SUPO

Översikt av den nationella säkerheten 2021

Sammanfattning av översikten

Underrättelseverksamhet och påverkan riktad mot Finland

Med hjälp av långsiktig inhämtning av personbaserade underrättelser försöker underrättelsetjänster komma över tillförlitlig och proaktiv information om Finland som annars inte finns att tillgå. Exempelvis arbetet med viktiga politiska ståndpunkter och spetsteknik är föremål för aktivt intresse.

Cyberhot

Det största cyberhotet är statligt cyberspionage. Det förekommer kontinuerliga försök till cyberspionage i Finland, och dessa aktiviteter förväntas heller inte avta ens på lång sikt.

Terrorism

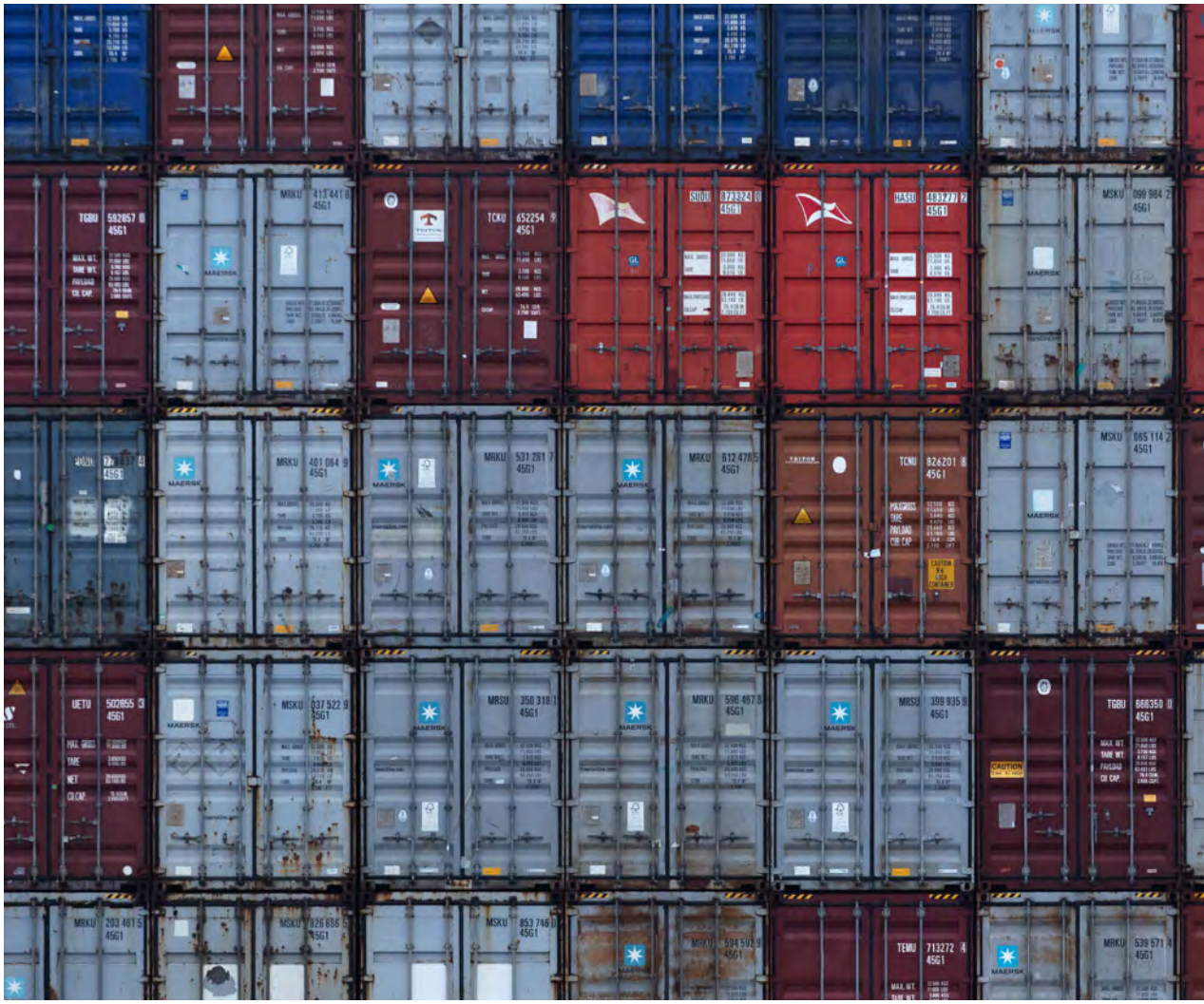
Det största terrorhotet i Finland orsakas av personer och smågrupper som stöder en högerextrem eller radikal islamistisk ideologi. En betydande del av verksamheten, såsom nätverksetableringen, sker på internet och i kommunikationsapplikationer.

Hot mot kritisk infrastruktur

Den kritiska infrastrukturen är ett långsiktigt föremål för utländsk underrättelseaktivitet i Finland. Också legitim verksamhet, såsom företagsförvärv och gemensamma projekt, kan ge diktatoriska stater tillgång till kritisk infrastruktur i Finland.

Produkter med dubbla användningsområden och massförstörelsevapen

Det förekommer försök att utnyttja Finland och finländska aktörer för anskaffning av massförstörelsevapen och deras komponenter. Finlands roll förblir sannolikt på kort sikt oförändrad i leveranskedjan för produkter med dubbla användningsområden.



Underrättelseverksamhet och påverkan riktad mot Finland

Det riktas kontinuerligt omfattande olaglig underrättelseaktivitet mot Finland och finländarna. I underrättelsehänseende är Finland intressant i synnerhet för Ryssland och Kina.

Med hjälp av långsiktig inhämtning av personbaserade underrättelser försöker underrättelsetjänster komma över tillförlitlig och proaktiv information om Finland som annars inte finns att tillgå. Exempelvis arbetet med viktiga politiska ståndpunkter och spetsteknik är föremål för aktivt intresse. Också Finlands relation till militäralliansen Nato, arktiska frågor samt cybersäkerhet och cyberkompetens intresserar.

Auktoritära stater sprider innehåll som stöder deras egen syn på saker i sociala och andra medier. Detta sker i förtäckt form och syftet är att forma de finländska beslutsfattarnas och diasporagemenskapernas tänkesätt i enlighet med den auktoritära satens egna intressen.

Diktatoriska stater har som mål att främja sina egna ekonomiska intressen även med förtäckta metoder.

Också mindre stater med auktoritärt styre bedriver förtäckt underrättelseverksamhet och påverkansarbete i Finland. Sådan småskaliga verksamhet riktar sig huvudsakligen mot människor som ursprungligen kommer från dessa länder men som vistas i Finland.

BEDÖMNING

Inga förändringar är att vänta i det hot som utländsk underrättelse- och påverkansverksamhet utgör för Finland, utan det kommer fortsatt att vara omfattande. Det är sannolikt att de försämrade stormaktsrelationerna, de ökande globala och regionala osäkerhetsfaktorerna och de växande spänningarna i världspolitiken kommer att öka de diktatoriska staternas behov av hemligt inhämtande av information och påverkansarbete.

Cyberhot

Cyberhot som äventyrar den nationella säkerheten kan manifesteras i form av cyberspionage eller cyberpåverkan från främmande staters håll. Också bieffekterna av cyberkriminalitet kan hota den nationella säkerheten, eftersom samhället för sin funktion i allt högre grad är beroende av att informationssystemen kan fungera störningsfritt.

Det största cyberhotet är statligt cyberspionage. Det förekommer kontinuerliga försök till cyberspionage i Finland, och dessa aktiviteter förväntas heller inte avta ens på lång sikt. Diktatoriska stater spionerar för att komma över information till stöd för det statliga beslutsfattandet och för att påverka de beslutsfattare som är föremål för spionaget. De kan också försöka skapa skrämseleffekt genom att visa sin förmåga att agera i cybermiljön.

Ett annat mål för cyberspionage kan vara att skaffa information om produktutveckling. Syftet är att ge de diktatoriska staterna och deras företag en starkare ställningen inom den globala konkurrensen. I Finland är det framför allt privata företag, men också högskolor och forskningsinstitut, som besitter sådan information.

Intrång i ett informationssystem som utsätts för cyberspionage kan göras via systemsårbarheter. En sårbarhet kan också möjliggöra cyberpåverkan, dvs. obehörig bearbetning av information eller förhindrande av tillgång till information. Ju mer digitalt samhället blir, desto större skada går det att åstadkomma genom att manipulera data eller hindra åtkomst till data.

Hotet om cyberpåverkan är i dagsläget kopplat till utpressningsbrottslighet med ekonomiska motiv. Även om avsikten inte är att hota Finland, utan att skaffa pengar, kan en sidoeffekt av sådan brottlighet ändå bli att Finlands nationella säkerhet äventyras, om de brottsliga aktiviteterna hindrar användningen av ett samhällskritiskt system.

Ett informationssystem kan bäst skyddas av systeminnehavaren. I Finland är en stor del av den kritiska infrastrukturen företagsägd. Att trygga kontinuiteten i verksamheten är en etablerad del av företagsledningens normala arbete, men skyddet av information ses fortfarande ofta som en teknikfråga för dem som ansvarar för informationsförvaltningen eller informationssäkerheten. Vid utläggning av funktioner är det vedertagen praxis att sörja för kontinuiteten i verksamheten genom avtalsvillkor, men det är ännu inte vanligt att man mäter hur effektiva åtgärderna för att skydda informationen är. Detta ökar risken för att bli utsatt för cyberbrottslighet.

BEDÖMNING

Det är mycket sannolikt att cyberspionaget fortsätter också på lång sikt, eftersom den globala polariseringen ökar de auktoritära staternas behov av att skaffa hemlig information om Finland samtidigt som den leder till ökad likgiltighet för Finlands suveränitet.
Det är osannolikt att fientlig cyberpåverkan från främmande stater på medellång sikt skulle riktas mot de finländska informationssystemen, såvida inte det säkerhetspolitiska läget skärps väsentligt.

Trots att Finland har en synnerligen välfungerande informationssäkerhetskultur är det sannolikt att något företag eller någon organisation inom den offentliga förvaltningen blir offer för ett kriminellt utpressningsprogram. Det är möjligt att detta får en hotande inverkan på den nationella säkerheten.

Terrorism

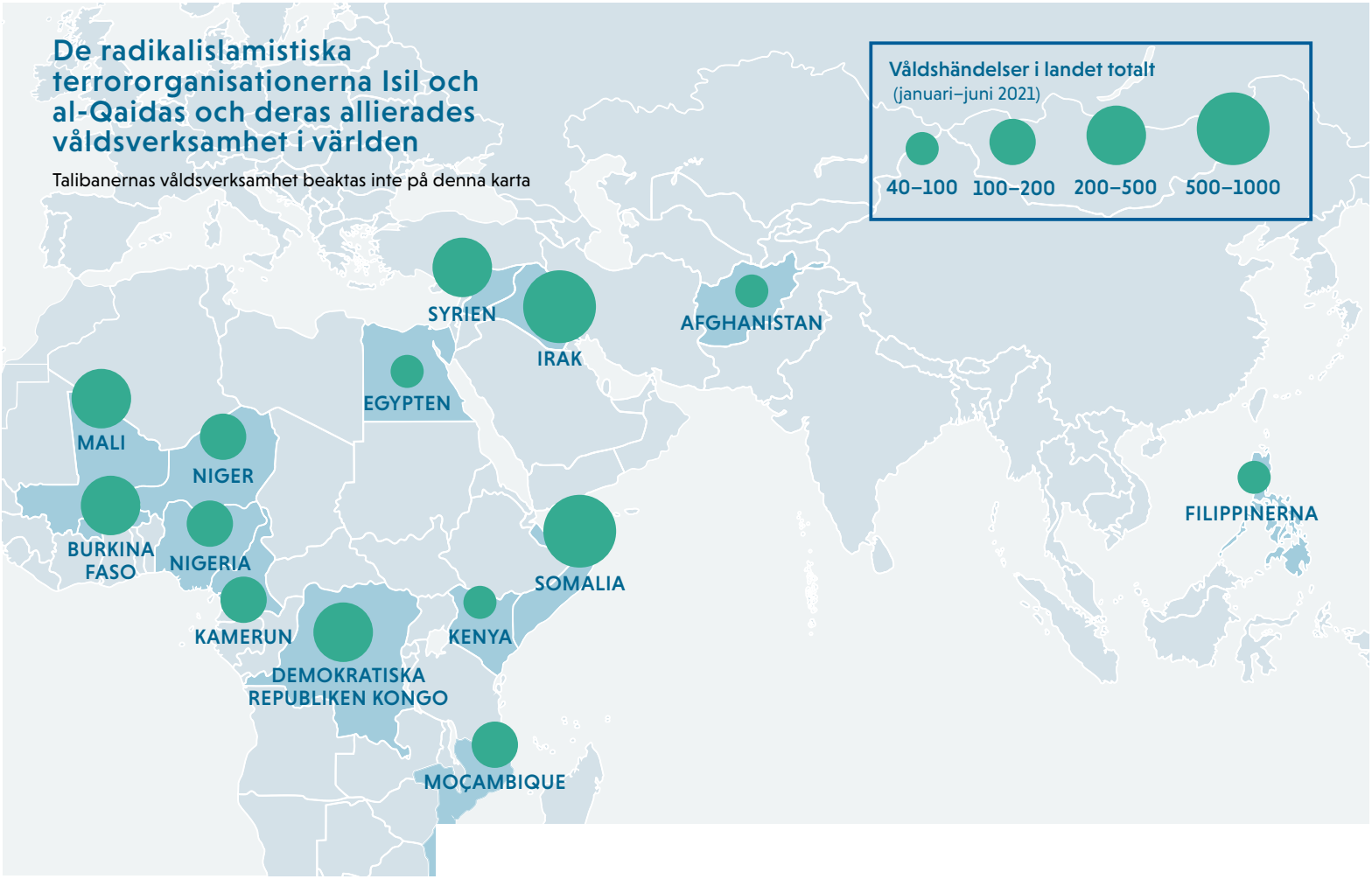
Det största terrorhotet i Finland orsakas av personer och smågrupper som stöder en högerextrem eller radikal islamistisk ideologi. Antalet målpersoner för kontraterrorism är oförändrat och ligger på cirka 390. Målpersonerna har omfattande inbördes nätverk och kontakter med utländska terroraktörer. En betydande del av verksamheten, såsom nätverksetableringen, sker på internet och i kommunikationsapplikationer.

Högerextrem terrorism utgör fortfarande ett hot i västländerna. Den senaste allvarliga attacken inträffade i Kanada i juni när fyra personer dog i ett antiislamistiskt våldsdåd. Också i Finland har det efter 2019 funnits tecken på förberedelse av konkreta gärningar. På kort sikt är högerextrema terrordåd möjliga i västländerna, och det går heller inte att utesluta möjligheten till attacker i Finland.

De globalt sett mest framträdande radikalislamistiska terroristorganisationerna är fortfarande "Islamiska staten" (Isil) och al-Qaida. De utgör fortfarande ett globalt hot och det är sannolikt att de inspirerar enskilda aktörer att utföra attacker även i Europa. Isils centrala ledning har inte förmågan att effektivt styra organisationens globala verksamhet, men dess underorganisationer är aktiva i konfliktområden och sviktande stater. Al-Qaida har under de senaste åren koncentrerat sig på att stödja sina regionala grupper och allierade. Båda organisationerna har blivit mer aktiva särskilt i Afrika söder om Sahara. Även om radikala islamistiska aktörer betraktar de fundamentalistiska talibanernas maktövertagande i Afghanistan som en seger, kommer händelserna sannolikt inte att ha några direkta konsekvenser för säkerhetsläget i Finland inom den närmaste framtiden.

Den radikalislamistiska terrorverksamhet som förekommer i Finland är i huvudsak stödverksamhet, såsom finansiering samt spridning av propaganda och en radikal ideologi, men också attacker är möjliga. De radikala islamistiska nätverken i Finland har också tidigare rekryterat utländska stridande till konfliktområden, och i Finland vistas personer som deltagit i och främjat väpnade gruppers verksamhet.

Hotet om vänsterextrem terror är lågt i Finland. Några frivilliga har rest från Finland till konfliktområdet i Syrien och Irak för att ansluta sig till väpnade, huvudsakligen kurdiska organisationer. Deras aktivitet gäller i huvudsak områden utanför Finland.



BEDÖMNING

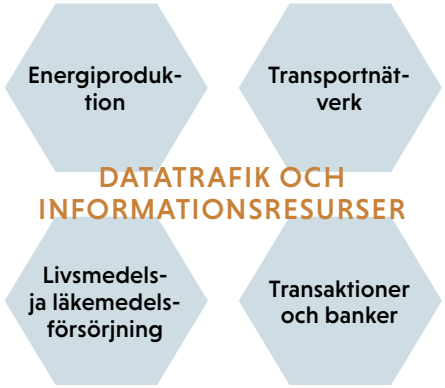
På en fyrgradig skala kvarstår terrorhotet på kort sikt sannolikt på nivå 2, dvs. förhöjt hot. Enskilda personer eller smågrupper är intresserade av att utföra terrorattentat i Finland. Det är sannolikt att fler personer återvänder till Finland från konfliktområdet i Syrien och Irak, vilket möjligt kommer att stärka de radikala nätverken i Finland och Europa. Terrorattacker i andra västländer påverkar möjligen terrorläget också i Finland.

Hot mot kritisk infrastruktur

Den kritiska infrastrukturen är ett långsiktigt föremål för utländsk underrättelseaktivitet i Finland. Också legitim verksamhet, såsom företagsförvärv och gemensamma projekt, kan ge diktatoriska stater tillgång till kritisk infrastruktur i Finland.

Aktörer från diktatoriska stater har varit intresserade av att investera i Finlands fasta infrastruktur. Hittills har det gjorts få investeringar. Utöver traditionell fast infrastruktur, såsom fastigheter och produktion, är också datatrafik samt data som behövs i informationsnät och för infrastrukturstyrning kritisk infrastruktur.

Bland annat kinesiska aktörer har varit intresserade av finländska nätinfrastrukturprojekt.



BEDÖMNING

Det är sannolikt att intresset för att investera i infrastruktur och datakommunikation kvarstår. Risken är särskilt stor i fråga om it-infrastruktur, eftersom den kan ge diktatoriska regimer tillgång inte bara till infrastruktur, utan också till uppgifter om finländare.

Den ökade övervakningen av företagsförvärv och investeringar försvårar sannolikt de diktatoriska staternas möjligheter att investera i kritiska funktioner i Finland.

Produkter med dubbla användningsområden och massförstörelsevapen

Det förekommer försök att utnyttja Finland och finländska aktörer för anskaffning av massförstörelsevapen och deras komponenter. Vidare förekommer det försök att i och via Finland skaffa exportkontrollerade produkter med dubbla användningsområden (PDA-produkter) samt annan känslig teknik med hjälp av enskilda företag och upphandlingsnätverk.

Med produkter med dubbla användningsområden avses teknik, tjänster och produkter som utöver att användas för civila ändamål också kan användas för militära ändamål. Företagen får inte exportera kontrollerade produkter med dubbla användningsområden utanför EU utan exporttillstånd. Det sker försök att kringgå exportrestriktioner bland annat genom företagsförvärv och forskningssamarbete.

Främmande stater strävar efter att påskynda den tekniska utvecklingen av sina väpnade styrkor genom anskaffningar och utländsk kompetens. Kvanttekniken och de komponenter som behövs i kvantdatorer är exempel på eftertraktad teknik från västländer, också Finland.

BEDÖMNING

Finlands roll förblir sannolikt på kort sikt oförändrad i leveranskedjan för produkter med dubbla användningsområden. Stormakterna använder exportrestriktioner aktivt i den internationella politikens kärna, och på kort sikt kommer sannolikt ny teknik och nya organisationer att omfattas av exportkontroll.

SUPO

BEGREPP SOM BESKRIVER SANNOLIKHET

Mycket osannolikt	5%
Osannolikt	20%
Sannolikt	75%
Mycket sannolikt	90%

BEGREPP FÖR ATT ANGE TID I RAPPORTEN

Den närmaste framtiden	0–6 månader
Kort sikt	6 månader–2 år
Medellång sikt	2–5 år
Lång sikt	mer än 5 år