Hotbild mot säkerhetskänslig verksamhet

Juni 2019

Produktion: Säkerhetspolisen, juni 2019
Grafisk formgivning: Säkerhetspolisen
Typografi: Eurostile och Swift

Innehåll

1 Introduktion 4

2 Ett förändrat hot mot Sveriges säkerhet 5

2.1 Statliga aktörer 5

2.1.1 Avsikt 5

2.1.2 Förmåga 6

2.2 Ideologiskt motiverade aktörer 6

2.2.1 Avsikt 7

2.2.2 Förmåga 7

1 Introduktion

Med grund i 2 kap. 7 §, Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd, ska Säkerhetspolisen tillhandahålla hotbilder till den som bedriver säkerhetskänslig verksamhet (verksamhetsutövaren) via tillsynsmyndigheterna och till verksamheter som står direkt under Säkerhetspolisens tillsyn.

Säkerhetspolisen tillhandahåller en övergripande hotbild. Syftet är att stödja verksamhetsutövare i arbetet med att identifiera hot mot den säkerhetskänsliga verksamheten.

Hotbilden utgör en beskrivning av hot från de statliga och ideologiskt motiverade aktörer som Säkerhetspolisen följer som säkerhetskänsliga verksamheter kan behöva skyddas mot. Hotbilden ska användas som underlag i den hotbedömning som ingår i verksamhetsutövares säkerhetsskyddsanalysarbete.

För mer information se Säkerhetspolisens vägledning för säkerhetsskyddsanalys.

2 Ett förändrat hot mot Sveriges säkerhet

Förändringar i omvärlden påverkar Sveriges säkerhet. Den säkerhetspolitiska utvecklingen i Östersjöregionen, Mellanöstern och det politiska samarbetsklimatet i Europa har förändrats de senaste åren, vilket även får betydelse för Sverige. Detta medför mindre förutsägbarhet i internationella relationer.

Digitaliseringen av samhället ökar, samt tillgängliggörandet av olika typer av information, vilket på många sätt stärker demokratiska värderingar om insyn och ansvarsutkrävande. Samma information kan dock komma att utnyttjas för att påverka och hota Sveriges säkerhet. Digitaliserad information kan även komma att göras otillgänglig, förändras eller förstöras.

Digitalisering av samhällsviktig infrastruktur kan därför innebära sårbarheter för säkerhetskänslig verksamhet, i det fall även brister i informationssäkerheten finns. Teknikutvecklingen skapar löpande nya potentiella sårbarheter som kan utnyttjas av antagonister och samhället har blivit mer sårbart, delvis på grund av en bristande kännedom om hotet.

Nedan beskrivs hotet från de aktörer som Säkerhetspolisen följer, vilka kan komma att utgöra säkerhetshot mot säkerhetskänslig verksamhet.

2.1 Statliga aktörer

Säkerhetspolisen har vetskap om ett 15-tal stater som bedriver olika former av underrättelseinhämtning i Sverige. Olovlig underrättelseverksamhet och spionage syftar till att skapa ett makt- och informationsövertag. Statliga aktörer har ett intresse i att inhämta information som kan användas för att uppnå och utveckla strategiska intressen som värderas som viktiga för exempelvis nationell försvarsförmåga, ekonomisk utveckling och stabilitet, eller internationella målsättningar. Informationsöverläge gällande till exempel militära eller ekonomiska frågor ses som avgörande för dessa länder i syfte att nå säkerhetspolitiska mål.

Olika typer av påtryckningar används för att få inflytande och uppnå mål, där verktygen är allt från officiella samarbeten, upprätthållande av förtroende och goda relationer, investeringar och strategiska uppköp via statsägda eller statskontrollerade företag, till olovlig underrättelseinhämtning och påverkan.

2.1.1 Avsikt

Ryssland är den statliga aktören med en antagonistisk avsikt som har störst konsekvenser för Sveriges säkerhet. Svensk teknologi och vetenskap är av säkerhetspolitiskt intresse för Ryssland, samt kartläggning av kritisk infrastruktur. Att öka kunskapen om Sveriges totalförsvarsplanering och militära förmåga är också av intresse.

Kina bedriver underrättelseinhämtning mot ekonomiska intressen, där tillvägagångssätt bland annat är uppköp av företag med eftertraktad teknologi och cyberangrepp. Intresset är globalt och drivs av en strävan att erhålla ekonomiska fördelar, i syfte att bibehålla ekonomisk tillväxt och nationell stabilitet, vilket också träffar verksamheter i Sverige.

Statliga aktörer riktar även in sig på lärosäten och industrier i syfte att skaffa sig tillgång till spetsteknologi och spetskompetens vad gäller produkter med dubbla

användningsområden, som kan användas för att tillverka civila produkter såväl som för att framställa massförstörelsevapen. Anskaffningsförsök av denna typ av produkter sker främst kommersiellt, men även underrättelsetjänster är delaktiga. I vissa fall kan anskaffningsbehov och skyddsvärden sammanfalla inom svenska lärosäten och svenska industrier.

2.1.2 Förmåga

Statliga aktörer eftersträvar en tillfällig eller över tid upparbetad tillgång till information, där inhämtningen sker öppet eller dolt. Det kan göras via personbaserad inhämtning som innebär kontaktsökande och en skapad direktåtkomst till uppgifter, där man söker sig till eller uppmanar alternativt rekryterar andra till positioner där denna åtkomst finns. En person som rekryterats av ett annat lands underrättelsetjänst kallas agent, medan en person anställd i en position där denne har tillgång till säkerhetskänsliga uppgifter och som på eget initiativ väljer att arbeta för ett annat lands underrättelsetjänst kallas insider. Ett känt tillvägagångssätt är att utländska underrättelseofficerare arbetar under diplomatisk täckmantel, och därmed har straffrättslig immunitet. Deras huvuduppdrag kan vara att hitta viktiga informationsbärare, utifrån access, motivation och lämplighet, som sedan kan värvas som agenter eller verka som insiders. Det medför att en helt legitim affärskontakt också kan vara agent för en statlig aktör.

Statliga aktörer använder även företag, organisationer, media och officiella delegationer som plattformar för underrättelseinhämtning i Sverige.

Inhämtningen kan ske genom tekniska hjälpmedel och en allt större del av utländskt spionage bedrivs med hjälp av teknisk inhämtning, vilket sker genom att en aktör utnyttjar sårbarheter i tekniken och på så sätt skapar möjlighet för inhämtning i nätverk eller it-system och applikationer.

Information som man vill ha gäller bland annat digital infrastruktur, kommunikation och beroenden, men även systemens innehåll i form av uppgiftssamlingar och informationsflöden. Mer skyddade system kräver oftast en mer målmedveten och resursstark antagonist som arbetar långsiktigt för att hitta möjliga ingångar. Att en antagonist har tekniska möjligheter att tillskansa sig information på kan därför också innebära att man via fjärråtkomst kan förändra samt förstöra uppgifter, tjänsten eller systemet. Det kan ske via skadlig programvara eller kod.

Förmåga till teknisk inhämtning innefattar även inhämtning av olika typer av signaler, exempelvis mobiltelefonsamtal, samt inhämtning via flyg- och satellitspaning som samlar underrättelser om anläggningar och verksamheter som kan observeras från luften eller rymden.

Underrättelseinhämtning sker också i öppna källor, på internet, i sociala medier, tidningar och böcker, där kartläggning av verksamhet, personal, beroenden, förhållanden och liknande kan göras.

Ett annat tillvägagångssätt för statliga aktörer att bedriva underrättelseinhämtning och skaffa sig inflytande är att försöka vinna upphandlingar hos bland annat svenska myndigheter.

Av de statliga aktörer som nämns ovan är Ryssland framträdande, med en hög materiell såväl som immateriell förmåga till underrättelseinhämtning. Även Kina har en motsvarande förmåga.

2.2 Ideologiskt motiverade aktörer

Ideologiskt motiverade brott begås utifrån politiska skäl eller religiös övertygelse och kan vara kopplat till en konflikt, en sakfråga eller en situation som uppfattas som

eller är orättvis. De brottsaktiva aktörer som Säkerhetspolisen i nuläget följer och som begår ideologiskt motiverade brott kopplas till tre extremistmiljöer: den våldsbejakande islamistiska miljön, vit makt-miljön och den autonoma miljön i Sverige. Alla ideologiskt motiverade brott kan dock inte kopplas till de aktörer som Säkerhetspolisen följer. Med extremistmiljö avser Säkerhetspolisen individer, grupper och organisationer som hålls samman av en ideologi och betraktas som våldsbejakande genom att de utifrån denna förespråkar, främjar, eller utövar våld, hot, tvång eller annan allvarlig brottslighet för att bland annat påverka samhällsordning, beslutsfattande eller myndighetsutövning. Säkerhetspolisen fokuserar på de brottsliga handlingar som är grova eller begås systematiskt för att direkt, såväl som indirekt, påverka demokratin. Hit hör bland annat våldsbrott, hot och sabotage. Det finns också personer som inte tillhör någon av extremistmiljöerna, men som utifrån samma värdegrund säger sig vilja genomföra ett attentat eller begå grövre våldsbrott.

2.2.1 Avsikt

Vad gäller terrorhotet mot Sverige, kommer i dagsläget det främsta hotet från den våldsbejakande islamistiska miljön. Terrorhotnivån i Sverige är sedan flera år tillbaka förhöjd, även om det antagligen är så att få personer har avsikt att utföra ett attentat i Sverige. Det mest troliga attentatshotet är ensamagerande aktörer som inspirerats av en våldsbejakande islamistisk ideologi, eller möjligen från aktörer inom vit makt-miljön eller med främlingsfientliga motivbilder. Terrorattentat såväl som attentatshot syftar bland annat till att injaga allvarlig fruktan i befolkningen, försöka tvinga fram åtgärder, eller på annat sätt skada grundläggande samhällsstrukturer, skada upplevda meningsmotståndare eller uppmärksamma en sakfråga.

Våldsbejakande islamister tenderar att välja mål utifrån ett så stort skadeutfall som möjligt eller utifrån symboliskt värde, där hela samhället, civilbefolkning och folksamlingar är legitima mål. Terrorhotet mot Sverige riktar sig utifrån dessa kriterier inte primärt mot säkerhetskänsliga verksamheter i Sverige. Samtidigt försöker terrororganisationer genom våldsbejakande propaganda styra och påverka potentiella målval och bland dessa kan säkerhetskänslig verksamhet förekomma. Att på ett allmänt hållet sätt peka ut en mängd olika potentiella mål ökar även osäkerheten hos utpekade meningsmotståndare.

Vad gäller annan ideologiskt motiverad brottslighet är det primärt aktörer inom vit makt-miljön respektive den autonoma miljön med avsikt att utföra brottsliga handlingar mot säkerhetskänsliga verksamheter, exempelvis genom att rikta hot och trakasserier mot företrädare för beslutsfattande organ eller brottsbekämpande myndigheter. Många av brotten är händelsestyrda och genomförs som reaktioner på politiska förslag, myndighetsbeslut eller aktiviteter som meningsmotståndare genomför. Vidare kan sabotage eller blockader riktas mot säkerhetskänslig verksamhet i syfte att väcka opinion och skapa debatt kring en viss fråga.

2.2.2 Förmåga

För att genomföra attentat, våld och hot krävs oftast inga större eller specifika materiella resurser i form av vapen eller sprängmedel, och taktiken att ”göra vad man kan där man befinner sig”, ofta med enkla medel, används av aktörer inom de tre extremistmiljöerna. Sabotage, anlagda bränder och andra aktioner kan drabba kritisk infrastruktur och liknande. Signalvärdet i uttalade hot och genomförda handlingar som bidrar till aktörers skrämselkapital är en minst lika viktig förmåga när målet är att tvinga fram åtgärder och därmed hota demokratiska fri- och rättigheter.

Säkerhetspolisen

Säkerhetspolisen • Box 12312 • 102 28 Stockholm
Tel: 010-568 70 00 • Fax: 010-568 70 10
E-post: sakerhetspolisen@sakerhetspolisen.se
www. sakerhetspolisen.se