



YTTRANDE

Ju2017/07534/L5

2018-02-02

Justitiedepartementet

103 33 Stockholm

**Remissyttrande av betänkandet "Förstärkt skydd för uppgifter av betydelse för ett internationellt samarbete för fred och säkerhet som Sverige deltar i" (SOU 2017:70) från Utlandsspioneriutredningen**

Samarbete inom försvars- och säkerhetsområdet bygger på förtroende. Förtroende för hur vi hanterar information, kunnande och teknik. Röjande av känsliga uppgifter som hanteras inom ramen för ett internationellt samarbete kan skada Sveriges samarbete med andra länder eller organisationer och naturligen även skada Sveriges försvarsindustriella samarbeten.

Utredningen har korrekt beskrivit konsekvenserna för vår verksamhet. Obehörig underrättelseinhämtning kan leda till allvarliga negativa konsekvenser för samarbeten, för försvarsexport och för kostnadsdelning. Viktigt är, vilket dock utredningen inte betonat kanske för att det är självklart, att utbytet av teknik och innovationer negativt skulle påverkas. Teknikutbytet är idag helt avgörande för företagets konkurrenskraft och samarbetet bygger på förtroende att utländsk teknik, från främst USA, Storbritannien och Frankrike, inte kommer andra främmande makter till del. Företagens möjligheter att medverka i olika internationella sammanhang begränsas om inte det finns förtroende för att svenska staten har förmåga att begränsa riskerna att hemlig information kommer främmande makt till kännedom. Att skapa regelverk och medel som mottverkar och hanterar en undermålig förmåga att hantera informationssäkerhet, är därför av yttersta vikt. Därför är utredningens arbete av betydelse liksom Sveriges förmåga att beivra och lagföra brott.

**Utredningen**

Föreningen understryker betydelsen av att spionage inte begränsas till försvarspolitiskt motiverade handlingar utan att den även omfattar andra former av spionage, inte minst syftande till att påverka företagets innovationsförmåga. Det är angeläget att våra rättsvärdande myndigheter har effektiva och ändamålsenliga verktyg för att bekämpa denna brottslighet och kan vidta de åtgärder som krävs för att öka landets säkerhet.

Föreningen noterar avgränsningen till att skydda "Sveriges förhållande till annan stat eller mellanfolklig organisation" samt "bestraffa röjandet av hemliga uppgifter", dock har föreningen inte kompetens att värdera om nuvarande lagstiftning är otillräcklig eller effektiviteten hos åtgärderna.

Enligt betänkandet utgörs ett av de allvarligaste hoten mot svensk säkerhet, vid sidan av de militära, av elektroniska angrepp av teknisk avlyssning. Teknisk avlyssning erbjuder med den ökade digitaliseringen främmande makt fler möjligheter att spionera under längre tidsperioder. Utredningen utvecklar utförligt exempelvis hur främmande makts underrättelsetjänster verkar i eller via media (s. 229) och exemplet Aurora 17 illustrerar att det inte är lätt att skilja mellan nationella

och internationella skyddsintressen. Det bör därför understrykas att den analys som görs (s. 573) även noga beaktas i ett nationellt sammanhang där omfattningen av information som är av värde, samlat torde vara större än på enskilda utländska kontor, samt att cyberbaserad industrispionage inte är geografiskt begränsat varpå analysen (s. 573) även bör beaktas i andra relevanta utrednings-/lagstiftningsarbeten, som tex:

- [Utkontraktering av säkerhetskänslig verksamhet, sanktioner och tillsyn – tre frågor om säkerhetsskydd](#)
- [En ny säkerhetsskyddslag](#)
- [Förbättrat skydd för totalförsvarsverksamhet](#)
- [Nationell strategi för samhällets informations- och cybersäkerhet](#)

Kritiska frågeställningar i dessa utredningar som bör beaktas är att:

- Identifiera företag som anses vara särskilt kritiska för Sveriges totalförsvarsbehov såväl i fredstid som i tider av konflikt eller ökad beredskap. Identifiera nödvändiga åtgärder hur dessa företag ska skyddas, tex preventiva åtgärder att minska risken för spioneri, cyberattacker, underleverantörs beroenden/risker, samt även granskning av utländska minoritetsinvesteringar som ger insyn i företagen eller rena förvärv av dessa företag, etc.
- Bredda begreppen för skyddsvärda objekt, dvs även se till att samhällsviktiga verksamheter och innovationer inom strategiska teknikområden omfattas. Även här identifiera vilka preventiva, tillsyns och brottsutredningsmässiga åtgärder och resurser krävs för att möta hotbilden.
- Säkerställa att leverantörer av samhällsviktig verksamhet (exempelvis IT- och telekom, energi), gör nödvändiga och tillräckliga riskbedömningar som både beaktar de tekniska men även andra relevanta riskbedömningar (beroende ställning, risker i leverantörsvärdekedjan) av underleverantörer av känslig eller kritisk utrustning för spioneri.
- Göra avvägningen för behov av granskning av leverantörer av känsliga produkter, tjänster, samt utkontraktering till samhällsviktig verksamhet. Då både gällande offentliga inköp avsedda för offentlig sektorns nyttjande samt privata aktörers inköp av känsliga produkter, tjänster samt utkontraktering ämnade för samhällsviktig/kritisk verksamhet.

Robert Limmegård,



Generalsekreterare

Säkerhets- och försvarsföretagen