SUPO

SKYDDSPOLISEN

ÖVERSIKT AV DEN NATIONELLA SÄKERHETEN

5.12.2019

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 riktar fortsatt omfattande underrättelseaktivitet mot Finland. Finland är särskilt intressant för Rysslands och Kinas underrättelsetjänster.

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

De utländska underrättelsetjänsternas verksamhet i Finland karakteriseras av långsiktighet och systematik. Det varierar självfallet vad som är aktuellt ur underrättelsesynpunkt, men att förutse delområdena för den politik som Finland kommer att driva och att påverka de politiska besluten hör till de viktigaste målen för verksamheten. Dessutom är de utländska underrättelsetjänsterna intresserade av finländsk teknologi och den anknytande kompetensen. Finland är särskilt intressant för Rysslands och Kinas underrättelsetjänster.

På längre sikt intresserar sig främmande makter för vår inhemska utrikes- och säkerhetspolitiska debatt, våra EU- och Natorelationer, vår energipolitik, den arktiska dimensionen, säkerhetsläget i Östersjöområdet och den ekonomiska aktiviteten och försörjningsberedskapen i samhället. Den senaste tiden har bland annat Finlands agerande som EU-ordförandeland, vår ställning inom EU:s sanktionspolitik, den nationella innovationsverksamheten och högteknologiprodukter varit föremål för särskilt intresse. Skyddspolisen har observerat att utländska underrättelsetjänster visar intresse också för vår nya underrättelselagstiftning och för strukturerna för cybersäkerhet och skyddet mot informationspåverkan.

Underrättelseaktörernas intresse för investeringar i Finlands kritiska infrastruktur och andra strategiska sektorer har ökat de senaste åren. Vissa säkerhets- och underrättelsetjänster strävar dessutom efter att kontrollera och utöva påtryckningar på sina nuvarande eller före detta medborgare som bor eller annars vistas i Finland. Även medborgare i ett annat land som är bosatta i Finland eller personer som hör till majoritetsbefolkningen kan bli föremål för verksamheten.

Finland har använts som transitland vid olaglig export av produkter med dubbla användningsområden. I upptäckta fall har försäljaren vilseletts i fråga om slutanvändaren. Den berörda tekniken är avsedd att användas för militära ändamål.

BEDÖMNING: Främmande staters underrättelseaktivitet mot Finland kommer att fortsätta i stor skala även de närmaste åren.

CYBERSPIONAGE

Cyberoperationerna mot Finland från vissa staters sida kommer att fortsätta även i den närmaste framtiden. Underrättelsetjänsternas intresse för Finlands kritiska infrastruktur har ökat.

Cyberspionage avser verksamhet där staten utan rätt skaffar sekretessbelagd information ur utländska informationssystem antingen genom tekniskt intrång eller genom påtryckningar på någon som underrättelseaktören har inflytande över och som har teknisk åtkomst till sekretessbelagd information som finns lagrad i en annan stat.

Många stater har tekniska förutsättningar att kringgå skydd och ta sig in i informationssystem, men av det följer ändå inte att de använder denna kapacitet mot Finlands nationella säkerhet. För att någon systematiskt ska gå in för cyberspionage krävs det uttrycklig beredskap att kränka en annan stats suveränitet samt likgiltighet för de företags eller personers rättigheter som är föremål för spionaget. Ett sådant beslut är enkelt att fatta endast i slutna auktoritära samhällen där den styrande elitens intressen går före allt annat när intressen vägs mot varandra.

Finland utsätts hela tiden för cyberoperationer vars syfte är att spionera på staten eller att kartlägga och påverka den tekniska miljön. Cyberspionaget gäller inte bara information som den offentliga förvaltningen har. Också nyckeluppgifter om företagens produktutveckling och enskilda personers konfidentiella kommunikation har utsatts. Observationsmaterialet visar att Turla framför allt riktar sig mot det utrikes- och säkerhetspolitiska beslutsfattandet, medan målet för vissa andra cyberoperationer verkar vara att främja en framväxande ekonomis ställning som teknisk stormakt på utländska företags bekostnad.

BEDÖMNING: Hotet mot den nationella säkerheten i cybermiljön är betydande även om det inte tar sig uttryck i fysisk förödelse. Med hjälp av inhämtad information kan en spionerande stat påverka beslutsprocessen i Finland i strid med Finlands intressen och väsentligt inskränka vår handlingsfrihet. Resultatet för de företag som är centrala för Finlands samhällsekonomi bygger på tekniskt utvecklingsarbete. Företagens – och därmed hela Finlands – konkurrenskraft undermineras om konkurrerande företag med hjälp av statsmaskineriet hemmavid lyckas lägga beslag på resultatet av de finländska företagens arbete. I öppna demokratiska rättsstater skyddas individens grundläggande fri- och rättigheter också mot olagliga åtgärder från statens sida. Spionerande stater försöker agera utom räckhåll för rättsstaten.

Samhällets störningsfria funktion bygger på information – dess tillgänglighet i rätt tid och dess integritet. Den nationella säkerheten är hotad om en stat som aktivt bedriver cyberspionage eller cyberpåverkan får kontroll över kritisk infrastruktur. Och hotet finns redan innan den spionerande staten beslutar att utöva sin makt.

TERRORHOTET I FINLAND

På en fyrgradig skala kvarstår terrorhotet på kort sikt sannolikt på nivå 2, dvs. förhöjt hot. En faktor som särskilt påverkar hotbilden är om utländska stridande eventuellt återvänder till Finland från konfliktområdet i Syrien och Irak.

Enligt en fyrgradig skala ligger terrorhotet i Finland på nivå 2, dvs. förhöjt hot. Det förekommer betydande terrorstödjande verksamhet i vårt land, men samtidigt framstår Finland inte som något primärt målland för terrorattacker. Skyddspolisen har identifierat grupper och personer som har motiv och förmåga att genomföra en terrorattack. Det största hotet utgörs av enskilda personer eller smågrupper vars motiv kommer från radikalislamistisk propaganda. Terrororganisationen ”Islamiska staten” (ISIL) och dess anhängare är fortfarande ett globalt hot och försöker utveckla nya taktiker för att genomföra attacker.

Antalet målpersoner för terrorismbekämpning är cirka 390. Antalet fortsätter att öka, och målpersonerna har alltfler kopplingar till internationell terrorism. En allt större del av dessa personer har deltagit i väpnad verksamhet eller fått utbildning i terrorism. Det som framför allt påverkar terrorhotet och ökningen av antalet målpersoner är den växande inhemska radikaliseringen och återverkningarna av konflikten i Syrien och Irak. På kort sikt är eventuellt återvändande utländska terroriststridande från konfliktområdet en starkt bidragande faktor till terrorhotet.

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 vars motiv kommer från radikalislamistisk propaganda samt av utländska terroriststridande som eventuellt återvänder från konfliktområdet.

HOTNIVÅ
4. Mycket hög
3. Hög
2. FÖRHÖJD
1. Låg

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 terrororganisationerna eller de personer och grupper som har kopplingar till dem och tidshorisonten för eventuella attackplaner.

HYBRIDPÅVERKAN

De statliga aktörernas beredskap att använda till och med kraftfulla metoder för hybridpåverkan mot Finland är fortsatt hög.

Finland är föremål för aktiv hybridpåverkan. Statlig påverkan inbegriper bland annat militära, politiska och ekonomiska åtgärder samt åtgärder inom informations- och cybersektorerna. Exempelvis görs det försök att styra relationerna mellan olika länder i önskad riktning med hjälp av ekonomisk makt. Den som agerar på önskat sätt belönas ekonomiskt, medan oönskat beteende kan leda till asymmetriska motåtgärder, såväl ekonomiskt som politiskt.

BEDÖMNING: På internationella nivå har det varit kännetecknande för de senaste åren att metodarsenalen för hybridpåverkan har blivit mångsidigare exempelvis i form av valhackning eller omfattande kampanjer i sociala medier med hjälp av statistisk analys. Denna utveckling väntas fortsätta inom den närmaste framtiden. De statliga aktörernas beredskap att främja sina syften med kraftfulla metoder för hybridpåverkan ligger kvar på en hög nivå, och även påverkansåtgärder på en måttfull nivå kan snabbt ändra riktning så att de kan äventyra stabiliteten i Finland. Å andra sidan 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 %

Termer som används i rapporten: tidsangivelser

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

www.supo.fi