Sändlista
Försvarsdepartementet
ju.remissvar@regeringskansliet.se
ju.L4@regeringskansliet.se

Ert tjänsteställe, handläggare
Linda Billung

Ert datum
2026-07-09

Er beteckning
Ju2026/01670

Vårt tjänsteställe, handläggare
IOF / Marika Ericson

Försvarshögskolans remissvar över betänkandet ”Effektiva ingripanden mot brott i cybermiljö”, SOU 2026:45

Försvarshögskolan konstaterar att utredningen har givit flera förslag till vidareutveckling av framför allt polisens verktyg för att ingripa mot brott i cybermiljön. Försvarshögskolan är positiv till flertalet av de förslag utredningen ger på såväl ny som ändringar i befintlig lagstiftning.

Försvarshögskolan har däremot specifika synpunkter på lagförslagen och i vissa delar synpunkter på utredningens avgränsningar och övriga förslag. Dessa synpunkter återfinns i det följande.

Generella frågor kring hur polisverksamhet bedrivs i cybermiljön

Polisens huvuduppgift är bland annat att förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen och säkerheten (2 § p.1 Polislagen (1984:387), att övervaka allmän ordning och säkerhet och ingripa när störningar har inträffat (2 § p. 2 polislagen) samt att utreda och beivra brott som hör under allmänt åtal (2 § p. 3 polislagen).

Eftersom brottsligheten, precis som utredningen konstaterar, idag i allt större utsträckning sker på eller genom cybermiljön behöver därmed även polisens verksamhet, uppgifter och verktyg självklart tolkas och anpassas till den omständigheten. Polismyndigheten måste få tillgång till ett tydligt lagstöd för att kunna ingripa mot brott och brottslig verksamhet i cybermiljön för att kunna utföra sin uppgift att upprätthålla ordning och säkerhet i samhället och ingripa mot pågående brottslighet.

Det skrivs tydligt i kap 11.1 att Polismyndigheten har samma möjligheter att utreda och lagföra brott i cybermiljön, men i flera andra delar av utredningen framstår det

delvis som att brottsbekämpande myndigheter idag saknar lagstöd för att ingripa mot brott i cybermiljö. Försvarshögskolan anser att dock att det är tydligt att polisens uppgift att förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av allmän ordning och säkerhet inbegriper även cybermiljön. Det innebär att det som saknas i själva verket är lagstiftning som tydliggör vilka befogenheter, vilka verktyg eller tvångsmedel, brottsbekämpande myndigheter kan använda sig av för att utföra sina uppgifter även i cyberrymden. De förmågor som anges som behov i utredningen skulle vid användning i många fall innebära att brottsbekämpande myndigheter själva bryter mot reglerna om dataintrång. Därav behövs en reglering av de förmågor som behöver användas i cybermiljön. Det kan framstå som en subtil skillnad, men Försvarshögskolan anser att det är viktigt att tydliggöra detta eftersom ett fokus på verktygen väcker frågor som utredningen inte riktigt besvarar. Hur kan verktygen specificeras i termer av förutsättningar för, syften och begränsningar i användningen av dem? Vems digitala kommunikation bör polisen få kartlägga, under vilka förutsättningar och för vilka syften? Utredningen anger till exempel att myndigheterna behöver tillgång till ”platser som är skyddade mot intrång”(s. 179), men vilka platser är detta och om platserna inbegriper enskildas privata sfär, vilka villkor och begränsningar behöver ett sådant tvångsmedel beläggas med i syfte att skydda rättssäkerheten för individer och den personliga integriteten särskilt för de personer som finns omkring en misstänkt person? Det här är frågor som inte riktigt besvaras i utredningen.

Utredningen beskriver bland annat att polisen behöver få möjligheter att etablera sig i en digital miljö, men också att påverka eller förändra den digitala miljön. Utredningen beskriver också hur brottsbekämpande myndigheter i andra länder fått möjlighet att bland annat störa och avbryta pågående brottslighet i cybermiljö. I grunden likställer utredningen den här typen av verksamhet med den typ av patrullering och inhämtning som brottsbekämpande myndigheter använder sig av i den fysiska miljön. Jämförelser med andra länder är värdefulla, men måste också bygga på en förståelse av de olika regler som gäller nationellt. Nya Zeeland, som utredningen hänför sig till, har till exempel inte regleringar av rätten till privatliv i sin nationella lagstiftning. Detta ger andra möjligheter att reglera befogenheter för polisiära myndigheter i den kontexten än i Sverige.

Cybermiljön skapar utmaningar på flera sätt för myndigheters möjligheter att skydda medborgarna mot att utsättas för brott eller att förhindra att medborgarna, ofta ovetandes, bidrar till brottsliga handlingar. Cybermiljön ger tillgång till snabba överföringar av pengar till hela världen, information har digitaliserats och kan utnyttjas för att utpressa eller stjäla såväl information som pengar även i situationer där förövare och offer fysiskt finns långt ifrån varandra och aldrig träffas. Cybermiljön ger betydligt större möjlighet för kriminella att utnyttja anonymiteten som den digitala miljön och särskilt internet ger och därigenom försvåra möjligheten för brottsbekämpande myndigheter att upptäcka och beivra brott som begås. Detta innebär utan tvekan att de brottsbekämpande myndigheterna behöver förbättrade verktyg för att uppnå såväl förhindrandet av brottslighet som för att möjliggöra en högre grad av lagföring av brott som begås.

Det går dock inte heller att bortse från att cybermiljön väcker särskilda frågor om hur en balans mellan effektiva åtgärder för brottsbekämpande myndigheter kan uppnås utan att individens rättigheter begränsas i en alltför stor omfattning. Enligt 2:20 RF kan bland annat rätten att inte utsättas för husrannsakan eller liknande intrång, intrång i förtroliga försändelser och meddelanden samt övervakning och kartläggning av den enskildes personliga förhållanden begränsas genom lag. Samtidigt ska begränsningarna tillgodose ändamål godtagbara i ett demokratiskt samhälle och inte gå utöver det nödvändiga med hänsyn till ändamålet som föranlett begränsningen, 2:21 RF.

Det är svårt att hitta balansen, och utredningen är konsekvent i att diskutera de föreslagna metoderna och verktygens påverkan på rättigheter för enskilda. Det förefaller dock också som att utredningen betonar effektiviteten över rättigheterna och i många fall beskriver nödvändigheten som så tvingande att det är rimligt att göra begränsningar i rättigheter för enskilda. Ur Försvarshögskolans perspektiv hade det varit önskvärt att utredningen dels på ett tydligare sätt beskrivit effekterna av de föreslagna åtgärderna och verktygen ur ett rättighetsperspektiv för enskilda. Det hade också varit önskvärt att utreda tydligare hur åtgärderna och verktygen påverkar personer omkring misstänkta cyberbrottslingar och hur deras rätt till privatliv kan säkerställas på ett effektivt sätt. Försvarshögskolan delar i den här delen synpunkterna i det särskilda yttrandet av experterna Ida Olsson och Andreas Persson rörande behovet av tydligare rättssäkerhetsgarantier.

Synpunkter på lagförslagen

Försvarshögskolan delar utredningens slutsatser rörande tillämpningsområdet för en framtida lag. Den tolkning som utredningen gör av principen om due diligence och de skrivningar som Tallinn-manualen innehåller rörande jurisdiktion ligger i linje med hur principerna används och tolkats i andra sammanhang. Däremot vill Försvarshögskolan påpeka att en omsättning av utredningens slutsatser i praktiken, utan samverkan med det land som påverkas av verksamheten, riskerar att leda till försämrat internationellt samarbete inom området. Utredningen hade i den här delen med fördel kunnat fokusera något mer på hur man kan få till ett effektivare samarbete med andra länders motsvarigheter och internationella samarbetspartner som Europol och Interpol.

Generellt förefaller de verktyg som utredningen föreslår för att förhindra brott och störa eller avbryta brottslig verksamhet syfta till att uppnå en form av polisiär verksamhet i cybermiljön som motsvarar eller liknar det polisen gör i sin ordinarie verksamhet genom t.ex. patrullering. Försvarshögskolan delar i grunden utredningens beskrivning av behoven av att t.ex. ändra och blockera eller att störa eller hindra användning av uppgifter som behandlas i informationssystem. Det finns dock också frågor som bör ställas, särskilt rörande avgränsningar och hur verktygen riskerar påverka tredje mans rättigheter till privatliv. Utredningen berör endast i begränsad utsträckning hur t.ex. överskottsinformation kommer att hanteras, samt hur begränsningar och avgränsningar i verktygens användning kan bidra till att minska

påverkan på tredje man. Detta bör också utgöra en del av regleringen och tydliggöras innan en ny lagstiftning implementeras.

Utredningen hanterar också frågor om beslutsnivåer. Utredningen gör i den delen, precis som i övriga delar av utredningen en vägning mellan behoven av snabbhet och effektivitet i beslutsfattandet kopplat till den effekt man vill uppnå och behovet av skydd för den enskildes rättigheter. I vägningen är det dock tydligt att behovet av snabbhet överväger och förslaget är att beslut om att bereda sig tillgång till informationssystem och till uppgifter i det i syfte att ändra eller blockera uppgifter eller störa eller hindra användningen av uppgifter i systemet ska ligga på befattningshavare vid Polismyndigheten, Säkerhetspolisen och Tullverket, inte åklagare eller allmän domstol. Däremot ska raderingsbeslut fattas av åklagare. Interimistiska beslut om radering ska kunna fattas av särskilt utsedda befattningshavare hos Polismyndigheten, Säkerhetspolisen eller Tullverket.

I grunden handlar Försvarshögskolans synpunkter även i detta fall om behovet av att hitta en balans mellan rättighetsskydd och effektivitet. Utredningen betonar i dessa delar tydligt effektiviteten och behovet av snabbhet och ger dessa en högre vikt än integritetsskyddet för enskilda. Försvarshögskolan hade i de här delarna velat se en större tydlighet i bedömningarna rörande skydd för enskilda. Förståelsen och acceptansen för åtgärderna och beslutsnivåerna hade också ökat om utredningen fört en tydligare diskussion om verktyg för att avgränsa och säkerställa skyddet för personer runt omkring de personer som ägnar sig åt eller misstänks ägna sig åt brottslig verksamhet. Med tanke på att verktygen ska kunna användas också för att förhindra brott innan de rent faktiskt begåtts blir rättsstatliga krav på legalitet och förutsägbarhet och därtill knutna skydds- och integritetsaspekter extra viktiga att tydliggöra och integrera i lagtexten och i en framtida tillämpning av lagen.

Försvarsmakten, underrättelsemyndigheterna och polisen – gränsytor och krockar

Utredningen innehåller i ytterst begränsad omfattning en analys av förhållandet till Försvarsmakten och den del av utredningen där frågan nämns fokuserar helt på den stödlagstiftning som finns för den fysiska miljön i form av lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning med tillhörande förordning.

En aspekt lämnas dock helt åt sidan i utredningen, hur myndigheternas verksamhet i cybermiljön riskerar att eventuellt överlappa eller på andra sätt skapa utmaningar för varandra och vikten av att myndigheterna samverkar. Ett informationssystem, en brottsling eller misstänkt brottsling kan också vara ett system eller en person av intresse för Försvarsmaktens verksamhet för att försvara Sverige och skydda svenskt territorium även i fredstid. På samma sätt kan system och personer som är av polisiärt intresse samtidigt vara av intresse för underrättelsemyndigheter som Försvarets radioanstalt och, inom kort, Sveriges utrikes underrättelsetjänst.

Försvarsmaktens verksamhet inom cyberdomänen är precis som utredningen konstaterat rörande polisiär verksamhet i stort behov av tydliggörande lagstiftning som

ger tydliga mandat och befogenheter för att utföra sina uppgifter. Försvarshögskolan anser att det finns risker för att flera myndigheter när de utför sina ordinarie uppgifter kan komma att i vissa fall befinna sig i samma informationssystem, eller bedriva verksamhet riktad mot samma personer. Detta är en aspekt som utredningen hade behövt analysera närmare och, eftersom frågan inte ingår i direktivet till den här utredningen, ge förslag på ytterligare utredning eller analys efter samverkan med Försvarsmakten och andra berörda myndigheter.

Beslut

Beslut i detta ärende har fattats av Försvarshögskolans rektor Robert Egnell, efter slutföredragning av lektor Marika Ericson. I beredningen har docent Ulrik Franke och lektor Carina Lamont deltagit.

Robert Egnell
Rektor

Marika Ericson
Lektor

Handlingen undertecknas elektroniskt.

Sändlista externt:
Justitiedepartementet
ju.remissvar@regeringskansliet.se
Ju.L4@regeringskansliet.se

Sändlista internt:
Centrum för totalförsvar och samhällets säkerhet
Försvarshögskolans studentkårer
Högskoleförvaltningen
Institutionen för försvarssystem
Institutionen för krigsvetenskap
Institutionen för ledarskap och ledning
Institutionen för militärhistoria
Institutionen för operativ juridik och folkrätt
Institutionen för statsvetenskap
Programledning Högre officersprogrammet
Programledning Officersprogrammet