Försvarsutskottet

Statsrådets redogörelse för den inre säkerheten

Till förvaltningsutskottet

INLEDNING

Remiss

Statsrådets redogörelse för den inre säkerheten (SRR 6/2025 rd): Ärendet har lämnats till försvarsutskottet för eventuellt utlåtande till förvaltningsutskottet. Tidsfrist: 05.11.2025.

Sakkunniga

Utskottet har hört
- specialsakkunnig Eeva Koivunen, inrikesministeriet
- äldre avdelningsstabsofficer Thomas Gentz, försvarsministeriet
- polisöverinspektör Vesa Pihajoki, Polisstyrelsen
- avdelningschef, brigadgeneral, Gräns- och sjöavdelningen Mika Rytkönen, Gränsbevakningsväsendet
- överstelöjtnant Tomi Iikkanen, Huvudstaben
- överdirektör Hannu Naumanen, Statens center för informations- och kommunikationsteknik
- ledande beredskapsexpert Mauri Vierula, Försörjningsberedskapscentralen
- verkställande direktör Timo Lehtimäki, Suomen Erillisverkot Oy.

UTSKOTTETS ÖVERVÄGANDEN

Allmänt

(1) I redogörelsen beskrivs verksamhetsmiljön för den inre säkerheten och dess förändring samt fastställs de viktigaste fokusområdena och målen för politiken för inre säkerhet. Redogörelsen fastställer tillsammans med riksdagens betänkande de centrala riktlinjerna för Finlands inre säkerhetspolitik under de kommande åren. Den innehåller också en översikt över den allmänna utvecklingen inom den inre säkerheten och de viktigaste förändringarna i förhållande till den föregående redogörelsen om inre säkerhet.

(2) Enligt utskottet visar redogörelsen väl att den inre och den yttre säkerheten bildar en helhet. Yttre hot är militära först i ett ytterst allvarligt läge, och ansvaret för att effektivt avvärja andra hot ligger hos aktörerna inom den inre säkerheten. Dessa har en nyckelroll när det gäller att trygga

samhällets störningsfria funktion, bemöta hybridhot, skydda den kritiska infrastrukturen och skydda befolkningen. Exempelvis är säkerheten och resiliensen hos den kritiska undervattensinfrastrukturen en central fråga för Finlands nationella säkerhet.

(3) Redogörelsen för den inre säkerheten bildar tillsammans med den utrikes- och säkerhetspolitiska och den försvarspolitiska redogörelsen en helhet av tre säkerhetsredogörelser. Vid beredningen av redogörelsen för den inre säkerheten har omvärldsanalysen i statsrådets utrikes- och säkerhetspolitiska redogörelse beaktats. Utskottet konstaterar att försvarsredogörelsen skiljer sig från de två övriga redogörelserna genom att dess tidsperspektiv är cirka tio år och att den innehåller konkreta riktlinjer för utvecklingen inom förvaltningsområdet. Redogörelserna för utrikes- och säkerhetspolitiken och den inre säkerheten fokuserar i stor utsträckning på en valperiod.

(4) Utskottet konstaterar att redogörelserna som analyserar den yttre och den inre säkerheten är Finlands politiska budskap till omvärlden om hur Finland ser på sin säkerhetsmiljö, vilka problem och hot som finns samt hur Finland avser att förbereda sig för dessa. Utanför Finland bedöms redogörelserna ur flera olika perspektiv.Det är viktigt att gränssnitten mellan inre och yttre säkerhet beaktas, eftersom dagens säkerhetshot inte längre följer den traditionella uppdelningen mellan inre och yttre hot. Att förstå och hantera gränssnitten säkerställer att säkerheten kan upprätthållas på ett övergripande och effektivt sätt.

(5) På grund av redogörelsernas långa tidsperspektiv är det nödvändigt att finna ett så brett parlamentariskt samförstånd som möjligt för att möjliggöra ett långsiktigt och konsekvent utvecklingsarbete. Utskottet upprepar här sin tidigare framförda uppfattning att det med tanke på helheten av redogörelser vore motiverat att samma parlamentariska uppföljningsgrupp styr beredningen av alla tre redogörelser.

Betydelsen av fungerande myndighetssamarbete i hanteringen av olika hot

(6) Samarbete mellan säkerhetsmyndigheter, informationsutbyte och en gemensam lägesbild samt lagstiftning som stöder denna helhet och tillräckliga myndighetsresurser är nödvändiga för hela Finlands säkerhet. Detta gäller inte bara cyberdimensionen utan också alla andra hotbilder. Utskottet betonar behovet av tydliga ledningsförhållanden och snabb reaktionsförmåga.

(7) Utskottet anser att polisen och Gränsbevakningsväsendet är Försvarsmaktens viktigaste samarbetspartner bland säkerhetsmyndigheterna. Samarbetet mellan polisen och Försvarsmakten har långa traditioner och verksamheten har kontinuerligt utvecklats och fördjupats. Under undantagsförhållanden kan Gränsbevakningsväsendet helt eller delvis anslutas till Försvarsmakten. Oavsett om en anslutning görs eller inte, fortsätter Gränsbevakningsväsendet med sina grundläggande uppgifter — gränsövervakning, gränskontroller och sjöräddning — men dess verksamhet anpassas till rikets allmänna försvar.

(8) Samarbetet mellan säkerhetsmyndigheterna i den operativa verksamheten, både i form av handräckning och andra gemensamma operationer samt i olika övningar, sker regelbundet och i praktiken varje vecka. Enligt utredning till utskottet har polisen och Försvarsmakten under de senaste åren övat på att bemöta sådana hybridhot som i inledningsskedet inte kan identifieras som militära, bland annat i lokalförsvarsövningar runt om i Finland.

(9) Den operativa verksamheten och myndighetsledningen påverkas i hög grad också av de it-system som används och deras informationssäkerhetsnivå. Enligt utredning till utskottet finns det fortfarande inget säkert system för informationsutbyte mellan myndigheterna. Detta måste ses som en mycket allvarlig brist, eftersom behovet av informationssäkra kommunikationsförbindelser ständigt ökar. Utskottet anser att det är viktigt att redogörelsen innehåller en skrivning om att Finland behöver ett säkert och kriståligt myndighetskommunikationsnätverk.

(10) Utskottet påpekar att polisen inte har någon egen reserv, utan den opererar under alla förhållanden med de resurser som finns tillgängliga redan under normala förhållanden. Ett mer omfattande eller långvarigt hybridhot orsakar uppenbara problem med tanke på polisens beredskap, och polisens verksamhet kan inte bygga på handräckning från andra myndigheter. Vid ett omfattande hybridhot är andra säkerhetsmyndigheters förmåga att stödja polisen med handräckning i vilket fall som helst begränsad, eftersom de fokuserar på sina egna kärnuppgifter. Enligt utskottets uppfattning har även polisen ett tydligt behov av en egen reserv, som fungerar både som ett verktyg för att reglera polisens beredskap och som en del av samhällets övergripande säkerhetsberedskap.

(11) Utskottet stöder starkt det som i redogörelsen för den inre säkerheten sägs om att polisens prestationsförmåga borde utvecklas så att den motsvarar de krav som följer av förändringarna i omvärlden. Målet bör enligt redogörelsen vara att öka den operativa personalen med totalt 10 procent under de två följande regeringsperioderna, till en nivå av minst 8 800 årsverken. Viktigt är också riktlinjerna om att Polisens och Gränsbevakningsväsendets driftskostnader och Gränsbevakningsväsendets investeringar borde indexjusteras årligen i efterhand för att motsvara den faktiska höjningen av kostnadsnivån.

Cybersäkerhet och informationspåverkan

(12) Enligt utskottets uppfattning behandlas cybersäkerhet och samhällets digitalisering ganska ytligt i redogörelsen, särskilt med tanke på att cybersäkerhetsfrågorna är av kritisk betydelse för hela samhällets funktionsförmåga. Utskottet påpekar att olika förvaltningsområden utvecklar cybersäkerheten till stor del på egen hand (silotänkande). Åtgärder som vidtas utan effektiv och samlad koordination och informationsutbyte blir oundvikligen ofullständiga och leder till slöseri med redan begränsade resurser. Det är särskilt viktigt att uppmärksamma ledningsstrukturerna. I en krissituation måste det alltid vara klart vilken myndighet som leder och styr verksamheten.

(13) Utskottet betonar att det är nödvändigt att anvisa resurser för cybersäkerhet och cyberförsvar. Finland använder årligen nästan 300 miljoner euro för att säkerställa cybersäkerheten inom statsförvaltningen, exklusive försvarsförvaltningens satsningar. Den förändrade omvärlden ökar ytterligare kraven på beredskap inför cyberhot. Försvarsutskottet har ingående behandlat frågor som rör cybersäkerhet och cyberförsvar ingående i sitt betänkande om försvarsredogörelsen (FsUB 5/2025 rd).

(14) Myndighetssamarbetet i Finland har till stor del baserats på frivillig nätverksbildning, men behovet av mer permanenta samarbetsstrukturer har identifierats. Mot denna bakgrund anser utskottet att det är ytterst nödvändigt att det i början av 2025 inrättades en permanent samarbets-

grupp för cybersäkerhet mellan olika ämbetsverk med företrädare för alla behöriga cybersäkerhetsmyndigheter.

(15) Kvanttekniken och den ständigt ökande användningen av artificiell intelligens kommer i framtiden att ha en betydande inverkan på Finlands försvar och säkerhet. Dess inverkan gäller särskilt underrättelseverksamhet, kommunikation, kryptering och beräkningskapacitet. Utskottet anser det vara ytterst viktigt att Finland har högklassig kompetens inom nationella krypteringslösningar.

(16) Digitaliseringen förbättrar den inre säkerheten genom att effektivisera myndigheternas informationsutbyte, krishantering och medborgarnas deltagande. Samtidigt ökar det dock beroendet av datanät och exponerar samhället för cyberhot, dataintrång och desinformation. Därför kan fördelarna med digitaliseringen uppnås endast genom satsningar på stark cybersäkerhet, dataskydd och medborgarnas mediekompetens.

(17) I redogörelsen konstateras att splittrad reglering och uppgiftsfördelning, olika verksamhetsmodeller och avsaknaden av gemensamma informationssystem kräver samverkan. Grunderna för denna samverkan beskrivs i cybersäkerhetsstrategin 2024 och i samhällets säkerhetsstrategi. Enligt redogörelsen bör upptäckten och bekämpningen av cyberhot i framtiden förbättras bland annat genom att säkerställa smidigt informationsutbyte mellan centrala aktörer samt tillräckliga befogenheter för myndigheterna.

(18) Som medlem av EU och Nato är Finland föremål för ständig fientlig informationspåverkan, som är av ett mer mångsidigt slag än tidigare. Utskottet konstaterar att informationspåverkan är ett av de allvarligaste globala hoten. Vid fientlig statlig informationspåverkan används nya tekniker och påverkningsplattformar, och utvecklingen av framför allt artificiell intelligens gör att informationspåverkan och den desinformation som ingår i dess metodutbud kan riktas mer exakt och är skadligare än tidigare. Det ställer krav på sammanhållningen och kriståligheten i hela samhället. I bekämpningen av informationspåverkan är det avgörande att öka medborgarnas och mediernas medvetenhet samt att satsa på medieutbildning.

Sammanfattning

(19) Ett nära samarbete mellan säkerhetsmyndigheter, informationsutbyte och en så gemensam lägesbild som möjligt samt lagstiftning som stöder denna helhet och tillräckliga myndighetsresurser är nödvändiga för hela Finlands säkerhet. Detta gäller inte bara cyberdimensionen utan också alla andra hotbilder. Utskottet betonar att det inte får finnas svaga länkar i säkerhetsmyndigheternas befogenheter och resurser. Försvarsmakten anvisas mycket betydande tilläggsresurser, men samtidigt måste det säkerställas att i synnerhet polisens och Gränsbevakningsväsendets resurser är på den nivå som den utmanande säkerhetsmiljön kräver.

(20) Utskottet påpekar att man vid toppmötet i Haag i juni 2025 kom överens om att Natoländerna senast 2035 ska använda 3,5 procent av sin bruttonationalprodukt till hård säkerhet och 1,5 procent till andra åtgärder som stöder säkerheten. De resurser som i Finland används för att utveckla den inre säkerheten kan enligt utskottet naturligt inkluderas i detta mål på 1,5 procent. Ut-

skottet påpekar att Ukrainas erfarenheter visar att de inre säkerhetsmyndigheterna spelar en central roll som förstainsatspersonal i en krissituation.

(21) Utskottet betonar att skyddet av kritisk infrastruktur också måste beakta Åland. Det är positivt att redogörelsen tämligen ingående bedömer Ålands betydelse (s. 16—17). Viktiga energi-, datakommunikations- och havsförbindelser går via Åland. Utskottet instämmer i redogörelsens uppfattning att samarbetet mellan polismyndigheterna i Fastlandsfinland respektive Åland bör fördjupas så att myndigheterna har beredskap att bemöta olika hybridhot. Samarbete mellan polisen i Fastlandsfinland och polisen på Åland i en krissituation kan försvåras av administrativa och lagstiftningsmässiga skillnader, utmaningar i kommunikationen och begränsade resurser på Åland. Också skillnader i språk och verksamhetskultur kan bromsa upp samarbetet.

(22) Utskottet uppmärksammar också behovet av att skydda el- och telekommunikationskablar samt den ryska skuggflottans verksamhet i Finska viken. Den utmanande utredningen i fallet Eagle S är ett bra exempel på oklarheterna i den internationella sjörätten när det gäller att ställa förövarna till svars för sina handlingar.

(23) I regeringsprogrammet för statsminister Orpos regering sägs det att antalet utomhusskjutbanor ska höjas till 1 000 före utgången av årtiondet. Utskottet konstaterar att det också pågår stora inomhusskjutbaneprojekt som, om de genomförs, i hög grad skulle betjäna myndighetsverksamheten. Det är viktigt att samhället stöder dessa projekt. Utskottet stöder starkt en verksamhetsmodell där inrikesministeriet tar en starkare roll i tillståndsregleringen för skjutbanor. Det skulle påskynda den för närvarande alltför långsamma tillståndsprocessen. Ett tillräckligt och rikstäckande nätverk av skjutbanor är också en fråga om inre säkerhet, eftersom skjutbanor har stor betydelse för myndighetsaktörer, reservister, sportskyttar och jägare.

(24) Nätverkande och partnerskapssamarbete mellan Försvarsmakten och aktörer i det civila samhället är av avgörande betydelse för Försvarsmaktens logistiska system under normala förhållanden och undantagsförhållanden. Strategiskt partnerskap är den djupaste formen av samarbete mellan Försvarsmakten och en tjänsteleverantör inom den privata sektorn. Utgångspunkten är ett avtalsbaserat starkt, hållbart och långvarigt samarbete som fortsätter också under undantagsförhållanden. Syftet med partnerskapen är att säkerställa försörjningsberedskapen, den övergripande säkerheten och försvarsförmågan också under undantagsförhållanden. Försvarsmaktens strategiska partner är till exempel Försvarsfastigheter och Suomen Erillisverkot Oy. Utskottet anser att också polisen och andra aktörer inom den inre säkerheten kan behöva olika slags partnerskap med forskningsinstitut, högskolor och företag.

FÖRSLAG TILL BESLUT

Försvarsutskottet föreslår

att förvaltningsutskottet beaktar det som sägs ovan.

Utlåtande FsUU 14/2025 rd

Helsingfors 6.11.2025

I den avgörande behandlingen deltog

ordförande Heikki Autto saml
medlem Miko Bergbom saf
medlem Timo Heinonen saml
medlem Hanna Holopainen gröna
medlem Tomi Immonen saf
medlem Riitta Kaarisalo sd
medlem Pauli Kiuru saml
medlem Jani Kokko sd
medlem Juha Mäenpää saf
medlem Jari Ronkainen saf
medlem Paula Werning sd
ersättare Sari Tanus kd.

Sekreterare var

utskottsråd Heikki Savola.