Regeringskansliet,
Justitiedepartementet
samt sändlista

Ert tjänsteställe, handläggare
Enheten för domstols- och åklagarfrågor

Ert datum
2026-07-09

Er beteckning
Ju2026/01670

Vårt tjänsteställe, handläggare
HKV FST JUR Ofr, Sara Westerlund,
sara.westerlund@mil.se

Vårt föregående datum

Vår föregående beteckning

Försvarsmaktens yttrande över betänkandet Effektiva ingripanden i cybermiljö (SOU 2026:45)

Försvarsmakten har beretts tillfälle att yttra sig över betänkandet Effektiva ingripanden i cybermiljö (SOU 2026:45). För Försvarsmaktens del skulle det kunna få positiva konsekvenser om brottsbekämpande myndigheter får bättre verktyg för att störa eller avbryta brottslig verksamhet i cyberdomänen, där det kan vara svårt att dra gränsen mellan kriminalitet och antagonistisk verksamhet. Det skulle sammantaget kunna ge bättre möjligheter för Sverige att ingripa mot aktiviteter som hotar totalförsvaret. Det finns dock ett antal frågor som enligt Försvarsmaktens mening inte har belysts i tillräcklig utsträckning i betänkandet, och som behöver omhändertas i den fortsatta beredningen av utredningens förslag.

Frågor om jurisdiktion

Utredningens förslag innebär att svenska brottsbekämpande myndigheter ska få ändra och radera data i informationssystem som finns i ett annat land, utan något krav på samtycke från det landet. Såsom framgår av betänkandet finns utrymme för olika tolkningar vad gäller folkrättsliga aspekter i cyberdomänen, och det är ett rättsområde under utveckling. Det innebär också att olika staters tolkningar och ställningstaganden får betydelse för de principer som tar form. Sådana ställningstaganden ger uttryck för vad en stat betraktar som ett legitimt agerande för egen del, och i gengäld även vad som får betraktas som legitimt agerande av andra stater.

I betänkandet hänvisas till den svenska regeringens positionspapper om tillämpningen av folkrätt i cybermiljö, där regeringen intar ståndpunkten att det

Postadress
Försvarsmakten
107 85 Stockholm

Besöksadress
Lidingövägen 24

Telefon
08-788 75 00

Telefax
08-788 77 78

E-post, Internet
exp-hkv@mil.se
www.forsvarsmakten.se

kan kränka en stats suveränitet att ändra och störa data utan att orsaka fysisk skada. En sådan suveränitetskränkning kan enligt positionspapperet vara för handen även när handlingen riktar sig mot cyberinfrastruktur som tillhör privatpersoner eller privata aktörer. I positionspapperet definieras inte närmare under vilka förutsättningar ett sådant intrång kan anses ha lett till en överträdelse av suveräniteten. Det konstateras att detta måste bedömas från fall till fall, med hänsyn till intrångets natur och karaktär.

Ett genomförande av utredningens förslag kan uppfattas som en vidareutveckling av de ställningstaganden som Sverige tidigare gjort i sin tolkning av folkrätten i cyberdomänen. För Försvarsmaktens del är det viktigt att ett sådant ställnings-tagande görs medvetet och efter en helhetsbedömning av hur det påverkar Sverige i relation till andra stater. Även brottsbekämpande åtgärder kan få säkerhets- eller försvarspolitiska konsekvenser, och det är inte alltid tydligt vem som är den egentliga aktören i cybermiljön. Försvarsmakten anser att detta bör belysas närmare i det fortsatta författningsarbetet.

Skyddet för viss verksamhet

Utredningen bedömer att vissa informationssystem och uppgifter bör ha särskilt skydd mot ingripanden. Försvarsmakten saknar här ett resonemang om i vilken mån ingripanden bör kunna göras när systemen stödjer säkerhetskänslig verksamhet.

Informationssystem som tillhör en aktör kan utnyttjas av en annan aktör som en del av dennas brottsliga verksamhet, utan att systemägaren har kännedom om detta. En cyberpersona kan, oavsett den bakomliggande aktörens faktiska hemvist, använda ett informationssystem som tillhör exempelvis en svensk myndighet som verktyg för brottslig verksamhet. När en brottsbekämpande myndighet för detta ändamål ser ett behov av att bereda sig tillträde till ett informationssystem som är av betydelse för Sveriges säkerhet behöver särskilda intresseavvägningar göras.

Påverkan på system som är av betydelse för Sveriges säkerhet kan få allvarliga konsekvenser även om systemen i sig inte innehåller säkerhetsskydds-klassificerade uppgifter. Behovet av ett snabbt brottsbekämpande ingripande behöver då vägas mot behovet av att upprätthålla systemens funktion och skydda den säkerhetskänsliga verksamheten. Ingripanden mot informationssystem som stödjer säkerhetskänslig verksamhet bör därför som utgångspunkt ske i samråd med den verksamhetsutövare som har rådighet över systemet. En sådan ordning skulle säkerställa att konsekvenserna för den berörda verksamheten kan bedömas innan ett ingripande genomförs. En samrådsskyldighet med berörd verksamhets-utövare bör därför införas i dessa fall.

Aktsamhetskrav

I utredningen föreslås att när ett ingripande genomförs får olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt. Ingripandet ska genomföras på sådant sätt att påverkan på annan som använder samma del av informationssystemet blir så begränsad som möjligt.

Försvarsmakten anser att det därutöver bör undvikas att de tekniska metoder som används vid ingripandet skapar nya sårbarheter som sedan kan exploateras av andra aktörer. Det bör förtydligas i lagtexten att ingripandet även ska genomföras så att påverkan på säkerheten blir så begränsad som möjligt.

Förhållandet till Försvarsmakten

Försvarsmakten delar inte utredningens uppfattning att de reglerade samarbetsformerna mellan polisen och Försvarsmakten begränsar sig till fysisk miljö. Lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning, som utredningen redogör för, innehåller inte någon sådan begränsning. Förordningen (2002:375) om Försvarsmaktens stöd till civil verksamhet innehåller inte heller någon sådan begränsning. Detsamma gäller förslaget i betänkandet Polisiär beredskap i fred, kris och krig (SOU 2025:57) till ny lag om Försvarsmaktens stöd till polisiär verksamhet i särskilda fall. Det är av stort värde att Försvarsmakten och de brottsbekämpande myndigheterna kan samverka i cybermiljön, eftersom det i vissa fall kan vara svårt att avgöra om det är fråga om rent kriminell verksamhet eller en antagonistisk statsaktör.

För det fall att Försvarsmakten kan antas ha intressen i den miljö där ingripandet sker, bör det finnas en mekanism för den ingripande myndigheten att informera Försvarsmakten och vid behov koordinera insatser. Ett ingripande skulle annars kunna störa en pågående operation av Försvarsmakten.

I det fall en brottsbekämpande myndighet avser att ingripa i en cybermiljö som förvaltas eller nyttjas av Försvarsmakten, eller som Försvarsmakten är beroende av, bör samråd ske med Försvarsmakten innan ingripandet sker. Försvarsmakten bör också hållas informerad om övriga åtgärder som kan påverka Försvarsmaktens verksamhet, exempelvis genom påverkan på kritisk infrastruktur. En sådan samrådsskyldighet bör därför införas.

Det finns även ett behov av att de brottsbekämpande myndigheterna delar relevant information till Försvarsmakten i underrättelsesyfte. Särskilt vid ingripanden som rör Försvarsmaktens verksamhet, men även i andra fall, kan information gällande t.ex. bedömt bakomliggande statsaktörer, intention och modus vara av stort värde för underrättelse- och säkerhetstjänsten, och ytterst för Sveriges försvar.

I beredningen av detta ärende har personal från cyberförsvarsledningen, cybersäkerhetsspecialist Joel Brandell och cybersäkerhetsspecialist Isak Wilkens deltagit.

Detta yttrande har beslutats av chefsjurist Kerstin Bynander**.** I den slutliga handläggningen har stabschef Marita Nolén, it-säkerhetschef Joanna Rutkowska, tf sektionschef Johanna Winblad och, som föredragande, försvarsjurist Sara Westerlund deltagit.

Bynander, Kerstin

Chefsjurist

Handlingen är fastställd i Försvarsmaktens elektroniska dokument- och ärendehanteringssystem.

Sändlista

Regeringskansliet, Justitiedepartementet	ju.remissvar@regeringskansliet.se, med kopia till ju.L4@regeringskansliet.se

Försvarsdepartementet (för kännedom e-post)

Inom myndigheten för kännedom
ÖB/GD
HKV FST CYBER
HKV OPL
MUST