Totalförsvarets forskningsinstitut

Datum	Diarienummer
2026-11-09	FOI-2026-1403

Justitiedepartementet

Er referens	Vår handläggare
Ju2026/01670	Alica Selmanovic Monokrousos

Remissvar gällande betänkandet Effektiva ingripanden i cybermiljö (SOU 2026:45)

Sammanfattning av FOI:s synpunkter

- Totalförsvarets forskningsinstitut (FOI) ställer sig positivt till utredningens förslag om att en ny lag om polisiära ingripanden i cybermiljön införs i svensk lagstiftning.
- FOI ställer sig positivt till att förslaget öppnar upp för en utvecklad praxis för löpande bedömningar av tillämpning av folkrätten i cybermiljön.
- FOI anser att ytterligare analys behövs i centrala delar för att utredningens förslag ska kunna genomföras. Detta gäller särskilt frågor om jurisdiktion och lagens tillämpningsområde, förhållandet till Försvarsmakten och andra berörda myndigheter samt frågan om underrättelse till enskilda.
- FOI tillstyrker utredningens förslag om att särskild tillsyn bör införas.
- FOI avstyrker utredningens förslag att beslut om ingripanden ska fattas av en särskild utsedd befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket.
- FOI avstyrker utredningens förslag om att beslut om ingripanden får fattas muntligen.
- FOI anser att de säkerhets- och utrikespolitiska konsekvenserna som kan uppstå till följd av myndigheternas ingripanden i informationssystem som finns i utlandet behöver analyseras i den fortsatta beredningen.
- FOI anser att den föreslagna lagen bör innehålla en uttrycklig samrådsskyldighet med berörda försvarsunderrättelsemyndigheter. Samråd är särskilt viktigt när polisiära ingripanden avser informationssystem som finns i utlandet.
- FOI bedömer att regeringen bör tillsätta en utredning med uppdrag att analysera och tydliggöra förhållandet mellan polisens befogenheter att ingripa

i cybermiljön och försvarsunderrättelsemyndigheternas uppdrag och befogenheter.

FOI:s utvecklade synpunkter

FOI har utifrån de utgångspunkter myndigheten har att beakta följande synpunkter på betänkandet.

En ny lag bör införas

FOI delar utredningens uppfattning att det behöver införas en ny lag som reglerar polisiära ingripanden i cybermiljö. FOI bedömer att skälen är välmotiverade, eftersom de åtgärder som de brottsbekämpande myndigheterna behöver kunna vidta för att förebygga och ingripa mot brott i cybermiljö inte kan genomföras inom ramen för nuvarande lagstiftning. Det finns därför ett behov av nya rättsliga verktyg för att möta den alltmer organiserade och tekniskt avancerade brottslighet som bedrivs i cybermiljön.

FOI menar att förslaget öppnar upp för en ny, mer flexibel, praxis i tolkningen av folkrätten där suveränitetsprincipen får bedömas utifrån omständigheterna. FOI välkomnar detta och stödjer bedömningen att denna förändring behövs med anledning av utvecklingen inom cyberkriminalitet och sabotage med cyberinstrumentet. Förändringen innebär dock ett behov av en ny utredning som förtydligar gränsdragningar, samrådsformer och uppföljning av påverkan mot försvarsunderrättelsemyndigheternas mandat.

Om begreppen cybermiljö och informationssystem

Mot bakgrund av att lagen innebär långtgående befogenheter i cybermiljön bedömer FOI att vissa centrala begrepp behöver preciseras närmare i lagtexten.

En definition av begreppet cybermiljö bör införas i lagtexten och inte enbart förklaras i allmänmotiveringen och författningskommentaren. Cybermiljö är en grundläggande term som den föreslagna författningen bygger på och som därmed är avgörande för lagens tillämpningsområde och räckvidden för de polisiära befogenheterna. En sådan definition måste vara teknikneutral.

FOI anser även att begreppet informationssystem bör definieras i lagen, se exempelvis cybersäkerhetslagen (2025:1506) 2 § 16 om nätverks- och informationssystem. Det bör även övervägas huruvida ”avgränsad del av informationssystem” i den föreslagna lagens 16 § bör få en närmare precisering i lagtexten. Eftersom uttrycket avgränsar vidden av befogenheten att ingripa i ett beslut om ingripanden bör det vara tydligt vilka delar av ett informationssystem som kan omfattas.

Vidare anser FOI att det bör tydliggöras huruvida det krävs internetuppkoppling för att det ska anses vara fråga om brottslig verksamhet i cybermiljö. Av författningskommentaren framgår att internet i vissa fall är en direkt förutsättning för att ett brott ska kunna begås, medan användningen av internet i andra fall utgör enbart ett medel för brottets genomförande (s. 388–389). Frågan uppstår om lagen då utesluter brott där hotaktören angriper ett internt nätverk eller utnyttjar det interna nätverket som medel för att utföra ett brott. Om internetuppkoppling är ett krav bör det framgå av lagtexten och inte överlåtas till författningskommentaren. Om internetuppkoppling däremot inte är ett krav bör även detta tydliggöras.

Lagens tillämpningsområde och frågor om jurisdiktion

Som nämndes ovan menar FOI att förslaget öppnar upp för en ny, mer flexibel, praxis där suveränitetsprincipen får bedömas utifrån omständigheterna.

I utredningen redogörs för Sveriges ståndpunkt avseende tillämpningen av folkrätt i cybermiljön.[1] Sverige anser bl.a. att stater har jurisdiktion och rätt att utöva myndighet på sina territorier inom ramen för folkrätten, vilket är ett uttryck för principen om statssuveränitet. En överträdelse av skyldigheten att respektera andra staters rättigheter till följd av statssuveräniteten skulle utgöra en folkrättsstridig handling och ge upphov till statsansvar. En stats jurisdiktion och befogenheter gäller för personer och objekt inom dess territoriella gränser, inklusive cyberrelaterad verksamhet. En stat har rätt att skydda personer och objekt inom sitt territorium, eller som på annat sätt står under dess jurisdiktion, mot påverkan genom cybermedel. I allmänhet anser Sverige att en överträdelse av suveräniteten kan uppkomma genom cyberoperationer som leder till skada eller funktionsförlust. Att orsaka en ändring eller på annat sätt påverka data, utan att orsaka fysisk skada, kan också utgöra en överträdelse av statssuveräniteten enligt den svenska ståndpunkten. Det omfattar även sådana cyberoperationer som riktas mot cyberinfrastruktur som tillhör privatpersoner eller privata juridiska personer. Inblandning i en annan stats statliga funktioner kan också utgöra en överträdelse av statssuveräniteten, även när inblandningen genomförs med cybermedel.

Utredningens förslag om polisiära ingripanden och motiven avseende verkställighetsjurisdiktion behöver förstås mot bakgrund av Sveriges, och andra staters, ståndpunkter i fråga om suveränitetsprincipen. Utredningens lagförslag kan medföra att ingripanden enligt lagen kan komma att bedömas som suveränitetsöverträdelser, särskilt i det fall skada eller funktionsförlust i digital infrastruktur uppstår. Vidare kan de i lagen föreslagna ingripanden anses som folkrättsstridiga om de orsakar förändringar eller annan påverkan på data.

[1] Regeringskansliet, Sveriges positionspapper om tillämpningen av folkrätt i cybermiljö, juli 2022.

Frågan om åtkomst till informationssystemet i utlandet har, som utredningen framhåller, varit föremål för prövning i Högsta domstolen (se NJA 2023 s. 231). Enligt nuvarande rättspraxis får en genomsökning i informationssystem på distans genomföras även om den eftersökta informationen kan vara lagrad i utlandet. Genomsökningen får dock endast ske på ett sådant sätt att den eftersökta informationen inte raderas eller på annat sätt påverkas till sitt innehåll. Det nuvarande lagförslaget innebär emellertid att de aktuella myndigheterna i Sverige kommer att kunna blockera, ändra eller radera uppgifter i informationssystem som finns i utlandet, utan krav på specifik befogenhetstilldelning enligt folkrätten eller giltigt samtycke från den andra staten att utöva jurisdiktion på dess territorium. Myndigheterna föreslås få använda de tekniska hjälpmedel som behövs. Vidare ska systemskydd kunna brytas eller kringgås och tekniska sårbarheter får utnyttjas.

Utredningen motiverar lagens tillämpningsområde och dess förenlighet med folkrätten genom att hänvisa till de begränsningar i lagen som utgår från faktorer som anknyter till Sverige (2 § p. 1–3). Att Sverige utövar preskriptiv jurisdiktion på grundval av dessa anknytningsargument innebär dock inte automatiskt att Sverige också bör utöva extraterritoriell verkställande jurisdiktion.

Extraterritoriell verkställande jurisdiktion kan, som utredningen också påpekar, vara förenligt med folkrätten under vissa omständigheter. Det behöver finnas en befogenhet enligt internationell rätt eller samtycke från utländsk regering. Enligt utredningen skulle krav på samtycke i alltför hög grad begränsa möjligheterna att tillämpa den nya lagen, särskilt mot bakgrund av hur snabbt uppgifter i digitala miljöer kan flyttas från ett land till ett annat. Utredningen hänvisar vidare till doktrin där experter lyfter att det ändå kan finnas omständigheter då svenska polisiära myndigheter får ingripa i cybermiljön, t.ex. när data finns i informationssystem i andra länder men informationen är allmänt tillgänglig på internet. Detta kan gälla även slutna onlineforum, t.ex. på Darknet, eftersom informationen även då är avsedd att vara tillgänglig från den berörda staten. Den föreslagna lagen är dock inte avgränsad till endast situationer när det råder sådana omständigheter.

Mot bakgrund av ovan önskar FOI framhålla att lagens tillämpningsområde inte får bli större än vad som är nödvändigt för att tillgodose det aktuella behovet. Vid lagens utformning behöver hänsyn tas till att en överträdelse av suveränitetsprincipen i cybermiljön är i hög utsträckning kontextberoende. Huruvida ett ingripande i cybermiljön enligt den föreslagna lagen är folkrättsstridigt får bedömas utifrån de konkreta omständigheterna, där bland annat ingripandets omfattning, graden av intrång samt eventuella skador eller ändringar i data är av betydelse. Lagen innehåller vissa aktsamhetskrav samt krav på proportionalitet (§§ 7, 18 och 19) men dessa är i

hög grad motiverade utifrån det integritetsintrång och det men som ingripanden kan innebära för enskilda och andra motstående intressen.

Underrättelse till enskild och till andra myndigheter

Ingripanden i cybermiljön kan komma att påverka enskilda som inte har någon koppling till det brott eller den brottsliga verksamhet som de aktuella myndigheterna vill störa eller förhindra. Detta gäller exempelvis när flera användare har tillgång till samma informationssystem eller användarkonto. Kriminella aktörer kan även infektera enskildas datorer utan deras vetskap. Ett exempel som innefattar skadlig kod som cybersäkerhetsmyndigheten i USA, CISA, tidigare har varnat för innebär att ett verktyg kallat Truebot installeras i en dator för att både angripa en viss dator och använda den datorn för att angripa andra informationssystem, som en del i ett botnät.[2] Ett skadeprogram kan således sprida sig i en kompromitterad miljö där enskilda kan vara ovetande om att deras informationssystem ingår i ett kriminellt nätverk.

I förslaget till ny lag är underrättelseskyldigheten enligt 21 § begränsad till situationer där uppgifter har raderats eller blockerats under längre tid än en månad. Eftersom ovan beskrivna exempel förekommer i cybermiljön kan det ifrågasättas om utredningens förslag om underrättelseskyldighet tar tillräcklig hänsyn till enskildas intressen. FOI anser, till skillnad från utredningen, att en underrättelse fyller en funktion när den enskilde märker att ett informationssystem inte fungerar som vanligt eller att uppgifterna inte längre är åtkomliga. I den fortsatta beredningen bör det övervägas om en skyldighet om underrättelse istället ska inträffa så snart en sådan upplysning inte längre riskerar att skada myndigheternas brottsutredningar.

Frågan om underrättelser är också av central betydelse för att den enskilde ska kunna göra gällande ett eventuellt skadeståndsanspråk. Som 21 § är utformad kan en enskild person, vars informationssystem har förlorat viss funktionalitet eller uppgifter på grund av ett ingripande enligt lagen, inte begära skadestånd i de fallen skadan i informationssystemet har skett omedelbart då blockeringen eller raderingen av uppgifterna genomfördes. Om raderingen eller blockeringen har skett under en kortare period än en månad finns inget krav på underrättelse och den enskilde kommer i sådana fall antagligen inte kunna veta orsaken till skadan på informationssystemet. Det kan hindra den enskildes möjlighet att tillvarata sin rätt till skadestånd.

Det bör även övervägas att ett beslut om ingripanden enligt lagen också, när det bedöms som lämpligt, ska innehålla villkor om att ett meddelande lämnas i informationssystemet från den aktuella myndigheten som har genomfört ingripandet,

[2] Se Increased Truebot Activity Infects U.S. and Canada Based Networks | CISA, Juli 2023.

exempelvis att en viss webbsida har tagits över av svenska myndigheter. I vissa fall kan ingen enskild aktör identifieras, vilket väcker frågan om myndigheterna då istället bör lämna ett meddelande i informationssystemet.

En fortsatt analys av frågan om underrättelser bör även innefatta frågan huruvida svenska myndigheter i vissa fall ska underrätta utländska myndigheter om att de ska genomföra ingripanden eller att de har genomfört ingripanden enligt lagen. Om en annan stat upptäcker ett dataintrång i informationssystem som ingår i deras cyberinfrastruktur, som kan attribueras till Sverige, och kontaktar svenska myndigheter i frågan, aktualiseras frågan om svenska myndigheter i sådana fall bör informera om att det var inom ramen för ett ingripande enligt den föreslagna lagen som dataintrånget genomfördes.

Besluten

FOI avstyrker utredningens förslag att beslut om ingripanden ska fattas av en särskild utsedd befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket.

Den internationella utblicken som utredningen redogör för visar också att beslut om ingripanden i cybermiljö i flera rättsordningar fattas av domstol, åklagare eller undersökningsdomare. FOI anser att den föreslagna ordningen inte erbjuder en tillräcklig grad av oberoende förhandskontroll. Detta särskilt vid ingripanden som kan medföra betydande integritetsintrång, påverka tredje part eller innebära säkerhets- och utrikespolitiska konsekvenser till följd av att ingripandet sker i informationssystem som finns i utlandet.

Vidare avstyrker FOI utredningens förslag om att beslut om ingripanden får fattas muntligen. Cyberoperationer är inte en högprecisionsverksamhet där det alltid går att förutse vilka informationssystem, uppgifter och personer som påverkas av att svenska myndigheter vidtar tekniska åtgärder vid ingripanden. Ett informations-system kan vara gemensamt för flera användare, sammankopplat med andra system eller ha tagits över av en aktör utan att systemets ägare eller andra användare har kännedom om detta. En tekniskt väl avgränsad åtgärd kan därför få konsekvenser även för tredje part. FOI menar att det ska finnas en god möjlighet till efterhandsgranskning. Ett beslut om ingripanden bör därmed vara skriftligt och innehålla den information som krävs enligt lagen för att på så sätt minska riskerna för negativa konsekvenser med sådana ingripanden samt säkerställa möjligheten att i efterhand externt granska besluten enligt motsvarande krav på andra myndigheter med liknande konsekvenser för den enskilde

Ett beslut bör även, utöver vad som anges i 16 §, innehålla en redogörelse av hur den beslutande myndigheten har beaktat kraven på proportionalitet och aktsamhet enligt 7 § respektive 18 §.

Om överklagande av beslut och tillsyn

FOI tillstyrker utredningens förslag att ingripanden i cybermiljö är en typ av ingripanden som bör omgärdas av särskilda rättssäkerhetsgarantier och att särskild tillsyn därför bör införas.

Utredningen har i avsnitt 16.2.4 funnit att åklagarens beslut om radering inte bör få överklagas eller på annat sätt prövas av någon fristående myndighet. Frågan är då hur kontrollen av sådana beslut ska säkerställas? I den fortsatta beredningen bör det även klargöras huruvida övriga beslut om ingripanden, som ska vara skriftliga och motiverade, ska kunna överklagas, överprövas eller i efterhand utvärderas på något sätt. Utredningen anser, vilket utvecklas närmare i avsnitt 19.3, att särskild tillsyn bör utövas över den nya lagen och att den ska utövas av Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd. Åklagaren bör därför underrätta tillsynsmyndigheten om besluten i fråga.

Säkerhets- och utrikespolitiska konsekvenser av myndigheternas ingripande i system i utlandet

Vidare anser FOI att det saknas en analys av de säkerhets- och utrikespolitiska konsekvenserna som kan uppstå till följd av myndigheternas ingripanden i informationssystem som finns i utlandet. Det är möjligt att den stat på vars territorium ett ingripande sker enligt svensk lag gör en annan folkrättslig bedömning av åtgärden än Sverige. Ett ingripande i cybermiljön som av Sverige bedöms vara förenligt med folkrätten kan således av den berörda staten uppfattas som en överträdelse av dess suveränitet. En sådan situation kan aktualisera frågor om Sveriges statsansvar och, under förutsättning att folkrättens krav är uppfyllda, den andra statens möjligheter att vidta motåtgärder.

I Sveriges relation med fungerande rättsstater bedömer FOI att frågan om folkrättsliga diskussioner inte kommer att uppstå. Samtidigt kan FOI konstatera att förslaget till lagändring främst handlar om att åtgärda begränsningar för Sverige att skydda sig mot kriminalitet, sabotage eller statsaktörer som verkar från en stat där staten inte agerar enligt internationell rätt eller utövar rättsskipning i de aktuella frågorna. Vissa av dessa stater har som metod att hävda att lagstiftningen riskerar att undergräva internationell stabilitet inom informationssäkerhet.

De säkerhets- och utrikespolitiska konsekvenserna av sådana situationer bör därför belysas i den fortsatta beredningen av förslaget.

Förhållandet till Försvarsmakten och andra underrättelsemyndigheter

I den fortsatta beredningen behöver frågor om stöd från Försvarsmakten, och samarbete mellan Polismyndigheten och Försvarsmakten, analyseras vidare. Detta är av central betydelse i cybermiljön mot bakgrund av det säkerhetspolitiska läget där statsaktörer kan antas ligga bakom vissa cyberangrepp, potentiellt som en del av bredare hybridhot. FOI noterar att utredningen endast kortfattat berör frågan om Försvarsmaktens stöd till polisen samt Försvarsmaktens uppdrag att försvara Sverige mot cyberattacker.

Som utredningen påpekar finns idag reglerade samarbetsformer mellan polisen och Försvarsmakten i olika författningar, bl.a. lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning. Det bör vidare noteras att samverkan på cyberområdet även är reglerad i förordning (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt. Även om samverkan och vissa former av stöd redan idag är möjliga enligt befintlig lagstiftning bör frågan om det ska införas särskilda bestämmelser för Försvarsmaktens stöd vid polisiär verksamhet i cybermiljön, exempelvis i den föreslagna lagen, analyseras vidare i den fortsatta beredningen av utredningens förslag.

Vidare bör den fortsatta beredningen innehålla en analys av eventuella överlappande uppgifter mellan Polismyndigheten, Säkerhetspolisen, Försvarets radioanstalt och Försvarsmakten. Att upptäcka, motverka och hantera cyberangrepp som hotar landets säkerhet ingår i dessa myndigheters uppdrag, om än från olika perspektiv. Lagförslaget har i sin nuvarande utformning exempelvis inga mekanismer avseende samordning mellan berörda myndigheter, så som samrådsskyldighet inför ingripanden mot brott som riktar sig mot den svenska staten eller kritisk infrastruktur. Det kan vara problematiskt i situationer då ett cyberangrepp som till synes kan hänföras till kriminella aktörer samtidigt kan utgöra ett led i en cyberoperation som har destabiliserande ändamål, där en statsaktör kan antas vara involverad. Attribuering – teknisk och juridisk – kan i sådana fall vara komplext och tidskrävande. Innan ett ingripande vidtas kan det därför finnas behov av samordning mellan berörda myndigheter och andra aktörer. Det finns även anledning att analysera behovet av samordning med Sveriges utrikes underrättelsetjänst.

Myndigheternas intressen kan dessutom skilja sig åt eller stå i konflikt med varandra. Det kan exempelvis vara av särskilt intresse för en myndighet att låta en viss brottslig verksamhet fortgå under kontrollerade former för att kunna kartlägga eventuell subversiv verksamhet eller kopplingar till statsunderstödda aktörer. Ett ingripande från Polismyndigheten eller Tullverket i syfte att omedelbart störa den pågående brottsliga verksamheten skulle i en sådan situation kunna försvåra eller omintetgöra

den andra myndighetens arbete. Det bör därför särskilt övervägas om det finns behov av former för informationsutbyte, samråd eller andra former av koordinering innan ingripanden vidtas i situationer där brottslig verksamhet kan ha samband med ett bredare cyberangrepp eller en säkerhetshotande cyberoperation.

Avslutningsvis bedömer FOI regeringen bör tillsätta en utredning med uppdrag att analysera och tydliggöra förhållandet mellan polisens befogenheter att ingripa i cybermiljön och försvarsunderrättelsemyndigheternas uppdrag och befogenheter. Utredningen bör särskilt analysera gränsdragningen mellan polisens brottsbekämpande uppdrag och försvarsunderrättelseverksamhetens uppdrag, inklusive hur ingripanden enligt den föreslagna lagen kan påverka försvarsunderrättelsemyndigheternas möjligheter att fullgöra sina uppgifter.

Övrigt

Om statliga myndigheters underrättelseskyldighet

FOI vill även uppmärksamma att den fortsatta beredningen bör behandla frågan huruvida regeringsformens bestämmelse i kap. 10 § 13 om statliga myndigheters underrättelseskyldighet kan komma att aktualiseras i vissa situationer då Polismyndigheten, Säkerhetspolisen och Tullverket vidtar åtgärder i informationssystem som befinner sig i en annan stat. Den aktuella bestämmelsen föreskriver att chefen för det departement som har hand om utrikesärendena ska hållas underrättad när en fråga som är av betydelse för förhållandet till en annan stat eller till en mellanfolklig organisation uppkommer hos en statlig myndighet.

Vad gäller underrättelsepliktens omfattning kan, enligt uttalanden från Konstitutionsutskottet, även till synes tekniska ärenden kunna rymma eller snabbt få utrikespolitisk betydelse och en central kontroll måste finnas över alla utrikesförbindelser som har någon utrikespolitisk betydelse eller kan medföra rättsliga förpliktelser för riket (se t.ex. 2012/13:KU20 s. 205 ff.). I det fall att berörda myndigheter bereder sig tillgång till informationssystem i en annan stat och blockerar, ändrar eller raderar uppgifter i det informationssystemet, t.ex. att säkerhetskänslig information raderas för att förhindra eller avbryta spioneri eller olovlig underrättelseverksamhet (s. 256), behöver den fortsatta beredningen belysa eventuell underrättelseskyldighet enligt regeringsformen.

Detta remissvar har beslutats av generaldirektör Jens Mattsson efter föredragning av analytiker Alica Selmanovic Monokrousos. I den slutliga handläggningen har även

Totalförsvarets forskningsinstitut

Datum 2026-11-09

Beteckning FOI-2026-1403

överdirektör Lisa Gustafsson, ställföreträdande avdelningschef Daniel Faria, jurist Helena Salberg, stabschef Niclas Karlsson och stabshandläggare Pär Eriksson deltagit.

Jens Mattsson *Alica Selmanovic Monokrousos*

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

Internt FOI:
Registrator
ÖD-sekreterare
Stabschef
Chefsjurist
AC Försvarsanalys
AC Cyberförsvar och ledningsteknik
Verksamhetsområdeschef Cyber
Verksamhetsområdeschef Civilt försvar