Skydda forskning och kunskap

En vägledning för att motverka spionage vid forskningssamarbeten

Teknikföretagen

SOFF

Innehåll

VAD SOM STÅR PÅ SPEL

”Internationellt forskningssamarbete är avgörande för att kunna bedriva excellent forskning och innovation. Öppenhet och samarbete riskerar dock att utnyttjas av främmande makt och andra aktörer på ett otillbörligt sätt. Forskningssäkerheten behöver därför stärkas, bland annat genom ökad kunskap och medvetenhet om risker med internationellt samarbete.”

- Nationell säkerhetsstrategi

”Cyberangrepp i syfte att genomföra industrispionage mot svenska mål är numera en del av vardagen. Angreppen får som resultat att innovativa svenska företag konkurreras ut av sina egna lösningar som stulits av statliga aktörer.”

- Nationellt Cybersäkerhetscentrum

”Svensk forskning och innovation är eftertraktad och Sverige ligger långt fram inom flera områden som främmande makt är intresserade av. Detta, i kombination med att det är relativt lätt att etablera och bygga upp en företagsverksamhet i Sverige, innebär att utländska underrättelsetjänster inhämtar spetsteknologi och kunskap från Sverige.”

- Säkerhetspolisen

1. Inledning

Denna vägledning vänder sig till personer som forskar vid lärosäten och företag. Primär målgrupp är företag, lärosäten, institut, teknikparker och inkubatorer som bedriver forskningssamarbeten parterna emellan. Den är dock relevant för alla som är involverade i forskning och innovationsarbete, både som utförare och som finansiärer.

I fokus för vägledningen står risker för forskningsspionage, det vill säga den otillbörliga form av informationsinhämtning som antagonister riktar mot näringslivet och forskningssamhället för att nå konkurrensfördelar och därmed ligga före oss i kunskapsskapande.

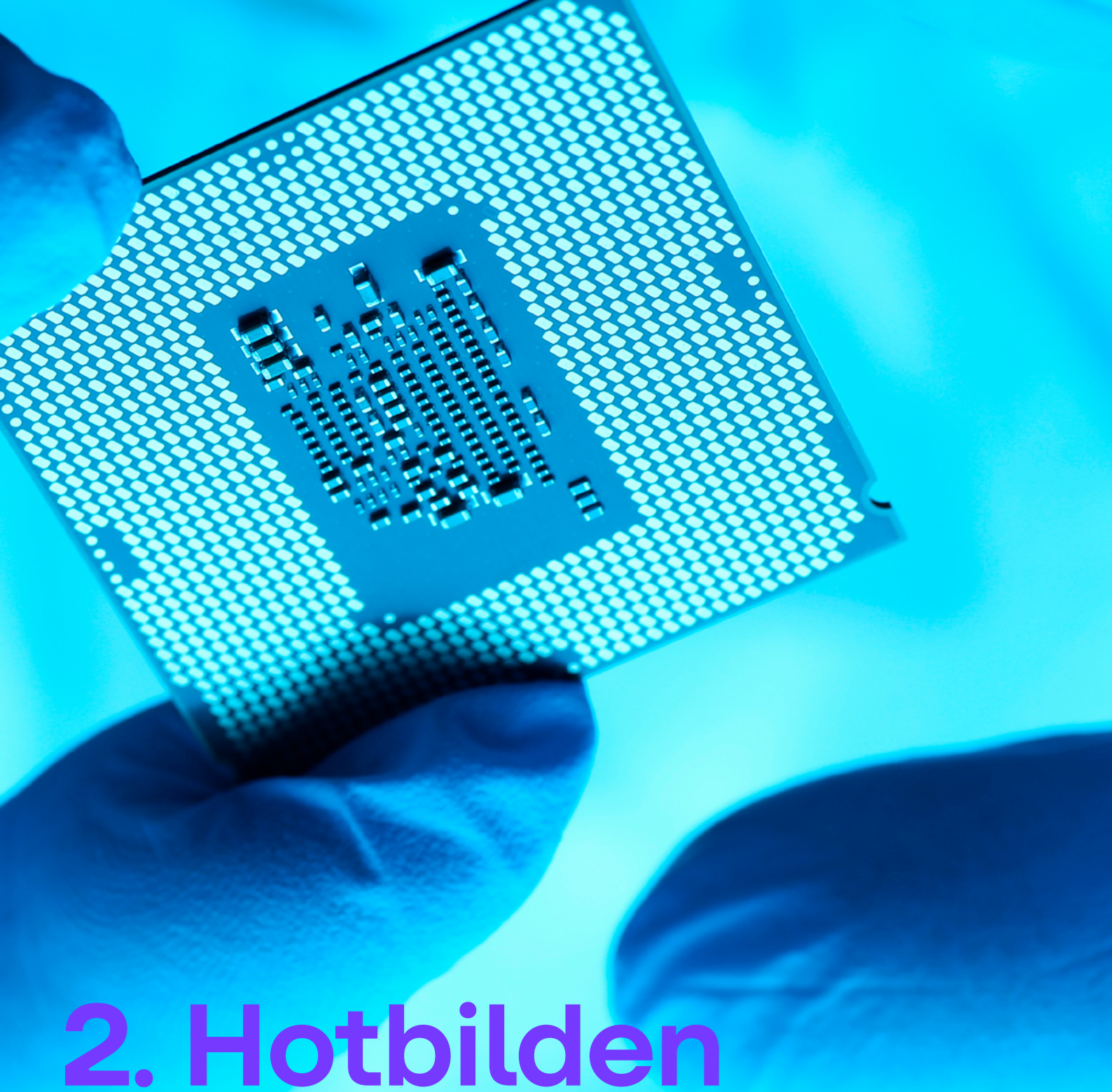
Enligt Säkerhetspolisen (Säpo) har spioneriet mot företag och forskning ökat och tagit sig nya former. Två aspekter står ut: för det första är spionaget allt oftare orkestrerat från statsunderstödda utländska aktörer; för det andra är lärosäten, forskningsinstitut och teknikparker, som samarbetar med företag, i ökande grad primära måltavlor. Kostnaden för de direkta skador orsakat av forskningsspioneri är både faktiska och långsiktiga. Säpo uppskattar de faktiska kostnaderna till flera miljarder kronor årligen, medan de långsiktiga kostnaderna handlar om vårt lands framtida ekonomiska säkerhet och konkurrenskraft.

Syftet med denna vägledning är att belysa säkerhetsdimensioner som bör beaktas vid det viktiga internationella forskningssamarbetet. Fokus är på forskningssamarbeten i allmänhet och internationella samarbeten i synnerhet. Genom att beakta säkerhetsaspekter så ökar möjligheten att arbeta mer effektivt tillsammans, samtidigt som risken minskar för att den framtida konkurrenskraften äventyras.

Vägledningen är framtagen genom ett samarbete mellan Teknikföretagen och Säkerhets- och försvarsföretagen (SOFF) i samråd med Sveriges universitets- och högskoleförbund (SUHF). Teknikföretagen organiserar över 4500 tillverkande och industrinära företag som leder teknikutvecklingen. SOFF företräder företag inom säkerhets- och försvarsområdet med verksamhet i Sverige. SUHF tillvaratar och samordnar 38 universitets och högskolors intressen i olika frågor.

Säkerhetspolisen

”Den tekniska utvecklingen och digitaliseringen skapar stora möjligheter som vi som land givetvis ska ta till oss. Men för att bygga säkerhet och motståndskraft behöver vi också vara medvetna om de hot och sårbarheter som den tekniska utvecklingen och digitaliseringen för med sig.”



2. Hotbilden

Vi befinner oss i ett nytt säkerhetspolitiskt läge i snabb förändring med bland annat Rysslands anfallskrig mot Ukraina, svenskt medlemskap i NATO och ett nationalistiskt och protektionistiskt USA, som håller på att förändra den världsordning vi är vana vid. Samtidigt har EU halkat efter Kina och USA i termer av konkurrenskraft, varför volymen av forskning och utveckling behöver öka. Det talas allt oftare om *de-risking* för att hantera samarbeten och beroenden som hotar vårt framtida välstånd och vår ekonomiska säkerhet. I begreppet ekonomisk säkerhet ingår forsknings-säkerhet för att värna forskningen mot spionage.

Sverige ligger i toppen vad gäller innovation i globala jämförelser, mycket tack vare de stora, systematiska och uthålliga investeringar som gjorts och fortsatt görs i forskning, utveckling och innovation. Internationella forskningssamarbeten är en grundbult och nödvändighet i vårt forskningssamhälle. Vår öppna och fria innovationskultur med nära samverkan mellan lärosäten, institut och näringsliv utgör motor i teknikutvecklingen. Men detta är också en måltavla för antagonistiska aktörer, vars mål är att stjäla spetskunskap och kontrollera nyckelteknologier för egen vinning. Notera att antagonister även kan ägna sig åt sabotage för att vinna tid och komma i kapp i innovation.

Tillsammans med cyberattacker är forskningsspionage en del av den gråzonsproblematik som brukar nämnas i sammanhang relaterade till försvars- och säkerhetssektorn, men som i realiteten omfattar hela samhället. Kunskap och tillgång till nyckelteknologier representerar enorma värden för de aktörer som vill ta genvägar i näringslivs- och teknikutveckling. Företag som utvecklat ny teknik i Sverige riskerar att konkurreras ut av sina egna lösningar, kommersialiserade av företag i länder som ägnar sig åt systematiskt och storskaligt forskningsspionerі. Notera att antagonister också kan ägna sig åt sabotage eller förseningar av forskningsresultat i syfte att vinna tid, hämma andras framsteg och gynna sin egen innovationsutveckling.

Särskilt utsatta områden är de som är strategiskt viktiga för vårt lands konkurrenskraft, försvarsförmåga och omställning till ökad miljömässig, social och ekonomisk hållbarhet. Dessa områden ligger inom främmande makts egna prioriteringar för att stärka deras ekonomiska, militära och säkerhetspolitiska intressen. Sveriges Nato-medlemskap och ökade satsningar på försvaret och därtill hörande forskning inom försvarsteknologi och teknologi med dubbel användning, gör oss som forskningsnation ännu mer påpassade och intressanta för antagonisterna.

Aktiviteterna för att stjäla teknik och forskningsresultat sker ofta i det fördolda under falska förespeglingar. Inte sällan är det utländska, statligt styrda aktörer som står bakom operationerna. Enligt Säpo bedriver idag ett femtontal stater en systematisk underrättelseverksamhet i Sverige med målet att gynna sina egna länders konkurrenskraft och militära förmåga. Aktiviteterna skapar årligen kostnader som uppgår till miljardbelopp för näringslivet och är ett säkerhetshot mot hela Sverige, inte minst vad gäller vår framtida konkurrenskraft och välfärd.

Bästa sättet att motverka att våra kunskapsproducenter, som svenska företag, lärosäten, institut, teknikparker och inkubatorer, utsätts för forskningsspionage är att vi alla är medvetna om vad som bör skyddas, vad antagonisterna är intresserade av och hur de arbetar. Denna skrift försöker därför ge handfasta tips på hur personer involverade i forskningssamverkan kan gå till väga för att skydda det som bör skyddas.

2.1. Hur bedriver främmande makt forskningsspionage?

Enligt både civila och militära säkerhetsmyndigheter är det **Ryssland, Kina och Iran** som bedriver mest spionage i Sverige. Att känna till vad dessa tre länder är ute efter kan ge en vägledning till vad som är särskilt viktigt att vara uppmärksam på vad gäller deras informationsinhämtning.

Enligt den svenska Militära underrättelse- och säkerhetstjänsten (Must) är **Ryssland** framför allt intresserat av västerländsk teknologi som kan bidra till att utveckla nya förmågor och upprätthålla befintliga. Komponenter från EU, däribland från Sverige, är särskilt intressanta eftersom de har avgörande betydelse för kvalificerade ryska vapensystem. De ryska säkerhets- och underrättelsetjänsterna har olika tillvägagångssätt för att komma över teknik, och använder bulvanföretag och ombud för att på ett dolt sätt köpa och importera teknik till ryska slutanvändare.

Kina agerar långsiktigt för att stödja sina globala ambitioner som inkluderar att leda utvecklingen av nyckeltekniker som AI, halvledare och avancerade material. För att uppnå detta använder den kinesiska staten en blandning av lagliga och olagliga metoder. Kinas intressen i Sverige är främst inom områden där vi är ekonomiskt starka eller där vi har framstående utveckling av teknologi. Kina inhämtar information framför allt genom forskningssamarbeten, investeringar, företagsuppköp och underrättelseverksamhet. Teknikområden som är särskilt intressanta är där Sverige ligger långt framme teknologiskt och vetenskapligt.

Iran är likt Kina och Ryssland intresserat av att anskaffa teknik och kunskap i Sverige. Det kan exempelvis handla om att inhämta information och spetskunskap genom svenska lärosäten eller anskaffa produkter med dubbla användningsområden inklusive utveckling av massförstörelsevapen och vapenbärare. Produkter som bygger på sådan teknik finns inom flera olika industrier och kunskapen inkluderar flera vetenskapsområden.

Enligt Säpo har dessa tre länder på senare tid börjat samarbeta och dela information med varandra, vilket gör att det blir ännu mer angeläget att förstå vad de är ute efter. Samtliga tre länder ägnar sig också åt cyberintrång, påverkanskampanjer och förföljelse av dissidenter.

Det finns **fler länder** som är intresserade av svensk forskning, och givet det geopolitiska läget i världen ändras situationen snabbt. Idag är det exempelvis inte ovanligt att använda engångsmobiler och laptops vid besök i **USA**.

2.2. Exempel på forskningsspionage

För att illustrera hur främmande makt arbetar följer här några fallstudier på hur det kan gå till när forskningsresultat stjäls. Fallstudierna nedan är avidentifierade incidenter som har inträffat på riktigt.

2.2.1. Exempel 1

En forskare inom ett teknikområde som är prioriterat av främmande makt blir inbjuden till en stor konferens i ett annat land. Forskaren är världsledande inom sitt område och håller på att avsluta en patentansökan som ska bli grunden i ett företag som forskaren planerar att starta med sina medarbetare i närtid. När forskaren ska göra sin powerpointpresentation vid konferensen kopplas datorn upp via VPN till hemuniversitetet och samtidigt lyckas någon ta sig in i dess system. Två månader senare kontaktas forskaren av kollegor i andra länder som berättar att de noterat att ett företag i det besökta landet har börjat marknadsföra produkter som ser ut att vara baserade på forskarens innovationer och nyss inlämnade patentansökan.

2.2.2. Exempel 2

En framstående professor vid ett tekniskt universitet erbjuds att bli gästprofessor under ett par år vid ett tekniskt institut i ett annat land. Professorn erbjuds ett alldeles nytt laboratorium med så högteknologisk utrustning att det inte finns en motsvarighet i Europa. Finansieringen är redan på plats liksom ett tjugotal doktorander och postdocs. Lönen för gästprofessuren är generöst tilltagen. En variant är att bli deltidsanställd gästprofessor vid samma instituts forskningsfilial i Europa, samtidigt som personen är kvar som professor vid det svenska lärosätet. På detta sätt kan landet i fråga få tillgång till känslig spjutspetsforskning på ett tidigt stadium.

2.2.3. Exempel 3

En utländsk forskare i ett naturvetenskapligt ämne börjar plötsligt intressera sig för ett forskningsområde som ligger utanför forskarens eget område. Forskaren börjar söka upp och träffa personer med kunskap inom området och ställer ingående frågor. Även om forskarens eget område inte anses vara känsligt så är det nya området så pass känsligt att forskarna som är verksamma där blir misstänksamma.

2.2.4. Exempel 4

Som en del i arbetet med att främja inkubatorer har en nation satt upp en tävling för start-ups inom vissa av landets prioriterade områden. Alla forskare som vill starta eget får möjlighet att delta i tävlingen genom att skicka in sina idéer, varpå de bästa förslagen väljs ut för en gratis resa till landet i fråga där forskarna får pitcha idéer till investerare på plats. Första pris är en gratis etablering med betald hyra under ett år i en teknikpark med skattefrihet och startkapital i storleksordningen flera miljoner kronor. På detta vis försvinner svenskfinansierad innovation till annat land, som kan kapitalisera på den i stället för att Sverige ökar sin konkurrenskraft.

2.2.5. Exempel 5

En forskare med ursprung i ett annat land blir erbjuden att föreläsa om sin karriär på sitt alma mater i hemlandet. Betalningen för föreläsningen är en gratis resa med uppehälle till hemlandet, där forskarens gamla sjuka föräldrar bor. Personen ansöker om semester för att besöka föräldrarna och berättar inte för sin arbetsgivare om föreläsningen. Forskaren tar med sig sin jobbdator och sammanställer en PowerPoint om sin forskning på flyget till landet i fråga. Av misstag inkluderas känslig information inbäddat i en powerpointbild från ett samarbetsprojekt med ett företag. På föreläsningen laddar forskaren ner presentationen på en annan dator, men glömmer att ta bort den efteråt och den hemliga informationen hamnar i fel händer.

2.2.6. Exempel 6

En gästprofessor från ett utländskt universitet bjuds in att forska vid ett svenskt universitet. Eftersom gästprofessorn bara ska vara där ett par månader och forskar inom ett ofarligt område görs ingen utökad riskbedömning av vistelsen. Gästprofessorn kommer att dela forskningsinfrastruktur, både fysiskt i form av lokaler och tekniskt i form av IT, med andra forskare som ägnar sig åt mer känslig forskning i Projekt X. Genom delade kataloger på gemensam server kommer gästprofessorn över intressant information från Projekt X, som vidarebefordrar till hemlandet utan att bli upptäckt. I fikarummet lär gästprofessorn känna forskare från Projekt X, som senare blir inbjudna att forska i personens hemland. På så sätt ökar landet sin informationsinhämtning utan att den har godkänts av lärosätet.

2.2.7. Exempel 7

En person kontaktar dig på LinkedIn och skriver att han/hon beundrar dig och din forskning och vill ha kontakt med dig för att följa dig i sociala medier. Du kontrollerar vem personen och vilka gemensamma kontakter ni har. Eftersom ni har många gemensamma kontakter så accepterar du inbjudan. Om du hade googlat personen via Google Scholar, eller bara gjort en vanlig webbsökning så hade du sett att personen inte finns på riktigt. Vad du inte vet är att era gemensamma kontakter har tackat ja på samma sätt som du har gjort: ”Eftersom A känner BCD så är nog A en reko person.” I verkligheten är det ingen av er som vet vem A är. Den personinformation som samlas in om dig kan senare användas för skräddarsydd rekrytering eller phishingförsök.

3. Checklista

För att synliggöra behovet av säkerhetsmedvetande vid forsknings-samarbeten finns nedan ett antal punkter som forskare med stöd av sin organisation kan vidta inför, under och efter ett samarbete.


Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Innovation
Branding
Solution
Marketing
Analysis
Ideas
Success
Management

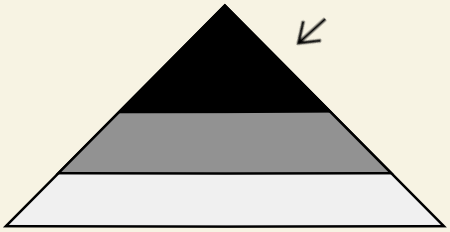
3.1. *Inför* ett samarbete: riskinventering och åtgärder

En riskinventering innebär att uppmärksamma eventuella risker, bedöma hur sannolikt det är att de inträffar och sedan agera för att motverka dem. Ett förslag är att i första hand identifiera reglerade risker och säkerhetsaspekter i projektet och därefter fokusera på säkerhetsaspekter och risker som inte är reglerade i dag, men ändå kan vara och bli problematiska på sikt.

I triangeln illustreras de områden som är känsliga och regleras genom säkerhetsskydds-lagstiftning, exportkontroll och investeringsgranskning i den svarta delen, medan den grå delen innefattar områden som är utmanande i nuläget och riskerar att bli reglerade i framtiden. De vita aspekterna handlar om mer ”mjuka” värden som framför allt innefattar den bredare definitionen av ansvarsfull internationalisering.

3.1.1 Identifiering av reglerade säkerhetsaspekter

Faller något av projektets olika delar inom områden som innefattar **teknik/produkter med dubbla användningsområden (PDA)**, berörs av **säkerhetsskydd** eller l**agen om utländska direktinvesteringar (UDI)**? Om någon av dessa frågor besvaras jakande så ska en ansökan om export-tillstånd göras tillsammans en säkerhetsskydds-analys (se 3.1.2. nedan) och säkerhetsprövning av individer som är med i forskningsprojektet. Därtill kan en anmälan om utländsk direktinvestering vara befogad.



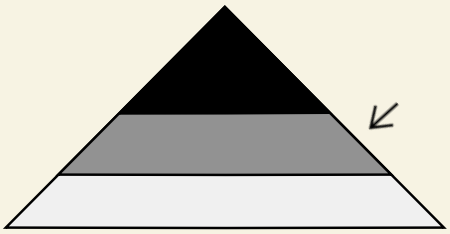
1. PDA/krigsmateriel
2. Säkerhetsskydd
3. Investeringsgranskning

→

1. Exporttillstånd
2. Säkerhetsskyddsanalys
3. Anmälan om utländsk direktinvestering

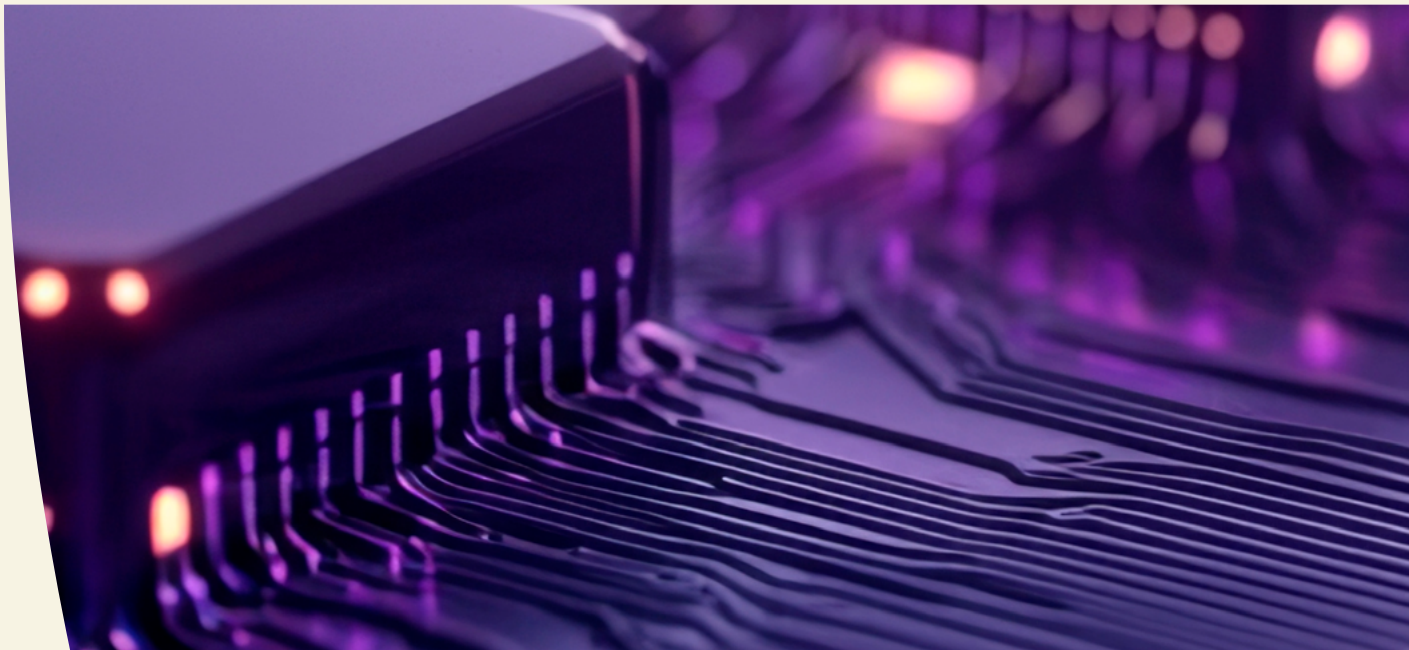
3.1.2. Identifiera icke-reglerade säkerhetsaspekter

När ett nytt forskningssamarbete etableras rekommenderas att en granskning genomförs, en due diligence, efter att riskanalysen gjorts ovan (inklusive eventuell säkerhetsskydds-analys). Syftet med due diligence är att upptäcka om det även förekommer säkerhetsaspekter och risker som faller utanför regleringarna, men som ändå kan vara problematiska eller bli problematiska i framtiden. Denna del av granskningen täcker in de områden som finns i **triangelns gråzon**, framför allt för att upptäcka säkerhetsaspekter utan reglering, men även för att upptäcka andra utmaningar.



Granskningen bör därför fokusera på att belysa problematiska etiska, juridiska, ekonomiska och nationella säkerhetsöverväganden, till exempel vilken roll potentiella samarbetspartners spelar i sina hemländer och om dessa aktörer har kopplingar till försvarsindustri eller militära intressen. Enkla initiala åtgärder är att begära in samarbetspartnerns CV och kontrollera deras bakgrund, inklusive utbildning och arbetslivserfarenhet, vilka forskningsinstitut och lärosäte som listats, samt att verifiera att årtalen hänger ihop så att personen inte har luckor i sin bakgrund. Förslag på olika frågor som kan ställas vid en granskning finns listade i appendix på denna skrift.

Vissa kinesiska universitet och forskningsinstitut arbetar nära den kinesiska försvarsmakten och försvarsindustrin. Australiensiska tankesmedjan ASPI har gjort en databas som kan ge indikationer över hur mycket militärt samarbete olika lärosäten och institut har. Notera att databasen är från 2019 och kan vara inaktuell inom vissa områden eftersom teknikutvecklingen går fort. En annan risk med Kina är kommunistpartiets närvaro på lärosätena och styrning av forskningen för att uppnå politiska mål på ett sätt som skiljer sig starkt från den svenska forskningsvärldens akademiska frihet.



Vad gäller strategiskt intressant forskning kan det finnas ett värde i att fundera över känsligheten i teknikområden som faller utanför de som är reglerade inom exportkontroll, produkter med dubbel användning och investeringsgranskning. De strategiskt intressanta teknologierna bedöms kunna komma att utgöra viktiga ekonomiska värden för både Sverige och EU i framtiden. De är en del av vår ekonomiska säkerhet och utgör en grund för vår ekonomiska tillväxt och i förlängningen vårt välstånd.

Eftersom världen är föränderlig så kan vi dock inte i dagsläget veta exakt vilka tekniker som kan komma att bli de avgörande och mest strategiskt intressanta inom ramen för vår ekonomiska säkerhet. Som vägledning kan man studera EU-kommissionens aktuella lista, se nedan, eller de teknikområden som Vinnova har identifierat som strategiskt viktiga för Sverige:

- Artificiell intelligens och autonoma system för samhällsomställning
- Avancerad digital teknik för produktivitet och säkerhet
- Kvantteknik för säkerhet och industriella tillämpningar
- Energiteknik för fossilfri elektrifiering
- Material- och produktionsteknik för omställning
- Bioteknik för hälsa och klimatomställning

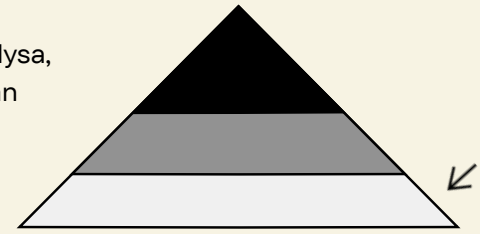
Vi rekommenderar att man som forskare reflekterar kring vad man själv tror skulle kunna vara känsligt och intressant för antagonister. Dessa listor är alltså inte reglerade i lag, men de kan ses som relevanta att ha med i *due diligence* för att komma åt det som skulle kunna bli intressant för antagonister och främmande makt.

När granskningen är gjord blir det lättare att få förståelse för hur forskningen i ett samarbete kan utföras i praktiken på ett säkert sätt. Notera att alla samarbeten bör genomlysas med viss regelbundenhet eftersom forskningsprojekt utvecklas och kan få nya inriktningar, samtidigt som lagstiftning tillkommer och den geopolitiska omgivningen är i ständig förändring, särskilt i dagsläget.

Lista över kritiska teknologier för EU:s ekonomiska säkerhet enligt EU Kommissionens rekommendationer från den 3 oktober 2023.

KRITISKA TEKNIKER	EXEMPEL PÅ INGÅENDE OMRÅDEN
Avancerad halvledarteknik	· Mikroelektronik, inbegripet processorer · Fotonikteknik och högenergilaserteknik · Högfrekvenshalvledare · Utrustning för tillverkning av halvledare
AI-teknik	· Högpresterande datorsystem · Moln- och kantdatorsystem · Dataanalysteknik · Datorseende och objektigenkänning · Bearbetning av språk
Kvantteknik	· Kvantdatorteknik · Kvantkryptografi · Kvantkommunikation · Kvantsensorteknik och radar
Bioteknik	· Teknik för genetisk modifiering · Nya genomiska metoder · Gendrivare · Syntetisk biolog
Avancerad konnektivitet, navigation och digital teknik	· Säker digital kommunikation och konnektivitet (ex. RAN, Open RAN och 6G) · Cybersäkerhetsteknik · Säkerhets och intrångssystem · Digital kriminalteknik · Sakernas internet och virtuell verklighet · Distribuerad databasteknik · Teknik för digital identitet · Vägleднings-, navigations- och kontrollteknik, flygelektronik, marin positionsbestämning
Avancerad sensorteknik	· Elektrooptiska, radarbaserade, kemiska och biologiska sensorsystem · Strålningsbaserade och distribuerade sensorsystem · Magnetometrar, magnetiska gradiometrar · Sensorer för elektriska undervattensfält · Gravimetrar
Rymd och framdrivningsteknik	· Rymdfokuserad teknik från komponent- till systemnivå · Teknik för rymdövervakning och jordobservation · Positionering, navigering och tidsbestämning (PNT) · Satellit i jordnära omloppsbana (LEO) · Framdrivningsteknik · Hypersonisk teknik · Komponenter för militär användning
Energiteknik	· Teknik för kärnfusion · Kärnreaktorer och elproduktion · Radiologisk omvandlings och anrikningsteknik · Väte och nya bränslen · Nettonollteknik, inbegripet fotocellteknik · Smarta nät och energilagring, batterier
Robotar och autonoma system	· AI-baserade system, drönare och fordon · Robotar, robotkontrollerade precisionssystem · Exoskelett
Avancerad material-, tillverkning och återvinningsteknik	· Teknik för nanomaterial och intelligenta material · Avancerade keramiska material · Stealth-material · Inbyggd säkerhet och hållbarhet hos material · Additiv tillverkning · Digitalstyrd mikroprecisionstillverkning · Småskaliga lasermaskiner och lasersvetsar · Teknik för utvinning och bearbetning, hydrometallurgisk återvinning, biolakning, nanoteknikbaserad filtrering, elektrokemisk bearbetning och svart massa

3.1.3. Identifiera andra viktiga aspekter



För att komma åt andra viktiga aspekter att belysa, som ligger i den vita delen av triangeln, kan man även göra en riskbedöming av internationella forskningssamarbeten genom att använda sig av SUHF:s checklista för Global responsible engagement. Notera att denna lista i viss mån även täcker de tidigare nämnda områdena i triangeln. Där ställs ett antal frågor inom följande områden:

1. Demokratiska principer och begränsad akademisk frihet.
2. Partnerns rykte och universitetets värderingar.
3. Konflikter gällande användning av data, IPR och patenträttigheter.
4. Felanvändning av forskning och negativa, icke-medveten användning.
5. Etisk dumpning och säkerhet runt personliga och biologiska data.
6. Personlig säkerhet.

3.1.4. Identifiera intressekonflikter

Att identifiera potentiella intressekonflikter är en viktig hörnsten i förberedelserna inför ett forskningssamarbete då det skapar medvetenhet om säkerhetsbehov och processer. Det handlar både om att analysera hur arbetet kan utföras och vad resultaten kan användas till.

3.2. Praktiska förberedelser inför samarbetet

Detta avsnitt beskriver mer detaljerat om några förberedelser som bör göras inför samarbetet. Notera att man måste ansöka om exporttillstånd osv innan projektet startas om det behövs. I denna del belyses särskilt säkerhetsskyddsanalys, riktlinjer, segmentering av data, och logga aktiviteter.

3.2.1. Säkerhetsskyddsanalys: viss verksamhet kan vara säkerhetskänslig

Säkerhetsskydd handlar om att värna den information och de verksamheter som är säkerhetskänsliga. Säkerhetsskyddsklassificerade uppgifter får inte villkorslöst förmedlas till organisationer utanför Sverige. Detta är primärt verksamhet som har bäring för Sveriges säkerhet, men inkluderar, utöver försvar och rättsväsende, bland annat forskningsverksamhet på lärosäten, institut, teknikparker och inkubatorer eller direkt hos enskilda företag. Det är organisationens eget ansvar att genomföra en säkerhetsskyddsanalys och ställa sig frågan om huruvida verksamheten kan vara säkerhetskänslig. I säkerhetsorganisationen finns normalt kompetens för att hantera området. Åtgärder och rutiner skall skrivas ner i en säkerhetsskyddsplan vid behov.

Inom ramen för säkerhetsskyddsområdet inryms flera aspekter, däribland säkerhetsskydds-analys, informationssäkerhet, fysisk säkerhet, personalsäkerhet och säkerhetsskyddad upphandling. På alla dessa områden, inklusive en introduktion för säkerhetsskydd, har Säpo publicerat lättöverskådliga vägledningar som är fritt tillgängliga via myndighetens webbsida. Området regleras av säkerhetsskyddslagen och säkerhetsskyddsförordningen.

Tips i vardagen – säkerhetsskydd

- Kontakta säkerhetsavdelningen som kan stötta och hjälpa till med säkerhetsskyddet under samarbetets gång.
- Graden av känslighet hos informationen avgör hur den bör delas.
- Se till att all delning av data skyddas av kryptering.

3.2.2. Publicera riktlinjer och arbetsrutiner för att undvika otillbörlig påverkan

Att ha en tydlig uppsättning principer - en uppförandekod - som beskriver hur arbetet rent praktiskt ska bedrivas i de fall utländsk påverkan misstänks, skapar ett ramverk för alla inblandade i ett forskningssamarbete. Uppförandekoden bör inkludera skrivelser om transparens kring rapportering av finansieringskällor (inklusive donationer) från utländska aktörer, för att undvika misstankar om korruption, samt översiktliga processer för hur otillbörlig påverkan ska hanteras om den upptäcks. Information om hur penningtvätt och korruption kan undvikas finns bland annat hos Business Sweden.

3.2.3. Segmentera åtkomst till data och resultat

Att säkerställa att data och resultat kan skyddas är fundamentalt inför ett samarbete. Data och resultat inom och mellan olika forskningssamarbeten bör segmenteras så att allt material inte finns på ett ställe dit alla har tillgång. Detta gäller både fysiskt och digitalt. I de fall digitala samarbetsplattformar och molntjänster används bör dessa granskas med avseende på var och hur lagring och åtkomst sker. Beakta också att risken har ökat för att internationella molntjänster kan stängas av med minimal förvarning.

Det ska framhållas att vissa länder har nationella cybersäkerhetslagar som innebär att data måste lagras i det aktuella landet vid forskningssamarbeten. Vid sådana situationer behöver valet göras kring vad det är för slags data som är lämplig att lagra på främmande mark, och vem som mer kan ha tillgång till denna data.

3.2.4. Skapa möjlighet att automatiskt logga aktiviteter

Att möjliggöra spårbarhet i ett samarbete har en preventiv effekt mot överträdelser och säkerhetshotande aktörer. Rutiner för att automatiskt logga aktiviteter bör därför inkluderas liksom att all access knyts till individuella konton. Olika konton bör rutinmässigt ges olika behörighetsnivåer som återspeglar vilken tillgång som faktiskt behövs för lämpligast segmentering av åtkomsten.

3.3. *Under* ett samarbete

Notera att många steg som ska göras under ett samarbete är sådana som redan har gjorts inför samarbetet och i vissa fall måste göras om kontinuerligt hela tiden. Det gäller exempelvis att fortlöpande se till att cybersäkerheten är bra. Nedan listas några av de åtgärder som behöver belysas extra noga.

3.3.1. Skydda all digital information

Skydd av data, resultat och information som delas digitalt är centralt i ett samarbete. Det finns alltid en risk att företag, lärosäten, institut, teknikparker och inkubatorer som arbetar med forskning kan utsättas för cyberangrepp.

På den mest grundläggande nivån bör processer och riktlinjer finnas till hand för att beakta de tio rekommendationer från Nationellt Cybersäkerhetscenter (se lista på nästa sida).

Exempel på intrångsförsök:

Genom ett phishingmail får mottagaren en adress för att registrera sig på sitt universitetsbibliotek. Via inloggningsuppgifterna kan antagonisten hämta data från det interna nätverket och utföra en cyberattack.

REKOMMENDERADE DIGITALA SÄKERHETSÅTGÄRDER

Källa: Nationellt Cybersäkerhetscenters rapport Cybersäkerhet i Sverige 2024.

1. Säkerställ förmågan att upptäcka säkerhetshändelser

För att effektivt kunna upptäcka säkerhetshändelser i den digitala miljön är det viktigt att skapa en förmåga att identifiera dessa så tidigt som möjligt. Det kan göras genom en kombination av manuella, tekniska och automatiserade metoder.

2. Installera säkerhetsuppdateringar skyndsamt

Se till att prioritera uppdateringar för informationssystem som är exponerade mot internet. Prioritera också system och tillämpningar som är verksamhetskritiska eller har sårbarheter som riskerar att utnyttjas. Målet bör vara att installera säkerhetsuppdateringar så snart de publiceras.

3. Förvalta behörigheter och använd stark autentisering

Kontrollera alla konton i den digitala miljön och inaktivera de som inte längre används. Tilldela bara nödvändiga behörigheter.

4. Begränsa och skydda användningen av höga behörigheter

Skyddet av administrativa behörigheter är viktigt för att minska säkerhetsrisker i den digitala miljön. Genom att införa tydliga rutiner för tilldelning och användning av dessa behörigheter kan organisationer skydda sina system och data.

5. Inaktivera oanvända tjänster och protokoll

För att skydda informationssystem från hot är det viktigt att stänga av funktioner som inte behövs för systemets drift. Genom att använda rätt säkerhetsåtgärder minskar risken för att systemet utsätts för attacker.

6. Säkerhetskopiera och testa återställning av information

Att skapa och testa säkerhetskopior är viktigt för att skydda information och system mot informationsförlust. Genom regelbundna säkerhetskopior kan organisationer snabbt återställa data och minimera störningar vid incidenter.

7. Segmentera och kontrollera åtkomst i digitala system

För att skydda organisationens digitala miljöer är det avgörande att segmentera nätverket för att begränsa och övervaka trafikflödena mellan olika delar av systemet. Det är också viktigt att säkerställa att endast godkänd utrustning tillåts ansluta.

8. Säkerställ att endast godkänd mjukvara får köras

Endast tillåten mjukvara ska köras i den digitala miljön. Genom att använda så kallad vitlistning kan organisationen skydda sina system och information genom att förhindra att otillåten mjukvara används.

9. Uppgradera mjuk- och hårdvara

Byt ut och ersätt gammal mjuk- och hårdvara för att minska sårbarheter och säkerställa att system fungerar som de ska och har tillräcklig säkerhet. För att minska sårbarheter bör mjuk- och hårdvara användas som fortfarande får uppdateringar och support från leverantören.

10. Kontrollera digital åtkomst via internet

För att skydda interna system och data från obehörig kommunikation med omvärlden är säker internetåtkomst avgörande. Åtgärder kan behövas för att förhindra att ett angripet system kan missbrukas för fjärrstyrning eller datastöld.

3.3.2. Var försiktig vid delning

USB-enheter, minneskort och molntjänster underlättar filöverföring både mellan organisationer och individer. Fem aspekter är dock värda att ha i åtanke:

- Källan till externa enheter som USB kan vara opålitlig och därmed osäker.
- Det är möjligt att köra skadlig kod om ”autorun” är aktiverat på enheten som informationen ska tas emot på.
- Avsaknad av automatisk genomsökning via antivirusprogram på externa enheter medför påtaglig risk att utsättas för skadlig kod.
- Kontrollera var information som lagras i molntjänster finns eftersom olika länder har olika lagstiftning om hur tillgängliga molnservrar ska vara.
- Om en molntjänst som används i ett projekt har servrar utomlands måste man se över att informationen som lagras där inte är föremål för exportkontroll.

3.3.3. Förhindra nätfiskeattacker (”phishing”)

Nätfiskeattacker är en av de mest förekommande metoderna som används för att otillbörligt försöka få tillgång till personlig eller kritisk information. Detta sker exempelvis genom att skicka med skadliga länkar eller bilagor via e-post. Meddelanden som skickas av nätfiskare förefaller ofta som autentiska genom att försöka utge sig för att vara från någon pålitlig källa.

Några viktiga medskick:

- Nätfiskare använder ofta information som finns tillgänglig på sociala medier. Granska därför personliga integritetsinställningar och tänk på vad som läggs upp online.
- Addera inte slentrianmässigt nya kontakter via LinkedIn, eller andra sociala plattformar. Se fallstudie 7 på sida 11.
- Tänk en extra gång på vad som faktiskt efterfrågas och varför – nätfiskare använder ofta en brådskande uppmaning att delge personlig information eller genomföra transaktioner.
- Vid misstanke: anmäl omedelbart till närmaste chef eller IT-ansvarig. Detta för att minimera potentiella skador.

3.3.4. Etablera ett säkerhetsmedvetande

Säkerhet handlar om mer än tekniska system. I stor utsträckning är graden av säkerhet en högst ”mänsklig” fråga, vilket gör att alla inom en organisation på olika sätt bidrar till att säkerhetsmedvetande kan etableras. Alla behöver tänka och agera på ett säkert sätt och ha medvetenhet om vilka säkerhetsföreskrifter som gäller samt varför de finns på plats.

Säkerhetsmedvetandet bör även omfatta informationsdelning vid tjänsteresor, vilket gör att det är av största vikt att anställda och inblandade i projektet vet vad som gäller när det kommer till att förflytta eventuell information mellan olika länder. Detta kan nämligen falla in under exportkontrollagstiftningen, *se vidare under punkt 3.3.7. om legala regelverk nedan*.

3.3.5 Genomför kommunikationsinsatser och utbildning

Kommunikationsstrategier och utbildningsprogram ökar medvetenheten kring de risker som finns och kommer av forskningssamarbete. Det är därför viktigt att kontinuerligt kommunicera om hotbilden för att hålla den aktuell. Ju högre medvetenheten är, desto mer stärks säkerhetskulturen och motståndet mot fientliga intrång och påverkan.

3.3.6. Fysiska åtgärder inklusive åtkomst av lokaler

I vissa forskningssamarbeten kan det även krävas rent fysiska åtgärder, som zonindelning i lokalerna där vissa delar endast är tillgängliga för de inblandade personerna. Genom att implementera det blir det lättare att kontrollera att obehöriga inte kommer in i dessa lokaler.

3.3.7. Följ legala regelverk

Exportkontroll

En inte alltid uppenbar aspekt av forskningssamarbete är att ha insyn i och förståelse för att den forskning som bedrivs kan vara föremål för exportkontroll. Forskningsaktiviteter omfattas nämligen av exportkontrollagstiftningen. Det kan därför behövas exporttillstånd för att få bedriva specifik forskning och dela resultat med aktörer utomlands. När det kommer till att dela kunskap med en utländsk aktör talas det ofta om teknologiöverföring, vilket i sig är exportkontrollerat i det fall informationen är exportkontrollklassad. Det är därför av vikt att klargöra huruvida forskningen är listad i något exportkontrollregelverk och agera därefter.

PDA står för ”produkter med dubbla användningsområden” vilket betyder att de kan ha både en civil och militär tillämpning. I EU:s PDA-förordning återfinns vad som är export-kontrollerat, bland annat: materialbearbetning, elektronik, datorer, telekommunikation och informations-säkerhet, sensorer och lasrar, navigation och avionik samt rymdteknik. EU-kommissionen har tagit fram en vägledning för forskningsorganisationer och forskare för att underlätta efterlevnaden av exportkontrollregelverket. För de flesta områden är Inspektionen för strategiska produkter (ISP) tillståndsmyndighet. Strålsäkerhetsmyndigheten är dock tillsynsmyndighet för kärnmaterial och relaterad utrustning.

När det gäller hantering av exportkontrollerade produkter eller information är det relevant att veta vad som gäller när det kommer till hur de får fraktas och även lagras. Tänk exempelvis på huruvida information lagras i molntjänster och var de fysiska servrarna är placerade, då detta kan bli ett exportkontrollerat förfarande. Vid frågor, kontakta den aktuella tillståndsmyndigheten. Mer översiktlig information om teknik och exportkontroll återfinns också på SOFFs informationssida Försvarsexport.se.

Lagen om granskning av utländska direktinvesteringar

Sedan december 2023 är ISP granskningsmyndighet enligt lagen om granskning av utländska direktinvesteringar. Lagen om granskning av utländska direktinvesteringar etablerar en skyldighet att anmäla investeringar som görs i ett antal skyddsvärda verksamheter (sju olika sektorer), som bedrivs av ett aktiebolag, ett europabolag, ett handelsbolag, en ekonomisk förening eller en stiftelse med säte i Sverige. Även investeringar i skyddsvärd verksamhet som bedrivs i ett enkelt bolag eller som enskild näringsverksamhet i Sverige omfattas.

De sju sektorer som omfattas är följande:

- Samhällsviktig verksamhet
- Säkerhetskänslig verksamhet
- Kritiska råvaror, metaller eller mineral
- Känsliga personuppgifter eller lokaliseringsuppgifter
- Krigsmateriel eller tekniskt stöd avseende krigsmateriel
- Produkter med dubbla användningsområden eller tekniskt bistånd
- Framväxande teknik eller annan strategiskt skyddsvärd teknik

Läs mer på ISP:s hemsida samt på MSB:s hemsida.

Lagen om företagshemligheter
Sedan 1 juli 2018 finns en lag om företagshemligheter, som syftar till att skydda känslig information som har ekonomiskt värde för företag och forskningsinstitutioner. En företagshemlighet är information som rör ett företags affärs- eller driftförhållanden, inte är allmänt känd eller lättillgänglig, har ekonomiskt värde just för att den är hemlig, och skyddas av företaget genom rimliga säkerhetsåtgärder. Ett angrepp på en företagshemlighet innebär att någon utan tillstånd anskaffar, utnyttjar eller röjer företagshemligheten. Det kan även inkludera att tillverka eller sälja produkter som bygger på en angripen företagshemlighet. Anställda får inte röja företagshemligheter under anställningen. Efter anställningen gäller skyddet för hemligheter som är särskilt känsliga eller där avtal finns. Läs mer om lagen om företagshemligheter här. Den som vill testa om ens företag har immateriella tillgångar kan göra det på PRV:s hemsida.

Annan lagstiftning
Vid ett internationellt forskningssamarbete, eller samarbete med en utländsk finansiär, är det också viktigt att kunskap finns om vilka lagar eller regelverk som kan påverka avtal eller partnerskap. Ett exempel är **General Data Protection Regulation (GDPR),** och/eller motsvarande lagstiftning utanför EU, och ansvaret som finns för att skydda personliga data och information. Om konkurrerande företag deltar i samma forskningssamarbete måste också konkurrenslagstiftning beaktas.

3.3.8. Genomför personkontroll kopplat till vilken verksamhet som bedrivs
Med internationellt samarbete följer ett särskilt behov av att ha förståelse för forskares bakgrund och tidigare arbete. Alla inblandade i forskningssamarbeten (såväl studenter och forskare som annan berörd personal) vilka ges tillgång till exempelvis forskningsinfrastruktur och test- och demonstrationsmiljöer bör granskas, både före och under projektets gång. Betänk också vilka förväntningar som kan finnas på de som är involverade i ett forskningsprojekt efter att samarbetet avslutats. Tydlighet kring sekretess och ”non-disclosure” i form av juridiskt bindande avtal kan vara nödvändigt att använda på rutinbasis.

Om svenska forskare arbetar på plats (utomlands) i ett land vars demokratiska eller etiska värderingar skiljer sig från Sveriges, kan det vara nödvändigt att göra en bredare riskbedömning för denna personal och kunna svara på frågor som:

- Vilka avtal finns det med den organisation som kommer att vara värd för dem utomlands?
- Vilka regler och lagar i landet de befinner sig i måste de följa?
- Strider någon av dessa lagar mot något av de avtal som ingåtts?
- Om något misstänkt inträffar, vem är ansvarig och hur ska rapportering ske?
- Kommer arbetet de utför vara föremål för exportkontroll i Sverige?
- Finns det någon risk för att personal kan hotas direkt eller indirekt (mot närstående) och om detta skulle inträffa: hur ska den utsatte rapportera detta samt hur ska det sedermera hanteras?

3.3.9. Anmälan till svenska myndigheter
I det fall en organisation bedriver säkerhetskänslig verksamhet och ett intrång har eller misstänks ha skett, ska en anmälan skyndsamt göras till Säpo. Om organisationen eller aktuell verksamhet faller under Försvarsmaktens tillsynsansvar ska anmälan göras där.

Vid misstanke om intrång bör alltid en polisanmälan göras. Notera att detta även gäller om misstanken uppstår under samarbetsprojektets gång.

Alla inblandade organisationer i ett forskningssamarbete bör ta ett ansvar för att upprätta tydliga rutiner för hur ärenden och incidenter ska hanteras och vem som är ansvarig för att detta sker. Det bör också finnas namngivna kontaktpersoner gentemot ansvariga myndigheter. Säpo listar ett antal scenarion där en anmälan ska göras:

1. Om en säkerhetsskyddsklassificerad uppgift kan ha röjts.
2. Om det inträffat en IT-incident i ett informationssystem där säkerhetskänsliga uppgifter finns.
3. Om verksamhetsutövaren får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet.

Mer information om proceduren för anmälan återfinns på Säpos hemsida.

3.4. *Efter* ett samarbete: utvärdering

Konkurrens, plagiering och spionerі är bekanta koncept för de som arbetar inom forskning och innovation. Om en fientligt inställd utländsk aktör skulle få access till exempelvis forskningsdata eller resultat kan en organisation och dess forskning påverkas på en rad sätt, exempelvis genom att organisationens förtroende äventyras genom ett försämrat rykte, vilket i sin tur leder till svårigheter att ta sig an forskningsprojekt i framtiden.

Efter ett genomfört samarbete bör därför en uppföljande samarbetsanalys genomföras där man ställer sig frågan om nya risker som inte förutsågs har uppstått. Utgångspunkten bör lämpligen vara den riskanalys som genomförts inför ett samarbete. Inom ramen för en sådan uppföljande analys går det att konstatera huruvida nya faktorer behöver bearbetas eller om nya risker uppkommit.

Notera att det också är viktigt att göra säkerhetsanalyser löpande under projektet för att undvika problem.

Appendix

Här är ett förslag på olika frågeställningar som bör belysas i en granskning av forskningsprojekt. Notera att de täcker in olika delar av den svart-grå-vita triangeln.

1. Förekommer verksamhet inom samhällsviktig sektor med fokus på eller koppling till sektorns funktionalitet, sårbarhet eller brister som inte är allmänt känd information? Samhällsviktig sektor faller inom ramen för säkerhetsskydd.

Kritiska sektorer *är energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, vatten och avlopp, förvaltning av informations- och kommunikationsteknik inklusive tjänster, offentlig förvaltning och rymden.*

Viktiga sektorer *är avfallshantering, digitala leverantörer av marknadsplatser online, sökmotorer och sociala nätverkstjänster, post- och budtjänster, produktion, bearbetning och distribution av livsmedel, tillverkning, produktion och distribution av kemikalier, tillverkning (motorfordon, datorer, osv).*

2. Förekommer forskning i samarbete med myndigheter som har koppling till samhällets förmåga att förebygga och hantera kriser eller större olyckor (dvs. totalförsvaret)? Dessa myndigheter kan falla inom ramen för säkerhetsskydd.

Exempel: MSB, Försvarsmakten, Post- och Telestyrelsen, Svenska Kraftnät.

3. Förekommer forskning kring geologiska förhållanden, exempelvis studier av berggrunden eller förekomst av mineraler?

4. Förekommer forskning eller hantering av farliga ämnen som vid sabotage skulle kunna orsaka stor samhällsskada (fokus på biologiskt, kemiskt eller radioaktivt hot)?

5. Rör forskningen tekniskt avancerade områden, så kallad nyckelteknologi, som har stor ekonomisk potential och/eller möjliggör grön omställning, och faller i den grå zonen?

6. Förekommer teknologi eller mjukvara som skulle kunna dubbel användning?

7. Är forskningen strategiskt intressant och skulle kunna ingå i vad EU definierat som kritisk teknologi som kan påverka vår ekonomiska säkerhet? *Se listorna över EU:s tio teknikområden och Vinnovas identifierade strategiskt viktiga tekniker för Sverige.*

Källor

ASPI China Defense University Tracker (2019)
https://unitracker.aspi.org.au/

Vinnovas rapport om strategiska teknikområden (2024)
https://www.vinnova.se/globalassets/publikationer/2024/rapport-ru-strategiska-teknikomraden_ver-01.0-final-1.pdf?cb=20241030174857

EU-kommissionens lista över kritiska teknologier för EU:s ekonomiska säkerhet (2023-10-03)
https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=OJ:L_202302113

SUHF:s checklista för Global responsible engagement
https://suhf.se/app/uploads/2023/04/SUHF-Checklist-Global-Responsible-Engagement-REC.-2023-4-230411-REVISED.pdf

Säpos vägledning om säkerhetsskydd
https://sakerhetspolisen.se/sakerhetsskydd.html https://sakerhetspolisen.se/sakerhetsskydd/lag-forordning-och-foreskrifter.html

Business Sweden om hur man undviker penningtvätt och korruption
https://guider.business-sweden.com/guider/exportguiden/tradecompliance/penningtvatt
https://guider.business-sweden.com/guider/exportguiden/tradecompliance

Internationella handelskammaren i Sveriges guide om ”Anti-korruption Due diligence på externa aktörer: en guide för små och medelstora företag”
https://www.icc.se/wp-content/uploads/2015/04/ICC-2017-Anti-korruption_Due-diligence-p%C3%A5-externa-akt%C3%B6rer-en-guide-f%C3%B6r-sm%C3%A5-och-medelstora-f%C3%B6retag.pdf

Nationellt cybersäkerhetscenter (NCSC) https://www.ncsc.se/

NCSC:s rapport om cybersäkerhet i Sverige 2024
https://www.ncsc.se/siteassets/publikationer/cybersakerhet-i-sverige-2024.pdf

EU:s PDA-förordning
https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32021R0821&from=EN

EU-kommissionen vägledning för forskningsorganisationer och forskare
https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32021H1700&from=EN

Inspektionen för strategiska produkter https://www.isp.se/

Strålskyddsmyndigheten https://www.stralsakerhetsmyndigheten.se/

Försvarsexport (SOFF) https://forsvarsexport.se/

Utländska direktinvesteringar https://isp.se/utlandska-direktinvesteringar/

Myndigheten för samhällsskydd och beredskap (MSB): Regler gällande direktinvesteringar
https://www.msb.se/sv/regler/gallande-regler/civilt-forsvar/msbfs-20249/

Lagen om företagshemligheter
https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2018558-om-foretagshemligheter_sfs-2018-558/

Patent- och registreringsverket (PRV) stöd om företags immateriella tillgångar
https://www.prv.se/sv/kunskap-och-stod/vanliga-ord-och-begrepp/foretagshemlighet/

Säpo: anmälan vid säkerhetshotande händelser
https://sakerhetspolisen.se/sakerhetsskydd/anmalan-vid-sakerhetshotande-handelser.html

Teknikföretagen SOFF

Publicerad: 2025