

Regeringskansliet  
Utrikesdepartementet  
Enheten för nedrustning och icke-spridning

103 33 Stockholm

Er referens  
UD2021/15100

FOI referens  
Mårten Sundmark

## Remissvar gällande Förstärkt kontroll av produkter med dubbla användningsområden (Ds 2021:32)

### Sammanfattning av Totalförsvarets forskningsinstituts (FOI) synpunkter

Totalförsvarets forskningsinstitut (FOI) konstaterar att den nya lagstiftningen ger en ökad kontroll och en ökad harmonisering inom EU. Det kan bidra till en ökad handel inom EU, medan länder utanför EU kan uppleva reglerna som handelshinder, vilket i sin tur skulle kunna få konsekvenser för svenska samarbeten utanför EU. För FOI kan detta specifikt innebära sämre möjligheter till internationella försvarsforsknings-samarbeten med organisationer utanför den Europeiska unionen.

FOI har – från de utgångspunkter myndigheten har att beakta – följande synpunkter och reflektioner på departementspromemorian.

### Disposition

Myndigheten har valt att dela upp synpunkterna enligt följande. Inledningsvis kommer ett avsnitt med fokus på cyberövervakningsprodukter, som följs av ett avsnitt om tekniskt bistånd. Därefter kommenterar FOI några av de förslag som framförs i skrivelsen, samt möjliga konsekvenser av dessa. Avslutningsvis görs några reflektioner om vad promemorian möjligen saknar.

### Utökning av kontrollområdet

#### Cyberövervakningsprodukter

Enligt förordningen art 2 (20) definieras cyberövervakningsprodukter som produkter som är särskilt konstruerade för att möjliggöra dold övervakning av fysiska personer genom monitorering, extraktion, inhämtning eller analys av data från informations- och telekommunikationssystem. Detta kan tolkas brett eller snävt beroende på läsaren.

Regelverk rörande skydd mot övervakning och insamling av data från individer hanteras idag inom EU, bland annat lagstiftningen rörande GDPR.

Produkter som befinner sig inom unionen ska i enlighet med den nya förordningen inte exporteras med mindre än att exportören kan visa att man uppfyller lagstadgat skydd avseende mänskliga rättigheter. Den fråga som behöriga myndigheter torde ha anledning att återkomma till är om företag, vars ursprungsländer saknar motsvarande integritetsskydd i sin lagstiftning, ska nekas tillstånd för export, eller kommer att nekas tillstånd utifrån exportörens ”due diligence”?<sup>1</sup> Gränsdragningen för exportörens undersökningsplikt är en frågeställning som kräver ytterligare beredning och eventuell praxisbildning.

Som en bakgrund kan noteras att de flesta programvaror idag som syftar till övervakning av information på nätet för extraktion och analys baseras på matematiska algoritmer. Flera av dessa algoritmer är öppet publicerade och allmänt tillgängliga, vilket innebär att personer med goda kunskaper i programmering eller matematik kan förstå och tillämpa algoritmerna och därmed, tillsammans med programmerare, skapa olika typer av programvaror där de allmänt tillgängliga algoritmerna utgör kärnfunktionen. Sådana programvaror kan naturligtvis vara tillämpbara på olika nivåer – en del kan hantera stora mängder data, medan andra fungerar mer uppsökande. Flera varianter av denna typ av programvaror används i militära eller polisiära funktioner över hela världen.

Otydligheterna i definitionen av begreppet informations- och telekommunikationssystem kan också ge upphov till frågeställningar om när detta ska användas. Enligt förordningens art 5 krävs tillstånd om exportören har informerats av behörig myndighet eller om exportörens egen undersökningsplikt visar att det finns risk för användning i samband med internt förtryck och/eller för att begå allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt. Frågan är, återigen, hur långt exportörens undersökningsplikt sträcker sig? Mjukvarubaserade säkerhetssystem som övervakar information och personers hantering av information – är det att betrakta som system designade för dold övervakning då de inte är synliga för användaren, även om användaren kan vara medveten om att detta sker?

Idag återfinns liknande krav i svensk lagstiftning avseende export av krigsmateriel (Lag (1992:1300) om krigsmateriel). Det beskrivs på följande sätt i prop. 2017/18:23 ”[r]espekt för mänskliga rättigheter och den mottagande statens demokratiska status utgör centrala villkor vid tillståndsprövningen”. Det är dock inte exportören som avgör detta, utan den tillståndsgivande myndigheten vilken kan neka export med hänvisning

<sup>1</sup> Begreppet due diligence översätts ofta med uttrycket ”företagsbesiktning”, men har egentligen en bredare betydelse. I betydelsen skäligen aktsamhet är begreppet vida spritt inom bland annat internationell rätt och enskilda rättsområden i angloamerikansk rätt. Begreppets ursprung kan härledas från 1800-talet då principen om rimlig hänsyn ("the due diligence rule") utvecklades i internationell rätt, vilken innebar att en stat måste vara skäligen aktsamma i att värna andra staters suveränitet, medborgare, miljö och intressen. Vi kommer använda det engelska begreppet due diligence genom hela detta dokument.

till kravet på mänskliga rättigheter och demokrati. Det är dock inte ett ovillkorligt hinder (som t.ex. vapenembargon utgör) utan ett nekande svar på en tillståndsförfrågan kan i vissa fall överklagas till regeringen.

Vid en jämförelse med exporten av krigsmateriel kan det noteras att sådan export skett under 2018 till ett flertal länder<sup>2</sup> trots krav på demokrati. Enligt FOI:s bedömning finns en tydlig risk att förfarandet avseende krigsmateriel kan göra det otydligt för exportörer huruvida de ska anmäla sin export av cyberövervakningsprodukter till den tillståndsgivande myndigheten eller inte.

Sammantaget ställer förordningen nya krav på exportören avseende vilken kunskap som erfordras vid export av cyberövervakningsprodukter. Promemorian anger att samma varningstecken som nämnts i bilaga 2 till kommissionens rekommendationer (EU) 2019/1318 kan nyttjas. De omständigheter som nämns handlar till stor del om till vem och hur anskaffningen har skett (ovanligt många varor, udda kvantitet, etc.). Dessa varningsflaggor fungerar bättre avseende fysiska produkter jämfört med matematiska algoritmer och mjukvara, där det finns anledning att diskutera vilka skydd för kopiering eller antal användare som finns. Rekommendationerna fungerar även sämre när exportören förväntas inse eller misstänka att varan eller tjänsten kan komma att användas i strid med art 5.1. Här bör tillståndsmyndigheterna ges möjlighet till rådgivning eller stöd i lag för att minska belastningen för både exportörer och tillståndsprovande myndigheter.

## Tekniskt bistånd

Tekniskt bistånd definieras i förordningen som ”tekniskt bistånd: allt tekniskt stöd som har samband med reparationer, utveckling, tillverkning, montering, provning, underhåll eller annan teknisk service, i form av exempelvis anvisningar, rådgivning, utbildning, förmedling av praktisk kunskap, färdigheter eller konsulttjänster, inbegripet genom elektroniska medel liksom per telefon eller andra muntliga former av bistånd”<sup>3</sup>. Till det definieras tillhandahållande bland annat följande: ”varje fysisk eller juridisk person eller varje partnerskap, som är bosatt eller etablerat i en medlemsstat, som tillhandahåller tekniskt bistånd till en person som är bosatt i ett tredjeland och som tillfälligt befinner sig i unionens tullområde”<sup>4</sup>. Gränsdragningen mellan det som undantas från förordningen (allmänt tillgänglig och grundforskning) från det som här benämns utbildning är oerhört svår att definiera. Detsamma gäller rådgivning.

Kravet på att använda ”due diligence” eller söka tillstånd vid export, som i första hand utgörs av tillhandahållande genom muntlig överlämning till utländsk person som tillfälligt befinner sig i Sverige kan vara en utmaning för olika forskningsutförare. Dessa

<sup>2</sup> ISP, Inspektionen för strategiska produkter, Verksamhet 2018, [https://isp.se/media/1311/isp\\_verksamhet2018\\_webb.pdf](https://isp.se/media/1311/isp_verksamhet2018_webb.pdf)

<sup>3</sup> EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2021/821 av den 20 maj 2021, p (7), Art 2 (9)

<sup>4</sup> Art 2 (10) (c)

måste därför ges bättre kännedom om vad eller vilka produkter och tjänster som anses vara produkter med dubbla användningsområden, utöver vad som framgår av bilaga 1 till förordningen.

För forskningsinstitut och universitet/högskolor är utbytet av information och kunskap viktigt för innovation och utveckling. Detta gäller även inom utbildningen. I förordningen definieras utbildning som sådan kunskapsöverföring som kan vara tillståndspliktig. Tillståndet ska då sökas baserat på om studenter eller doktorander kommer från länder där kunskap som skulle kunna erhållas vid studierna kan utnyttjas som ett hinder för mänskliga rättigheter. Sammantaget ställer definitionen av tekniskt bistånd stora krav på exportören.

FOI anser att regeringen bör ge behöriga myndigheter i uppdrag att särskilt informera forskningsinstitut och universitet/högskolor om lagförändringen för att säkerställa att Sverige inte felaktigt bidrar till spridning av kunskap eller tjänster som kan utnyttjas i strid med art 5.1.

### **Förslag framförda i promemorian**

*Sverige bör utnyttja bemyndigandet med möjlighet att införa tillståndskrav för export av cyberövervakningsprodukter och tekniskt bistånd*

Det är av stor vikt att Sverige inte exporterar produkter som kan användas för förtryck eller i strid med mänskliga rättigheter. Regeringens bemyndigande att införa tillståndskrav bör därför, enligt FOI:s uppfattning, införas i svensk lagstiftning. Denna lagstiftning borde även inkludera ett förtydligande av vad som kan anses som produkter eller tjänster som kan utgöra sådant hot mot demokratiska friheter. Kravet skulle då kunna medföra en större säkerhet för exportören, än att förlita sig på exportörens egna "due diligence". Ett eget regelverk, eller vilken form som är lämpligast, skulle även kunna förenkla för den enskilde om vad som bör anses tillståndspliktigt eller inte och därmed minska belastningen på tillståndsmyndigheterna. I samband med detta bör regeringen följa förordningens rekommendationer och särskilt beakta exportörernas storlek och organisationsstruktur<sup>5</sup>.

### **Konsekvenser**

#### **Belastningen på tillståndsmyndigheter**

Promemorian nämner att belastningen på tillsynsmyndigheterna inte förväntas öka. Mycket talar för att denna bedömning saknar fog. Promemorian noterar att de flesta företag som berörs av förslaget regelverk redan sedan tidigare har god kännedom om existerade regelverk. Dock saknas perspektivet att nytillkomna fysiska personer eller mindre innovationsföretag kan komma att beröras av den nya lagstiftningen. Dessa

<sup>5</sup> EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2021/821 av den 20 maj 2021, p (7)

entiteters läroprocess och tillståndshantering kan mycket väl komma att öka belastningen hos den behöriga myndigheten då sanktionerna kan leda till ett system där det är mer kostnadseffektivt för mindre och nytillkomna aktörer att söka tillstånd än att själva göra en tidskrävande analys med bristfälligt informationsramverk. Det är samtidigt osäkert om detta sannolika förfarande kommer att leda till ökade intäkter för den behöriga myndigheten, då exporten av programvara eller tekniskt bistånd kanske inte överstiger minimibeloppet för avgiften, det vill säga 2,5 MSEK. Om omsättningen av produkten skulle överstiga beloppet kan avgiften anses för hög för mindre företag som kanske väljer att exportera eller avstå, båda skeendena är någonting som bör undvikas.

Sammantaget finns det uppgifter som talar för att ISP och SSM mycket väl kan komma att behöva ökade anslagsramar. Det som tydligt saknas i promemorians konsekvensanalys är uppdraget att informera om förändringarna, framför allt inom forskning och utbildning där tillståndskravet kan upplevas som något nytt från tillståndsmyndigheternas sida.

Definitionen av tekniskt bistånd ställer stora krav på forskningsinstitut och universitet/högskolor vilket torde medföra stora risker för ökad administration eller utbildningsinsatser. Tillsammans med eventuella avgifter till ISP kan det utgöra en finansiell belastning som inte alls beaktas i promemorian. Detta är en brist.

## Exporttillstånd

Förslaget utgår ifrån att fördelningen mellan de behöriga myndigheterna fortsätter att gälla även när det gäller cyberövervakningsprodukter och tillståndskrav avseende andra länders kontrollistor. När det gäller cyberövervakningsprodukter så handlar förbudet i första hand om att förhindra spridning av produkter som kan innebära risk för att människors utsätts för förföljelse eller i strid med mänskliga rättigheter.

Uppdelningen av ansvarsområdena mellan de behöriga myndigheterna ska vara kvar, vilket är skäligt med hänsyn till de olika kompetensområden som berörs och information som finns tillgängligt hos respektive myndighet. Det bör dock framgå att cyberövervakningsprodukter enbart hanteras hos ISP utifrån kraven i art 5.1.

## Två nya generella exporttillstånd

Av de två nya generella exporttillstånden som införts i bilaga II kan noteras att koncernintern överföring av programvara och teknik inte påverkar programvara och teknik inom staten (inkl. forskningsinstitut och universitet/högskolor).

Det generella tillståndet för kryptering kan underlätta just för kommunikation och hantering av känslig information, till exempel inom finansvärlden där krypteringsprogram är vanliga. Kryptering är också något som kan komma att bli nödvändigt inför större europeiska försvarssamarbeten (till exempel inom Europeiska

försvarsfonden, EDF) där behovet av gemensamma krypteringssystem kan vara nödvändigt.

### **Saknas i promemorian**

I förordningens bilaga 1 noteras att informationssäkerhetsprodukter eller –funktioner ska värderas enligt 5.2 även om de är komponenter, programvara eller funktioner i andra system eller i annan utrustning. Informationssäkerhetsfunktionalitet (oavsett om det är hårdvara eller mjukvara) ingår ofta i militära system. Om det räknas som ett militärt system med militär slutkund ska det bedömas enligt Lag (1992:1300) om krigsmateriel där kraven ser något annorlunda ut. Det borde ske en större harmonisering mellan de olika lagstiftningarna utifrån de krav som ska ställas på exportören.

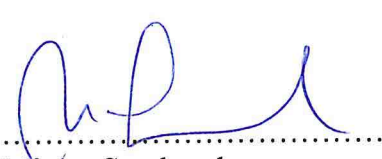
I förordningens punkt (13) noteras att "[o]lika kategorier av personer kan vara inblandade i export av produkter med dubbla användningsområden, inbegripet fysiska personer såsom tjänsteleverantörer, forskare, konsulter och personer som på elektronisk väg överför produkter med dubbla användningsområden." Detta, tillsammans med kravet på sanktioner vid brytande av exportregler, borde tydliggöras med nya instruktioner till tillståndsmyndigheterna om att genom information öka medvetenheten om riskerna för att reglerna inte ska inverka hindrande på forskningssamarbeten. I detta bör texten i punkt 13 beaktas i sin helhet.

Detta remissvar har beslutats av generaldirektör Jens Mattsson efter föredragning av internationell direktör Mårten Sundmark. I den slutliga handläggningen har även överdirektör Lena Nyberg, internationell samordnare Anders Lindblad, chefsjurist Eva Liljefors samt särskild rådgivare Mikael Wiklund deltagit.

Kista som ovan



.....  
Jens Mattsson



.....  
Mårten Sundmark

Sändlista:

ud.remissvar@regeringskansliet.se

ud-nis@gov.se

För kännedom:

Försvarsdepartementet Fö/MFU, RS

Internt FOI:

Registrator

GD-sekreterare

Särskild rådgivare

Chefsjurist

Internationell direktör