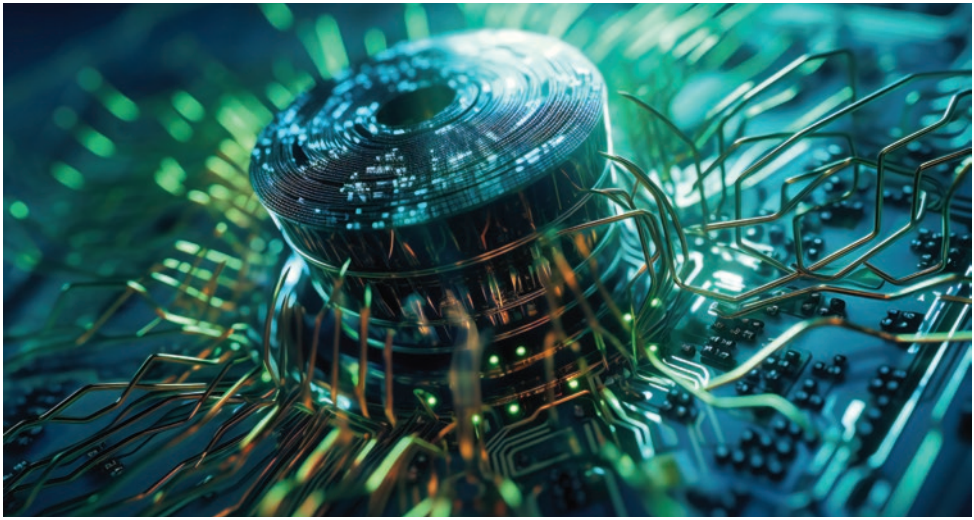


Er jeres forskning i fare?

Gode råd til forskere og medarbejdere
om at forebygge spionage

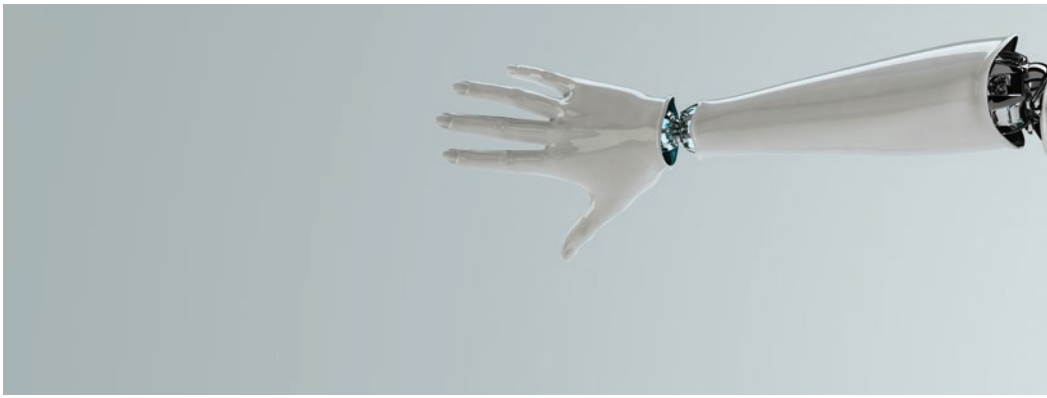
INDHOLD

Introduktion

Danmark er på en række områder førende i verden inden for teknologi, innovation og forskning. Samtidig med at den danske førerposition udgør et væsentligt indtægtsgrundlag for dansk økonomi og ofte bidrager til at løse globale udfordringer, fx i forbindelse med grøn omstilling og sundhed, betyder det også, at danske forskningsinstitutioner og virksomheder er et attraktivt mål for spionage.

Dansk forskning er i skarp international konkurrence, og danske forskningsinstitutioner og virksomheder indgår aktivt i internationalt samarbejde. Det er i langt størstedelen af tilfældene til Danmarks fordel, men PET ser eksempler på, at forskningen uretmæssigt havner i de forkerte hænder. Det kan skade mulighederne for dansk forskning og få både økonomiske og sikkerhedspolitiske konsekvenser for Danmark. Derfor er det vigtigt at opnå den rette balance, hvor danske universiteter og virksomheder arbejder så åbent som muligt – og så sikkert som nødvendigt.

PET har i samarbejde med Uddannelses- og Forskningsstyrelsen og Erhvervsstyrelsen udarbejdet en række anbefalinger til jer, der arbejder på forskningsinstitutioner og i forskningstunge virksomheder, for at forebygge og håndtere spionage. Det er anden gang denne type publikation udkommer – for truslen mod dansk forskning er fortsat markant og kompleks, og de seneste år er flere tiltag sat i søen for at beskytte området.

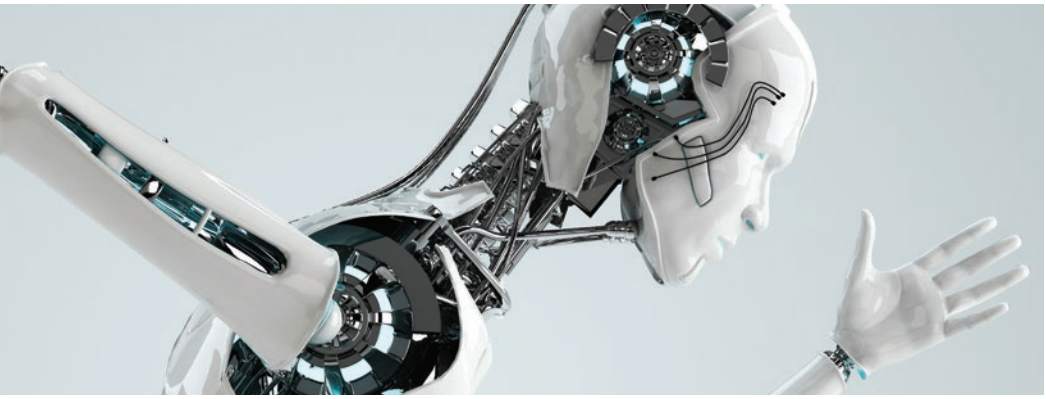


RETNINGSLINJER FOR INTERNATIONALT FORSKNINGS- OG INNOVATIONSSAMARBEJDE

I 2020 nedsatte Uddannelses- og Forskningsministeriet et nyt udvalg kaldet URIS – Udvalg om retningslinjer for internationalt forsknings- og innovationssamarbejde. Udvalget udgav i maj 2022 sin rapport med en række nye retningslinjer, som skal være med til at sikre dansk forskning mod økonomiske, sikkerhedsmæssige og etiske risici i forsknings- og innovationssamarbejde.

URIS anbefaler bl.a., at I identificerer og beskytter jeres kritiske forskning, undersøger jeres internationale samarbejdspartnere og afgrænser, hvilke forskningsområder der samarbejdes på. Disse retningslinjer flugter med rådene i denne publikation. I kan finde URIS' retningslinjer på Uddannelses- og Forskningsministeriets hjemmeside: *https://ufm.dk/publikationer/2022/afrapportering-udvalg-om-retningslinjer-for-internationalt-forsknings-og-innovationssamarbejde.*

Som opfølgning på offentliggørelsen af retningslinjerne har Uddannelses- og Forskningsministeriet etableret et permanent forum for international koordination og samarbejde. Forummet har til formål at understøtte forskningsinstitutionernes og -fondenes implementering af de nye retningslinjer samt understøtte videndeling og en koordineret indsats for at være med til at beskytte dansk forskning mod misbrug og uønsket udenlandsk indblanding.



Dansk forskning er et attraktivt mål

Danmarks teknologiske og forskningsmæssige førerposition gør Danmark til et attraktivt mål for spionage. Fremmede stater forsøger gennem statsfinansieret industrispionage og ulovlig anskaffelsesvirksomhed at få fat i den nyeste viden og teknologi.

PET kan bl.a. konstatere, at fremmede efterretningstjenester løbende forsøger at opbygge kontakter til studerende, forskere og virksomheder, der vil kunne udlevere produkter og konkret viden om den nyeste danske teknologi og forskning.

Udenlandske studerende og forskere i Danmark kan medvirke til at overføre sensitiv viden til fremmede stater. De kan være underlagt stærkt pres fra hjemlandets efterretningstjenester, og det bør være et opmærksomhedspunkt, at enkelte autoritære stater har love, der pålægger deres lands statsborgere at bistå efterretningstjenesterne med oplysninger af interesse for staten.

SPIONAGE er bl.a. når man indhenter eller videregiver information om forhold, som af hensyn til den danske stat eller det danske samfunds interesser skal holdes hemmelige. Det er ligeledes spionage, hvis man røber eller videregiver oplysninger, der kan være til fare for fx den danske stats sikkerhed eller samfundsinteresser eller en enkeltpersons sikkerhed. Det er også spionage, hvis man i øvrigt foretager sig noget, der kan sætte en fremmed stats efterretningstjeneste i stand til at virke inden for den danske stats område.

PÅVIRKNINGSVIRKSOMHED er, når en fremmed stats efterretningstjeneste sættes i stand til at påvirke beslutningstagere eller den almene meningsdannelse inden for den danske stats område. Formålet med påvirkningsvirksomheden kan fx være at påvirke den offentlige debat, internationale samarbejdsrelationer eller omverdenens syn på Danmark for at fremme egne interesser.

ULOVLIG ANSKAFFELSESVIRKSOMHED er aktiviteter, hvor fremmede stater ulovligt omgår eksportkontrol for at skaffe sig adgang til produkter, teknologi og viden, som staterne kan anvende til at opbygge militære kapaciteter.

Det kan bl.a. ske, ved at danske virksomheder eller universiteter eksporterer produkter eller overfører viden, der via mellemmænd ender i de forkerte hænder.

De fremmede stater vil ofte benytte sig af komplicerede netværk med mange aktører på tværs af landegrænser i et forsøg på at skjule produkternes endelige slutbrug og derved omgå eksportkontrol.

PROBLEMATISKE AKTIVITETER I GRÅZONEN – Spionage, påvirkningsvirksomhed og ulovlig anskaffelsesvirksomhed er strafbare handlinger, defineret i straffelovens kapitel 12, §§ 107-109, samt i kapitel 12, §110 c, og kapitel 13, §114 h. Der er dog også en række hemmelige og problematiske aktiviteter, som udføres af, eller på vegne af, en fremmed stat, men som ikke nødvendigvis falder ind under de førnævnte paragraffer.

Fx kan det være problematisk, hvis kritisk dansk infrastruktur ejes af virksomheder fra en stat, som Danmark er i et modsætningsforhold til. Eller hvis udenlandske ph.d.-studerende tager viden, som kan benyttes til uetiske forhold, med sig tilbage til hjemlandet.

Det er vigtigt at holde sig for øje, at visse stater, herunder Kina, benytter sig af en tilgang, der aktiverer alle dele af samfundet. Dvs. en tilgang, hvor man ikke begrænser sig til at benytte sig af statslige organer, men også kan aktivere private virksomheder, akademiske kredse, mediehuse, frivillige organisationer m.fl. til at nå et fælles mål – et mål som fx kan være at opnå en teknologisk førerposition inden for et prioriteret område.

Udsatte forskningsområder

PET kan konstatere, at fremmede staters efterretningsvirksomhed kontinuerligt har fokus på de højteknologiske og forsvarspolitiske områder. Det gælder særligt energiteknologi, bioteknologi, kvanteteknologi, rumteknologi, robotteknologi, forsvarsindustrielle produkter og produkter omfattet af eksportkontrol. I takt med den globale udvikling sker der dog en konstant udvikling i, hvilke forskningsområder der er særligt udsatte, og en række forskningsområder og produkter kan benyttes både civilt og militært, såkaldt dual-use, hvilket er med til at gøre problemstillingen mere kompleks.

Spionagen mod dansk forskning kan både være kommercielt og politisk motiveret. Stater kan søge at opnå konkurrencemæssig og kommerciel fordel ved at kende til forskernes arbejde og danske forskningsresultater, før de offentliggøres. På områder, der har særligt politisk fokus, kan fremmede stater få indsigt i den forskning og rådgivning, som regeringen og Folketinget baserer vigtige beslutninger på.

Alle forskningsinstitutioner og forskningstunge virksomheder kan potentielt set blive udset som mål for fremmede efterretningstjenester.

SPIONAGE MOD GRØN TEKNOLOGI

I sommeren 2020 blev en russisk statsborger, der havde boet i Danmark i tolv år, anholdt. Året efter idømte retten i Aalborg ham tre års fængsel for spionage samt udvisning af Danmark. Den dømte var tiltalt for spionage mod DTU, hvor han havde taget sin ph.d., samt en nordjysk virksomhed, som arbejder med grøn teknologi.

Den dømte havde i en årrække udleveret oplysninger mod betaling til en russisk efterretningstjeneste. Dommen blev stadfæstet i Vestre Landsret i november 2021, som udviste tiltalte for bestandig og konfiskerede hans udbytte.

EKSPORTKONTROL & INVESTERINGSSCREENING

Eksportkontrol og investeringsscreening har bl.a. til formål at beskytte dansk forskning og udvikling.

EKSPORTKONTROL

Eksportkontrol skal sikre, at produkter, der potentielt set kan være farlige, ikke falder i de forkerte hænder. Der kan være flere grunde til, at et bestemt produkt er i søgelyset og derfor kræver en eksporttilladelse.

Et produkt kan være en konkret vare, teknologi eller viden. Det kan også dreje sig om en serviceydelse, fx teknisk bistand eller rådgivning. Produktets funktion og anvendelsesmuligheder kan være afgørende for, om I skal søge om eksporttilladelse. Grundforskning, der ikke sigter mod anvendelse, og teknologi, der allerede er i det offentlige rum, er ikke omfattet af eksportkontrol.

Dansk eksportkontrol baserer sig på internationale regler og kontrollister over materialer og teknologier, der kan misbruges, fx til udvikling af masseødelæggelsesvåben, krænkelse af menneskerettigheder eller overvågningsformål. Det er vigtigt at kende gældende love og regler for eksport, hvis jeres forskningsinstitution eller virksomhed arbejder med produkter inden for fx kommunikation, overvågning, software, rumfart, medico, bioteknologi eller kemi.

Nogle produkter kan både bruges til civile og militære formål (såkaldt dual-use). Det kan fx være sensorer og lasere eller programmer og software. Hvis produktet står på EU's kontrolliste over kritiske produkter, vil det kræve en tilladelse at eksportere ud af EU. Inden for EU's grænser er der mere lempelige regler – her kræver kun de farligste produkter en eksporttilladelse.

Produkter, som ikke står på EU's kontrolliste, kan også være omfattet af reglerne, hvis de falder ind under de såkaldte catch-all-bestemmelser, der er et ekstra sikkerhedsnet i eksportkontrollen. Det er fx vigtigt, hvem I eksporterer til, og i hvilket land jeres køber befinder sig. Det er forskningsinstitutionernes ansvar at overholde eksportkontrolreglerne,

herunder evt. at søge om eksporttilladelse, men Erhvervsstyrelsen hjælper med vejledning og kundecheck.

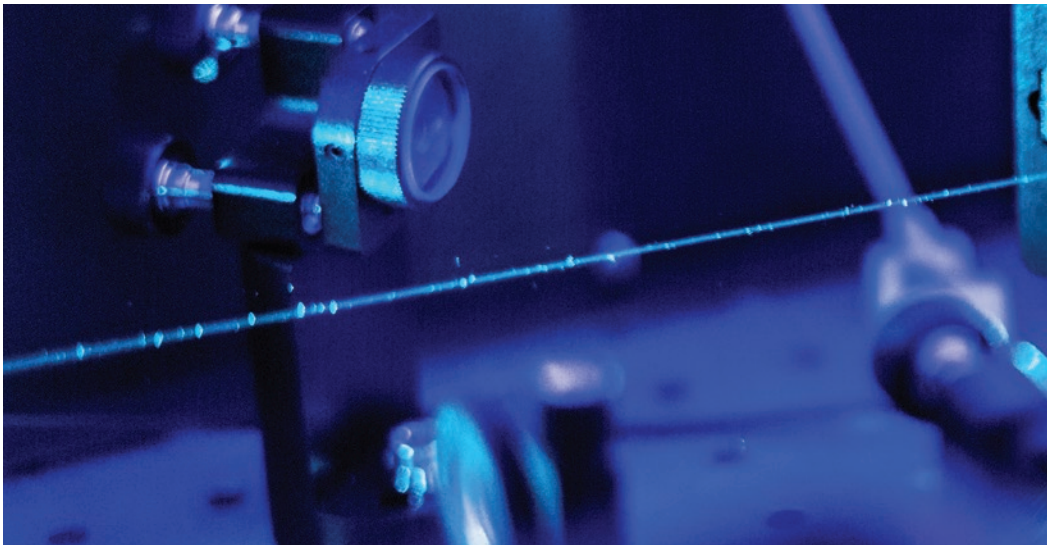
INVESTERINGSSCREENING

Hvor eksportkontrol har til formål at beskytte dansk forskning og udvikling i forbindelse med udførsel af produkter, så retter investeringsscreening sig mod situationer, hvor en udenlandsk part investerer i Danmark. Forsknings- og udviklingsaktiviteter kan være omfattet af investeringsscreeningslovgivningen, hvis aktiviteterne finder sted inden for særligt følsomme sektorer og dermed kan true dansk sikkerhed.

FÅ FLERE INFORMATIONER

Bliv klogere på eksportkontrol, se EU's kontrolliste over kritiske produkter, læs mere om catch-all-bestemmelserne m.v.: *www.eksportkontrol.dk.*

Læs mere om investeringsscreening: *https://erhvervsstyrelsen.dk/screening-af-udenlandske-investeringer.*



Store konsekvenser

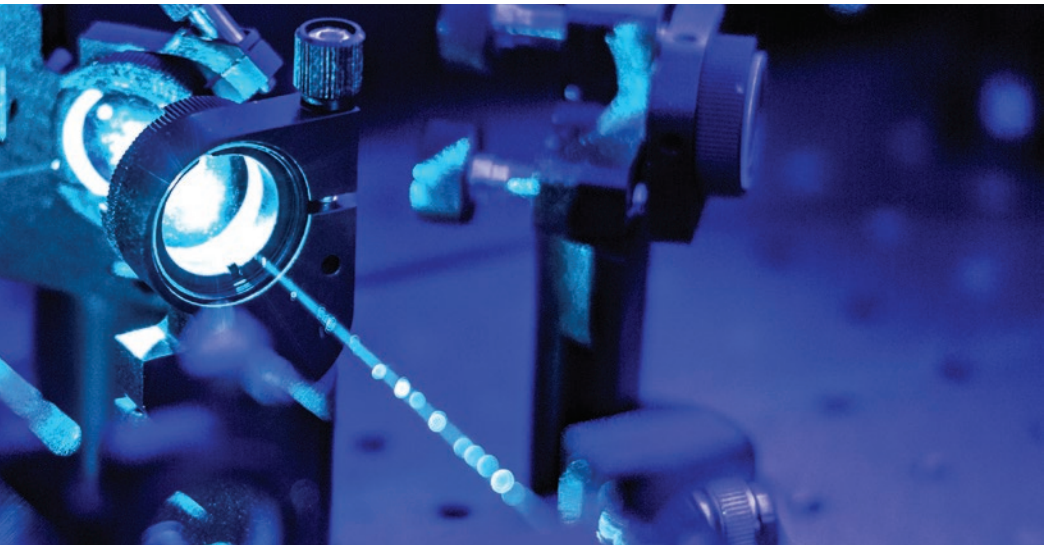
– for den enkelte og for Danmark

Det kan få store konsekvenser for Danmark, hvis andre stater får uønsket adgang til jeres forskning. Det kan også skade danske forskningsinstitutioner og virksomheders ry og skabe problemer med fremtidig finansiering, rekruttering og mulighed for samarbejde.

Spionage skaber risiko for tab af:

• Tillid og omdømme

Tilliden til jeres forskningsinstitution, virksomhed eller egen person risikerer at forsvinde, og jeres omdømme kan lide skade, hvis de beskyttelsesværdige data og produkter, I har adgang til, bliver misbrugt, stjålet eller på anden vis ender i de forkerte hænder.



• Muligheder
Muligheden for at blive krediteret for jeres arbejde, at offentliggøre forskning eller tage patent begrænses, hvis der er sket tab af forskningsresultater el.lign.

• Frihed
Økonomisk afhængighed skaber risiko for økonomisk pression. Direkte eller indirekte trusler om at trække finansieringen til et projekt kan lægge pres på for at lempe på etiske standarder eller for at gå på kompromis med den akademiske frihed, formidlings- og ytringsfriheden.

• Finansiering
Fremtidig finansiering besværliggøres, hvis det rygtes, at jeres forskning, teknologi eller produkter utilsigtet er endt hos en fremmed stat. I kan ligeledes lide økonomisk tab, hvis nogen får adgang til data eller informationer, der ejes af jeres finansieringskilder.

Hvor udsatte er I?

Du bør, sammen med din forskningsinstitution eller virksomhed, overveje, hvor udsatte I er over for spionage og ulovlig anskaffelsesvirksomhed. Den enkelte organisation bør, bl.a. ud fra URIS-retningslinjerne (se s. 4) vurdere både sårbarhed og risiko. Men jer, der arbejder på forskningsinstitutionen eller i virksomheden, har også en afgørende rolle i forhold til at vurdere den potentielle interesse og de bredere anvendelsesmuligheder af jeres viden, teknologier eller produkter.

Forskningsprojekter kan være udsatte, hvis:

- Det er sandsynligt, at forskningen fører til et fremtidigt kommercielt eller patenterbart resultat.
- Der anvendes følsomme data eller personligt identificerbare oplysninger som fx genetiske oplysninger eller kommercielle testdata.
- De kan anvendes af udenlandsk militær eller både kan have militære- og civile anvendelsesmuligheder (dual-use).
- De potentielt danner grundlag for internationale strategiske politiske forhandlinger eller beslutninger.
- Der benyttes sensitivt laboratorieudstyr.

Produkter og teknologier kan være udsatte, hvis:

- De er underlagt eksportkontrol.
- De kan anvendes af udenlandsk militær eller både kan have militære- og civile anvendelsesmuligheder (dual-use).
- Der er tale om banebrydende eller avanceret teknologi. Jo færre, der kan matche produktets egenskaber, desto større er risikoen.

DEN ”BRASILIANSKE” FORSKER

I oktober 2022 anholdt norsk politi en forsker med brasiliansk statsborgerskab på Tromsø Universitet, hvor han siden 2021 havde forsket i Norges nordlige region og hybride trusler.

Ifølge norsk politi opererede forskeren under falsk identitet og var i virkeligheden russisk statsborger på opgave for en russisk efterretningstjeneste. I dag sidder forskeren varetægtsfængslet, mens den norske sikkerhedstjeneste, PST, er ved at undersøge, hvorvidt forskeren har opbygget et netværk af personer med adgang til oplysninger, som han kan have videregivet til en russisk efterretningstjeneste.

Spionagemetoder

– sådan gør fremmede stater

Fremmede stater gør brug af mange forskellige metoder til at indhente oplysninger og produkter. Metoder, der strækker sig i et kontinuum mellem lovligt og ulovligt med en del, der ligger i en problematisk gråzone. Typisk benyttes metoderne i et komplekst samspil.

Traditionelt akademisk engagement er en af mange måder, en udenlandsk efterretningstjeneste kan benytte til at få adgang til jer. Det kan fx foregå ved at udvise interesse for jeres forskning på konferencer eller sociale medier som fx LinkedIn.

Internationalt samarbejde giver statslige aktører en legitim adgang til at indhente forskning uden at benytte sig af traditionel spionage eller cyberangreb. Samarbejdet kan dog risikere at give uønsket adgang til mennesker, IT-netværk og indsigt i forskning, der kan være beskyttelsesværdig.

Handel, investeringer og leverandøraftaler kan ligeledes være en metode til at anskaffe sig den ønskede viden, teknologier eller produkter. Foregår handlen via dækfirmaer for at omgå sanktioner og eksportkontrol, er der tale om ulovlig anskaffelsesvirksomhed. Se s. 8 om eksportkontrol.

METODER – SOM TYPISK KOMBINERES

Nogle metoder til indhentning af viden, teknologier og produkter er ulovlige, mens andre metoder ligger i gråzoner eller ligefrem er lovlige. De kan dog stadig have et problematisk potentiale, som man bør være opmærksom på.

ØKONOMISKE METODER

- Legater og tilskud, som kan indeholde problematiske krav eller medføre selvcensur
- Tilbageholdelse af midler eller trussel herom
- Investering i projekt med dertilhørende adgang til viden m.v.
- Opkøb af produkter med sløring af, hvem der egentlig er køber
- Bestikkelse

MENNESKERETTEDE METODER

- Rekruttering af studerende og undervisere til udlandet for derigennem at indhente viden.
- Hvervning af studerende og undervisere, fx til spionage.
- Elicitering, dvs. at lokke informationer ud af en person gennem psykologisk manipulering. Oftest vil målpersonen være uvidende om, at elicitering har fundet sted.
- Placering af efterretningsofficer, der arbejder under dække af at være fx forsker, studerende eller investor.
- Afpresning, trusler og tvang.

DIGITALE METODER

- Informationssøgning på åbne medier, som fx kan danne grundlag for elicitering
- Påvirkningskampagner for at skabe en holdningsændring, fx over for en fremmed stat
- Cyberangreb

FYSISKE METODER

- Overvågning
- Tyveri og indbrud

10 gode råd

1. Vær bevidst om truslen
En forudsætning for at beskytte jeres forskning er, at I er bevidste om spionagetruslen og -metoderne. I kan dermed holde trusselsbilledet op imod de værdier, fx data og teknologier, som I vurderer, I bør beskytte – se næste punkt. På den baggrund kan I sikre, at jeres sikkerhedsprocedurer og -tiltag er på det ønskede niveau. Det er desuden vigtigt at udbrede kendskabet til spionagetruslen, så der er konsensus om at gøre en fælles indsats. Orienter jer gerne i de trusselsvurderinger, som PET løbende udgiver.

2. Vurder værdien
Det er jer, der fx er tilknyttet en forskningsinstitution eller en højteknologisk virksomhed, der er de bedste til at vurdere værdien og anvendelsesmulighederne af et forskningsprojekt, en teknologi eller et produkt. Overvej om forskningsresultater, nye teknologier m.v. er kommercielt interessante, er relateret til sikkerheds- og forsvarsteknologier, har både civile og militære anvendelsesmuligheder m.m. Helt enkelt kan man sige, at I skal overveje, hvilke informationer og data I ikke har "råd" til at miste. Ud fra jeres vurdering af værdi kan I også beslutte, hvem der skal have adgang til hvad, både fysisk og elektronisk. Se afsnittene "Udsatte forskningsområder" og "Hvor udsatte er I?", s. 7 og 12.

3. Kend lovgivningen
En lang række varer og teknologier er kategoriseret kritiske af EU og er derfor underlagt eksportkontrol. Det er vigtigt at holde sig for øje, at lovgivningen både gælder fysiske produkter og videnoverførsel. Hertil kommer, at der er fastsat lovgivning angående direkte investeringer for at forhindre, at udenlandske investeringer kan udgøre en trussel mod Danmarks sikkerhed.
Se s. 8.

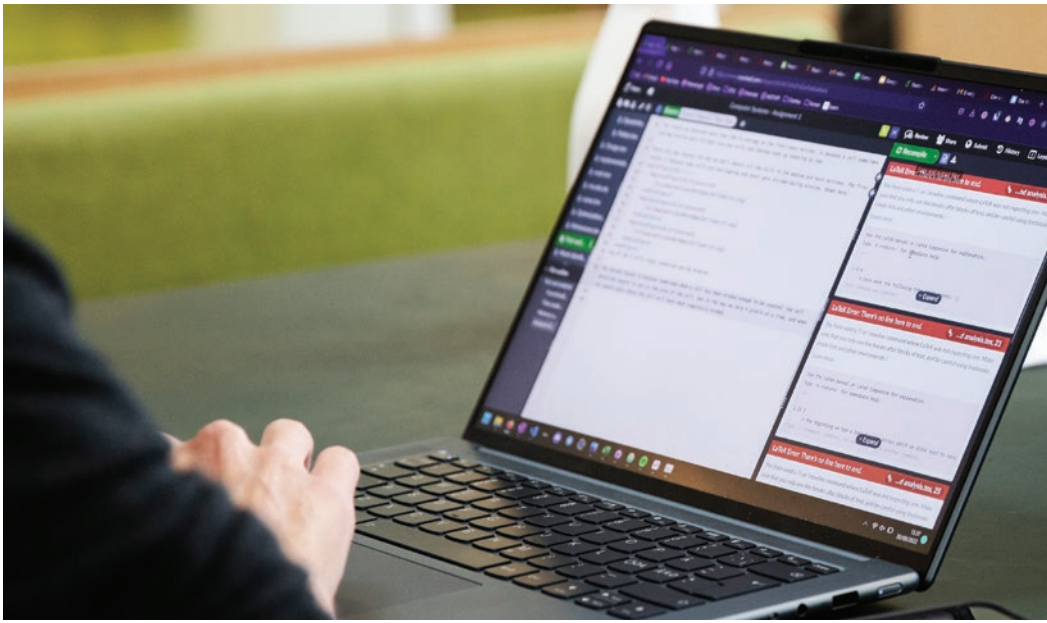
4. Kend jeres samarbejdspartnere
Foretag et grundigt baggrundstjek af jeres internationale samarbejdspartnere. Virker forskningsinstitutionen eller virksomheden legitim? Er den finansie-

ret af, eller har samarbejde med, landets militære institutioner? Har samarbejdspartneren et værdisæt, som harmonerer med jeres organisation? Overvej altid værdien af et samarbejde op imod potentielle risici, og afgræns, hvad I ønsker at dele med samarbejdspartneren. Udform en samarbejdsaftale, så der er klare retningslinjer for samarbejdet.

5. Pas godt på medarbejdere og kolleger

Når I ansætter nye medarbejdere, er det en god ide med et grundigt baggrundstjek for at se, om CV'et virker legitimt. Tjek bl.a. referencer og vurder, om de angivne publikationer er reelle. Se også, om der skulle være noget bekymrende i forhold til jeres organisations værdier og interesser.

I hverdagen er medarbejdertrivsel vigtig – også ud fra et sikkerhedsperspektiv. Arbejdspres og mistrivsel kan føre til fejl, som kan åbne for sikkerhedsmæssige sårbarheder. I værste fald kan mistrivsel medvirke til, at en ellers loyal medarbejder eller kollega kan ende som kilde for en konkurrent eller en



fremmed efterretningstjeneste. Vær også opmærksom, hvis en udenlandsk medarbejder eller kollega kan være underlagt et pres fra hjemlandets efterretningstjeneste.

Overvej, hvilken adgang den enkelte skal have til jeres beskyttelsesværdige viden, teknologi og produkter – også i tiden op til og efter kontraktudløb. Se gerne PET's publikation "Pas godt på dine medarbejdere".

6. Hav fokus på IT-sikkerheden

Når det kommer til IT-sikkerhed, er der dels den tekniske, dels den menneskelige side af sagen. Teknisk set er der forskellige procedurer og tiltag, der kan forbedre sikkerhedsniveauet, inkl. en installering af en effektiv sikkerhedspakke med bl.a. antivirusprogram og spamfilter samt adgang via en VPN-forbindelse. Alt IT-udstyr bør opdateres jævnligt, så det har de nyeste sikkerhedsopdateringer.

Hertil kommer den menneskelige adfærd. Du er bedre beskyttet, hvis:

- Du opdeler dit arbejdsliv og privatliv, så du ikke bruger din private e-mailadresse og mobiltelefon i arbejdsregi. For alt udstyr gælder det, at du bør lå-

se skærmen, når du forlader den, så et øjebliks uopmærksomhed ikke kan betyde, at uvedkommende får adgang.

- Du tjekker dine privatlivsindstillinger på de sociale medier og overvejer, hvilke personlige informationer du lægger ud. Oplysninger fra sociale medier vil bl.a. kunne blive brugt imod dig eller dine kolleger til spear-phishing.
- Du aldrig klikker på vedhæftede dokumenter eller links, som du ikke er sikker på kommer fra en troværdig kilde.
- Du ikke benytter brugte USB-stik, medmindre du stoler på personen eller firmaet, de kommer fra. USB-stik kan indeholde malware, så det bliver muligt at tilgå din computer.

For yderligere råd om IT-sikkerhed kan du med fordel besøge *www.cfcs.dk* og *www.sikkerdigital.dk*.

7. Hav fokus på den fysiske sikkerhed

I kan arbejde med den fysiske sikring for at reducere risikoen for tyveri af viden, teknologi og produkter. Mange tiltag skal realiseres centralt. Det gælder fx valg af adgangskontrol, alarmer og overvågning.

Men den enkelte kan også gøre en forskel:

- Har I adgangskoder, så beskyt dem, så uvedkommende ikke kan aflæse dem.
- Bær dit ID-kort synligt, når du er på arbejde. Det reducerer bl.a. muligheden for "tail-gating" – at en person uden ID-kort hægter sig på en, der har det, og på den måde skaffer sig uautoriseret adgang. Gem dit ID-kort væk, når det ikke er relevant længere, fx til og fra din arbejdsplads.
- Begræns mulighederne for indkig udefra. Indret din arbejdsplads så skærme, tavler mv. vender væk fra fx vinduer. Alternativt kan du bruge gardiner og persienner efter behov.
- Vær opmærksom på det fysiske miljø – er der fx tegn på, at der har været forsøg på indbrud.
- Vær opmærksom på kompromittering af fysiske sikringsforanstaltninger som fx kiler i sikringsdøre.
- Etabler og overhold en procedure for sikker opbevaring. Har du et skab med kode, bør du sikre, at den ikke kan blive aflæst.
- Etabler og overhold en lukkeprocedure, så fx vinduer, døre og skabe lukkes, når lokalet forlades.
- Etabler og overhold en politik for sik-

ker bortskaffelse af dokumenter og lignende. Brug fx en makulator.

8. Sæt rammer for besøg

Der kan opstå forskellige problematiske situationer i forbindelse med besøg fra udlandet. Inden besøget kan I vurdere, hvilke informationer I gerne vil dele med jeres gæster, og særligt hvad I ikke ønsker at dele. Vær opmærksom på, hvis der foretages ændringer i deltagerlisten i sidste øjeblik. Gå lokalerne igennem inden besøget, så der ikke ligger beskyttelsesværdige informationer fremme, der hvor de besøgende får adgang.

Under besøget kan I være opmærksom på, om gæsternes adfærd afviger fra normalbilledet. Fotograferer og filmer de atypisk meget? Er der deltagere, der ikke holder sig til gruppen, men forsvinder og dukker op uventede steder? Bliver der stillet spørgsmål, som falder uden for besøgets formål? Tillad ikke, at fremmed software og hardware bliver installeret – heller ikke i forbindelse med præsentationer. Det er bedre, hvis de besøgende kobler deres egen computer til en projektor frem for at benytte et USB-stik i jeres computer. For at undgå kritiske situationer bør I bl.a. sørge for et tilstrækkeligt antal medarbejdere, der kan ledsage gæsterne og holde opsyn.

I er meget velkomne til at orientere PET på forhånd, hvis I får besøg, der har national sikkerhedsinteresse ud fra delegationens sammensætning og besøgets formål.

9. Vær forsigtig på rejser

Det er værd at være sikkerhedsmæssigt godt klædt på til rejseaktivitet, konferencer og udlandsophold. For i udlandet er I generelt mere udsatte for tyveri, cybertrusler m.m. Derfor bør I inden afrejse vurdere, hvor mange beskyttelsesværdige informationer, I har behov for at medbringe – og naturligvis have en backup. Det kan også være en god ide at udfærdige en liste over, hvilke dokumenter og data I medbringer. På den måde kan I have et overblik over, hvilken information der kan være blevet tilgået af uvedkommende.

Vær opmærksom, hvis I "tilfældigt" støder ind i mennesker, som udviser ekstra interesse for jeres arbejde eller for jer

som privatpersoner. Det kan være en måde, en fremmed efterretningstjeneste forsøger at indhente oplysninger på. Bor I på hotel, skal I være opmærksomme på, at personale m.fl. med al sandsynlighed godt kan tilgå værdiboksen.

Wi-fi i udlandet kan være overvåget, så I bør ikke tilgå beskyttelsesværdigt materiale via denne forbindelse. Brug derfor en VPN-tjeneste eller mobildata. Hav jeres udstyr under opsyn, lån det ikke ud, og benyt ikke fremmed udstyr.

Slå også gerne Bluetooth fra på alle jeres enheder. På konferencer er det meget normalt at få udleveret USB-stik. Vær opmærksom på, at de kan indeholde malware – se råd om IT-sikkerhed s. 18.

Det optimale er at medbringe låneudstyr på rejsen. Alternativt kan det være en ide at slette så meget som praktisk muligt, fx opkaldshistorik, beskeder etc. fra eget udstyr. Når du er hjemme igen, kan du vælge at udskifte dine kodeord til de tjenester, som du har brugt under rejsen.

10. Sig noget, hvis I ser noget
– har I en bekymring, eller er skaden sket?

Det er vigtigt at have en god sikkerhedskultur i hverdagen, hvor det er muligt at drøfte bekymringer af sikkerhedsmæssig karakter. Det kan fx dreje sig om mistænkelig opførsel hos en samarbejdspartner eller en besøgende.

Alt efter jeres institutions organisering kan I melde jeres bekymring eller mistanke til nærmeste chef, til ledelsen, den sikkerhedsansvarlige eller den relevante myndighed. PET kan levere konkret rådgivning i forhold til implementering af eventuelle forebyggende og sikkerhedsmæssige foranstaltninger eller procedurer – skriv til *civ@pet.dk.* Hvis I har en bekymring eller en observation, som I gerne vil dele, kan I gøre det via kontaktformularen på *www.pet.dk.*

Er hændelsen cyberrelateret, bør I kontakte Center for Cybersikkerhed, CFCS, samt PET.

Se "Kontakt" s. 23.

Kontakt

POLITIETS EFTERRETNINGSTJENESTE
Klausdalsbrovej 1
2860 Søborg
Tlf. 45 15 90 07
E-mail: *pet@politi.dk*
www.pet.dk

CENTER FOR CYBERSIKKERHED
FORSVARETS EFTERRETNINGSTJENESTE
Postadresse: Kastellet 30
Besøgsadresse: Holsteinsgade 63
2100 København Ø
Tlf. 33 32 55 80
E-mail: *cfcs@cfcs.dk*
www.cfcs.dk

UDDANNELSES- OG FORSKNINGSSTYRELSEN
Haraldsgade 53
2100 København Ø
Tlf. 72 31 78 00
E-mail: *ufs@ufm.dk*
www.ufm.dk

ERHVERVSSTYRELSEN
Langelinie Allé 17
2100 København Ø
Tlf. 35 29 10 00
E-mail: *erst@erst.dk*
www.erst.dk

Udgivet: Marts 2024
Grafisk design: Permild & Ko
Fotos:
Side 2, 17, 18-19, 20: Ditte Valente
Side 1, 4-5, 9, 10-11, 13: Adobe Stock

ERHVERVSSTYRELSEN

PET

Uddannelses- og Forskningsstyrelsen