Sverige i en digital värld

En strategi för Sveriges utrikes- och säkerhetspolitik inom cyberfrågor och digitala frågor

Innehåll

Förord

Den utrikes- och säkerhetspolitiska dagordningen för att hantera cyberfrågor och digitala frågor växer i omfattning och betydelse. Framväxten av nya strategiska digitala tekniker som artificiell intelligens, kvantteknik, avancerade halvledare och nästa generationens kommunikationsnätverk (6G) är viktiga faktorer för internationellt samarbete och globala maktförhållanden. EU är, i kraft av sin roll som ledande global aktör, med en bredd av instrument till förfogande, Sveriges viktigaste utrikespolitiska plattform också kring cyberfrågor och digitala frågor.

Sverige ska föra en solidarisk politik inom ramen för EU och Nato samt, utifrån våra utrikespolitiska intressen och värderingar, vara en central aktör i internationella sammanhang, inklusive i förhållande till strategiska partners. Samarbetet med den privata sektorn om internationella och gränsöverskridande hot och angrepp är också en viktig del. För att stärka Sveriges roll och inflytande internationellt är det avgörande att driva en sammanhållen och integrerad utrikes- och säkerhetspolitik inom cyberfrågor och digitala frågor. Hela utrikespolitiken – säkerhet, handel och bistånd – berörs. Det är mot denna bakgrund som denna strategi ska ses. Ytterst handlar det om att värna Sveriges säkerhet, välstånd och konkurrenskraft

För svensk utrikesförvaltning handlar arbetet med cyberfrågor och digitala frågor om att främja svensk innovation och industri, främja svenska värderingar och intressen, stärka utvecklingssamarbetet samt fördjupa säkerhetspolitiska samarbeten i syfte att stärka Sveriges bemötande, motståndskraft och avskräckningsförmåga med fokus på statliga antagonistiska aktörer.

Denna strategi ligger i linje med regeringens nationella säkerhetsstrategi. Den är även utformad för att fungera ömsesidigt förstärkande med den nationella cybersäkerhetsstrategin som kommer beslutas under 2025. Nationell förmåga och utrikes- och säkerhetspolitiska instrument hänger nära samman. Genom en samlad ansats står sig Sverige starkare.

Maria Malmer Stenergard

Utrikesminister

En digital värld

Det internationella systemet befinner sig i en snabb förändring där frågor om cyber och digitalisering utgör en central del av den globala utvecklingen. Det blir allt mindre meningsfullt att skilja på den digitala och fysiska verkligheten, inklusive inom utrikes- och säkerhetspolitiken. Den geopolitiska dynamik som utspelar sig i den fysiska världen har sin spegelbild i den digitala miljön.

Nätverks- och informationssystem utgör i allt högre grad den underliggande infrastrukturen för alla delar av våra samhällen. Beroendet av den digitala infrastrukturen och utvecklingen av kommande generationer av telekominfrastruktur fördjupas genom bland annat utbyggnaden av 5G/6G.

Utvecklingen innebär att frågor om teknik, ekonomi, demokrati och säkerhet alltmer sammanflätas i internationella relationer. Framväxande teknik, som artificiell intelligens, förväntas få en avgörande betydelse för maktförhållanden och den geopolitiska konkurrensen. Säkerhetspolitiken behöver hantera hot på nya arenor, där samhällsviktiga tjänster kan slås ut på distans utan kinetisk verkan och kostnaden för att idka otillbörlig informationspåverkan blir försumbar.

Den digitala ekonomin blir allt viktigare för nationellt välstånd och samtidigt en tydligare del av geopolitiken. Digitaliseringen kan bidra till att lyfta länder ur fattigdom och bidra till tekniksprång, men en digital utveckling som inte bygger på demokratiska värderingar kan i stället bidra till mer auktoritära samhällen.

Offentliga och privata aktörer i Sverige utsätts återkommande för cyberangrepp från främmande makter. Förmågan att hantera och bemöta antagonistiska cyberhot mot centrala system och tjänster blir därför avgörande. Effektiv avskräckning på cyberområdet uppnås genom en trovärdig resiliens och en förmåga att vidta svarsåtgärder.

Denna strategi lägger grunden för en sammanhållen och integrerad utrikes- och säkerhetspolitik inom cyberfrågor och digitala frågor och syftar ytterst till att värna Sveriges säkerhet, välstånd och konkurrenskraft. Övergripande svenska prioriteringar handlar om att befästa en global, öppen, fri och säker cyberrymd med rättsstatens principer som grund. EU, Nato, bilaterala strategiska partnerskap samt samarbete med den privata sektorn är särskilt betydelsefulla för att få genomslag för svenska intressen och prioriteringar.

1.Säkerhetspolitik

Sverige står inför en rad utmaningar inom området för cyberfrågor och digitala frågor som behöver bemötas, integreras och hanteras i ett säkerhetspolitiskt sammanhang. Det handlar om att främja svensk innovation och industri, främja svenska värderingar och intressen,

fördjupa säkerhetspolitiska samarbeten om ny teknik samt i syfte att stärka Sveriges motståndskraft, avskräckningsförmåga och bemötande av externa cyberhot, med fokus på statliga antagonistiska aktörer.

Strategiska digitala tekniker

Framväxten av nya strategiska digitala tekniker som artificiell intelligens, kvantteknik, avancerade halvledare och nästa generationens kommunikationsnätverk (6G), kommer vara en viktig drivkraft i global politik och påverka internationellt samarbete och globala maktförhållanden. Kontrollen över teknik, data, liksom över nödvändiga råvaror, komponenter och kunskap används allt oftare som ett instrument i det geopolitiska maktspelet. Detta får konsekvenser för produktion, världshandeln och globala värdekedjor.

I synnerhet utvecklingen av AI behöver förstås ur ett geopolitiskt perspektiv. Från en säkerhetspolitisk synvinkel kommer de omfattande investeringar som nu görs i AI-forskning och relevanta tillämpningar att påverka den framtida maktbalansen mellan stater. En slags AI-kapplöpning har inletts, inte olik den som skett på andra tekniska områden med säkerhets- och försvarspolitisk tillämpning. Samtidigt som användningen av AI har stor potential att bidra till lösningar på globala utmaningar finns det också risker, som kräver både reglering och internationellt samarbete.

Sverige är ett framstående land inom forskning och utveckling av ny teknik och har goda förutsättningar att på flera områden ligga i framkant och påverka utvecklingen av regler, normer och standarder för ny teknik. Internationellt samarbete och partnerskap är centralt i forskning och innovation samt nödvändigt för att säkra vår tillgång till kompetenser, teknik, kapital, råvaror och komponenter. Sverige ska uppfattas som en kompetent och pålitlig partner i hanteringen, användningen och kontrollen av kritisk teknik, liksom i utvecklingen av globala standarder, normer och regelverk.

Det finns ett stort utländskt intresse för svensk teknikutveckling. Intresset är positivt och leder till kommersiella samarbeten och utländska direktinvesteringar. Men det finns även utmaningar med uppköp av svenska företag, inte minst forskningsintensiva små företag, samt i ökad utsträckning även industrispionage. Det finns därför ett behov av att skydda nationella säkerhetsintressen.

Den snabba utvecklingen av teknik med dubbla användningsområden skapar nya utmaningar i att hantera framväxande skyddsvärda tekniker ur ett exportkontrollperspektiv. I många fall har tekniken ännu inte listats i de internationella exportkontrollregimerna (till exempel Wassenaar-arrangemanget) vilket ställer krav på stater, inklusive Sverige, att nationellt skydda sin teknik för att hindra att den sprids till oönskade mottagare.

Internets fortsatta utveckling är nära sammankopplat med framväxten av ny digital teknik och utgör i sig självt ett strategiskt intresse. Sverige ska fortsatt verka för ett öppet, globalt och

interoperabelt internet som styrs genom flerpartssamverkan. Auktoritära länders strävan efter ökad statlig kontroll, även på global nivå, ska motverkas.

Utrikes- och säkerhetspolitisk hantering av antagonistiska cyberhot och cyberangrepp

Ett antal länder genomför cyberangrepp mot Sverige. Förmågan att hantera cyberhot och cyberangrepp är grundläggande för Sveriges säkerhet. Cyberangrepp kan handla om underrättelseinhämtning av olika slag, men också om aktiviteter som syftar till att påverka eller manipulera tillgängligheten i olika tjänster och system, eller rentav förstöra dem. Detta genomförs även som ett av flera olika instrument i hybridoperationer för att påverka Sverige och skada svenska intressen. Därutöver måste Sverige utgå från att mer kraftfulla offensiva cyberangrepp kan riktas mot mål i Sverige i händelse av en ytterligare försämrad säkerhetspolitisk utveckling.

Sverige ska föra en solidarisk politik inom EU och Nato. Det regelbaserade internationella systemet, försvaret av demokrati, respekten för FN-stadgan, och skydd för mänskliga rättigheter är fortsatt grundläggande för utrikespolitiken. Mot bakgrund av de skärpta geopolitiska spänningarna och att cyberhoten är gränsöverskridande, samt det svenska samhällets fortsatt snabba digitalisering, måste cyber- och digitaliseringsområdet integreras fullt ut i Sveriges utrikes- och säkerhetspolitik. Frågorna behandlas bilateralt, inom EU, Nato och OSSE, såväl som i den breda FN-kontexten.

Utlandsmyndigheterna har en viktig roll att bidra till Sveriges samlade lägesmedvetenhet. Sverige kommer även fortsatt att vara pådrivande i utvecklingen av utrikespolitiska och diplomatiska verktygslådor för att kunna bemöta hot och angrepp, mot Sverige, EU och Nato. Sverige ska också fortsatt vara en aktiv del av utvecklandet av internationella regelverk, rekommendationer och policys i syfte att höja den gemensamma cybersäkerheten och att stärka motståndskraften på cyberområdet. Även en effektiv brottsbekämpning på EU-nivå och internationellt är väsentlig. Det är av vikt att stärka utrikesförvaltningens kompetens, samt utveckla samverkan mellan utrikesförvaltningen, sakdepartementen och berörda myndigheter, avseende cyberfrågor och digitala frågor.

Arbetet för att direkt och indirekt bemöta statliga antagonistiska aktörer omfattar bland annat:

i) Motverka cyberhot och cyberangrepp

Internationell samverkan är av fundamental betydelse för att motverka hot mot freden och vår säkerhet, också inom cyberområdet. Detta bör främst ske inom ramen för EU och Nato i samverkan med andra likasinnade stater. Det innefattar samverkan och informationsutbyte kring lägesmedvetenhet, principer och rutiner för offentliga utpekanden och attribuering, samt olika typer av utrikespolitiska svarsåtgärder, till exempel uttalanden och riktade sanktioner.

Samarbetet inom EU och Nato samt med strategiska partners bidrar till avskräckning och motståndskraft. Sverige konstaterar, liksom Nato, att cyberangrepp under vissa förutsättningar kan likställas med ett militärt väpnat angrepp.

ii) Stärka motståndskraften och förbättra kapaciteten på cyberområdet genom internationellt samarbete

Internationellt cybersäkerhetssamarbete, inom ramen för bland annat EU och Nato, är även en viktig del i arbetet med att stärka motståndskraften och förbättra kapaciteten på cyberområdet både internationellt och nationellt. Internationella regelverk, liksom rekommendationer och policys, stödjer åtgärder för att skapa en hög gemensam cybersäkerhetsnivå. Sverige ska, i internationella samarbeten, verka för åtgärder som stärker och effektiviserar samverkan på cybersäkerhetsområdet i syfte att höja den gemensamma cybersäkerheten.

iii) Stärka tillämpningen av folkrätten och den internationella människorättslagstiftningen inom cyberområdet

Sverige eftersträvar efterlevnad av en regelbaserad världsordning. Folkrätten, inklusive FN-stadgan i sin helhet, den internationella humanitära rätten och mänskliga rättigheter, gäller även inom cyberområdet. Det finns dock ett behov av att närmare analysera hur folkrättens regler ska tolkas och tillämpas i en cyberkontext. Sverige ska verka för att folkrätten respekteras och tillämpas i cyberrymden. Sverige kommer att vara pådrivande i internationella diskussioner som rör folkrättens tillämpning inom cyberområdet.

iv) Verka för normer för staters ansvarsfulla uppträdande

Vid sidan av bindande folkrättsliga regler har ett antal icke-bindande normer och principer utvecklats. Längst har diskussionen kommit inom FN, där elva icke-bindande normer och principer för staters ansvarsfulla uppträdande i cyberrymden överenskommits. De rör grundläggande frågor som skyddet av kritisk infrastruktur, integritet för individer, motverkande av terrorism samt brottslig eller skadlig it-verksamhet, och internationell samverkan. Dessa normer utgör nu en viktig utgångspunkt för hur stater bör agera gentemot varandra i cyberrymden. Detta ramverk ger också förutsättningar för förbättrad dialog och utgör ett stöd för ansvarsutkrävande. Sverige ska verka för att existerande normer respekteras och tillämpas, samt i tillämpliga fall vidareutvecklas baserat på till exempel den globala utvecklingen och ny teknik.

v) Stärka förtroendeskapande åtgärder

Risken för missförstånd kring bakomliggande orsaker vid incidenter eller haveri i nätverks- och informationssystem är hög. Systemfel, handhavandefel och incidenter i samverkande system ger inte sällan samma slags utfall som vid cyberangrepp. Den tekniska analysen är ofta komplex och tidskrävande. Bristen på internationell transparens och förståelse för olika begreppsapparater kring cybersäkerhet ökar risken för konflikter. Både FN och OSSE har därför antagit ett antal förtroendeskapande åtgärder på cyberområdet. Sverige verkar för att

dessa ska konkretiseras, genomföras och utvecklas. Samverkan mellan incidenthantering och rättsvårdande verksamhet i utredning av störningar och incidenter inom ramen för internationella säkerhetssamarbeten eller gränsöverskridande myndighetssamverkan leder ofta till ökad transparens. Detta bidrar till att öka förtroende mellan parter och till att snabbare kunna fastställa faktiska orsaker till störningar. Sverige vill bidra till att internationella samarbeten kring praktiska förtroendeskapande åtgärder intensifieras.

vi) Värna det digitala informationsflödet

Det fria informationsflödet på internet utnyttjas i allt högre utsträckning för antagonistiska syften. En central fråga är hur demokratin, dess institutioner och processer bör försvaras mot informationspåverkan från illasinnade aktörer, samtidigt som repressiva krav på begränsningar av fria informationsflöden motverkas. Statliga aktörer som Kina och Ryssland, liksom våldsbejakande extremistiska grupper, nätverk och individer använder internet och sociala medier för spridande av propaganda och desinformation. AI som används för att filtrera och även generera innehåll riskerar förstärka polarisering och inverka negativt på konfliktsituationer, såväl inom som mellan stater. EU har tagit viktiga steg i att bli en globalt normgivande aktör på området. Samtidigt finns det aktörer som vill utnyttja den växande debatten kring plattformarnas inflytande och makt för att driva igenom mer repressiva normer. Sverige ska verka för att framväxande normer och regler ska utgå från folkrätten, ha ett rättighetsperspektiv och grundas i demokratiska principer samt bidra till goda förutsättningar för innovation och ökad konkurrenskraft. Sverige ska prioritera ökat skydd av demokratiska institutioner och processer från otillbörlig och skadlig informationspåverkan. Påverkan på valprocesser, med sikte på hela valcykeln är särskild viktig att uppmärksamma – nationellt såväl som på global nivå.

vii) Främja internationellt samarbete kring systemhotande cyberbrottslighet

De utrikespolitiska cybersäkerhetsdiskussionerna fokuserar på hot från statliga aktörer. En stor andel av cyberbrottsligheten är gränsöverskridande och har ofta flera aktörer inblandade. Det finns flera exempel på aktörer inom organiserad brottslighet med nära, men dolda, kopplingar till antagonistiska statliga aktörer. Stater kan också, genom att aktivt underlåta att ingripa mot organiserad cyberbrottslighet som bedrivs från eget territorium, använda dessa grupper som ett säkerhetspolitiskt instrument. Det finns vidare exempel på hur statliga aktörer har använt sig av metoder och verktyg från cyberbrottslighetens område i syfte att dölja sin verksamhet. Gränsen mellan icke-statliga och statliga aktörer är således ofta otydlig.

Cyberbrottslighet utgör ett gränsöverskridande problem, ofta med säkerhetspolitiska dimensioner, som kräver ett ökat internationellt samarbete för att kunna förebyggas och bekämpas effektivt. En effektiv och rättssäker brottsbekämpning är en förutsättning för att grundläggande rättigheter ska kunna upprätthållas och för att cyberområdet inte ska kunna utgöra en fristad för kriminella. Sverige kommer fortsatt att ta aktiv roll i internationella samarbeten, särskilt med utgångspunkt i gemensamt EU-agerande, mot cyberbrottslighet inkluderat i utrikespolitiska samarbeten. Det är samtidigt viktigt att nya instrument respekterar folkrättens regler inklusive mänskliga rättigheter, och inte används för att öka

staters kontroll över internets centrala infrastruktur, eller för att legitimera och underlätta förtryck.

Fokusområden – säkerhetspolitik

- Utveckla Sveriges internationella samarbeten kring AI och annan strategisk ny teknik, inklusive säkerhetsaspekter, med prioriterade samarbetsländer, organisationer och aktörer.
- Främja samarbete och interoperabilitet avseende regler och standarder mellan USA-EU och inom multilaterala fora. Försvara internets styrningsmodell som bygger på flerpartssamverkan.
- Utveckla, inom ramen för EU och Nato, Sveriges förmåga att avskräcka och bemöta externa cyberhot och cyberangrepp med utrikes- och säkerhetspolitiska instrument. Detta inbegriper en utvecklad nationell samordning kring lägesmedvetenhet, attribuering och svarsåtgärder.
- Stödja genomförandet och den fortsatta utvecklingen av förtroendeskapande åtgärder, multilateralt inom FN och OSSE, samt genom samarbeten med andra länder.
- Verka för att folkrätten och existerande normer respekteras och tillämpas i cyberrymden.
- Utveckla dialogen och samarbetet med den privata sektorn kring global normering av ny teknik samt internationellt samarbete om gränsöverskridande hot och angrepp.
- Stödja internationella samarbeten vad gäller exportkontroll och granskning av investeringar inom området strategiska tekniker.
- Utveckla utrikesförvaltningens kompetens inom cyberfrågor och digitala frågor.

2. Handel, välstånd och konkurrenskraft

Sverige hör till världens ledande nationer inom digital utveckling. Den digitala ekonomin är central för Sveriges ekonomiska utveckling, inklusive Sveriges konkurrenskraft och ställning på den inre marknaden och globalt. Främjande av svensk digital teknik och företagens förutsättningar att verka på en internationell marknad är en central uppgift för handelspolitiken. Den geopolitiska utvecklingen understryker samtidigt vikten av att föra en samstämmig och integrerad politik med avseende på handel och säkerhet i cyberfrågor och digitala frågor.

Handel och säkerhet som integrerade delar i svensk utrikespolitik

Innovation kopplad till digitalisering och ny teknik är sedan lång tid ett centralt ekonomiskt och handelspolitiskt intresse för Sverige. Svenska företag ligger långt framme vad gäller innovativt skapande och användning av digital teknik som kan bidra till lösningar på de stora globala utmaningarna. Sverige verkar dock på en global marknad där många länder gör betydande satsningar på forskning och utveckling av ny och avancerad teknik. Det finns en global efterfrågan på teknik som utvecklas av svenska företag och inom vissa strategiska sektorer besitter svenska företag en betydande ställning. Det ger Sverige ett inflytande men understryker även vikten av att värna och främja denna förmåga för Sveriges framtida

ekonomiska bas. Digitala produkter och digital handel får allt större inverkan på samhällets grundläggande funktionssätt. Ett helhetsgrepp för dessa frågor innefattar i allt större utsträckning utrikes- och säkerhetspolitiska överväganden.

Varor och tjänster med digitalt innehåll tillverkas, säljs och används idag på en global marknad. Sverige ska verka för att skydda den globala marknaden från produkter och mjukvara som har undermåliga säkerhetsfunktioner eller som kan utgöra en säkerhetsrisk – i synnerhet i relation till auktoritära stater. Samhällsviktiga tjänster är beroende av digital teknik, vilket ställer nya krav på förbättrad cybersäkerhet. Lagar, förordningar och standarder är viktigt för att stärka den gemensamma cybersäkerheten, men kan även innebära ökade nationella eller regionala preferenser och begränsad öppenhet i form av handelshinder för den digitala utvecklingen. Sverige vill minimera de negativa handelseffekterna av reglering samt värna dess WTO-förenlighet

Sveriges handels- och säkerhetspolitiska intressen inom cyber och digitala frågor ska vägas samman och så långt som möjligt vara ömsesidigt stödjande.

Privat och offentlig samverkan

Den privata sektorn står för majoriteten av de medel som spenderas på digital forskning i Sverige och är drivande i den tekniska utvecklingen. Konkurrensen mellan länder att attrahera företagens investeringar och spetskompetens tilltar, speciellt inom forskning och innovation kring avancerad teknik. Privata företag har ett ökande inflytande på säkerhet, demokratins mekanismer, arbetsmarknad, innovation samt på medielandskapet. Sverige har en kraftfull och innovativ digital tekniksektor som är framstående globalt. Den utgör idag inte bara en viktig del av Sveriges ekonomiska bas utan kan också ge väsentliga bidrag i arbetet med att hitta lösningar på de globala utmaningarna. Samverkan och utbyte av *best practices* kring innovation och teknik kan förstärka bilaterala samarbeten, effektivisera utvecklingssamarbeten inom den digitala sektorn, skapa exportmöjligheter och även bidra till att göra Sverige till en attraktiv investeringsnation.

Deltagande från privat sektor i internationella samarbeten inom till exempel EU, Nato, och FN bidrar på ett positivt sätt till initiativ rörande internationella normer och regler. Mer sådana samarbeten bör uppmuntras.

EU:s utveckling och den digitala inre marknaden

EU är en ledande global aktör vad gäller reglering och normgivning inom cyberfrågor och digitala frågor. Sverige verkar för att europeiska förhållningssätt ska bli globalt normsättande. Inom EU har frågan om så kallad öppen strategisk autonomi, och dess digitala motsvarighet digital suveränitet, varit föremål för återkommande diskussion. Målsättningen för det digitala årtiondet är att den inre marknaden ska göras fullt ut datadriven till 2030, där EU etablerar en modell för nyttjande av data med individens intressen och europeiska värderingar i centrum.

Sverige verkar för att EU utvecklas till en starkare aktör på det digitala området. Diskussionen om ekonomisk säkerhet och resiliens kommer att fortsätta och Sverige måste vara delaktig i dessa diskussioner med mål om ökad motståndskraft och fortsatt öppenhet — samt minskade sårbarheter och riskfyllda beroenden visavi i synnerhet auktoritära stater. Målsättningen måste dock vara att fokusera på samarbete och öppenhet också gentemot tredje land. Eventuella begränsningar måste noga avvägas för att inte försvaga svenska intressen och nationell kompetens. Sverige ser att en ökad europeisk förmåga inom forskning och innovation gynnas av ett öppet globalt samarbete. Sverige bör verka för att digital suveränitet uppnås på en öppen marknad och i samverkan med strategiska partners i syfte att motverka en regionalisering och fragmentering som annars kan leda till såväl ekonomiska som säkerhetspolitiska konsekvenser.

I juni 2023 presenterade kommissionen ett meddelande om en europeisk strategi för ekonomisk säkerhet. Strategin framhåller de spänningar som finns mellan att stärka den ekonomiska säkerheten och att säkerställa att EU fortsätter att dra nytta av en öppen ekonomi. I arbetet med dessa processer välkomnar Sverige en balanserad ansats där EU stärker säkerheten, samtidigt som vi stärker Europas långsiktiga konkurrenskraft och produktivitet. Negativa effekter av stärkt säkerhet, för den inre marknaden och de globala institutionerna, inklusive för öppenhet och frihandel, som Sveriges välstånd är beroende av måste så långt som möjligt begränsas.

Den inre marknaden stärker de svenska företagens konkurrenskraft. Europa ska fullt ut utnyttja fördelarna av den innovation och skaparkraft som samhällen med frihet och konkurrens för med sig. Det s.k. D9+-nätverket, där Sverige ingår, är ett viktigt nätverk för samarbete med möjlighet att påverka och leda den digitala agendan på EU-nivå. EU-kommissionen har presenterat en rad förslag som syftar till att reglera strukturer och aktörer i det digitala landskapet. Värdet av data ska fullt ut realiseras i linje med den europeiska datastrategin. Omfattande investeringar i de tekniska strukturer som ska underbygga regleringarna görs via strategiska projekt i fonder och program som Horisont Europa, Fonden för ett sammanlänkat Europa och Programmet för ett digitalt Europa. Dessa EU-gemensamma regler av digitala tjänster och varor påverkar såväl den inre marknaden som den externa handeln med omvärlden. Sverige välkomnar som princip en reglering som skulle stärka förutsägbarheten. Sverige vill att lagstiftningen föregås av konsekvensanalyser för att inte hämma företagens konkurrenskraft och innovation. Regelverk som är interoperabla med strategiska partners system bör eftersträvas.

Leverantörssäkerhet inom strategiska teknikområden

Digitaliseringen har gjort den globala ekonomin allt mer beroende av vissa nya strategiska produkter, mineraler och tekniker. Det gäller i särskilt hög utsträckning för Sverige som är en handels-, innovations- och digitaliserad ekonomi med ett fokus på en global, grön, säker och digital omställning. Det ställer nya krav på Sverige att agera strategiskt när intressen motiverade av handelspolitik och säkerhetspolitik hamnar i konflikt.

Globalt riktas särskilt stor uppmärksamhet mot framtidens kommunikationsteknik. Digitala telekommunikationer kan liknas vid blodomlopp för samhällens, ekonomiers och staters funktionalitet, med mycket stor strategisk betydelse. Det faktum att en av ett fåtal betrodda leverantörer har sin forskningsverksamhet koncentrerad till Sverige har en betydelse som går utöver exportfrämjande. Det ger Sverige en roll och ett ansvar, att agera strategiskt och sammanhållet i utrikes- och säkerhetspolitiska, liksom i handelspolitiska dialoger och processer. Särskild uppmärksamhet behöver nu riktas mot nästa generations system (6G osv.) och förutsättningarna avseende säkerhet, forskning och innovation, liksom statliga interventioner som påverkar konkurrens och spelregler. Grundläggande svenska ingångsvärden är teknikneutralitet, stabilitet, säkerhet och diversifiering i informations- och kommunikationstekniklevera nskedjorna (IKT) och vikten av globala standarder.

Infrastruktur

Sverige är beroende av internationella fiberoptiska kablar för kommunikation med omvärlden och i praktiken även för att säkra de nationella behoven av elektronisk kommunikation och tillgång till digitala tjänster. Företagens konkurrenskraft är beroende av väl fungerande konnektivitet. Fysiska angrepp eller cyberangrepp mot internationell konnektivitet utgör ett betydande hot och det förändrade säkerhetspolitiska läget har aktualiserat sårbarheten i EU och Sveriges konnektivitet med Asien. Det är av vikt för Sverige att främja en redundans och motståndskraft för den digitala infrastrukturen.

Dataflöden, digitala handelshinder och lagring

Förmåga att hantera och realisera värdet av data utgör grunden för utvecklingen av ny teknik och för handel med såväl varor som tjänster. Därmed blir fungerande och öppna dataflöden centrala för svensk och europeisk konkurrenskraft. EU:s företag, oavsett storlek eller bransch, blir i allt högre utsträckning beroende av dataflöden, och förmågan att kapitalisera värdet av data lägger grunden för helt nya företag och affärsmodeller. Hänsyn måste tas till förutsättningarna för såväl teknikutveckling, innovation och handel som till skyddet av information. Genom ett dimensionerat och anpassat skydd för information, bland annat personuppgifter och immateriella tillgångar, ges förbättrade förutsättningar för svensk innovation och teknikexport.

För att data ska kunna användas räcker dock inte endast fria flöden. Från handelssynpunkt är det viktigt att motverka digitala handelshinder i tredje land såsom oberättigade krav på datalokalisering samt utlämnande av källkoder. Det finns också behov av att data, med respekt för individers rätt, kan hanteras på ett kontrollerat sätt och kan delas och lagras stabilt och säkert. Detta är centralt för den ekonomiska modell som underbygger de flesta internet- och teknikföretag. Teknikbranschen utgör idag en ökande andel av många länders ekonomier, inklusive Sveriges. Utan fria dataflöden och stabil och säker datahantering riskeras svensk handel och konkurrens- och innovationskraft. Därmed hotas på längre sikt Sveriges

ekonomiska säkerhet och utveckling. Sverige som ett innovativt och informations- och datatungt land behöver kunna driva dessa frågor internationellt för att värna svenska handelsintressen. Inom handelspolitiken eftersträvar Sverige ambitiösa regler om digital handel i EU:s handelsavtal samt i multilaterala e-handelsförhandlingar i WTO.

Standarder

Internationella standarder på teknik- och cyberområdet är centrala för att säkerställa att olika produkter är interoperabla och kan säljas på en global marknad, vilket kan gynna diversifiering, konnektivitet och konkurrens. Sverige har länge haft ett betydande inflytande inom internationell standardisering eftersom svenska intressenter, dvs. företag, myndigheter, forskning och akademi varit välrepresenterade i de internationella standardiseringsorganen. Under senare år har utvecklingen av internationella standarder på teknik- och cyberområdet präglats av ökad stormaktskonkurrens. Det ökade engagemanget från auktoritära stater inom standardiseringsprocesserna har exempelvis märkts i frågor om internets arkitektur och ansiktsigenkänningsteknik i Internationella teleunionen (ITU), men även i den stärkta närvaron av statsstyrda företag inom organisationen Internationella standardiseringsorganisationen (ISO). Fortsätter den nuvarande trenden med ökad konkurrens skulle det försvaga de multilaterala handelspolitiska och marknadsekonomiska principer som varit grunden för de senaste decenniernas stora välståndsökningar.

För svenskt vidkommande är det centralt att beakta WTO:s avtal om tekniska handelshinder och att standarder kan maximera nyttan och möjligheten med tekniken, vara icke-diskriminerande, transparenta och teknikneutrala. För Sveriges del är det angeläget att intressentstyrningen och nuvarande samverkansformer för standardisering värnas. Samtidigt behöver Sverige aktivt motverka att standarder sätts utifrån politiska och strategiska bevekelsegrunder som inte ligger i linje med Sveriges intressen.

Cybersäkerhetscertifiering

Genomförandet av EU:s cybersäkerhetsakt innebär att EU utarbetar egna certifieringsordningar inom ramen för EU:s regelverk, och därmed förenklar för en inre marknad för varor och tjänster med en lämplig cybersäkerhetsnivå. För Sverige är det angeläget att verka för att EU:s ramverk för cybersäkerhetscertifiering inte leder till att företag behöver ansöka om dubbla och fördyrande certifieringar, med påföljande risk för handelshinder samt att reciprocitet gäller med avseende på tillgång till marknad under olika certifieringsordningar. Det transatlantiska samarbetet på cybersäkerhetscertifieringsområdet är också en viktig aspekt.

Fokusområden – handel, välstånd och konkurrenskraft

- Bidra till arbetet för ett starkare och ett mer sammanhållet EU på det digitala området, inklusive en fördjupning av EU:s digitala inre marknad, öppen digital suveränitet och ett stärkt EU-samarbete kring digital diplomati (unionens externa digitala politik).
- Främja ekonomisk säkerhet och resiliens med mål om både ökad motståndskraft och fortsatt öppenhet — samt minskade sårbarheter och riskfyllda beroenden visavi i synnerhet auktoritära stater
- Främja, genom EU och andra internationella samarbeten, stabila och diversifierade leveranskedjor för strategiska tekniker, komponenter och insatsvaror.
- Främja att internationella dataflöden är och förblir fria.
- Främja svensk digital tekniksektor och föra dialog med svenskt näringsliv för att tillvarata dess kompetens och intressen i internationella sammanhang. Främja export från och investeringar till Sverige inom den digitala sektorn. Föra dialog med näringslivet för att tillvarata kompetens och intressen i internationella sammanhang i enlighet med Utrikeshandelsstrategin.
- Verka för att dialogen om internationella normer och regler mellan regeringar och den privata sektorn utvecklas på EU- och internationell nivå.
- Verka för att utvecklingen av reglering kring internationell handel följer WTO:s regler.
- Verka för ambitiösa regler om digital handel och dataflöden i handelsavtal, inklusive de plurilaterala e-handelsförhandlingarna i WTO, tillsammans med likasinnade EU-medlemsstater.
- Bidra till nya standarder och certifieringar som förenklar och möjliggör ökad handel, samt att sådana som kan utgöra otillbörliga hinder för handel eller konkurrensnackdelar för svenska företag undviks. Interoperabilitet i regelverken mellan EU och dess strategiska partner ska aktivt eftersträvas.
- Främja Sveriges förmåga att hantera en mer konkurrensutsatt internationell standardiseringsprocess och att aktivt försvara svenska positioner och intressen, bland annat genom att värna att de internationella standardiseringsorganen förblir intressentdrivna och de negativa konsekvenserna av mellanstatlig konkurrens inom standardiseringsorganen minimeras.
- Aktivt medverka inom ITU:s standardiseringssektor.
- Främja Sveriges ställning som prioriterad partner för grön, säker och digital omställning globalt. En hållbar handel med kritiska råvaror, mineraler och andra insatsvaror av strategisk betydelse för grön och digital omställning ska säkerställas.

3. Utveckling och demokrati

Sverige behöver verka inom en rad områden för att befästa en öppen, fri och säker cyberrymd med rättsstatens principer som grund.

Digitalisering och demokrati

Det digitala mediet skapar möjligheter att fördjupa demokratin men gör också demokratin mer sårbar för olika slags digitala attacker. Såväl statliga som ickestatliga aktörer använder sig av digitala verktyg och ny teknik, till exempel AI, som ett medel att övervaka, utöva kontroll och trakassera meningsmotståndare, journalister och människorättsförsvarare, särskilt kvinnor. Skyddet mot digitala förföljelser för dessa grupper måste säkerställas.

Otillbörlig informationspåverkan undergräver demokratiska institutioner, destabiliserar demokratin och ökar risken för politiskt våld. Otillbörlig informationspåverkan utgör ett hot mot ett öppet och demokratiskt samhälle och den fria åsiktsbildningen och måste bemötas på såväl nationell som internationell nivå för att skydda demokratins kärna.

Samtidigt ökar digitaliseringen möjligheterna för civilsamhället och människorättsförsvarare att agera, organisera sig och påverka. Tillgång till ett fritt, öppet och säkert internet är avgörande för att främja politiskt och socialt deltagande.

Digitalisering och utveckling

Digitalisering kan lyfta samhällen ur fattigdom genom att ge nya möjligheter att delta i världshandeln och den globala ekonomiska utvecklingen. En väsentlig del av den infrastruktur som möjliggör välstånd är digital. En ökad digitalisering skapar således stora utvecklingsmöjligheter för låginkomstländer. Stora delar av världens befolkning har dock inte förutsättningarna för att fullt ut kunna dra nytta av digitaliseringen, och fördelarna med den digitala utvecklingen. Det gäller särskilt kvinnor och flickor. Tillgången till internet är markant bättre i demokratiska länder än i autokratier. En ambitiös och inkluderande digitaliseringsagenda kan bidra till att accelerera genomförandet av Agenda 2030 och de globala målen för hållbar utveckling (SDGs), bland annat genom att möjliggöra innovation inom till exempel finansiell inkludering, tillgång till sjukvård, förbättrat jordbruk och miljö- och klimat. Det krävs ett fortsatt fokus på ökad och säker tillgång till informations- och kommunikationsteknik. Utvecklingssamarbete kopplat till digital handel (e-handel) är av stor betydelse för att stödja utvecklingsländers deltagande i världshandeln. E-handeln kan skapa gynnsamma fördelar för små och mellanstora företag (SMEs), kvinnor samt marginaliserade grupper genom att minska exportbarriärer och tillgängliggöra fler produkter till en lägre kostnad. Digitala lösningar bidra till att motverka mobilitetshinder, diskriminering, och kvinnliga entreprenörers utsatthet för våld. Samtidigt måste den digitala utvecklingen åtföljas parallellt av ett systematiskt informations- och cybersäkerhetsarbete för att skapa motståndskraftiga samhällen.

Kapacitetsuppbyggnad och kapacitetsutveckling inom digitalisering och cybersäkerhet

Stöd inom digitalisering måste åtföljas av en stärkt cybersäkerhetsförmåga. Exempelvis saknar många utvecklingsländer nationella myndigheter med uppgift att stödja samhället i att bygga

motståndskraft på cyberområdet. Samtidigt blir en allt större del av samhällstjänsterna, också på områden som hälsa och utbildning, digitala. En förbättrad kapacitet att bygga rättstatsbaserade institutioner och regler, och att bygga motståndskraft och göra teknikval utifrån en rättighetsbaserad ansats, har stor betydelse för den bredare utvecklingen inom mänskliga rättigheter, demokrati och rättsstatens principer.

Det finns behov av en utökad satsning på kapacitetsbyggande inom digitalisering inklusive uppbyggnad av demokratiska samhällen, offentliga institutioner och system för digital förvaltning, och cybersäkerhet. Kapacitetsbyggande insatser inom digitalisering och cybersäkerhet är därför nödvändigt. Det ligger i Sveriges intresse att länder med vilka Sverige vill fördjupa sina politiska och ekonomiska relationer stärker motståndskraften mot externa cyberhot och förbättrar kapaciteten att på egen hand stärka sin suveränitet i cyberrymden. I denna kontext är Ukraina prioriterat för kapacitetsbyggande gällande cybersäkerhet. Sveriges ambition inom kapacitetsutveckling bör främst koordineras genom multilaterala initiativ inom EU, Nato, FN och OSSE.

Sveriges utvecklingssamarbete inom digitalisering och cybersäkerhet

Sverige arbetar aktivt med att integrera digitala komponenter i det bilaterala utvecklingssamarbetet. Det sker bland annat som del av stödet för att främja mänskliga rättigheter, demokrati och rättsstatens principer. Det svenska utvecklingssamarbetet ska stödja insatser som främjar ett öppet, fritt och säkert internet, samt insatser som minskar den digitala klyftan – särskilt för kvinnor, flickor och andra grupper som är särskilt utsatta.

Sverige avser också att, genom utvecklingssamarbetet, bidra till arbetet mot otillbörlig informationspåverkan och för att stärka motståndskraften och förbättra kapaciteten inom digitaliserings- och cybersäkerhetsområdet. Till exempel handlar det om verksamhet som stärker och säkrar organisationers och människorättsförsvarares digitala verktyg, men stöd handlar också om att öka medvetandet om risker och sårbarhet som en ökad digitalisering innebär. Arbetet innebär också att lyfta och synliggöra digitaliseringens utmaningar i allt från hot och våld, olaglig handel, otillbörlig informationspåverkan, övervakning och hot mot individens integritet. Normer och principer för mänskliga rättigheter, demokrati och rättsstatens principer behöver vara vägledande för utvecklingen av en inkluderande digital förvaltning. Stöd på det digitala området behöver alltid åtföljas av ett systematiskt informations- och cybersäkerhetsarbete för att inte skapa nya sårbarheter.

Sveriges utvecklingssamarbete stödjer organisationer i deras påverkansarbete med att säkerställa att internet förblir öppet och säkert för individer, journalister, oberoende forskare och människorättsförsvarare. Stödet innehåller även kapacitetsuppbyggnad, mentorskap och utbildning samt stöd i akuta situationer som exempelvis hot mot enskilda, nedstängning av internet eller blockering av kommunikationskanaler. Stödet till människorättsförsvarare, även i digitala miljöer, ska utvecklas. Därtill får flera organisationer stöd i arbetet med att hjälpa organisationer och marginaliserade grupper i repressiva miljöer med verktyg och teknik för de

ska kunna ha kontroll över sin egen information och försvara sig mot digitala attacker såsom otillbörlig informationspåverkan, uppvigling, övervakning, trakasserier och våld.

En ökad digitalisering underlättar för ekonomisk utveckling och välstånd och skapar stora utvecklingsmöjligheter. Det är därför av vikt att främja de möjligheter som digitaliseringen för med sig för individer, näringsliv och civilsamhälle.

Den privata sektorn utgör också en viktig tillgång och kompetens gällande kapacitetsutbyggnad avseende cybersäkerhet. Ett stärkt samarbete mellan den privat och offentlig sektor är nödvändigt för att kunna utveckla cybersäkerhet i utvecklingsarbetet.

Sverige ser därför över möjligheterna med nya instrument och finansieringslösningar inom ramen för utvecklingssamarbetet med syfte att bredda det svenska erbjudandet och bidra till ett ökat deltagande av det svenska näringslivet i digitala omställningsprojekt i låg- och medelinkomstländer.

Multilaterala samarbeten

Sveriges multilaterala utvecklingssamarbete bidrar till samarbetsländernas möjligheter att dra nytta av den digitala teknikens potential och samtidigt kunna hantera riskerna genom stärkt cybersäkerhet. Stöd till policyutveckling, fysiska investeringar och kapacitetsutveckling sker i ökad utsträckning genom multilaterala organisationer, inom ramen för EU:s, FN:s och utvecklingsbankernas verksamhet. Världsbanksgruppen har en viktig roll för att minska de globala digitala klyftorna. Sverige bidrar också med stöd till utvecklingsländerna för att de ska kunna dra nytta av och möta utmaningarna vad avser den digitala ekonomins snabba utveckling.

Digitalisering och jämställdhet

Den ojämlika fördelningen av teknisk kompetens och tillgång till internet får särskilt negativa konsekvenser för kvinnor och flickor. Sverige har förutsättningar att bidra till stärkta möjligheter och rättigheter för kvinnor och flickor inom det digitala området genom att utveckla egna kapacitetsutvecklingsprojekt med bidrag från svenska myndigheter med spetskompetens på området. Sådana insatser behöver ta sikte på kvinnors och flickors meningsfulla deltagande i hela kedjan från teknikutveckling till användning, inklusive relevanta politiska beslutsprocesser på teknikområdet.

Ett ökande antal kvinnor och flickor drabbas av könsrelaterat och sexuellt våld, hot, hat och kränkningar på internet och sociala medier. Digitala tekniker kan också förstärka problemen med könsrelaterat våld och sexuellt utnyttjande av barn offline, genom att underlätta förföljelse och exploatering av offer. Våld, hot, hat och övergrepp online får allvarliga konsekvenser, inte bara för kvinnors och flickors fysiska och psykiska hälsa utan också deras möjligheter att delta i det demokratiska samtalet.

Fokusområden – utveckling och demokrati

- Verka för mänskliga rättigheter, demokrati och rättsstatens principer i digitala miljöer inom det svenska utvecklingssamarbetet, bland annat genom att säkerställa skydd och kapacitetsuppbyggnad för människorättsförsvarare, jämställdhet, civilsamhällesaktörer och demokratirörelser.
- Verka för att digitalisering och cybersäkerhet blir en horisontell fråga för att uppnå de utvecklingspolitiska målen. Kapacitetsutveckling för digitalisering och cybersäkerhet bör därför integreras inom ramen för Sveriges bilaterala och multilaterala utvecklingsarbete. Det gäller bland annat att bidra till att säkra digitala samhällstjänster och kompetensinsatser samt minska de digitala klyftorna mellan män och kvinnor.
- Verka för synergier mellan främjande, handel-, utrikes- och säkerhetspolitik i internationellt utvecklingssamarbete rörande digitalisering och cybersäkerhet.
- Verka i multilaterala sammanhang för de mänskliga rättigheterna inom cyberområdet, inte minst yttrandefriheten, tillgång till information och rätten till privatliv.
  Fortsatt fördjupa samarbetet med likasinnade rörande digitalisering och demokrati, såväl i multilaterala sammanhang som bilateralt.
- Aktivt bidra till ITU:s arbete med att stärka utvecklingsländers kapacitetsutveckling inom cyber- och digitaliseringsområdet samt främja en inkluderande digitaliseringsagenda till stöd för att uppnå de globala hållbarhetsmålen.

4. Internationella samarbeten

EU:s cyberdiplomati och digitala diplomati

EU är, i kraft av sin roll som ledande global aktör, med en bredd av instrument till förfogande, Sveriges viktigaste plattform för den breda utrikespolitiken kring cyberfrågor och digitala frågor. I en hård geopolitisk konkurrens kring teknik och digitala frågor är ett starkt, sammanhållet och öppet EU centralt för att främja svenska intressen inom och utanför unionen. EU:s externa relationer på området hanteras övergripande i två spår, cyberdiplomati och digital diplomati. Eftersom det i grunden är olika aspekter av samma tekniska utveckling som avses, verkar Sverige för att externa cyberfrågor och digitala frågor ska hanteras i nära samordning.

Gemensamt EU-agerande är ett av Sveriges skarpaste utrikes- och säkerhetspolitiska verktyg inom cyberområdet. Det ligger i Sveriges intresse att EU stärker sin roll som utrikes- och säkerhetspolitisk aktör i cyberfrågor. Utvecklingen av gemensamma åtgärder på EU-nivå för att bemöta cyberhot och cyberangrepp har gett EU en större global aktörsroll på området. Som ett svar på den försämrade säkerhetssituationen började EU 2017 utveckla en diplomatisk verktygslåda för att bemöta cyberhot och cyberangrepp mot EU och dess medlemsstater. Verktygslådan omfattar bland annat démarcher och gemensamma uttalanden,

stöd till kapacitetsutveckling och ett tematiskt sanktionsinstrument. Sedan sanktionsregimen skapades 2019 har flera listningar av cyberaktörer baserade i Ryssland, Kina och Nordkorea genomförts. EU har även gjort ett flertal gemensamma uttalanden om antagonistisk cyberaktivitet, såväl gentemot sådan som riktats direkt mot EU, som sådan som riktats mot partners till EU.

För Sverige utgör verktygslådan en möjlighet att agera solidariskt med EU:s medlemsstater och att få stöd av unionen när cyberhot och cyberangrepp riktas mot svenska intressen. Svensk förmåga till konkreta bidrag i form av exempelvis sanktionsförslag kopplat till den tematiska cybersanktionsregimen bör fortsätta utvecklas. Vidare bör Sverige aktivt stödja den fortsatta utvecklingen av den cyberdiplomatiska verktygslådan och cyberfrågornas fortsatta integration i EU:s gemensamma utrikes- och säkerhetspolitik, med respekt för att nationell säkerhet faller under medlemsstaternas kompetens enligt EU:s fördrag. Sverige vill se en mer strategisk, långsiktig ansats i förhållande till centrala hotaktörer, stärka cybersanktionsregimen och utveckla EU:s samarbeten på området, bland annat med privata sektorn och med Nato.

Sverige vill även fortsätta utveckla EU:s digitala diplomati med sikte på ett mer strategiskt och sammanhållet agerande från unionens sida. Ett sätt är att främja den så kallade Team Europe-ansatsen som samlar EU:s olika institutioner såväl som medlemsländerna. Den digitala diplomatin behöver integreras fullt ut i EU:s bredare externa relationer. Samarbeten med andra demokratier, särskilt USA, är en nyckelfråga inom digital diplomati.

EU har potential att ta en än mer framträdande roll i globala processer kring normer och regler inom cyberfrågor och digitala frågor, inte minst inom FN. I kraft av EU:s inre marknad och regleringsmakt kan EU, givet hur inre marknadspolitiken påverkar andra länder, inta en stark position i förhållande till stater som Kina och Ryssland. EU:s gemensamma agerande är också nödvändigt för att kunna utveckla dialog och samverkan med USA på jämbördiga villkor, både i säkerhetspolitiska frågor och i frågor som rör dataflöden, lagring och reglering av digitala plattformar. EU-USA:s handels- och teknikråd (TTC) har potential att fördjupa och bredda den transatlantiska handels- och investeringsrelationen, undvika nya handelshinder och samarbeta kring nya standarder och tekniker. Det är angeläget med en så hög grad av samsyn som möjligt mellan EU, USA och andra demokratiska länder i frågor om normer och regelverk, för att motverka en splittrad global marknad och stärka det gemensamma arbetet med globala normer och regler. EU:s regelbundna cyberdialog med USA ger möjlighet att etablera normer för internationell cybersäkerhet.

EU har idag också en växande uppsättning strukturerade samarbeten med viktiga länder och regionala organisationer som kan utvecklas och stärkas ytterligare. Det gäller till exempel handels- och teknikrådet med Indien, de digitala partnerskapen med länder som Japan, Kanada och Sydkorea liksom regionala samarbeten, som med Latinamerika och Karibien (EU-LAC Digital Alliance).

EU har också instrument för att bidra med stöd till kapacitetsutveckling till resurssvagare länder, inom ramen för grannskapspolitiken såväl som utvecklingspolitiken.

Samarbetet inom Nato

Nato har ett växande fokus på strategiska cyber- och teknikfrågor, inte minst kopplat till de allierades intresse av att möta utmaningar från Ryssland och Kina. Nato har ett omfattande samarbete inom cyberförsvarsområdet, samt kring strategiska tekniker.

Det svenska Natomedlemskapet medför nya möjligheter till att stärka Sveriges cyberförsvarsförmåga, cybersäkerhet, cyberresiliens och säkerhet i bredare bemärkelse. Det medför även krav på Sveriges förmåga att samverka inom alliansen och med enskilda allierade. Nato lägger stort fokus på samverkan med den innovationsdrivna privata sektorn. Sverige vill som Natomedlem ge ett tydligt mervärde till alliansen inom dessa områden. Integreringen i Nato kommer också ge Sverige nya kontaktytor för att utveckla vårt arbete med innovation och ny teknik samt en plattform att främja svensk industri.

EU och Nato bör verka kompletterande och ömsesidigt förstärkande. Sverige bör verka för fortsatt utökat samarbete mellan Nato och EU, särskilt inom cyberförsvars-, cybersäkerhets- och cyberresiliensområdena. Onödig duplicering mellan organisationerna kan riskera hämma förmågeutvecklingen och bör undvikas.

Nordiskt och nordiskt-baltiskt samarbete

Som komplement till europeiskt och euro-atlantiskt samarbete vill Sverige utveckla den utrikes- och säkerhetspolitiska dialogen och samarbetet mellan de nordiska länderna. Det gäller både i policyprocesser inom EU och Nato, men också i konkreta säkerhetspolitiska frågor kopplat till hantering och bemötande av antagonistiska cyberhot från exempelvis ryska aktörer. Samarbetet med de nordiska och nordisk-baltiska länderna bör fördjupas ytterligare, inte minst med ett fokus på närområdet och för att fördjupa ett transatlantiskt samarbete. Sverige ska även verka för att fortsätta att utveckla det nordisk-baltiska samarbetet inom cyberområdet (NB8).

Samarbete med USA

Cyber- och teknikfrågor ges ett betydande fokus i USA:s utrikes- och säkerhetspolitik, inte minst som en del i konkurrensen med Kina, samt i USA:s hantering av cyberrelaterade hot från till exempel Ryssland, Iran och Nordkorea. USA arbetar aktivt för att skapa en global allians av likasinnade demokratier kring cyber- och teknikfrågorna, inklusive i etablerandet av globala normer, standarder och regelverk. Sverige bör eftersträva att medverka i USA:s tekniksamarbeten, eller på annat sätt säkerställa att svenska intressen beaktas. Sverige ska även verka för interoperabilitet mellan EU:s och USA:s positioner i internationella processer i syfte att säkerställa transatlantiskt och demokratiskt ledarskap i utvecklandet av globala digitala standarder och regelverk.

Cyber- och teknikfrågorna blir också allt viktigare i Sveriges bilaterala relation med USA där särskilt fokus riktas mot strategiska teknikfrågor som telekom, cybersäkerhet och rymdfrågor samt instrument för att skydda ny teknik. Sverige har ett flertal bilaterala avtal med USA på teknikområdet som bör användas som bas och utgångspunkt för fördjupat samarbete. Sverige för också en dialog med USA kring utvecklingen av diplomatiska och politiska instrument för att hantera antagonistiska cyberhot och attacker. En formaliserad bilateral dialog kring cyberfrågor och digitala frågor inrättades 2024.

Strategiska partners

Strategiska partnerskap är av stor betydelse för att stärka Sveriges inflytande i och samverkan med tekniskt avancerade och innovationsdrivna demokratier. Sverige ska fördjupa sina utrikespolitiska bilaterala dialoger med USA samt ledande länder inom EU och Nato och globalt, inte minst med länder i den indo-pacifiska regionen.

Sverige har ett antal samarbeten med strategiska partners inom mindre grupper av länder, med huvudfokus på utrikes- och säkerhetspolitiska aspekter och bemötande av antagonistiska cyberhot. Sådana informella kretsar ger Sverige möjlighet till insyn och inflytande i dialog med länder inom Sveriges krets av likasinnade.

Sverige deltar i ett antal koalitioner och samarbeten om digitala frågor. Ett exempel är Freedom Online Coalition som består av omkring 40 medlemsländer, däribland USA, flera EU-länder men också länder som Sydkorea och Chile. Koalitionen är en viktig plattform för Sverige i arbetet med frihets- och rättighetsfrågor på internet.

FN och multilaterala organisationer

FN har en viktig roll att spela för att etablera globala normer och hantera gränsöverskridande utmaningar och risker. För Sveriges del är det därför viktigt att värna och främja ett regelbaserat internationellt samarbete och starka multilaterala institutioner, däribland FN.

Cybersäkerhet och digitalisering behandlas i flera processer inom FN. De innefattar den grundläggande frågan om hur folkrätten ska tillämpas, genomförande av frivilliga normer för staters ansvarsfulla uppträdande, genomförande av förtroendeskapande åtgärder, inkludering av civilsamhället i beslutsfattande och motverkande av systemhotande cyberbrottslighet. I den öppna arbetsgruppen för cyber och internationell säkerhet pågår det ett centralt arbete att upprätthålla den fria världsordningen på cyberområdet. Sverige ska verka för att en permanent, frivillig och öppen flerpartsmodell kommer till stånd i och med den internationella konferensen för cybersäkerhet 2026. Ett uppföljningsarbete av den nyligen antagna internationella konventionen för att motverka cyberbrottslighet är påkallat.

Generalförsamlingen har 2024 beslutat om ett globalt digitalt ramverk, *Global Digital Compact*, för en öppen, fri och säker digital framtid med utgångspunkt i en tillämpning av folkrätten och som möjliggör genomförandet av Agenda 2030.

FN utvecklar även arbetet med företagande och mänskliga rättigheter avseende nya digitala tekniker. Detta innefattar att främja teknikbolagens respekt för mänskliga rättigheter både online och offline, liksom att företagen arbetar med tillbörlig aktsamhet i sina värdekedjor.

Det är välkommet att FN generellt stärker sin roll på digitaliseringsområdet när det gäller att både tillvarata digitaliseringens möjligheter, tillse att de kommer hela jordens befolkning till del, samt att hantera dess risker och utmaningar.

Sveriges plats i ITU:s råd gör att vi har en god plattform för att verka för bättre standarder och att det för utvecklingsländer mest centrala arbetet – att kunna få bli en del av den digitala ekonomin, sker på ett sätt som är transparent, effektivt och på basis av mänskliga rättigheter, internationella regler och principer.

FN har en viktig roll att spela för hur internationella relationer bör hanteras och utvecklas i ett digitalt tidevarv. Samtidigt måste det ske på ett sätt som bygger på och tillvaratar de etablerade normer, principer och processer som existerar för att diskutera olika digitaliseringsfrågor. Flerpartssamverkan bör generellt prägla FN:s arbete med cyberfrågor och digitala frågor för att fånga upp olika kompetenser och perspektiv. För Sverige är det centralt att styrningen och förvaltningen av internet fortsatt sker genom flerpartssamverkan, inklusive den privata sektorn.

Utöver FN finns andra organisationer som kan utgöra samarbetspartners. Sverige är medlem i International Institute for Democracy and Electoral Assistance (IDEA) som arbetar med länken mellan demokrati och digitalisering. Organisationen har särskild expertis inom skydd av valprocesser och institutioner. Två andra samarbetsorganisationer, European Endowment for Democracy och Pragcentret bidrar till att stärka civilsamhällen, människorättsförsvarare och fri media i den digitala sfären, samt verkar för ökat politiskt deltagande och högre motståndskraft gentemot exempelvis otillbörlig informationspåverkan.

OSSE

Organisationen för säkerhet och samarbete i Europa (OSSE) har antagit 16 förtroendeskapande åtgärder på cyberområdet. Bland annat har ett kontaktpunktssystem etablerats där de 57 deltagande staterna anger politiska och tekniska kontaktuppgifter för att kunna utbyta information (exempelvis i händelse av cyberincidenter). Cyberfrågorna diskuteras återkommande i en informell arbetsgrupp. Sverige stödjer OSSE:s fortsatta arbete med cyberfrågor. Sverige har tillsammans med andra länder åtagit sig att driva och utveckla den förtroendeskapande mekanismen om offentlig och privat samverkan.

Världsbanken

Världsbanksgruppen och de regionala utvecklingsbankerna stärker nu stödet till samarbetsländernas digitala utveckling och omställning genom kapacitetsutveckling, policydialog och investeringar i teknisk och digital infrastruktur. För Sverige är det viktigt att

inom ramen för Världsbanksgruppen säkerställa en digital ekonomisk utveckling som inkluderar ett cybersäkerhetsperspektiv samt främja digitaliseringens potential att bidra till att Agenda 2030 kan nås. Sverige vill främja Världsbanksgruppens arbete med att dels integrera cyber och digitala frågor inom Världsbanken, dels inom ramen för Världsbanksgruppens partnerskap och strategier. Detta är än mer angeläget i ljuset av de nödvändiga reformer som Världsbanksgruppen står inför.

Fokusområden – internationella samarbeten

- Främja EU:s förmåga att agera som en sammahållen utrikespolitisk aktör inom cyberfrågor och digitala frågor. Bidra till samordningen mellan EU:s cyberdiplomati respektive digitala diplomati. Fortsätta utveckla EU:s förutsättningar att förebygga, hantera och bemöta cyberhot och cyberangrepp med utrikespolitiska och diplomatiska medel, med fokus på utvecklingen av EU:s cyberdiplomatiska verktygslåda.
- Etablera Sverige som utrikes- och säkerhetspolitisk aktör i Natos pågående arbeten och processer inom teknik-, innovations- och cyberområdena, med målsättning att ge ett tydligt mervärde till alliansen och för Sverige.
- Utveckla det nordiska och nordisk-baltiska samarbetet inom cyberområdet och det digitala området, samt med andra strategiska partners.
- Utveckla den formaliserade bilaterala dialogen med USA om cyberfrågor och digitala frågor, samt fördjupa det bredare samarbetet kring strategisk teknik.
- Utveckla Sveriges samarbeten med utvalda likasinnade kring avskräckning på cyberområdet.
- Verka för ett närmare samarbete mellan EU och USA inom ramen för TTC och andra relevanta fora för att säkerställa transatlantiskt ledarskap i utvecklingen av internationella normer och standarder.
- Utveckla Sveriges, EU:s och Natos samarbeten avseende stöd till Ukraina på cyber- och digitaliseringsområdet.
- Aktivt delta i FN:s policyutveckling och förhandlingar inom cyber- och digitaliseringsområdet, med fokus på tillämpning av folkrätt, utveckling och genomförande av normer och förtroendeskapande åtgärder. Verka i FN för att flerpartssamverkan generellt ska prägla arbetet. Försvara internets styrningsmodell som bygger på flerpartssamverkan
- Bevaka Sveriges och EU:s intressen och värderingar inom ramen för genomförandet av FN:s färdplan för digitaliseringsfrågor, samt FN:s Global Digital Compact.