Skydda forskning och kunskap

En vägledning för att motverka företagsspionage vid forskningssamarbeten

Teknikföretagen

SOFF
Säkerhets- och försvarsföretagen

”Internationellt samarbete och forskningsutbyte utgör en viktig grund för Sverige som forskningsnation. Statliga och statsunderstödda aktörer bedriver dock spionage för att komma över information om forskning och innovationer från bl.a. svenska företag och myndigheter.”

Regeringen

”Många företag och lärosäten har sina servrar fulla med forskningsresultat, utvecklingsprojekt och patentansökningar. Dessa representerar enorma värden för den stat som vill gå genvägar i sin egen näringslivs- och teknikutveckling. I praktiken kan det innebära att de företag som utvecklat ny teknik konkurreras ut av sina egna lösningar”

Försvarets radioanstalt

”Främmande makt lägger ner mycket tid [...] för att främja sin egen ekonomiska utveckling och utveckla sin militära förmåga.[...] Det sker genom omfattande [...] stöld av teknologi, forskning och utveckling. Det här måste vi förhålla oss till [...]”

Säkerhetspolisen

Inledning

Denna vägledning vänder sig till aktörer som samarbetar med forskande och utvecklande företag. Primär målgrupp är därför institut, lärosäten och teknikparker. I fokus för vägledningen står företagsspioneri, det vill säga den otillbörliga form av informationsinhämtning som riktas mot näringslivet för att nå konkurrensfördelar.

Enligt uppgift från Säkerhetspolisen har företagsspioneriet i Sverige under de senaste åren nått alarmerande nivåer och tagit sig nya former. Två aspekter är särskilt tydliga. För det första är spionaget i stor utsträckning orkestrerat från statsunderstödda utländska aktörer och för det andra är lärosäten, institut och teknikparker som samarbetar med företag i ökande grad primära måltavlor. Prislappen för de direkta skador företagsspioneriet genererar uppgår årligen till flera miljarder kronor.

Syftet med denna vägledning är att belysa viktiga aspekter som ger bättre möjlighet att integrera en säkerhetsdimension vid forskningssamarbeten. Fokus är på samarbeten i allmänhet och internationella samarbeten i synnerhet. Utgångspunkten är att beaktande av säkerhet ökar möjligheten att arbeta mer effektivt tillsammans och minskar risken för att den framtida konkurrenskraften äventyras. Vägledningen vänder sig primärt till företrädare på institut, lärosäten och teknikparker som ansvarar för, eller bedriver, forskningssamarbeten med näringslivet. Innehållet har dock relevans för alla som arbetar med forskning, utveckling och innovation.

Som underlag har information primärt inhämtats från Säkerhetspolisen, Teknikföretagen, Australian Strategic Policy Institute (ASPI), australiensiska Department of Education, Skills and Employment, brittiska Centre for the Protection of National Infrastructure (CPNI) och Säkerhets- och försvarsföretagen (SOFF).

Vägledningen är framtagen genom ett samarbete mellan arbetsgivarorganisationen Teknikföretagen och branschföreningen Säkerhets- och försvarsföretagen (SOFF). Teknikföretagen organiserar över 4200 tillverkande och industrinära företag som leder teknikutvecklingen. SOFF företräder företag inom säkerhets- och försvarsområdet med verksamhet i Sverige.

Stockholm hösten 2021

Innehåll

1 Hotbilden – varför är svensk forskning och innovation en måltavla för företagsspioneri? 5
2 Checklista 6
2.1 Inför ett samarbete 6
2.1.1 Säkerhetsskyddsanalys – viss verksamhet kan vara säkerhetskänslig 6
2.1.2 Genomför en granskning ("due diligence") 6
2.1.3 Identifiera intressekonflikter 6
2.1.4 Publicera riktlinjer och arbetsrutiner för att undvika otillbörlig påverkan 7
2.1.5 Segmentera åtkomst till data och resultat 7
2.1.6 Skapa möjlighet att automatiskt logga aktiviteter 7
2.2 Under ett samarbete 7
2.2.1 Skydda all digital information 7
2.2.2 Var försiktig med hur du delar 8
2.2.3 Förhindra nätfiskeattacker ("phishing") 8
2.2.4 Etablera ett säkerhetsmedvetande 8
2.2.5 Genomför kommunikationsinsatser och utbildning 8
2.2.6 Följ legala regelverk 9
2.2.7 Genomför personkontroll 9
2.3 Efter ett samarbete 10
2.3.1 Utvärdering – har nya risker uppstått som inte förutsågs? 10
2.4 Anmälan till svenska myndigheter 10

1 Hotbilden – varför är svensk forskning och innovation en måltavla för företagsspioneri?

Varje dag utsätts aktörer i Sverige för påverkan från antagonistiska aktörer. Syftet med påverkansförsöken är ofta att stjäla spetskunskap och ta kontroll över nyckelteknologier. Tillsammans med cyberattacker är dessa aktiviteter delar av den gråzonsproblematik som brukar omnämnas i sammanhang relaterade till försvars- och säkerhetssektorn men som i realiteten omfattar hela samhället. Angrepp sker frekvent mot kunskapsområden och teknik som är strategiskt viktig för konkurrrenskraften och samhällets omställning mot ökad miljömässig, social samt ekonomisk hållbarhet.

Påverkansaktiviteterna sker ofta i det fördolda under falska förespeglingar. Inte sällan är det utländska, statligt styrda aktörer som står bakom operationerna. Enligt uppgifter från Säkerhetspolisen 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.

Sverige rankas i internationella jämförelser som en global innovationsledare. En av Sveriges styrkor är de stora, systematiska och uthålliga investeringar som görs i forskning, utveckling och innovation. En annan framträdande styrka är en öppen och fri innovationskultur med nära samverkan mellan lärosäten, institut och näringsliv. Kunskap om, liksom tillgång till, exempelvis nyckelteknologier representerar enorma värden för den stat som vill ta genvägar i sin egen näringslivs- och teknikutveckling. Detta kan leda till att företag som utvecklat ny teknik i Sverige konkurreras ut av sina egna lösningar, realiserade av företag i de länder som ägnar sig åt företagsspioneri. Att information och hemligheter stjäls kan påverka sysselsättning, tillväxt och välstånd negativt. Då svenska institut, lärosäten och teknikparker är viktiga kunskapsproducenter, partners och motorer i forskning, innovation och teknikutveckling är de också måltavlor för företagsspioneri, särskilt när de samarbetar med företag.

”Statsstyrt företagsspioneri innebär att främmande makt bedriver spionage mot svenska företag med avsikt att få tillgång till företagshemligheter. Till skillnad från traditionellt spionage, som syftar till att underminera ett lands säkerhet, är företagsspioneriets motiv främst att skaffa ekonomisk vinning och inhämta teknisk kunskap.”

Bättre skydd för tekniska företagshemligheter

2 Checklista

För att synliggöra behovet av säkerhetsmedvetande vid forskningssamarbeten återfinns nedan ett antal punkter som en organisation kan vidta **inför**, **under** och **efter** ett samarbete. Nedanstående kompletterar den guide som Teknikföretagen tagit fram för att öka skyddet av digital information och system.

2.1 *Inför* ett samarbete

2.1.1 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. Det är primärt verksamhet som har betydelse för Sveriges säkerhet men inkluderar, utöver försvar och rättsväsende, bland annat forskningsverksamhet på institut, lärosäten eller direkt hos enskilda företag. Det är organisationens eget ansvar att genomföra en säkerhetsskyddsanalys och ställa sig frågan om huruvida verksamheten kan vara säkerhetskänslig. Det underlättar därför om det finns en utpekad säkerhetsansvarig som kan hantera alla frågor som rör säkerhet. Åtgärder och rutiner bör också sättas på pränt i en säkerhetsskyddsplan.

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

Tips i vardagen – säkerhetsskydd

- Utbilda **säkerhetsskyddskoordinatorer** 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 sker krypterat

2.1.2 Genomför en granskning (”due diligence”)

När ett nytt forskningssamarbete ska etableras rekommenderas att en genomlysning genomförs (”due diligence”). Genomlysningen bör fokusera på att belysa etiska, juridiska, ekonomiska och nationella säkerhetsöverväganden – till exempel vilken roll en potentiell samarbetespartner spelar i sina hemländer, om denne har kopplingar till försvarsindustri eller militära intressen. Ett viktigt syfte med genomlysningen är att få förståelse för hur forskningen inom ett samarbete kan utföras i praktiken. Här kan exemeplvis policyinstitutet GPPi, med sina tydliga vägledningar, ge en indikation på potentiella risker. Även befintliga samarbeten bör med viss regelbundenhet genomlysas.

Det är viktigt att vara medveten om att hotbilden ökar om samarbetet berör tekniskt avancerade områden som har stor ekonomisk potential. Exempel på sådana områden är nästa generations informationsteknologi, datorstyrda verkstadsmaskiner och robotteknik.

2.1.3 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.

2.1.4 Publicera riktlinjer och arbetsrutiner för att undvika otillbörlig påverkan

Att ha en tydlig uppsättning principer - en uppförandekod - som beskriver hur arbetet 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 processer för hur otillbörlig påverkan ska hanteras.

2.1.5 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 access. 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.

2.1.6 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 access som faktiskt behövs.

2.2 *Under* ett samarbete

2.2.1 Skydda all digital information

Skydd av data, resultat och information som delas digitalt är centralt i ett samarbete. På den mest grundläggande nivån bör processer och riktlinjer finnas till hand för att beakta följande:

I. Använd företrädelsevis lösningar (t.ex program, appar och nät) från leverantörer med en för ändamålet god säkerhetsnivå

II. Installera de senaste app- och programuppdateringarna

III. Säkra utrustning så som laptops, smartphones och surfplattor med ett skärmlås

IV. Om organisationen har godkänt funktionen kan en lösenordshanterare användas för att skapa och komma ihåg lösenord

V. Säkerhetskopiera alltid viktig data och förvara den på en åtskild plats

VI. Aktivera, om möjligt, tvåfaktorautentisering för all digital åtkomst

2.2.2 Var försiktig med hur du delar

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

- Källan till enheten 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

Det är också viktigt att ha i åtanke att information som lagras på molntjänster kan vara föremål för exportkontroll, se mer under punkten 2.2.6 nedan.

2.2.3 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 punkter:

- Nätfiskare använder ofta information som finns tillgänglig på sociala medier. Granska därför personliga integritetsinställningar och tänk på vad som läggs upp online.
- 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.

2.2.4 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 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 2.2.6 nedan.*

2.2.5 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. Ju högre medvetenheten är, desto mer stärks säkerhetskulturen och motståndet mot fientliga intrång och påverkan.

Det är även av stor vikt att inkludera de delar av verksamheten som har en stöttande funktion, exempelvis en IT-avdelning, i utbildningsmomenten.

2.2.6 Följ legala regelverk

❑ **Exportkontroll**

En viktig 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 exportkontrollerat, bland annat: materialbearbetning; elektronik; datorer; telekommunikation och "informationssäkerhet"; 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 viktigt att veta vad som gäller när det kommer till hur de får fraktas och även lagras. Tänk exempelvis på huruvida er 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.

❑ **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.

2.2.7 Genomför personkontroll

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. Detta innefattar kontroll av visum. 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?

2.3 *Efter* ett samarbete

2.3.1 Utvärdering – har nya risker uppstått som inte förutsågs?

Konkurrens, plagiering och spioneri 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. Utgångspunkt kan 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. En viktig aspekt är också att utvärdera om säkerhetsåtgärder vidtagits för att det inte ska uppstå problem efter ett avslutat samarbete.

2.4 Anmälan till svenska myndigheter

I det fall din organisation bedriver säkerhetskänslig verksamhet och ett intrång har eller misstänks ha skett, ska en anmälan göras till Säkerhetspolisen. Om organisationen eller aktuell verksamhet faller under Försvarsmaktens tillsynsansvar ska anmälan göras där.

Vid misstanke om intrång bör alltid en polisanmälan göras.

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.

Säkerhetspolisen 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 Säkerhetspolisens hemsida.