VURDERING AF SPIONAGETRUSLEN MOD DANMARK

Truslen fra fremmede staters efterretningsvirksomhed mod Danmark

01

FORORD

Truslen fra fremmede staters efterretningsvirksomhed mod Danmark er blevet mere markant, og i PET har vi i de senere år styrket vores kontraspionageindsats. Indsatsen består i at forebygge, efterforske og modvirke efterretningsaktiviteter udført af fremmede stater i Danmark og mod danske interesser i udlandet. Som et led i vores styrkede indsats offentliggør vi nu for første gang en samlet vurdering af den aktuelle trussel mod Danmark. Vurderingen er også relevant for Grønland og Færøerne.

Fremmede stater udfører først og fremmest efterretningsaktiviteter for at styrke deres politiske, militære og økonomiske position, og Danmark er i kraft af sin aktive rolle på den internationale scene og medlemsskab af internationale organisationer som EU, NATO og FN et attraktivt mål for fremmed efterretningsvirksomhed. Hertil kommer, at dansk teknologi og forskning på en række områder er verdensførende og dermed attraktivt at få adgang til.

Vi har udarbejdet vurderingen på baggrund af PET's samlede oplysninger om fremmede staters efterretningsaktiviteter, herunder oplysninger fra konkrete operationer. De fleste af oplysningerne i disse operationer er klassificerede, men i nogle tilfælde kan vi henvise til konkrete sager, der er kommet til offentlighedens kendskab, heriblandt sager fra udlandet, der illustrerer det trusselsbillede, som vi også ser herhjemme. Vi har i beskrivelsen af trusselsbilledet inddraget vurderinger fra Forsvarets Efterretningstjeneste (FE) og Center for Cybersikkerhed (CFCS).

Udgivelsen af denne vurdering står naturligvis ikke alene. Den suppleres af en omfattende rådgivningsindsats, der er rettet mod de dele af det danske samfund, der er særligt sårbare over for fremmede staters efterretningsvirksomhed.

I PET følger vi udviklingen i trusselsbilledet tæt, og vi opdaterer vurderingen, når ændringer i trusselsbilledet tilsiger det.

Vi har baseret vurderingen på oplysninger og efterretninger, der er blevet behandlet før den 1. december 2021.

God læselyst!

Anders Henriksen
Afdelingschef for Kontraspionage

INDHOLD

02

OVERORDNET OM TRUSSELSBILLEDET

Truslen fra fremmede staters efterretningsvirksomhed mod Danmark og danske interesser i udlandet stiller vores samfund over for nogle væsentlige politiske, sikkerhedsmæssige og økonomiske udfordringer. PET har i de seneste år afdækket flere sager, der vidner om, at en række fremmede stater aktivt udfører efterretningsvirksomhed mod Danmark. Myndighederne i andre vestlige lande har på tilsvarende vis afdækket sager, der viser, at der er en trussel mod deres samfund.

Det er PET's vurdering, at der er en specifik og vedvarende trussel fra fremmede staters efterretningsvirksomhed i Danmark. Den fremmede efterretningsvirksomhed omfatter spionage, påvirkning, chikane, forsøg på ulovligt at anskaffe produkter, teknologi og viden samt i helt særlige tilfælde likvideringsforsøg. Metoder og mål varierer alt efter, hvilken statslig aktør der står bag aktiviteterne. Truslen udgår primært fra Rusland, Kina og Iran, men der er også eksempler på, at andre stater udfører efterretningsaktiviteter i Danmark.

Hvis fremmede stater uretmæssigt får adgang til klassificerede og beskyttelsesværdige informationer, kan det skade Danmarks sikkerhed og handlefrihed. Hvis det drejer sig om informationer, der omhandler Danmarks forhold til andre lande, kan informationerne undertiden bruges både mod Danmark og mod de lande, som vi samarbejder med. Spionage mod virksomheder og forskningsinstitutioner i Danmark kan skade Danmarks konkurrenceevne og føre til tab af indtægter, arbejdspladser og anseelse.

Danmark står over for en bredspektret og kompleks trussel fra fremmede staters efterretningsvirksomhed. Danmarks aktive rolle på den internationale scene, den øgede globalisering og internationale konkurrence, den generelle åbenhed i samfundet, digitaliseringen og et højt teknologisk vidensniveau bidrager til at gøre Danmark til et attraktivt mål for fremmed efterretningsvirksomhed. Hertil kommer, at de sikkerhedspolitiske vilkår er under forandring, og at der i disse år er en øget rivalisering mellem stormagterne Rusland, Kina og USA.[1]

Rusland har ligesom under den kolde krig fortsat fokus på at indhente informationer om politiske, økonomiske og militære forhold samt om forhold, der kan styrke Ruslands position inden for udvikling af ny teknologi.

Kina ønsker at øge sin politiske, økonomiske og militære indflydelse i verden og at blive teknologisk selvforsynende og førende. De kinesiske efterretningstjenester har vide beføjelser til at indsamle oplysninger fra kinesiske selskaber, organisationer og individer, uanset hvor i verden de befinder sig. Det kinesiske etpartisystem anlægger en *whole of society*-tilgang, som indebærer, at alle niveauer i det kinesiske samfund i princippet kan blive mobiliseret for at nå de strategiske mål, som den kinesiske ledelse løbende melder ud. Dertil kommer, at Kina anvender et meget bredt spektrum af både lovlige og ulovlige midler og tilgange til bl.a. at opnå adgang til viden og produkter og til at fremme et positivt narrativ om Kina.

1) *Se Forsvarets Efterretningstjenestes 'UDSYN 2021'.*

Endelig har PET set eksempler på, at lokale og regionale konflikter i og mellem visse lande undertiden finder vej til Danmark.

PET kan konstatere, at politikere, embedsmænd, ansatte i efterretningstjenesterne, Forsvaret og i virksomheder, forskere, studerende samt flygtninge og dissidenter løbende indgår som mål i fremmede staters efterretningsvirksomhed mod Danmark.

Fremmede stater udfører bl.a. **spionage** mod Danmark for at indhente oplysninger om udenrigs-, sikkerheds- og forsvarspolitiske forhold, om kritisk infrastruktur, om forhold internt i Rigsfællesskabet og om deres egne indenrigspolitiske og regionale modstandere, der eventuelt måtte befinde sig i Danmark. PET kan herudover konstatere, at flere lande udviser en stigende interesse for visse forskningsområder og teknologier, som har det til fælles, at de indgår i et større teknologisk kapløb, som kan have betydning for globale sikkerhedspolitiske, militære og økonomiske magtforhold.

Påvirkningsvirksomhed mod Danmark vil først og fremmest kunne udføres for at påvirke danske beslutningstagere, den almene meningsdannelse i Danmark og/eller omverdenens syn på Danmark eller en fremmed stat. Formålet vil typisk være at skabe sympati for denne fremmede stats egne politikker eller for at skade sammenhængskraften i Danmark, Rigsfællesskabet eller i de internationale organisationer, som Danmark indgår i. Påvirkningsvirksomhed varierer i metode alt afhængig af, hvilken stat der står bag. Den kan bl.a. foregå ved at bringe fordrejede nyhedshistorier i medier, at miskreditere personer på sociale medier, at forstærke eksisterende konflikter mellem befolkningsgrupper eller ved direkte at holdningspåvirke enkeltindivider eller grupper. Påvirkningsvirksomhed kan antage form af "hack og læk"-operationer, hvor en aktør skaffer sig adgang til sensitive informationer via et cyberangreb og efterfølgende lækker informationerne offentligt, evt. i fordrejet form. Påvirkningsvirksomhed vil ofte være målrettet eksisterende skillelinjer i befolkningens holdning, hvor det er let at skabe konflikt og polarisering. Aktiviteterne kan være målrettet konkrete begivenheder, såsom valghandlinger. PET har hidtil ikke afdækket fremmed statslig påvirkningsvirksomhed i forbindelse med valg i Danmark.

Der er også visse fremmede stater, der udøver forskellige former for **overvågning og påvirkning af egne statsborgere**, der opholder sig i Danmark. Det drejer sig bl.a. om aktiviteter, der er rettet mod flygtninge og dissidenter. Formålet med aktiviteterne kan være at undergrave eller eliminere politisk opposition.

HVAD SIGER LOVEN OM SPIONAGE OG PÅVIRKNING?

Spionage og påvirkning er omfattet af straffelovens kapitel 12 (§§ 107-109).

Ifølge straffeloven er det strafbart at indhente eller videregive information om forhold, som af hensyn til den danske stats eller det danske samfunds interesser skal holdes hemmelige, til personer, der virker i fremmed magts eller organisations tjeneste.

Det forstås også som spionage, hvis man røber eller videregiver information om regeringens fortrolige forhandlinger, drøftelser eller beslutninger i sager, der har betydning for statens sikkerhed eller rettigheder i forhold til fremmede stater, eller hvis emnet vedrører betydelige samfundsøkonomiske interesser over for udlandet.

Det er også strafbart i øvrigt at hjælpe en fremmed efterretningstjeneste med at virke inden for den danske stats område, eksempelvis ved at videregive informationer om borgere i Danmark til den fremmede tjeneste.

Det er endvidere strafbart at hjælpe eller sætte en fremmed efterretningstjeneste i stand til at foretage påvirkningsvirksomhed inden for den danske stats område for at påvirke beslutningstagning eller den almene meningsdannelse.

En række stater er involveret i **ulovlig anskaffelsesvirksomhed** ved i strid med bl.a. eksportkontrol- og sanktionsregimer at forsøge at anskaffe eller omdirigere produkter og teknologi fra Danmark for at anvende dem i egen våbenproduktion eller i militære programmer. Truslen fra ulovlig anskaffelsesvirksomhed er primært rettet mod virksomheder og forskningsinstitutioner, der leverer produkter, forskning eller viden, som visse stater har brug for til udvikling af deres militære formåen.

Truslen mod Danmark fra fremmede stater kan også tage form af visse **udenlandske direkte investeringer,** hvor en udenlandsk aktør har ikke-kommercielle hensigter. De sikkerhedsmæssige konsekvenser af den type investeringer kan være alvorlige og vedrører bl.a. langsigtede, strukturelle forhold, der kan underminere samfundets modstandskraft og interesser. Det gælder eksempelvis investeringer, der giver adgang til dansk teknologiudvikling, medfører tab af kontrol med dele af den danske kritiske infrastruktur eller indebærer uhensigtsmæssige økonomiske afhængighedsforhold til en fremmed stat.

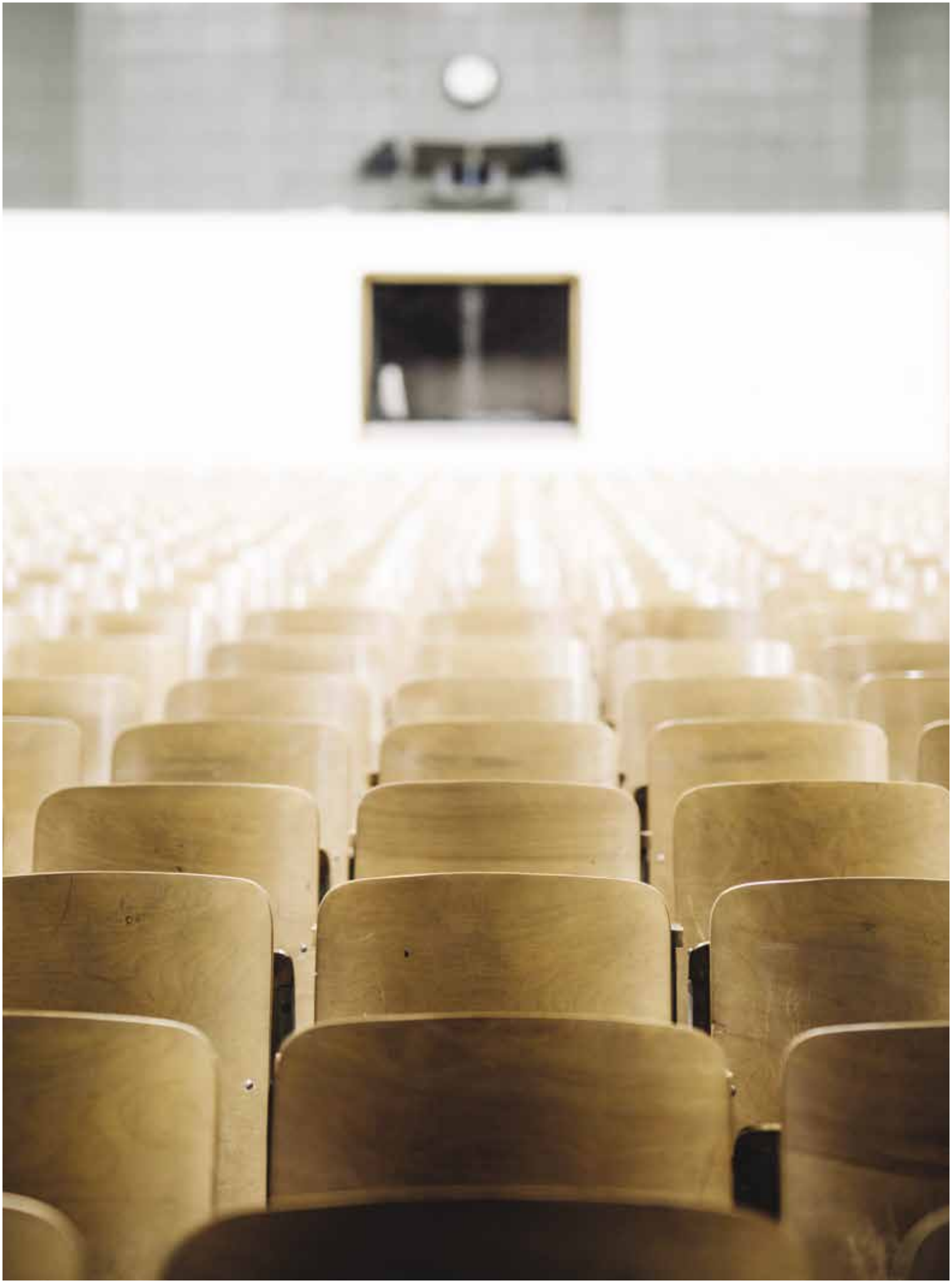
Fremmede staters efterretningstjenester er kendetegnet ved at være professionelle modstandere med en høj kapacitet, der i nogle tilfælde planlægger og gennemfører aktiviteter med en lang tidshorisont. Fremmede efterretningstjenester har ofte mange ressourcer til rådighed, og de udnytter løbende teknologiske fremskridt til at udvikle nye måder at operere på. Nogle stater tildeler deres efterretningstjenester meget vide rammer til at operere både hjemme og i udlandet.

De fremmede efterretningstjenester, der er aktive i Danmark, gør bl.a. brug af trænede efterretningsofficerer, der arbejder under dække af at være diplomater udstationeret i Danmark. Rusland har eksempelvis et antal efterretningsofficerer på deres ambassade i Danmark. Disse efterretningsofficerer forsøger kontinuerligt at hverve kilder med adgang til klassificerede eller beskyttelsesværdige informationer af interesse for Rusland.

De fremmede efterretningstjenester anvender også avancerede hackergrupper, der via cyberangreb er i stand til at kompromittere og skabe adgang til it-systemer. Denne adgang kan efterretningstjenesterne anvende til at udføre cyberspionage.[2]

Derudover kan en fremmed efterretningstjeneste udnytte en række andre kanaler, som eksempelvis andre statslige myndigheder, organisationer, forskellige former for mellemmænd, såsom lobbyister, kriminelle netværk og private virksomheder. Det er ikke altid, at disse aktører er vidende om, at de i praksis bistår med at udøve efterretningsvirksomhed for en fremmed stat, herunder samarbejder med en fremmed efterretningstjeneste.

2) *For yderligere se 'Cybertruslen mod Danmark 2021', Center for Cybersikkerhed*



03

HVILKE MÅL GÅR DE FREMMEDE EFTERRETNINGSTJENESTER EFTER?

- REGERINGEN, FOLKETINGET OG CENTRALADMINISTRATIONEN
- TEKNOLOGI OG FORSKNING
- FORSVARET
- FLYGTNINGE OG DISSIDENTER
- RIGSFÆLLESSKABET
- DANSKE INTERESSER I UDLANDET

PET kan konstatere, at fremmede efterretningstjenester særligt udviser interesse for politikere og embedsmænd i den danske centraladministration. Det gælder i særdeleshed de politikere og embedsmænd, der beskæftiger sig med udenrigs-, sikkerheds og forsvarspolitik eller med områder og sager, der vedrører energi og råstoffer. Danmarks aktive deltagelse i internationale organisationer som NATO, EU og FN er også i fokus for fremmede efterretningstjenester. Efterretningstjenesterne interesserer sig bl.a. for at skaffe informationer om danske og udenlandske forhandlingspositioner, samarbejdsrelationer, nøglepersoner og mødeaktiviteter.

TIDLIGERE MEDARBEJDER I TYSK TÆNKETANK TILTALT FOR SPIONAGE TIL FORDEL FOR KINA

I maj 2021 tiltalte de tyske myndigheder en pensioneret tysk statsborger for at udlevere oplysninger til en kinesisk efterretningstjeneste. Den tiltalte er uddannet politolog og har tidligere arbejdet for en tysk tænketank. Gennem sit arbejde ved tænketanken havde den tiltalte et stort netværk og mødtes bl.a. med højtstående politiske samtalepartnere. Ifølge de tyske myndigheder blev den tiltalte hvervet af en kinesisk efterretningstjeneste i forbindelse med en rejse til Shanghai i juni 2010, og siden skulle han regelmæssigt have videregivet oplysninger til den kinesiske efterretningstjeneste før og efter statsbesøg eller internationale konferencer og om aktuelle spørgsmål. Den tyske statsborgers tysk-italienske ægtefælle er tiltalt for at medvirke til spionageaktiviteterne.

4 TEKNOLOGI OG FORSKNING

Danmark er på en række områder førende i verden inden for teknologi, innovation og forskning. Det gælder bl.a. inden for energi og bioteknologi, og inden for visse kritiske teknologier. Danmarks førerposition inden for disse områder udgør et væsentligt indtægtsgrundlag for dansk økonomi, men den gør samtidig Danmark til et attraktivt mål for fremmede stater som Kina, Rusland og Iran, der gennem spionage, herunder statsfinansieret industrispionage, og ulovlig anskaffelsesvirksomhed forsøger at få fat i den nyeste viden og teknologi. Nogle teknologier kan både anvendes til civilt og militært brug – såkaldt dual-use (dobbelt anvendelse).

Kina har i sin seneste femårsplan (2021-2025) understreget betydningen af innovation og teknologi for Kinas ønsker om at sikre sig øget global indflydelse. Kina har herudover en national strategi for "militær-civil fusion", der sigter på, at viden og teknologi lettere kan udvikles i samspillet mellem civile universiteter og militæret.

PET kan konstatere, at fremmede efterretningstjenester løbende forsøger at opbygge kontakter til studerende, forskere og virksomheder, der vil kunne udlevere informationer om den nyeste danske teknologi og forskning. Det gælder særligt energiteknologi, bioteknologi, kvanteteknologi, robotteknologi, forsvarsindustrielle produkter og produkter omfattet af eksportkontrol. Udenlandske studerende og forskere i Danmark kan medvirke til at overføre sensitiv viden til fremmede stater.

RUSSISK STATSBORGER DØMT FOR SPIONAGE MOD DTU OG DANSK ENERGIVIRKSOMHED

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 den Aalborgbaserede energivirksomhed SerEnergy A/S, og han havde i flere år udleveret oplysninger mod betaling til en russisk efterretningstjeneste. SerEnergy A/S udvikler bl.a. brændselsceller, der kan omdanne brint til grøn strøm.

I de seneste år har der været flere sager i Europa om spionage mod teknologi og forskning.

August 2020
I august 2020 anholdt norsk politi en norsk statsborger med indisk baggrund på en restaurant, hvor han mødtes med en diplomat fra den russiske ambassade. I virkeligheden var diplomaten russisk efterretningsofficer, som kort efter episoden blev udvist af **Norge**. Den norske statsborger er sigtet for at have udleveret statshemmeligheder til Rusland mod betaling. Møderne skal være foregået skjult og over en længere periode. Den tiltalte arbejdede hos selskabet DNV GL, som bl.a. beskæftiger sig med olie, gas og grøn energiteknologi.

December 2020
I december 2020 udviste **Nederlandene** to diplomater fra Ruslands ambassade i Haag, som ifølge nederlandske myndigheder i virkeligheden arbejdede for den russiske udenrigsefterretningstjeneste SVR. En af diplomaterne havde ifølge de nederlandske myndigheder opbygget et omfattende netværk af kilder, som var eller havde været aktive i den højteknologiske industri. Efterretningsofficererne havde målrettet deres efterretningsaktiviteter mod nederlandske virksomheder, som bl.a. arbejdede med kunstig intelligens og nanoteknologi.

Juni 2021
I juni 2021 anholdt **tyske myndigheder** en russisk statsborger anklaget for spionage til fordel for en russisk efterretningstjeneste. Den anholdte, der arbejdede som videnskabelig medarbejder ved et naturvidenskabeligt teknisk institut på et tysk universitet, er anklaget for at have mødtes mindst tre gange med en russisk efterretningsofficer og på to af disse møder mod betaling at have udleveret oplysninger.

September 2021
I september 2021 blev en 47-årig svensk konsulent idømt tre års fængsel for spionage. Manden havde i en længere periode mod betaling videregivet oplysninger til en russisk efterretningstjeneste. Han er uddannet fra et teknisk universitet i **Sverige** og blev dømt for at videregive oplysninger fra sit arbejde hos den svenske køretøjsfabrikant Scania. Konsulenten blev pågrebet af det svenske sikkerhedspoliti SÄPO i begyndelsen af 2019 under et møde på en restaurant med en russisk diplomat fra ambassaden i Stockholm. Diplomaten arbejdede ifølge den svenske anklagemyndighed i virkeligheden for en russisk efterretningstjeneste.

Marts 2021
I marts 2021 blev en estisk forsker med tilknytning til NATO og **Estlands** forsvarsministerium idømt tre års fængsel for spionage til fordel for en kinesisk efterretningstjeneste. Ifølge Estlands efterretningstjeneste KAPO blev forskeren rekrutteret i 2018 under et besøg i Kina. Under forløbet, der blev afbrudt i september 2020, modtog forskeren flere rejser til forskellige asiatiske lande. Desuden modtog han omkring 17.000 euro fra sin kinesiske kontakt, der udgav sig for at komme fra en kinesisk tænketank.

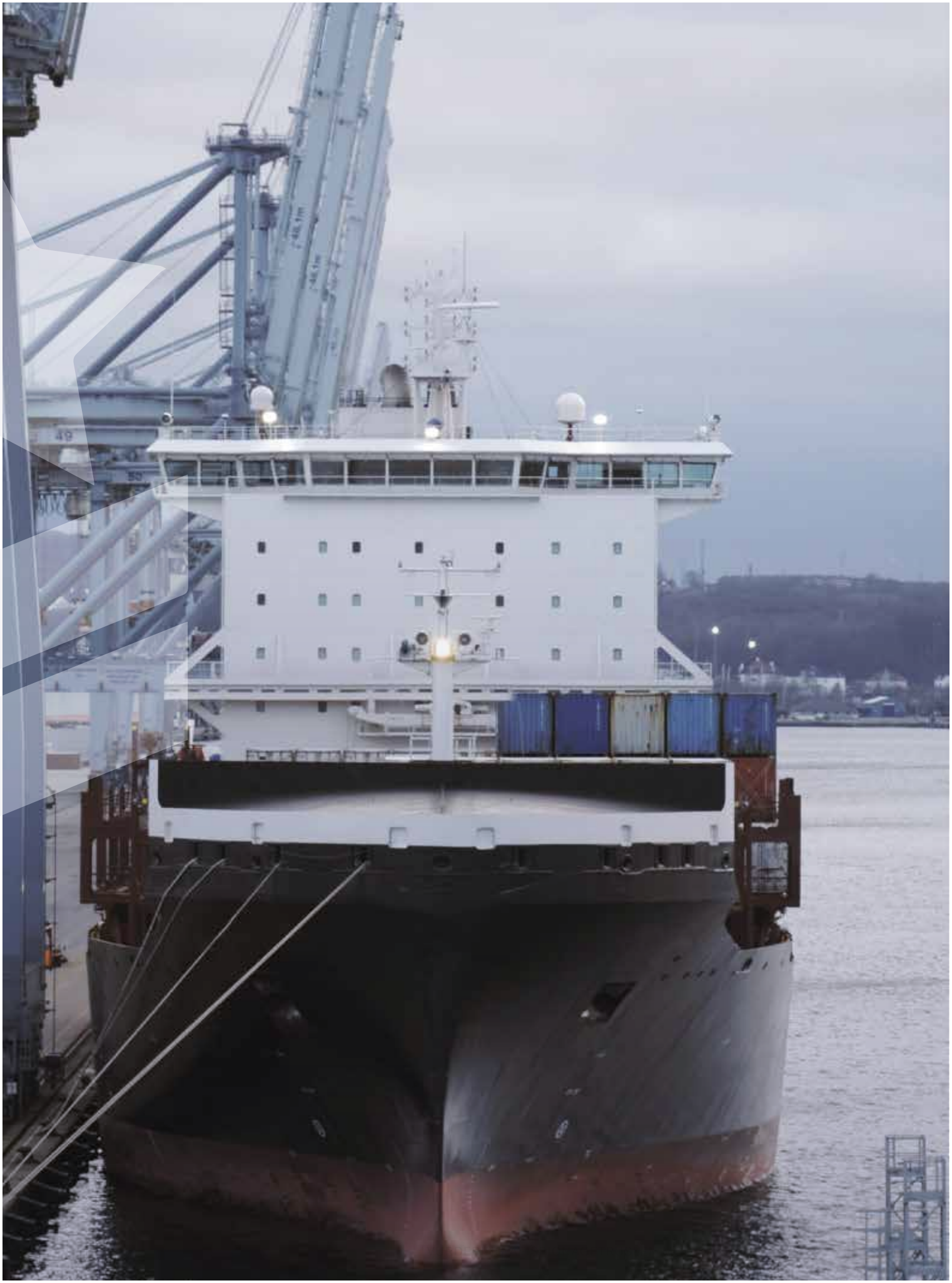
Fremmede efterretningstjenester udfører også efterretningsaktiviteter mod Forsvaret. Forsvaret er bl.a. et interessant spionagemål på grund af Danmarks geografiske placering, forsvarssamarbejde med NATO og USA og Forsvarets deltagelse i internationale operationer. Opgaven med at beskytte det danske forsvar mod fremmed efterretningsvirksomhed varetages af Forsvarets Efterretningstjeneste (FE).

Forsvaret er typisk mål for fremmede militære efterretningstjenester, som anvender et komplekst spektrum af både civile og militære kapaciteter til lands, til vands, i luften og i cyberdomænet. Fremmede stater forbereder sig også i fredstid til både krise og krig i alle domæner. Fremmede militære efterretningstjenester udfører derfor efterretningsaktiviteter rettet mod Forsvaret og civile strukturer, som samlet set understøtter forsvaret af Danmark og Rigsfællesskabet eller NATO's kollektive forsvar.

Havnefaciliteter og anden samfundskritisk civil infrastruktur udgør væsentlige elementer i forhold til Danmarks rolle i NATO-sammenhæng. Danske virksomheder er leverandører til både Forsvaret, NATO og forsvarsindustrien i NATO. Civile statslige og private leverandører udgør derfor mål for fremmede militære efterretningstjenester, som har til opgave at underminere NATO's handlekraft og teknologiske overlegenhed.

ITALIENSK FLÅDEKOMMANDØR MISTÆNKT FOR SPIONAGE TIL FORDEL FOR RUSLAND

I marts 2021 blev en italiensk flådekommandør anholdt i forbindelse med et møde med en efterretningsofficer fra den russiske ambassade i Rom, der arbejdede under dække af at være diplomat. Ifølge åbne medier havde den italienske kommandør mod betaling udleveret beskyttelsesværdige dokumenter til den russiske efterretningsofficer. Der var bl.a. tale om hemmelige NATO dokumenter. Den russiske efterretningsofficer blev sammen med en anden medarbejder på den russiske ambassade udvist af Italien.



PET kan konstatere, at visse fremmede stater med hjælp fra deres efterretningstjenester udfører forskellige former for overvågning og påvirkning af egne statsborgere, der opholder sig i Danmark. Det drejer sig bl.a. om flygtninge og dissidenter. Formålet er typisk at neutralisere, undergrave eller eliminere politisk opposition. Fremmede staters efterretningstjenester kan også anvende ambassadepersonale, kriminelle netværk og egne statslige organisationer eller institutioner til at gennemføre aktiviteterne. Der er flere eksempler på, at fremmede stater bruger egne statsborgere, der bor i Danmark, som meddelere. De fremmede staters overvågning af egne statsborgere i Danmark kan eksempelvis bestå i at føre registre over personerne og deres politiske tilhørsforhold eller at overvåge demonstrationer, hvor egne statsborgere deltager. I helt særlige tilfælde kan fremmede stater iværksætte operationer med henblik på likvideringer af dissidenter.

IRANSKE LIKVIDERINGSPLANER OG SPIONAGE TIL FORDEL FOR SAUDI-ARABIEN

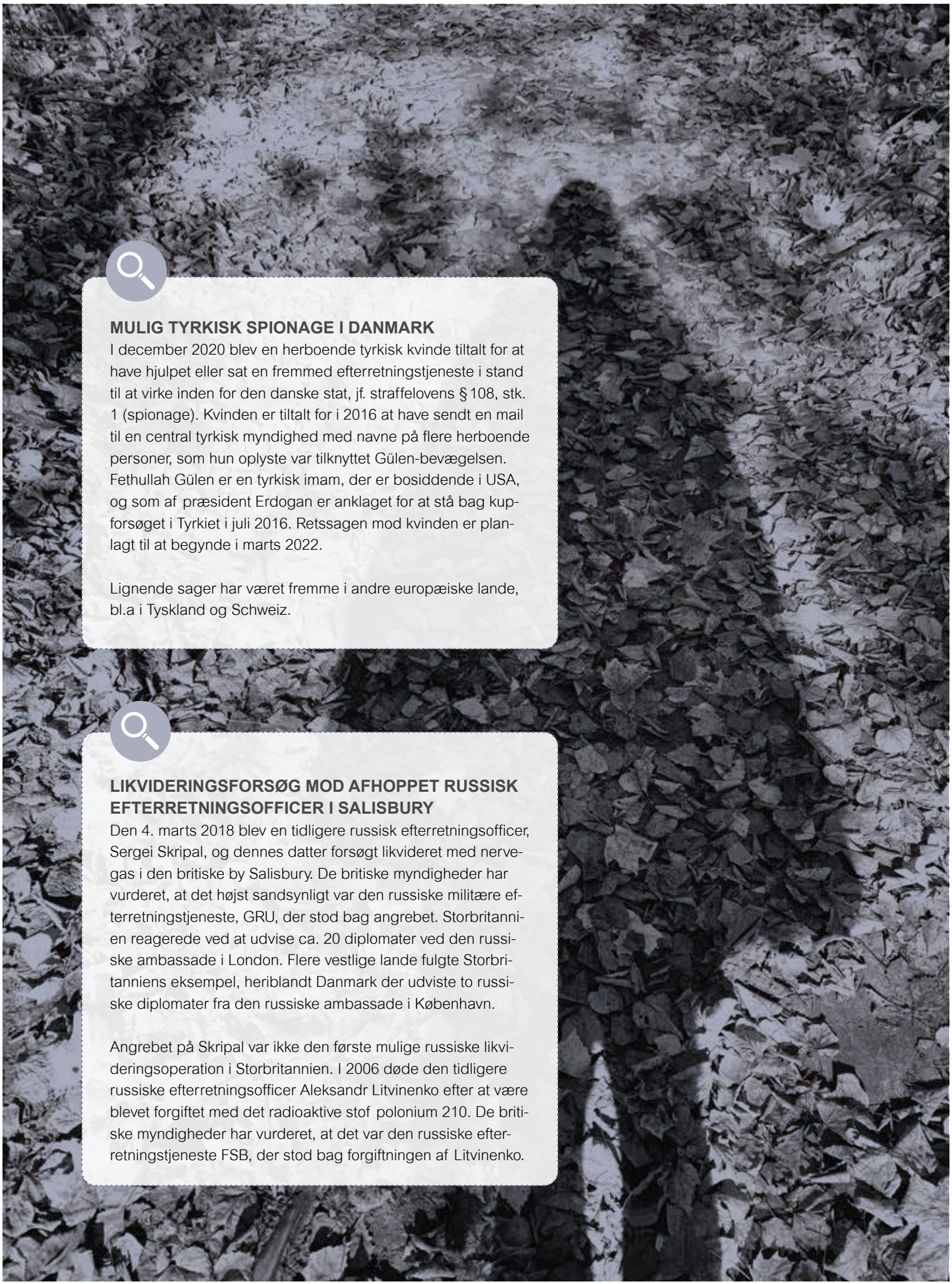
Den 6. maj 2021 stadfæstede Østre Landsret en dom på syv års fængsel til en norsk-iransk statsborger. Personen blev dømt for forsøg på manddrab (straffelovens § 237, jf. § 21, jf. § 23) og spionage (straffelovens § 108, stk. 1), og udvist med indrejseforbud for bestandigt. Personen blev dømt for at have sat en iransk efterretningstjeneste i stand til at virke inden for den danske stats område vel vidende, at denne bistand var til brug for planer om drab på et ledende medlem af ASMLA (Arab Struggle Movement for the Liberation of Ahwaz), der er bosiddende i Danmark. ASMLA er en oppositionsbevægelse i Iran.

I februar 2020 blev den norsk-iranske statsborgers iranske føringsofficer varetægtsfængslet in absentia i sagen.

Iranske efterretningstjenester er bl.a. mistænkt for at stå bag likvideringer og bortførelser af mindst otte modstandere af det iranske styre med ophold i Europa og Tyrkiet i perioden fra 2015 til 2020.

I forlængelse af sagen mod den norsk-iranske statsborger blev tre ledende medlemmer af ASMLA anholdt og sigtet efter straffelovens § 108, stk. 1 (spionage) for i en periode fra 2012 til 2020 at have udført ulovlig efterretningsvirksomhed i Danmark på vegne af en saudiarabisk efterretningstjeneste. De tre personer er sigtet for at have indsamlet oplysninger om enkeltpersoner og virksomheder i Danmark og i udlandet og videregivet disse oplysninger til en saudiarabisk efterretningstjeneste. De tre mænd er siden også blevet tiltalt for billigelse af terror og terrorfinansiering samt spionage mod militære anliggender efter straffelovens § 108, stk. 2.

Retssagen begyndte den 29. april 2021 ved Retten i Roskilde. Sagen har forbindelse til ovenstående sag, idet det var et af de tre ASMLA-medlemmer, der var mål for angrebsplanlægningen.



MULIG TYRKISK SPIONAGE I DANMARK

I december 2020 blev en herboende tyrkisk kvinde tiltalt for at have hjulpet eller sat en fremmed efterretningstjeneste i stand til at virke inden for den danske stat, jf. straffelovens § 108, stk. 1 (spionage). Kvinden er tiltalt for i 2016 at have sendt en mail til en central tyrkisk myndighed med navne på flere herboende personer, som hun oplyste var tilknyttet Gülen-bevægelsen. Fethullah Gülen er en tyrkisk imam, der er bosiddende i USA, og som af præsident Erdogan er anklaget for at stå bag kupforsøget i Tyrkiet i juli 2016. Retssagen mod kvinden er planlagt til at begynde i marts 2022.

Lignende sager har været fremme i andre europæiske lande, bl.a i Tyskland og Schweiz.

LIKVIDERINGSFORSØG MOD AFHOPPET RUSSISK EFTERRETNINGSOFFICER I SALISBURY

Den 4. marts 2018 blev en tidligere russisk efterretningsofficer, Sergei Skripal, og dennes datter forsøgt likvideret med nervegas i den britiske by Salisbury. De britiske myndigheder har vurderet, at det højst sandsynligt var den russiske militære efterretningstjeneste, GRU, der stod bag angrebet. Storbritannien reagerede ved at udvise ca. 20 diplomater ved den russiske ambassade i London. Flere vestlige lande fulgte Storbritanniens eksempel, heriblandt Danmark der udviste to russiske diplomater fra den russiske ambassade i København.

Angrebet på Skripal var ikke den første mulige russiske likvideringsoperation i Storbritannien. I 2006 døde den tidligere russiske efterretningsofficer Aleksandr Litvinenko efter at være blevet forgiftet med det radioaktive stof polonium 210. De britiske myndigheder har vurderet, at det var den russiske efterretningstjeneste FSB, der stod bag forgiftningen af Litvinenko.

DET FORFALSKEDE BREV

I november 2019 blev et forfalsket brev, der fremstod som en henvendelse fra Grønlands daværende landsstyremedlem for udenrigsanliggender til en amerikansk senator, delt på en række blogs og medier. Af brevet fremgik det bl.a., at den "grønlandske regering" snarest muligt ville organisere en folkeafstemning om uafhængighed fra Danmark, og at man fra grønlandsk side accepterede et amerikansk forslag om, at Grønland skulle have status som et organiseret alliancefrit territorium. Det er meget sandsynligt, at brevet blev fabrikeret og formidlet på internettet af russiske påvirkningsaktører, der ville skabe forvirring og mulig konflikt i forholdet mellem Danmark, USA og Grønland.

Kina, Rusland, USA samt flere europæiske lande har i stigende grad geostrategiske, sikkerhedspolitiske og økonomiske ambitioner i Arktis og Nordatlanten. Nogle af disse lande konkurrerer om bl.a. adgang til ressourcer, søruter, forskning og militært vigtige positioner. Færøerne og Grønland er geografisk placeret på strategisk vigtige områder for skibe, ubåde og fly, der passerer mellem Arktis og Nordatlanten, og Grønland er samtidig hjemsted for den amerikanske Thulebase, der udgør et centralt knudepunkt i USA's missilvarslings- og missilforsvarssystem. Hertil kommer, at der blandt stormagterne er en interesse for de ressourcer, der befinder sig i den grønlandske undergrund.

Det er på denne baggrund PET's vurdering, at der er en trussel fra både kinesisk og russisk efterretningsvirksomhed, særligt i form af påvirkningsvirksomhed og spionage, der bl.a. kan udføres via cyberangreb, mod visse danske, færøske og grønlandske myndigheder, beslutningstagere, virksomheder og forskningsinstitutioner. PET vurderer, at Kina og Rusland bl.a. er interesserede i at indhente oplysninger om militære, politiske og økonomiske forhold, Rigsfællesskabets og de enkelte rigsdeles positioner i internationale drøftelser og forskning med militær, politisk eller økonomisk betydning.[3] Derudover har Kina og Rusland interesse i at vanskeliggøre USA og andre vestlige staters position på Færøerne og i Grønland.

Rigsfællesskabet er særligt sårbart i det omfang, at kinesiske eller russiske efterretningstjenester kan udnytte kontroversielle emner til at forsøge at skabe spændinger i eller mellem de tre rigsdele eller problematisere forholdet til allierede, særligt USA.

For lande som Kina og Rusland vil internationalt samarbejde, investeringer og samhandel undertiden kunne have geostrategiske eller sikkerhedspolitiske formål, der rækker ud over de interesser, som disse lande officielt fremhæver som årsager til samarbejdet. F.eks. vil visse former for investeringer og samarbejde, der involverer kritisk infrastruktur, herunder infrastruktur der kan bruges til både civile og militære formål (såkaldt *dual-use* infrastruktur), undertiden kunne have efterretningsmæssige eller militære formål.

Det er PET's vurdering, at der kan være risici forbundet med visse former for internationalt samarbejde og omfattende investeringer og samhandel med Kina og Rusland, da sådanne aktiviteter efter omstændighederne vil kunne gøre Færøerne og Grønland mere sårbare overfor spionage og påvirkningsaktivitet.

PET kan konstatere, at mange kinesiske virksomheder er delvist ejet af den kinesiske stat eller på andre måder er under den kinesiske stats kontrol, selvom virksomhederne formelt set er private. Det er derfor vanskeligt at lave en klar skelnen mellem statslige og private aktiviteter, som det kendes for vestlige aktører.

3) *Se Forsvarets Efterretningstjenestes 'UDSYN 2021'.*

Danmarks diplomatiske repræsentationer i udlandet og tilrejsende delegationer fra Danmark, heriblandt erhvervsdelegationer, er udsatte mål for fremmede staters efterretningsvirksomhed. I kraft af deres beliggenhed i udlandet er de diplomatiske repræsentationer særligt sårbare. Hertil kommer, at Danmarks diplomatiske repræsentationer er i besiddelse af mange oplysninger, der kan være af interesse for fremmede stater, og at repræsentationerne kan blive brugt som "indgang" til at udføre spionage mod myndigheder og virksomheder i Danmark.

Fremmede efterretningstjenester har tradition for at operere i de diplomatiske miljøer rundt om i verden. En række fremmede efterretningstjenester udstationerer efterretningsofficerer på diplomatiske repræsentationer og i internationale organisationer, hvor de arbejder under dække af at være diplomater. På den måde færdes fremmede staters efterretningsofficerer ofte i de samme miljøer som almindelige diplomater. Eksempelvis kan en dansk diplomat udstationeret i et vesteuropæisk land risikere at blive kontaktet af en russisk diplomat, som i virkeligheden er en trænet efterretningsofficer.

Der er i en række lande en skærpet trussel fra de lokale efterretningstjenester mod dansk diplomatisk tilstedeværelse. Det drejer sig først og fremmest om autoritære stater, hvor de lokale efterretningstjenester har meget vide retlige, politiske og tekniske muligheder for at gennemføre forskellige indgreb, såsom ransagning af hotelværelser eller diplomatboliger, aflytning af tele- og datatrafik eller fysiske tilbageholdelser. Truslen kan også være rettet mod danskere, der opholder sig i udlandet for at arbejde, forske eller studere.

I nogle lande er det en udbredt praksis, at de lokale efterretningstjenester jævnligt kontakter lokaltansat personale på diplomatiske repræsentationer med henblik på at rekruttere dem eller på anden vis bruge dem til at skaffe adgang til oplysninger fra repræsentationen. Kontakten til den lokalansatte kan ske direkte eller indirekte, og de lokalansatte kan enten samarbejde frivilligt med den lokale efterretningstjeneste eller blive udsat for forskellige former for pression, der undertiden også kan omfatte pression mod familiemedlemmer.

Danske diplomater og danskere, der f.eks. opholder sig i udlandet for at arbejde, forske eller studere, kan også blive udsat for forskellige former for hvervningsforsøg.

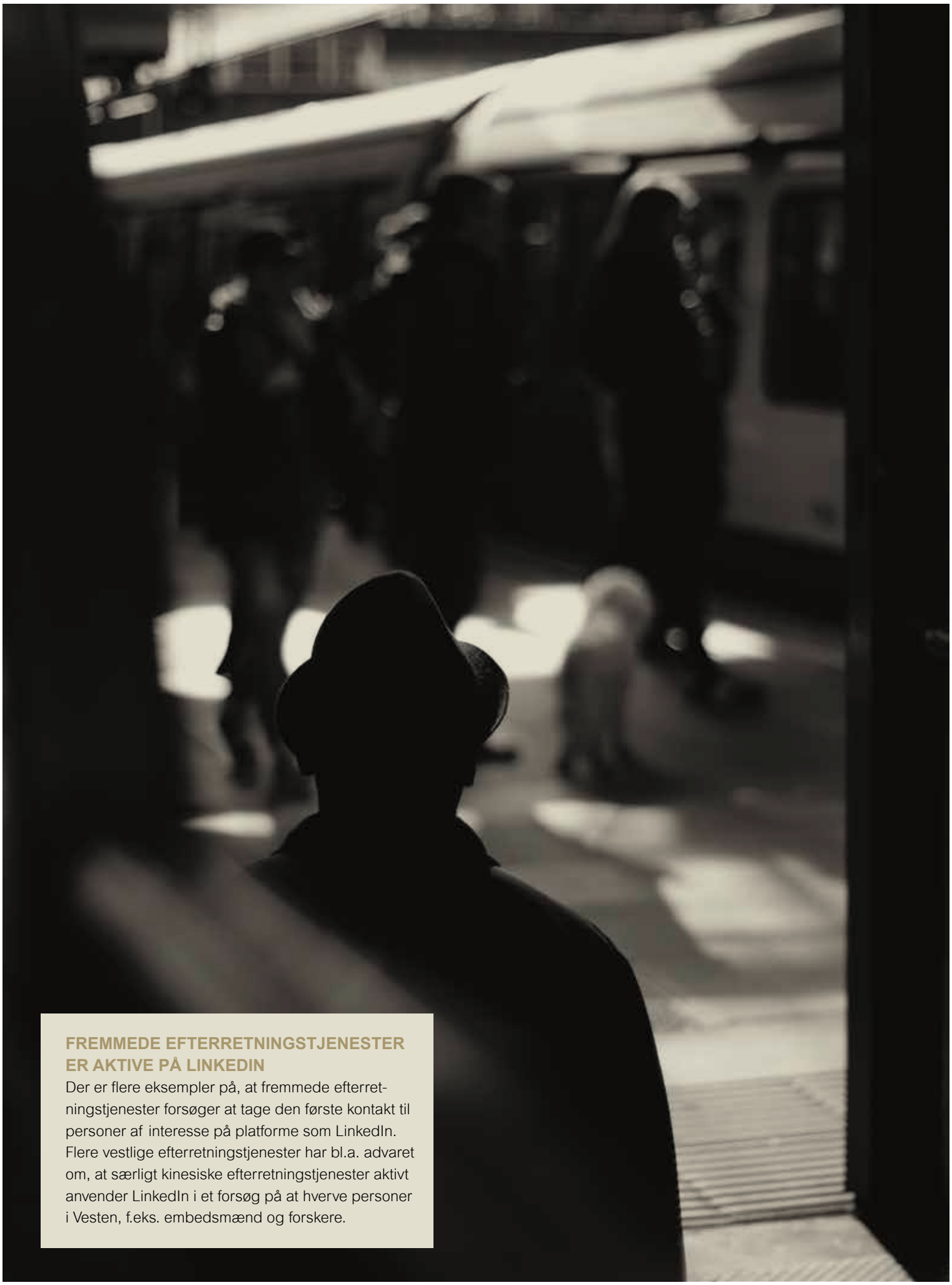
Der er eksempler på, at lokale efterretningstjenester i visse lande, herunder i Rusland og Kina, udøver forskellige former for chikane mod diplomater og lokalansatte ved diplomatiske repræsentationer, f.eks. ved at ransage boliger eller at foretage åbenlys fysisk overvågning. Formålet med sådan chikane er ofte at intimidere det diplomatiske personale og begrænse den diplomatiske aktivitet. Der er eksempler på, at fremmede efterretningstjenester har øget deres aktiviteter mod udenlandske diplomater, herunder udført mere åbenlys chikane, i perioder, hvor der har været en nedkøling af relationerne mellem de involverede stater. PET vurderer, at tilrejsende delegationer også kan blive udsat for chikane.

NATO UDVISTE OTTE RUSSISKE EFTERRETNINGSOFFICERER

Den 6. oktober 2021 udviste NATO otte medlemmer af den russiske delegation ved NATO. Udover at fjerne akkrediteringen fra de otte diplomater blev antallet af stillinger, som Rusland fremover kan modtage akkreditering til i NATO, halveret til ti. Ifølge NATO var de otte udviste russiske delegationsmedlemmer i virkeligheden efterretningsofficerer, der arbejdede under dække af at være diplomater.

LOKALANSAT MEDARBEJDER VED DEN BRITISKE AMBASSADE MISTÆNKT FOR SPIONAGE TIL FORDEL FOR RUSLAND

I august 2021 meddelte den tyske føderale anklagemyndighed, at en 57-årig britisk statsborger var blevet anholdt for mistanke om at have virket som agent for en russisk efterretningstjeneste. Den britiske statsborger var på anholdelsestidspunktet ansat som sikkerhedsvagt på den britiske ambassade i Berlin. Den anholdte skal hen over en længere periode have leveret klassificerede dokumenter mod kontantbetaling til en russisk efterretningsofficer.



FREMMEDE EFTERRETNINGSTJENESTER ER AKTIVE PÅ LINKEDIN

Der er flere eksempler på, at fremmede efterretningstjenester forsøger at tage den første kontakt til personer af interesse på platforme som LinkedIn. Flere vestlige efterretningstjenester har bl.a. advaret om, at særligt kinesiske efterretningstjenester aktivt anvender LinkedIn i et forsøg på at hverve personer i Vesten, f.eks. embedsmænd og forskere.

04

HVORDAN SPIONERER FREMMEDE EFTERRETNINGSTJENESTER MOD DANMARK?

Fremmede stater benytter sig typisk af spionage for at opnå viden eller skabe en situation, der kan styrke deres egen position eller sikkerhed. Det kan eksempelvis være i forhandlinger, i en konkurrencesituation, under en krise eller i en konflikt. De fremmede staters efterretningstjenester er professionelle modstandere, der ofte har mange ressourcer til rådighed og løbende udvikler nye måder at indhente oplysninger på. Fremmede staters efterretningsaktiviteter bliver i nogle tilfælde planlagt og gennemført med en lang tidshorisont. Ofte anvender efterretningstjenesterne en kombination af fremgangsmåder, eksempelvis brug af en menneskelig kilde kombineret med indhentning via cyberangreb.

Den menneskelige kilde

Fremmede efterretningsofficerer arbejder bl.a. under dække af at være diplomater, journalister eller forskere, og de er trænede i at udvælge og opbygge fortrolige kontakter til personer, som typisk kan give dem adgang til klassificerede og beskyttelsesværdige informationer. Efterretningsofficerer søger typisk efter informationer om personer af interesse for efterretningstjenesten på åbne medier, hvor der ofte ligger mange oplysninger frit tilgængeligt. På de sociale medier kan en efterretningsofficer eksempelvis tit finde oplysninger om en persons arbejde, familiesituation, fritidsinteresser eller lignende. Denne viden kan efterretningsofficeren bruge til at skabe den første kontakt til en person, som han/hun måske har interesse i at hverve som kilde.

En efterretningsofficer vil ofte forsøge at tilnærme sig en person af interesse i forbindelse med offentlige begivenheder, såsom konferencer. I begyndelsen vil efterretningsofficeren kommunikere med sin kontakt på en åben måde og kun stille "ufarlige" og konverserende spørgsmål. Men hvis efterretningsofficeren vurderer, at kontakten har potentiale til eventuelt at kunne blive hvervet som kilde, vil efterretningsofficeren efterhånden varetage forbindelsen mere skjult. Herefter vil møder ikke længere blive aftalt over telefonen eller foregå ved større officielle begivenheder, men derimod under mere diskrete former, eksempelvis på en restaurant eller en bar. Efterretningsofficeren vil langsomt begynde at spørge ind til fortrolige emner. Hvis efterretningsofficeren vurderer, at kontakten har "potentiale", vil officeren på et tidspunkt gå skridtet videre og forsøge at hverve kontakten – eksempelvis ved at tilbyde økonomisk kompensation og/eller ved afpresning f.eks. ved viden om ægteskabelige sidespring eller økonomiske problemer. Men da hvervning er en tidskrævende og risikabel proces, har efterretningsofficerer typisk mange fortrolige kontakter, og kun få hvervede kilder. En fortrolig kontakt er ikke nødvendigvis vidende om, at han/hun i virkeligheden mødes med en fremmed efterretningsofficer.

Fremmede efterretningstjenester kan også bruge mellemmænd til at skaffe de ønskede oplysninger. PET kan konstatere, at eksempelvis virksomheder eller lobbyister bliver hyret og herefter anvendt til at fremskaffe oplysninger til aktører, der er tilknyttet en fremmed efterretningstjeneste. De pågældende virksomheder eller lobbyister er ikke altid vidende om, at de informationer, de fremskaffer til deres kunder, bliver viderebragt til en fremmed efterretningstjeneste.

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.

Brug af cyberangreb

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. Der kan også være tale om destruktive cyberangreb eller forberedelse heraf, hvis primære formål er sabotage af en myndighed, institution eller virksomhed.[4]

Cyberspionage er på mange måder en attraktiv fremgangsmåde for fremmede efterretningstjenester, da denne form for spionage er forbundet med lav risiko og ofte kan udføres uden at efterlade særligt synlige spor. Hertil kommer, at cyberspionage kan udøves fra hjemlandet uden fysisk tilstedeværelse eller kontakt til en menneskelig kilde i det ramte land. Samtidig kan succesfuld cyberspionage give adgang til meget store mængder data.

4) *For yderligere se 'Cybertruslen mod Danmark 2021', Center for Cybersikkerhed*

Aflytning af tele- og datatrafik

Fremmede efterretningstjenester udvikler løbende deres kapacitet til at aflytte tele- og datatrafik. Kapaciteterne omfatter bl.a. overvågning af elektronisk kommunikation, der strækker sig fra eksempelvis mobilsamtaler, sms'er og e-mails til radiokommunikation. Den form for aflytning forudsætter ikke nødvendigvis fysisk tilstedeværelse i Danmark. PET vurderer, at det især er visse politikere og embedsmænd, der er prioriterede mål for fremmede efterretningstjenesters aflytningsaktiviteter.

05

ULOVLIG ANSKAFFELSESVIRKSOMHED

PET vurderer, at en række stater er involveret i ulovlig anskaffelsesvirksomhed ved på ulovlig vis at forsøge at anskaffe eller omdirigere produkter fra Danmark for at anvende dem i egen våbenproduktion eller i militære programmer. Truslen er særligt rettet mod virksomheder og forskningsinstitutioner, der leverer produkter, viden eller tjenesteydelser, som disse stater har brug for til opbygning af deres militære formåen.

PET arbejder aktivt for at modvirke og bekæmpe ulovlig anskaffelse af produkter, teknologi og viden fra Danmark. PET's indsats på området er bl.a. reguleret i straffeloven, ved kontrollister eller sanktioner fastsat i f.eks. EU-forordninger og ved særlovgivning.

PET vurderer, at stater som Rusland, Kina, Iran, Pakistan, Nordkorea og Syrien ulovligt forsøger at anskaffe eller omdirigere danske produkter og teknologi for at anvende dem i egen våbenproduktion eller militære programmer. Det er også PET's vurdering, at fremmede efterretningstjenester medvirker til at støtte den ulovlige anskaffelsesvirksomhed. Det sker bl.a. ved at bidrage til at identificere relevante danske firmaer og/eller ved, at tjenesterne via deres kontakter og netværk bidrager til at sende produkter til militæret i deres hjemlande.

Ulovlig anskaffelsesvirksomhed kan bl.a. ske ved, at danske virksomheder eksporterer produkter eller leverer teknisk bistand, der via mellemmænd ender i de forkerte hænder. Det kan ofte være svært at opdage, at modtageren af et produkt samarbejder med militæret i et andet land, da den reelle modtager ofte vil forsøge at skjule sig bag dækvirksomheder. Ulovlig anskaffelsesvirksomhed kan også ske ved, at produkter fra Danmark sendes til mellemdestinationer, før de havner hos den reelle modtager, eller ved at forskere i god tro overfører viden fra forskningsinstitutioner i Danmark til forskningsmiljøer, der bidrager til opbygningen af andre landes våbenprogrammer.

Hvis dansk forskning eller teknologi uretmæssigt ender hos visse fremmede stater, kan det udgøre en trussel mod danske arbejdspladser, eksport- og forsvarsinteresser, og i værste fald også udgøre en trussel mod dansk sikkerhed.

På eksportkontrolområdet er Rigspolitiet ansvarlig myndighed for udførsler af våben og militært udstyr, mens Erhvervsstyrelsen er ansvarlig myndighed for udførsler af udstyr, der både kan anvendes civilt og militært (dual-use). PET indgår sammen med en række andre myndigheder i det nationale arbejde med eksportkontrol på dual-use-området. PET undersøger, om tjenesten har kritiske oplysninger om bl.a. de virksomheder, myndigheder, personer og produkter, der indgår i handlerne, herunder om der er mistanke om omdirigering eller urigtige oplysninger i forbindelse med, hvem der er den reelle endelige bruger af produktet.

TYSK-IRANSK FORSKER VED NORSK UNIVERSITET TILTALT FOR BRUD PÅ EKSPORTKONTROLREGLER

I september 2021 blev en tysk-iransk forsker ved et norsk universitet tiltalt for at medvirke til hacking af universitetets datasystem, der indeholder information, som er underlagt eksportkontrol. Forskeren er også tiltalt for at videregive oplysninger om norsk forsvarsmateriel til en gruppe iranske gæsteforskere og for at give dem adgang til universitetets laboratorier uden at indhente de nødvendige tilladelser fra det norske udenrigsministerium eller orientere universitetets ledelse.

06

UDENLANDSKE DIREKTE INVESTERINGER

Udenlandske investeringer er grundlæggende gode for erhvervslivet og til gavn for det danske samfund. Visse udenlandske investeringer kan dog være en trussel mod den nationale sikkerhed og offentlige orden.

Ved udenlandske direkte investeringer forstås erhvervelse af kontrol eller betydelig indflydelse i en virksomhed eller enhed hjemmehørende i Danmark ved direkte eller indirekte besiddelse af eller kontrol over ejerandele eller stemmerettigheder i virksomheden eller tilsvarende kontrol ved andre midler, herunder køb af aktiver og langfristede lån.

De sikkerhedsmæssige konsekvenser kan være alvorlige og skal ses i sammenhæng med fremmede aktørers interesser i Danmark. Det knytter sig især til teknologiske, økonomiske, politiske og militære forhold.

Derfor har Danmark og en række allierede lande i de seneste år styrket den sikkerhedsmæssige indsats omkring udenlandske investeringer. En fælles europæisk screeningsordning trådte i kraft den 11. oktober 2020. Den 1. juli 2021 trådte en dansk investeringsscreeningslov i kraft med anvendelse pr. 1. september 2021.

PET er involveret i det nationale arbejde med investeringsscreening for at belyse, hvorvidt der er en trussel forbundet med visse udenlandske direkte investeringer. Arbejdet omfatter bl.a. undersøgelser af, om tjenesten har kritiske oplysninger om de personer, virksomheder og andre entiteter, som investeringen omhandler, herunder om der er tale om urigtige oplysninger.

07

BILAG 1

PET'S LOVGRUNDLAG VEDRØRENDE SPIONAGE OG PÅVIRKNING

Bestemmelserne om spionage og påvirkning fremgår af straffelovens §§ 107-109:

§ 107
Den, som i fremmed magts eller organisations tjeneste eller til brug for personer, der virker i sådan tjeneste, udforsker eller giver meddelelse om forhold, som af hensyn til danske stats- eller samfundsinteresser skal holdes hemmelige, straffes, hvad enten meddelelsen er rigtig eller ej, for spionage med fængsel indtil 16 år.

Stk. 2
Såfremt det drejer sig om de i § 109 nævnte forhold, eller handlingen finder sted under krig eller besættelse, kan straffen stige indtil fængsel på livstid.

§ 108
Den, som, uden at forholdet falder ind under § 107, i øvrigt foretager noget, hvorved fremmed efterretningstjeneste sættes i stand til eller hjælpes til umiddelbart eller middelbart at virke inden for den danske stats område, herunder samarbejde om at udøve påvirkningsvirksomhed med henblik på at påvirke beslutningstagning eller den almene meningsdannelse, straffes med fængsel indtil 6 år.

Stk. 2
Såfremt det drejer sig om efterretninger vedrørende militære anliggender, eller virksomheden finder sted under krig eller besættelse, kan straffen stige indtil fængsel i 12 år. Det samme gælder, hvis påvirkningsvirksomheden efter stk. 1 udøves i forbindelse med de valg og stemmeafgivninger, der er omfattet af § 116.

§109
Den, som røber eller videregiver meddelelse om statens hemmelige underhandlinger, rådslagninger eller beslutninger i sager, hvorpå statens sikkerhed eller rettigheder i forhold til fremmede stater beror, eller som angår betydelige samfundsøkonomiske interesser over for udlandet, straffes med fængsel indtil 12 år.

Stk. 2
Foretages de nævnte handlinger uagtsomt, er straffen bøde eller fængsel indtil 3 år.

POLITIETS EFTERRETNINGSTJENESTE
VURDERING AF SPIONAGETRUSLEN MOD DANMARK
UDGIVET 2022

FOTOS FRA UNSPLASH:
SIDE 2 OG 4: KRISZTIAN TABORI
SIDE 9: NATHAN DUMLAO
SIDE 22: DAVID SINCLAIR
SIDE 24: MATHEW SCHWARTZ
SIDE 27: MICHAEL LONGMIRE
ALLE ØVRIGE: ADOBE STOCK

POLITIETS EFTERRETNINGSTJENESTE
KLAUSDALSBROVEJ 1
2860 SØBORG
45 15 90 07 • PET@PET.DK • WWW.PET.DK