KUSTBEVAKNINGEN

Försvarsdepartementet

Organisatorisk enhet
Rätts- och säkerhetsenheten

Handläggare
Anna S Berglund

Datum
2024-05-16

Dnr
2024–579:2

Informationssäkerhetsklassificering
Begränsat skyddsvärde

Ert datum
2024-03-06

Er referens
Fö2024/00496

Remissvar avseende delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Sammanfattande synpunkter – Kustbevakningen behöver undantas

Kustbevakningen avstyrker utredningens förslag till utformning av 1 kap. 11 och 12 §§ cybersäkerhetslagen samt 6 och 7 §§ cybersäkerhetsförordningen.

Det är synnerligen angeläget att författningsförslaget justeras i dessa delar och att Kustbevakningen helt undantas från tillämpningsområdet av den föreslagna cybersäkerhetslagen.

De teoretiska och praktiska gränsdragningsproblem som följer om Kustbevakningen även i det fortsatta lagstiftningsärendet skulle omfattas av förslaget till 1 kap. 12 § cybersäkerhetslagen är omfattande, svårhanterliga och motsvaras inte av någon egentlig säkerhetsvinst.

I det följande utvecklas skälen för Kustbevakningens inställning.

Inledning

Kustbevakningen välkomnar utredningens förslag och vill inledningsvis framhålla att det är angeläget med regelverk som syftar till att åstadkomma en hög cybersäkerhetsnivå inom samhällsviktig verksamhet, genom utökning av antalet sektorer som omfattas av förslaget samt skärpta krav på tillämpning av regelverket på aktörernas hela verksamhet.

Kustbevakningen konstaterar att myndigheten omfattas av utredningens förslag till ny cybersäkerhetslag och inte är en av de myndigheter som föreslås undantas i sin helhet

POSTADRESS
Kustbevakningen
Box 536
371 23 KARLSKRONA

TELEFON
0776-70 70 00 (växel)

TELEFAX
0455-105 21

E-POST OCH INTERNET
registrator@kustbevakningen.se
www.kustbevakningen.se

från lagen (1 kap. 3 § och 11 § cybersäkerhetslagen samt 6 och 7 §§ cybersäkerhetsförordningen).

Kustbevakningen omfattas i stället av den del av lagförslaget som innebär att viss – men inte all – verksamhet ska undantas från kraven i den nya lagen (1 kap. 12 § cybersäkerhetslagen).

Mot denna bakgrund har Kustbevakningen, utifrån sitt verksamhetsområde, följande synpunkter på utredningens förslag.

Om tillämpningen av den föreslagna 1 kap. 12 § cybersäkerhetslagen

Enligt den föreslagna 1 kap. 12 § cybersäkerhetslagen ska vissa i paragrafen närmare angivna krav inte gälla för de delar av en statlig myndighets verksamhet som är säkerhetskänslig eller som utgör brottsbekämpning. För övriga delar av verksamheten gäller lagen i dess helhet.

Hänvisningarna i 1 kap. 12 §

Hänvisningen i 1 kap. 12 § till att kraven i 6 § andra och fjärde stycket inte gäller framstår som svårförståelig. Detta eftersom 6 § avser enskilda verksamhetsutövare. Det som stadgas om gränsöverskridande verksamhetsutövare i 6 § andra och fjärde stycket borde alltså inte omfatta statliga myndigheter, helt oaktat hänvisningen i 12 § (jfr 1 kap. 3 §, 4 § p. 2 samt 13 §).

Avgränsningen av tillämpningsområdet för 1 kap. 12 §

Vad gäller tillämpningen av den föreslagna 1 kap. 12 § framgår det av författningskommentaren att säkerhetskänslig verksamhet definieras i säkerhetsskyddslagen (2018:585) och att i begreppet brottsbekämpning ingår förebyggande, utredning, upptäckt och lagföring av brott (se s. 370 i delbetänkandet).

I 1 kap. 1 § säkerhetsskyddslagen stadgas att den lagen gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet).

Med uttrycket säkerhetskänslig verksamhet enligt säkerhetsskyddslagen avses alltså det som anges i ovan nämnda paragraf. Lagen innehåller ingen närmare definition än så av begreppet ”säkerhetskänslig verksamhet”. I fråga om vad som utgör ”verksamhet som är av betydelse för Sveriges säkerhet” kan de förhållanden som är av betydelse för Sveriges säkerhet förändras över tiden och behovet av säkerhetsskydd kan pendla över tid mellan olika skyddsintressen. (Se lagkommentaren, Lexino, till 1 kap. 1 § säkerhetsskyddslagen.) Som ett exempel kan anges att en uppgifts skyddsvärde varierar över tid beroende på kraven på konfidentialitet, riktighet och tillgänglighet samt beroende på den aktuella hotbilden och vilka risker som är kopplade till denna.

I 1 kap. 2 § säkerhetsskyddslagen stadgas vad som avses med säkerhetsskydd, nämligen skydd av säkerhetskänslig verksamhet mot spioneri, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.

Vad som kan och ska anses utgöra säkerhetskänslig verksamhet enligt säkerhetsskyddslagen är alltså föränderligt och behöver bedömas utifrån de aktuella skyddsvärdena samt den aktuella hotbilden mot dessa. Detta kan förmodas ge upphov till gränsdragningsproblem vid tillämpningen av den föreslagna 1 kap. 12 § cybersäkerhetslagen.

Kustbevakningen noterar att regeringens uttryckliga direktiv till utredaren har varit att inriktningen för förslagen ska vara att säkerhetskänslig verksamhet undantas från den nya regleringen i den utsträckning som är möjlig (se kommittédirektiv 2023:30, s. 412 i delbetänkandet). För att uppnå denna ambition bör det analyseras närmare vilka praktiska konsekvenser som kan följa av den reglering som nu föreslås. Enligt Kustbevakningens bedömning kan det av förslagets nuvarande utformning följa sådana gränsdragningsproblem vid tillämpningen som riskerar att undergräva regeringens ambition att säkerhetskänslig verksamhet ska vara undantagen från den nya regleringen.

Att så är fallet beror på att gränsdragningsproblematiken avseende tillämpningsområdet inte enbart är av teoretisk karaktär. I en komplex verksamhet kan det förväntas bli synnerligen komplicerat att löpande avgöra vilken eller vilka delar av eller moment av verksamheten som ska anses vara säkerhetskänslig, eller avse brottsbekämpning, eller inget av detta, vid tillämpningen av den nya cybersäkerhetslagen.

Kustbevakningens verksamhet

Bestämmelser om Kustbevakningens uppgifter finns bland annat i förordningen (2019:84) med instruktion för Kustbevakningen samt i kustbevakningslagen (2019:32) och kustbevakningsförordningen (2019:83). Som framgår av dessa författningar är Kustbevakningens verksamhet bred och komplex.

Säkerhetskänslig verksamhet hos Kustbevakningen

Kustbevakningen noterar att det inte går att utläsa av delbetänkandet hur utredningen har resonerat i fråga om i vilken utsträckning Kustbevakningens verksamhet är att bedöma som säkerhetskänslig (jfr s. 162 f.).

Det kan i anslutning till detta framhållas att verksamhetsutövaren själv ska bedöma vilka delar av verksamheten som är säkerhetskänslig och att detta kan variera över tid.

Säkerhetsskyddslagen gäller för den som till någon del bedriver säkerhetskänslig verksamhet, dvs. för Kustbevakningen (se 1 kap. 1 § säkerhetsskyddslagen). Den som till

någon del bedriver säkerhetskänslig verksamhet, s.k. verksamhetsutövare, ska utreda behovet av säkerhetsskydd, en s.k. säkerhetsskyddsanalys (se 2 kap. 1 § säkerhetsskyddslagen). Säkerhetsskyddsanalysen ska uppdateras vid behov och åtminstone vartannat år (se 2 kap. 1 § säkerhetsskyddsförordningen [2021:955]). Detta är ett uttryck för att vad som bedöms vara säkerhetskänslig verksamhet kan variera över tid.

Kustbevakningen är en beredskapsmyndighet som ingår i både det civila och i det militära försvaret. Detta innebär bl.a. att Kustbevakningen ska kunna ingå med resurser i Försvarsmakten. Kustbevakningen har alltså en viktig roll i totalförsvaret, något som har accentuerats på senare tid. Detta har påverkat organisationen i bredare bemärkelse; Kustbevakningen är numera en myndighet som hör till Försvarsdepartementet, i stället för som tidigare Justitiedepartementet. Tillsynsmyndighet för Kustbevakningen är numera den Militära underrättelse- och säkerhetstjänsten, i stället för som tidigare Säkerhetspolisen (jfr 6 kap. 1 § säkerhetsskyddslagen och 8 kap. 1 § säkerhetsskyddsförordningen). Det kan i sammanhanget också noteras att Försvarsmakten får meddela föreskrifter för Kustbevakningen för den del av verksamheten som under höjd beredskap ska bedrivas av Försvarsmakten (se 32 § förordningen (2007:1266) med instruktion för Försvarsmakten).

I samband med det sagda understryker Kustbevakningen att myndighetens samarbete med Försvarsmakten tydligt fortsätter att öka i omfattning och att detta är en utveckling som kommer att fortgå och vara nödvändig över tid.

Det anförda illustrerar att Kustbevakningens verksamhet i bredare bemärkelse är av betydelse för Sveriges säkerhet. Av naturliga skäl är det mycket svårt att begränsa vilka delar av den dagliga verksamheten som har en sådan betydelse till en specifik mängd information.

Brottsbekämpande verksamhet hos Kustbevakningen

Som framgår av de tidigare nämnda relevanta författningarna om Kustbevakningens uppgifter arbetar Kustbevakningen med både s.k. direkt och indirekt brottsbekämpning, dels självständigt, dels genom biträde till andra brottsbekämpande myndigheter. Sådan verksamhet är i sin helhet en tätt sammanlänkad del av den dagliga och totala verksamhet som Kustbevakningen bedriver. Kustbevakningens operativa verksamhet är händelsestyrd och komplex. Verksamheten är minutoperativ, vilket innebär att det kan skilja från en minut till annan – givet samma förutsättningar med fartyg, besättning, uppdrag och rutt – vilken verksamhet som ska bedömas vara bedriven enligt uppdelningen i 1 kap. 12 § cybersäkerhetslagen. Som framgått av författningskommentaren till 1 kap. 12 § cybersäkerhetslagen ingår förebyggande, upptäckt, utredning och lagföring av brott i begreppet brottsbekämpning enligt paragrafen.

Kustbevakningens operativa verksamhet bedrivs längs hela Sveriges kust samt i Vänern, Vättern och Mälaren, utifrån 20 kuststationer och en flygkuststation. För att leverera enligt sitt uppdrag har myndigheten utformat ett visst arbetssätt, den s.k. *kombinationstanken*. Detta innebär att Kustbevakningen kombinerar grunduppdraget med beredskap för

miljöräddningstjänst med att självständigt och på uppdrag av andra myndigheter utföra olika insatser kopplat till räddningstjänst, sjöövervakning (brottsbekämpning, kontroll- och tillsynsverksamhet och ordningshållning) och krisberedskap för att effektivt använda våra resurser och skapa mervärde för samhället. Detta arbetssätt präglar hela planeringen och genomförandet av verksamheten, liksom de enheter och kompetenser vi har för att utföra vårt jobb.

Personal, fartyg, annan materiel och ledningscentral planeras således för att hålla ständig beredskap och förmåga för räddningstjänst och miljöskydd. Den resurs Kustbevakningen har för räddningstjänstuppdraget, används samtidigt som stöd för att lösa uppgifter åt andra myndigheter. Ett exempel på en sådan uppgift är tullkontroller. Tullverket är ansvarigt för kontrollen av varor vid införsel till och utförsel från Sverige och har enligt lagen (2000:1225) om straff för smuggling även ett huvudansvar för tillhörande brottsbekämpning. Då Tullverket inte förfogar över egna fartyg, flyg, eller dykresurser utgör Kustbevakningen den maritima plattformen.

Fler exempel är fiskerikontroller som vi utför till sjöss i samråd med Havs- och vattenmyndigheten, lastsäkrings- och farligt godskontroller åt Transportstyrelsen och gränsövervakning åt Polismyndigheten, som också begär biträden i polisiära ärenden och uppgifter där Kustbevakningens kompetens och förmåga behövs.

Kustbevakningen har härmed ingen avdelad resurs enbart för brottsbekämpande verksamhet, utan denna utförs längs hela Sveriges kust av våra kustbevakningstjänstemän på de olika kuststationerna och flygkuststationen.

Utöver komplexiteten i Kustbevakningens uppdrag, tillkommer att myndighetens informationssystem är uppbyggda på ett sådant sätt att de motsvarar de krav som ställs i de regelverk som Kustbevakningen redan omfattas av enligt gällande rätt. I dagsläget används dessa för att tillgodose informationsbehovet som är anpassat till uppdragets omfattande karaktär, oavsett om det sker inom ramen för exempelvis kontroll och tillsyn eller brottsbekämpning. Den praktiska tillämpningen i Kustbevakningens IT-miljö enligt utredningens förslag vore svårhanterlig och verklighetsfrämmande. Det skulle inte heller medföra några säkerhetsvinster, utan istället försvåra informationshanteringen för myndighetens medarbetare väsentligt. Detta i sig skulle kunna öka risken för att konfidentialitet, riktighet samt tillgänglighet i myndighetens informationssystem äventyras.

Även vad gäller brottsbekämpning kommer det att följa påtagliga gränsdragningsproblem för Kustbevakningen vid tillämpning av 1 kap. 12 §. Det är så gott som omöjligt att särskilja myndighetens ordinarie verksamhet till sjöss från i vart fall ”förebyggande” respektive ”upptäckt” av brott. De insatser som genomförs inom ramen för myndighetens uppdrag avseende kontroll och tillsyn kan i sin tur resultera i upptäckt av brott och därmed övergå till brottsbekämpande verksamhet.

Cybersäkerhet hos Kustbevakningen

Som nämndes inledningsvis är det angeläget med regelverk som syftar till och som åstadkommer en hög cybersäkerhetsnivå. För Kustbevakningens vidkommande uppnås emellertid en hög cybersäkerhetsnivå redan i dag, genom gällande rätt (jfr säkerhetsskyddslagen, säkerhetsskyddsförordningen, förordningen (2022:524) om statliga myndigheters beredskap samt de föreskrifter som meddelats av Myndigheten för samhällsskydd och beredskap; MSBFS 2020:6, 2020:7 och 2020:8).

Av det sagda följer att Kustbevakningen redan i dag tillgodogör sig de säkerhetsvinster som är tänkta att följa av den nya cybersäkerhetslagen. Det kan också lyftas, vad gäller krav på utbildning av ledningen om riskhanteringsåtgärder (förslaget till 3 kap. 3 § cybersäkerhetslagen), att Kustbevakningen betraktar detta som något positivt och mycket viktigt; detta tillgodoses hos Kustbevakningen genom de ovan nämnda regleringarna oavsett om myndigheten formellt omfattas av förslaget till 3 kap. cybersäkerhetslagen eller ej.

Tillämpning av den föreslagna 1 kap. 12 § cybersäkerhetslagen, med den fragmentisering av verksamheten som det innebär, skulle enligt Kustbevakningens mening inte tjäna utan i stället tynga myndighetens verksamhet och arbetet med anknutna säkerhetsfrågor.

Incidentrapportering och tillsyn

I delbetänkandet föreslås att Myndigheten för samhällsskydd och beredskap ska vara s.k. CSIRT-enhet och vissa länsstyrelser föreslås vara tillsynsmyndigheter för offentlig förvaltning.

Vid betydande incidenter ska verksamhetsutövaren inom vissa lagstadgade tidsfrister lämna underrättelse, incidentanmälan samt lägesrapport och/eller slutrapport till CSIRT-enheten. (Se 3 kap. 4–7 §§ i förslaget till cybersäkerhetslag).

Tillsynsmyndigheten ska utöva tillsyn över att cybersäkerhetslagen och föreskrifter som meddelats med stöd av lagen följs. Tillsynsmyndigheten har undersökningsbefogenheter och ska på begäran tillhandahållas den information som behövs för tillsyn, och har rätt att få tillträde till områden, lokaler och andra utrymmen som används i verksamheten. (Se 4 kap. 2 § och 4–7 §§ i förslaget till cybersäkerhetslag).

Mot bakgrund av den föreslagna regleringen blir det svårare för Kustbevakningen att hantera och bedöma IT-incidenter. Myndigheten kommer att på mycket kort tid behöva bedöma och avgöra hur en viss IT-incident ska kategoriseras – enligt säkerhetsskyddsförordningen, enligt EU:s dataskyddsförordning, enligt MSB:s föreskrifter om incidentrapportering för statliga myndigheter, eller enligt den nya cybersäkerhetslagen – och därmed till vilken aktör den ska rapporteras. Dessutom kan detta innebära att Kustbevakningens sårbarheter exponeras för en aktör som inte är behörig till den aktuella informationen.

Förslaget i delbetänkandet innebär vidare att Kustbevakningen får fler tillsynsmyndigheter. I fråga om tillsyn enligt den nya cybersäkerhetslagen finns en betydande skillnad mellan de myndigheter som är helt undantagna från lagen (1 kap. 11 §) och de som är delvis undantagna (1 kap. 12 §). Bestämmelserna om tillsyn enligt 4 kap. gäller enligt förslaget fullt ut för den som omfattas av 1 kap. 12 §, dvs för Kustbevakningen.

Gränsen kommer att vara hårfin vad gäller att avgöra vad som för Kustbevakningen faller under ansvaret för vilken tillsynsmyndighet. Det kan ifrågasättas om det är ägnat att gagna säkerhetsarbetet. Enligt Kustbevakningens bedömning vore det naturligt och en fördel om myndigheten, liksom flera andra myndigheter inom Säkerhetspolisens och Försvarsmaktens tillsynsområde, undantas från cybersäkerhetslagens tillsynsområde (jfr utredningens resonemang om tillsynsmyndigheter på s. 220 i delbetänkandet).

Alternativ lagteknisk utformning för undantag från cybersäkerhetslagen

NIS2-direktivet ger ett visst handlingsutrymme för den nationella utformningen av undantag för vissa myndigheter från de nya cybersäkerhetsreglerna. De som *till övervägande del* bedriver verksamhet på vissa uppräknade områden bör undantas, medan de vars verksamhet *endast marginellt* hänför sig till dessa områden inte bör undantas från tillämpningsområdet. (Se artikel 2.7 och skäl 8 i ingressen till NIS2-direktivet).

Det bör särskilt noteras att direktivet inte kräver att *någon av* de uppräknade verksamheterna, endast sedd för sig, bedrivs till övervägande del för att undantag från direktivets tillämpningsområde ska vara tillåtet. Det bör alltså finnas utrymme för att i stället göra en helhetsbedömning av den verksamhet som en myndighet sammantaget bedriver på de aktuella områdena.

Förslaget med undantag enligt förordningen på grund av om verksamheten är till övervägande del *antingen* säkerhetskänslig *eller* brottsbekämpande får enligt Kustbevakningens mening olyckliga konsekvenser genom att lösningen inte medger tillräcklig hänsyn till helhetsbilden av en komplex och föränderlig verksamhet.

En möjlig annan lösning för att genomföra direktivet i denna del i svensk rätt – som också står i samklang med både NIS2-direktivet och regeringens ambition att säkerhetskänslig verksamhet ska vara undantagen i den utsträckning som är möjlig – vore bestämmelser som medger en helhetsbedömning av om myndighetens *sammantagna* verksamhet till övervägande del är säkerhetskänslig *och/eller* brottsbekämpande. Detta kan åstadkommas genom mindre justeringar i de föreslagna 1 kap. 11 § första stycket cybersäkerhetslagen samt 6 § och 7 § cybersäkerhetsförordningen.

Beslut om detta yttrande har fattats av generaldirektör Lena Lindgren Schelin. I ärendets handläggning har deltagit säkerhetshandläggaren Emina Begovic, chefen för enheten för

IT-säkerhet Mats Dufva, säkerhetschefen Anders Kolberg, chefen för rätts- och säkerhetsenheten Nina Andersson, chefsjuristen Sara Thörngren och verksjuristen Anna S Berglund, föredragande.

Lena Lindgren Schelin

Anna S Berglund

Extern digital kopia till:
Försvarsdepartementet, enheten för samhällsskydd
Försvarsdepartementet, rättssekretariatet

Intern digital kopia till:
Ledningsgruppens ledamöter
SRAT
TULL KUST
SEKO