Modus

Hvordan opererer fremmede stater og deres efterretningstjenester?

INTRODUKTION

Her kan du læse mere om, hvordan fremmede stater og deres efterretningstjenester opererer, når de eksempelvis spionerer eller benytter mere offensive hybride virkemidler som bl.a. sabotage, påvirkning, chikane og likvideringer.

Visse fremmede stater er desuden involveret i forsøg på ulovligt eller på uønsket vis at anskaffe produkter, viden og teknologi.

De fremmede stater og deres efterretningstjenester benytter ofte flere forskellige metoder i kombination til at opnå deres mål.

- ELICITERING OG HVERVNING
- BRUG AF ÅBNE MEDIER
- AFLYTNING AF TELE- OG DATATRAFIK
- CYBERSPIONAGE
- FYSISK SKADEVOLDENDE AKTIVITETER
- PÅVIRKNINGSVIRKSOMHED
- ULOVLIG ANSKAFFELSESVIRKSOMHED
- ULOVLIG OG UØNSKET OVERFØRSEL AF TEKNOLOGI

Modus

Hvordan opererer fremmede stater og deres efterretningstjenester?

INDHOLD

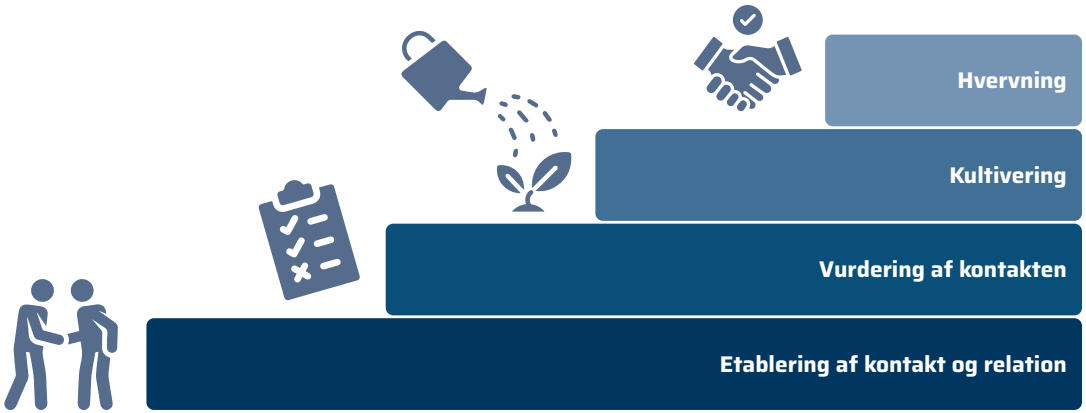
ELICITERING OG HVERVNING AF MENNESKELIGE KILDER – HUMINT

Fremmede efterretningstjenester tillægger fortsat stor værdi til den klassiske spionagedisciplin med at skaffe efterretninger via menneskelige kontakter og kilder, også kaldet HUMINT (Human Intelligence). En god fortrolig kontakt eller kilde kan bidrage med en bedre helhedsforståelse ved bl.a. at sætte oplysninger ind i en kontekst og rapportere om adfærd, interne dynamikker og magtrelationer fx i en organisation eller et netværk.

Det at hverve en menneskelig kilde er en tidskrævende og risikabel proces. Det er langt fra alle personer, som fremmede efterretningstjenester etablerer kontakt til, der ender med at blive hvervede kilder og fx modtager betaling for de informationer, som de videregiver. Men efterretningstjenesterne kan i mange tilfælde også nøjes med mindre. PET vurderer, at truslen fra såkaldt elicitering er omfangsrig, og de fremmede efterretningstjenester lykkes i mange tilfælde ad den vej med at få adgang til værdifulde informationer, som de kan bruge i deres operative aktiviteter.

Elicitering er, når man gennem almindelig samtale diskret forsøger at skaffe informationer, uden at samtalepartneren bemærker det. Efterretningsofficerer, der er specialiseret inden for HUMINT-disciplinen, er trænede i at elicitere og udnytte psykologiske mekanismer i samspillet med andre mennesker.

Forløbet frem til at hverve en person som kilde følger som regel en række trin i det, der kaldes hvervningstrappen. På ***første trin*** etableres kontakt til en person af interesse for efterretningsofficeren. Her handler det typisk om at etablere en indledende relation, hvor efterretningsofficeren som regel kun stiller ufarlige og konverserende



Modus

Hvordan opererer fremmede stater og deres efterretningstjenester?

ELICITERING OG HVERVNING AF MENNESKELIGE KILDER – HUMINT

spørgsmål. Her får efterretningsofficeren bl.a. mulighed for at vurdere, om der er grundlag for at fortsætte kontakten. De indledende kontakter vil ofte, men ikke altid, finde sted ved større arrangementer, hvor der er andre mennesker, f.eks. ved en konference eller en reception, men den første kontakt kan også finde sted online.

RUSSISK STATSBORGER DØMT FOR SPIONAGE

Den 17. november 2021 blev en russisk statsborger idømt tre års fængsel ved Vestre Landsret for spionage (straffelovens § 108, stk. 1) og udvist med indrejseforbud for bestandigt. Personen havde spioneret mod Danmarks Tekniske Universitet (DTU) og en dansk energivirksomhed i Aalborg. Den russiske statsborger havde i flere år udleveret oplysninger mod betaling til en russisk efterretningstjeneste, som han jævnligt holdt møder med.

Hvis efterretningsofficeren vurderer, at den pågældende person måske har potentiale til at blive hvervet som kilde, vil efterretningsofficeren på det ***andet trin*** indlede en nærmere vurdering af personen og bl.a. forsøge at blive klogere på, om den pågældende har adgang til oplysninger eller personer af interesse for efterretningsofficeren. Her vil kontakterne også begynde at foregå mere skjult, og møder vil ikke længere blive aftalt over telefonen eller foregå ved officielle begivenheder. Efterretningsofficeren vil som regel i stedet foreslå at mødes på mere diskrete steder eller måske invitere kontakten til en konference i efterretningsofficerens hjemland eller i venligtsindede lande tæt på for at mindske risikoen for at blive opdaget.

Det ***tredje trin*** er kultiveringsfasen, hvor efterretningsofficeren forsøger at indlede en form for venskabelig relation til den pågældende person. Personen vil blive udsat for en charmeoffensiv og få uskyldige opgaver for at teste relationen. Det kan eksempelvis være, at personen bliver bedt om at overdrage dokumenter eller vurderinger,

LOKALANSAT VED DEN BRITISKE AMBASSADE I BERLIN DØMT FOR SPIONAGE

En lokalansat sikkerhedsvagt ved den britiske ambassade i Berlin blev i februar 2023 ved en domstol i London idømt 13 års fængsel for spionage til fordel for Rusland. Den dømte britiske statsborger erkendte under retssagen, at han over en længere periode leverede klassificerede oplysninger mod kontantbetaling til en russisk efterretningsofficer ved den russiske ambassade i Berlin. Oplysningerne omhandlede britiske embedsfolk, herunder deres identiteter, adresser, telefonnumre og mødeaktiviteter. Sikkerhedsvagten videregav også oplysninger om ambassaden i Berlin og dens ansatte, heriblandt fotos og beskrivelser af ambassadens personale samt af videoovervågnings- og kommunikationssystemer. Under retssagen fremgik det, at den dømte udover et økonomisk motiv også var drevet af utilfredshed med sin arbejdsgiver og pro-russiske synspunkter.

Modus

Hvordan opererer fremmede stater og deres efterretningstjenester?

INDHOLD

ELICITERING OG HVERVNING AF MENNESKELIGE KILDER – HUMINT

som ikke er klassificerede. I denne fase – der kan strække sig over flere år – vil personen også blive vænnet til at modtage gaver og andre ting, der bl.a. skal svække personens dømmekraft. Herefter vil personen blive betragtet som den form for kilde, der i efterretningssammenhæng kaldes for en fortrolig kontakt. En fortrolig kontakt er ikke altid selv klar over, at vedkommende taler med en fremmed efterretningstjeneste. Hvis efterretningsofficeren vurderer, at en egentlig hvervning af personen ikke er nødvendig for at få personen til at levere brugbare oplysninger, eller at et hvervningsforsøg vil være for risikabelt, vil relationen mellem efterretningsofficeren og personen nogle gange forblive på dette stadie.

På trappens ***sidste trin*** pågår den egentlige hvervning som kilde. Her vil efterretningsofficeren bede den potentielle kilde om at udlevere fortrolig information. Hvervningsfasen er det sværeste øjeblik i processen, men hvis efterretningsofficeren har succes, er personen blevet kilde for et andet lands efterretningstjeneste.

PRIMÆRE MOTIVATIONSFAKTORER FOR AT LADE SIG HVERVE

Penge – En klassisk motivationsfaktor er betaling eller tilsvarende modydelser for at udøve spionage for en fremmed efterretningstjeneste. Der indgår et element af finansiel motivation i de fleste sager, hvor en person er blevet hvervet af en fremmed efterretningstjeneste.

Ideologi – Sympati over for den politik eller ideologi, som den fremmede stat repræsenterer, kan også være en faktor, der motiverer en person til at udøve spionage.

Tvang – En fremmed efterretningstjeneste kan true med at dele eller offentliggøre uønskede eller problematiske detaljer om en persons privatliv, eksempelvis over for den nære familie eller en arbejdsgiver, for at presse vedkommende til at udføre spionage.

Ego – En person, der ikke føler sig værdsat og anerkendt på sit arbejde, kan motiveres til at udføre spionage for en fremmed efterretningstjeneste. Det kan eksempelvis være ved, at den fremmede efterretningstjeneste i modsætning til arbejdspladsen opfylder personens behov for at blive set som vigtig og talentfuld. Personer, der føler sig overset og ikke-værdsat, kan være i besiddelse af en hævnfølelse over for deres arbejdsgiver, som den fremmede efterretningstjeneste ligeledes kan udnytte til at rekruttere vedkommende.

Modus

Hvordan opererer fremmede stater og deres efterretningstjenester?

INDHOLD

BRUG AF ÅBNE MEDIER – OSINT

Fremmede efterretningstjenester gør i høj grad brug af forskellige åbne medier til at danne sig et førstehåndsindtryk af deres mål og identificere mulige sårbarheder.

Denne efterretningsmetode bliver kaldt OSINT (Open Source Intelligence). Efterretningstjenesterne har ansat medarbejdere med speciale i at søge efter og sammenstykke oplysninger om en persons arbejde, familiesituation, fritidsinteresser eller andet, som bl.a. kan bruges til at etablere kontakt til en person. Det kan være oplysninger, der ligger frit tilgængeligt på internettet og sociale medier samt i andre medier som fx avisartikler, fjernsynsudsendelser og bøger. Det kan også være oplysninger, der er blevet gjort tilgængelige via tidligere datalæk.

I åbne, digitaliserede informationssamfund deler enkeltindivider, myndigheder, virksomheder og organisationer ofte mange oplysninger og spor, der ligger frit tilgængelige online – også for fremmede efterretningstjenester. Udover spionage kan disse oplysninger i nogle tilfælde understøtte planlægning af skadevoldende aktiviteter såsom destruktive cyberangreb eller sabotage.

Modus

Hvordan opererer fremmede stater og deres efterretningstjenester?

AFLYTNING AF TELE- OG DATATRAFIK – SIGINT

Fremmede efterretningstjenester udvikler løbende deres kapaciteter til at opfange, lagre og udnytte tele- og datatrafik, også kaldet SIGINT (Signals Intelligence).

Denne indhentningsform sker typisk ved at efterretningstjenesterne overvåger udstrålede signaler fra elektronisk kommunikation eller har fysisk adgang til kommunikationsinfrastruktur.

Ved hjælp af SIGINT forsøger efterretningstjenesterne bl.a. at indhente mod mobiltelefoni (herunder opkald, sms'er, data fra apps og geolokation), e-mails, krypteret kommunikation og radiokommunikation.

Selvom en efterretningstjeneste ikke nødvendigvis kan gennemskue indholdet af kommunikationen, kan den give brugbar viden om målpersoner, fx hvilke netværk målpersoner er en del af, og hvilke vaner og bevægelsesmønstre de har. SIGINT kan dermed muliggøre yderligere spionageaktiviteter.

Det er meget vanskeligt at opdage en kompromittering, der er udført ved brug af SIGINT. Det skyldes, at fremmede efterretningstjenester kan overvåge kommunikation uden at påvirke selve transmissionen. Der er med andre ord tale om en såkaldt "passiv" indhentningsform, som heller ikke forudsætter fysisk tilstedeværelse ved målet.

Det er dog PET's vurdering, at fremmede efterretningstjenester har etableret forskellige former for fremskudte lyttestationer i udlandet. Eksempelvis kan diplomatiske repræsentationer have fysiske installationer, der gør mere lokal aflytning af tele- og datatrafik mulig. Fremmede efterretningstjenester kan også benytte mobile elektroniske enheder, der kan opfange lokal tele- og datatrafik.

Modus

Hvordan opererer fremmede stater og deres efterretningstjenester?

INDHOLD

CYBERSPIONAGE

Cyberspionage kan give adgang til meget store mængder data, der kan lagres og anvendes umiddelbart eller på sigt. Cyberspionage er på mange måder en attraktiv fremgangsmåde for fremmede efterretningstjenester, da den er forbundet med lav risiko og ofte kan udføres uden at efterlade særligt synlige spor. Cyberspionage kan udøves fra hjemlandet uden fysisk tilstedeværelse eller kontakt til en menneskelig kilde i det ramte land.

Fremmede efterretningstjenester benytter i betydeligt omfang cyberangreb til at forsøge at skaffe sig adgang til oplysninger fra danske myndigheder, uddannelsesinstitutioner, virksomheder og privatpersoner. Efterretningstjenesterne gør bl.a. brug af avancerede hackergrupper, der har kapacitet til at udføre yderst gennemgribende kompromitteringer af it-systemer.

Cyberangreb kan være vanskelige at opdage og modvirke, og det kan være svært efterfølgende at udbedre skaderne. I yderste konsekvens kan en fremmed efterretningstjeneste få kontinuerlig adgang til mailkorrespondance og dokumenter hos eksempelvis en myndighed.

Cyberspionage kan også blive brugt til at forberede destruktive cyberangreb, som en fjendtlig stat vil kunne iværksætte i tilfælde af en eskalerende krise eller krig.

Styrelsen for Samfundssikkerhed (SAMSIK) udgiver jævnligt vurderinger om cybertruslen, heriblandt Cybertruslen mod Danmark og Cybertruslen mod Grønland. Du kan finde SAMSIK's vurderinger her *[LINK]*.

CYBERANGREB MOD DET NORSKE STORTING

I august 2020 blev det norske Storting ramt af et omfattende cyberangreb. Det norske sikkerhedspoliti, PST, konkluderede i december 2020, at en række e-mailkonti var blevet kompromitteret, og at det var lykkedes for aktøren at hente sensitivt indhold fra disse konti. Ifølge PST er det sandsynligt, at operationen blev udført af den russiske cyberaktør APT28, også kaldet Fancy Bear, der er tilknyttet Ruslands militære efterretningstjeneste GRU.

Modus

Hvordan opererer fremmede stater og deres efterretningstjenester?

INDHOLD

FYSISK SKADEVOLDENDE AKTIVITETER

Visse fremmede efterretningstjenester bruger fysisk skadevold eller truslen om samme til at opnå konkrete mål. Fysisk skadevold kan dels være rettet mod personer i form af trusler, chikane, vold, bortførelser og i yderste instans likvideringer. Dels kan der være tale om sabotage, hærværk og anden ødelæggelse af ejendom, hvilket ligeledes kan være til fare for mennesker.

Når fremmede efterretningstjenester vil iværksætte fysisk skadevold i Vesten, råder de over deres egne, trænede operatører, men de rekrutterer også i stigende grad blandt sympatisører, kriminelle netværk og økonomisk sårbare personer. Fremmede efterretningstjenester anvender blandt andet sociale medier til at rekruttere personer bosiddende i Europa til at udføre vold og sabotage til gengæld for løfter om belønning, som de i sidste ende typisk ikke indfrier.

PET kan også konstatere, at de russiske efterretningstjenester løbende udfører spionage mod kritisk infrastruktur i Vesten, som understøtter deres planer for sabotage af kritisk infrastruktur, som kan aktiveres i tilfælde af en eskalerende konflikt. Spionage mod kritisk infrastruktur kan give adgang til oplysninger, der kan muliggøre fremtidige sabotageaktioner af både fysisk og digital karakter.

HVAD ER HYBRIDE VIRKEMIDLER?

Hybride virkemidler er en samlebetegnelse for forskellige typer af offensive operationer, som fremmede stater anvender til at gennemtvinge deres udenrigs- og sikkerhedspolitiske målsætninger uden at ty til direkte militær konfrontation. Formålet med virkemidlerne er gradvist at svække sammenhængskraften i og blandt de ramte stater fx ved at underminere befolkningernes følelse af sikkerhed, påvirke beslutningsprocesser samt øge mistilliden til demokratiske institutioner og myndighedernes krisestyringsevne. Efterretningstjenesterne anvender ofte virkemidlerne i kombination, heriblandt påvirkningsoperationer, destruktive cyberangreb og sabotage.

RUSLAND BEORDREDE BRANDSTIFTELSE I LONDON

Den 20. marts 2024 påsatte tre mænd en brand på et lager i et industriområde i London fyldt med forsyninger bestemt til Ukraine. Branden forårsagede skader for ca. 1 million pund.

En efterforskning ledet af Met's Counter Terrorism Command har efterfølgende vist, at gruppens leder, Dylan Earl (21), i 2023 havde etableret kontakt til Wagner-gruppen, som er en privat militærorganisation, der handlede på vegne af den russiske stat. Earl rekrutterede derefter en gruppe unge mænd til at sætte ild til lageret i London og han organiserede overvågning af to andre virksomheder som forberedelse til yderligere brandstiftelsesangreb.

I oktober 2025 blev Earl og fire andre unge mænd idømt fængselsstraffe på mellem otte og 23 år for deres involvering i sabotage på vegne af Rusland.

Modus

Hvordan opererer fremmede stater og deres efterretningstjenester?

INDHOLD

PÅVIRKNINGSVIRKSOMHED

En række fremmede stater og deres efterretningstjenester forsøger løbende at påvirke politiske beslutningsprocesser og den almene meningsdannelse i Europa. Påvirkningsvirksomhed kan både foregå via traditionelle fysiske påvirkningsagenter (personlig påvirkning) og via spredning af falsk eller misledende information på internettet (informationspåvirkning). Aktiviteterne kan være målrettet konkrete begivenheder, såsom fx valghandlinger, men foregår i ligeså høj grad i det daglige.

HVAD ER DESINFORMATION OG MISINFORMATION?

Misledende information kan overordnet set opdeles i to hovedkategorier, henholdsvis desinformation, dvs. den bevidste produktion og spredning af vildledende information, og misinformation, dvs. den ubevidste spredning af vildledende information.

Formålet med fremmede staters påvirkningsvirksomhed er typisk at fremme egne udenrigspolitiske interesser ved at påvirke politiske beslutningsprocesser og den almene meningsdannelse i andre lande.

Påvirkningsvirksomhed er ofte rettet mod at udnytte eksisterende skillelinjer i en befolknings holdninger, hvor det er let at skabe konflikt og polarisering. Påvirkningsvirksomhed handler ikke alene om at sprede "falske nyheder", men også om at fordreje, fremme eller overeksponere eksisterende konflikter og sårbarheder i eksempelvis et land eller en gruppe af lande.

Desinformation og misinformation kan spredes hurtigt og bredt på internettet via sociale medier. Det skyldes bl.a., at sociale medier ikke er underlagt streng redaktionel kontrol, samt at mulighederne for at få fjernet indhold på sociale medieplatforme er yderst begrænsede. Udviklingen af kunstig intelligens har desuden givet fremmede stater og andre aktører bedre muligheder for at producere og sprede desinformation, herunder også indhold målrettet mindre sprogområder.

Kunstig intelligens (AI)

Den teknologiske udvikling har frembragt en række nye redskaber, som fremmede stater og deres efterretningstjenester kan anvende til at understøtte påvirkning.

Bl.a. har udviklingen af AI – særligt generativ AI – potentiale til at øge truslen fra påvirkningsvirksomhed ved at give fjendtlige aktører flere værktøjer til at producere og sprede desinformation af indholdsmæssig høj kvalitet.

PET vurderer, at udviklingen af generativ AI kan få betydning for både indholdet og mængden af desinformation i informationsrummet. Generative AI-teknologier kan bl.a. bruges til at gøre desinformation mere realistisk og målrettet, hvilket kan øge risikoen for, at borgere i fremtiden træffer beslutninger på baggrund af manipuleret information.

Modus

Hvordan opererer fremmede stater og deres efterretningstjenester?

PÅVIRKNINGSVIRKSOMHED

Generative AI-teknologier kan desuden øge omfanget af desinformationskampagner ved at accelerere produktionshastigheden og gøre det muligt for en bredere gruppe af aktører at producere manipulerende information.

RUSSISK PÅVIRKNINGSOPERATION UDNYTTEDE DANSK MEDLEM AF FOLKETINGET

FE vurderer, at Rusland stod bag en påvirkningsoperation i januar 2025, hvor et falsk opslag om den danske politiker og Folketingsmedlem, Karsten Hønge, blev delt på medier og sociale medieplatforme. Det falske opslag kom oprindeligt fra en påvirkningsaktør, som tidligere har promoveret Ruslands dagsorden i Ukraine. Ifølge oplysninger fra den franske anti-desinformationsmyndighed, Viginum, er aktøren del af et påvirkningsnetværk, som handler på vegne af den russiske stat.

Budskabet i det falske opslag var, at Danmark vil bede om hjælp fra Rusland til at forhindre, at Grønland bliver en del af USA. Opslaget havde efter alt at dømme til formål at udnytte den offentlige debat i og om Grønland til at forværre forholdet mellem Danmark og USA.

Påvirkningsoperationen skal ses som en del af den løbende påvirkning, hvor Rusland forsøger at skabe splid i det transatlantiske forhold og undermine den vestlige støtte til Ukraine.

Det er mindre sandsynligt, at det falske opslag var et forsøg på at påvirke udfaldet af det grønlandske valg.

Modus

Hvordan opererer fremmede stater og deres efterretningstjenester?

INDHOLD

ULOVLIG ANSKAFFELSESVIRKSOMHED

PET kan konstatere, at en række fremmede stater forsøger at anskaffe eller omdirigere produkter, viden eller tjenesteydelser i strid med sanktioner og eksportbegrænsninger, for at anvende dem i egen våbenproduktion eller i militære programmer.

Fremmede efterretningstjenester medvirker ofte i den ulovlige anskaffelsesvirksomhed, bl.a. ved at bidrage til at identificere relevante virksomheder og ved, at tjenesterne via deres kontakter og netværk bidrager med at anskaffe produkter til landets militær.

Udenlandske netværk, der ulovligt forsøger at anskaffe produkter og teknologi, er interesseret i en række forskellige danske produkter, herunder maritim- og undervandsteknologi, sensor- og laserudstyr, test- og laboratorieudstyr samt industrimaskiner og komponenter til produktionsudstyr.

Det er i mange tilfælde produkter, der er klassificeret som dual use, og de er dermed underlagt eksportkontrol og sanktioner, hvis de eksporteres til eksempelvis Rusland. Men PET har også flere eksempler på ikke-regulerede produkter, der bliver efterspurgt af lande, der skal bruge dem i deres militære våbenprogrammer.

En måde at sløre den reelle modtager af et produkt på er ved at lade produktet gå igennem en række mellemdestinationer (omdirigeringslande), inden det havner hos den egentlige slutbruger.

På samme måde kan betalinger for varer ske gennem en række mellemmænd i forskellige lande og i forskellig valuta, der kan gøre det vanskeligt at kortlægge forbindelsen mellem varens ophav og den endelige slutbruger.

TYSK-IRANSK FORSKER VED NORSK UNIVERSITET BRØD EKSPORTKONTROLREGLER

I november 2022 blev en professor ved et norsk universitet (NTNU) dømt for flere overtrædelser af norsk eksportkontrol. Han havde givet gæsteforskere fra Iran adgang til et laboratorium med følsomt udstyr og til et af universitetets datasystemer, der er underlagt eksportkontrol. Her installerede en af gæsteforskerne et program, der gav ham fjernadgang til data fra systemet.

Modus

Hvordan opererer fremmede stater og deres efterretningstjenester?

INDHOLD

ULOVLIG OG UØNSKET OVERFØRSEL AF TEKNOLOGI

Ikke-ligesindede stater forsøger systematisk og målrettet at hjemtage viden og knowhow om kritiske teknologier på ulovlig og uønsket vis, bl.a. ved at misbruge udveksling af studerende og forskere, forskningssamarbejder, talentprogrammer, stipendier og investeringer i Vesten mv.

Private aktører, herunder virksomheder, forskningsmiljøer og individer, kan mobiliseres af stater som Kina, Rusland og Iran til geostrategiske eller efterretningsmæssige formål. Det betyder bl.a., at eventuelle investeringer og samhandel kan have formål, der rækker udover de interesser, som officielt bliver fremhævet som årsager til et samarbejde.

Landene har endvidere vidtgående politikker for civil-militær fusion, der sigter mod at styrke forsknings- og udviklingssamarbejdet mellem civile universiteter, private virksomheder og militæret.

Det betyder, at danske samarbejdspartnere uforvarende risikerer at overføre viden, der kan anvendes til militær kapacitetsopbygning.

HVAD ER ULOVLIG OG UØNSKET OVERFØRSEL AF TEKNOLOGI?

PET skelner mellem ***ulovlig*** og ***uønsket*** vidensoverførsel. ***Ulovlig*** vidensoverførsel forekommer, når viden overføres i strid mod gældende lovgivning, eksempelvis via spionage fra fremmede efterretningstjenester.

Uønsket vidensoverførsel omfatter i stedet de tilfælde, hvor danske forskningsinstitutioner eller virksomheder på lovlig vis overfører viden eller færdigheder til entiteter med forbindelse til ikke-ligesindede stater som Kina, Rusland og Iran, der direkte kan anvende den overførte viden på en måde, der strider mod danske eller allierede staters interesser. Det kan eksempelvis være til at opbygge deres militære kapaciteter, at kortlægge sårbarheder i dansk kritisk infrastruktur eller andre forhold, der kan give disse stater fordele under en krise eller konflikt.

RUSSISK FORSKER I ESTLAND DØMT FOR SPIONAGE

En russisk forsker ved universitetet i Tartu, Estland, blev i juni 2024 idømt seks år og tre måneders fængsel for at handle på vegne af den russiske militære efterretningstjeneste, GRU.

Den russiske forskers samarbejde med GRU blev allerede påbegyndt i begyndelsen af 1990'erne, da han blev rekrutteret som studerende ved Sankt Petersborgs statsuniversitet.

Han blev dog en særlig værdifuld kilde for GRU, da han fik ansættelse ved universitetet i Tartu og opnåede et udbredt internationalt netværk i den akademiske verden. Den russiske forsker videregav bl.a. informationer om, hvordan Ruslands handlinger blev opfattet i Estland og om forholdet mellem Estland og Rusland.