Säkerhetspolisen

2022–2023

Sveriges oberoende och vår demokrati är värden som kan låta självklara och som vi ofta tar för givna. Men de utmanas varje dag.

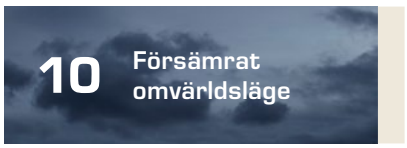
Charlotte von Essen, säkerhetspolischef

Säkerhetspolisen 2022/2023

04 Accelererande hot

Motståndskraft i en orolig omvärld 4

Hot och sårbarheter mot Sveriges säkerhet 8



10 Försämrat omvärldsläge

Förändrad hotbild när främmande makt agerar allt mer offensivt 12

Gapet mellan hot och skydd skapar sårbarheter 16

Hot mot demokratin när förtroendet för samhället undergrävs 18

20 Främmande makts verksamhet i Sverige

Så hotar Ryssland, Kina och Iran Sveriges säkerhet 22

Spionage i Sverige 26

28 Sårbarheter i en digitaliserad värld

Våldsbejakande extremism i en digital värld 30

Baksidan av det sammankopplade samhället 34

Cyberangrepp från främmande makt 38

Svensk infrastruktur del i kinesiska cyberangrepp 40

42 Det breda hotet mot samhället

Rysk teknikanskaffning i Sverige för ökad militär förmåga 44

En insider i Rysslands tjänst 46

Ensamagerande gärningspersoner ger en komplex hotbild 48

En utredning på havets botten 49

Uppdrag – genomföra ett säkert val 50

Ett ökat underrättelsehot mot svenskt beslutsfattande 52

Säkerhetshot i Sverige 53

Högre vaksamhet gav fler incidentrapporter 54

Ökat antal registerkontroller 55

56 Samverkan för att skydda Sverige

Säkerhetspolisen i korthet 58

2022 i korthet 60

Intensifierat arbete för att möta hotet mot Sverige 62

Motståndskraft i en orolig omvärld

Ryssland utgör ett allvarligt hot mot Sveriges säkerhet och är tillsammans med andra auktoritära stater allt mer aggressivt i sitt agerande. Samtidigt bidrar den oroliga omvärlden till en växande extremism, ett ökat attentatshot och ett bredare författningshot. Uppgiften att skydda den nationella säkerheten har aldrig varit viktigare.

Under det senaste året har säkerhetsläget allvarligt försämrats. Det innebär en direkt påverkan på Sverige, de yttre hoten har betydelse för den inre säkerheten. Omvärldsutvecklingen är svårbedömd, hoten förstärker varandra och förändringar sker snabbt. När främmande makts och våldsbejakande extremisters agendor sammanfaller accelererar hotet.

Spänningarna mellan den ryska regimen och västliga demokratier ökar och den nationella säkerheten måste beaktas utifrån att Ryssland ser Sverige som en del av Europa och en del av Nato. Rysslands agerande är oberäkneligt och regimen är benägen att ta stora risker. Vi kan förvänta oss både ökande rysk underrättelseverksamhet och säkerhetshotande aktiviteter mot Sverige. Det kan handla om förberedelse för sabotage, desinformation eller att regimen använder våldsbejakande extremister för att destabilisera det svenska samhället.

Främmande makts underrättelseverksamhet och säkerhetshotande aktiviteter pågår ständigt. Samtidigt som Ryssland i nuläget är det enskilt största hotet, bedriver bland andra Kina och Iran omfattande och systematiskt spionage, anskaffar teknik samt kartlägger och försöker påverka personer i Sverige som regimerna uppfattar som hot. Kina är ett växande och långsiktigt hot.

Säkerhetspolisen har under de senaste åren kunnat iaktta hur auktoritära stater blivit allt mer offensiva i sitt agerande. De skyr inga medel för att uppnå sina mål, de agerar aggressivt och använder alla samhällets resurser. Hotbilden påverkas av att auktoritära stater samverkar i högre grad i syfte att stärka det egna landet.

Situationen som råder efter att Ryssland inledde sitt anfallskrig mot Ukraina påverkar och kommer att påverka Europas och Sveriges säkerhet i många år ›

Charlotte von Essen,
säkerhetspolischef

Det försämrade säkerhetsläget innebär en direkt påverkan på Sverige, de yttre hoten har betydelse för den inre säkerheten. Omvärldsutvecklingen är svårbedömd, hoten förstärker varandra och förändringar sker snabbt.

framåt. Detta ökar betydelsen av samhällets motståndskraft och ett fungerande totalförsvar.

Som nationell säkerhetstjänst är Säkerhetspolisen en viktig del av det civila försvaret. Vårt uppdrag är att skydda Sverige och det demokratiska systemet. Säkerhetspolisen bedriver både underrättelse- och säkerhetsarbete, vi ska veta och kunna agera för att förhindra och avvärja hot mot Sveriges säkerhet och vår demokrati. Säkerhetspolisen ska se till att det som inte får hända, inte heller händer.

Det förändrade säkerhetsläget understryker vikten av att Sverige som nation bygger motståndskraft. En avgörande del i det är att vi skyddar våra hemligheter, det mest skyddsvärda. När behovet av teknik, information och kunskap hos främmande makt ökar är Sverige ett attraktivt mål. Skärpt vaksamhet behövs därför inom flera sektorer för att skydda mot såväl spionage som sabotage.

Främmande makt söker ständigt efter svagheter. Det kan röra allt från sårbarheter i it-system till luckor i svensk lagstiftning som kan utnyttjas och brott mot liv och hälsa. Eller motsättningar mellan grupper i samhället som går att förstärka.

Att försvaga ett samhälle är något som kan göras på många olika sätt. Att skapa splittring är ett av dem. Att hota och rikta hat mot samhällsföreträdare, till exempel politiker och journalister, är ett annat.

Säkerhetspolisen ser hur utvecklingen i omvärlden bidrar till en växande extremism och ett bredare författningshot. Misstron mot de som upplevs ha skapat problemen i samhället skapar en polarisering som driver extremism och det kan också påverka attentatshotet. Gränsen mellan extremism och våldsbejakande extremism suddas ut.

På digitala plattformar förekommer en spridning av konspirationsteorier och antistatliga budskap som ligger nära våldsbejakande extremistisk ideologi. Detta riskerar att på sikt undergräva förtroendet för samhällets institutioner, politikers beslutsfattande och statens legitimitet. Det här är en situation som oroar, den utnyttjas av såväl våldsbejakande extremister som främmande makt. Under senare år har vi också sett konsekvenserna av subversiv verksamhet, till exempel vid stormningen av Kapitolium i USA och händelserna i Brasilien och Tyskland.

Vi behöver tillsammans skydda de grundläggande demokratiska värderingarna. I ett läge där färre står upp för demokratin riskerar både motståndskraft och försvarsvilja att minska, vilket spelar främmande makt i händerna. Samtidigt utgör våldsbejakande extremister fortsatt ett attentatshot. Det visar inte minst händelseutvecklingen där manifestationer som koranbränningarna i Stockholm i januari 2023 lett till ett ökat hot mot Sverige och svenska intressen. Att beskriva Sverige som ett islamfientligt land och att påverka den svenska Nato-processen är ett exempel på agendor och intressen som sammanfaller. Attentatshotet påverkas också av att utvecklingen med ensamagerande gärningspersoner med oklar ideologi, ibland minderåriga och ibland drabbade av psykisk ohälsa, som radikaliserats online fortsätter.

Tillsammans utmanar detta Sveriges säkerhet. Som säkerhetstjänst följer Säkerhetspolisen hela tiden noga utvecklingen i Sverige och omvärlden.

Vi vidtar ständigt åtgärder för att skydda Sverige och säkra framtiden för demokratin. Men att hitta de okända hoten innan de blir verklighet blir en allt större utmaning när informationsmängderna i samhället växer. Att få använda teknikens möjligheter och ha tillgång till rätt information vid rätt tillfälle är därför helt avgörande för att fortsatt förhindra terroristattentat och spioneri. Här är också den egna tekniska förmågan, där teknik och operativ verksamhet inom Säkerhetspolisen arbetar nära, viktig.

Säkerhetspolisens arbete handlar om att ligga steget före och motverka aktörer som på olika sätt vill skada Sverige och vår demokrati. Det gör vi i nära samverkan med nationella partners, som Försvarets radioanstalt, Militära underrättelse- och säkerhetstjänsten, Åklagarmyndigheten och Polismyndigheten, samt med internationella partners. Samverkan har under det senaste året varit avgörande för att till exempel nå framgång i arbetet med att säkerställa ett tryggt och säkert val, skapa förutsättningar för Sveriges ordförandeskap i EU och nå framgång i utredningar kring misstänkta brott mot Sveriges säkerhet. För att skydda Sverige mot ett föränderligt hot som avspeglar sig även på cyberarenan är samverkan med myndigheterna inom Nationellt cybersäkerhetscentrum (NCSC) värdefull.

Sveriges oberoende och vår demokrati är värden som kan låta självklara och som vi ofta tar för givna. Men de utmanas varje dag. Säkerhetspolisens uppdrag att skydda den nationella säkerheten och det demokratiska systemet har aldrig varit viktigare. ■

Charlotte von Essen, säkerhetspolischef

Sverige som nation måste bygga motståndskraft. En avgörande del i det är att vi skyddar våra hemligheter, det mest skyddsvärda. När behovet av teknik, information och kunskap hos främmande makt ökar är Sverige ett attraktivt mål.

Hot och sårbarheter mot Sveriges säkerhet

Auktoritära stater stärker sina positioner

Hotet från främmande makt är högt. Ryssland, men också Kina och Iran, utgör fortsatt de största säkerhetshoten mot Sverige. Auktoritära stater har de senaste åren blivit allt mer offensiva i sitt agerande. De agerar aggressivt och använder alla samhällets resurser. Hotbilden påverkas av att auktoritära stater samverkar i högre grad.

Främmande makt – hot på kort och lång sikt

Ryssland är det enskilt största hotet mot Sverige. Agerandet är oberäkneligt och regimen är benägen att ta stora risker. Ryssland har förmåga att utföra både attentat och sabotage. Samtidigt utgör Kina ett växande och långsiktigt hot mot Sverige. Iran utgör ett påtagligt säkerhetshot.

Totalförsvarsförmågan riskerar att röjas

Den snabba tekniska utvecklingen och den pågående svenska totalförsvarsuppbyggnaden innebär ökade sårbarheter. Allt fler verksamheter omfattas av Sveriges säkerhet. Brister inom säkerhetsskydd innebär att totalförsvarsförmågan riskerar att röjas allt eftersom den byggs upp. Säkerhetsskydd ska utgöra en tröskel mot angrepp.

Ett skiftande och föränderligt hot

Säkerhetshotande verksamhet från främmande makt pågår ständigt genom exempelvis olovlig underrättelseverksamhet, påverkansoperationer och cyberangrepp. Det oroliga omvärldsläget bidrar till ett föränderligt hot där främmande makts tillvägagångssätt och målval, framför allt på cyberarenan, kan skifta snabbt.

Säkerhetshotande teknikanskaffning

Främmande makt lägger omfattande resurser på att anskaffa avancerad teknologi i Sverige. Omvärldsläget och kriget i Ukraina har bland annat inneburit att Ryssland har ett ökat behov av teknologi för att kunna upprätthålla sin militära förmåga. Även Kina och Iran anskaffar teknik och kompetens, bland annat i form av forskning, i hög utsträckning.

Attentatshot och radikalisering

Det finns ett ökat attentatshot till följd av händelseutvecklingen i omvärlden. Samtidigt driver den breda extremismen på den våldsbejakande extremismen och påverkar attentatshotet. Gärningspersoner, ofta med oklar ideologisk övertygelse och ibland med inslag av psykisk ohälsa samt ibland minderåriga, radikaliseras online.

Ett brett hot mot demokratin

Utvecklingen i omvärlden bidrar till ett bredare författningshot. Spridning av konspirationsteorier och antistatliga budskap ökar. Detta riskerar att undergräva förtroendet för samhällets institutioner, politikers beslutsfattande och statens legitimitet som det demokratiska systemet. Det här är något som utnyttjas av såväl våldsbejakande extremister som främmande makt.

Förtroendet för samhället undergrävs

Våldsbejakande extremister uppmanar till att infiltrera eller påverka olika delar av samhället. Anledningen kan till exempel vara att höja sin egen förmåga, men även att påverka exempelvis myndighetsbeslut. Uppmaningar till infiltration kan även handla om att långsiktigt undergräva förtroendet för samhället.

Försämrat omvärlds

Den kraftigt försämrade omvärlds-utvecklingen medför att hotet från främmande makt är högt och säkerhetshotande verksamhet pågår ständigt. Utvecklingen bidrar även till ett bredare författningshot.


läge

Lägesbild kontraspionage

Förändrad hotbild när främmande makt agerar allt mer offensivt

Motsättningarna mellan stormakterna fortsätter att öka och den rådande världsordningen försvagas. Rysslands anfallskrig mot Ukraina i kombination med att även andra auktoritära stater agerar mer aggressivt medför ökade risker för Sveriges säkerhet.

Dagligen sker säkerhetshotande verksamhet mot Sverige i form av underrättelseverksamhet, påverkansoperationer och cyberangrepp. Hotet från främmande makt är fortsatt högt. Säkerhetspolisen ser en förändrad hotbild där auktoritära stater under de senaste åren blivit allt mer offensiva i sitt agerande när de försöker befästa sina positioner. Sverige är en arena för en större konflikt. Sammantaget ser Säkerhetspolisen hur den kraftigt försämrade omvärldsutvecklingen ökar risken för Sveriges säkerhet.

– Vi ser ett upptrappat läge där insatserna ökar. Främmande makt använder alla medel och hela det egna samhällets resurser för att nå sina mål. Det innebär att hotet mot Sverige ökar och de potentiella konsekvenserna är mycket allvarliga, säger Henrik Edwinsson, senior analytiker vid Säkerhetspolisen.

Omvärldsutvecklingen har medfört att hotet delvis ändrat karaktär där Ryssland både utgör ett militärt hot i Sveriges närområde och ett hot mot Sveriges inre säkerhet. Ryssland ser Sverige som en del av Europa, av västvärlden och som en del av Nato.

– Ryssland agerar mer oberäkneligt och riskbenäget än tidigare. Den ryska statsledningen har även visat att den inte drar sig för att använda omfattande våld för att uppnå sina mål. Samtidigt har anfallskriget mot

Säkerhetspolisen ser ett upptrappat läge där insatserna ökar. Främmande makt skyr inga medel för att nå sina mål och använder det egna samhällets alla resurser. Det innebär att hotet mot Sverige ökar och de potentiella konsekvenserna är mycket allvarliga.

Henrik Edwinsson,
senior analytiker vid Säkerhetspolisen

Ukraina en bredare dimension där Ryssland uppfattar sig vara i konflikt med det kollektiva väst och med Nato. Dessutom har USA och Europa inklusive Sverige på olika sätt stöttat Ukraina och detta påverkar hotbilden, säger Henrik Edwinsson.

Det förändrade hotet från Ryssland mot Sverige kan bland annat komma att yttra sig i form av cyberangrepp och informationspåverkan. Samtidigt ser Säkerhetspolisen en utveckling där Ryssland tillsammans med andra auktoritära stater i högre grad samarbetar med varandra och där de hjälps åt att kringgå sanktioner, vilket inte bara är en utmaning för Sverige utan även globalt.

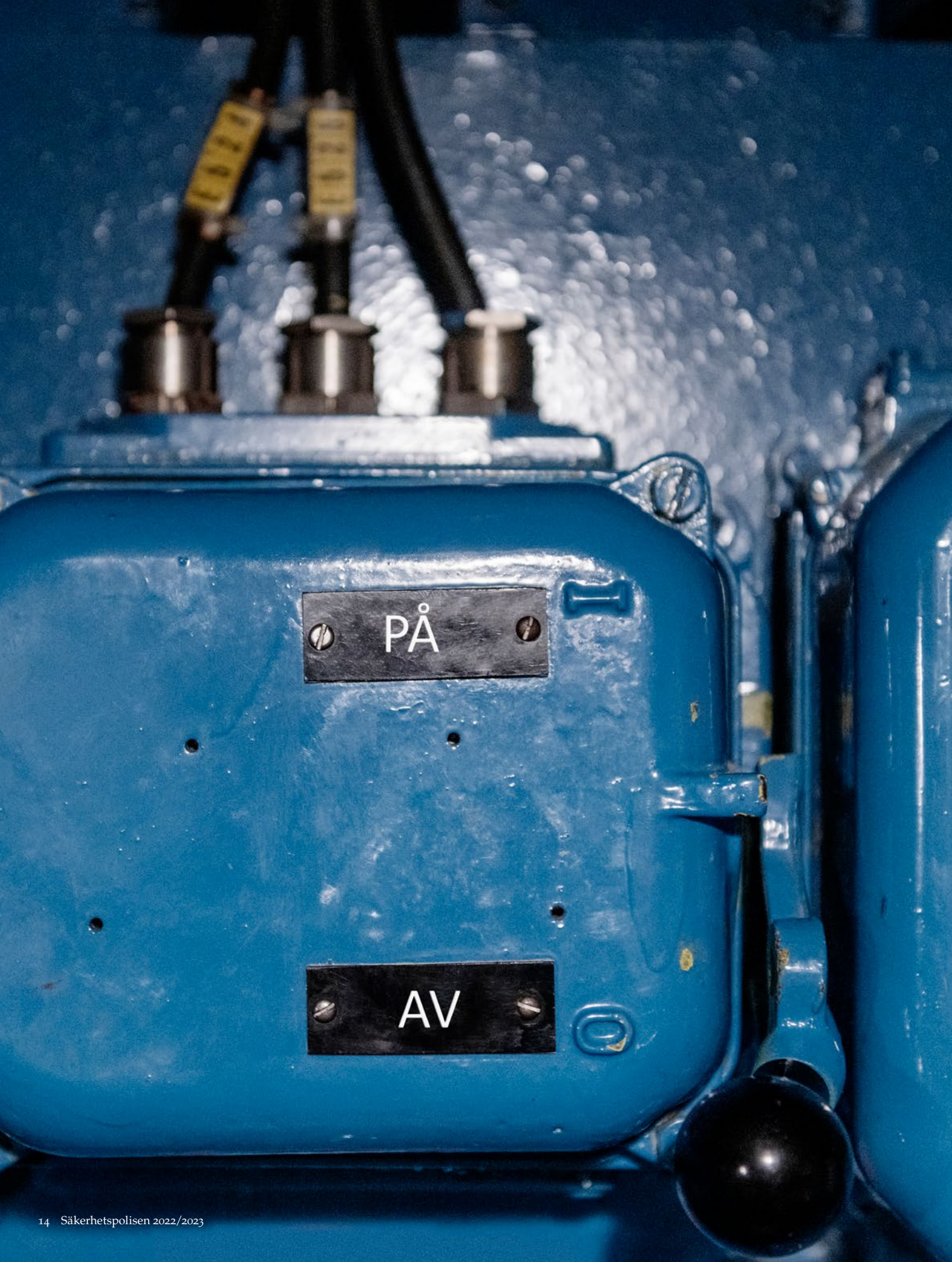
– För att skapa motståndskraft i Sverige kan vi inte se på Sverige som en isolerad del utan vi behöver bygga säkerhet med andra, både nationellt och internationellt. Samtidigt blir hotbilden mer komplex när auktoritära stater samverkar i högre grad än de gjort tidigare, vilket även kan påverka det sammantagna hotet mot Sverige, säger Henrik Edwinsson.

Främmande makt har ett stort intresse för svensk forskning och industri, och Sverige ligger i framkant inom en mängd områden som är kopplade till militära förmågor. Säkerhetspolisen ser hur teknikanskaffning blir allt viktigare för Ryssland, Kina och Iran. Det pågår dagligen en dold teknik- och kunskapsinhämtning från bland annat dessa länder i syfte att höja de egna förmågorna.

– Teknikanskaffning från främmande makt är ett stort problem. Omvärldsläget och kriget i Ukraina har bland annat inneburit att Ryssland har ett ökat behov av teknikanskaffning för att kunna upprätthålla sin militära förmåga, men även Kina anskaffar teknik och kompetens dolt i hög utsträckning, säger Henrik Edwinsson.

Västvärldens åtgärder innebär att Ryssland har fått det svårare att bedriva underrättelseinhämtning eller säkerhetshotande verksamhet via officiella plattformar. Ryssland kan därför komma att utnyttja ombud i form av företag eller institutioner för att påverka svensk opinion och svenskt beslutsfattande eller för att inhämta information. Det kan också handla om att använda personer inom våldsbejakande extremism i syfte att undergräva och destabilisera samhället, vilket kan ske genom exempelvis desinformation eller sabotage.

Om Ryssland är ett konkret hot mot Sveriges säkerhet här och nu utgör Kina ett mer långsiktigt och ›


PÅ
AV

växande hot mot Sverige. För Kina är det övergripande målet att säkerställa regimens fortlevnad vilket även är syftet med den säkerhetshotande verksamhet som bedrivs mot Sverige. Kina använder sina säkerhets- och underrättelsetjänster för att främja kinesiska intressen inom bland annat politik, ekonomi, vetenskap och teknik. Kinesiska medborgare är även skyldiga enligt lag att bistå underrättelsetjänsterna vid behov. Kina bedriver en mångsidig och kvalificerad verksamhet mot mål i andra länder. Denna verksamhet riktas även mot Sverige och mot svenska intressen utomlands.

För att bygga ett starkt, rikt och oberoende Kina krävs teknisk spetskompetens, innovationsförmåga och militär förmågeutveckling. I detta syfte bedriver både privata och offentliga kinesiska aktörer och individer inhämtning mot svenskt näringsliv, svensk försvars- och rymdindustri samt svenska forskningsinstitutioner och universitet.

Svensk teknik, produkter, kunskap och information bedöms vara av stort värde för Kinas militära utveckling. Kinesiska investeringar och uppköp i Sverige har under det senaste decenniet ökat kraftigt inom sektorer där Sverige har spetskompetens. Konsekvenserna av den omfattande kinesiska inhämtningen mot svenska företag och forskningsinstitutioner riskerar att dränera Sverige på innovationsförmåga och konkurrenskraft.

– Den inhämtning av teknik och kunskap samt påverkan som den kinesiska staten bedriver i Sverige är inte alltid olaglig, men den utgör ett hot mot Sveriges säkerhet. I Sverige finns det fortfarande en relativt utbredd okunskap om det kinesiska hotet, vilket i sig utgör en stor sårbarhet. Detta gör svenskar i alla samhällsfunktioner och svenska företag sårbara för kinesisk påverkan och inflytande samt för inhämtning, säger Henrik Edwinsson.

För auktoritära stater som Ryssland, Kina och Iran är regimens fortlevnad högst prioriterad. Under hösten 2022 har stora demonstrationer ägt rum i Iran vilket medför att regimen har ett stort fokus på det som sker inom landet. De iranska underrättelsetjänsterna har dock under en längre tid agerat utanför sitt egna lands gränser och om regimen pressas ytterligare så ökar möjligen hotet mot oppositionella även utomlands.

De iranska underrättelsetjänsterna utgör ett säkerhetshot mot Sverige genom att de bedriver olovlig underrättelseverksamhet mot i första hand oppositionella som befinner sig här. Regimen bedriver underrättelseinhämtning i Sverige och det finns också globalt ett påtagligt hot om våld gentemot oppositionella. Givet att det finns en stor iransk diaspora i Sverige där många nyttjar sina grundlagsfästa rättigheter att uttrycka kritik mot den iranska regimen, finns det också ett intresse från de iranska underrättelse- och säkerhetstjänsterna att kartlägga personer i Sverige.

Med en orolig omvärld där främmande makt agerar mer offensivt och oberäkneligt ökar även osäkerheten för Sverige.

– Under det senaste året har vi sett att det förekommer mellanstatliga konflikter och även protester och ett ökat missnöje i många auktoritära stater. Utvecklingen ökar risken för ett oberäkneligt beteende hos dessa regimer. Detta skapar en rad osäkerhetsfaktorer och gör att omvärldsläget och dess påverkan på Sverige i vissa delar kan vara svårbedömt, säger Henrik Edwinsson. ■

Sammanfattning kontraspionage

Säkerhetspolisen ser en förändrad hotbild mot Sverige. Ryssland och andra auktoritära stater agerar mer aggressivt och samarbetar vilket medför ökade risker för Sveriges säkerhet. De tre länder som utgör det största säkerhetshotet är Ryssland, Kina och Iran. Främmande makts olovliga teknikanskaffning är ett stort problem.

Lägesbild säkerhetsskydd

Gapet mellan hot och skydd skapar sårbarheter

Omvärldsläget har skapat ett föränderligt hot där främmande makts målval kan skifta snabbt. Samtidigt saknar verksamheter kunskap kring de egna skyddsvärdena, vilket riskerar att skapa sårbarheter.

Säkerhetsskyddet ska vara utformat för att klara av förändringar i hotbilden. Rysslands anfallskrig mot Ukraina får globala konsekvenser, vilket i sin tur skapar ett föränderligt hot. Främmande makts tillvägagångssätt och målval, framför allt på cyberarenan, kan skifta snabbt utifrån händelseutvecklingen. Därför behöver verksamhetsutövare kontinuerligt testa och utvärdera det egna säkerhetsskyddet.

Det försämrade säkerhetspolitiska läget bidrar till att återuppbyggnaden av totalförsvaret blir allt viktigare för Sveriges säkerhet. Såväl offentliga som privata verksamheter är centrala i denna återuppbyggnad. Flera aktörer får i samband med detta utökade eller nya uppdrag och roller som har betydelse för Sveriges säkerhet och som därmed kräver ett fullgott säkerhetsskydd.

Återuppbyggnaden av totalförsvaret innebär att det är fler än tidigare som bedriver säkerhetskänslig verksamhet. Det gör samtidigt att riskerna ökar, då verksamheter som tidigare inte haft tillgång till säkerhetskänslig information nu behöver kunna hantera det på ett säkert sätt, och där ser Säkerhetspolisen att det finns brister.

– Säkerhetsskydd ska utgöra en tröskel för angrepp. Därför är det bekymmersamt att verksamhetsutövare har ett delvis bristande säkerhetsskyddsarbete. Om säkerhetsskyddet brister så riskerar Sveriges

Främmande makts tillvägagångssätt och målval, framför allt på cyberarenan, kan skifta snabbt utifrån händelseutvecklingen.

David Hughes, chef inom verksamhetsområde säkerhetsskydd vid Säkerhetspolisen

Sammanfattning säkerhetsskydd

Främmande makt genomför ständigt punktinsatser för att skapa osäkerhet och för att bedriva påtryckningar. Det finns brister i verksamheters förmåga att skydda sig mot både spionage och sabotage. Verksamheter saknar även kunskap kring de egna skyddsvärdena vilket tillsammans med brister i säkerhetsskyddsarbetet riskerar att röja Sveriges totalförsvarsförmåga.

totalförsvarsförmåga att röjas allt eftersom den byggs upp, säger David Hughes, chef inom verksamhetsområde säkerhetsskydd vid Säkerhetspolisen.

Det finns idag brister i säkerhetsskyddet hos säkerhetskänsliga verksamheter inom alla områden, det vill säga inom personalsäkerhet, fysisk säkerhet och informationssäkerhet. Verksamheter saknar bland annat förmåga att upptäcka intrång i informationssystem och har grundläggande brister i exempelvis den säkerhetsskyddsanalys som verksamhetsutövare är skyldiga att göra. Det finns även brister inom säkerhetsskyddade upphandlingar.

Säkerhetspolisen ser samtidigt hur utvecklingen i omvärlden innebär svårigheter för verksamhetsutövare att bedöma vad som är säkerhetskänslig verksamhet. Det i kombination med en bristfällig identifiering av skyddsvärden skapar potentiellt sårbarheter. Även om det finns en osäkerhet kring vad som ska klassas som säkerhetskänslig verksamhet finns en större medvetenhet idag kring vikten av att skydda den.

– Det finns en större förståelse och medvetenhet om att det finns ett hot. Gapet mellan säkerhetsskyddet och våra motståndares förmågor kvarstår, men i takt med att medvetenheten ökar skapas förutsättningar för att i vart fall minska skillnaden. Hos många verksamhetsutövare pågår ett intensivt förbättringsarbete, men det finns en resurs- och kompetensförsörjningsbrist som är ett reellt problem, säger David Hughes.

Under 2022 har Säkerhetspolisen gått ut till verksamhetsutövare vid flera tillfällen och uppmanat till stärkt säkerhetsskydd och en ökad vaksamhet med anledning av det försämrade omvärldsläget. Detta riktade sig särskilt till sektorer där angrepp skulle kunna orsaka särskilt stor skada för Sverige säkerhet, och i vissa fall för övriga Europa eller västvärlden.

Uppmaningarna bidrog till att antalet inrapporterade incidenter ökat kraftigt under året.

– Främmande makt genomför ständigt olika typer av punktinsatser för att skapa osäkerhet och för att bedriva påtryckningar. I ljuset av det som nu sker i vår omvärld är det viktigt att säkerhetskänsliga verksamheter har en ökad vaksamhet. Det är ett gemensamt ansvar att hålla Sverige säkert, säger David Hughes. ■

Lägesbild kontraterrorism

Hot mot demokratin när förtroendet för samhället undergrävs

Utvecklingen i omvärlden innebär att hotet mot Sverige och det demokratiska systemet är omfattande. Såväl våldsbejakande extremister som främmande makt verkar för att destabilisera samhället. Samtidigt finns ett förhöjt attentatshot.

Det försämrade säkerhetspolitiska läget i världen påverkar de aktörer inom våldsbejakande extremism som Säkerhetspolisen följer. De använder och reagerar på händelser i omvärlden som bevis för en påstått negativ samhällsutveckling och som motiv för att göra något åt det. Aktörerna använder sig av en mängd olika metoder som riktar sig mot olika måltavlor.

– Det traditionella attentatshotet består, men det bredare hotet mot demokratin blir allt mer framträdande. Våldsbejakande extremister använder sig av samma metoder som främmande makt i form av subversiv verksamhet, som infiltration och påverkan, för att ytterligare öka splittringen i samhället, säger Fredrik Hallström, chef för kontraterrorism och författningsskydd vid Säkerhetspolisen.

Det traditionella attentatshotet utgörs främst av ensamagerande gärningspersoner som motiveras av våldsbejakande islamistisk extremism eller våldsbejakande högerextremism. Attentatshotet kan snabbt ändras, vilket utvecklingen efter manifestationer som koranbränningen vid Turkiets ambassad i början av 2023 visar. Säkerhetspolisen ser i underrättelseflödet ett ökat antal attentatshot mot Sverige och svenska intressen utomlands, där Sverige står i större fokus för våldsbejakande islamistisk extremism. Det här är en händelseutveckling som även gynnar främmande makt och som påverkar den våldsbejakande högerextremismen.

Motståndet mot staten, samhället och dess företrädare har alltid varit en grundbult i den våldsbejakande extremismen oavsett ideologisk drivkraft. Säkerhetspolisens uppdrag utgår från det säkerhetshot som våldsbejakande extremister utgör. Men hotet består idag inte bara av brottsliga handlingar. Säkerhetspolisen ser en skiftning från rena attentatshot till ett bredare hot mot samhället.

– Det finns många sätt att försvaga det demokratiska samhället på, för att på kort och lång sikt undergräva förtroendet för samhället, och det är långt ifrån allt som är beskrivet i brottsbalken, säger Fredrik Hallström.

En del av aktiviteterna utgörs av spridande av desinformation som inte sällan utgår från konspirationsteorier om att staten är illegitim och korrupt. Konspirationsteorier återfinns även utanför de våldsbejakande extremistmiljöerna. Extrema idéer och antistatliga narrativ har fått fäste i ett bredare samhällsskikt. Det här är något som utnyttjas av såväl våldsbejakande extremister som främmande makt.

– Konspirationsteorier i sig är inte brottsliga, och ett

Det allvarligaste hotet behöver inte nödvändigtvis vara detsamma som det akuta hotet mot liv och hälsa. Det kan istället handla om verksamhet som i sig inte är olaglig, men som går ut på att i det fördolda eller på ett lågmält sätt verka för att omkullkasta samhället och vår demokrati.

Fredrik Hallström, chef för kontraterrorism och författningsskydd vid Säkerhetspolisen

motstånd mot etablissemanget har så gott som alltid funnits. Men de sprider ett narrativ som kan bidra till ett eroderat förtroende för samhället och dess institutioner. Det kan i sin tur vara säkerhetshotande. Det såg vi exempel på vid stormningen av Kapitolium i USA 2021 och tillslaget i Tyskland 2022, där det finns misstankar om en planerad statskupp, säger Fredrik Hallström.

Säkerhetspolisen ser hur våldsbejakande extremister uppmanar till att infiltrera olika delar av samhället för att kunna höja sin egen förmåga, till exempel i strid och vapenhantering, men även för att kunna påverka beslut och inriktningar. Uppmaningar till infiltration kan även handla om att långsiktigt undergräva förtroendet för samhället. På sikt kan detta betyda att synen på terrorism och hotet från våldsbejakande extremism, och hur detta ska motverkas, behöver förändras.

– Det allvarligaste hotet behöver inte nödvändigtvis vara detsamma som det akuta hotet mot liv och hälsa. Det kan istället handla om verksamhet som i sig inte är olaglig, men som går ut på att i det fördolda eller på ett lågmält sätt verka för att omkullkasta samhället och vår demokrati. Det här är en stor utmaning för Säkerhetspolisen att upptäcka och motverka, säger Fredrik Hallström. ■

Sammanfattning kontraterrorism

Utvecklingen i omvärlden innebär att hotet mot Sverige och det demokratiska systemet är omfattande. Det traditionella attentatshotet från våldsbejakande islamistisk extremism och våldsbejakande högerextremism består och ökar i vissa delar, medan det bredare hotet mot demokratin blir allt mer framträdande. Våldsbejakande extremister bedriver subversiv verksamhet i form av infiltration och påverkan för att öka splittringen i samhället.

Subversiv verksamhet

Säkerhetshotande verksamhet som syftar till att i det fördolda störta eller förändra det demokratiska statsskicket eller sätta landet i beroende av främmande makt. Subversiv verksamhet bedrivs bland annat genom metoder som propaganda, desinformation, infiltration, kriminalitet, sabotage och hot om terror.

Främmande verksamhet i Sverige

Länder som Ryssland, Kina och Iran bedriver säkerhetshotande verksamhet mot Sverige. Det sker i form av bland annat spionage, cyberangrepp, olovlig teknikanskaffning och påverkanskampanjer.

de makts amhet

Så hotar Ryssland, Kina och Iran Sveriges säkerhet

Ryssland, Kina och Iran bedriver alla omfattande underrättelseverksamhet och säkerhetshotande aktiviteter i Sverige, vilket innebär ett hot mot den territoriella suveräniteten och ett oberoende beslutsfattande. Det leder även till att grundläggande fri- och rättigheter undermineras samt att jobb och kunskap försvinner från Sverige.

Ryssland – det största hotet

Ryssland är den enskilt största hotaktören mot Sveriges säkerhet, och bedöms även vara den enda aktören i Sveriges närområde som utgör ett militärt hot.

De ryska underrättelse- och säkerhetstjänsterna utgör ett verktyg i den ryska regimens strategiska mål att stärka landets geopolitiska, ekonomiska, teknologiska och militära mål. Uppdraget är också att undanröja hot mot den egna regimen.

Ryssland bedriver kontinuerligt underrättelseinhämtning i Sverige. Det sker bland annat från ryska diplomatiska beskickningar i Sverige där underrättelseofficerare verkar under diplomatisk täckmantel. De inhämtar löpande information om svensk politik, försvar och ekonomi. Vissa ägnar sig även åt anskaffning av civil och militär teknik.

Den huvudsakliga säkerhetshotande verksamhet som Ryssland bedriver i och mot Sverige består av underrättelseinhämtning. Det handlar bland annat om verksamhet riktad mot politiker och tjänstemän i Sverige, det svenska totalförsvaret, civil och militär industri samt individer i Sverige som kritiserar den ryska regimen.

Genom cyberspionage och signalspaning ägnar sig Ryssland åt underrättelseinhämtning från rysk mark. Den tekniska inhämtningen bedrivs metodiskt och långsiktigt.

Ryssland ägnar sig åt dold anskaffning av avancerad teknologi och kunskap i syfte att bland annat höja sin egna militära förmåga.

Ryssland använder sig av proxys, ombud, i syfte att destabilisera, etablera plattformar för påverkansverksamhet och förmåga till sabotage samt krigsförberedelser. De använder sig även av företag som kan ligga i gråzonen för vad som är lagligt. Ryssland använder Sverige som en plattform för att öka sin militära förmåga.

En del av den säkerhetshotande verksamhet som Ryssland bedriver i och mot Sverige utgörs av påverkansverksamhet. Framför allt sker det mot personer inom den ryska diasporan i Sverige, men det bedrivs även påverkan mot bland annat politiker och tjänstemän, och desinformation sprids i syfte att påverka bilden av Ryssland.

Kina – ett långsiktigt och växande hot

De kinesiska underrättelsetjänsterna bedriver en systematisk och omfattande underrättelseverksamhet och säkerhetshotande verksamhet mot Sverige och svenska intressen. Målet är att nå Kinas långsiktiga ambition att positionera sig som en global stormakt.

Den kinesiska underrättelseverksamheten riktas mot ett brett spektrum av områden i det svenska samhället. Den för Sverige mest allvarliga underrättelseverksamheten utgår från resande underrättelseofficerare och underrättelseofficerare som arbetar från och i Kina, liksom från kinesiska nätverksangrepp.

Kina har ambitioner att bli ledande inom flera teknikområden, bland annat rymdteknik. Svensk teknik, produkter, kunskap och information bedöms vara av stort värde för att uppnå Kinas långsiktiga mål. Kinesiska investeringar i Sverige har under det senaste decenniet ökat kraftigt inom sektorer där Sverige har spetskompetens samt inom kritisk infrastruktur. Det sker bland annat i syfte att tillgodogöra sig teknik, innovation och kunskap, personal samt skapa access till nätverk och utvecklingsplattformar inom prioriterade sektorer, men även för att möjliggöra påverkan av svenskt beslutsfattande. Kinesisk verksamhet i form av strategiska uppköp, anskaffning av teknik, särskilda produkter och särskild kunskap kan utgöra ett allvarligt hot mot Sverige och svenska intressen.

Även andra kinesiska aktiviteter, som forsknings- och affärsutbyten, strategiska produktanskaffningar, investeringar och uppköp, teknik- och kunskapsöverföring via rekryteringsprogram kan utgöra allvarliga säkerhetshot mot Sverige. Förutom att dessa aktiviteter kan möjliggöra för Kina att inhämta stora mängder information ger de även ofta access till känslig information, kunskap, produkter och teknologi.

Kina kartlägger dissidenter i Sverige och bedriver omfattande underrättelse- och hotaktiviteter mot regimkritiker för att reducera deras yttrande- och handlingsfrihet. Kina lägger avsevärda resurser på att påverka internationell opinion och åtgärder för att få individer att idka självcensur, även i Sverige.

Det finns en mycket hög förmåga hos kinesiska aktörer gällande elektroniska angrepp, och Kina använder cyberangrepp för att inhämta information.

Kina bedriver påverkanspolitik i syfte att omforma globala normer och värderingar samt för att stoppa regimkritiska åsikter. De försöker även förmå andra länder att fatta beslut som gynnar Kinas intressen.

Kinesiska medborgare är enligt 2017 års nationella underrättelselag skyldiga att bistå underrättelsetjänsterna vid behov.

Den sammantagna kinesiska säkerhetshotande verksamheten riskerar att undergräva svensk export och innovationsförmåga och den kan på sikt allvarligt påverka svensk konkurrenskraft och sysselsättning och är ett allvarligt ekonomiskt hot mot Sverige.

Iran – ett påtagligt säkerhetshot

Iran bedriver underrättelseverksamhet och säkerhetshotande verksamhet i och mot Sverige och svenska intressen i form av underrättelseinhämtning, påverkan mot oppositionella och genom anskaffningsverksamhet. De iranska underrättelsetjänsterna har också under en längre tid genomfört angrepp mot personer som uppfattas hota den iranska regimens stabilitet.

I Sverige är Irans underrättelseverksamhet i första hand riktad mot ledande oppositionella inom den iranska diasporan.

Det är vanligt förekommande att personer som reser till Iran blir utsatta för närmanden från de iranska underrättelsetjänsterna. Under senare tid har risken att utsättas för närmanden och godtyckliga frihetsberövanden ökat.

Svensk teknologi som produkter med dubbla användningsområden och kritiska spetsprodukter för både civil och militär användning är av intresse för Iran. Iran anskaffar både teknik och kunskap genom olovliga metoder, och utvecklar bland annat sin egen förmåga på svenska universitet och lärosäten.

Iran bedriver industrispionage som främst riktas mot svensk högteknologisk industri och svenska produkter som kan användas i kärnvapenprogram.

Under senare år har flera fall uppmärksammats i Europa där Irans underrättelsetjänster har utfört eller planerat att utföra attentat. Det finns även fall i Sverige, där bland annat en person under 2019 dömdes för grov olovlig underrättelseverksamhet mot person. Även därefter finns det konkreta fall där Säkerhetspolisen har avvärjt attentatsplaner som har varit kopplade till iranska underrättelsetjänster.

Utöver att använda mänskliga källor för inhämtning utnyttjar Iran även nätverksangrepp som ett inhämtningsverktyg.

Spionage i Sverige

De senaste åren har flera spioner gripits både i Sverige och runt om i Europa. Spioneri pågår här och nu och flera länder har underrättelseofficerare på plats i Sverige med uppdrag att samla in information. Det är information som kan skada Sveriges säkerhet om den avslöjas för främmande makt.

Att ett flertal spioner gripits i Europa under det senaste året kan bero på ett ökat underrättelsebehov från främmande makt i samband med ökade sanktioner och ett oroligt omvärldsläge. Samtidigt har Säkerhetspolisen förstärkt arbetet med kontraspionage liksom samarbetet både nationellt och internationellt.

Ett flertal länder bedriver spionage mot Sverige, men de tre länder som bedöms utgöra de största säkerhetshoten mot Sverige är Ryssland, Kina och Iran. Spionaget är till stor del riktat mot Sveriges territoriella suveränitet, ekonomi och välstånd, självständiga beslutsfattande och grundläggande fri- och rättigheter.

Olika länder har olika syften med sitt spionage, och Sverige är ett attraktivt land för länder som olovligen vill komma över både kunskap, information och teknik för militära och civila ändamål. För en stat som har ambition att bli en global stormakt är teknikanskaffning en viktig del, likaså forskning som bedrivs på svenska universitet och lärosäten. Spionage kan också handla om att skaffa kunskap om politiska beslut eller försök att kartlägga dessa, samt om att kartlägga dissidenter och påverka dem genom hot.

Det finns i korthet två sätt att bli agent. Det kan dels ske genom värvning, dels genom att en person själv uppsöker representanter för en annan stat i syfte att sälja eller ge hemlig information. Varje år sker värvningsförsök av personer i Sverige, och främmande makt lägger både tid och resurser på att kartlägga och försöka värva potentiella agenter. Processen inleds med en kartläggning som kan ske över flera år, och syftar till att hitta sårbarheter hos en person som kan utnyttjas vid en värvning. Det handlar till exempel om personliga egenskaper, svagheter, ekonomi och familjesituation. Även personer med dubbla medborgarskap eller som har en annan typ av anknytning till en auktoritär stat löper risk att utsättas för påtryckningar och hot.

Utöver användandet av mänskliga källor använder främmande makt även teknisk inhämtning. Cyberspionage sker både i syfte att stjäla information och för att förbereda sabotage, och kan pågå under lång tid utan att den verksamhet som utsätts för det upptäcker intrånget. ■

Så värvas en agent

1. Analys över vilken information som behövs.

2. Målsökning i syfte att hitta en person som kan dela med sig av den eftersökta informationen.

3. Studie där personen i fråga kartläggs.

4. Närmande sker där en underrättelseofficer tar kontakt med den utpekade personen.

5. Vänskap blir nästa steg om själva närmandet varit lyckat. Denna fas kan vara i flera år.

6. Värvning av personen genom att den ombeds dela med sig av hemlig information. Om det lyckas har främmande makt lyckats rekrytera en agent.

Sårbarheter digitali

Den digitala utvecklingen i samhället ökar möjligheterna för främmande makt att inhämta information och genomföra förstörande angrepp. Samtidigt innebär digitaliseringen också att våldsbejakande extremister kan nå fler och skapa nya allianser.


i en
serad värld

Våldsbejakande extremism i en digital värld

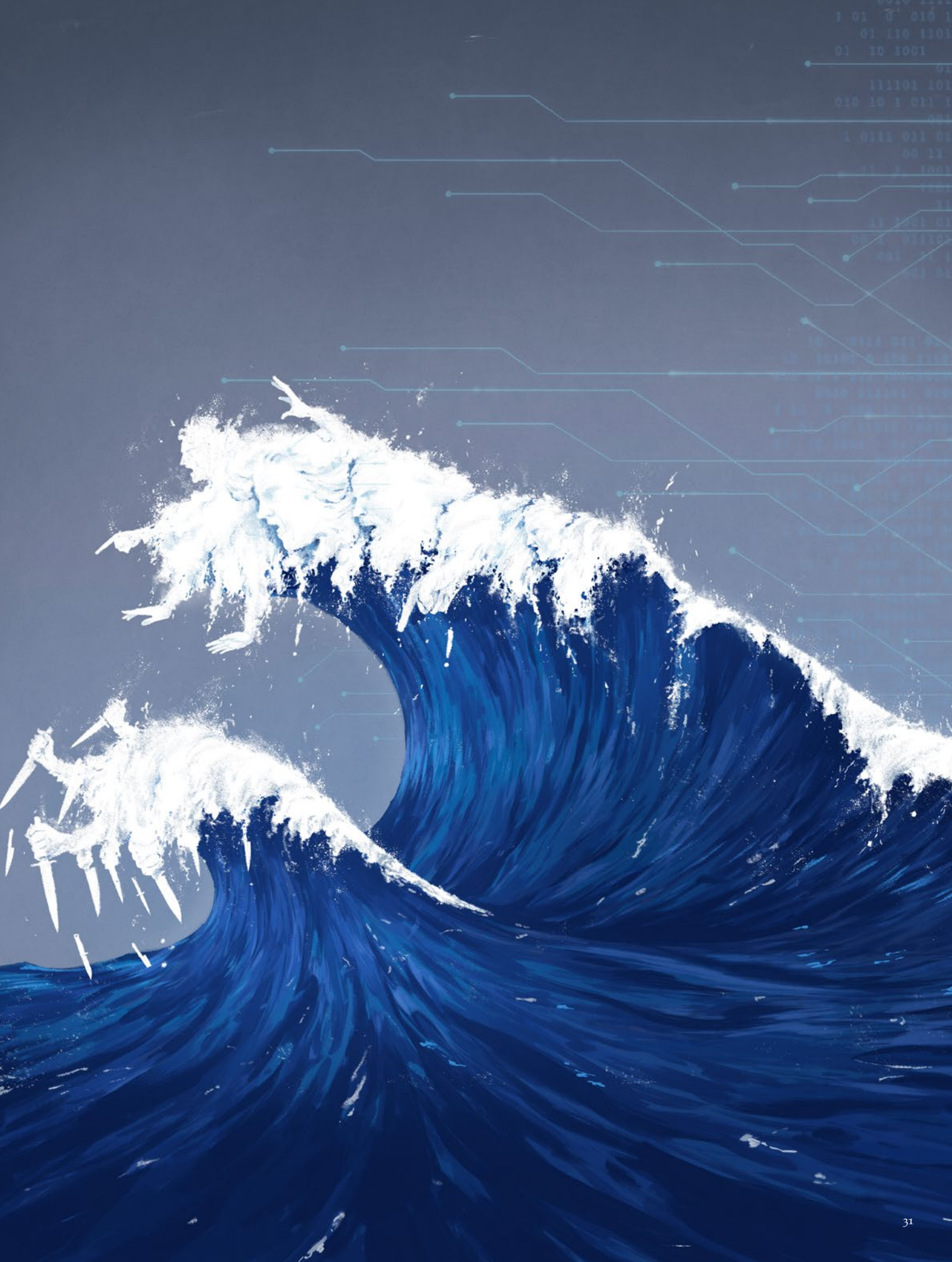
I takt med digitaliseringen har en stor del av den våldsbejakande extremismens aktiviteter flyttat ut på nätet. Där sker såväl radikalisering som rekrytering. Utvecklingen innebär att det blir svårare att upptäcka hoten.

Den digitalisering som pågår i samhället, och som har pågått under en längre tid, påverkar de aktörer som Säkerhetspolisen följer. Idag nås allt fler av våldsbejakande extremisters budskap och Säkerhetspolisen ser att avhumanisering och legitimering av våld blir vanligare.

Interaktionen sker främst på digitala plattformar. Hastigheten, räckvidden och möjligheten att både skapa nya allianser och att nå andra som delar samma världsbild är alla bakomliggande faktorer. Utvecklingen kan bidra till att tröskeln för att engagera sig i en våldsbejakande extremistisk miljö och ge uttryck för brottsliga handlingar sänks. Extrema tankar och uttryck har normaliserats och i viss mån accepteras.

– Det här gör det svårt att veta vem som är våldsbejakande extremist, det vill säga vem som vill göra något för att skada samhället och vem som bara uttrycker sig extremt. Särskilt eftersom personer som ger uttryck för hat, konspirationsteorier och en negativ syn på samhällsutvecklingen, och som även uppmuntrar till våld, driver på radikalisering av våldsbejakande extremister. Många av dessa tillbringar även en stor del av sin tid i den digitala världen där risken är stor att personen fastnar i en form av ekokammare. I dessa förstärks och uppmuntras narrativ och tankegångar snarare än utmanas, säger Susanna Trehörning, biträdande chef för kontraterrorism och författningsskydd vid Säkerhetspolisen.

Flera av de aktörer som på egen hand har planerat eller utfört attentat eller andra grova våldsbrott ingår i digitala gemenskaper där de interagerar med likasinnade i olika delar av världen. I flera fall sker detta i de krypterade delarna av internet, där information ›



Personer som ger uttryck för hat, konspirationsteorier och en negativ syn på samhällsutvecklingen, och som även uppmuntrar till våld, driver på radikalisering av våldsbejakande extremister. Många av dessa tillbringar även en stor del av sin tid i den digitala världen där narrativ och tankegångar förstärks och uppmuntras snarare än utmanas.

Susanna Trehörning, biträdande chef för kontraterrorism och författningsskydd vid Säkerhetspolisen

enbart är tillgänglig en kort tid. Detta skapar allt större utmaningar. Säkerhetspolisen bearbetar idag stora mängder information, något som ökade ytterligare efter manifestationer som koranbränningen i Stockholm i januari 2023. Och utvecklingen bedöms fortsätta.

– Sedan manifestationerna har vi sett en mycket stor ökning av konkreta attentatshot. Samtidigt fortsätter spridningen av hat och konspirationsteorier, säger Susanna Trehörning.

Den digitala utvecklingen innebär att möjligheterna att verka i det dolda ökar.

– Det i sin tur betyder att det bedömda mörkertalet av hotaktörer som befinner sig online kommer att öka avsevärt och vi måste därför ha rätt verktyg för att hitta hoten. Säkerhetspolisen behöver till exempel få utökade möjligheter att hantera information på ett sätt som ökar vår förmåga att både bedöma och förebygga hot. Vi har dessutom tidigare talat om behovet av att kriminalisera innehav av avrättnings- och tortyrfilmer, för att stävja en utveckling där våldsanvändning normaliseras, säger Susanna Trehörning.

Säkerhetspolisen ser även hur radikaliserade krafter sänder ut sina budskap i kanaler där barn och unga

spenderar tid, som populära sociala mediekanaler samt gaming- och streamingplattformar. Att våldsbejakande extremister söker sig till platser där yngre finns i syfte att försöka påverka och rekrytera är inte ett nytt fenomen. I grund och botten handlar det om att våldsbejakande extremister finns där unga finns, oavsett om det handlar om en närvaro i den digitala världen eller i den fysiska.

– Det beror delvis på att våldsbejakande extremister har en långsiktig målsättning med sin verksamhet och därför fokuserar på att rekrytera ungdomar som anses vara påverkningsbara. Men också på att många våldsbejakande extremister själva är unga och kan interagera relativt ostört med sina jämnåriga i sociala medier, säger Susanna Trehörning.

Säkerhetspolisen har sett exempel på hur unga individer från sina pojk- och flickrum kunnat ha kontakt med ideologiskt övertygade personer, ta del av instruktioner och manualer om vapen- och sprängmedelstillverkning och uttrycka hat mot samhället eller grupper.

För utomstående kan det vara svårt att upptäcka radikalisering, särskilt när den sker digitalt. Dessutom möjliggör digitala plattformar anonymitet, vilket kan göra det svårt att avgöra vem som ligger bakom det som delas. Antidemokratiska, ofta falska, budskap döljs i flöden av korrekt information. Aktörerna paketerar sina budskap på sätt som passar en yngre målgrupp. Oftast görs det med ord och bilder som i sig inte är brottsliga, men som kan bidra till att forma en uppdelning mellan ”vi och dom” i tidig ålder.

De negativa konsekvenserna av detta handlar inte bara om radikalisering utan även om näthat, kränkningar och trakasserier. Detta kan i sin tur bidra till en ökad mottaglighet för de budskap som våldsbejakande extremister sänder.

– I våra flöden ser vi många unga. Därför är det så viktigt att hela samhället hjälps åt och att närvarande vuxna och goda förebilder ser och bekräftar barn och unga och därmed bidrar till att de onda krafterna inte får fäste. Det är även viktigt att bryta de effekter som ekokammare medför där det blir en rundgång av åsikter och radikaliserande krafter till stor del får stå oemotsagda. Det kan bland annat ske genom en ökad dialog. Alla som finns där unga finns kan bidra till att öka motståndskraften mot våldsbejakande extremism, säger Susanna Trehörning. ■

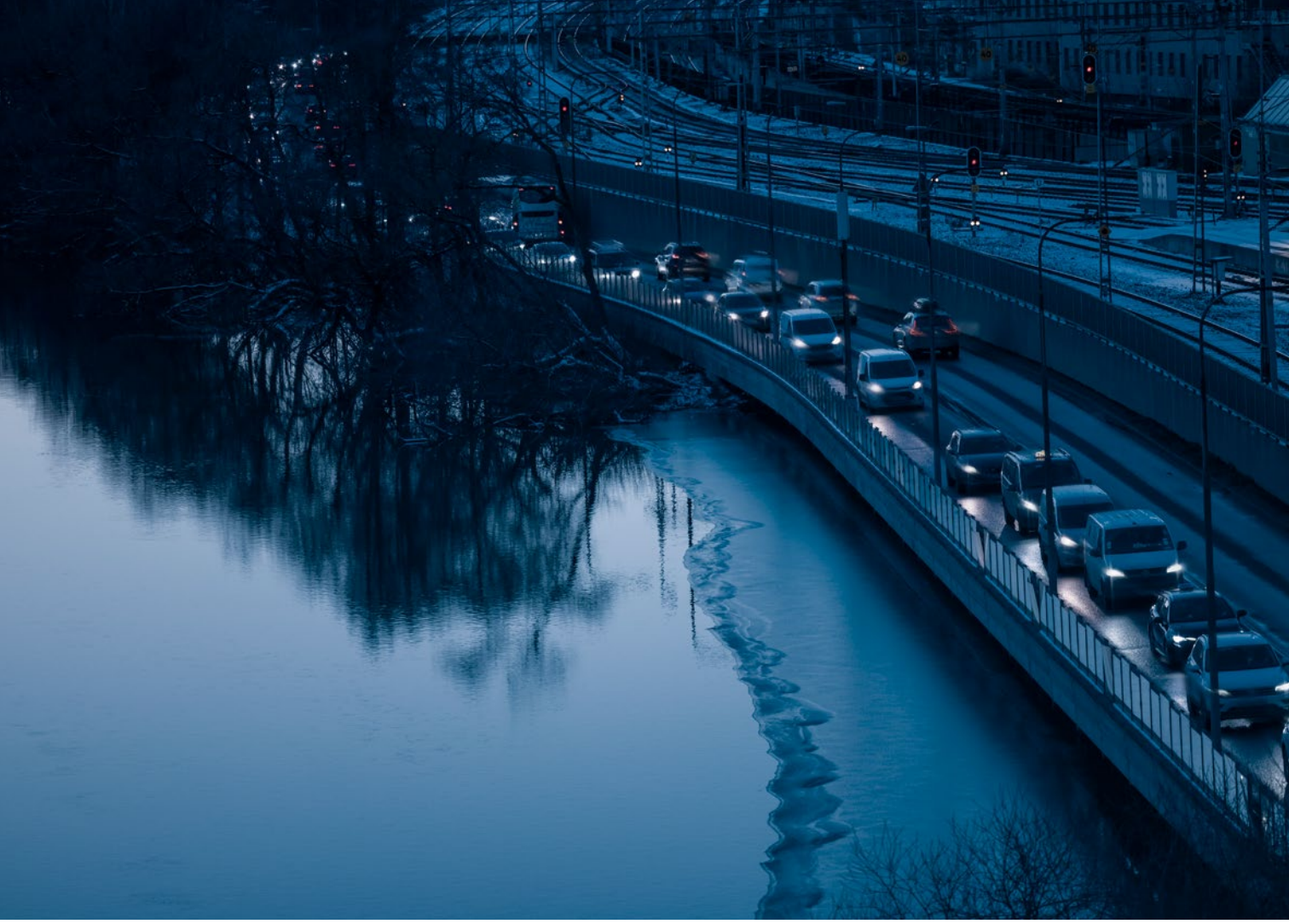
Baksidan av det sammankopplade samhället

Stora delar av samhället är allt mer beroende av digitaliseringen för att kunna driva den dagliga verksamheten. Cyberangrepp i syfte att komma åt, skada, störa ut eller manipulera stödfunktioner och system riskerar att få allt större påverkan. Verksamheter måste kunna stå emot i de värsta av lägen.

I takt med den digitala utvecklingen ökar främmande makts och kriminella grupperingars möjligheter till såväl informationsinhämtning som förstörande angrepp. Cyberangrepp kan nyttjas som verktyg för en mängd olika syften, som att skapa utrikes- och säkerhetspolitiska fördelar, gynna landets egen forskning och utveckling, skapa konkurrensfördelar för inhemska företag eller för att ta fram underlag för påverkansoperationer. I vissa fall förbereds cyberförstörande angrepp som kan användas i en upptrappad situation.

– Ytterst kan cyberangrepp användas som en del i ett väpnat angrepp på ett land och då riktas in mot att slå ut samhällsviktiga funktioner och infrastruktur. Detta har vi sett i Ukraina under det gångna året. Från kriminella grupperingar har cyberangrepp allt mer kommit att kretsa kring intrång, stöld av känslig information och kryptering av verksamhetskritiska system i syfte att utpressa offer på pengar, även kallat ransomware. Detta hot har växt och riskerar att slå mot samhällsviktig verksamhet, däribland säkerhetskänslig verksamhet, säger Nils Alenius, informationssäkerhetsexpert vid Säkerhetspolisen.

En modern it-miljö hos en verksamhet består idag av en komplex sammansättning av system, applikationer och förbindelser, där mycket är kopplat till internet- och molnbaserade lösningar. Detta innebär både en exponering av data och system mot omvärlden, liksom sårbara och svårhanterliga beroenden för bland annat säkerhetskänsliga verksamheter. I de fall där en leverantör har långtgående åtkomst till system eller en viss hård- eller mjukvara som är nödvändig för en verksamhet, blir det extra allvarligt när ett angrepp sker mot leverantören eller leveranskedjan som sådan. >



Ett intrång hos en leverantör eller genom en leveranskedja, som till exempel mjukvaruuppdateringar, kan generera åtkomst till en mängd olika it-miljöer, och kan även indirekt drabba säkerhetskänsliga verksamheter, utan att specifikt vara riktade mot dessa. Beroenden av komponenter, mjukvara, tjänster, kompetens och de leveranskedjor som försörjer dessa skapar sårbara beroenden som kan skada Sverige.

– Digitaliseringen har medfört mycket positivt, och en stor del av den digitalisering som har skett är idag nödvändig för att upprätthålla ett effektivt och konkurrenskraftigt samhälle. Med digitaliseringen följer dock tyvärr ett antal komplexa beroenden och sårbarheter som inte alltid har omhändertagits i tillräcklig omfattning. Brister i säkerhetsarbetet hos en leverantör eller samarbetspartner, som exempelvis en missad säkerhetsuppdatering, kan snabbt få eskalerande konsekvenser för den egna organisationens it-miljö. Det är nödvändigt att bedriva ett heltäckande säkerhetsskyddsarbete för att skydda sig mot de angrepp som digitaliseringen öppnar upp för, säger Nils Alenius.

Vissa typer av system är ständigt uppkopplade mot internet, vilket gör dem sårbara för elektroniska angrepp i form av överbelastningsangrepp, intrång och ibland direkta sabotage.

– Vi ser hur verksamheter många gånger inte på förhand gjort en tillräckligt grundlig och genomgripande identifiering och värdering av de fördelar och nackdelar som införskaffning eller utveckling av olika it-system och it-tjänster medför. Detta innebär i slutänden att organisationer som helhet, och i värsta fall de säkerhetskänsliga delarna av dessa, är sårbara för den komplexitet och svårhanterliga beroendekedjor som digitaliseringen medför, säger Nils Alenius.

I takt med att funktioner i samhället, ekonomiska värden och ytterst människors liv och hälsa knyts till sammankopplade system bedömer Säkerhetspolisen att cyberangrepp riskerar att få allt värre konsekvenser. Bland annat ökar hotet i takt med att allt fler samhällsfunktioner automatiseras med stöd av mer eller mindre avancerade AI-lösningar.

Oavsett vem som ligger bakom angreppen räcker det inte bara att skydda mot angrepp på en övergripande nivå. Verksamheter måste kunna stå emot även i de värsta av lägen. Vi ser nu en eskalering i omvärlden där cyberangrepp används som en del i krigföringen, vilket är en oroväckande utveckling.

Nils Alenius, informationssäkerhetsexpert vid Säkerhetspolisen

– Teknikutvecklingen kan innebära nya sårbarheter samtidigt som den kan reducera gamla, vilket AI är ett bra exempel på. De växande informationsmängderna i samhället och utvecklingen i omvärlden gör att Säkerhetspolisen måste ha en bättre förmåga att snabbt kunna hämta in, bearbeta, analysera och tillgängliggöra relevant information. Vi behöver få ta tillvara på teknikens möjligheter, bland annat i form av AI, i informationshanteringen för att kunna hitta det okända hotet innan det blir verklighet, säger Nils Alenius.

Cyberangrepp sker dagligen mot verksamheter runt om i Sverige. De som ligger bakom cyberangreppen kan vara både främmande makt och kriminella grupperingar och hotbilden från dessa är hög. En tydlig trend är att kriminella skapar en bakdörr till system för att därefter sälja vidare till andra. De i sin tur utför själva angreppen, exempelvis genom stöld av värdefull information och utpressning genom ransomware.

En annan utveckling Säkerhetspolisen ser är att kriminella aktörer blir allt mer strategiska och långsiktiga där de bland annat använder information de tillskansat sig vid tidigare cyberangrepp. Det finns exempel på hur kriminella använt sig av e-post som stulits vid tidigare intrång vid nya phishingförsök. På så sätt skapar de en legitimitet där avsändaren ser ut att komma inifrån organisationen, vilket ökar sannolikheten att någon klickar på en länk med skadlig kod.

– Oavsett vem som ligger bakom angreppen räcker det inte bara att skydda mot angrepp på en övergripande nivå, utan verksamheter måste kunna stå emot även i de värsta av lägen. Vi ser nu en eskalering i omvärlden där cyberangrepp används som en del i krigföringen, vilket är en oroväckande utveckling. När cybervapen används i konflikter finns det också alltid en risk att de riktas direkt mot svenska mål, eller att de genom olika digitala leveranskedjor med globala förgreningar indirekt påverkar svenska mål och intressen, säger Nils Alenius. ■

Cyberangrepp från främmande makt

Ett flertal länder genomför cyberangrepp mot Sverige. Ofta finns en långsiktig agenda. Säkerhetspolisen ser en utveckling där stater använder privatpersoners infrastruktur i syfte att genomföra angrepp.

Ju större del av samhället som digitaliseras och ju mer information som finns tillgänglig digitalt, desto större möjligheter har angripare att inhämta information via cyberangrepp.

– Samtidigt genomför dessa aktörer inte bara angrepp för att inhämta information. De genomför även angrepp för att kunna bygga upp en egen infrastruktur i syfte att förbereda angrepp längre fram eller för att få tillgång till system eller metoder som kan vara av nytta i framtiden, säger Mia* som arbetar inom kontraspionage vid Säkerhetspolisen.

Att bygga upp ett eget nätverk som till stor del består av privatpersoners internetuppkopplade

Cyberangrepp – fem olika faser

Kartläggning – Angriparen kartlägger sårbarheter hos potentiella mål, eller hos specifika produkter, för framtida angrepp.

Försök – Angriparen försöker skaffa sig tillgång till it-system via exempelvis skadlig kod, sårbarheter i mjukvara eller spear phising, för att utnyttja någon av de sårbarheter som tidigare kartlagts.

Access – Angriparen har tillgång till ett system och påbörjar försök att öka behörigheten samt etablera permanent access på ett dolt vis. Accessen behöver inte användas direkt utan den kan ligga vilande under lång tid.

Exfiltrering – Arbetet med att föra ut data påbörjas. Angriparen kan välja att föra ut data kontinuerligt över lång tid, eller snabbt under kort tid för att sedan lämna systemet. Underrättelseuppdraget styr metodiken.

Sabotage – Angriparen förstör eller förhindrar åtkomst till data som gör att it-systemet inte kan användas.

enheter är något i första hand Kina ägnar sig åt, men även Ryssland och Iran samt andra aktörer gör det. Tillvägagångssättet gör det svårt att upptäcka, följa och utreda de angrepp som genomförs. Anledningen till att privatpersoners internetuppkopplade enheter används är att dessa sällan uppdateras och därmed har fler sårbarheter.

– När vi pratar om cyberangrepp från främmande makt är det flera stater som är aktiva, men de två som utför flest angrepp och som är de största säkerhetshoten mot Sverige är Ryssland och Kina. Främmande makts tillvägagångssätt skiljer sig delvis åt, där de i vissa fall använder anställda vid de egna underrättelsetjänsterna för att genomföra angrepp direkt från tjänsternas kontor. I andra fall använder de sig istället av externa bolag eller universitet, detta för att göra det svårare att koppla angreppen till den stat som utfört angreppet, säger Mia.

Främmande makt har både stora resurser och en hög förmåga att genomföra elektroniska angrepp. Ett flertal länder har egna avdelningar inom underrättelse- och säkerhetstjänsterna som bedriver inhämtning via cyberangrepp. Dessa hackergrupper kallas ofta för APT:er, Advanced Persistent Threat. En liten andel av dessa aktörer genomför även elektroniska angrepp för att förstöra andra staters infrastruktur eller annan samhällsviktig verksamhet, även om fler aktörer har förmågan att göra det. ■

** Personen är anonymiserad av säkerhetsskäl.*

Svensk infrastruktur del i kinesiska cyberangrepp

Mellan 2020 och 2021 bedrevs omfattande cyberangrepp mot mål över hela Europa. Angreppen var en del av en större kampanj som bedrevs av en kinesisk cybergruppering kallad APT31. En del av angreppen skedde från infrastruktur i Sverige.

Säkerhetspolisen arbetar med att förhindra främmande makts underrättelseinhämtning mot svenska mål. Främmande makt använder agenter på plats i Sverige, men inhämtning görs även av statliga hackare via elektroniska angrepp. Historiskt har Kina inriktat sin cyberinhämtning mot framför allt forskning, teknologi och innovationer i syfte att främja den egna industrin och ekonomin. Sedan något år tillbaka har de dock i högre grad riktat in sig mot politiska mål. Med denna nya inriktning och ett delvis nytt tillvägagångssätt angreps flera europeiska parlament och myndigheter mellan 2020 och 2021. I Sverige byggde en kinesisk gruppering, som bland annat kallas APT31, upp infrastruktur som förberedelse för framtida angrepp.

Från att till en början ha använt sig av hyrda virtuella servrar ändrade hackergruppen sitt tillvägagångssätt till att istället använda ett helt nätverk av hackade routrar som i första hand tillhörde privatpersoner i hela Europa. En stor del av den infrastruktur som APT31 byggde upp fanns i Sverige, och i vissa fall skedde angrepp mot andra länder från routrar i Sverige.

Säkerhetspolisen har haft en omfattande samverkan både nationellt och internationellt med andra säkerhets- och underrättelsetjänster för att kartlägga cyberangreppen från APT31. Genom att bygga upp ett nätverk av hackade routrar kan de infekterade routrarna kommunicera med varandra, samtidigt som det försvårar för utredning och spårning av infrastrukturen.

I samband med att certifikaten för den typ av routrar som hackats löpte ut avslutade APT31 angreppen. Även om hackad infrastruktur har använts vid angrepp tidigare var detta den första större kampanjen där främmande makt använde denna metod. Tillvägagångssättet är något som bedöms kommer att användas även framöver. I samband med angreppen mot Europa gick bland annat EU och flera länder ut och namngav APT31 för att ligga bakom angreppen. ■

Europaparlamentet i Strasbourg.
Foto: Fred Marvaux

Fakta om APT31

APT står för "Advanced Persistent Threat" och är en benämning som används för att identifiera grupperingar som ägnar sig åt olika former av cyberangrepp. Ett flertal länder har egna APT-grupperingar som de använder för att bedriva underrättelseinhämtning via cyberangrepp. APT31 utgår från Kina och bedöms av flera länder vara en del av den kinesiska underrättelsetjänsten Ministry of State Security (MSS).

Det breda hotet samhället

Ett flertal händelser som Säkerhetspolisen hanterar visar tydligt på det breda och accelererande hotet från främmande makt och våldsbejakande extremism.


mot

Rysk teknikanskaffning i Sverige för ökad militär förmåga

I november 2022 greps två personer misstänkta för att ha bedrivit en verksamhet som innebär ett allvarligt hot mot Sverige och andra stater. De tros ha anskaffat teknik som Ryssland använder i militärt syfte.

Misstankarna gäller grov olovlig underrättelseverksamhet och handlar om att avancerad teknologi som kan användas militärt i exempelvis robotar, satelliter och annan vapenteknik förts över till Ryssland och dess militära underrättelsetjänst GRU. Överföringen ska ha skett genom det företag de misstänkta personerna driver tillsammans. Det finns även misstankar om att de skaffat teknik från USA som sedan slussats vidare till Ryssland via Sverige.

Förundersökningen pågår och bedrivs av Säkerhetspolisen under ledning av åklagare vid Riksenheten för säkerhetsmål. Den fortsatta förundersökningen får visa om åtal går att väcka i ärendet.

Ryssland har stort behov av avancerad teknologi och kunskap för att utveckla och höja sin egen förmåga. Genom att införskaffa teknik dolt kan Ryssland kringgå de sanktioner som införts i olika omgångar sedan annekteringen av Krim 2014. Ryssland använder en mängd olika sätt att stjäla information från Sverige. Det kan handla om alltifrån strategiska uppköp, till att skicka underrättelseofficerare under diplomatisk eller annan täckmantel för att bland annat värva agenter i Sverige. Ryssland använder sig även av företagsstrukturer som ofta är legala, men där teknik olovligen införskaffas i syfte att föras vidare till Ryssland.

– Sverige är ett attraktivt mål för Ryssland då vi ligger i framkant inom de områden som Ryssland är intresserat av. Dessutom har vi ett öppet forsknings- och företagarklimat och det är en gynnsam miljö att verka i för länder som Ryssland. Det är viktigt för företag och forskare att förstå att teknik som används i civila sammanhang, som exempelvis halvledare, även kan användas för militära syften. Den här typen av teknik som Ryssland olovligen anskaffar är i slutänden en förutsättning för att kunna föra krig, säger Charlie*, som arbetar inom kontraspionaget vid Säkerhetspolisen.

Teknik- och kunskapsinhämtning är något som pågår hela tiden, men sett till de senaste åren har Ryssland ökat sin inhämtning.

– För Säkerhetspolisen och Sverige är det av högsta prioritet att motverka och förhindra Rysslands teknikanskaffning på området. Dels för att undvika att svensk teknologi används olagligt i kriget mot Ukraina eller mot andra stater, dels för att tekniken skulle kunna användas för att utgöra ett säkerhetshot riktat direkt mot Sverige, säger Charlie. ■

** Personen är anonymiserad av säkerhetsskäl.*

En insider i Rysslands tjänst

Ett flertal länder bedriver underrättelseverksamhet mot Sverige. I syfte att inhämta information används teknisk inhämtning såväl som mänskliga källor. I september 2021 griper Säkerhetspolisen en person som misstänks ha verkat som insider och spionerat för Ryssland.

Att det finns en insider i en organisation är en risk varje säkerhets- och underrättelsetjänst lever med. Det pågår ständiga försök att infiltrera verksamheten och främmande makt värderar insiders i säkerhetstjänster högre än i andra organisationer. De lägger ner mycket tid, pengar, resurser och teknik när det kommer till underrättelseverksamhet och skyr inga medel för att komma över Sveriges hemligheter. Det gör att det är oerhört svårt att upptäcka och utreda denna typ av händelser.

Under 2017 inleddes en förundersökning av åklagare vid Riksenheten för säkerhetsmål eftersom det fanns misstankar om att en person som tidigare jobbat på Säkerhetspolisen och inom Försvarsmakten allvarligt missbrukat sitt förtroende genom att ha spionerat för Ryssland. I samband med det inleddes ett arbete för att tillsammans med Försvarsmakten omhänderta skadorna. Under förundersökningen har Säkerhetspolisen haft en nära samverkan med Försvarsmakten. Säkerhetspolisen har på olika sätt arbetat med att inhämta bevis, bland annat med hjälp av hemliga tvångsmedel. Sedan förundersökning inleddes och fram till gripandet har den misstänkte stått under uppsikt.

– Det som har hänt är mycket allvarligt. Samtidigt ser vi det som en styrka både att vi lyckades identifiera den misstänkte insidern och att vår förundersökning lett fram till en dom i tingsrätten. Detta är mycket komplicerade brott att utreda, säger Anders Kassman, avdelningschef vid Säkerhetspolisen.

Anledningen till att någon väljer att bli spion varierar, men skälen kan bland annat vara ekonomiska, ideologiska eller att personen agerar utifrån ett missnöje eller ett hämndbegär.


Anders Kassman, avdelningschef vid Säkerhetspolisen.

– Sedan misstankarna uppstod har vi vidtagit en mängd åtgärder för att förhindra att det ska kunna ske igen. Samtidigt bygger vårt system på människors lojalitet och samarbete, och det innebär att det aldrig är hundraprocentigt vattentätt. Om en anställd bestämmer sig för att vara illojal och gå främmande makt tillhanda är det en utmaning att fånga upp, säger Anders Kassman.

Några månader efter att den misstänkta insidern häktades i september 2021 greps även hans bror. De båda åtalades i november 2022 för grovt spionerи och i januari 2023 fälldes de av en enig Stockholms tingsrätt till livstids fängelse respektive fängelse i nio år och tio månader.

Enligt tingsrätten är det ställt utom allt rimligt tvivel att bröderna gemensamt och i samråd obehörigen anskaffat, befordrat samt röjt uppgifter vars uppenbarande för främmande makt kan medföra men för Sveriges säkerhet. I domen framgår att deras syfte har varit att gå Ryssland och den ryska militära underrättelsetjänsten GRU tillhanda för egen ekonomisk vinning. Domen har överklagats.

– Det är ett ytterst allvarligt brott, som handlar om att de gamla traditionella inhämtningsmetoderna lever kvar, där främmande makt fortsätter att använda sig av mänskliga källor, säger Anders Kassman. ■

Fakta spioneri

För att en handling ska räknas som spioneri krävs att någon obehörigen anskaffar, lämnar, befordrar eller röjer uppgifter i avsikt att gå främmande makt tillhanda och vars innehåll kan medföra skada för Sveriges säkerhet om den kommer främmande makt till del.

Ensamagerande gärningspersoner ger en komplex hotbild

Utmaningarna med att upptäcka personer som på egen hand planerar och begår attentat eller andra grova våldsbrott är en del av en komplex hotbild som utmanar säkerhetstjänster i hela världen. Mordet och förberedelsen till terroristbrott under Almedalsveckan är ett exempel på detta.

Det finns ingen entydig definition av en ensamagerande gärningsperson och de är heller ingen homogen kategori aktörer. Varför någon agerar självständigt kan variera.

Historiskt sett har våldsbejakande extremister anpassat sin verksamhet i takt med att förutsättningar och omständigheter förändrats. När exempelvis säkerhetstjänster världen över blivit bättre på att upptäcka och kartlägga grupperingar och organisationer som kan och vill hota samhället har ensamagerande gärningspersoner blivit vanligare, bland annat för att undgå upptäckt. Men även personliga omständigheter som bristande förmåga till sociala och fysiska kontakter kan ligga bakom varför de väljer att agera på egen hand.

Ensamagerande refererar ofta till en övergripande målsättning utifrån en övertygelse snarare än till en viss organisation. Samtidigt delas uppfattningar och hörsammandet av uppmaningen att «göra något» ofta med andra och kan upplevas ge legitimitet att agera. Tillsammans utgör ensamagerande ett större sammanhang som i allt högre utsträckning finns på sociala plattformar där det är svårt att upptäcka, bedöma och motverka det som sker.

Säkerhetspolisen ser att individer interagerar via digitala plattformar med andra ideologiskt övertygade personer som ibland finns långt utanför Sveriges gränser. De tar både del av instruktioner och manualer om vapenanskaffning och sprängmedelstillverkning och uttrycker hat mot samhället eller vissa grupper.

Samverkande ideologiska och personliga omständigheter innebär att det finns en stor variation av tänkbara måltavlor för den som har avsikt att skada samhället. Vem, vad eller vilka som faktiskt utsätts eller drabbas är inte alltid bestämt från början eller när olika förberedelser görs, utan det kan vara tillfället som avgör.

I den information som Säkerhetspolisen får om enskilda individer finns ofta inslag av psykisk ohälsa. Många av dem är unga. Det finns också indikationer på att våldet i sig kan vara en drivkraft. Inte sällan utgår uppfattningen om oförrätter eller vilka som bär skulden för det aktörerna anser vara en negativ samhällsutveckling från olika konspirationsteorier. Gemensamt är uppfattningen om att samhället måste förändras eller till och med störtas.

Den man som under Almedalsveckan i juli 2022 mördade Sveriges kommuner och regioners (SKR) psykiatrisamordnare var en ensamagerande gärningsperson utan tydlig tillhörighet i någon ideologiskt orienterad gruppering. Han åtalades också för att ha planerat att mörda en partiledare. Stockholms tingsrätt dömde honom för mord och förberedelse till terroristbrott till sluten rättspsykiatrisk vård med särskild utskrivningsprövning. Domen har vunnit laga kraft. ■

En utredning på havets botten

Det misstänkta grova sabotaget av gasledningarna Nord Stream 1 och 2 påverkar flera länder. Säkerhetspolisen har bedrivit en unik utredning där samverkan står i fokus.

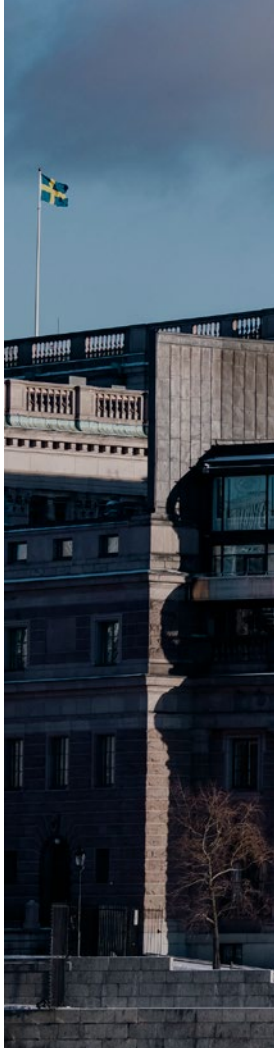
I slutet av september 2022 började gas läcka från både Nord Stream 1 och 2 i Östersjön. Kort efter de upptäckta läckorna tog Säkerhetspolisen över utredningen under ledning av åklagare från Riksenheten för säkerhetsmål. Detta då händelsen rör ett allvarligt brott som delvis kan vara riktat mot svenska intressen och det inte heller går att utesluta att främmande makt ligger bakom detonationerna.

Händelsen har gett både säkerhetspolitiska och energipolitiska konsekvenser och sabotaget har påverkat flera länder.

Ett väl fungerande samarbete mellan de svenska myndigheterna har varit viktigt under utredningen. Även om den främsta samverkan som skett har varit nationell och mellan svenska myndigheter har Säkerhetspolisen även samverkat med andra länder.

Vid genomförandet av de två brottsplatsundersökningarna vid gasledningarna fick Säkerhetspolisen särskilt stöd av Försvarsmakten, Kustbevakningen och Polismyndigheten. Undersökningarna har hittills bekräftat att det rör sig om grovt sabotage och spår av sprängämnen har säkrats. Utredningen pågår fortfarande. ■

Uppdrag – genomföra ett säkert val



Cyberangrepp och ett ökat antal hot mot personer i den centrala statsledningen var det Säkerhetspolisen i första hand lyfte som troliga hot under valrörelsen 2022. Det blev en valrörelse som följde den förväntade hotbilden.

Säkerhetspolisens uppgift under ett val är att skydda Sverige, den centrala statsledningen och svenska intressen.

– En viktig del av vårt uppdrag vid riksdagsvalet förra året var att säkerställa att vi hade en uppdaterad lägesbild som vi kunde agera utifrån. Under årets gång ändrades den beroende på händelser i omvärlden och vi såg till att ha en bra beredskap för vad som skulle kunna ske, säger Fredrik Bratt, kommenderingschef för arbetet med valet vid Säkerhetspolisen.

Säkerhetspolisens lägesbilder baseras på myndighetens uppdrag att förebygga och förhindra spionage och våldsbejakande extremism, att skydda säkerhetskänslig verksamhet och att säkerställa att den centrala statsledningen kan verka under säkra former. Säkerhetspolisens lägesbild inför valet var att utvecklingen i stort sett följde den förväntade normalbilden där extremister från både den höger- och den vänsterextrema miljön skulle bli mer tongivande ju närmare valdagen kom. I lägesbilden ingick även att hotet från enskilda hotaktörer skulle öka när politiker allt mer exponerades i media under valrörelsen.

– Det här var och är något vi tar höjd för i vårt arbete både under ett val och i vardagen. Det som vi även var beredda på var att det skulle ske cyberangrepp med koppling till valrörelsen, vilket visade sig stämma. Det vi såg var främst överbelastningsangrepp med en begränsad påverkan. Här hade vi en bra samverkan med andra myndigheter, bland annat inom ramen för Nationellt cybersäkerhetscenter (NCSC). Detta för att kunna förebygga och snabbt få en gemensam bild av vad som inträffat, men även kunna stötta om något inträffade, säger Fredrik Bratt.

Förutom cyberhotet var hotet från ensamagerande det som var mest påtagligt under valrörelsen.

– Hoten mot politiker ökar under ett valår. Det får anses som en naturlig följd av den ökade exponeringen. Ensamagerande gärningspersoner är oerhört svåra att upptäcka. Både metoder och lagstiftning behöver utvecklas för att skapa bättre förutsättningar att identifiera hoten, säger Fredrik Bratt.

Något som blev tydligt under 2022 års valrörelse var polariseringen i debatten. Under valrörelsen såg Säkerhetspolisen också ett ökat antal hot mot personer

i den centrala statsledningen, och att vissa personer blev mer utsatta än andra.

– Vi har en långtgående yttrandefrihet i Sverige, men vi ser att ett uppskruvat tonläge i den politiska debatten får efterföljare i sociala medier där både hot och hat förekommer. Detta kan i sin yttersta form innebära att tröskeln för fysiskt våld sänks. Det är i slutänden ett hot mot vår demokrati om våra folkvalda politiker inte kan utföra sitt jobb tryggt och säkert, säger Fredrik Bratt.

Utöver det arbete som skedde inom myndigheten förekom också en nära samverkan med Polismyndigheten och även andra. Säkerhetspolisen samverkade bland annat inom ramen för det nationella valnätverket för att tillsammans med andra myndigheter bidra till att stärka skyddet av valet. Valnätverket är inrättat och lett av Valmyndigheten. I det ingår förutom Säkerhetspolisen även länsstyrelserna, Myndigheten för psykologiskt försvar (MPF), Myndigheten för samhällsskydd och beredskap (MSB) och Polismyndigheten. ■

Fredrik Bratt, kommenderingschef för valet och chef för personskydd vid Säkerhetspolisen.

Ett ökat underrättelsehot mot svenskt beslutsfattande

Det finns ett ökat underrättelsehot där främmande makt riktar sin säkerhetshotande verksamhet mot politiskt beslutsfattande.

Ryssland, Kina och Iran är de länder som utgör det största säkerhetshotet mot Sverige, men det finns även andra länder som har intresse av Sverige och svenskt beslutsfattande och strategiska ställningstaganden. Frågor som i nuläget är av intresse för främmande makt rör bland annat beslutsfattande som påverkar Arktis, EU, Nato och den egna staten. Säkerhetshotet omfattar exempelvis spionerи, påverkansoperationer och cyberangrepp.

Säkerhetspolisen ser att det finns en ökad risk för att främmande makt bedriver olovlig underrättelseinhämtning för att inhämta skyddsvärd information kopplat till beslutsfattande och offentlig förvaltning. De försöker även på olika sätt påverka svenska ställningstaganden.

Att som politisk beslutsfattare bli kartlagd eller utsatt för olovlig underrättelseinhämtning är en risk som det är viktigt att vara medveten om. Risken för att som politiker eller tjänsteman bli utsatt skiljer sig åt beroende på uppdrag, men konsekvenserna är allvarliga och kan innebära ett hot mot den demokratiska processen och Sveriges suveränitet. ■

Säkerhetshot i Sverige

Vid slutet av 2022 fanns hundratals individer i Sverige som Säkerhetspolisen har identifierat som säkerhetshot. Det rör sig om individer som Säkerhetspolisen bedömer utgör ett säkerhetshot, som inte är svenska medborgare och där Säkerhetspolisen förordar utvisning. En del av dessa är kvalificerade säkerhetshot som har utvisningsbeslut enligt lagen om särskild kontroll av vissa utlänningar (LSU). Svårigheter att verkställa utvisningar gör att det ackumulerade säkerhetshotet alltjämt är stort.

Möjligheterna att använda tvångsmedel mot individer med ett utvisningsbeslut enligt LSU har ökat till följd av en ny lagstiftning. Säkerhetspolisens insatser har bland annat lett till att flera kvalificerade säkerhetshot självmant lämnat Sverige under 2022. ■

Högre vaksamhet gav fler incidentrapporter

Under 2022 gick Säkerhetspolisen ut och uppmanade säkerhetskänsliga verksamheter att vara extra uppmärksamma på händelser som avvek från normalbilden och rapportera in dessa till myndigheten. Det resulterade i en kraftig ökning av inrapporterade incidenter där en extern part misstänks ligga bakom.

Incidenter som Säkerhetspolisen fick inrapporterade under 2022, där en antagonist misstänks ligga bakom, handlade bland annat om olaga intrång och inbrott, vandalisering, fotografering av skyddsobjekt, överbelastningsattacker och dataintrång.

Verksamhetsutövare som bedriver säkerhetskänslig verksamhet är skyldiga att anmäla säkerhetshotande händelser och verksamhet till Säkerhetspolisen. Jämfört med 2021 har antalet inrapporterade incidenter med koppling till fysisk säkerhet ökat kraftigt. Säkerhetspolisen bedömer däremot inte att ökningen indikerar en faktisk ökning av incidenter inom säkerhetskänslig verksamhet. Istället tros den bero på en större vaksamhet.

Under 2022 har informationssäkerhetsincidenter minskat, men är fortsatt det område som har flest inrapporterade incidenter. De inrapporterade fallen rörande fysisk säkerhet handlar i stor utsträckning om inbrott, inbrottsförsök och vandalisering av objekt där säkerhetskänslig verksamhet bedrivs, medan det för informationssäkerhet bland annat berör dataintrång, överbelastningsattacker och ransomwareangrepp.

Incidenter kopplade till upptäckta interna brister hos verksamhetsutövare ligger, till skillnad mot incidenter där en utomstående misstänks ligga bakom, kvar på samma nivå som under 2021. Anmälningarna handlar till stor del om incidenter där säkerhetsskyddsklassificerade uppgifter varit möjliga för obehöriga att ta del av. Exempelvis har handlingar lämnats obevakade eller skickats till fel mottagare.

Säkerhetspolisen bedömer att ett mindre antal av de incidenter som rapporterats in under 2022 har utgjort ett allvarligt hot mot säkerhetskänslig verksamhet. Många incidenter rör potentiella hot mot eller sårbarheter i säkerhetsskyddet. Att Säkerhetspolisen även fortsättningsvis får in anmälningar är viktigt. Rapporterade incidenter utgör en central informationskälla i arbetet med att identifiera hot mot och sårbarheter i säkerhetsskyddet hos verksamhetsutövare som bedriver säkerhetskänslig verksamhet. ■

Ökat antal registerkontroller

Säkerhetspolisen ansvarar för att genomföra registerkontroller av personer som är placerade i säkerhetsklass. Registerkontroller är en del av den övergripande säkerhetsprövningen som ska göras av arbetsgivaren inom säkerhetskänslig verksamhet enligt lag.

Under 2022 har Säkerhetspolisen genomfört cirka 155 000 registerkontroller, att jämföra med cirka 135 000 under 2021. Säkerhetspolisen bedömer att ökningen beror på att fler verksamheter än tidigare hanterar säkerhetsskyddsklassificerad information, bland annat som en följd av upprustningen av totalförsvaret. Men också som en följd av förändrad lagstiftning där fler säkerhetskänsliga verksamheter än tidigare är skyldiga att genomföra säkerhetsprövningar. Säkerhetspolisen bedömer även att vissa säkerhetskänsliga verksamheter haft ett uppdämt personalbehov efter borttagna pandemirestriktioner, vilket haft en påverkan på antalet utförda registerkontroller.

Under 2022 har Säkerhetspolisen utvecklat ett system som digitaliserat den egna registerkontrollprocessen, vilket bland annat lett till minskade handläggningstider. Systemet möjliggör även för verksamhetsutövare att skicka registerkontroller i digital form i större utsträckning än tidigare. ■

Samverkan för att Sverige

Säkerhetspolisen arbetar målmedvetet och långsiktigt med att avvärja och förebygga brott mot Sveriges säkerhet, bekämpa terrorism och skydda den centrala statsledningen.

skydda

Säkerhetspolisen i korthet

Säkerhetspolisen är en nationell säkerhetstjänst med uppdrag att förebygga och avvärja hot mot Sveriges säkerhet och demokratin. Säkerhetspolisen bedriver säkerhets- och underrättelseverksamhet för att skydda den centrala statsledningen och Sveriges hemligheter samt bekämpa spionage, våldsbejakande extremism och terrorism.

Verksamhetsområden och regionala kontor

Kontraspionage

Säkerhetspolisen förebygger och avslöjar spioneri och annan olovlig underrättelseverksamhet. Denna kan rikta sig mot Sverige och svenska intressen utomlands samt mot utländska intressen i landet och mot flyktingar.

Säkerhetsskydd

Säkerhetspolisens arbete med säkerhetsskydd är förebyggande och långsiktigt. Säkerhetsskydd innebär att höja säkerhetsnivån i samhället genom analyser, registerkontroller, tillsyn och rekommendationer till myndigheter och företag vars verksamhet har bäring på Sveriges säkerhet.

Kontraterrorism

Säkerhetspolisen förebygger och förhindrar terroristbrott. Det kan röra sig om attentat och finansiering, utbildning, rekrytering, uppmaning och samröre kopplad till en terroristorganisation.

Författningsskydd

Säkerhetspolisen förebygger och förhindrar brott som syftar till att påverka det demokratiska statsskickets funktioner.

Personskydd

Säkerhetspolisen ansvarar för säkerheten kring den centrala statsledningen, men även andra länders beskickningsmedlemmar samt vid statsbesök eller liknande händelser. Personskyddet handlar till stor del om ett förebyggande arbete för att skyddspersonerna ska kunna utföra sina uppdrag på ett tryggt och säkert sätt.

Säkerhetspolisen arbetar även med uppdragen icke-spridning och utlänningsärenden. Uppdrag icke-spridning innebär att förhindra spridning, anskaffning och produktion av massförstörelsevapen. Arbetet sker i nära samverkan med andra myndigheter. Uppdrag utlänningsärenden syftar till att förhindra att personer som är eller kan bli ett säkerhetshot mot Sverige uppehåller eller etablerar sig i landet. En viktig del i det förebyggande arbetet är Säkerhetspolisens uppdrag som remissinstans till Migrationsverket.

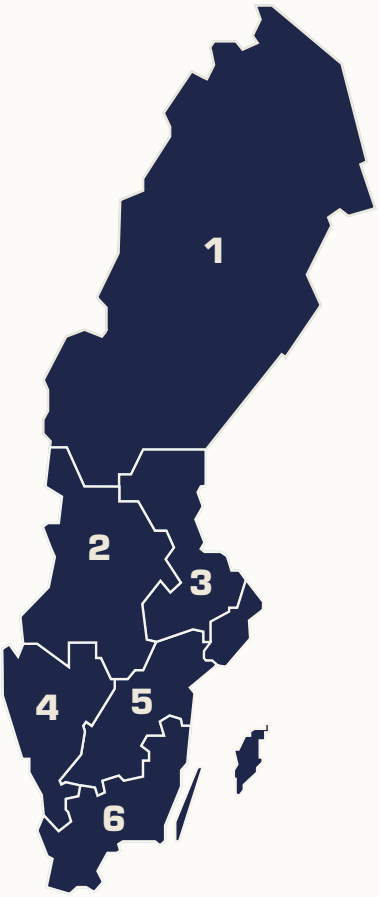
Underrättelsearbete

Säkerhetspolisen bedriver underrättelsearbete både nationellt och internationellt. Det är en del av arbetet med att förebygga och avslöja brott mot Sveriges säkerhet. Inhämtning inom Sverige sker bland annat genom spaning, källor, samtal samt kontakter med andra myndigheter och organisationer. Internationellt sker det främst genom samverkan med andra säkerhets- och underrättelsetjänster. Informationen Säkerhetspolisen får in bearbetas och analyseras för att sedan i vissa fall övergå i en förundersökning eller hanteras genom andra åtgärder. Även regeringen, andra myndigheter och organisationer kan få information för att själva kunna vidta åtgärder inom sina områden.

Styrning och insyn

Säkerhetspolisen lyder under regeringen och leds av säkerhetspolischefen. Myndigheten styrs bland annat genom en instruktion och ett regleringsbrev där mål och uppdrag specificeras. Säkerhetspolisen styrs även av olika författningar, till exempel polislagen. De flesta av Säkerhetspolisens styrande, planerande och avrapporterande dokument är sekretessbelagda med hänsyn till Sveriges säkerhet. Av operativa skäl och utifrån Sveriges säkerhet kan Säkerhetspolisen ofta inte vara öppen med vad som görs och varför.

Säkerhetspolisen granskas bland annat av Justitiekanslern och Justitieombudsmannen. Säkerhets- och integritetsskyddsnämnden (SIN) utför bland annat inspektioner för att kontrollera hur myndigheten behandlar personuppgifter och kontrollerar på begäran av enskilda hur hemliga tvångsmedel används. Regeringen utser dessutom medlemmar till Säkerhetspolisens insynsråd, vilket har till uppgift att utöva medborgerlig insyn. Samtliga riksdagspartier är representerade i rådet.



Säkerhetspolisen – en nationell säkerhetstjänst

Säkerhetspolisen finns i hela landet. Säkerhetspolisen har sex regionala kontor utöver huvudkontoret i Solna. Den regionala verksamheten arbetar inom samtliga verksamhetsområden. Kontoren finns placerade i:

1. Region Nord i Umeå: Jämtlands, Norrbottens, Västerbottens och Västernorrlands län.
2. Region Bergslagen i Örebro: Dalarnas, Värmlands och Örebro län.
3. Region Mitt i Uppsala: Gävleborgs, Uppsala och Västmanlands län.
4. Region Väst i Göteborg: Hallands och Västra Götalands län.
5. Region Öst i Linköping: Jönköpings, Södermanlands och Östergötlands län.
6. Region Syd i Malmö: Blekinge, Kalmar, Kronobergs och Skåne län.
Huvudkontor: Solna
Säkerhetspolisens huvudkontor ansvarar för Stockholms och Gotlands län.

2022 i korthet

Rysslands anfallskrig mot Ukraina

Den 24 februari inleds Rysslands anfallskrig mot Ukraina vilket innebär att det säkerhetspolitiska läget i Europa allvarligt försämras. Under året varnar Säkerhetspolisen både för ett ökat antal cyberangrepp och för påverkansförsök inför en svensk Nato-ansökan. Samtidigt har Säkerhetspolisen intensifierat sitt arbete med att minska handlingsutrymmet för främmande makt att agera i Sverige.

Foto: Stina Stjernkvist/TT

Dådet i Visby

Mitt under Almedalsveckan i början av juli 2022 mördas Sveriges kommuner och regioners (SKR) psykiatrisamordnare. Den 11 juli tar Säkerhetspolisen över förundersökningen och brottsrubriceringen ändras till terroristbrott genom mord. Personen misstänks även för förberedelse till terroristbrott genom förberedelse till mord. I november 2022 döms personen av Gotlands tingsrätt för mord och förberedelse till terroristbrott till rättspsykiatrisk vård med särskild utskrivningsprövning.

Personer döms för resandebrott

Två personer grips i februari 2022 misstänkta för resandebrott i samband med att de är på väg att lämna Sverige. Männen misstänks för att ha varit på väg att ansluta sig till IS. Båda döms till åtta månaders fängelse i både tingsrätten och hovrätten.

Grovt sabotage vid Nord Stream

I slutet av september 2022 upptäcks gasläckor från Nord Stream 1 och 2 i Östersjön. Kort efteråt tar Säkerhetspolisen över den förundersökning som Polismyndigheten inlett. Säkerhetspolisen genomför under hösten två brottsplatsundersökningar på plats med bistånd av Kustbevakningen, Försvarsmakten och Polismyndigheten. Undersökningarna stärker misstankarna om grovt sabotage och på plats hittas föremål som tas i beslag. Det finns även spår av sprängmedel. Med anledning av sabotaget uppmanar Säkerhetspolisen aktörer med ansvar för central infrastruktur inom energiförsörjning att skärpa sin förmåga att upptäcka och förhindra incidenter. Förundersökning pågår. Läs mer på sida 49.

En person misstänkt för grov olovlig underrättelseverksamhet

I november 2022 griper Säkerhetspolisen två personer i Stockholmsområdet. En av de gripna är häktad och misstänks för grov olovlig underrättelseverksamhet mot Sverige samt mot främmande makt. Det som ska ha inträffat drabbar ytterligare ett land, USA. Den andre är misstänkt för medhjälp och försatt på fri fot medan förundersökningen pågår. Läs mer på sida 44.

Flera resor till aktiv krigszon

Säkerhetspolisen är ofta med och skyddar den centrala statsledningen oavsett var de befinner sig i världen. Det senaste året har Säkerhetspolisens förstärkta livvaktsskydd fått en ny typ av resa att förhålla sig till. Under 2022 har myndigheten vid flera olika tillfällen rest till Ukraina tillsammans med skyddspersoner i den centrala statsledningen. Även om resor till konfliktzoner förekommit tidigare är det första gången som Säkerhetspolisen rest in i en aktiv krigszon där det allvarligaste hotet kommer i form av robotar och raketer.

Två personer åtalas för grovt spioneri

Två personer åtalas i november 2022 vid Stockholms tingsrätt misstänkta för grovt spioneri. Enligt åtalet har de obehörigen anskaffat hemliga uppgifter och överlämnat dessa till Ryssland. De båda greps i september respektive november 2021, och döms i januari 2023 för grovt spioneri. Domen är överklagad av bägge männen. Läs mer på sida 46.

Person med koppling till högerextremism döms för vapenbrott

I november 2021 griper Säkerhetspolisen en person misstänkt för förberedelse till allmänfarlig ödeläggelse. Misstankarna utökas sedan även till bland annat grovt vapenbrott då personen i fråga tillverkat egna 3D-vapen. Personen döms i september 2022 till tre år och sex månaders fängelse för grovt vapenbrott, brott mot lagen om brandfarliga och explosiva varor och brott mot lagen om sprängämnesprekursorer.

Flera fall av grov obehörig befattning

Under perioden april till november 2022 åtalas tre personer vid olika tillfällen för grov obehörig befattning med hemlig uppgift. De misstänks för att ha spridit hemliga och känsliga uppgifter om försvarsanläggningar. Av dessa döms en person i november till villkorlig dom och samhällstjänst. För de andra två väntas dom under 2023. Åtalen är tre av flera åtal mot personer som från september 2015 fram till februari 2019, misstänks ha spridit uppgifter som gör det möjligt att kartlägga militär infrastruktur i Sverige. Hittills har sex personer dömts. Tillsammans har de samlat information kring olika försvarsanläggningar som sammantaget innebär en risk för rikets säkerhet.

Charlotte von Essen, Säkerhetspolisen, Björn Lyrvall, FRA och Lena Hallin, Must.

Medverkan och samverkan under året

Under året som gått har Säkerhetspolisen medverkat i flertalet olika evenemang, mässor, möten och seminarier. Bland annat har representanter från myndigheten deltagit vid Folk och Försvars rikskonferens, Almedalsveckan och på Stockholm Pride. Det har även skett regelbundna möten med bland annat de nordiska säkerhets- och underrättelsetjänsterna och Säkerhetspolisen har diskuterat cybersäkerhet vid ett kungligt symposium. Ämnen som diskuterats under året har bland annat varit underrättelsehotet, det förändrade omvärldsläget, totalförsvaret, extremism och demokrati. Säkerhetspolisens chef Charlotte von Essen har under året även samverkat regelbundet och haft möten med cheferna för myndigheter inom olika delar av totalförsvaret, inte minst med Polismyndigheten, Militära underrättelse- och säkerhetstjänsten (Must) och Försvarets radioanstalt (FRA).

Intensifierat arbete för att möta hotet mot Sverige

Det kraftigt försämrade omvärldsläget har inte bara påverkat säkerhetsläget i Sverige. Det har även fått följdverkningar på Säkerhetspolisen och verksamheten.

– Vi ser att Ryssland till följd av det förändrade omvärldsläget har ett allt större behov av underrättelseinhämtning, samtidigt som även Kina och Iran fortsatt utgör ett allvarligt säkerhetshot mot Sverige. Det här har inneburit att vi som myndighet har skruvat upp vårt kontraspionagearbete ytterligare, säger Magnus Krumlinde, biträdande säkerhetspolischef.

Ett förstärkt kontraspionage innebär att Säkerhetspolisen har intensifierat arbetet för att minska handlingsutrymmet för främmande makt, men även för att stärka motståndskraften hos skyddsvärd verksamhet. Detta både genom att försvåra och förhindra främmande makts olovliga underrättelseverksamhet och genom att skapa förståelse kring vilket hot som främmande makt utgör.

– Vi har under flera år stärkt vår samverkan både nationellt och internationellt, vilket är viktigt i den globala värld vi lever i. Efter invasionen av Ukraina har vår samverkan intensifierats ytterligare vilket är nödvändigt för att tillsammans med andra skydda Sverige, säger Magnus Krumlinde.

Ryssland ser Sverige som en del av det kollektiva väst, där Sverige stödjer Ukraina på flera olika sätt. I det här läget vill Ryssland veta hur andra länder resonerar och vilka beslut som kan komma att fattas, bland annat i Nato-frågan. Det finns också ökad risk för cyberangrepp.

– Vi måste möta det breda och accelererande hotet från främmande makt, där det förändrade omvärldsläget påverkar inriktningen på vårt arbete under en lång tid framöver. Ett eventuellt Nato-medlemskap innebär att Säkerhetspolisen blir del av nya sammanhang, säger Magnus Krumlinde.

– Samtidigt fortlöper de andra delarna i vårt grunduppdrag. Det vill säga att skydda den centrala statsledningen, säkerhetsskydd och terrorbekämpning, och inte minst vårt uppdrag kopplat till författningsskyddet där vi ser antistatliga tendenser, subversiv verksamhet och en ökad misstro mot samhället, säger Magnus Krumlinde. ■

> *Vi måste möta det breda och accelererande hotet från främmande makt, där det förändrade omvärldsläget påverkar inriktningen på vårt arbete under en lång tid framöver.*
>
> *Magnus Krumlinde, biträdande säkerhetspolischef*

Produktion: Säkerhetspolisen
Grafisk formgivning: Intellecta
Illustrationer: Fredrik Tjernström
Foto: Säkerhetspolisen, TT
Tryck: Stibo Complete A/S Horsens Danmark

ISBN: 978-91-86661-23-6
Beställning: Publikationen kan laddas ner från sakerhetspolisen.se eller beställas via sakerhetspolisen@sakerhetspolisen.se

Det är Säkerhetspolisens ansvar att det som inte får hända, inte heller händer. Därför arbetar vi förebyggande. Vi avvärjer hot mot Sveriges säkerhet och mot medborgarnas fri- och rättigheter, för vårt uppdrag är att skydda och säkra framtiden för demokratin. Vi utför uppgiften handlingskraftigt och långsiktigt. Vi skyddar den centrala statsledningen och Sveriges hemligheter. Vi motverkar spionage, extremism och terrorism. För oss är de viktigaste händelserna de som aldrig inträffar.

Säkerhetspolisen