Förvaltningsutskottet

Statsrådets försvarsredogörelse

Till försvarsutskottet

INLEDNING

Remiss

Statsrådets försvarsredogörelse (SRR 8/2021 rd): Ärendet har remitterats till förvaltningsutskottet för utlåtande till försvarsutskottet.

Sakkunniga

Utskottet har hört
- äldre avdelningsstabsofficer Tero Koljonen, försvarsministeriet
- lagstiftningsråd Jenni Herrala, försvarsministeriet
- teamledare Lauri Hirvonen, utrikesministeriet
- konsultativ tjänsteman Eero Kytömaa, inrikesministeriet
- polisöverinspektör Janne Paavola, Polisstyrelsen
- avdelningschef Jyri Rantala, skyddspolisen
- stabschef Risto Lohi, centralkriminalpolisen
- ansvarsområdesdirektör, överstelöjtnant Mikko Leppänen, Huvudstaben
- avdelningsstabsofficer, kommendörkapten Klaus Seppänen, Huvudstaben.

Skriftligt yttrande har lämnats av
- Tullen
- Finlands Polisorganisationers Förbund rf
- Officersförbundet.

UTSKOTTETS ÖVERVÄGANDEN

De senaste säkerhetsredogörelserna

Under den pågående valperioden har statsrådet, precis som under den förra valperioden, lämnat tre säkerhetsredogörelser: en utrikes- och säkerhetspolitisk redogörelse (FvUU 11/2021 rd – SRR 4/2020 rd), den aktuella försvarsredogörelsen (SRR 8/2021 rd) och en redogörelse om den inre säkerheten (SRR 4/2021 rd). Av dem är redogörelse om den inre säkerheten den viktigaste med avseende på förvaltningsutskottets ansvarsområde. För närvarande behandlas redogörelsen i ut-

skottet, som ska lämna ett betänkande om den. Förvaltningsutskottet anser det vara viktigt att beredningen av säkerhetsredogörelserna bygger på en gemensam lägesbild, trots att omvärlden delvis beskrivs utifrån olika prioriteringar.

I utlåtandet om den utrikes- och säkerhetspolitiska redogörelsen (FvUU 11/2021 rd) anser utskottet det vara positivt att säkerheten ses ur ett brett perspektiv i redogörelsen. Också redogörelsen om den inre säkerheten baserar sig på ett brett säkerhetsbegrepp. Det är nödvändigt att betrakta säkerhetsfrågorna ur ett sammanhållet perspektiv för att kunna upptäcka ömsesidiga beroendeförhållanden och se faktorer och fenomen med stor relevans för Finlands säkerhet. Olika typer av hot och risker är allt tätare sammanflätade med varandra. Säkerheten kan inte längre delas in i yttre och inre säkerhet, utan dessa två dimensioner av säkerheten är nära förbundna med varandra. Finlands militära försvar och den övergripande säkerheten knyts allt närmare till varandra. Följaktligen understryks vikten av en gemensam lägesbild för myndigheterna i en föränderlig omvärld.

Omvärldsanalysen i den utrikes- och säkerhetspolitiska redogörelsen har styrt beredningen av försvarsredogörelsen. I försvarsredogörelsen läggs de försvarspolitiska riktlinjerna för att upprätthålla och utveckla Finlands försvarsförmåga fast. Med försvarsredogörelsen och verkställigheten av den säkerställer statsrådet att Finlands försvarsförmåga motsvarar kraven i omvärlden. Kraven på försvarsberedskapen är i allt högre grad kopplade till cybervärlden, rymden och informationsaktiviteter. Riktlinjerna i redogörelsen sträcker sig till slutet av 2020-talet.

Alla dessa redogörelser lyfter fram det instabila och svårförutsägbara säkerhetsläget i Finlands och Europas närområden. Av omvärldsbeskrivningarna i redogörelserna framgår sambandet mellan globala förändringskrafter och inre säkerhet. Vid sidan av de traditionella hoten lyfts helt motiverat också globala utvecklingstrender, den tilltagande stormaktskonkurrensen och statliga hybridattacker.

Under valperioden har det tillsatts parlamentariska uppföljningsgrupper med uppdrag att följa upp beredningen av den utrikes- och säkerhetspolitiska redogörelsen, försvarsredogörelsen och redogörelsen om den inre säkerheten. Förvaltningsutskottet anser det viktigt att säkerhetsredogörelserna också i fortsättningen bereds i parlamentariskt samarbete.

Utskottet har i sina utlåtanden om tidigare redogörelser ansett det vara viktigt att de till buds stående, relativt begränsade resurserna med avseende på den övergripande säkerheten i allt högre grad också avsätts för arbete inom utrikes- och säkerhetspolitiken. Också i försvarsredogörelsen nämns behovet av att utnyttja alla samhälleliga resurser för att upprätthålla en försvarsförmåga som motsvarar kraven i omvärlden. Extra viktigt är det att myndigheterna inom den inre säkerheten har adekvata resurser. De myndigheter som svarar för den inre säkerheten, framför allt polisen och Gränsbevakningsväsendet, intar en framträdande roll för att skydda samhället. De här myndigheterna är också de första att möta de nya typer av säkerhetshot som beskrivs i redogörelsen, exempelvis olika former av hybridangrepp. Myndigheterna måste dessutom ha uppdaterade befogenheter och adekvata resurser för att möta nya typer av hot. Också i riksdagsbehandlingen av redogörelser är det nödvändigt att tydligare granska den övergripande säkerhet som skapas utifrån den inre och den yttre säkerheten och dess kontaktytor.

Bredspektrig påverkan (hybridpåverkan)

Försöken att skada vårt samhälle har ökat och metoderna är många, enligt försvarsredogörelsen. Trots det skärpta internationella läget är Finland inte utsatt för något direkt militärt hot, men vi måste räkna med att Finland kan komma att utsättas för eller utsättas för hot om militär makt.

I flera utlåtanden på senare tid har utskottet behandlat hybridangrepp i ett samlat perspektiv, där metoderna kan bestå av exempelvis politiska, diplomatiska, ekonomiska och militära medel samt informationspåverkan och cyberangrepp. Utskottet hänvisar till sina tidigare kommentarer i ärendet (t.ex. FvUU 11/2021 rd och FvUB 5/2017 rd).

Försvarsredogörelsen betraktar hoten ur militär synvinkel som påverkan över ett brett spektrum. Bred påverkan inbegriper metoder för hybridangrepp, men i hotbilden ingår också öppen användning av militära maktmedel mellan parterna. Påverkan med ett brett spektrum beskrivs som systematisk verksamhet som kombinerar olika metoder och ofta är långvarig. Det kan vara svårt att upptäcka den typen av påverkan, och den utnyttjar sårbarheter i samhället redan under normala förhållanden. Syftet är att rubba försvarsförmågan i målstaten, till exempel genom att skapa osäkerhet bland befolkningen och försämra försvarsviljan och handlingsförmågan hos den politiska ledningen.

Det har uppstått en systematisk konkurrenskonstellation mellan demokratiska rättsstater och en auktoritär förvaltningsmodell och den styr främmande staters underrättelse- och påverkansverksamhet i Finland. Underrättelse i cybermiljö ökar hela tiden. Även i övrigt är Finland fortfarande ständigt föremål för omfattande underrättelseverksamhet från främmande stater. Bland de viktigaste syftena med underrättelseverksamheten här är att göra prognoser av skeenden inom olika delområden i Finlands politik och i övrigt påverka det politiska beslutsfattandet. Också tillämpad teknisk forskning och produktutveckling vid universitet, forskningsinstitut och företag ingår i underrättelseverksamheten.

Även migration och asylsökande kan användas som verktyg för hybridpåverkan. Det har på senare tid kunnat observeras vid gränsen mellan Schengenområdet och Vitryssland. Påverkan kan också ske under förevändning av epidemier och pandemier. Åtgärderna är ofta diskreta och mållandet kan inte vara säkert på om det är en avsiktlig insats som leds av en främmande stat. Enligt utskottet måste också Finland räkna med den här typen av påverkan, och vår lagstiftning måste ge myndigheterna ett tillräckligt stort urval av metoder för att ingripa i fenomenet.

Utskottet konstaterar att det i dag är betydligt svårare att identifiera aktörerna bakom hybridhoten och att uppfatta kombinationerna av olika hot. Bakom hoten kan det dölja sig enskilda personer eller grupper av personer, men också statliga aktörer. De kan utnyttja organiserade kriminella grupper eller enskilda medlemmar i sådana grupper för sina syften. Enligt uppgifter till utskottet finns det tecken som tyder på att det var fallet exempelvis när Ryssland intog Krim.

I sakkunnigutfrågningen lyftes så kallad flyktingspionage fram. Därmed avses att en främmande stat försöker inhämta information eller utöva påtryckning och uttala hot mot sina egna eller tidigare medborgare som är bosatta i Finland. Med avseende på lagstiftningen påpekar utskottet att

exempelvis underrättelseverksamhet som en främmande stat riktar sig mot personer är olaglig i till exempel Sverige och Norge, men inte har inte kriminaliserats i Finland.

Gemensamt för hybridhoten är att de är avsiktliga störningar som inte är lika allvarliga som traditionell krigföring, exempelvis terroristhandlingar eller andra brottsliga handlingar. De uppfyller trots det inte nödvändigtvis brottsrekvisiten. I Finland är det polisen och i vissa fall Gränsbevakningsväsendet som har ansvar för att bekämpa och utreda hybridhot, om gärningen uppfyller brottsrekvisiten eller om det handlar om att förhindra eller avslöja en sådan gärning. Myndigheterna inom den inre säkerheten ska därför ha förmåga att upptäcka och identifiera hot av olika grad och tillräckliga resurser för att förhindra och hantera dem.

Försvarsmakten garderar sig inför bredspektrig påverkan tillsammans med de andra aktörerna som ett led i den modell för övergripande säkerhet som är under utveckling, enligt redogörelsen. Samarbetet mellan myndigheterna måste alltjämt utvecklas inom cyberförsvar, strategisk kommunikation och informationsförsvar. Vid bekämpningen av bredspektrig påverkan är det viktigt att alla aktörer kan ta ansvar för sina uppdrag enligt principerna i lagstiftningen och för den övergripande säkerheten, framhåller utskottet. Även om det i synnerhet i cybermiljö inte alltid är fullkomligt klart om hot mot samhällsfunktioner i grunden är militära hot, är det för möjligheterna att bekämpa hoten av största vikt att de civila och militära myndigheternas roller och uppgiftsfördelning är så tydligt definierade som möjligt i lagstiftningen.

För att kunna svara på metoderna för bredspektrig påverkan krävs det, som det sägs i redogörelsen, att modellen för den övergripande säkerheten och myndighetssamarbetet ses över. Statsledningens och myndigheternas gemensamma lägesuppfattning och ledningsförmåga intar en framträdande roll vid en omfattande militär kris. För beredskapen inför sektorsövergripande hybridhot krävs det överlag en gemensam lägesbild och en övergripande utveckling av prognostiseringen. Hybridoperationer måste kunna upptäckas så tidigt som möjligt för att de ska kunna förhindras effektivt. Detta förutsätter nära samarbete mellan myndigheterna, en heltäckande lägesbild och en samordnande ledningsstruktur. I sektorsövergripande situationer som utvecklas snabbt måste ledningsstrukturerna kunna möjliggöra effektiv ledning och samordning av verksamheten. Utskottet betonar vikten av en smidig information vid rätt tidpunkt och ett tydligt ledningssystem som ett led i mekanismen. Det är också viktigt med samarbete mellan den statliga och den lokala nivån samt mellan myndigheterna och den privata sektorn.

Utskottet understryker betydelsen av effektiv gränsförvaltning i bekämpningen av hybridhot. Gränsbevakningsväsendet är behörig myndighet med en självständig roll i gränszonen mellan inre och yttre säkerhet. Gränsbevakningsväsendets höga beredskap, befogenheter och prestationsförmåga ska enligt redogörelsen utnyttjas som stöd för försvarssystemet för att övervaka och säkerställa den territoriella integriteten. När situationen kräver det ansluts gränstrupperna till försvarsmakten.

Cybersäkerhet

Utskottets utlåtande om den utrikes- och säkerhetspolitiska redogörelsen (FUU 11/2021 rd) innehåller en omfattande behandling av frågor om säkerheten i cybermiljön.

Den pågående omvälvningen i den tekniska utvecklingen gäller nästan alla delområden i samhället. Tekniken erbjuder nya verktyg och ökade möjligheter att effektivisera informationsutbytet och växelverkan. Digitala lösningar kan medverka till större säkerhet.

Digitalisering kommer också att i allt större omfattning inverka på omvärlden i försvarssammanhang. Ny teknik och digitalisering möjliggör nya påverkansmöjligheter som kan äventyra samhällets vitala funktioner och vara ett hot mot den kritiska infrastrukturen. Kontaktytorna mellan normala förhållanden och olika typer av konflikter har delvis suddats ut. Förvarningstiden för konflikter har blivit kortare och oförutsägbarheten har ökat. Det är faktorer som ställer större krav på beslutsfattandet och verkställigheten av beslut, och i synnerhet på att förbättra lägesbilden, beredskapen och förvarningsförmågan.

Försvarsredogörelsen lyfter fram hur utvecklingen av digitalisering, artificiell intelligens, autonom teknik och sensorteknik påverkar i synnerhet cyber-, rymd- och informationsförsvaret. Ny teknik kan användas till exempel för att behandla information, skapa lägesbilder, styra vapensystem och hantera logistik. Beslutsfattandet kan stödjas med mer exakt och snabbare information. Samtidigt är det nödvändigt att på bred front förstå de säkerhetshot, de möjligheter till missbruk och det ömsesidiga beroende som är förenade med utvecklingen. Riskerna och hoten mot säkerheten i kommunikationsnäten och sårbarheten i den kritiska infrastrukturen i samhället har ökat. Samhällena bygger i allt högre grad på den nya generationens kommunikationsnät, bland annat 5G-nät och artificiell intelligens. I takt med samhällets digitalisering är det extra viktigt att säkerställa en säker cybermiljö.

Utskottet har också tidigare påpekat att den förändrade digitala omvärlden kräver nära nationellt och internationellt samarbete. Integreringen av cyberförsvaret i den operativa verksamheten bör fortsätta, sägs det i redogörelsen. Cyberförsvarsförmågan ska också inkluderas i samarbetet mellan ansvarsområdena, myndigheterna och det övriga samhället. Statsrådet godkände 2019 ett principbeslut om en strategi för cybersäkerheten i Finland. I riktlinjerna betonas internationellt samarbete, ledarskap, planering, beredskap och kompetensutveckling inom cybersäkerheten. Utifrån strategin har det senare upprättats ett program för utveckling av cybersäkerheten. Utskottet konstaterar att det behövs lägesförståelse och tydligt ledningsansvar för den strategiska ledningen av cybersäkerheten. Betydelsen av ett smidigt informationsflöde framhävs också.

Cyberspionage handlar om intrång i informationssystem för att inhämta hemlig information. Syftet med cyberspionage är att inhämta information som ger spionagestaten en bättre ställning i den globala konkurrensen eller minskar målstatens spelrum. Ofta kränker cyberspionage de grundläggande fri- och rättigheterna för befolkningen i mållandet, bland annat rätten till privatliv eller förtrolig kommunikation. Cyberspionage är ett verktyg för auktoritära stater, eftersom det krävs en uttrycklig vilja från den statens sida att kränka en annan stats suveränitet.

Förändringarna i den allvarliga och organiserade brottsligheten i Europa får återverkningar också i Finland, understryker utskottet. Den organiserade brottsligheten har blivit mer utbredd, tuffare och mer internationell. Samtidigt ökar och utvecklas brottsligheten över eller med hjälp av nätet snabbt, likaså cyberbrottsligheten. Utöver det ökade antalet nätbedrägerier mot enskilda medborgare har också fallen av överbelastningsattacker och dataintrång och anknytande utpressning blivit fler. De kan användas för att skada och förhindra verksamheten i företag och myndigheter

som är av kritisk betydelse för samhället. Enligt en sakkunnigbedömning kommer cyberbrottsligheten i framtiden att utgöra ett nästan lika stort hot mot den inre säkerheten som den traditionella brottsligheten, som också i allt högre grad flyttar över till nätet. För att kunna bekämpa cyberbrottsligheten behövs det omfattande internationellt samarbete. Polisen måste få faktiska möjligheter att bekämpa cyberbrottslighet. Också det internationella samarbetet måste stärkas ytterligare.

Utskottet anser det viktigt att cybersäkerheten ägnas större uppmärksamhet inom alla verksamhetsnivåer. Cybersäkerheten måste förbättras över hela linjen och utvecklingsåtgärderna måste planeras och genomföras omsorgsfullt. Samhället är helt beroende av den digitala omvärlden och de vitala samhällsfunktionerna måste därför kunna säkras under alla förhållanden.

För att försvarssystemets cyberlägesbild ska kunna förbättras och cyberhoten förhindras och avvärjas krävs det att myndigheterna förbättrar sitt informationsutbyte, får nya befogenheter och ser över sina nationella samarbetsstrukturer, enligt redogörelsen. Enligt utskottets uppfattning fungerar samarbetet mellan myndigheterna mycket bra i Finland. I synnerhet samarbetet mellan säkerhetsmyndigheterna är smidigt och ledningsansvaret huvudsakligen tydligt. Trots det är det motiverat att utreda vilka behoven det finns att utveckla myndighetssamarbetet, anser utskottet.

Utveckling av lagstiftningen

Hoten inom cybermiljön och de anknytande nationella utvecklingsåtgärderna bedöms enligt redogörelsen i utvecklingsprogrammet för cybersäkerhetsstrategin och i ett kommande utredningsarbete. I utredningen bedöms myndigheternas förutsättningar för att trygga nationell cybersäkerhet, bekämpa cyberbrottslighet och deras möjligheter vara aktiva inom cyberförsvaret och i snabbt eskalerande situationer där cybersäkerheten i samhället är hotad. Utgående från utredningsarbetet inleds åtgärder för att utveckla cyberförsvaret, inbegripet nödvändig lagberedning. Åtgärderna syftar till att säkerställa att cyberförsvaret har de befogenheter, den kompetens och de rättigheter att få information som säkerhetsmiljön kräver.

Utskottet konstaterar att tidigare lagändringar har förbättrat myndigheternas kapacitet inför olika typer av säkerhetshot. Lagstiftningen om gränsbevakningen ändrades under den förra valperioden. Det har förbättrat möjligheterna för myndigheterna att bedriva samarbete och vidta åtgärder också vid hybridangrepp. Vidare har den nya underrättelselagstiftningen förbättrat myndigheternas möjligheter möta hot mot den nationella säkerheten. Myndigheterna måste ha tillräckliga befogenheter att tillämpa till buds stående metoder i störningssituationer proaktivt, snabbt och flexibelt. Tillräckliga befogenheter måste dessutom vara tillgängliga redan under normala förhållanden.

Enligt redogörelsen har handräckningsuppdragen blivit mer krävande och tidskritiska. Riksdagen behandlar för närvarande en proposition om en ny lag om Försvarsmaktens handräckning till polisen (RP 106/2021 rd). Propositionen förtydligar och uppdaterar bestämmelserna om handräckning till polisen för att de ska motsvara de förändrade kraven i säkerhetsmiljön. I redogörelsen nämns dessutom behovet av att se över beredskapslagen (1552/2011) och ändra territorialövervakningslagen (755/2000). Beredskapslagens definition av undantagsförhållanden innefattar exempelvis inte allvarligt äventyrande av den inre säkerheten eller situationer med omfat-

tande invandring. Sakkunniga framhöll också behovet av att se över lagstiftningen om kriminalunderrättelse, polisens skyldighet att göra förundersökning och informationsutbyte mellan myndigheterna. Enligt uppgifter till utskottet uppfyller den gällande lagstiftningen inte till alla delar kraven på operativ kriminalunderrättelse inom polisen, som är brottsbekämpande myndighet i den förändrade säkerhetspolitiska miljön. Dessutom är det viktigt att polisen omedelbart och på de villkor som ställs i lagstiftningen får tillgång till uppgifter som den behöver för att kunna bekämpa, avslöja och utföra förundersökning av brott och hot.

FÖRSLAG TILL BESLUT

Förvaltningsutskottet anför

att försvarsutskottet bör beakta det som sägs ovan.

Helsingfors 28.10.2021

I den avgörande behandlingen deltog

ordförande Riikka Purra saf
medlem Tiina Elo gröna
medlem Jussi Halla-aho saf
medlem Eveliina Heinäluoma sd
medlem Hanna Holopainen gröna
medlem Aki Lindén sd
medlem Mauri Peltokangas saf
medlem Juha Pylväs cent
medlem Matti Semi vänst
medlem Kari Tolvanen saml
medlem Heidi Viljanen sd
ersättare Ben Zyskowicz saml.

Sekreterare var

utskottsråd Henri Helo.