



# Översikt av den nationella säkerheten 2020

**SUPO**  
SUOJELUPOLIISI  
SKYDDSPOLISEN



I denna översikt av den nationella säkerheten granskas fenomen som hör till Skyddspolisens verksamhetsområde och görs en bedömning av hur fenomenen utvecklas.

## Underrättelseverksamhet riktad mot Finland och finländarna

Främmande stater har fortsatt att rikta underrättelseverksamhet mot Finland, även om coronaviruspandemin försvårade verksamheten våren 2020. I förhållande till landets storlek är antalet personer anställda av utländska underrättelsetjänster stort i Finland.

Det finns flera tiotal anställda inom utländska underrättelsetjänster med permanent stationering i vårt land. Dessutom utför anställda inom främmande makters underrättelseorganisationer årligen kortvariga operativa uppgifter i Finland.

Verksamheten för främmande staters underrättelsetjänster i Finland försvårades våren 2020 när restriktioner infördes till följd av coronaviruspandemin. Efter det att restriktionerna lyftes återupptogs den personbaserade underrättelseverksamheten på samma nivå som tidigare. De omfattande reserestriktionerna har betydligt försvårat gränsöverskridande verksamhet inom den olagliga personbaserade underrättelseinhämtningen.

Av de stater som i underrättelsehänseende opererar mot Finland och finländska intressen är Ryssland och Kina de mest betydande. De utländska underrättelsetjänsternas verksamhet i Finland är av långvarig, målinriktad och planmässig karaktär. När det gäller aktuella fenomen, förekommer det variation i underrättelsefrågorna, men i bakgrunden ligger det ett långtidsintresse gentemot Finland. Till de mest centrala målen för verksamheten hör framför allt att förutse olika delområden i den finländska politiken och att påverka politiska beslut i Finland. De utländska underrättelsetjänsterna är också intresserade av finländsk teknologi och den anknytande kompetensen. Dessutom används Finland fortfarande i omfattande skala som transitland för olaglig teknikexport. Det är då framför allt fråga om sådan västerländsk teknik för militära ändamål som omfattas av exportförbud.

Inom den personbaserade underrättelseinhämtningen har information skaffats gällande samma breda ämnesområden inom Finlands utrikes- och inrikespolitik som före coronaviruspandemin. Intressanta områden för främmande staters personbaserade underrättelseinhämtning har varit bland annat Finlands arktiska politik och beslutsfattande, investeringar i vår kritiska infrastruktur och i andra strategiska områden samt finländska politiska organisationers verksamhet.

Det finns kännedom om konkreta fall där främmande stater försökt skaffa hemliga informationskällor i Finland för att komma åt information som inte finns offentligt tillgänglig. Dessutom försöker underrättelseorganisationer värva medhjälpare som gör det möjligt att direkt eller indirekt påverka den politiska beslutsprocessen eller den allmänna opinionen.

Vissa länders underrättelsetjänster försöker kontrollera sina nuvarande eller före detta medborgare som bor eller annars vistas i Finland. Bakom detta finns en strävan från underrättelsetjänstens sida att stärka den egna statens politiska system, och därför riktas övervakning och trakasserier typiskt sett mot den politiska oppositionen eller oliktkänkare. Ett annat mål är att värva informationskällor som kan leverera information om målgrupperna.

**BEDÖMNING:** Främmande staters underrättelseverksamhet mot Finland kommer att fortsätta i stor skala. De största hoten mot Finland orsakas av de ryska och kinesiska underrättelsetjänsternas långvariga aktivitet inom olika sektorer av det finländska samhället.

## Cyberspionage

Coronaviruspandemin har i någon mån flyttat fokus inom spionage mot cybermiljön. Systematiskt cyberspionage idkas mot Finland av samma länder som även annars är underrättelsemäsigt intresserade av Finland, dvs. Ryssland och Kina.

I början av coronaviruspandemin försvårade de restriktioner som infördes i Finland den olagliga personbaserade underrättelseinhämtningen, men samtidigt öppnades nya möjligheter för spionerande länder att genom intrång i informationssystem skaffa information om Finland. En stor del av samhällets viktigaste funktioner flyttades ut på nätet och sköttes genom distanskontakter. Fjärranvändningen antog så pass stora proportioner att det på kort tid krävdes beslut om lösningar där tillgången till information ofta var den mest centrala komponenten inom informationssäkerheten. Situationen ledde till att även europeiska stater med långtgående digitalisering, såsom Finland, blev sårbara på ett nytt sätt.

De länder som bedriver cyberspionage mot Finland lyckades inte genast fullt utnyttja de nya möjligheter som öppnats upp, eftersom coronaviruspandemin påverkade även deras egen verksamhet. Statligt spionage är systematisk verksamhet under någons ledning, och styrprocessen kräver tid, medan cyberkriminalitet med ekonomiska motiv snabbare kan anpassa sig till förändringar.

Om pandemin fortsätter är det ännu viktigare än under normala förhållanden att bedriva ett omsorgsfullt dataskyddsarbete. Cyberspionage bedrivs för närvarande mer aktivt än vanligen, och det är nu svårare än normalt att identifiera avvikelser som hotar säkerheten.

**BEDÖMNING:** Det är ytterst sannolikt att de länder som bedriver spionage fortsätter med aktivt cyberspionage, eftersom coronaviruspandemin försvårar resandet. Därtill har pandemin medfört att cyberspionage numera riktas även gentemot nya sektorer: läkemedelsindustrin och forskningsinstitut.

Det är sannolikt att auktoritära stater försöker utnyttja den internationella splittringen till följd av coronaviruspandemin, presidentvalet i Förenta staterna och Storbritanniens EU-utträde för att genomföra operationer som de under andra omständigheter skulle ha spärrat för.

I nuläget har betydelsen av ett omsorgsfullt dataskyddsarbete ökat. Den nationella säkerheten äventyras om tillgången till information ges företräde framför alla andra komponenter av informationssäkerheten i nyckelssystemen.

## Terrorhotet i Finland

Målpersonerna för kontraterrorism har betydande internationella kontakter. Hotet från högerextrem terrorism har ökat i västländerna, också i Finland.

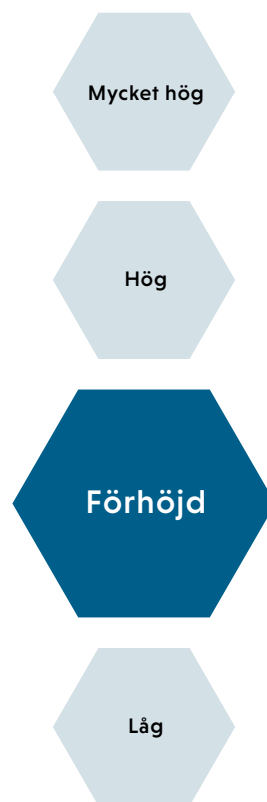
Det finns cirka 390 målpersoner för kontraterrorism. Antalet har hållit sig oförändrat, men Skyddspolisen har identifierat grupper och personer med motivation och förmåga att genomföra terroråd i Finland.

Det förekommer betydande terrorstödande verksamhet i Finland, och den tar sig uttryck exempelvis i finansiering och ideologispridning. Målpersonernas kopplingar till utländska terroristiska aktörer och nätverk är betydande. Personer som deltagit i väpnade grupperingar verksamhet eller på annat sätt bidragit till gruppernas verksamhet har kommit till Finland från konfliktområden.

Terroristorganisationerna "Islamiska staten" (Isil) och al-Qaida med sina anhängare är fortfarande ett globalt hot. Deras medlemmar och anhängare har sannolikt för avsikt att både utveckla nya taktiker för att genomföra attacker och att fortsätta att uppmuntra till attacker i västländerna.

Hotet från högerextrem terrorism har stärkts i västländerna, och planerna på terrorattacker där man försöker maximera antalet offer har ökat under de senaste arton månaderna. Personer som stöder eller sympatiserar med högerextrem terrorverksamhet har identifierats även i Finland. Högerextremismens gränsöverskridande karaktär stärks av internationella högerextrema grupper på nätet och kommunikationen på plattformarna för sociala medier.

**BEDÖMNING:** På en fyrgradig skala kvarstår terrorhotet på kort sikt sannolikt på nivå 2, dvs. förhöjt hot. Det största hotet utgörs av enskilda personer eller smågrupper som stöder en radikalislamistisk eller högerextrem ideologi och vars motiv kommer från terroristisk propaganda.



Hotnivåerna används för att beskriva hotet om terrorism mot Finland och Finlands intressen. Bedömningen av hotnivån sker utifrån den tillgängliga underrättelseinformationen, kapaciteten och motiven hos terroristorganisationerna eller de personer och grupper som har kopplingar till dem och tidshorizonten för eventuella attackplaner.



## Hybridpåverkan

Hybridpåverkan är verksamhet som bedrivs i synnerhet av auktoritära stater i syfte att med hjälp av en bred metodarsenal främja egna intressen, i allmänhet till skada för målstaten.

Det som hybridpåverkan främst försöker uppnå är att inskränka en annan stats självbestämmanderätt. Verksamheten går ut på att utnyttja målstatens sårbarheter, och den faktiska aktören bakom verksamheten vill ofta inte bli avslöjad.

Finland är föremål för hybridpåverkan, men i dagsläget är försöken att skadligt påverka landet begränsade. Hybridpåverkan inbegriper åtgärder bland annat inom den politiska, ekonomiska och militära sektorn samt inom informations- och cybers sektorn.

Utöver faktisk påverkan kan det också vara fråga om förberedelser för hybridpåverkan i framtiden.

År 2020 har det inom informationspåverkan förekommit även försök att dra nytta av coronaviruspandemin. Tills vidare har det inte lett till några betydande resultat.

**BEDÖMNING:** De statliga aktörernas beredskap att främja sina syften med till och med kraftfulla metoder för hybridpåverkan ligger kvar på en hög nivå. Samtidigt bidrar västländernas satsningar på att bekämpa hybridpåverkan till att minska hotet från sådan påverkan.

## Termer som används i rapporten

### SANNOLIKHET:

Mycket sannolikt 90 %

Sannolikt 75 %

Eventuellt 50 %

Osannolikt 20 %

Mycket osannolikt 5 %

### TIDSANGIVELSER:

Den närmaste framtiden 0–6 månader

Kort sikt 6 months–2 år

Medellång sikt 2–5 år

Lång sikt mer än 5 år