Utlåtande FvUU 7/2018 rd– RP 198/2017 rd

Förvaltningsutskottet

Regeringens proposition till riksdagen med förslag till lag om ändring av 10 § i Finlands grundlag

Till grundlagsutskottet

INLEDNING

Remiss

Regeringens proposition till riksdagen med förslag till lag om ändring av 10 § i Finlands grundlag (RP 198/2017 rd): Ärendet har remitterats till förvaltningsutskottet för utlåtande till grundlagsutskottet.

Sakkunniga

Utskottet har hört
- lagstiftningsdirektör Tuula Majuri, justitieministeriet
- specialsakkunnig Anu Mutanen, justitieministeriet
- riksdagens justitieombudsman Petri Jääskeläinen, Riksdagens justitieombudsmans kansli
- referendarieråd Mikko Eteläpää, Riksdagens justitieombudsmans kansli
- äldre justitieombudsmannasekreterare Minna Ketola, Riksdagens justitieombudsmans kansli
- direktör Teija Tiilikainen, Utrikespolitiska institutet
- äldre forskare Teemu Tammikko, Utrikespolitiska institutet
- kanslichef Hiski Haukkala, Republikens presidents kansli
- polisavdelningens lagstiftningsdirektör Katriina Laitinen, inrikesministeriet
- lagstiftningsråd Marko Meriniemi, inrikesministeriet
- konsultativ tjänsteman Heli Heikkola, inrikesministeriet
- gränsbevakningsöverinspektör Reijo Lahtinen, inrikesministeriet
- gränssäkerhetsexpert, överstelöjtnant Jussi Sainio, inrikesministeriet
- lagstiftningsdirektör Hanna Nordström, försvarsministeriet
- regeringssekreterare Kosti Honkanen, försvarsministeriet
- ledande expert, ambassadör Marja Lehto, utrikesministeriet
- överinspektör Maija Rönkä, kommunikationsministeriet
- direktör Matti Saarelainen, Europeiska kompetenscentret för motverkande av hybridhot
- polisöverdirektör Seppo Kolehmainen, Polisstyrelsen
- chef, polisråd Robin Lardot, centralkriminalpolisen
- chef, polisråd Antti Pelttari, skyddspolisen
- polischef, poliskommendör Lasse Aapio, Helsingfors polisinrättning
- forskare, doktor i militärvetenskaper Saara Jantunen, Försvarsmaktens forskningsanstalt

- underrättelsechef Harri Ohra-aho, Huvudstaben
- äldre avdelningsstabsofficer Juha-Antero Puistola, Säkerhetskommittén
- biträdande professor Katri Pynnöniemi, Alexanderinstitutet, Helsingfors universitet
- direktör Jarkko Saarimäki, Kommunikationsverket
- Direktör, planerings- och analysavdelningen Christian Fjäder, Försörjningsberedskapscentralen
- Cyber Security Advisor Erka Koivunen, F-Secure Oy
- professor Mikael Hidén
- professor Jarno Limnéll
- professor Olli Mäenpää.

Skriftligt yttrande har lämnats av
- justitiekanslersämbetet
- professor Martti Lehto, Jyväskylä universitet.

PROPOSITIONEN

I propositionen föreslår regeringen att grundlagsbestämmelserna om skyddet för hemligheten i fråga om förtroliga meddelanden ändras. Grundlagen ska kompletteras med en bestämmelse där all reglering om begränsning av hemligheten i fråga om förtroliga meddelanden samlas. Enligt den föreslagna grundlagsbestämmelsen ska det genom lag kunna föreskrivas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid bekämpning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång, vid säkerhetskontroll och under frihetsberövande samt för att inhämta information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten.

UTSKOTTETS ÖVERVÄGANDEN

Allmänt

Finland har inte hittills haft någon lagstiftning som uttryckligen reglerar underrättelseverksamhet. Exempelvis på området för inre säkerhet bygger skyddspolisens befogenheter på de allmänna lagarna om polisens verksamhet, huvudsakligen polislagen (872/2011), förundersökningslagen (805/2011) och tvångsmedelslagen (806/2011). Enligt den gällande lagstiftningen ska utövandet av informationsinhämtningsbefogenheterna anknyta till förebyggande, avslöjande och utredning av brott samt i vissa fall till avvärjande av fara. Villkoret för att använda de lagfästa metoderna för informationsinhämtning är att informationsinhämtningen endast gäller avvärjande av ett brott som stämmer överens med ett specifikt rekvisit och med en viss sannolikhet kommer att begås av en enskild, identifierad person som befinner sig i Finland.

Det har visat sig behövas ett brett spektrum av metoder och en utveckling av de metoder som står till buds för att man ska kunna reagera på nya hot och förändringar i omvärlden. I sitt betänkande FvUB 5/2017 rd framhåller förvaltningsutskottet det nödvändiga i att uppdatera den nationella lagstiftningen så att våra myndigheter har behörighet och förmåga att få behövlig information om

hot mot Finlands vitala intressen. Varje land har skyldighet att sörja för sin egen och sina medborgares säkerhet och bygga säkerhetsbesluten på självförvärvad information. Enligt betänkandet är det därför nödvändigt att förvärva underrättelseinformation om verksamhet och händelser som allvarligt hotar den nationella säkerheten. Bland annat måste vi effektivt kunna avvärja dataintrång som allvarligt hotar den nationella säkerheten. När det gäller att inhämta information som rör vår nationella säkerhet får vi inte vara alltför beroende av andra stater.

Riksdagen behandlar för närvarande ett lagstiftningspaket om underrättelseverksamhet. Hit hör förutom den föreliggande propositionen om ändring av 10 § i grundlagen också propositioner om civil underrättelseinhämtning (RP 202/2017 rd), militär underrättelseinhämtning (RP 203/2017 rd) respektive övervakning av underrättelseverksamheten (RP 199/2017 rd). Till lagstiftningspaketet hör också talmanskonferensens förslag om ändring av riksdagens arbetsordning (TKF 1/2018 rd), som handlar om den parlamentariska tillsynen över underrättelseverksamheten.

I den aktuella propositionen (RP 198/2017 rd) föreslår regeringen att grundlagsbestämmelserna om skyddet för hemligheten i fråga om förtroliga meddelanden ändras. I 10 § i grundlagen föreslås ett nytt 4 mom. med samlade bestämmelser om begränsningar i hemligheten i fråga om förtroliga meddelanden. Enligt den föreslagna grundlagsbestämmelsen ska det genom lag kunna föreskrivas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid bekämpning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång, vid säkerhetskontroll och under frihetsberövande samt för att inhämta information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten.

I propositionerna om civil respektive militär underrättelseinhämtning föreslår regeringen nya befogenheter för både de civila och de militära underrättelsemyndigheterna. Ett av de viktigaste syftena med det nu aktuella lagförslaget är att göra det möjligt att bredda underrättelsemyndigheternas befogenheter på de sätt som föreslås i propositionerna. De befogenheter som ingriper i skyddet för hemligheten i fråga om förtroliga meddelanden förutsätter en ändring i 10 § i grundlagen. I den föreslagna lagstiftningen om civil underrättelseinhämtning gäller de här befogenheterna teleavlyssning och inhämtande av information i stället för teleavlyssning, teleövervakning, teknisk avlyssning, kopiering av försändelser och underrättelseinhämtning som avser datatrafik.

Om den nu föreslagna grundlagsändringen behandlas i normal grundlagsordning kan bestämmelserna om dessa befogenheter träda i kraft kanske först i början av 2020, står det i motiveringen till propositionen om ändring av 10 § i grundlagen. Om brådskande grundlagsordning tillämpas kan bestämmelserna träda i kraft tidigare, eventuellt redan i slutet av 2018, beroende på behandlingen av propositionerna i riksdagen. Om behandlingen av propositionerna i riksdagen pågår ända till slutet av denna valperiod minskar behovet av ett brådskande förfarande.

I det här utlåtandet beskriver utskottet med avseende på sitt fackområde den säkerhetspolitiska miljön i Finland och de förändringar som skett den senaste tiden.

Militär verksamhet

I den föreslagna lagstiftningen om militär underrättelseinhämtning avses med militär verksamhet militärt organiserade truppers verksamhet eller verksamhet i anslutning till militära maktmedel,

såsom beväpning och militärmateriel. Verksamheten kan vara både statlig och icke-statlig. Statlig verksamhet härrör från verksamhet som bedrivs av en främmande stats väpnade styrkor eller från därmed jämställbar verksamhet som bedrivs av en internationell militär allians eller organisation. Icke-statlig verksamhet avser sådan militärt organiserad, beväpnad eller utrustad verksamhet som inte har ovan avsedda statliga ursprung eller där ett sådant ursprung inte kan identifieras.

Inhämtningen av information om militär verksamhet omfattar kartläggning och övervakning av externa militära åtgärder som riktar sig mot Finland. Exempelvis kan det handla om att följa utvecklingen av den militära verksamhet som är av betydelse med tanke på Finlands säkerhetspolitiska miljö i syfte att skapa en lägesbild. Uttrycket omfattar bland annat kontinuerlig informationsinhämtning om utvecklingen av andra länders militära kapacitet samt informationsinhämtning om militär underrättelseverksamhet utomlands som riktar sig mot Finlands försvar. Inhämtande av information om militär verksamhet som avses i bestämmelsen ska inte förutsätta att verksamheten utgör ett allvarligt hot mot den nationella säkerheten. Militär verksamhet måste enligt propositionen ofta följas långsiktigt och systematiskt utan att den verksamhet som övervakas behöver utgöra en överhängande fara under den tid övervakningen pågår.

Verksamhet som allvarligt hotar den nationella säkerheten

Med verksamhet som allvarligt hotar den nationella säkerheten avses i den föreslagna lagstiftningen om civil underrättelseinhämtning verksamhet som hotar den demokratiska stats- och samhällsordningen, grundläggande samhällsfunktioner, ett stort antal människors liv eller hälsa eller internationell fred och säkerhet. En förutsättning är att verksamheten har någon koppling till Finland och att den hotar uttryckligen Finlands nationella säkerhet, även om verksamheten geografiskt sett kan ske utanför Finlands gränser. Det kan röra sig om verksamhet som allvarligt hotar Finlands nationella säkerhet och som hänför sig till terrorism, våldsbejakande radikalisering eller utländska underrättelsetjänsters verksamhet. Dessutom kan det handla om oroligheter i en stat som är central med tanke på Finlands säkerhet.

Den hotfulla verksamhet som avses i bestämmelsen gäller inte i första hand en enskild individ utan mer allmänt samhället och den mänskliga gemenskapen. Men till exempel våldsdåd som riktar sig mot enskilda individer såsom statsledningen eller personer som sköter grundläggande samhällsfunktioner kan vara sådan verksamhet som avses i bestämmelsen, om de är av betydelse för den nationella säkerheten och således kan utgöra ett allvarligt hot mot denna. Bestämmelsen förutsätter inte att den nationella säkerheten omedelbart håller på att äventyras, utan informationsinhämtningen kan också gälla verksamhet som kommer att äventyra den nationella säkerheten om den fortsätter.

Utskottet understryker att den föreslagna bestämmelsen förutsätter att verksamhet som omfattas av dess tillämpningsområde utgör ett allvarligt hot mot den nationella säkerheten. Villkoret att hotet ska vara allvarligt höjer tröskeln för att tillämpa bestämmelsen. Vilket som helst hot mot den nationella säkerheten uppfyller alltså inte villkoret.

Den övergripande säkerheten i samhället

Tre säkerhetsredogörelser

Under den innevarande valperioden har riksdagen behandlat tre säkerhetspolitiska redogörelser: den utrikes- och säkerhetspolitiska redogörelsen (SRR 6/2016 rd), redogörelsen för den inre säkerheten (SRR 5/2016 rd) och den försvarspolitiska redogörelsen (SRR 3/2017 rd). Redogörelserna och framför allt de behöriga utskottens betänkanden om dem utgör den viktigaste referensramen för den övergripande säkerheten i vårt land.

I sitt betänkande om redogörelsen för den inre säkerheten (FvUB 5/2017 rd) noterar förvaltningsutskottet att hotbilderna i redogörelserna är likartade. På grund av de olika sektorspecifika utgångspunkterna är hotbilderna ändå inte helt identiska utan fokus varierar efter sektor när det gäller mål och åtgärder.

Finlands utrikes- och säkerhetspolitik vilar på värderingarna och rättigheterna enligt grundlagen och på skyldigheterna att främja dessa. Enligt den utrikes- och säkerhetspolitiska redogörelsen är målet för Finlands utrikes- och säkerhetspolitik att stärka Finlands internationella ställning, trygga vår självständighet och territoriella integritet, förbättra finländarnas säkerhet och välfärd och upprätthålla ett fungerande samhälle. I sista hand är målet för Finlands utrikes- och säkerhetspolitik att undvika att hamna i en militär konflikt.

I sitt utlåtande om redogörelsen konstaterar utskottet att de utrikes- och säkerhetspolitiska åtgärder som vidtas också påverkar den inre säkerheten. De åtgärder som faller inom den inre säkerheten påverkar på motsvarande sätt den yttre säkerheten. Här understryker utskottet att 14 av 15 prioriteringar i USP-redogörelsen i högre eller lägre grad gäller den inre säkerheten och dess aktörer. Den tyngdpunktsförskjutning som skett är väsentlig (SRR 6/2016 rd — FvUU 40/2016 rd).

Försvarsredogörelsen beskriver regeringens försvarspolitiska riktlinjer för upprätthållande, utvecklande och användning av försvarsförmågan. Försvarsredogörelsen och genomförandet av den ska säkerställa att Finlands försvarsförmåga motsvarar säkerhetsmiljön.

USP-redogörelsen och försvarsredogörelsen sträcker sig tidsmässigt ända till mitten av nästa årtionde. De väger in det faktum att också bruk av militärt våld och hot om militärt våld åter ingår i metodarsenalen i vår säkerhetspolitiska miljö, åtminstone i ett bredare perspektiv.

Förvaltningsutskottet har tidigare kommit med ett omfattande, heltäckande och ingående betänkande (FvUB 5/2017 rd) om redogörelsen för den inre säkerheten, som var den första i vårt lands historia. I betänkandet tar utskottet upp förändringarna i det säkerhetspolitiska läget och de nya hoten mot säkerheten. Utskottet noterar att den inre respektive yttre säkerheten blir allt mer sammankopplade. I det nya läget får den inre säkerheten en framträdande betydelse. Den inre säkerheten utgör grundvalen för demokratin och välfärdssamhället. Dessutom finns det skäl att minnas att lägesbilden för den traditionella inre säkerheten har förändrats i grunden. Arbetsfältet sträcker sig i dag mer än tidigare in över den traditionella USP-sektorns arbetsfält. Perspektivet för analysen i betänkandet om redogörelsen för den inre säkerheten omfattar tidsperioden fram till hälften av nästa årtionde. Detsamma gäller de två andra redogörelserna.

Omvärldsförändringarna och betänkandet om redogörelsen för den inre säkerheten

Av betänkandet för den inre säkerheten framgår det att Finlands inre säkerhet är beroende av säkerhetsläget i de övriga EU-staterna och i grannländerna. Den europeiska säkerhetspolitiska miljön har förändrats snabbt till följd av kriserna i närområdena, inte minst krisen i Syrien, terrorismen, invandringskrisen och den fortsatta konflikten i Ukraina.

Det verkar fortsatt ske förändringar i Finlands närområden och globalt. Hoten mot den inre och den yttre säkerheten blir allt mer sammanflätade. Det som sker i Syrien och andra krisområden påverkar också den inre säkerheten i Finland. Den största förändringen har skett i de faktorer som påverkar säkerheten i Finland utifrån. De här faktorerna kan också utöva påverkan över långa avstånd. Hit hör bland annat den våldsbejakande extremismen och terrorismen i Mellanöstern och Afrika samt det våld som utövas av IS. Exempelvis den organiserade brottsligheten är i hög grad gränsöverskridande och utnyttjar de samhälleliga problemen, människors svårigheter och bristen på lag och ordning. Bland annat människosmugglingen vittnar om detta.

De försämrade relationerna mellan Ryssland och väst hör till de viktigaste nya hoten i vår säkerhetspolitiska miljö. Här måste man komma ihåg att till exempel den illegala invandringen också kan utnyttjas som maktpolitiskt redskap. Det har blivit allt svårare att förutse morgondagens säkerhetsläge, och situationen förväntas inte bli bättre inom överskådlig tid. Gränsen mellan militära och icke-militära hot har blivit otydligare. I det här läget måste man med tanke på den inre säkerheten också beakta att icke-militära medel planmässigt kan användas i syfte att utöva påverkan på vårt samhälle.

Samtidigt har förhållandet mellan inre och yttre säkerhet omformats och gränsen mellan dem suddats ut. I betänkandet om redogörelsen lyfter utskottet också fram att det inom säkerhetsområdet har upptäckts relativt nya asymmetriska genomgripande hot om vilka det överordnade begreppet hybridhot kan användas. Inom till exempel hybrid-, cyber- eller informationspåverkan är det dock inte uteslutande fråga om hot, utan om verksamhet som för närvarande pågår i vårt land eller som riktas mot vårt land och som kräver åtgärder av myndigheterna. Det har skett en kraftig och snabb förändring i omvärlden för och tillståndet i den övergripande säkerheten i Finland.

Utskottet hänvisar dessutom mer allmänt till det som står i betänkandet om redogörelsen för den inre säkerheten, framför allt beträffande skyddspolisen, terrorismen, cyberhoten, informationspåverkan och hybridhoten i ett samlat perspektiv. Ståndpunkterna i betänkandet (FvUB 5/2017 rd) talar för att den nu aktuella propositionen godkänns.

Lägesbild för den nationella säkerheten

Allmänna synpunkter

De redogörelser som nämns ovan och betänkandet om redogörelsen för den inre säkerheten har starka kopplingar till vår nationella säkerhet. Innehållet i den nationella säkerheten bestäms utifrån lagstiftningen om civil underrättelseinhämtning, som nu ska stiftas inom förvaltningsutskottets fackområde (RP 202/2017 rd).

Skyddspolisen, som står direkt under inrikesministeriet, svarar för bekämpning av hot mot den nationella säkerheten. Skyddspolisen har till uppgift att bekämpa förehavanden och brott som kan äventyra stats- eller samhällsskicket eller rikets inre eller yttre säkerhet. Skyddspolisen ska även upprätthålla och utveckla en allmän beredskap för att förebygga verksamhet som äventyrar rikets säkerhet.

Skyddspolisens informationsinsamling har försvårats avsevärt till följd av den kraftiga digitaliseringsutvecklingen. De personer som polisen vill samla in uppgifter om använder medier med avsevärt större informationsvolymer än tidigare. Det här beror bland annat på de sociala mediernas snabba utveckling och den tilltagande användningen av dem för kommunikation. Det här, tillsammans med den ökande krypteringen av system, har lett till ett stadigt växande behov av it- och personalresurser.

Skyddspolisen arbetar med betoning på underrättelsemässiga tillvägagångssätt (FvUB 5/2017 rd). Underrättelseinformationen är viktig också därför att den bidrar till att statens beslutsfattande grundar sig på relevant, aktuell och tillförlitlig information.

Den allmänna utvecklingen har lett till att enskilda staters säkerhetsangelägenheter har blivit internationella. De fenomen som hotar vårt lands säkerhet och bakgrundsfaktorerna till fenomenen hänger i hög grad samman med delvis svårgripbara händelser och utvecklingstrender som ligger utanför vårt land. På grund av säkerhetsfrågornas gränsöverskridande karaktär har behovet av underrättelseinformation som rör säkerheten vuxit avsevärt. En effektiv säkerhetsunderrättelse om globala hot kräver mångsidigare metoder och angreppssätt än tidigare.

Allmänt om förändringar i omvärlden med avseende på säkerhet

I motiveringen till lagstiftningsordning hänvisar regeringen till de propositioner som gäller lagstiftningen om civil och militär underrättelseverksamhet, där aspekterna på den försvagade och allt mer komplexa säkerhetssituationen i Finland beskrivs ingående. Förändringen i säkerhetssituationen i Finland är en följd av bland annat den ökade militära aktiviteten och de ökade militära spänningarna i våra närområden. De allvarligaste hoten mot den nationella säkerheten har numera mycket ofta internationellt ursprung eller internationella kopplingar och är därför svårare att hantera. Dessutom har den snabba utvecklingen inom kommunikationstekniken effektiviserat och underlättat kontakterna och nätverkandet mellan de aktörer som hotar Finland och gjort det svårare att identifiera de aktörer som står bakom hoten. De olika aktörerna kommunicerar i stor utsträckning över statsgränserna. Den tekniska utvecklingen har gjort det möjligt att förbereda och genomföra handlingar som hotar den nationella säkerheten på betydligt kortare tid än tidigare. När hoten har realiserats har effekterna samtidigt blivit mer omfattande, mer mångbottnade och farligare än tidigare för både enskilda människor och samhället i stort.

Landets externa säkerhetspolitiska miljö har försvagats kraftigt inom många områden de senaste åren. Säkerhetsläget i våra närområden har fortsatt blivit sämre allteftersom de internationella politiska spänningarna fått återverkningar allt längre norrut geografiskt sett. Det verkar bli allt svårare att förutse vad stormakterna kommer att göra och hur relationerna mellan dem kommer att utvecklas.

I stället för konventionell krigföring försöker länderna stärka sina positioner med hjälp av hybridpåverkan och olika informationsoperationer. De senaste åren har en lång rad europeiska länder utsatts för operationer av den här typen. Syftet är att åstadkomma osäkerhet, missämja och rädsla i de politiska beslutssystemen och bland medborgarna. Förberedelserna för operationerna och själva genomförandet stöds med hjälp av spionage i målländerna. Enligt utredning får skyddspolisen fortlöpande kännedom om konkreta fall där främmande stater försöker få åtkomst till information som är ytterst viktig för Finlands säkerhet och samhällsekonomi.

Vid sidan av traditionellt spionage förekommer nu också cyberspionage, där den stat som står bakom spionaget kan få åtkomst till mycket stora mängder information som är skadlig med tanke på mållandets säkerhet utan någon betydande risk för att bli avslöjad. Eftersom de vitala samhällsfunktionerna är nätbaserade och beroende av varandra är den kritiska infrastrukturen och försörjningsberedskapen allt mer utsatta för statligt sabotage och genomgående lamslagning via datanäten.

Samtidigt som olika slags statliga hot har ökat har också läget i fråga om terrorism blivit allvarligare än någonsin tidigare. Antalet personer med kopplingar till internationella terroristorganisationer har ökat rekordsnabbt. Exempelvis har antalet personer som bevakas av skyddspolisen fördubblats på några år. Finland är därmed på samma nivå som de andra nordiska länderna i fråga om hotbilden. Jihadister som återvänder från konflikterna i Syrien och Irak utgör ett akut och långvarigt hot mot säkerheten i Finland och övriga Europa. Läget kompliceras dels av de internationella flykting- och invandrarströmmarna, dels av det faktum att de är svåra att hantera och att de utnyttjas i statlig hybrid- och informationspåverkan för att sprida osäkerhet och åstadkomma samhälleliga konflikter i de västeuropeiska demokratierna.

De snabba förändringarna i den säkerhetspolitiska miljön kräver att myndigheterna effektivare förmår upptäcka även hot av helt nya slag. Informationen om nya hot behöver förmedlas till de myndigheter som svarar för den nationella säkerheten för att hoten ska kunna motverkas men också till den högsta statsledningen till underlag för beslut. Underrättelseinhämtning är ofta det bästa, och ibland det enda, sättet att göra en första observation och ta fram information om de här hoten.

Terrorism

Skyddspolisen bedömer att terrorhotnivån för närvarande är förhöjd (dvs. på nivå 2 på en fyrstegad skala). Hotet är allvarligare än någonsin tidigare. Enligt utredning har skyddspolisen nu fått kännedom om allvarligare planer och projekt med kopplingar till terrorism än tidigare. Terrorhotet i Finland är nu uppe på samma nivå som i de andra nordiska länderna, och trenden verkar inte vara att hotet minskar. Tvärtom är det sannolikt att hotet ökar på medellång sikt. Det väsentliga är att hotsituationen i Finland har förändrats så snabbt. I de övriga nordiska länderna har förändringen skett över en längre tidsperiod än i Finland, och de har därför kunnat bygga upp beredskapen steg för steg.

Antalet personer som är föremål för skyddspolisens terrorbekämpning har ökat kraftigt de senaste åren. Antalet är uppe i ungefär 370 för närvarande. Personerna har allt mer direkta kopplingar till terrorverksamhet. Men ännu mer oroväckande än det snabbt ökade antalet är den kvalitativa

förändringen. Skyddspolisen har fått kännedom om terroranknutna projekt och planer av allvarligare slag än tidigare. I ett flertal fall är dessa projekt och planer kopplade till aktörer utanför Finland. Antalet personer som måste bevakas väntas öka också under de närmaste åren, till följd av radikaliseringen och avslöjandet av nya nätverk. En stor del av dem som bevakas har terroristisk övertygelse samt förmåga och färdigheter att begå terroristbrott.

Läget med avseende på terrorism är i hög grad beroende av de internationella utvecklingsförloppen och trenderna. Konfliktområden spelar en viktig roll för framväxten av radikal islamistisk terrorism. På senare år har framför allt konfliktområdet i Syrien och Irak varit grogrund för terrorism. Konfliktområdet genomgår nu en omvälvning som leder till att de radikala islamistiska nätverken omvärderar sin verksamhet också i Europa.

Utländska stridande som företeelse inverkar i stor utsträckning på terrorhotet i Finland. Effekterna är både direkta och indirekta. Ett direkt hot mot säkerheten orsakas av utländska stridande som återvänder eller försöker återvända, och av deras nätverk. Ett indirekt hot uppstår till följd av propaganda, värvning och påverkan. De utländska stridande som företeelse har dessutom lett till att de radikala nätverk som är verksamma i Finland eller har kopplingar till Finland blir integrerade i de internationella nätverken. Följaktligen blir det mer sannolikt att finländare eller personer med anknytning till Finland blir inkopplade på terroristiska projekt, antingen inom landet eller utomlands. Enligt utskottets uppfattning visar tillgängliga uppgifter att det för närvarande är enskilda aktörer och små grupper som utgör det största hotet i Finland. Här vill utskottet påpeka att värvningen också berör personer som inte har koppling till radikala nätverk eller bakgrund som gör dem mottagliga för radikalisering.

I Syrien och Irak vistas för närvarande tiotals personer, bland dem ett flertal barn, som har rest dit från Finland. I de områden som tidigare kontrollerades av terroristorganisationer i Syrien och Irak har det vuxit fram en ny generation av jihadister. Bland dem finns det också finländare. Därför väntas företeelsen få återverkningar i Finland en lång tid framöver. Via stridande som kommit från Finland har också utländska radikala islamister nu bättre kännedom om Finland.

I den radikala islamistiska propagandan har Finland fått en höjd profil. Finländare har förekommit till exempel i terroristorganisationen Islamska statens (IS/Daesh) propaganda. En del propaganda har publicerats på finska och terroristerna uppmanar också till attacker i Finland. Det är känt att både finländare och personer som lämnat Finland har medverkat i propagandan och i vissa fall har de uttryckligen riktat sitt budskap till Finland. Detta bidrar till att mana radikala i Finland att tillgripa våld. Virtuella nätverk har börjat spela en allt mer framträdande roll. Propagandan sprids nu företrädesvis via skyddade applikationer för direktmeddelanden. Det är en särskild utmaning med tanke på underrättelseinhämtning och motåtgärder från myndigheterna.

Illegal utländsk underrättelseverksamhet

Bekämpningen av illegal underrättelseverksamhet har snabbt blivit mer komplicerad. Utländska underrättelsetjänster bedriver aktiv underrättelseverksamhet i Finland. Utländska underrättelseorganisationer inhämtar underrättelser om finska statens säkerhetsintressen i form av en omfattande, långvarig och kontinuerlig personbaserad underrättelseinhämtning, samtidigt som spiona-

ge till betydande delar numera sker i datanät. Finland är ett av de västländer som har flest permanent placerade utländska underrättelseofficerare i förhållande till invånarantalet.

De utländska underrättelsetjänsternas centrala mål är att förutse Finlands politik och påverka beslutsfattandet. Försök att påverka den allmänna opinionen upptäcks regelbundet. Informationsinhämtningen och påverkningsförsöken riktas framför allt mot de aktörer som bereder och fattar beslut.

Den statliga underrättelseverksamheten i Finland är långsiktig och fokuseras framför allt på den politiska ledningens och befolkningens attityder till ett eventuellt medlemskap i Nato, de energipolitiska besluten och försörjningsberedskapen i fråga om energi samt cybersäkerhetsstrukturen.

Myndigheterna känner till konkreta fall där främmande stater försökt värva hemliga informationskällor som ska leverera information som inte finns tillgänglig i offentligheten. Underrättelseorganisationerna siktar dessutom på att få assistans av personer med vars hjälp det är möjligt att påverka de politiska besluten och den allmänna opinionen. Den illegala underrättelseinhämtning som bedrivs av statliga aktörer är också skadlig för finländska företag och forskningsinstitut inom högteknik. Verksamheten kan förorsaka kritisk skada på företagsnivå och kan också ha samhällsekonomisk betydelse.

Statliga och andra aktörer med stora resurser försöker via datanäten aktivt få tillgång till information som anknyter till politiska beslut och viktiga produktinnovationer. För att kunna skydda oss och ingripa mot nätspionage och påverkan via nätet — och trygga den nationella säkerheten — behöver vi den lagstiftning som nu föreslås på området. Det viktigaste syftet med kontraspionage är att hitta de personer som bedriver underrättelseverksamhet och vars verksamhet utgör ett allvarligt hot mot den nationella säkerheten.

Med tanke på bekämpningen av underrättelseverksamhet är också frågan om dubbelt medborgarskap viktig. En finsk medborgare med dubbelt medborgarskap kan nämligen försättas i en ställning där han eller hon kan se sig nödgad att handla i strid med Finlands intressen. Till exempel är alla ryska medborgare trots det dubbla medborgarskapet skyldiga att enligt rysk lag bistå Rysslands säkerhetsmyndigheter.

Cyberhot

Förändringarna i cyberomgivningen är snabba och effekterna av dem svåra att förutse. Cybersäkerheten baserar sig på ett långsiktigt och tillräckligt utvecklande av kapaciteterna, på en flexibel användning av dem i rätt tid samt på de vitala funktionernas förmåga att tåla störningar i cybersäkerheten.

Med cyberhot avses hot som riktar sig mot cyberomgivningen och som, om de realiseras, äventyrar korrekt eller avsedd funktion i omgivningen eller en del av den. Hoten är ofta förknippade med hot mot den elektroniska omgivningens säkerhet, dvs. mot såväl själva informationen som exempelvis digitala styrsystem som kontrollerar och styr mycket av samhällets vitala infrastruktur och även annan infrastruktur från datanät till applikationer.

Cyberhoten kan vara av antingen civil eller militär art beroende dels på vem som står bakom dem, dels på vad syftet med dem är. Hot mot datasystem och datanät kan vara allvarliga också av den orsaken att datasystemen är integrerade och sammankopplade till ett globalt nätverk. Störningar i en del av nätverket kan sprida sig långt utöver den enskilda, angripna tjänsten. Konsekvenserna av sådana störningar kan vara svåra att förutse. I värsta fall kan en cyberattack lamslå hela samhället.

I sitt betänkande om redogörelsen för den inre säkerheten noterar utskottet att man enligt uppgift i ett flertal europeiska länder observerat att externa aktörer har försökt att genom it-tekniska metoder inventera vilka programversioner som används i system som styr kritisk infrastruktur. Om en annan stat eller aktör känner till programversionerna i en cyberomgivning, kan den enligt uppgift snabbt välja effektiva attackmetoder i en krissituation. Enligt uppgift upptäcks i Finland fortgående cyberspionage också mot det utrikes- och säkerhetspolitiska beslutsfattandet.

Enligt utredning till utskottet finns det också klara tecken på att aktörer med tillgång till statliga resurser försökt påverka samhällets kritiska infrastruktur. Ett känt exempel på en omfattande operation är cyberattacken mot tre regionala elbolags nätinfrastruktur i Ukraina i december 2015. Med hjälp av sabotageprogram slog attacken då ut elnätsoperatörernas kontrollsystem, vilket ledde till att 255 000 konsumenter blev utan el.

Massiva överbelastningsattacker har på senare år riktats mot finska medier, bankers nättjänster och den offentliga förvaltningens nättjänster. Den senaste tidens utveckling på internationell nivå tyder på att kapaciteten att utföra överbelastningsattacker har ökat betydligt. Attackkapaciteten kan, också enligt uppgifter i offentligheten, vara så stor att den i värsta fall skulle kunna slå ut finländska nätoperatörer. Det bör också noteras att i fråga om internationellt sammanlänkade system kan en attack mot en utländsk aktör ge konsekvenser också i Finland.

Enligt olika bedömningar formas cybersäkerheten främst av det expanderande området för cyberattacker, de förbättrade kunskaperna hos dem som står bakom attackerna, den industrialiserade cyberbrottsligheten och informationsläckorna. Angriparna i cybervärlden får nya mål för sina attacker: sakernas internet, molntjänster, stora datamängder och ökad användning av mobila enheter. När molntjänster blir vanligare får angriparna nya möjligheter. Molntjänster levereras ofta av tredje parter, så kunden får ingen ordentlig insyn i kvaliteten på eller säkerheten i tjänsten. Smarta big data-tillämpningar används mycket redan nu, men riskerna för oavsiktligt eller avsiktligt missbruk ökar när de stora datalagren blir vanligare. Mobila arbetssätt och ny teleterminalutrustning ska effektivisera arbetet. En del av människornas arbete utförs mobilt. Den här utvecklingen har lett till att mobila enheter allt oftare drabbas av sabotageprogram och attacker.

Utskottet konstaterar att vårt samhälle, dess verksamhet, ekonomi och beslutsfattande, är helt beroende av den digitala omgivningen. Detta beroende kommer öka kraftigt framöver. Utskottet bedömer att man inom det finländska beslutsfattande ännu inte inser hur snabb och kraftig förändringen är. Det kan utsätta samhället och dess organisationer för ett ständigt ökande antal cyberhot.

Cyberbrottsligheten och bekämpningen av den kan anses utgöra en stor utmaning också på ett globalt plan. Volymerna växer, och i takt med det ökar ständigt också den skada brottsligheten tillfogar samhället. Myndigheternas befogenheter, bestämmelserna om informationsutbyte och

de internationella överenskommelserna ger i dag inget riktigt stöd åt cyberbrottsbekämpningen. Bekämpningen kräver därför, vid sidan av lämplig lagstiftning, en bred samverkan på nationell och internationell nivå. Svårigheterna ökas av att brottslingarna och offren kan finnas i många olika länder och brottsbevisen måste sökas på servrar i olika delar av världen.

Utskottet framhåller att de behöriga myndigheterna måste ha hög kompetens och lämpliga befogenheter för att kunna bekämpa cyberattacker. Brister i kompetensen och befogenheterna kan exponera samhället för ännu större attacker som lamslår samhällsfunktionerna och som det inte går att bereda sig på. I cybervärlden kommer det i framtiden att vara väsentligt att samhället har kapacitet att tåla konsekvenserna av cyberattacker. Det blir en krävande situation för hela samhället om det exempelvis uppstår ett långvarigt elavbrott vintertid eller om alla nätoperatörer slås ut samtidigt för mer än en kort tid.

Utskottet understryker att cyberomvärlden hela tiden får större betydelse för den nationella säkerheten. Cybermetoder används bland annat för att uppnå politiska mål. Gränsöverskridande spionage i datanät har blivit ett betydande hot. Sådan verksamhet möjliggör åtkomst till stora datamängder på en gång, vilket kan leda till irreparabel skada för den utsatta statens säkerhet och dess intressen. Sabotage och förvrängda data i datanäten utgör också betydande hot för den nationella säkerheten. Information som förvärvats genom cyberspionage kan också användas för informationskrig. Något som hävdas vara ett exempel på detta är påverkan på valet i Förenta staterna.

Alla de främmande makter som är väsentliga med tanke på hur Finlands säkerhetspolitiska omgivning utvecklas satsar enligt uppgift på att bygga upp sin offensiva cyberkapacitet. Det betyder att de här staterna allt mer måste få stöd från underrättelseverksamhet i den reella världen, till exempel genom att information om potentiella mål för cyberspionage samlas in med hjälp av personbaserad underrättelseinhämtning eller att sådana personer söks upp som av misstag eller avsiktligt kan hjälpa till med att få in ett sabotageprogram i målorganisationens datasystem. I offentligheten har det rapporterats om kapacitet att göra intrång, och ett lyckat försök att göra intrång, i ett slutet datasystem hos en myndighet i en stor EU-stat.

Cyberspionage är ett närapå riskfritt sätt för en stat att få åtkomst till information oavsett ekonomisk och social utvecklingsnivå. Cyberspionage är en billig informationsinhämtningsmetod i relation till den mängd information som potentiellt sett finns tillgänglig.

Mörkertalet är stort när det gäller attacker som avser att stjäla kunskapskapital från privata företag, eftersom företagen och tredje sektorn inte har beredskap att identifiera de hot som statliga aktörer förorsakar. Ett särskilt kritiskt hot är enligt utskottet de cyberattacker där angriparen direkt utnyttjar betrodda funktioner inom servicekedjan i organisationen. Enligt uppgift kommer attacker av den här typen till Skyddspolisens kännedom nästan utan undantag i form av tips från utländska partner. I ett medelstort företag kan värdet på det stulna kunskapskapitalet vara så mycket som tiotals miljoner euro per år. Om attackerna upptäcks snabbt minimeras mängden stulen information och därmed också de potentiella förlusterna för företaget.

Attacker i datanät är ett ytterst allvarligt hot av två orsaker: 1) den teknik som används för ändamålet utvecklas kontinuerligt och 2) statliga aktörer får ofta hjälp av hackare och personer som förknippas med organiserad brottslighet. Statlig verksamhet, civilt samhälle och brottslighet blir

sammanflätade. För att motverka hoten bör våra säkerhetsmyndigheter ha mycket hög teknisk kapacitet, rentav högre än angriparna. Samtidigt bör befogenheterna att använda den höga kapaciteten göra det möjligt att föregripande upptäcka hot och i varje fall så tidigt som möjligt. Om myndigheterna bara har kapacitet att reagera när skadan redan är skedd, befinner sig de vitala samhällsfunktionerna och därmed också den nationella säkerheten i ytterst stor fara.

Påverkan genom information

Påverkan genom information är inget nytt fenomen. Dess medel och genomslagskraft har dock förändrats väsentligt i dagens digitala medieomgivning. Syftet med den typ av informationspåverkan som berör den nationella säkerheten är bland annat att i sista hand påverka beslutsfattarna och beslutsprocessen och att få objektet att fatta beslut som är skadliga för det själv eller gynnsamma för påverkaren. Det kan ske genom varierande metoder och åtskilliga mediala plattformar. Påverkan sker ofta indirekt via den breda allmänheten, men kan också rikta sig direkt mot beslutsfattare eller beslutsprocesser. Exempelvis kan man försöka påverka utgången av ett val genom att via Twitter — från andra sidan jorden — rikta meddelanden till de röstberättigade om hur kandidaterna klarat sig i en valdebatt.

Exempelvis kan påverkaren försöka kontrollera det mentala tillståndet genom att forma den allmänna opinionen. I ett öppet samhälle kan det räcka att skapa splittring i samhället. Det kan påverka myndigheterna och den politiska ledningen och göra det svårare att skapa och dela med sig en lägesbild. När de divergerande åsikterna är tillräckligt starka och får understöd blir beslutsprocessen och avgörandena över lag svårare. Dessutom kan det bli omöjligt för beslutsfattarna att agera och fatta beslut. Beroende på graden av påverkan kan man rentav tala om informationskrig.

Påverkan genom information är ett medel för såväl hybrid- som cyberpåverkan. För definitionen av fenomenet är det oväsentligt om påverkaren är en statlig eller en icke-statlig aktör. Det är typiskt för informationspåverkan att det syftar till att styra beslutsfattandet bland annat genom desinformation eller ofullständig information. Att underlåta att sprida information kan också vara informationspåverkan, liksom att selektivt sprida i sig korrekt information till olika målgrupper. Det kan ske till exempel genom reklam i syfte att påverka objektets föreställningar och känslor.

Vid så kallad trollning kan man påverka olika informationsaktörer bland annat genom att ifrågasätta riktigheten i den information de och medierna sprider eller rentav genom att gå till personliga angrepp och/eller ifrågasätta personens trovärdighet. Det bakomliggande syftet kan variera, men själva informationspåverkan är riktad. I praktiken har det förekommit fall där journalister som rapporterat om påverkan genom information har utsatts för systematiska, massiva och långvariga informationsattacker. Upphovsmännen har även lyckats engagera inhemska nättroll. Den omfattande yttrandefriheten har åberopats bland annat i samband med nätmobbning, hot och förföljelse. Syftet verkar vara att stoppa all rapportering om informationspåverkan.

I forskarkretsar inser man att nuläget bara är en början på ett allt kraftigare utnyttjande av informationspåverkan. I en brytningstid där den sammanhållna kulturen vittrar sönder och mediefältet splittras, bedömer forskarna att det i ett öppet samhälle som vårt uppstår ett nytt slags medielandskap, där statens roll som central auktoritet hotar att marginaliseras. För dem som ägnar sig åt informationspåverkan eller informationskrig och annan fientlig påverkan öppnar detta många nya

möjligheter. De samhälleliga skiljelinjerna och det polariserade klimatet skapar ett förträffligt underlag för lättmanipulerade målgrupper.

Med tanke på landets förmåga till underrättelseinhämtning har det framhållits som ett relevant faktum att doktrinen på stormaktsnivå förenar samtidigt bruk av mjuka medel (soft power) och hårda medel och skapandet av en slags ”psykologisk intressesfär” i närområdet. Det är frågan om psykologisk påverkan genom en omfattande metodarsenal. Till exempel utrikespolitiska påtryckningar kan vara ett sätt att påverka inrikespolitiken i ett land. I vissa fall utnyttjas också det inbördes beroendet mellan den inre och den yttre säkerheten. Psykologisk påverkan kommer att få ökad betydelse i den framtida säkerhetsomgivningen, vilket betyder att det kan bli normalt att vädja till känslor och försöka påverka beteendet.

Digitaliseringen och den it-tekniska utvecklingen medför nya utmaningar när det gäller att bedöma informationens pålitlighet. Tekniken utvecklas och gör det allt enklare att förfalska information. Den som vill sänka förtroendet för någon kan till exempel offentliggöra förfalskade handlingar om den aktuella personens hälsotillstånd. Redan i dag utvecklas teknik för att i realtid bearbeta videosändningar. Riktad informationspåverkan och anknytande kampanjer hänför sig i framtiden inte enbart till politiska beslutsfattare och samhälleliga nyckelpersoner. Också enskilda medborgare utsätts för åtgärderna, eftersom man genom dem kan påverka viktiga aktörer i samhället. I en lyckad informationsoperation vet de som är föremål för operationen inte om att de utsatts för påverkan.

När den sammanhållna kulturen faller sönder finns det fler konkurrerande tolkningar, synvinklar och rent felaktiga eller lögnaktiga uppgifter i informationsomgivningen, vilket gör det allt svårare att korrigera den felaktiga informationen. De medier som följer de journalistiska principerna ställs dessutom inför dilemmat hur de i det rådande läget ska kunna säkra ekonomin och samtidigt bibehålla en högklassig, faktaorienterad informationsförmedling. Ett fungerande ledarskap i rätt tid i samhället bygger på en gemensam och delad lägesbild. Utskottet menar att upprätthållandet av en korrekt lägesbild kräver att experters och forskares kompetens utnyttjas. Förfalskning och manipulering av information kan syfta till att fördunkla lägesbilden. I det läget sätts allmänhetens allmänna kunskapsbas och mediekompetens och värderingar på prov. I värsta fall kan informationspåverkan och dess följder hota demokratin och samhällsfreden.

Enligt en sakkunnig har Finlands statsledning hittills inte haft en tillräckligt stark kultur för strategisk kommunikation, noterar utskottet i sitt betänkande om redogörelsen för den inre säkerheten. Den strategiska kommunikationen är likväl ett av de viktigaste ledningsredskapen under informationseran. Strategisk kommunikation skulle förbättra statsledningens och myndigheternas förmåga att agera i oklara situationer och skulle utgöra ett redskap för de ansvariga aktörernas strävan att bygga upp förtroendefulla samhällsrelationer. Om beslutsfattare och myndigheter inte förmår delge det övriga samhället en aktuell och korrekt lägesbild kan det däremot uppstå misstro.

Hybridhot

Definitionen av hybridhot varierar, eftersom man önskat hålla definitionen öppen och flexibel på grund av hotens föränderliga och varierande karaktär. Hybridhot definieras därför i regel genom

en beskrivning av de olika medel som utnyttjas vid hybridpåverkan. Hybridpåverkan innebär att många olika påverkningsmedel kombineras och smidigt anpassas efter situationen. Några gemensamma drag vid hybridpåverkan är att man utnyttjar sårbarheter hos objektet, sår tvistefrön och stör beslutsprocessen. Desinformationskampanjer, utnyttjande av sociala medier och gynnande av radikalisering är typiska metoder vid hybridpåverkan. Ett väsentligt inslag i hybridhoten, som i vissa fall också kan innefatta cyberhot, är hot mot den elektroniska miljöns säkerhet och hot som orsakas av elektronisk utrustning. Hybridpåverkan kan bilda kombinationer av hot som det saknas tillräcklig beredskap för och som det är krävande att bereda sig på.

Begreppet hybridhot avser olika åtgärder som riskerar säkerheten och skadar samhället (politiska, diplomatiska, militära, ekonomiska, informationsrelaterade eller tekniska åtgärder eller åtgärder som påverkar infrastrukturen). Det rör sig om konventionella och nya metoder som kan tillämpas samordnat av statliga eller icke-statliga aktörer för att nå vissa mål. Hybridpåverkan syftar ofta till att påverka inte bara samhället utan också individen. Avsikten kan vara att utmana samhälleliga grundstenar som exempelvis välfärden, sammanhållningen och samverkan. På ett mer utvecklat plan kan det vara frågan om överraskande aktioner mot vitala samhällsfunktioner samtidigt som olika delområden utsätts för tryck på det sätt angriparen önskar. Beredskapen inför hybridhot är nära förknippad med samhällets och allmänhetens kristålighet.

Hybridhot kan handla om att en främmande stat påverkar en annan stats och dess beslutsfattares verksamhet fientligt med en bred metodarsenal. Den främmande staten försöker i regel genomföra gärningen på så sätt att den stat som är föremål för gärningen inte kan vara helt säker på om det är frågan om en operation som styrs av den främmande staten eller inte. Målet kan beroende på situation vara att antingen skyla över statens försök till påverkan, så att inblandningen kan bestridas, eller att skapa osäkerhet kring huruvida handlingen var ett medvetet försök av staten att påverka. Hybridhotet fungerar då som ett redskap för den statliga maktpolitiken.

Som term fick hybridhot större spridning i samband med Ukrainakrisen. Själva fenomenet är dock inte nytt. Stormakterna har alltid strävat efter att påverka omvärlden på olika sätt. Den datatekniska utvecklingen ger dock påverkningsmöjligheterna helt nya dimensioner och erbjuder nya handlingsmodeller. Graden av fientlighet varierar dock beroende på det aktuella politiska läget. Att motverka påverkan har, vid sidan av kontraspionaget, således också tidigare utgjort en central uppgift för säkerhets- och underrättelsetjänsterna.

En uppgift för Europeiska kompetenscentret för motverkande av hybridhot, som inrättades i Helsingfors 2017, är att skapa en gemensam medvetenhet om hybridhot i EU-länderna. Det hybridanalyscenter (EU Hybrid Fusion Cell) som inrättats vid EU IntCen har också en viktig roll i den operativa verksamheten.

I fråga om beredskap för och bekämpning av hybridhot kommer utskottet i sitt betänkande om redogörelsen för den inre säkerheten till slutsatsen att hybrid-, cyber- och informationsoperationer är dagens verklighet och att de här hoten måste kunna identifieras mer effektivt. Det är alltså inte bara ett hot utan faktum är att hybridverksamhet riktas mot vårt land.

Hybridpåverkan ingår i stormakters och starka politiska eller väpnade gruppers verksamhet för att öka sitt inflytande, störa fientlig verksamhet och nå egna ekonomiska och politiska och/eller mi-

litära mål. Aktörerna inom hybridpåverkan brukar delas in i statliga och icke-statliga aktörer. Främmande stater har nu mer varierande metoder för hybridpåverkan (militära, politiska, ekonomiska, infrastruktur, information, kultur, övriga). Med avseende på nationell säkerhet är underrättelsemyndigheten enligt utredning i synnerhet intresserad av de hybridhot som utgörs av påverkan genom information och propaganda samt cyberverksamhet. Dagens brotts- och personbaserade befogenheter ger inte myndigheterna tillräckliga förutsättningar att identifiera eller avvärja utländska statliga hybridhot som allvarligt kan riskera vår nationella säkerhet.

Riskfaktorer för att samhällsfunktioner lamslås

Det strategiska syftet med den nationella försörjningsberedskapen är att se till att infrastrukturen, produktionen och tjänsterna fungerar så att de kan tillgodose befolkningens, näringslivets och försvarets mest kritiska grundläggande behov under alla omständigheter.

Målet är att också de allvarligaste undantagsförhållandena ska kunna hanteras nationellt. Men Finlands försörjningsberedskap är i kritisk utsträckning beroende av internationella kontakter. Exempelvis importerar vi två tredjedelar av all energi från utlandet, varav två tredjedelar från Ryssland. Även till exempel logistiken och finanssektorn hör i allt väsentligt till det globala nätverket.

Samtidigt som försörjningsberedskapen blir mer beroende av de internationella strömmarna i fråga om materiel, logistik, information och finanser har omvärlden blivit mer oförutsebar. Gränsöverskridande hot, framför allt cyberhot mot kritisk infrastruktur och hybridpåverkan, kan störa måluppfyllelsen för försörjningsberedskapen.

Enligt säkerhetsstrategin för samhället, som uppdaterades 2017, finns följande bland de viktigaste hoten mot ekonomin, den kritiska infrastrukturen och försörjningsberedskapen: allvarliga störningar i livsmedelsförsörjningen, energiförsörjningen, transportlogistiken, finans- och betalsystemet samt datakommunikation och informationssystem, störningar i tillgången på finansiering för den offentliga ekonomin, cyberhot, storolyckor, extrema naturfenomen och miljöhot. Också terrorism och annan brottslighet som äventyrar samhällsordningen kan riskera de här funktionerna.

En fungerande energiförsörjning och framför allt en oavbruten eltillförsel är nödvändiga för att de vitala samhällsfunktionerna ska vara säkrade. Systemen för styrning och övervakning av näten är till stor del beroende av datakommunikation. Näten för överföring och distribution av energi kan därför bli föremål för terrorattacker, organiserad brottslighet eller militär påverkan.

Den globala cyberomgivningen består av ett komplext, globalt informationsnätverk som innefattar privata människors, myndigheters och företags datanät samt styr- och övervakningssystem för kritisk infrastruktur. De flesta tjänster och funktioner i samhället är via datakommunikation nära kopplade till elektroniska tjänster.

Merparten av de kritiska tjänsterna i samhället bygger på dataöverföring och användning av digitala datalager. Tjänsterna är datatekniskt styrda eller utgör i sin helhet elektroniska tjänster. Datasystemen och de dataöverföringsnät som sammankopplar dem smälter samman och blir omfat-

tande, rentav globala, sammanhängande nät. Störningar i deras funktion kan spridas från enskilda tjänster till hela system och systemhelheter. Här noterar utskottet att beredskapen för hoten i allt väsentligt påverkas av att tekniken utvecklas mycket snabbt. Den elektroniska infrastrukturen kan utgöra en sårbar och svårhanterlig helhet. Det är ett stort hot, inte minst därför att de data- och kommunikationssystem som används för att leda samhället och varna befolkningen i störningssituationer är beroende av el. Utskottet påminner samtidigt om att försörjningsberedskapen kräver olika slags fysiska rutter.

E-tjänsterna och kommunikationen kan äventyras till följd av olyckor orsakade av naturfenomen, mänsklig verksamhet och tekniska fel samt avsiktliga cyberattacker och fysiska attacker mot systemen. En metod som enligt utredning ofta använts på senare år är att tjänsterna störts genom överbelastningsattacker via internet. Syftet är att överbelasta nätservrarna eller tjänsteleverantörens kapacitet med hjälp av automatiska meddelanden. Det finns också åtskilliga andra möjligheter att störa tjänster på internet.

En avsiktlig cyberattack mot finska staten eller samhället utförd av en statlig aktör eller exempelvis en terroristorganisation kan ingå som en del av en mer omfattande kris eller konflikt i Europa. På grund av sin betydelse i samhället är datakommunikationen och e-tjänsterna viktiga element också i politiska och militära kriser. Den militära beredskapen i de flesta stater inbegriper beredskap att störa, utnyttja och förstöra informationssystem. Informationskrigföring är en integrerad del av den moderna militära beredskapen. Utöver attacker via nätet kan systemen bli utsatta för mer konventionella angrepp med kraftigare konsekvenser, såsom elektromagnetisk puls (EMP), mikrovågsvapen (HPM) eller fysisk förstöring. Statliga cyberattacker ingår sannolikt bara som ett av flera element i övrig påtryckning, så de är troligtvis förenade med politisk, ekonomisk och måhända också militär påtryckning och påverkan i sociala medier och andra medier. Här kan man tala om hybridoperation.

Cyberattacker mot kritisk infrastruktur på finansmarknaden kan rubba stabiliteten på finansmarknaden och lamslå betalningsförmedlingen som är nödvändig för att samhället ska fungera. Om social- och hälsovårdssystemet, energiproduktionen eller styrsystemen i industrin drabbas av en cyberattack kan det i värsta fall leda till materiell förstörelse och dödsfall. Angriparna kan dessutom tillgripa åtgärder som orsakar fysisk förstörelse.

Oavsiktliga eller avsiktliga störningar i nätet kan drabba alla aktörer som använder datanät, såsom handeln, industrin, olika sammanslutningar och offentliga tjänster. En fungerande försörjningsberedskap kräver mer än tidigare att den säkerhetspolitiska miljön bevakas tidsenligt och med framförhållning. Bevakningen kan inte avgränsas till närområdet, utan vi bör bli bättre på att upptäcka mer avlägsna hot. Enligt utredning är vår kapacitet att föregripande och tidsenligt bevaka den globala omvärlden svag i nuläget.

Utskottet framhåller att det ökande beroendet av dels kritiska datasystem och kommunikationssystem, dels cyberomgivningen markerar hur viktig cybersäkerheten är för de kritiska samhällsfunktionerna. Sårbarheten för störningar ökar av att olika funktioner och system är beroende av varandra och blir allt mer komplicerade. Därför är det viktigt att förbättra de olika aktörernas möjligheter att bekämpa cyberattacker mot kritisk infrastruktur.

Sammanfattning

Finlands säkerhetspolitiska omvärld har förändrats på många sätt. Förändringarna har pågått i en lång tid nu, men farten har tilltagit de senaste åren.

Den nationella cyberkapaciteten kommer att bli allt viktigare för den övergripande säkerheten, de vitala samhällsfunktionerna och landets konkurrenskraft. Finland är ett av de mest digitaliserade samhällena i världen.

Dagens säkerhetspolitiska miljö präglas av snabba förändringar, oförutsedd instabilitet och komplexitet. Tekniken och digitaliseringen berör nästan alla områden i livet. Till följd av den här utvecklingen har samhället blivit allt mer beroende och å andra sidan också mer sårbart än någonsin tidigare. För närvarande väger vår lagstiftning inte in de särskilda egenskaperna hos cyberomgivningen. Den senaste tidens oroväckande utveckling i vår säkerhetspolitiska miljö understryker behovet av att inom kort skapa regelverk och metoder för att förbättra kapaciteten att bekämpa och förutse cyberhot.

Konsekvenserna av cyberhoten har blivit mer varierande och skadliga för både enskilda människor, företag och det finländska samhället.

Utöver att terrorhotet mot landet är allvarligare än någonsin har det på senare tid väckt särskild oro att extremistgrupper och terrorister har höjt sin kapacitet i den digitala omvärlden. Exempelvis har IS effektivt dragit nytta av olika digitala kanaler för att sprida sin propaganda, rekrytera, hantera penningströmmarna och kommunicera internt. Extremistgruppernas mål att skapa rädsla och göra vansinniga attacker har gett skäl att ta upp frågan om IS de närmaste åren kommer att ha kapacitet att via den digitala världen göra attacker med livshotande konsekvenser i den fysiska världen. Framför allt i Förenta staterna och Storbritannien har man räknat med att IS genom cyberattacker kommer att försöka påverka kritisk infrastruktur såsom vattenverk och kraftverk.

Samhällets beroende av tillförlitlig informations- och kommunikationsteknik och automation blir allt mer accentuerat. Beroendet leder till sårbarhet. Genom att avsiktligt störa teknisk infrastruktur går det att påverka processerna i samhället i stort, allt från betalningar till kollektivtrafik och via informationsförmedling till energidistribution, industriell produktion och rentav val. Det är angeläget att med hjälp av underrättelseinhämtning i förväg få information om attacker som förbereds.

I cybervärlden finns det många förändringsfaktorer, varav den viktigaste är tiden. Cyberattacker kan förberedas i hemlighet under en lång tid, men själva attacken kan utföras på en mycket kort tid. I januari 2003 spred sig nätmasken Slammer på ungefär tio minuter till uppskattningsvis 90 procent av de planerade målen (servrar som styr internet). Nätet blev långsammare överallt i världen. Kostnaderna beräknades uppgå till 750 miljoner euro.

Datanäten och systemen utsätts allt oftare för riktade attacker, kränkningar av informationssäkerheten och sabotageprogram. Antalet sabotageprogram som upptäcks per år ökade mellan 2012 och 2017 från 100 miljoner till mer än 700 miljoner (400 000 nya sabotageprogram varje dag). Attackerna riktas mot nationell sekretessbelagd information, immateriellt kapital och personupp-

gifter. Underrättelseorganisationerna har som mål att samla in information som de är intresserade av för att få politiska, ekonomiska eller militära fördelar.

Särskilt skadliga är specifikt inriktade attacker (APT), där målet är noga utvalt och angriparen har samlat in den behövliga mängden information för att utföra attacken. Angriparen utnyttjar aktivt sårbarheter och svagheter hos målorganisationens tjänster. Sårbarheter finns i människors verksamhet, organisationers säkerhetsprocesser och teknik (program och hårdvara). Attackerna kan omformas och utvecklas så att svagheterna i målorganisationen kan utnyttjas så mycket som möjligt. Riktade attacker utförs ofta i form av kampanjer bestående av en serie misslyckade och lyckade försök att tränga allt djupare in i målorganisationens nät.

Följaktligen anser utskottet att vi i Finland behöver ny lagstiftning som gör det möjligt för de behöriga myndigheterna att effektivt inhämta underrättelseinformation om
— utvecklingen i landets säkerhetspolitiska miljö till underlag för statsledningens beslut
— verksamhet som allvarligt hotar den nationella säkerheten och som åtminstone inte ännu har kommit så långt att den utgör brott
— verksamhet som allvarligt hotar landets nationella säkerhet och som sker utomlands
— verksamhet som allvarligt hotar landets nationella säkerhet och som bedrivs av okända personer.

Sammantaget anser utskottet att propositionen med förslag till ändring av 10 § i grundlagen är behövlig och lämplig och tillstyrker lagförslaget. På grundval av hittills erhållen utredning anser utskottet också att en lag om civil underrättelseinhämtning behöver stiftas. Utskottet går närmare in på frågan i sitt betänkande om proposition RP 202/2017 rd. Rent allmänt noterar utskottet här att en lag om civil underrättelseinhämtning kommer att ge skyddspolisen nya befogenheter att säkerställa statsledningens tillgång till information och bekämpa verksamhet som allvarligt hotar vår nationella säkerhet.

Förvaltningsutskottet tar inte ställning till frågan om brådskande grundlagsordning, eftersom den ingår i grundlagsutskottets behörighet. Utskottet påpekar dock att det i sitt betänkande om redogörelsen för den inre säkerheten (FvUB 5/2017 rd) framhåller det nödvändiga i att uppdatera den nationella lagstiftningen så att våra myndigheter har behörighet och förmåga att få behövlig information om hot mot Finlands vitala intressen. Enligt betänkandet är det därför nödvändigt att förvärva underrättelseinformation om verksamhet och händelser som allvarligt hotar den nationella säkerheten. Dessutom har de sakkunniga som utskottet hört vid behandlingen av den föreliggande propositionen på bred front varit eniga om att det hade varit befogat att sätta lagstiftningen om civil underrättelseinhämtning enligt proposition RP 202/2017 rd i kraft ännu tidigare.

FÖRSLAG TILL BESLUT

Förvaltningsutskottet föreslår

att grundlagsutskottet beaktar det som sägs ovan.

Utlåtande FvUU 7/2018 rd

Helsingfors 11.4.2018

I den avgörande behandlingen deltog

vice ordförande Timo V. Korhonen cent
medlem Anders Adlercreutz sv
medlem Antti Kurvinen cent
medlem Sirpa Paatero sd
medlem Olli-Poika Parviainen gröna
medlem Juha Pylväs cent
medlem Veera Ruoho saml
medlem Joona Räsänen sd
medlem Vesa-Matti Saarakkala blå
medlem Matti Semi vänst
medlem Mari-Leena Talvitie saml
medlem Tapani Tölli cent
ersättare Lasse Hautala cent.

Sekreterare var

utskottsråd Ossi Lantto
plenarråd Henri Helo.