare ett kunskapslyft i medie- och informationskunskap. Också källtillit är en viktig komponent i det demokratifrämjande arbetet. Om man inte vågar lita på etablerade medier skapas en misstro som gör att alla fakta värderas utifrån samma premisser. Det riskerar att skada den svenska demokratin, vilken i hög utsträckning bygger på tillit.

Regeringen bör ge relevanta myndigheter i uppdrag att inrätta ett kunskapslyft för lärare i medie- och informationskunskap. Detta bör riksdagen ställa sig bakom och ge regeringen till känna.

För att nå hela den svenska befolkningen och höja kunskapen om digitala sårbarheter och hur dessa motverkas behövs folkbildning. Precis som när samhället tidigare har genomgått stora förändringar på det digitala området, när persondatorer och smarta telefoner blev tillgängliga för alla, behövs informationsinsatser, möjlighet att lära mer, diskutera och hjälpas åt. Detta görs bäst genom folkbildning, hos studieförbund och föreningar.

6.3 En AI-policy med etisk kod

Artificiell intelligens (AI) är ett samlingsbegrepp för maskinbaserade system med förmågan att efterlikna mänsklig intelligens. Utvecklingen går snabbt framåt och har potential att ge en mängd ekonomiska och samhälleliga vinster. Samtidigt som det finns många positiva saker med AI som möjligheter till utveckling och effektivisering, t.ex. snabbare handläggning och beslut hos myndigheter, så finns också negativa sidor, särskilt inom brottsbekämpning och säkerhetsbranschen med ansiktsigenkänning, mer övervakning, ansvarsutkrävande och gråzonsproblematik.

AI bygger på statistiskt underlag. Om underlaget präglas av fördomar kommer utslaget att bli därefter. Det märks bl.a. i hur ansiktsigenkänning fungerar olika väl beroende på hudfärg och i hur olika rekryteringsverktyg föredrar män framför kvinnor. En dåligt fungerande AI riskerar att misstänkliggöra människor utifrån mänskliga förutfattade meningar.

AI-utvecklingen lyfter en rad frågor om bl.a. ägande, demokratisk kontroll och etiska principer. Även ansvarsfrågan är central. I mars 2023 uppmanade en rad ledande AI-forskare och experter världen att pausa utvecklingen av AI i ett halvår medan vi ser över vilka risker som finns och hur de kan motverkas. Experterna menade att den nödvändiga försiktigheten och planeringen kring AI saknas. Det finns behov av en öppen och transparent debatt om AI och om den reglering som måste till.

Att använda sig av AI i militära syften är inte i sig problematiskt. Det finns områden där teknologin kan användas för goda ändamål som t.ex. minröjning eller cybersäkerhet. Men att överlåta etiska avgöranden till algoritmer kan aldrig vara acceptabelt i en fri, demokratisk och rättssäker värld.

Det finns många exempel på hur AI-teknik såsom ansiktsigenkänning används av totalitära och reaktionära stater för att kontrollera sin befolkning. Den statliga övervakningen av uigurer i Kinesiska Xinjiang och ockupationsmaktens Israels ständiga kontroll av palestinier är bara två exempel. Men den omfattande övervakningen av civilbefolkningen förekommer även i andra länder. I indiska Hyderabad byggs t.ex. just nu världens största databas för ansiktsigenkänning.

Vänsterpartiet anser att etiska, integritets- och säkerhetsmässiga aspekter måste väga tungt vid all utveckling av AI, oavsett om det sker inom näringslivet, välfärden, rättsväsendet eller försvaret av Sverige. Just nu pågår arbetet med EU:s AI-förordning. Där regleras AI i olika risknivåer som sedan ligger till grund för hur den ska hanteras. Förordningen kan komma att spela stor roll för utvecklingen även utanför EU.

Vi vill se en nationell policy med etisk kod för användning och utveckling av AI.

För att AI ska kunna användas av offentlig verksamhet ska det krävas att den är utvecklad i enlighet med en nationell policy med etisk kod. Detta bör riksdagen ställa sig bakom och ge regeringen till känna.

I väntan på en sådan bör man i offentlig verksamhet använda sig av de riktlinjer för AI som redan finns. Där kan t.ex. Unescos rekommendation om etik och artificiell intelligens vara en utgångspunkt. Läs mer i vår motion Demokrati, integritet och transparens (2023/24:V627).

6.3.1 Förbud mot mördarrobotar

Helt autonoma vapensystem är system som förmår agera helt utan mänsklig kontroll. Till skillnad från en obemannad drönare som kontrolleras av en pilot som fjärrstyr den har helt autonoma vapensystem förprogrammerade algoritmer som själva väljer ut sina mål. Sådana system kallas ofta för killer robots eller mördarrobotar, eftersom de har programmerats till att avgöra frågor om liv och död. I dag utvecklar 12 stater den typen av system. Däribland Kina, Ryssland, Frankrike, Storbritannien och USA. Även Sverige bidrar till utvecklingen genom företaget Saab som partner till det franska företaget Dassault.

Vänsterpartiet menar att helt autonoma vapensystem bör förbjudas enligt internationell lag. Sverige ska aldrig vara med och främja utvecklingen av eller delta i annan verksamhet som rör helt autonoma vapensystem. Läs mer i vår motion Förbud mot mördarrobotar (2023/24:V320).

Hanna Gunnarsson (V)

Andrea Andersson Tay (V)

Kajsa Fredholm (V)

Lotta Johnsson Fornarve (V)

Håkan Svenneling (V)

Linda W Snecker (V)