Trusselen fra statlige aktører

Politiets sikkerhetstjeneste. Den sentrale enhet. Postadresse: Postboks 4773 Nydalen, 0421 Oslo
Besøksadresse: Nydalen allé 35 0484 Oslo. Telefon: 23 30 50 00, Faks: 23 30 51 20
Epost: post@pst.politiet.no, www.pst.no

Har du eller din virksomhet kunnskap, teknologi eller informasjon som andre stater ikke bør få tak i?

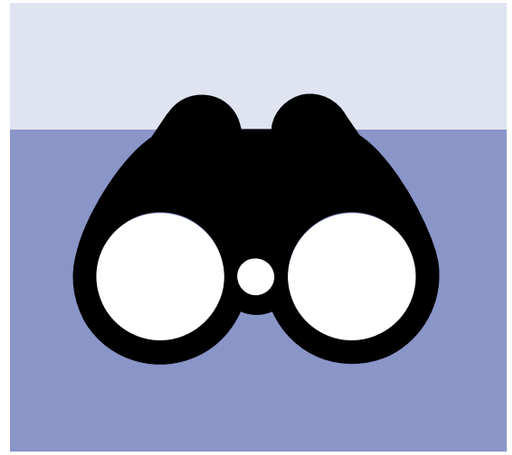
Norge utsettes daglig for etterretningsvirksomhet fra flere land. Dette kan være svært skadelig for våre økonomiske, politiske og sikkerhetsmessige interesser. Slik etterretningsaktivitet kan også rettes mot deg og din virksomhet. PST skal beskytte nasjonens sikkerhet og selvstendighet mot trusler utført av fremmede stater. I dette oppdraget ligger det at vi skal forebygge og etterforske ulovlig etterretningsaktivitet fra statlige aktører. Vi skal også forebygge og etterforske brudd på eksportkontrollregelverket og hindre spredning av masseødeleggelsesvåpen. For å lykkes i dette arbeidet er PST avhengig av hjelp fra ulike samfunnsaktører, bedrifter, organisasjoner og enkeltpersoner.

I denne brosjyren presenterer vi gjennom eksempler etterretningsaktivitet fra statlige aktører som du og din virksomhet kan utsettes for, og råd om risikoreduserende tiltak. Vi håper dette kan bidra til at dine verdier identifiseres og beskyttes.

Statlig etterretningsvirksomhet

Fremmede stater utøver etterretningsaktivitet mot Norge med formål om å påvirke eller skaffe informasjon om politiske, militære eller andre forhold av samfunnsmessig betydning. Dette kan styrke eget lands posisjon og ambisjoner, og skade norske interesser.

Flere lands etterretningstjenester har blant annet i oppgave å understøtte virksomhet som kan styrke egen forsvarsevne og bidra til utvikling av egen sivil og militær teknologi. Andre sentrale oppgaver kan være å innhente informasjon om infrastruktur og politiske beslutningsprosesser. Avsløringer viser også hvordan flere stater benytter etterretningstjenestene til å sikre fremtidig tilgang på energi og naturressurser, og dermed trygge egne nasjonale interesser og økonomiske forhold.



Det er viktig å påpeke at ikke alle land i verden har et like tydelig skille mellom politikk, kommersielle interesser og etterretningstjenester som vi har i Norge.

Etterretningsoffiserer som opererer i Norge utøver sin aktivitet under dekke av å være diplomater, journalister, næringsdrivende, tilreisende teknologer og akademikere. Slik fordekt virksomhet omtales ofte som spionasje, men kan mer presist beskrives som etterretningsoperasjoner. Etterretningsoffiserer benytter seg av metoder som relasjonsbygging og kultivering, men ofte også mer alvorlige metoder som bestikkelser, nettverksoperasjoner og utpressing. Fremmede stater kan også plassere – eller utnytte – ansatte med tilgang til skjermingsverdig informasjon, til å utføre oppdrag på deres vegne.

Utstasjonerte etterretningsoffiserer i Norge vier mye tid til å påvirke politiske beslutningsprosesser og innhente sensitiv sivil og militær informasjon. De søker gjerne kontakt med ledere og ansatte i utvalgte statlige og private bedrifter og organisasjoner for å få tilgang til e-postadresser, kontaktregistre og telefonnummer. Slik informasjon vil kunne utnyttes til å gjennomføre styrte datanettverksoperasjoner, hvilket PST har registrert en betydelig økning av i Norge de siste årene.

Vår digitale verden har ikke gjort spionen overflødig, tvert i mot; Datanettverk, digital lagring og åpne kilder (inkludert internett og sosiale medier) har økt tilfanget av spionens verktøy.

PST vet at alle innhentingsmetodene benyttes aktivt av statlige aktører i deres etterretningsaktivitet, også ved nordmenns reiser i utlandet.

Informasjonen du eller din virksomhet besitter og har tilgang til kan ha stor verdi for andre stater!

Er du et mål for fremmed etterretning?

Tenk igjennom følgende:

- Hva er dine og din virksomhets verdier?
- Har du verdier som kan være interessante for andre?
- Hvilke verdier må beskyttes?
- Hvilke sårbarheter kan utnyttes?
- Hvordan vil dine verdier kunne rammes?
- Kan enkelte ansatte være særlig sårbare for trusler og press?
- Hvilke konsekvenser vil det ha at andre får tak i dine verdier?

Relevant informasjon finnes bl.a i PST og Etterretningstjenestens årlige, ugraderte vurderinger.

Case

STATLIG ETTERRETNINGSVIRKSOMHET

En stortingspolitiker fra et opposisjonsparti kommer i snakk med en utenlandsk diplomat under et utenrikspolitisk seminar. Et par uker senere inviteres politikeren på lunsj av diplomaten. Lunsjen følges opp med flere møter over en lengre periode. Diplomaten ber politikeren om kopi av ugraderte dokumenter fra Stortinget. Han ber også stortingspolitikeren om å legge til rette for møter med ledelsen i partiet. Hva tror du diplomaten ønsker å oppnå med denne kontakten?

PST vet at diplomaten var en utstasjonert etterretningssoffiser under dekke og har tatt kontakt med politikeren. Kan det samme skje deg? Kan din arbeidsplass og din posisjon være et attraktivt mål for statlig etterretningsvirksomhet?

Mistenker du at din virksomhet eller dine kollegaer kan ha vært utsatt for andre staters etterretningsvirksomhet? Ta kontakt med PST.

Flyktningspionasje

Etterretningsvirksomhet benyttes også til å kartlegge og svekke dissidenters støtte til opposisjonell virksomhet i hjemlandet. Dette kalles flyktningspionasje. Formålet med slik etterretningsvirksomhet er hovedsakelig å sikre territoriell integritet.

PST har avdekket at enkelte lands myndigheter spionerer på egne borgere som oppholder seg lovlig i Norge. Dette kan være asylsøkere, flyktninger eller andre personer som hjemlandets myndigheter er interessert i. Informasjonen som søkes er ofte knyttet til personens aktiviteter eller identifisering av dissidenter og opposisjonelle.

Denne typen etterretningsvirksomhet kan bli utført av andre flyktninger som opererer i en dobbeltrolle, av tilreisende eller av personer knyttet til det aktuelle landets ambassade. PST er kjent med eksempler der det er blitt overlevert informasjon om borgere i Norge til hjemlandets myndigheter. Dette er hovedsakelig totalitære regimer eller land med sterkt behov for å kontrollere informasjon om eget land og borgere.

Flyktningspionasje kan være til stor skade for personen som utsettes for aktiviteten, deres slektninger, venner og bekjente i hjemlandet.

I ytterste konsekvens kan det føre til negative konsekvenser for personens liv og helse, økonomi, frihet og eiendom i Norge eller utlandet. Informasjonen kan også brukes aktivt for å fengsle opposisjonelle i aktuelle land, hindre meningsytringer og unngå kritikk av et sittende regime.

Vær bevisst på at andre stater kan legge press på deg eller ansatte i din virksomhet. Etater, institusjoner og organisasjoner som befatter seg med asylsøkere og flyktninger fra totalitære regimer bør være særlig oppmerksomme.

Case

FLYKTNINGSPIONASJE

En ung mann flyktet fra et totalitært regime i Midt-Østen. Familien ble igjen i hjemlandet. Den unge mannen fortsatte med sin regimekritikk etter at han kom til Norge, blant annet gjennom bruk av sosiale og tradisjonelle medier. Med familien som pressmiddel ble vedkommende tvunget til å møte representanter for hjemlandets myndigheter i Norge flere ganger. Disse personene presset mannen til å gi fra seg informasjon, som trolig førte til at andre personer i hjemlandet ble arrestert og fengslet.

Mistenker du at noen du kjenner kan ha vært utnyttet av andre staters etterretningsvirksomhet? Ta kontakt med PST.

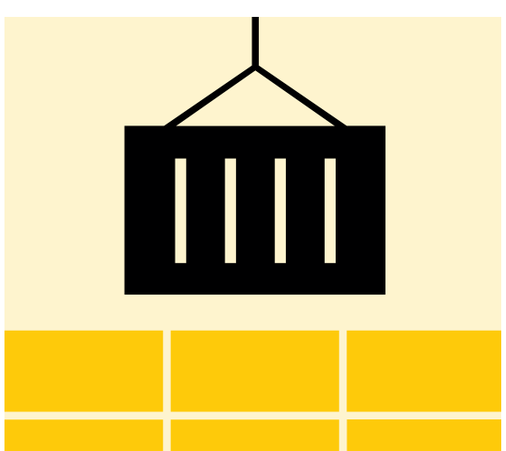
Ikke-spredning

Hva er det du eksporterer?
Og til hvem?

Mange norske virksomheter og utdanningsinstitusjoner produserer eller videreformidler varer, teknologi, tjenester og kunnskap som kan benyttes både sivilt og militært. Visste du for eksempel at vanlige produkter som visse former av stål og aluminiumslegeringer, enkelte typer ventiler, vakumpumper, metallpulver og maskinutstyr kan benyttes i utviklingen av masseødeleggelsesvåpen? Slike produkter omtales ofte som flerbruksvarer.

PST vet at enkelte stater forsøker å anskaffe flerbruksvarer og tilhørende kompetanse til bruk i utvikling av masseødeleggelsesvåpen. Dette gjøres hovedsakelig på fordekte måter, for eksempel via opprettelse av falske frontfirmaer og alternative fraktruter i forsøk på å skjule sluttbruker.

Også norske virksomheters samarbeid med selskaper i andre land kan benyttes og utnyttes for å legitimere anskaffelsesforsøket. Det er derfor viktig at din virksomhet er bevisst på at dere kan være utsatt for slik aktivitet, og at dere iverksetter tiltak som sikrer at virksomheten ikke bidrar til spredning av masseødeleggelsesvåpen.



Case

IKKE-SPREDNING

En norsk produsent av navigasjonssystemer mottar en forespørsel fra en ny europeisk kunde som ønsker å videreeksportere produsentens varer til Asia. Eksporten gjelder en flerbruksvare som ligger like under terskelen for hva som utgjør eksportkontrollerte varer. Varens spesifikasjoner tilsier allikevel at den kan benyttes til å stabilisere missiler som bærer masseødeleggelsesvåpen.

Åpent tilgjengelig informasjon viser at kunden har et omfattende internasjonalt nettverk og at varen skiller seg ut fra kundens ordinære virksomhet. Hvilke tiltak ville du iverksatt for å få mer kunnskap om hva varen du eksporterer faktisk skal benyttes til, og av hvem?

Ta kontakt med Utenriksdepartementet hvis du har tekniske og juridiske spørsmål knyttet til eksportkontrollregelverket. www.eksportkontroll.no / 23 95 06 50.
Ta kontakt med PST hvis du mottar mistenkelige henvendelser.

Gjennomfør en egenvurdering på hvorvidt varen din virksomhet eksporterer kan brukes til utvikling og produksjon av masse-ødeleggelsesvåpen.

Vær oppmerksom på tegn som kan tyde på at din virksomhet bidrar til ulovlige an-skaffelser. Forespørsler som er avvikende når det gjelder form og innhold kan indikere dette. Eksempler kan være:

- Det er usikkert hvem kunden egentlig er
- Kunden er motvillig til å gi opplysninger om sluttbruker og/eller sluttbruk
- Kunden har svært liten kunnskap om produktet
- Det er uoverensstemmelse mellom varens funksjon og oppgitt anvendelse
- Et spedisjonsfirma, en havn eller et lager er oppgitt som destinasjon
- Uvanlige ønsker knyttet til emballasje, deklarering, betaling eller frakt
- Kjøper ber om uvanlig små eller store kvanta, eller produkter av uvanlig høy kvalitet i forhold til oppgitt bruk
- Ambassaden fra kundens hjemland involveres i kjøpsprosessen
- Kunden nøler når det gjøres oppmerksom på at varen er underlagt eksportkontroll eller når det bes om bedre dokumentasjon

Vær bevisst på at eksport av enkelte varer kan være lisenspliktig

Kunnskapsoverføring

PST vet at stater underlagt internasjonale sanksjoner ønsker å utvikle egen teknologi som blant annet kan benyttes til produksjon av masseødeleggelsesvåpen. Vet du hvordan kunnskapen og kompetansen til å utvikle denne teknologien innhentes?

Ett av verktøyene som benyttes er studenter og forskere. Disse sendes ut eller kontaktes i studieløpet for å innhente relevant kunnskap. Dette foregår blant annet ved universiteter og forskningsinstitutter i Norge.

Hvilke fagområder tror du inneholder kunnskap som kan benyttes i utviklingen av masseødeleggelsesvåpen og deres leveringsmidler?

1. Materialteknologi
2. Kjemi
3. Matematikk
4. Biologi
5. Elektronikk

Svar: Alle fagområdene kan på høyere grads nivå inneholde tematikk som kan være relevant for utvikling av masseødeleggelsesvåpen. Et slikt arbeid krever kunnskap og erfaring innen et bredt spekter av fagområder, mange fler enn de som er listet opp på denne siden. Det er viktig at alle universiteter, høyskoler og forskningsinstitutter gjør en egenvurdering av hvorvidt fag som tilbys og forskning som utføres ved deres organisasjon er relevant for produksjon og bruk av masseødeleggelsesvåpen og deres leveringssystemer.

Case

KUNNSKAPSOVERFØRING

En utenlandsk student har søkt stilling ved et norsk universitet for å skrive en doktoravhandling om satellitt-teknologi, hvorav deler av teknologien er regulert i vedleggene til eksportkontrollforskriften. Temaet for avhandlingen er i utgangspunktet ordinær sivil teknologi, men har også relevans for utvikling av ballistiske missiler.

Studenten har bakgrunn fra et universitet i hjemlandet, og enkle undersøkelser i åpne kilder viser at dette universitetet kan være involvert i forskning og utvikling for organisasjoner tilknyttet militære enheter. Studenten har tidligere vært tilknyttet forskningsprosjekter med militær relevans.

Hva innebærer dette? Kan det være grunn til bekymring for at kunnskapen og nettverkene studenten vil tilegne seg vil kunne bli utnyttet til fordel for hjemlandets missilprogram? Hva kan universitetet gjøre?

Ta kontakt med Utenriksdepartementet hvis du har tekniske og juridiske spørsmål knyttet til eksportkontrollregelverket. www.eksportkontroll.no / 23 95 06 50.
Ta kontakt med PST hvis du mottar mistenkelige henvendelser.

Digital spionasje

Datanettverksbaserte etterretningsoperasjoner, eller digital spionasje, er én av flere etterretningsmetoder fremmede staters etterretningstjenester eller statstilknyttede grupperinger benytter seg av. Dette er en metode med stort potensiale innenfor informasjonsinnhenting, men som også kan benyttes til påvirkning eller sabotasjeformål.

De siste årene er en rekke forsøk på nettverksbaserte etterretningsoperasjoner mot mål i Norge blitt avslørt. PST vurderer at denne måten å drive ulovlig etterretningsvirksomhet på, vil bli en av våre største utfordringer på sikt.

Digital spionasje er mer kostnadseffektivt og mindre ressursskrevende enn andre etterretningsmetoder. En statlig aktør som benytter seg av slike metoder kan jobbe på tvers av landegrenser, og kan i tillegg hente ut store mengder informasjon raskere og mer diskret enn den tradisjonelle etterretningsoffiseren. Det tekniske potensialet metoden gir for å skjule ulovlig etterretningsaktivitet, og identitet, vurderes som fordelaktig fordi det er svært liten risiko for at en aktør blir avslørt.

Case

DIGITAL SPIONASJE

Ledelsen ved en norsk bedrift mottar e-post fra en tilsynelatende intern avsender. E-posten ser autentisk ut og omhandler informasjon om oppdaterte sikkerhetsrutiner for bruk av data og annet teknisk utstyr. Mottakerne av e-posten oppfordres til å åpne et vedlagt Word-dokument for detaljert informasjon om de nye rutinene. Mottakeren anmodes også om å trykke på lenken i e-posten for å oppdatere programvaren på maskinen som et ledd i de nye sikkerhetsrutinene.

- Er det trygt å åpne vedlegg eller linker når e-posten tilsynelatende kommer fra en intern avsender?
- Finnes det verdier eller skjermingsverdig informasjon i din virksomhets datasystemer?
- Gjør det noe om et konkurrerende selskap får tilgang til deres bedriftshemmeligheter og forhandlingsstrategier?

Mange tror at deres bedrift ikke har verdier som kan være av interesse for andre, og at digital spionasje derfor ikke er en reel problemstilling. En slik oppfatning endres raskt når bedriften taper sine konkurranse-fortrinn fordi en statlig aktør forer hoved-konkurrenten med bedriftssensitiv informasjon. Økt datasikkerhet trenger ikke å være dyrt, og med enkle tiltak er du og din virksomhet på god vei.

- Oppgradering av programvare. Nyere versjoner kommer ofte med flere sikkerhetsfunksjoner og færre sikkerhets-hull enn eldre utgaver.
- Blokkér kjøring av ikke-autoriserte programmer. En sluttbruker bør kun ha mulighet til å kjøre nødvendige programmer som virksomheten har forhåndsgodkjent.
- Ikke gi sluttbruker administratorrettigheter på lokal maskin. Dette vil gi system-administrator bedre oversikt, og slutt-brukerne vil kun få tilgang til de programmene og systemer de trenger.
- Etablér sentralisert logging og rutine for å fange opp uregelmessigheter, spesielt på innlogging til virksomhetenes e-post og VPN-løsninger.
- Bytt passord ofte, og ikke bruk samme passord på flere systemer/brukerkontoer.
- Sett i gang interne kampanjer og informer medarbeiderne om hvilke trusler som finnes. Med god kunnskap og økt årvåken-het blant de ansatte er man langt på vei.

På Nasjonal Sikkerhetsmyndighets (NSM) hjemmesider www.nsm.no, kan du lese mer om enkle tiltak din bedrift kan gjøre for å øke beskyttelsen mot dataangrep.

Nøkkelen til god datasikkerhet er økt kunnskap og godt samarbeid!

Generelle sikkerhetsråd

Gjør en grundig risiko- og sikkerhetsvurdering av deg og din virksomhet.
Kartlegg følgende:
- Virksomhetens verdier og konsekvens ved kompromittering eller bortfall.
- Hvilke sårbarheter kan utnyttes?
- Hvilke trusler kan virksomheten være utsatt for?
- Hvilke verdier må beskyttes?

Det finnes flere metoder for å gjennomføre en risikovurdering. Norsk standard 5832 beskriver en metode spesielt egnet for tilsiktede handlinger. Sikringshåndboka til Forsvarsbygg kan være et godt referanseverk for gjennomføring av tiltak.

Etablér en relevant grunnsikring basert på risikovurderingen.
Den kan inkludere fysiske barrierer, adgangskontroll, soneinndeling, aktive/passive sensorer, kameraovervåkning, og ekstra belysning ute og inne.

Utpek en sikkerhetsansvarlig, og sørg for at de ansatte er kjent med virksomhetens sikringstiltak og betydningen de har for beskyttelse av verdiene.

Sørg for at ansatte har kunnskap om og et bevisst forhold til mulige etterretningstrusler fra statlige aktører.
- Hvorfor er bedriften interessant for andre stater?
- Hvorfor må informasjon, teknologi og kunnskap beskyttes?

Etablér en god sikkerhetskultur i virksomheten.
- Sørg for at sensitiv informasjon ikke ligger åpent tilgjengelig.
- Etablér et bevisst forhold til hvilken informasjon som kan tas med utenfor arbeidsstedet, og hvordan informasjonen håndteres.
- Etablér retningslinjer for bruk av PC og mobiltelefon på reise til enkelte land.
- Opprett rutiner som sikrer rapportering av mistenkelige hendelser, trusler og sårbarheter.
- Lag rutiner for hvilken informasjon som skal legges ut på nettsider og vurdér sensitiviteten av innholdet.
- Vær bevisst på at andre stater kan legge press på ansatte.

Etablér gode rutiner for å hindre digital spionasje.
- Bytt passord ofte.
- Lag en sikkerhetspolicy for bruk av PC, nettbrett, mobiltelefoner og nettskyer.
- Innskrenk antall brukere med administratorrettigheter.
- Ha til enhver tid oppdatert programvare og anti-virusprogram.

Ønsker du mer informasjon:
Nasjonal sikkerhetsmyndighet /NorCERT
www.nsm.stat.no
NorSIS, www.norsis.no
Næringslivets sikkerhetsråd, www.nsr-org.no

Beskytt dine verdier

Har du spørsmål knyttet til brosjyrens innhold ber vi deg ta kontakt med PSTs seksjon for statlige aktører eller ditt lokale PST-kontor. www.pst.no