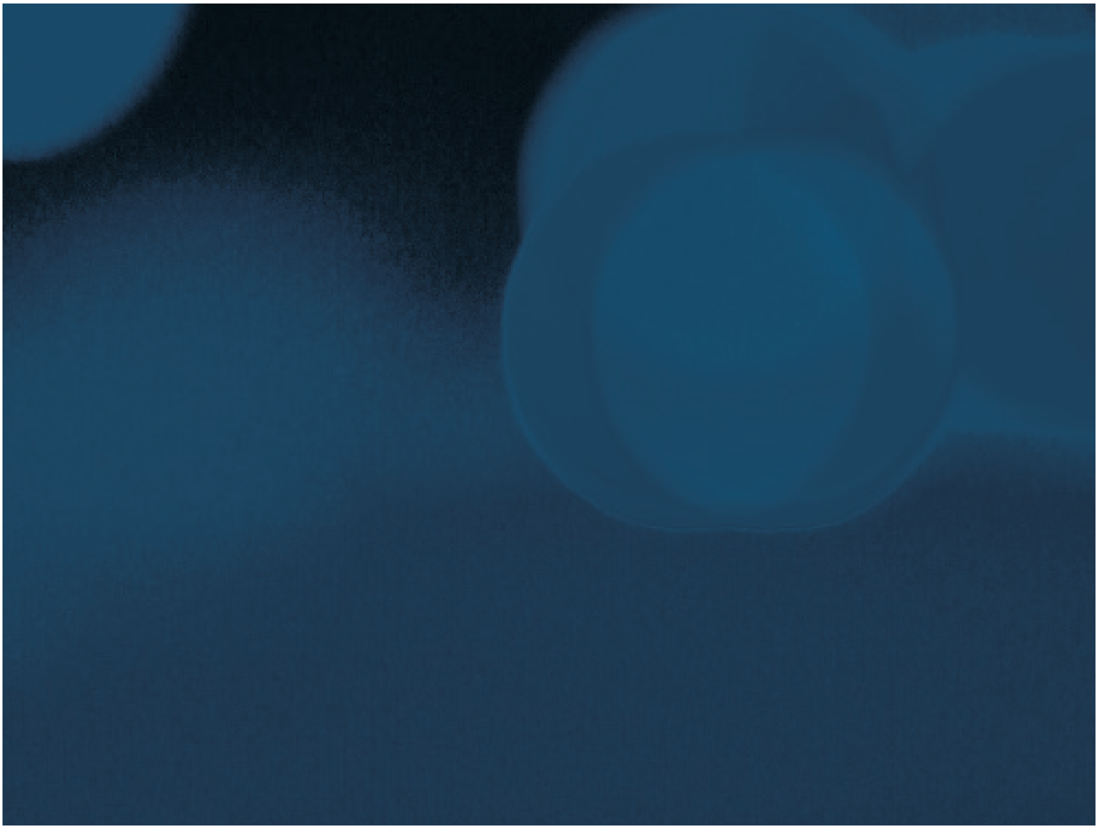
SUPO

Översikt av den nationella säkerheten 2025



DEN GLOBALA SÄKERHETSMILJÖN OCH FINLAND

SPIONAGE OCH PÅVERKAN

TERRORISM

SKYDDSPOLISENS ÅR

Det dystra säkerhetsläget satte underrättelseverksamheten i fokus inom utrikes- och säkerhetspolitiken

Juha Martelius
Chef för Skyddspolisen

Staten och den nationella säkerheten står åter i centrum för politiken. I dessa tider av dystra tongångar inom stormaktskonkurrensen och mellanstatlig polarisering har säkerhets- och underrättelsetjänsterna fått en allt större roll inom utrikes- och säkerhetspolitiken.

Också i Finland har underrättelseinformationens ökande betydelse lyfts fram i statsrådets utrikes- och säkerhetspolitiska redogörelse från i somras. Det är viktigt för statsledningen att veta vad motparten planerar och att förstå utvecklingen i den säkerhetspolitiska miljön. Samtidigt måste man också veta vad som inte är påverkan från motpartens sida, utan exempelvis felaktiga antaganden och spekulationer som uppstår i den offentliga debatten. Den informationen finns vanligen inte att få i offentliga källor. Skyddspolisen utnyttjar fullt ut de metoder som underrättelselagstiftningen medger för att inhämta information om utvecklingsförlopp som hotar vår nationella säkerhet.

I lägesbilden för både underrättelseinhämtning och bredspektrig påverkan har de proxyaktörer som olika stater använder fått en allt större roll. Statliga aktörer försöker sopa igen spåren efter sig genom mellanhänder, oavsett om det är fråga om Ryssland, Kina eller Iran. Med hjälp av proxyaktörer vill kraftmyndigheterna i diktatoriska länderna fördunkla verkligheten, göra det lättare att bestrida handlingar och skapa en ny typ av osäkerhet. Rekryteringen kan skötas i sociala medier och betalningen med kryptovalutor. Den som utför ett uppdrag vet inte nödvändigtvis själv för vems räkning han eller hon agerar.

Ett exempel på användning av proxyaktörer är den ryska sabotageverksamheten i Europa. Den har fått allt farligare former och visar likgiltighet för utomstående offer. Skalan är bred och inbegriper allt från mycket komplexa cyberattacker till enkel förstörelse. Huvudmålet är att få västländernas stöd till Ukraina att vackla.

Finland har tills vidare inte varit föremål för kraftig påverkan från Rysslands sida, utan påverkansarbetet har framför allt riktats mot stora EU-länder, men samtidigt också mot länder som exempelvis har en stor rysk minoritet eller proryska partier.

Mediebilden och därmed också allmänhetens bild av rysk påverkan motsvarar inte alltid verkligheten, utan till exempel vanlig inhemsk vandalism antas vara utförd av Ryssland. Detta passar Ryssland väl, eftersom det ökar den ryska avskräckningen och skapar en bild av att landet har oinskränkt makt.

Genom sina påverkansåtgärder testar Ryssland ständigt väst och Nato samt ger akt på deras reaktioner och resiliens. Ryssland förstår sig dåligt på väst och Finland, exempelvis överrumplades den ryska ledningen av Finlands anslutning till Nato. Förståelsen för logiken i Finlands agerande kan eventuellt försämras ytterligare och samtidigt finns det en ovilja att föra oönskade nyheter till den högsta ledningen. Detta kan medföra en risk för missförstånd, och då kan Ryssland reagera utifrån sina egna misstolkningar.

Påverkan sker alltmer i en gråzon och det kräver också alltmer underrättelseinhämtning. Skyddspolisens målsättning är att ge statsledningen en förvarning om rysk icke-militär påverkan. Också myndigheterna använder Skyddspolisens underrättelseinformation för att effektivt avvärja de mest allvarliga hoten, såsom terrorism.

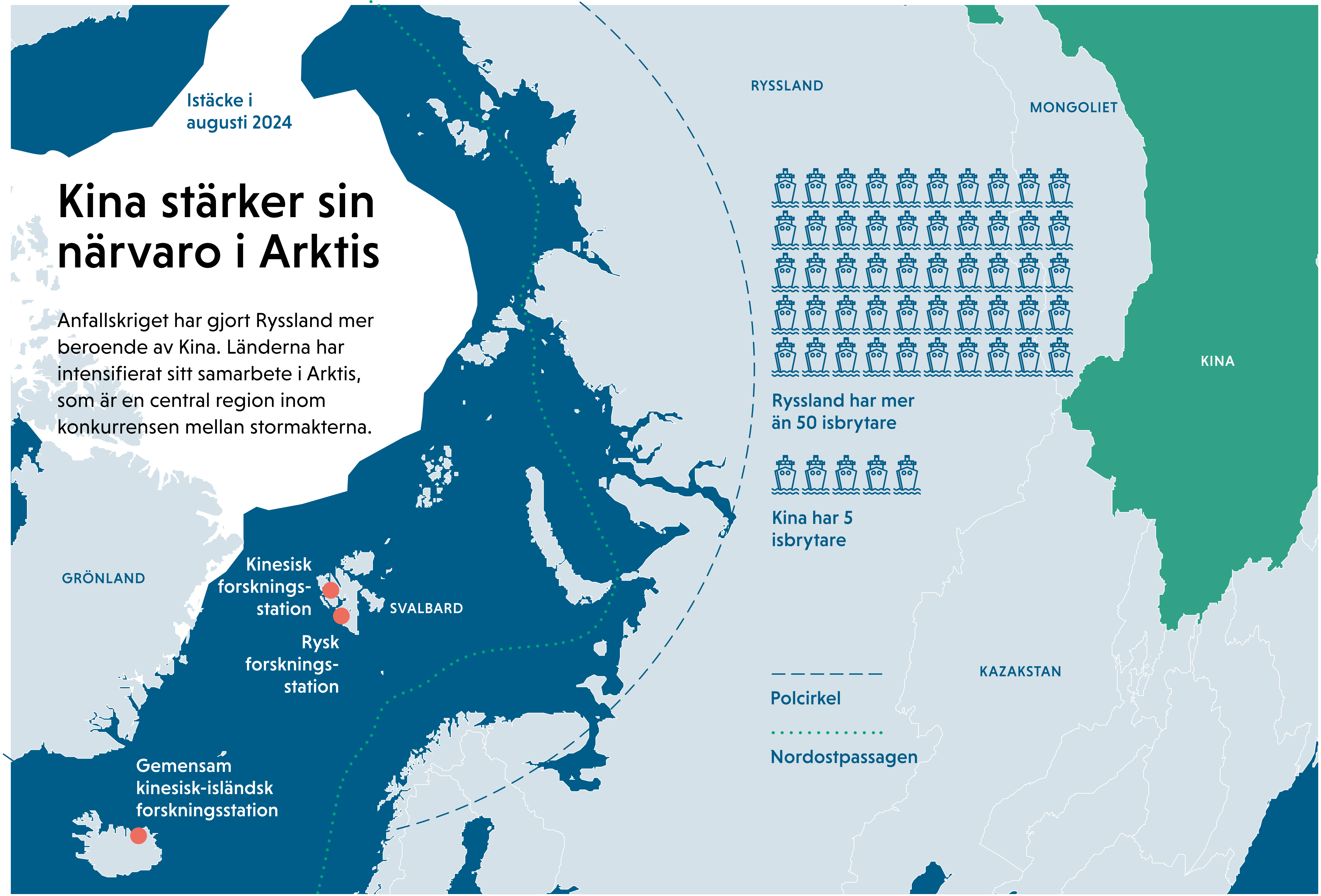
De regler som gäller i underrättelsevärlden kräver extremt förtroende för varandra, och därför kan endast likasinnade underrättelsetjänster delta i det internationella informationsutbytet. I detta avseende är underrättelsetjänsterna oersättliga verktyg för nationalstaterna. Om Skyddspolisen och den militära underrättelseverksamheten inte har tillräckliga resurser för att delta i samarbetet med sina utländska partner, är dessa dörrar helt stängda för Finland.

Det står klart att i synnerhet Ryssland har förändrat säkerheten i vår omvärld på ett betydande sätt. Och ingen utveckling mot det bättre är i sikte. Ryssland är en aggressiv stat med expansiva ambitioner, och det är berett att använda alla medel för att nå sina politiska mål. Rysslands alltmer framträdande imperialism, historietolkningar utan faktabas och decennielånga manipulation av nationen att tro på Rysslands historiska mission förutsätter att vår underrättelseverksamhet är kompetent och stark och kan ge en första varning om eventuella åtgärder mot vårt land. ■

Den globala säkerhetsmiljön och Finland

Kina stärker sin närvaro i Arktis

Anfallskriget har gjort Ryssland mer beroende av Kina. Länderna har intensifierat sitt samarbete i Arktis, som är en central region inom konkurrensen mellan stormakterna.



Sanktioner som införts till följd av anfallskriget mot Ukraina har gjort Ryssland mer beroende av Kina. Det nya läget skapar förutsättningar för ett ännu närmare samarbete mellan Ryssland och Kina i den arktiska regionen. Kina har successivt kunnat stärka sin närvaro i regionen genom samarbetet med Ryssland. Ryssland har därför kommit att bli Kinas primära väg till Arktis.

Ländernas intensifierade samarbete i norr märks på många sätt. Rysslands och Kinas kustbevakningar patrullerade för första gången tillsammans i den arktiska regionen hösten 2024. Länderna har organiserat gemensamma militära övningar också i Finska viken.

Ryssland får också tekniskt stöd och investeringar från Kina för energiprojekt i Arktis. Ländernas arktiska forskningssamarbete har intensifierats.

Den allt hårdare konkurrensen mellan stormakterna i Arktis återspeglas i Finland

Den arktiska regionen är en av de centrala arenorna för stormaktskonkurrens. Kinas ökande närvaro i regionen kommer sannolikt att driva på konkurrensen ytterligare. Finland är en arktisk stat, så det är uppenbart att maktbalansen i regionen också påverkar oss.

Som underrättelsetjänst har Skyddspolisen till uppgift att inhämta information om sådana utvecklingsförlopp som påverkar Finlands nationella säkerhet på ett betydande sätt.

De allt tätare relationerna mellan Kina och Ryssland påverkar Finland på många sätt. Ryssland ser Nato som ett direkt hot mot sig självt. Också Kina motsätter sig alla militära allianser där Förenta staterna är med. Den arktiska regionen är betydelsefull när det gäller utveckling, användning, upptäckt och bekämpning av kärnvapen och kärnvapenbestyckade robotar.

Dessutom har risken ökat för att know-how och teknik från oss förs till Ryssland via Kina. Finland besitter mycken arktisk kompetens som är av intresse för Kina och Ryssland. Byggandet av isbrytare och andra isförstärkta fartyg är bara ett exempel på detta.

Arktis är en nyckelregion för exempelvis satellitteknik

Den arktiska regionens läge är väsentligt av säkerhets-, handels- och teknikrelaterade skäl. Det har redan länge varit känt att nya farleder öppnas när istäcket smälter och att även naturresurser såsom mineraler, gas och olja frigörs. Kina är en stormakt och vill därför vara med och utnyttja dessa möjligheter.

Den arktiska regionen är också viktig för satellittekniken, eftersom polarområdena är idealiska för satellitmarkstationer. Många militära och civila positionerings- och kommunikationssystem är beroende av satellitteknik.

Kina har velat inrätta satellitmarkstationer i de nordiska länderna. Finland och de andra nordiska länderna har förhållit sig kritiska till dessa planer. Finland har reagerat genom att införa tillståndsplikt för mark- och radarstationer. Tillståndsprövningen ska enligt den gällande lagstiftningen också ske med tanke på den nationella säkerheten.

Enligt kinesiskt tankesätt ska en stormakt också ha en flotta som kan operera var som helst, också i arktiska förhållanden. Kinas långsiktiga mål är att skaffa sig en självständig operativ förmåga i regionen. Därför har landet bland annat satsat på att utveckla sin isbrytarkapacitet.

Ryssland behöver Kina

Rysslands anfallskrig har haft en betydande inverkan på dynamiken i den arktiska regionen. Arktiska rådets arbete har stannat upp till följd av kriget. Den största förändringen har ändå skett i relationerna mellan Kina och Ryssland.

Så sent som för ett årtionde sedan var Ryssland mycket mer skeptiskt inställt till arktiskt samarbete med Kina, eftersom landet ville bevara sin egen maktposition i regionen. Även om Kina och Ryssland har samstämmiga mål och samarbetet har intensifierats de senaste åren hyser de fortfarande misstro mot varandra.

Kina har nu en bättre förhandlingsposition i samtalen om arktiskt samarbete med Ryssland än landet hade före anfallskriget. Den ryska krigsindustrin är mycket beroende av teknik från Kina. Ryssland importerar därför bland annat mikrochipp och olika komponenter från Kina. Också Rysslands ekonomiska beroende av Kina har ökat. Tack vare stöd från Kina kan Ryssland fortsätta sitt aggressiva agerande i Europa.

Men samtidigt får man heller inte underskatta Ryssland alltför mycket. I Arktis är Ryssland fortsatt den starkare aktören tack vare sin långa historia, även om landet får lov att tolerera Kina mer än tidigare. Det är beskrivande för situationen att Ryssland har mer än 50 isbrytare, medan Kina har fem.

Stärkt arktisk närvaro är en del av Kinas mer långtgående ambitioner

Kinas övergripande mål är en global militär närvaro, så dess intresse för Arktis ingår i landets mer långtgående ambitioner. Det viktigaste för Kina är stormaktskonkurrensen med Förenta staterna.

Kina drar nytta av att Ryssland blivit en närmare partner i fronten mot Förenta staterna. Kina arbetar för att stärka internationella strukturer som är oberoende av väst. Ett exempel på detta är det tätare samarbetet mellan Brics-länderna.

Även Ryssland har nytta av att de internationella strukturer som är oberoende av väst stärks, trots att de är klart Kinaledda.

Kina har ingen vilja att kraftigt utöva påtryckning på Ryssland och därmed äventyra de goda bilaterala förbindelserna. Ett stabilt Ryssland frigör kinesiska resurser för det viktigaste, dvs. stormaktskonkurrensen med Förenta staterna. Kina kan därför låta saker utvecklas av egen kraft och vänta på att Ryssland måste be landet om hjälp. ■

Ryssland positionerar sig på nytt globalt

Ryssland uppträder hotfullt gentemot Europa, men vill återupprätta handelsförbindelserna med de europeiska länderna. Att försvaga stödet till Ukraina och lindra sanktionerna är Rysslands globala huvudmål. Samtidigt riktar Ryssland blicken mot nya väderstreck.

Kriget i Ukraina har pågått i tre år, och det har tvingat Ryssland till en betydande internationell ompositionering. Ryssland uppträder självsäkert i sin utrikespolitik, men samtidigt står det klart att landet fått minskad tyngd globalt.

Förändringen har varit mest dramatisk inom relationerna mellan Ryssland och västländerna, som gjort en verklig djupdykning. Ryssland har genom sitt eget agerande avsevärt försämrat sina möjligheter att påverka västländerna.

När de sedvanliga påverkansmetoderna har mindre effekt har Rysslands agerande i Europa blivit mer aggressivt. Men samtidigt har västländerna sämre möjligheter att påverka Ryssland, eftersom väst nu känns alltmer avlägset för ryssarna.

En sådan konstellation ökar avsevärt risken för missförstånd och överdrifter. När de traditionella myndighetskontakterna har brutits så gott som helt, sker dialogen i allt större utsträckning via offentligheten. Behovet av underrättelseinformation ökar på båda hållen när tillgången till information via sedvanliga kanaler är dålig.

Ryssland riktar blicken österut och söderut

Ryssland är emellertid inte så isolerat från den övriga världen som det kan se ut sett från vår horisont i väst. Ryssland riktar nu huvudsakligen blicken mot Kina. Landet har i allt högre grad förbundit sig till Kina och dess utrikespolitiska mål. Det står klart att Kina är den starkare parten. Ryssland och Kina strävar efter att stärka de internationella strukturer där västländerna inte ingår.

Ryssland tittar i riktning mot det globala syd, dvs. Afrika, Asien och Sydamerika. Ett forum för detta är samarbetet mellan Brics-länderna. Ryssland undersöker möjligheter till handel i det globala syd, men försöker också öka sin politiska tyngd, vilket syns till exempel i satsningarna på diplomater.

Det är uppenbart att det globala syd inte kan ersätta Europa, dit en stor del av den ryska handeln tidigare riktade sig. Här kommer också logistiken med in i bilden – det går inte att bygga gasledningar i nya riktningar hur snabbt som helst.

Och inte heller i det globala syd är den ryska spelplanen helt enkel. Det militära företaget Wagnergruppen var tidigare en kanal för rysk påverkan i flera afrikanska länder. Efter det väpnade upproret sommaren 2023 har Rysslands försvarsministerium avvecklat Wagnergruppen. Den stela byråkratiska apparaten har inte haft förmåga att ersätta företaget, som var en påverkanskanal av smidigare typ. På detta sätt har Ryssland också förlorat inflytande i Afrika.

Trots högmod vill Ryssland ändå återupprätta handelsförbindelserna med Europa

Rysslands president **Vladimir Putin** har suttit vid makten längre än någon europeisk ledare, vilket ger honom en viss självsäkerhet. Den ryska ledningen behöver inte tänka i valcykler när den fattar beslut, så den tror sig kunna matta ut motparten i många frågor.

Ryssland vill framför allt försvaga stödet till Ukraina genom sitt påverkansarbete. Landet kan delvis sägas ha lyckats med detta, eftersom det har förmått skapa bromsar för västvärldens militära stöd. Men samtidigt har västländernas stöd till Ukraina fortsatt och fördjupats när kriget dragit ut på tiden.

Även om Ryssland uttrycker sig självsäkert och aggressivt har landet en önskan att återupprätta handelsförbindelserna med de europeiska länderna. Ett annat förstahandsmål för Ryssland är att sanktionerna ska avvecklas eller åtminstone lindras.

Rysslands strategi är att rikta budskapet i Europa till dem som vill återupprätta normala handelsförbindelser. I Finland har stödet till Ukraina varit mycket enhälligt, men i många andra europeiska länder är situationen inte lika klar. De ekonomiska argumenten står i fokus när Ryssland gör sina påverkansförsök.

I den ryska ledningens världsbild är västländerna inte absolut onda, utan delas in i det goda och det onda väst. Västvärldens ledare representerar den så kallade onda väst som försöker isolera Ryssland. Det goda väst består av det vanliga folket och dem som är beredda att fortsätta handeln med Ryssland. Ryssland värdesätter inte demokrati och förstår inte heller att den politiska ledningen i de europeiska länderna återspeglar folkets åsikter.

Det står klart att det inte finns någon återgång till det gamla i handelsrelationerna mellan Europa och Ryssland ur någondera partens synvinkel. Sett från Europa skulle ett återupprättat förtroende kräva en radikal och osannolik förändring i Ryssland. Ryssland å sin sida vill inte på nytt bli lika beroende av väst som landet var före kriget.

Små stater står inte i centrum för rysk påverkan

I Europa riktar Ryssland in sin påverkan framför allt på de stora länderna och naturligtvis Ukraina. Ryssland är inte allsmäktigt när det gäller att påverka, utan måste som krigförande land prioritera när det väljer handlingssätt. Små länder som Finland är inte de viktigaste föremålen för påverkan ur rysk synvinkel.

Ryssland ser sig självt som en stormakt vars huvudmotståndare är Förenta staterna. Men Ryssland upplever sig också vara hotat – och att det agerar enligt reciprocitetsprincipen också när landet enligt västländernas sätt att se på saken eskalerar situationen. Rysslands vill först och främst upprätthålla sin egen interna stabilitet.

Ryssland är det största hotet mot Finland, men ur Rysslands synvinkel är Finland inte lika väsentligt som omvänt. Ur rysk synvinkel är små länder som Finland en spelplan för de större staternas intressen. Ryssland ser framför sig en värld där små stater blir satellitstater till några få större stater som kan komma överens om saker utan att bry sig om de mindre staterna.

Samtidigt är Östersjön av stor betydelse för Ryssland. Skuggflottan i Östersjön är i dagsläget det ekonomiskt och logistiskt mest lönsamma alternativet för Ryssland att transportera olja sjövägen. Den ryska ekonomin har stor nytta av att använda skuggflotta för att kringgå sanktionerna mot råolja.

Det är uppenbart att relationen mellan Ryssland och Finland har förändrats i grunden. Ryssland anser Finland vara ett ovänligt land bland annat i och med Natomedlemskapet. Det upplever att Finland har svikit dess förtroende när Finland blev allierat med Förenta staterna.

Ryssland förbereder sig för ännu djupare motsättningar med västländerna och försöker upprätthålla redskap som landet kan tillgripa vid behov. Det rustar sig för många former av fientliga åtgärder mot västländerna, även Finland. Beredskapen är ändå inte ett bevis på beslut att omedelbart vidta sådana åtgärder. ■

Ryssland försöker allt oftare kringgå sanktionerna genom EU-interna leveranskedjor

Rysslands metoder att kringgå de införda sanktionerna och exportrestriktionerna är allt svårare att identifiera. När leveransrutterna blir alltmer komplexa kan företag omedvetet bidra till kringgåendet.

Ryssland försöker hela tiden hitta nya och mer diskreta metoder för att kringgå de sanktioner och exportrestriktioner som införts mot landet. Allt oftare skapar Ryssland leveranskedjor också på EU:s inre marknad.

Ryssland försöker allt effektivare dölja leveranskedjorna, eftersom myndigheter i väst allt bättre känner till hur landet kringgår sanktionerna och exportrestriktionerna. Med allt fler mellanhänder i leveranskedjorna blir det allt svårare för myndigheter och företag att veta vem de slutligen gör affärer med.

Att leveranskedjorna också når Europeiska unionens inre marknad innebär att någon kan ta kontakt med ett finländskt företag inom Finland eller EU. Företaget märker inte nödvändigtvis någon tydlig koppling till Ryssland eller något annat land utanför EU.

I leveranskedjorna ingår både enskilda företag och mer omfattande anskaffningsnätverk som Ryssland kan använda för att dölja att behövligt material styrs till landet.

Kedjor med upprinnelse på EU:s inre marknad fortsätter ofta med hjälp av en lång kedja av mellanhänder i tredjeländer utanför EU.

Effekterna av sanktionerna märks i Ryssland

Ryssland försöker kringgå sanktionerna och exportrestriktionerna för att skaffa sig produkter och teknik som landet behöver.

Finländska företag, universitet och forskningsinstitut besitter rikligt med internationellt erkänd kompetens och avancerad teknik. Rysslands anskaffningsförsök kan gälla såväl avancerad teknik som vanliga komponenter, såsom kretskort. Exempelvis olika elektroniska komponenter, mätinstrument, verktygsmaskiner, materialteknik, optik, sjöfartsteknik och kvantteknologisk know-how intresserar Ryssland.

Rysslands försöker också skaffa produkter med dubbla användningsområden, som omfattas av exportkontroll genom en EU-förordning. Med produkter med dubbla användningsområden avses teknik eller produkter som lämpar sig både för civila ändamål och för militära ändamål eller utveckling av massförstörelsevapen.

Sanktionerna och exportrestriktionerna mot Ryssland försvårar och fördröjer landets anskaffning av de berörda produkterna och gör dem också dyrare. Anskaffningarna är nödvändiga för Ryssland framför allt för att landet ska kunna upprätthålla sin militära kapacitet.

Det gäller att vara uppmärksam vid kontakter som avviker från det normala

När Rysslands leveransrutter blir alltmer komplexa och alltmer sammankopplade med EU:s inre marknad kan företag omedvetet bidra till att sanktioner och exportrestriktioner kringgås.

Företag bör därför fästa uppmärksamhet vid anskaffningsförsök eller kontakter som avviker från det normala. Det kan exempelvis röra sig om kontakttagande från ett nyligen bildat företag eller ett företag i ett land med obekant företagsklimat. Det kan vara fråga om en aktör som gjort affärer med Ryssland länge eller som gjort stora förändringar exempelvis i fråga om betalningsarrangemang vid export, import och anskaffning.

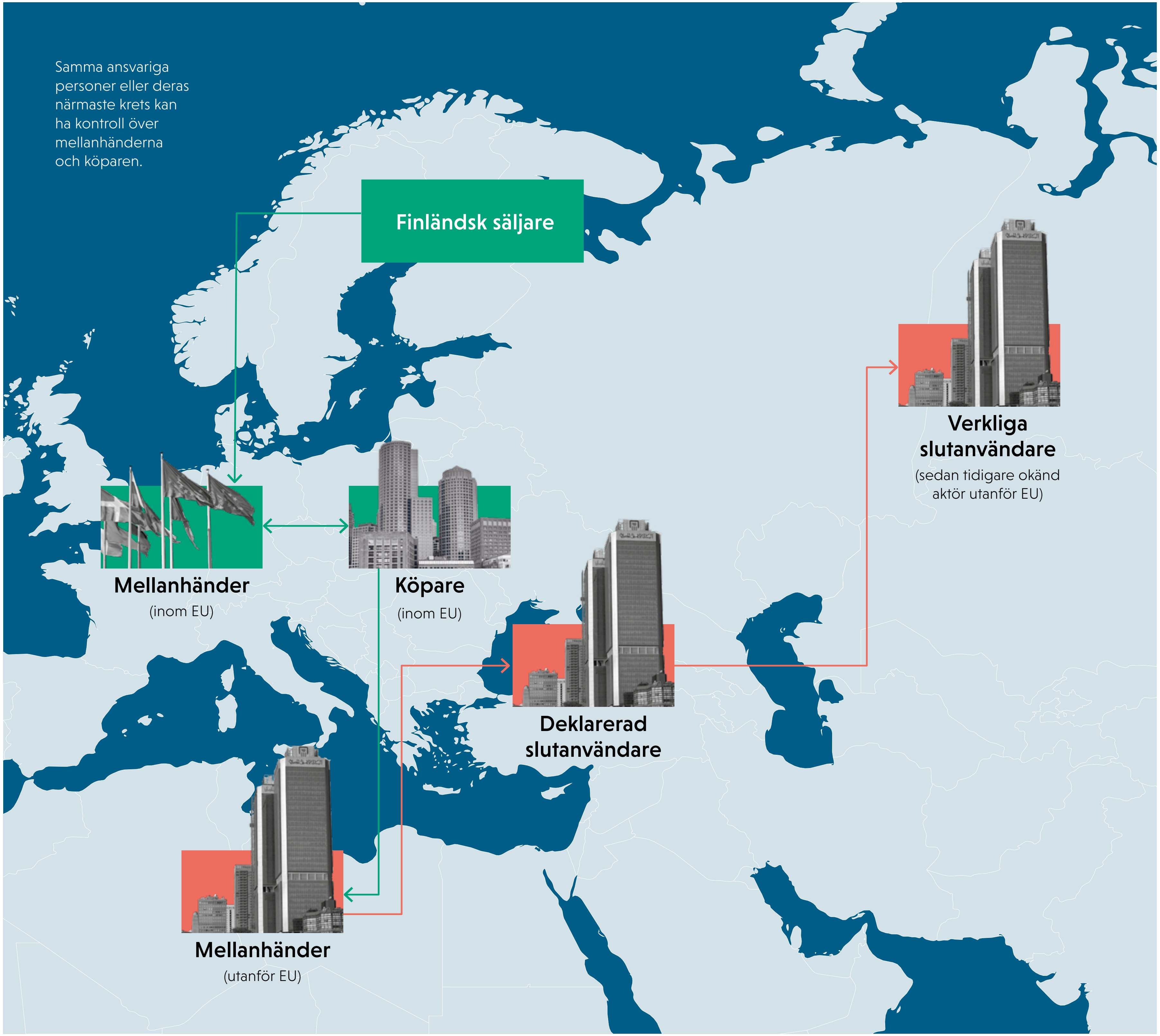
Företagen bör också vara alerta när det gäller affärspartner vars kommunikation sker endast via olika mellanhänder eller befullmäktigade företrädare för företaget. Det är också bra att vara försiktig när det gäller ovanliga betalningsarrangemang där köparen till exempel vill betala genom en tredje part eller via bankkonton i skatteparadis.

Genom effektiv avtalshantering och god kundkännedom kan företagen minska risken för att oavsiktligt bli en del av ett nätverk för kringgående av sanktioner eller exportrestriktioner.

Ryssland kringgår sanktioner för att kunna föra krig

Europeiska unionen och andra västländer har infört sanktioner som svar på Rysslands anfallskrig. Sanktionerna är utrikespolitiska åtgärder och ett av syftena är att försvaga Rysslands förmåga att fortsätta sin invasion av Ukraina. Sanktionerna gäller till exempel energi-, transport-, teknik- och försvarssektorerna. På senare tid har åtgärder också vidtagits för att förhindra att sanktionerna kringgås.

Ryssland försöker i synnerhet kringgå sanktionerna mot teknikimport och energiexport, eftersom de påverkar landets möjligheter att föra krig i Ukraina. Dessutom kommer landet sannolikt också i fortsättningen att försöka påverka EU-ländernas beslut om nya sanktioner och rikta motåtgärder mot de sanktioner som EU och andra västländer har infört.



Företagen ansvarar för att sanktionerna och exportrestriktionerna iakttas

Företagen måste veta vem de gör affärer med. De har det yttersta ansvaret för att förvissa sig om var de produkter de säljer slutligen hamnar.

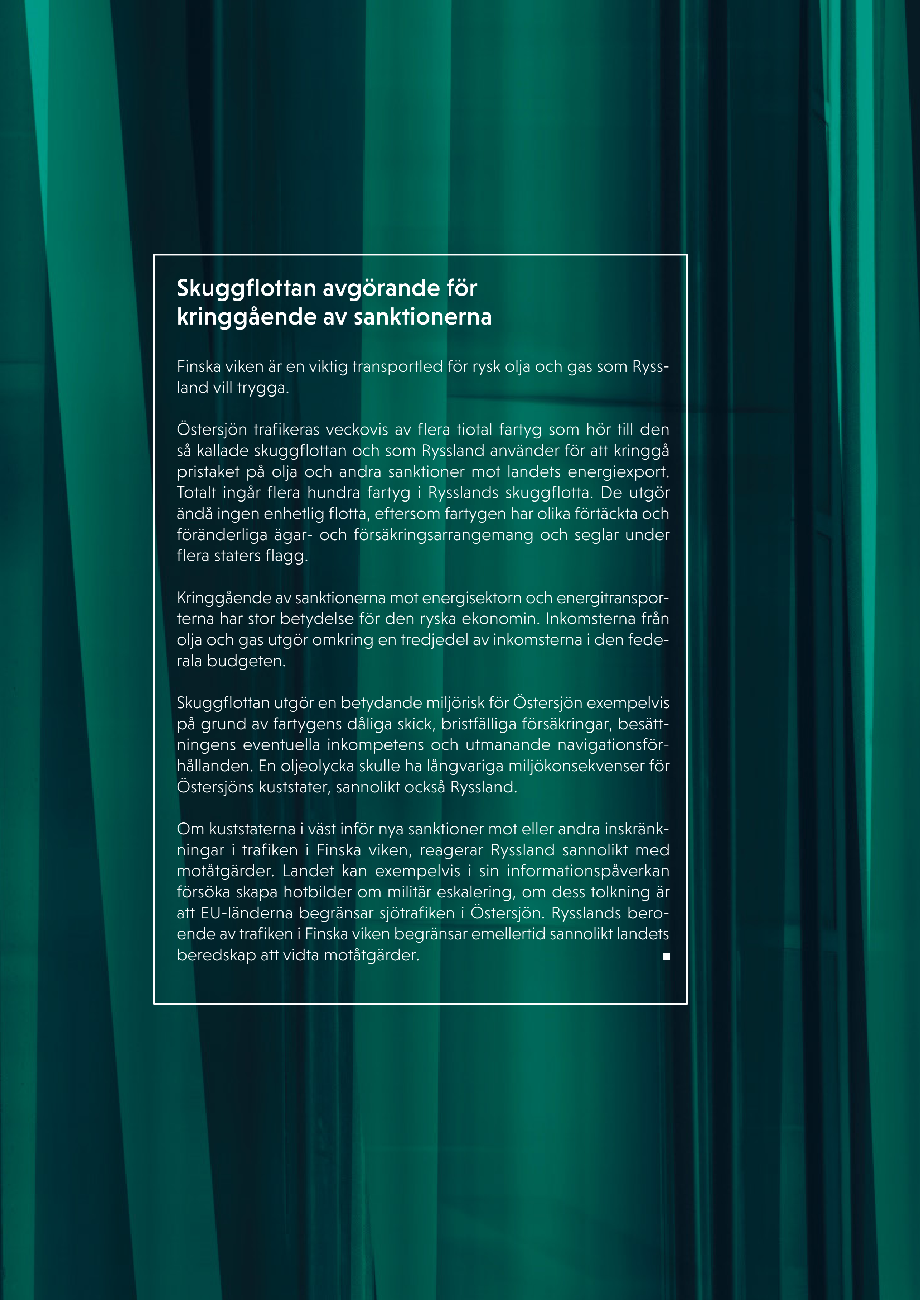
Företag och andra privata aktörer bör vara medvetna om riskerna med att kringgå sanktioner och exportrestriktioner. Företagsledningen har straffrättsligt ansvar för att EU:s sanktioner och exportrestriktioner iakttas. Affärer med aktörer som är föremål för sanktioner kan också inverka negativt på företagets egen affärsverksamhet och försvåra betalningar och finansiering.

Utöver straffrättsliga påföljder innebär involvering i kringgående av sanktioner och exportrestriktioner betydande skada för företagets anseende. Och skadan gäller inte nödvändigtvis bara företagets eget anseende. Den kan leda till skadat anseende också för samarbetspartner och kunder till företag som kringgår sanktioner eller exportrestriktioner.

I ärenden som gäller allmänna tullförfaranden och tullbrott kan företagen kontakta Tullen. I frågor som gäller sanktioner och deras tolkning samt exportrestriktioner och exporttillstånd för produkter med dubbla användningsområden ger utrikesministeriet råd.

Skyddspolisen har till uppgift att tillsammans med andra myndigheter övervaka att teknik eller produkter som omfattas av exportrestriktioner inte exporteras från eller via Finland. Företag och organisationer som kontaktas på ett misstänkt sätt kan kontakta Skyddspolisen via kontaktformuläret på vår webbplats.

→



Skuggflottan avgörande för kringgående av sanktionerna

Finska viken är en viktig transportled för rysk olja och gas som Ryssland vill trygga.

Östersjön trafikeras veckovis av flera tiotal fartyg som hör till den så kallade skuggflottan och som Ryssland använder för att kringgå pristaket på olja och andra sanktioner mot landets energiexport. Totalt ingår flera hundra fartyg i Rysslands skuggflotta. De utgör ändå ingen enhetlig flotta, eftersom fartygen har olika förtäckta och föränderliga ägar- och försäkringsarrangemang och seglar under flera staters flagg.

Kringgående av sanktionerna mot energisektorn och energitransporterna har stor betydelse för den ryska ekonomin. Inkomsterna från olja och gas utgör omkring en tredjedel av inkomsterna i den federala budgeten.

Skuggflottan utgör en betydande miljörisk för Östersjön exempelvis på grund av fartygens dåliga skick, bristfälliga försäkringar, besättningens eventuella inkompetens och utmanande navigationsförhållanden. En oljeolycka skulle ha långvariga miljökonsekvenser för Östersjöns kuststater, sannolikt också Ryssland.

Om kuststaterna i väst inför nya sanktioner mot eller andra inskränkningar i trafiken i Finska viken, reagerar Ryssland sannolikt med motåtgärder. Landet kan exempelvis i sin informationspåverkan försöka skapa hotbilder om militär eskalering, om dess tolkning är att EU-länderna begränsar sjötrafiken i Östersjön. Rysslands beroende av trafiken i Finska viken begränsar emellertid sannolikt landets beredskap att vidta motåtgärder. ■

Data kan också utnyttjas för ändamål som hotar Finland

Geopolitiken med sina nya risker berör också datahanteringen. Informationsdelningen måste allt oftare bedömas i förhållande till eventuella risker.

Det rådande ambitionen i Europa har varit att främja tillgången till data som producerats med offentliga medel. Att någon missbrukar data har varit en kvarstående risk – ett godtagbart pris för att vem som helst med hjälp av data ska kunna skapa smarta applikationer för att underlätta vardagen.

Inom den akademiska forskningen har traditionen med öppna data varit grunden för verksamheten. Det är tveklöst att den har tjänat både grundforskningen och den tillämpade forskningen mycket framgångsrikt.

När säkerheten i omvärlden förändras måste det i allt högre grad beaktas att data kan utnyttjas också för ändamål som allvarligt kan äventyra Finlands eller finländarnas säkerhet.

När beräkningskapaciteten ökar och AI-algoritmerna utvecklas har de auktoritära staternas metoder för att utnyttja och kombinera till synes harmlösa datamassor tagit ett stort steg framåt.

I Finland finns redan insikten att kommunikationen behöver skyddas mot risker förknippade med tillverkaren. Konkreta åtgärder har också vidtagits i fråga om allmän tillgång till positionsdata för kritisk infrastruktur. Allt oftare måste också delningen av annan information bedömas i förhållande till de risker som är förknippade med att informationen används. Det är uttryckligen fråga om riskbedömning. Det finns fortfarande mycket information som kan vara allmänt tillgänglig utan risk.

Biodata kan användas för att bota sjukdomar, men också för att skapa sådana

Ett exempel på en öppen datapolitik är biodata, dvs. hälso- och gendata. Finland är ett land med täckande och välorganiserade hälsodataregister där data funnits relativt allmänt tillgängliga för forskningsändamål. Forskning bedrivs ofta som internationellt akademiskt och kommersiellt samarbete, vilket innebär att man vant sig vid att dela data.

Delning av biodata har möjliggjort effektiva sätt att utveckla medicinen, men delningen är förknippad med en risk för att data missbrukas. I det nuvarande geopolitiska läget har risken för missbruk ökat enormt jämfört med tidigare.

I nuläget samlar exempelvis Kina aktivt in biodata från olika länder, samtidigt som landet inte delar sina egna. Också Ryssland har en lång tradition inom militärmedicin.

Enligt de allvarligaste scenarierna kan biodata missbrukas för att utveckla patogener och bedöma deras spridningseffekter inom en viss målgrupp. Genom att erbjuda biodata kan Finland oavsiktligt bidra till att sådana tillämpningar utvecklas. Genom att kombinera artificiell intelligens och bioinformatik snabbas all forskning upp på gott och ont. ■

Spionage och påverkan

Lägesbild över statligt spionage och statlig påverkan

Ryssland och Kina utgör det största underrättelsehotet mot Finland. Det har blivit svårare för Ryssland att bedriva personbaserad underrättelseinhämtning i Finland, men landets cyberverksamhet mot Finland har ökat. Kinas underrättelseintresse för Finland är långvarigt och kontinuerligt. Finland intresserar också vissa tredjeländer, såsom Iran, ur underrättelsesynpunkt.

Ryssland förhåller sig till Finland som ett ovänligt land

Ryssland är Finlands största underrättelse- och påverkanshot på kort och lång sikt. Av särskilt intresse för den ryska underrättelseverksamheten i Finland är det utrikes- och säkerhetspolitiska beslutsfattandet, såsom Finlands Natopolitik, och vår kritiska infrastruktur, militära försvarsförmåga och försvarsindustri. Ryssland försöker inhämta information i Finland med hjälp av såväl personbaserad underrättelseinhämtning som cyberunderrättelseinhämtning.

Påverkan har alltid hört till de ryska underrättelse- och säkerhetstjänsternas verksamhet, men dess objekt och aktivitet har varierat beroende på det världspolitiska läget. Rysslands är i underrättelsehänseende särskilt intresserat av sina Natoanslutna gränsgrannar. När relationerna mellan Ryssland och västländerna har svalnat har Rysslands påverkansarbete tagit ett steg i allvarligare riktning. Landets sabotageverksamhet i Europa kan ses som ett exempel på detta.

I Finland har de ryska underrättelsetjänsterna utnyttjat traditionella påverkansmetoder, såsom informationspåverkan eller kontakter med politiska beslutsfattare och journalister. Ryssland utnyttjar olika informationspåverkare för att stärka narrativen mot västländerna och Finland och för att förvränga historien.

Ryssland försöker påverka ryskspråkiga utomlands bland annat genom ”landsmannapolitik” och exempelvis genom traditionella och sociala medier som den rysktalande befolkningen följer samt snabbmeddelandetjänster. Sådana påverkansförsök är heller inte uteslutna i Finland, men Rysslands möjligheter att påverka den ryskspråkiga befolkningsdelen i Finland är begränsade.

Numera förhåller sig Ryssland till Finland som ett ovänligt land, så också finländarna måste bereda sig på aktivare och fientligare påverkan än tidigare. Ryssland är emellertid ett krigförande land vars huvudfokus ligger på annat håll än Finland.

Den ryska cyberunderrättelseinhämtningen i Finland har ökat och blivit mer fokuserad

De ryska underrättelsetjänsternas verksamhet mot Finland i cybermiljön har varit mycket aktiv redan i flera år, men de senaste åren har den ökat och blivit mer fokuserad. Denna cyberverksamhet gäller huvudsakligen statsförvaltningen och utrikes- och säkerhetspolitiken.

Cyberspionage erbjuder en kostnadseffektiv kanal för informationsinhämtning som flerfaldigas och är oberoende av tid och plats. Ryssland utnyttjar Finland också som transitland för cyberunderrättelser, dvs. ryska underrättelsetjänster använder regelbundet it-infrastrukturen i Finland vid cyberoperationer mot tredjeländer.

Riskerna för direkta och indirekta konsekvenser av rysk cyberverksamhet har ökat. I sitt krig mot Ukraina använder Ryssland aktivt cyberpåverkan för att störa och lamslå det ukrainska samhället. Det är emellertid inte enkelt att rikta in cyberpåverkan i en digitaliserad värld. Därför är det nu mer sannolikt att cyberattacker och informationsoperationer oavsiktligt riktas mot Finland eller andra utomstående stater.

Ett mer synligt fenomen under det gångna året har varit överbelastningsattackerna från proryska hacktivistgrupper mot Finland och andra västländer. Hacktivisternas verksamhet efterliknar annan cyberpåverkan i Rysslands intresse och är åtminstone sanktionerad eller till och med ledd av ryska staten.

Ryssland har redan i flera år erbjudit cyberkriminella grupper och hacktivistgrupper gynnsamma verksamhetsförutsättningar inom vissa gränser, men på senare år har samordningen och samarbetet med grupperna eventuellt ökat. Genom att utnyttja proxyaktörer för cyberpåverkan kan Ryssland bestrida sin egen delaktighet.

Den senaste tidens överbelastningsattacker kan i synnerhet ses som en signal till medborgarna. De syftar framför allt till att skapa misstroende och avskräckning.

Det har blivit svårare för Ryssland att bedriva personbaserad underrättelseinhämtning i Finland

De ryska säkerhets- och underrättelsetjänsterna har traditionellt haft permanent närvaro både i Finland och i andra länder. De som arbetat för underrättelsetjänsterna har i huvudsak gjort det under diplomatisk täckmantel.

Den ryska underrättelsetjänstens närvaro i Finland och på annat håll i Europa har emellertid minskat betydligt i och med att underrättelseofficerare som arbetat under diplomatisk täckmantel utvisats som vedergällningsåtgärd mot anfallskriget. Andra bidragande orsaker är reserestriktionerna och att allt färre i Finland på grund av kriget vill ha ryska kontakter.

Det hot som rysk personbaserad underrättelseinhämtning utgör har dock inte minskat på lång sikt, eftersom Rysslands informationsbehov inte har försvunnit någonstans.

Omvärldsförändringarna har även tvingat de ryska underrättelse- och säkerhetstjänsterna att ändra strategi. Ryssland går alltmer in för att använda sig av mellanhänder och andra täckmantlar än diplomatin. De kommer varken snabbt eller i stor skala att ersätta nyttan med diplomattäckmantel. Ryssland försöker även fortsatt att placera ut underrättelseofficerare som diplomater.

De ryska underrättelseaktörerna är i allt större utsträckning tvungna att bedriva sin verksamhet från Ryssland. Underrättelseinhämtningen kan gälla bosatta i Finland som uppehåller sig eller reser i Ryssland. I Ryssland kan också osakliga metoder förekomma.

Finland är föremål för kinesisk påverkan och underrättelseinhämtning

Kinas underrättelseintresse gentemot Finland är kontinuerligt och långvarigt. De kinesiska underrättelseaktiviteterna mot Finland består av personbaserad underrättelseinhämtning och cyberspionage. Stormaktskonkurrensen, västländernas ökande Kinakritik, exportrestriktionerna och den interna situationen i Kina påverkar vad som är föremål för landets intresse.

Den kinesiska underrättelseinhämtningen gäller utrikes- och säkerhetspolitiskt beslutsfattande, arktiska frågor, spetsteknik och grupper som den kine-

siska regeringen ser som ett hot. Också Natomedlemskapet och dess inverkan på Finlands inställning till Kina har ökat intresset för vårt land.

Kinas påverkansarbete är globalt och också Finland är föremål för det. Det bedrivs av flera organisationer med kopplingar till kinesiska staten och kommunistpartiet. Landets påverkansarbete och underrättelseinhämtning är ofta nära kopplade till varandra, och det försöker också bedriva påverkansarbetet i det fördolda.

Syftet med påverkansarbetet är också i Finland bland annat att styra det politiska beslutsfattandet och debatten om Kina i en riktning som motsvarar Kinas egna ändamål och att avstyra behandling av frågor som är oönskade ur Kinas synvinkel. Påverkansinsatserna riktas exempelvis mot politiska beslutsfattare, den allmänna opinionen och i Finland bosatta personer med kinesisk bakgrund.

Kina bedriver också flyktingspionage i Finland, dvs. samlar in information om, övervakar och försöker kontrollera sina tidigare och nuvarande medborgare som bor i Finland. Typfallet för flyktingspionage är en person som representerar en grupp som den kinesiska regeringen betraktar som ett hot mot sig själv. Sådana personer och deras närstående kan utsättas för trakasserier från de kinesiska myndigheternas sida.

Fokus för kinesiska cyberoperationer ligger framför allt på kritisk infrastruktur och utnyttjande av nätutrustning för konsumenter

Kina riktar cyberoperationer mot Finland och utnyttjar aktivt den finländska it-infrastrukturen i sina cyberoperationer mot tredjeländer. De kinesiska cyberoperationernas kapacitet och fokus har på senare tid i ökad utsträckning koncentrerats på kritisk infrastruktur i väst. Kina försöker skapa gynnsamma tillfällen till cyberpåverkan mot väst.

Det ökande underrättelsehotet om cyberpåverkan och mot kritisk infrastruktur i väst ökar hotet mot Finlands nationella säkerhet.

De kinesiska cyberhotsaktörerna utnyttjar i allt högre grad dåligt skyddade konsumentapparater. Vid systematiska intrång i dessa apparater och uppbyggnad av driftinfrastruktur används även i stor utsträckning kinesiska privata it-företag. Bakom förändringen ligger både en mindre risk för att åka fast och det stora antalet sårbara apparater. Allt fler konsumentapparater har internetuppkoppling, och särskilt oskyddade och icke-uppdaterade hemmaroutrar utgör nu en betydande risk för den nationella säkerheten.

Kina är ute efter spetskompetens och spetsteknik från utlandet

Kina vill vara internationellt ledande inom banbrytande nyckeltekniker, bland annat artificiell intelligens och kvantteknik. Kina försöker skaffa teknik från utlandet till stöd för landets egen ekonomiska utveckling bland annat genom att utnyttja investeringar, annat kommersiellt samarbete och forskningssamarbete.

Landet skaffar kompetens och teknik från utlandet också för militära ändamål. Flera tiotal universitet i Kina har kopplingar till landets väpnade styrkor, och landet använder också akademiskt samarbete i sina försök att lyckas locka till sig behövlig kompetens.

Förenta staternas exportrestriktioner i fråga om halvledare och deras tillverkningsteknik ökar Kinas behov av att skaffa information också genom underrättelseinhämtning. Också i Finland finns det rikligt med sådan teknisk kompetens som Kina är intresserat av.

Också vissa andra länder riktar spionage mot Finland

I underrättelsehänseende är Finland intressant i synnerhet för Ryssland och Kina, men också för vissa andra länder, såsom Iran. Auktoritära stater utövar ofta spionage och påverkan på personer som i sitt ursprungsland hör till den politiska oppositionen eller någon annan grupp som betraktas som hot av makthavarna. ■

Ryssland försöker påverka europeiska länder genom sabotage

Den ryska sabotageverksamheten har oftast kopplingar till den militära underrättelsetjänsten GRU. Syftet med skadegörelserna är att väcka rädsla och underminera västländernas stöd till Ukraina.

Flera europeiska länder har under de senaste två åren upplevt sabotage med kopplingar till rysk underrättelseverksamhet. Skadegörelse är ett sätt för Ryssland att bedriva påverkansarbete i Europa. Aktiviteten har riktats mot de stora europeiska länderna plus ett antal andra stater.

Rysslands möjligheter till inflytande i Europa försvagades märkbart efter det att landet inledde sitt storskaliga angrepp mot Ukraina 2022. Ryssland har traditionellt använt diplomatisk täckmantel för underrättelseinhämtning, men efter krigsutbrottet har västländerna utvisat ett stort antal underrättelseofficerare från ambassaderna.

Ryssland har tvingats ändra sätten att bedriva underrättelseverksamhet för att anpassa sig till det förändrade läget. Ryssland har gjort en omställning till krigssamhälle, vilket har återspeglats i landets sätt att agera också utanför Ukraina.

En aktivare sabotageverksamhet är en följd av denna utveckling. Verksamheten är i huvudsak kopplad till den ryska militära underrättelsetjänsten GRU. Den är en del av Rysslands försvarsmakt, så direkt agerande är mer typiskt för dess verksamhet än för landets andra huvudsakliga aktör inom underrättelseinhämtning som avser utländska förhållanden, den civila underrättelsetjänsten SVR. Den ryska federala säkerhetstjänsten FSB är för sin del till största delen verksam inom Rysslands gränser, trots att den också har befogenheter och även historik av verksamhet utomlands.

Sabotaget har antagit allvarligare former

Tidigare när ryska underrättelseorgan genomförde sabotage utomlands var det så gott som genomgående Rysslands egna utbildade underrättelseofficerare som gjorde det. Sabotageoperationerna var färre, men de var mer omsorgsfullt planerade och mer inriktade på strategiska mål. Exempel på detta är när GRU:s militära enhet 29155 försökte lönnmörda far och dotter Skripal i Storbritannien och sprängningen av ammunitionslagret i Tjeckien 2014.

Numera använder Ryssland mellanhänder för att åstadkomma förstörelse. Det rör sig exempelvis om brottslingar eller andra som är intresserade av ekonomisk vinning. De kan till exempel utföra mordbränder till och med mot en liten summa pengar utan att veta vem den ursprungliga uppdragsgivaren de facto är. Sådana proxyaktörer rekryteras vanligen i sociala medier och de är inte särskilt professionella.

Förstörelsearbetena har gällt enkla och lättillgängliga objekt som är symboliska eller av sekundär betydelse med tanke på det egentliga stödet till Ukraina, såsom köpcentrum eller andra svagt skyddade objekt. Också det militära stödet till Ukraina kan bli föremål för attack, till exempel tillverkning, transport eller lagring.

Rysslands sabotageverksamhet i Europa har dock fått allt farligare former. Landet visar genom sitt agerande likgiltighet till och med för utomstående offer. Något som vittnar om detta är rapporterna från tyska och brittiska myndigheter 2024 om självantändande paket inom godstrafiken.

Ryssland vill skapa rädsla

Syftet med ryska sabotage är att påverka den allmänna opinionen och medborgarnas säkerhetskänsla och att belasta myndigheterna. Målen i sig saknar större strategisk betydelse. Exempelvis skulle enskilda skadegörelser riktade mot det militära stödet inte ha någon betydande inverkan på frontläget i Ukraina.

Den eftersträvade effekten är mer psykologisk. Ryssland vill skapa ett hotläge där landet kan påverka beslut i väst. Eftersom det är GRU som ligger bakom verksamheten är också målen militära.

Det egentliga huvudmålet är att den allmänna opinionen i väst ska vända sig mot stödet till Ukraina.

Ryssland vill visa sin förmåga att agera också i väst och skapa sig ett framtida förhandlingsläge. Även om åtgärderna riktas mot strategiskt mindre viktiga objekt än tidigare har de fått större genomslag.

Det kan mycket väl hända att vi får se förändringar i de ryska underrättelsetjänsternas verksamhet i framtiden. När fallen av sabotage blir kända kan Ryssland komma på nya sätt att påverka. Landet agerar ofta opportunistiskt, det vill säga testar olika tillvägagångssätt och drar den nytta som går att dra.

Förändringarna i relationerna mellan Ryssland och väst påverkar också landets strategier. Om exempelvis förutsättningarna för rysk underrättelseverksamhet i väst blir bättre, kan Ryssland mycket väl åter börja prioritera mer klassiska metoder för underrättelseinhämtning i sin verksamhet. Det är först på längre sikt som vi märker om den nuvarande sabotageverksamheten blir landets vedertagna sätt att agera.

Finland är inte det viktigaste målet, men sabotage kan inte uteslutas

Finland är sannolikt inte ett särskilt väsentligt mål för Rysslands agerande med avseende på genomslag och beaktansvärdhet. Ur Rysslands synvinkel är Finland inte en sådan nyckelaktör som skulle kunna påverka besluten i väst.

Risken för sabotage är ändå verklig och måste tas på allvar även här. Finland har blivit ett ovänligt land ur Rysslands synvinkel och skärpt sina ståndpunkter i fråga om Ryssland. Skyddspolisen har redan en längre tid beaktat sabotagehotet i sina bedömningar.

Också i Finland är det mest sannolika målet för ryskstött sabotage aktörer med kopplingar till det materiella stödet till Ukraina, såsom försvarsindustrin. Rysk sabotageverksamhet utgör i dagsläget inget hot mot de kritiska tjänsterna.

→

Ryska underrättelse- och säkerhetstjänster

Den militära underrättelsetjänsten GRU
Den militära underrättelsetjänsten GRU är nyckelaktören för den ryska underrättelseverksamhetens utrikesoperationer. GRU utför både personbaserad underrättelseinhämtning och cyberunderrättelseinhämtning. GRU har blivit känt för sina specialoperationer, såsom lönnmord. GRU har också specialförband som har deltagit i krigshandlingar i Ukraina, Afghanistan och Georgien. GRU är underställt försvarsmakten i Ryssland.

Den federala säkerhetstjänsten FSB
FSB är den största aktören av de tre och det grundades för att fortsätta det sovjettida KGB:s arbete. Dess viktigaste uppgift är att upprätthålla den interna stabiliteten i Ryssland. FSB är huvudsakligen verksamt inom Ryssland, även om det har rätt att vara verksamt också utomlands. FSB:s uppdrag omfattar bland annat kontraspionage, underrättelseinhämtning och gränsbevakning. FSB är direkt underställt Rysslands president.

Utrikesunderrättelsetjänsten SVR
SVR är en traditionell underrättelsetjänst som grundades för att fortsätta KGB:s underrättelseverksamhet avseende utländska förhållanden. SVR bedriver underrättelseverksamhet utanför Rysslands gränser. Bland annat personbaserad underrättelseinhämtning under diplomatisk täckmantel hör till SVR:s specialiteter. Även SVR lyder direkt under presidenten. ■

De auktoritära staternas cyberekosystem hotar den internationella stabiliteten

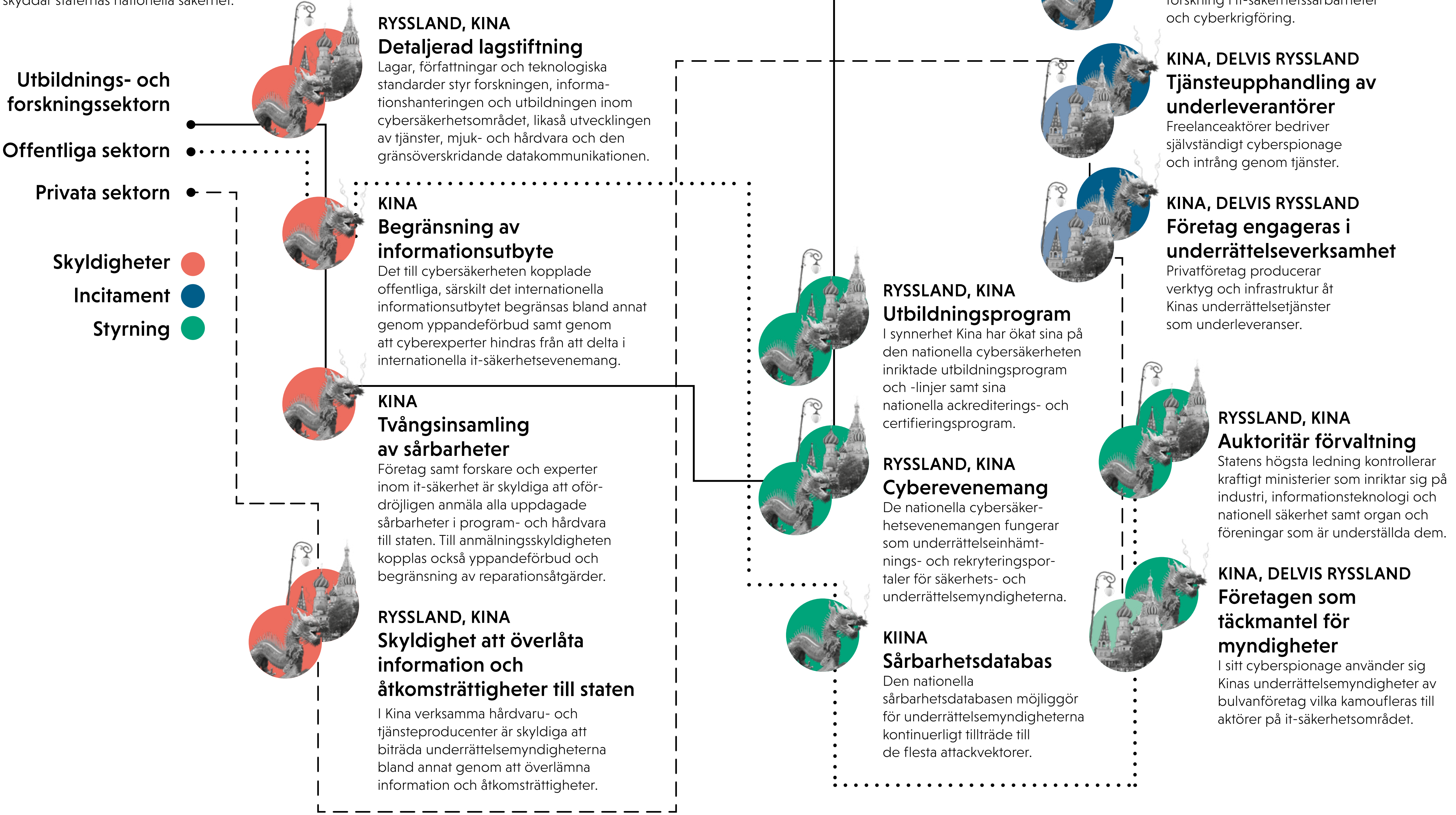
För att klara sig i cybervärlden som ständigt utvecklas behöver staterna förutom myndigheter även kompetensen hos akademiska institutioner, privatföretag och sakkunniga. Sammansmältningen av olika aktörers förmågor och färdigheter i invecklade nätverk kallas cyberekosystem. I auktoritära länder, såsom Ryssland och Kina, kan företag och forskare inom cyberområdet också bli indragna i det statliga spionage- och påverkansmaskineriet.

Cybervärlden har blivit en skådeplats för geopolitisk styrkeuppvisning. Världen digitaliseras snabbt och staterna har varit tvungna att koncentrera resurser på avvärjande cyberfunktioner. Starka cyberekosystem främjar på ett mera övergripande sätt staters nationella säkerhet och motståndskraft mot cyberhot. När de geopolitiska spänningarna ökar håller gränserna mellan avvärjande och offensiva kapaciteter och målsättningar dock på att suddas ut. Särskilt i auktoritära stater har utvecklingsarbetet på cyberområdet inriktats på att inlemma cybersäkerhetsresurserna som en del av underrättelse- och påverkansverksamheten i statlig regi. Samma kapaciteter används i auktoritära stater också för intern kontroll.

Både i Ryssland och Kina har de statliga förvaltningarna strävat efter att assimilera kompetensen hos cyberområdets företag och experter i sitt spionage- och påverkansmaskineri. Båda staterna har främjat detta bland annat genom att strama åt lagstiftningen, satsa på forskning och utbildning inom cyberområdet samt genom att öka den privata sektorns andel av tjänsteproduktionen. Särskilt Kina har utvecklat sina cyberekosystem i aldrig skådad omfattning.

Vad då för cyberekosystem?

Ingen kan ensam försvara staten i cybermiljön, utan här krävs samarbete mellan olika aktörer. Cyberekosystemen bildas av företag, underrättelse- och säkerhetsmyndigheter, stridskrafterna, forskningsinstitutioner, medier och andra organisationer som medverkar i skyddet av eller produktionen av tjänster för cybermiljön och som behövs för att skydda den nationella säkerheten i cybermiljön. Cyberekosystemen kopplar samman dessa olika aktörers resurser och färdigheter så att de på ett mer övergripande sätt skyddar staternas nationella säkerhet.



Utbildnings- och forskningssektorn

Offentliga sektorn

Privata sektorn

Skyldigheter ●

Incitament ●

Styrning ●

RYSSLAND, KINA

Detaljerad lagstiftning

Lagar, författningar och teknologiska standarder styr forskningen, informationshanteringen och utbildningen inom cybersäkerhetsområdet, likaså utvecklingen av tjänster, mjuk- och hårdvara och den gränsöverskridande datakommunikationen.

KINA

Begränsning av informationsutbyte

Det till cybersäkerheten kopplade offentliga, särskilt det internationella informationsutbytet begränsas bland annat genom yppandeförbud samt genom att cyberexperter hindras från att delta i internationella it-säkerhetsevenemang.

KINA

Tvångsinsamling av sårbarheter

Företag samt forskare och experter inom it-säkerhet är skyldiga att ofördröjligen anmäla alla uppdagade sårbarheter i program- och hårdvara till staten. Till anmälningsskyldigheten kopplas också yppandeförbud och begränsning av reparationsåtgärder.

RYSSLAND, KINA

Skyldighet att överlåta information och åtkomsträttigheter till staten

I Kina verksamma hårdvaru- och tjänsteproducenter är skyldiga att biträda underrättelsemyndigheterna bland annat genom att överlämna information och åtkomsträttigheter.

RYSSLAND, KINA

Utbildningsprogram

I synnerhet Kina har ökat sina på den nationella cybersäkerheten inriktade utbildningsprogram och -linjer samt sina nationella ackrediterings- och certifieringsprogram.

RYSSLAND, KINA

Cyberevenemang

De nationella cybersäkerhetsevenemangen fungerar som underrättelseinhämtnings- och rekryteringsportaler för säkerhets- och underrättelsemyndigheterna.

KIINA

Sårbarhetsdatabas

Den nationella sårbarhetsdatabasen möjliggör för underrättelsemyndigheterna kontinuerligt tillträde till de flesta attackvektorer.

RYSSLAND, KINA

Finansiering

Staten finansierar nationell forskning i it-säkerhetssårbarheter och cyberkrigföring.

KINA, DELVIS RYSSLAND

Tjänsteupphandling av underleverantörer

Freelanceaktörer bedriver självständigt cyberspionage och intrång genom tjänster.

KINA, DELVIS RYSSLAND

Företag engageras i underrättelseverksamhet

Privatföretag producerar verktyg och infrastruktur åt Kinas underrättelsetjänster som underleveranser.

RYSSLAND, KINA

Auktoritär förvaltning

Statens högsta ledning kontrollerar kraftigt ministerier som inriktar sig på industri, informationsteknologi och nationell säkerhet samt organ och föreningar som är underställda dem.

KINA, DELVIS RYSSLAND

Företagen som täckmantel för myndigheter

I sitt cyberspionage använder sig Kinas underrättelsemyndigheter av bulvanföretag vilka kamoufleras till aktörer på it-säkerhetsområdet.

Analys

För Ryssland är cybermiljön en spelplan för moderna konflikter

Rysslands cyberekosystem förenar traditionell propaganda med modern teknologi.

Rysslands inställning till cybermiljön är tudelad. Å ena sidan är cybermiljön en påverkansplattform som hotar statens interna stabilitet, kultur, värden och nationella identitet, varför landet vill minska sitt beroende av västerländsk teknologi. Ryssland vill begränsa sina medborgares tillträde till det fria internet men också begränsa västländernas möjlighet att spionera eller inverka på Rysslands system. Samtidigt använder Ryssland aktivt cybermiljön som ett medel för att nå sina statliga intressen, och sörjer för att den utanför Ryssland riktade cyberkriminaliteten blomstrar i landet.

Ryssland ser informationsmiljön som en spelplan för konflikter. Den här tanken har väglett Ryssland att i landet målmedvetet organisera cyberekosystem, där staten får stöd av det övriga samhället för sina cyberfunktioner. I kärnan av Rysslands cyberekosystem sitter den högsta statsledningen och säkerhets- och underrättelsetjänsterna som svarar för den strategiska planeringen, prioriteringen och inarbetandet av de nationella cyberresurserna. Ryssland har i själva verket lyckats skapa ett system som förenar traditionell propaganda och modern teknologi.

Det anpassbara cyberekosystemet har prövats i praktiken

Ryssland har byggt upp sitt cyberekosystem på många områden. Landet har satsat på utbildning av experter på cybersäkerhetsområdet i både högskolor och i säkerhetsmyndigheternas egna utbildningsprogram. De akademiska institutionerna stöder den statliga cyberverksamheten också genom utbildning och expertis.

Ryssland har också investerat i de nationella cybersäkerhets-, informations- kommunikations- och teknologiområdena och genom lagstiftning förbättrat sina möjligheter att i sin underrättelse- och påverkansverksamhet utnyttja den know-how som aktörer inom den privata sektorn besitter. De statliga och statsstödda medieorganisationerna sprider narrativ i enlighet med Rysslands intressen. Också de strängt reglerade nationella teknologi- och kommunikationsplattformarna ger möjlighet till övervakning och kontroll av informationsflödena.

Föreningen av dessa olika kapaciteter gör Rysslands cyberekosystem till en flexibel helhet som landets säkerhetsmyndigheter konkret har utnyttjat både för krigsoperationer i Ukraina och för påverkan och spionage riktade mot västländerna. Ryssland har genom sin cyberverksamhet strävat efter att skaffa utrikes- och säkerhetspolitisk information men också information som man senare utnyttjat som medel för påverkan.

Dessutom har Rysslands säkerhetsmyndigheter genomfört talrika cybersabotageoperationer, genom vilka man velat störa samhällslivet i Ukraina. Gemensamt för dessa verksamheter är att man vill uppamma rädsla, osäkerhet och misstro och därigenom försvaga den nationella och internationella samhörigheten i länder och olika allianser som från Rysslands synpunkt klassas som ”ovänliga”.

Ryssland vill isolera sig från det västerländska internet

Ryssland ser den fortlöpande kontrollen av informationsflödet som en viktig kugge när det gäller att bevara landets digitala suveränitet. Landets administration upplever att det nationella informationsflödet måste skyddas mot yttre påverkan. Officiellt har Ryssland uppställt som mål att bekämpa fientlig utländsk verksamhet och främja Rysslands kultur och värden, men i verkligheten är fri tillgång till information också ett allvarligt hot mot det auktoritära förvaltningssystemet.

Ryssland har velat hindra vanliga ryssar att få tillgång till västerländska nyhetssajter, och samtidigt har flera ryska myndigheters webbsidor stängts för västerländska användare. Ryssland har också målmedvetet strävat efter att frigöra sig från de västerländska datanätens planeringsprinciper, såsom datasäkert realiserade krypteringssystem.

Som ett led i sin målsättning att utöva hårdare statlig kontroll av internet har Ryssland också långsiktigt utvecklat nationella alternativ till datanät, lagring av information och kommunikation. Genom att ersätta utlandsproducerade tjänster med inhemska lösningar försöker Ryssland kontrollera den del av internet som fysiskt befinner sig inom den ryska statens gränser eller till vilken Rysslands rättsliga befogenhet sträcker sig.

Ryssland möjliggör avsiktligt cyberkriminalitet

Ryssland har också redan i åratal erbjudit gynnsamma förutsättningar för kriminell cyberverksamhet, under förutsättning att verksamheten riktas utanför Ryssland och den inte står i strid med Rysslands nationella eller utrikespolitiska intressen. Till de cyberkriminellas handlingssätt har hört exempelvis attacker som genomförts med hjälp av utpressningsprogram, av vilka också Finland fått sin beskärda del.

Denna samlevnad mellan förvaltningen, de cyberkriminella och hacktivistgrupper har fått nya former när de geopolitiska spänningarna ökat särskilt efter att Ryssland startade sitt anfallskrig mot Ukraina. Överbelastningsattacker som genomförs av proryska så kallade hacktivister har regelmässigt riktats mot västländerna – inklusive Finland. Den ökande hacktivismen och cyberkriminaliteten speglar Rysslands intressen att försvaga västerländska medborgares förtroende för samhällets funktion, även om de inte i samtliga fall skulle styras av statliga aktörer. Den påverkan som sker via proxyaktörer ger Ryssland möjlighet att bestrida sin delaktighet.

Analys

Kina eftersträvar status som cyberstormakt

Kinas till omfånget exceptionella cyberekosystem utgör en betydande utmaning för västländerna.

Kinas cyberekosystem karakteriseras av sitt exceptionella omfång. Landet har utvecklat sin cyberkapacitet till en nivå där dess cyberresurser är mångfaldiga jämfört med flertalet västländer. Situationen är resultatet av ett långsiktigt arbete som redan pågått ett tiotal år, där landets informationsteknologi- och cybersäkerhetsområden har använts för att maximera statens cyberkapaciteter genom styrning och lagstiftning.

Kinas strävan efter att nå status som teknologisk stormakt har fungerat som ledstjärna för utvecklingen av landets cyberekosystem. Kina utnyttjar sina kapaciteter för politisk och ekonomisk påverkan och som medel för informationsinhämtning samt för intern och extern kontroll. Genom ekonomisk påverkan förbättrar Kina också sina egna möjligheter till cyberverksamhet utomlands men förbättrar genom sin cyberverksamhet samtidigt sina möjligheter till ekonomisk påverkan.

Omfånget hos Kinas cyberspionage har ökat betydligt under senare tid och lett till omfattande stölder av politiskt och ekonomiskt betydelsefulla data. Kinas cyberoperationer utvecklas fortlöpande, och de använder sig av alltmer avancerade metoder. Statens cyberoperationer inriktas inte längre på enbart informationsinhämtning utan siktar till att skapa förutsättningar för cyberpåverkan bland annat genom intrång i västerländsk kritisk infrastruktur.

Kinas satsningar på sitt cyberekosystem har lett till en grundlig omvälvning av cybersäkerhetsfältet och utgör nu ett betydande hot mot Finlands och de övriga västländernas nationella säkerhet och stabilitet. Västländerna möter en allt komplexare utmaning, där Kina om det så önskar på bred front och flexibelt kan sätta in alla sina cybersäkerhetsresurser för att nå sina ekonomiska, politiska och militära mål.

Kinas kommunistiska parti och underrättelsemyndigheter i kärnan av cyberekosystemet

I likhet med Ryssland och många andra länder har också Kina centraliserat regleringen och koordineringen av cyberområdet direkt under statsledningen. I Kina innebär detta att det kommunistiska partiet har en viktig roll i styrningen av cyberområdet. De till cyberförvaltningen knutna organen leder de nationella cyberstrategierna och försöker genom traditionell diplomati modifiera det internationella samfundets normer och standarder för cyberverksamhet så att de är mera förenliga med Kinas nationella intressen. Underrättelsemyndigheternas offensiva operationer kan styras direkt av statsledningen.

Dessutom styr lagar, författningar och teknologiska standarder i stor utsträckning utbildningen, forskningen och informationshanteringen inom cybersäkerhetsområdet, men ålägger också cyberområdets organisationer och privatpersoner att stöda underrättelse- och spionageverksamhet i linje med Kinas intressen. Utöver allt detta styr myndigheterna genom ekonomiska incitament privatföretagens utveckling av tjänster, mjuk- och hårdvara så att den svarar mot underrättelseverksamhetens behov.

Genom centraliserad styrning och lagstiftning har Kina varit i stånd att samla landets olika aktörer till ett unikt cyberekosystem runt ämbetsverken och underrättelsetjänsterna. Till exempel den privata sektorn främjar Kinas underrättelseverksamhet i rollen som underleverantör genom att producera för landets säkerhets- och underrättelseverksamhet lämpad cyberinfrastruktur och -verktyg.

Kina har dessutom lyckats skapa incitament för skapande av skadlig cyberverksamhet: privata underleverantörer genomför självständigt intrång och cyberspionage i enlighet med underrättelsemyndigheternas intressen. Också bulvanföretag som kamoufleras till aktörer på it-säkerhetsområdet har en framträdande plats i Kinas internationella cyberspionageoperationer.

Kinas cyberekosystem ger också landet ett potentiellt övertag i eventuella konfliktsituationer – ett mångsidigt nätverk av aktörer på cyberområdet kan snabbt producera cyberkapaciteter för aktuella behov men kan också erbjuda förebyggande eller avskräckande skydd mot verksamhet riktad mot Kina.

Kina integrerar utbildnings-, forsknings- och företagssektorn som en del av cyberverksamheten

Kinas cyberekosystem har starka kopplingar till utbildnings- och forskningssektorn. Kinesiska staten finansierar högskolornas och forskningsinstitutionernas forskning i it-säkerhetssårbarheter och cyberkrigföring. Kina samlar in sårbarhetsobservationer i en nationell sårbarhetsdatabas där de genast är tillgängliga för underrättelsetjänsterna.

Kina finansierar frikostigt studerande som reser till utländska universitet men förpliktar dem att efter studierna för en viss tid återvända till Kina. Samtidigt begränsar dock Kina kinesiska it-säkerhetsexperters möjligheter att delta i internationella it-säkerhetsevenemang och tävlingar där de skulle kunna redovisa de sårbarheter de funnit för en större publik. I stället har Kina satsat kraftigt på nationella it-säkerhetsevenemang som arrangeras i samarbete mellan statliga institutioner och aktörer inom den privata sektorn och fungerar som fora för kartläggning av teknologiska kapaciteter.

Kina använder utbildningssektorn för att ersätta cyberkompetensbrister som uppdagats i cybersäkerhetsstrategin genom att man ökar utbudet av utbildningsprogram och -linjer som inriktas på cybersäkerhet. Enskilda kinesiska högskolor har också direkt stött Kinas underrättelsemyndigheters cyberspionageverksamhet via internationell mål- och sårbarhetskartläggning och genom innovationer av cybermetoder, utvecklingsarbete och expertis. Både de nationella it-säkerhetsevenemangen och högskolorna fungerar som plattformar för rekrytering av arbetare för säkerhets- och underrättelsetjänsterna. ■

Kina utnyttjar sociala medieplattformar för underrättelseinhämtning

Risken för att underrättelseaktören ska åka fast är mindre vid rekrytering på distans via sociala medier än vid personliga möten. Det kan vara svårt att inse att kontakter på sociala medieplattformar har att göra med kinesisk underrättelseverksamhet.

Kinesiska underrättelseaktörer

Kina har flera statliga organisationer som är specialiserade på underrättelseverksamhet och påverkan

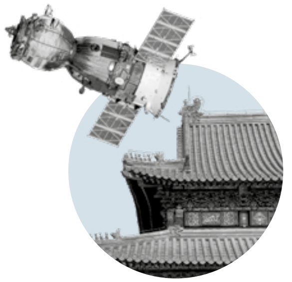
Kinas civila underrättelsetjänst MSS bedriver kontraspionage och underrättelseverksamhet, bland annat personbaserad underrättelseinhämtning och cyberunderrättelser som avser utländska förhållanden.

Kinas militära underrättelsetjänst MID

Kinas ministerium för allmän säkerhet MPS har ett centralt ansvar bland annat för den kinesiska polisen, brottsutredningen, kontraterrorn, gränskontrollen och invandringen, men bedriver också kontraspionage och utlandsoperationer.

Det kinesiska kommunistpartiets internationella avdelning IDCPC upprätthåller det kinesiska kommunistpartiets (KKP) relationer till politiska partier i andra länder, men samlar också in information om det politiska läget i andra länder och har som mål att främja en positiv bild av Kina bland beslutsfattare i andra länder.

Centrala avdelningen för enhetsfronten UFWD är ett organ som lyder under kommunistpartiet och som har det huvudsakliga samordningsansvaret för enhetsfrontens arbete. Målet med det arbetet är att främja det kinesiska kommunistpartiets intressen både i och utanför Kina bland annat genom att involvera personer med kinesisk bakgrund utanför Kina i påverkansarbete som främjar KKP:s intressen.



Kinesiska underrättelsetjänster använder aktivt olika sociala medieplattformar, såsom LinkedIn, för att rekrytera fysiska källor. Också finländare är intressanta för den kinesiska underrättelseverksamheten.

Det är både effektivt och ekonomiskt för de kinesiska underrättelsetjänsterna att rekrytera eller försöka rekrytera fysiska källor på sociala medieplattformar. På plattformar som LinkedIn är det lätt att välja ut och närma sig lämpliga personer.

Risken för att åka fast är mindre när man använder sociala medieplattformar än vid sådan personbaserad underrättelseinhämtning där man möts ansikte mot ansikte, eftersom aktören inte behöver lämna sitt hemland fysiskt. Det kan i synnerhet till en början vara svårt att bevisa att kontakterna har kopplingar till kinesisk underrättelseverksamhet.

Utöver rekryteringsverksamheten samlar underrättelsetjänsterna aktivt in information för olika användningsändamål från sociala medieplattformar.

Kontaktförsök är svåra att identifiera

En rekryteringsprocess på LinkedIn börjar vanligen så att en underrättelseofficer eller en person som handlar för dennes räkning tar kontakt med den utvalda personen i ett företags namn. Målpersonen kan bes skriva en rapport eller föra konsultationssamtal med den som tagit kontakt. Det kan röra sig om ett ämne som är av intresse för Kina, såsom politiska beslutsprocesser eller kompetens inom spetsteknik.

Den som ber om tjänsten går inte nödvändigtvis att koppla direkt till Kina. Personen kan exempelvis föreställa en representant för ett fiktivt eller existerande rekryterings- eller konsultföretag som till synes inte har några kopplingar till Kina.

Den information som begärs i initialskedet är ofta allmänt tillgänglig. Begäran kan också vara förenad med ersättning. Om den utvalda personen går med på begäran, kan personen senare bes om information om mer hemligt material. Det kan också hända att personen lockas att resa till Kina.

Om den som ursprungligen tog kontakt inte själv är underrättelseofficer, försöker personen i något skede överföra kontakten till den egentliga underrättelseofficeren.

Kontakta Skyddspolisen om du kontaktas på ett suspekt sätt

Underrättelseinhämtning och rekryteringsförsök bland annat på LinkedIn är en inarbetad strategi för kinesisk underrättelseinhämtning. Det lönar sig att förhålla sig skeptiskt till oväntade kontakter som avviker från det normala. Det är bra att i första hand ta upp saken med den egna organisationens säkerhetsansvariga.

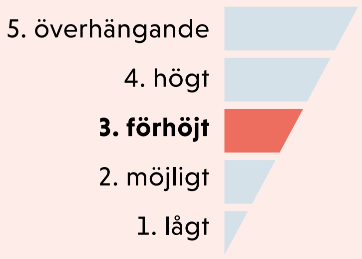
Vid suspekta rekryteringsförsök går det också att kontakta Skyddspolisen. Det lönar sig att ta kontakt även om en eventuell rekryteringsprocess redan har framskridit.

De kinesiska underrättelsetjänsterna kommer med största sannolikhet att fortsätta att vara aktiva på sociala medieplattformar också i framtiden. De kommer sannolikt att försöka utveckla ännu mer sofistikerade tillvägagångssätt så att det blir allt svårare att förknippa kontakterna med Kina. I framtiden kan kontakterna exempelvis kamoufleras som en jobbrekrytering. Även artificiell intelligens ger nya möjligheter att agera.

Om den som tagit kontakt i allt högre grad begär känslig information eller försöker locka målpersonen att resa till Kina, kan det vara fråga om kontakter med kopplingar till kinesiska underrättelsetjänster. ■

Terrorism

Nationell terrorhot-bedömning 2025



Skyddspolisen har tagit i bruk en ny femgradig skala för terrorhot. På den nya skalan ligger hotet om högerextrem och radikalislamistisk terrorism på nivå tre, dvs. förhöjt. Det mest sannolika terrorhotet utgörs fortfarande av enskilda individer och smågrupper som stöder en högerextrem eller radikalislamistisk ideologi.

På den nya skalan ligger hotet om högerextrem och radikalislamistisk terrorism på nivå tre, dvs. *förhöjt*. Detta är en svag ökning jämfört med den tidigare hotnivån. Under senare år har flera utvecklingstrender observerats i Finlands säkerhetsmiljö, vilka höjer terrorhotet.

Det mest sannolika terrorhotet utgörs fortfarande av enskilda individer eller smågrupper som stöder en högerextrem eller radikalislamistisk ideologi. I Finland finns personer som har vilja och förmåga att genomföra terrorattacker. Hotet från annan terrorism är lågt.

Också i Finland hämtar man troligen inspiration från terrorattacker i västländerna. I extremisternas propaganda framträder internationellt enskilda befolkningsgrupper, såsom etniska, religiösa och sexuella minoriteter samt myndigheter och politiska beslutsfattare. De eskalerande konflikterna i Mellanöstern har aktiverat olika extremistgrupper i Europa, vilket inverkar på hotnivån också i Finland.

Radikalisering på sociala medier för unga är en central internationell trend. Det avspeglas också i Finland i både de radikalislamistiska och högerextrema miljöerna. Radikalisering av unga kommer de närmaste åren sannolikt att synas också bland kontraterrorismens målpersoner. I radikaliseringen av unga kan man observera ett uttalat allmänt intresse för våld, och unga radikaliseras snabbare än tidigare.

Webben är central i extremhögerns verksamhet

Antalet målpersoner för bekämpning av högerextrem terrorism har ökat i Finland på 2020-talet. Högerextrema terrorister är intresserade av skjutvapen och sprängmedel, men också enkla redskap såsom eggvapen används. De sannolikaste attackmålen är etniska, religiösa och sexuella minoriteter samt aktörer vilka upplevs som ideologiska motståndare, såsom politiker och myndigheter.

Extremhögerns organiserade verksamhet utgör inte ett direkt terrorhot i Finland men kan vara en grogrund för radikalisering av enskilda individer och smågrupper och för ideologiskt motiverade våldsdåd. Inom extremhögern i Finland finns intresse för att skaffa skjutvapen och sprängmedel och utbilda sig i att använda dem. Intresset för vapen kan delvis förklaras av den från idévärlden härstammande tanken om att man måste bereda sig på samhällets kollaps.

Målpersonerna för högerextrem kontraterrorism är typiskt unga män som attraheras av våld, av vilka en del har mentalhygieniska problem och livshanteringsproblem. I den högerextrema retoriken accentueras hoten mot den vita befolkningsgruppen, beredskap för instabilitet och krigsliknande tillstånd i samhället, inspiration från attacker som fått stor mediesynlighet och glorifiering av terror på webben.

Webben är central i extremhögerns verksamhet. Finländare deltar aktivt i diskussioner som glorifierar våld. Bland deltagarna finns också minderåriga. Både i Finland och internationellt har flera planerade attacker kopplats till den webb-baserade Siege-kulturen, vars anhängare stöder omstörtning av den nuvarande samhällsordningen genom politiskt våld.

De internationella utvecklingstrenderna höjer hotet om radikal islamistisk terror i Finland

Radikalislamistiska terrorattacker utförs mest sannolikt med enkla redskap på offentliga platser. Den internationella radikalislamistiska propagandan uppmanar till våld särskilt mot aktörer vilka tolkas som fientligt inställda till islam. Attackuppmaningarna riktas mot mål som representerar kristendom, Israel och judendom samt mot sexuella minoriteter. Terroristorganisationer i konfliktområden försöker fortfarande genomföra och främja attacker i västländerna, men en omfattande attack i Finland är osannolik.

I Finland inriktas den radikalislamistiska verksamheten fortfarande huvudsakligen på stöd till den internationella terrorismen, innefattande spridning och produktion av propaganda, finansiering av terrorism och utbyggnad av stödnätverken. Under de sistlidna två åren har man kunnat observera

Varför ändrades hotnivåskalan?

Skyddspolisen angav åren 2017–2024 terrorhotnivån på en fyrgradig skala. Från år 2025 togs en femgradig skala i bruk. Med hotnivåskalan bedöms och kommuniceras hur högt hotet om en terrorattack i Finland eller mot finländska intressen utomlands är. Den nationella hotnivån för terrorism bestäms av det högsta hotet.

En femgradig skala är bättre ägnad än en fyrgradig för uppskattning och kommunicering av hotet.

”Under senare år har flera utvecklingstrender förekommit i Finlands säkerhetsmiljö, vilka höjer hotet om terrorism. Av denna orsak uppgår hotet på den nya femgradiga skalan till nivå 3, dvs. *förhöjt*. Det är viktigt för oss att exaktare än tidigare kunna beskriva även en sådan ökning av hotet”, säger Skyddspolisens specialforskare **Anna Santaholma**.

Också de andra nordiska länderna använder ett femgradigt system för bedömning av terrorhotnivån.

Skyddspolisen granskar fortlöpande hotnivån och publicerar en hotbedömning minst en gång om året.

internationella utvecklingstrender som höjer hotet om radikal islamistisk terror också mot Finland och finländska intressen.

Skändningarna av Koranen och i synnerhet de eskalerande konflikterna i Mellanöstern har fungerat som radikaliserande och mobiliserande faktorer i den radikalislamistiska verksamhetsmiljön i Europa. Ändringarna har visat sig bland annat som en ökning av antalet terrorattacker och ett större antal planerade och förhindrade attacker.

De nätverk som byggts upp i Europa med närområden av terroristorganisationen "Islamiska staten" (Isil) och dess afghanska provins (ISKP) har aktiverat sig. I gruppens internationella verksamhet framträder särskilt radikalislamister med ursprung i Centralasien och Kaukasus.

Centralkriminalpolisen (CKP) inledde i höstas en förundersökning gällande Isil om deltagande i en terroristgrupps verksamhet. CKP kom de misstänkta på spåren tack vare Skyddspolisens underrättelseinhämtning, och Skyddspolisen stöder också undersökningen med sin egen sakkunskap.

Globalt utgörs det mest betydande terrorhotet fortfarande av Isil och al-Qaida samt de grupper som svär dem trohet. De har utnyttjat symboliskt viktiga händelser i sin propaganda och intensifierat sina uppmaningar till attacker mot västländerna. Hotet från terroristorganisationerna är huvudsakligen riktat mot oroliga områden i Afrika, Mellanöstern och Sydasien, dit organisationerna också lockar utländska stridande.

I konfliktområdena i Irak och Syrien har Isil fortsatt sin terroristiska verksamhet och strävat efter att inspirera till, stöda och genomföra terrorattacker i Europa. Den radikalislamistiska Hayat Tahrir al-Shams (HTS) maktövertagande i Syrien och den därav följande instabiliteten ökar sannolikt möjligheterna för Isil att verka i området. De vidare verkningarna av förändringen i Syrien och utanför landet visar sig först på sikt.

Till Finland återvände år 2024 en person som rest från Finland till konfliktområdet i Syrien och Irak. I området finns fortfarande ca 50 personer som rest från Finland. De flesta är troligen döda, men på grund av de förhållanden som råder i området har dödsfallen inte kunnat bekräftas.

Hotet om annan terrorism är lågt

Hotet om annan terrorism i Finland är lågt. Extremvänsterns verksamhet i Finland är i huvudsak fredlig och inriktas på att stöda kurdaktörer och på radikal antifascism. Inom extremvänstern finns dock enskilda personer som är beredda att ta till våld. Våld förekommer i synnerhet i sammandrabbningar med extremhögerns demonstranter. Terroristorganisationen Kurdistans arbetarpartis (PKK) verksamhet i Finland fokuserar huvudsakligen på stödverksamhet.

I övriga europeiska länder har extremvänsterns attacker riktats mot företag och den offentliga sektorn. Typiskt riktas extremvänsterns terrorattacker i form av sabotage mot infrastruktur. Vid demonstrationer förekommer dock våld, vilket företrädesvis riktas mot aktörer vilka upplevs som fiender, såsom politiska motståndare och myndigheter. ■

Radikalisering av minderåriga har blivit ett permanent problem i Europa

Radikalisering av barn och unga hänför sig till både radikal islamistisk terror och högerextrem terror. Fenomenet förekommer också i Finland.

Minderårigas intresse för våldbejakande extremism och deras deltagande i terrorverksamhet har de senaste åren varit en växande trend i Europa. Både unga som stöder en radikal islamistisk ideologi och högerextrema unga har deltagit i verksamheten allt mer.

Nätet spelar en central roll när minderåriga radikaliseras oberoende av bakomliggande ideologi. Minderåriga deltar vanligen bland annat genom att ta fram, översätta och distribuera material med radikalt innehåll.

Det är också vanligare än tidigare att minderåriga deltar i våldshandlingar. Under de senaste åren har europeiska myndigheter avbrutit flera misstänkta attacker där minderåriga deltagit. Dessutom genomförde en minderårig person i fjol en terrorattack med radikalislamistiska förtecken i Europa.

Flera europeiska länder har uttryckt sin oro över radikalisering bland barn och unga. Det står klart att fenomenet har blivit ett långvarigt utvecklingsförlopp som också berör Finland. Här märks framför allt unga vuxna i detta sammanhang, men extremism har även visat sig väcka intresse bland minderåriga. Fenomenet har observerats alltmer på senare år.

Det är ytterst viktigt att myndigheterna samarbetar när radikaliseringen bland barn och unga ska bekämpas. Skyddspolisen har ordnat relevant utbildning exempelvis för kommunanställda inom sektorn för fostran.

Nätgemenskaper i fokus

Plattformarna för sociala medier har gjort att radikala ideologier, inklusive aktörer och gemenskaper, är lättare tillgängliga för unga på ett mer riskfritt sätt. Virtuella gemenskaper utgör en viktig kamratgrupp för dem som stöder eller är intresserade av extrema ideologier. Inom gruppen kan de egna åsikterna förstärkas och få acceptans.

Gemenskaperna använder sig av slutna meddelandeappar och diskussionsplattformar för att sprida propaganda, uppmana till attacker och ge incitament till våldsdåd. Det är i synnerhet små, slutna utbrytargrupper från större gemenskaper som uppmanar och uppmuntrar till handlingar utanför den virtuella miljön.

Både radikalislamistiska och högerextrema nätgemenskaper är internationella, men det finns också mer lokala eller språkspecifika gemenskaper. Också finländska ungdomar är medlemmar i dessa gemenskaper.

Nätet är i allmänhet inte den enda orsaken till radikalisering, utan det finns många bakomliggande faktorer som gör unga mottagliga för påverkan. Nätgemenskaperna och nätgrupperna erbjuder emellertid sådan social delaktighet som kan vara en starkt bidragande orsak till radikaliseringen. De som söker sig till gemenskaperna kan vara ute efter social acceptans eller en känsla av betydelse.

Det har observerats att den individuella radikaliseringsprocessen har förkortats allt eftersom nätaktivitet får ökad betydelse. I de mest oroväckande fallen blir individerna våldsbenägna snabbare än tidigare.

Barn och unga som exponeras för extremistiska tankegångar i sin närmaste krets är ett eget kapitel. De är genomsnittligt mer benägna att radikaliseras. Generationsövergripande radikalisering förekommer också i Finland både inom högerextremism och inom radikal islamism.

Populärkulturen utnyttjas för propaganda

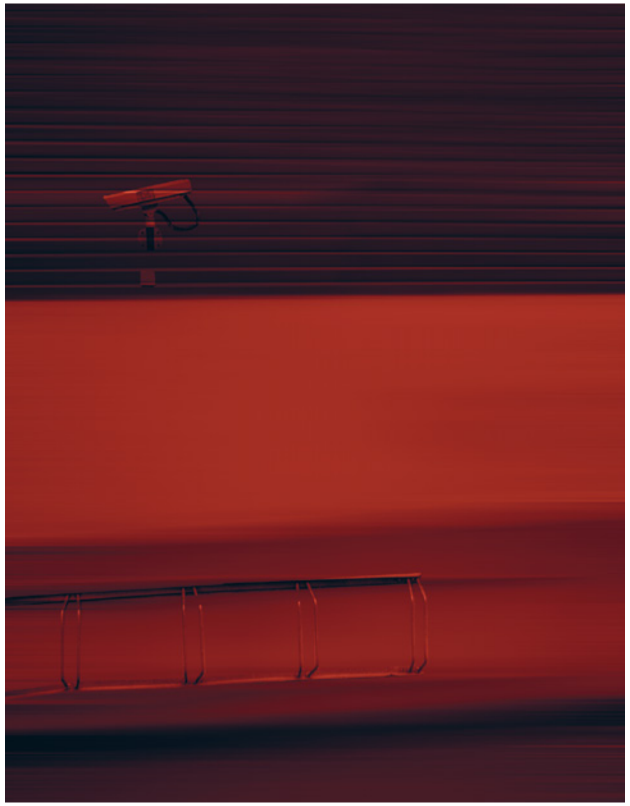
Radikala aktörer riktar sin propaganda till barn och unga, men minderåriga kan också själva aktivt producera innehåll för varandra och vuxna. I radikala nätgemenskaper kan barn föreställa äldre än de i själva verket är och även inta vuxenroller.

Propagandamakare plockar upp innehåll från populärkulturen och populära spel bland ungdomar. Både den radikalislamistiska och den högerextremistiska propagandan utnyttjar numera skickligt kortvideor, mems och spelifierat innehåll. På senare år har de enskilda oberoende aktörernas betydelse för produktionen av propaganda accentuerats.

Det vanliga är att man bygger upp sin egen världsbild genom att kombinera tankar från olika ideologier. ■

Fler observationer kopplade till radikal högerextremism i samband med säkerhetsutredningar

Det ligger flera orsaker bakom det ökade antalet observationer. Inga klara indikationer finns på att högerextrema aktörer systematiskt skulle söka sig till vissa branscher.



Antalet säkerhetsutredningar som Skyddspolisen gör har ökat betydligt. År 2019 gjordes knappa 70 000 säkerhetsutredningar. År 2024 steg antalet utredningar för första gången till mer än etthundra tusen.

Antalet observationer som kan förknippas med organiserad eller terrorkopplad extremhöger, såsom den genom domstolsbeslut förbjudna Nordiska motståndsrörelsen, har ökat bland Skyddspolisens säkerhetsutredningar på senare år. De är sex gånger fler än 2019. Någon direkt slutsats om att extremhögern blivit mer aktiv kan inte dras av detta, även om det är en av de förklarande faktorerna. En bidragande orsak till ökningen är att det allokerats mer resurser till övervakning.

Skyddspolisen har i flera år i sin terrorhotbedömning slagit fast att radikal islamism och extremhögern utgör det största terrorhotet i Finland. Extremism inbegriper många olika grader av allvarlighet, och terrorverksamhet är den allvarligaste och mest sällsynta formen.

Det mest sannolika hotet om terrorattentat utgörs av enskilda aktörer och smågrupper. Den organiserade extremhögern kan fungera som plattform för radikalisering av enskilda individer och smågrupper och öka risken för att de begår våldsdåd.

Det förekommer variation i hur pass starka de iakttagna kopplingarna till högerextremism är. Allt fler iakttagelser är av färskt datum. Merparten av de allvarliga fallen gäller den organiserade extremhögern eller högerextrem terrorism. I de allvarligaste fallen har det varit fråga om att en person med starka kopplingar till den organiserade extremhögern har sökt sig till en säkerhetskritisk uppgift eller organisation.

Extremhögern har inte systematiskt sökt sig till vissa branscher

Skyddspolisen har inte funnit några indikationer på att personer med kopplingar till extremhögern i större utsträckning skulle ha sökt sig till vissa arbetsgivare eller vissa uppgifter. Ju större organisation det är fråga om, desto fler iakttagelser görs det, eftersom det görs fler säkerhetsutredningar åt dem. Flest fall förekommer i utredningar inom byggbranschen och it-branschen.

Ser man på alla säkerhetsutredningar så ger omkring 2–4 procent ett resultat med information som meddelas arbetsgivaren. I sådana fall underrättar Skyddspolisen arbetsgivaren skriftligen.

De skriftliga underrättelserna gäller för det mesta omnämnanden i polisens register eller ekonomiska svårigheter. Dessa utgör cirka 90 procent av fallen. Iakttagelser som på något sätt gäller högerextremism utgör inte någon stor andel av all information arbetsgivarna får, även om antalet fall har ökat.

Skyddspolisen bedömer alltid från fall till fall om något är så väsentligt att en eventuell kommande arbetsgivare ska underrättas om det. Alla iakttagelser kommer alltså inte automatiskt till arbetsgivarens kännedom. ■

Säkerhetsutredningen bedömer tillförlitligheten

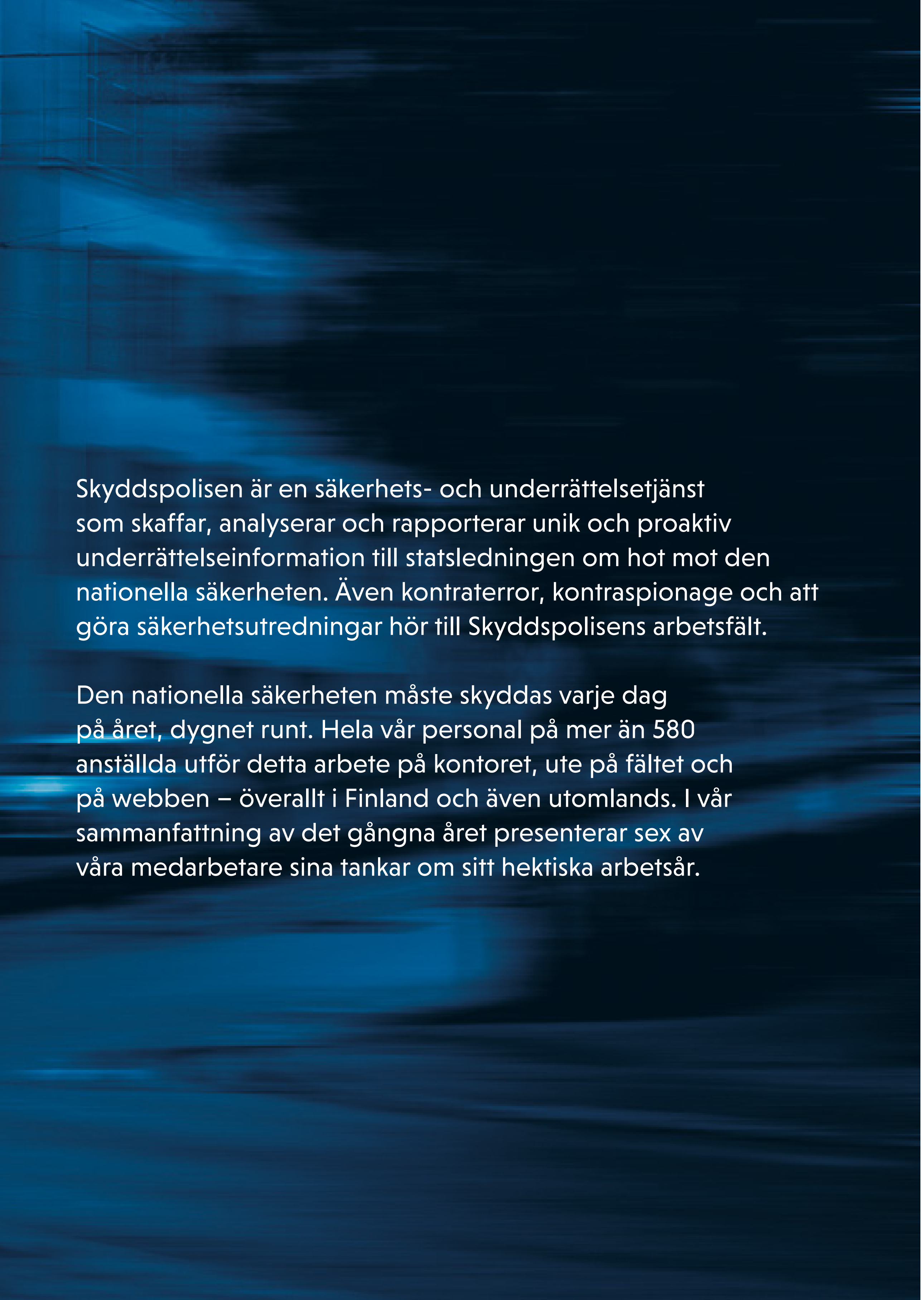
Säkerhetsutredningarna fyller en viktig funktion i det förebyggande säkerhetsarbetet. Syftet med utredningarna är att förhindra att information som är viktig för Finlands säkerhet hamnar i händerna på exempelvis främmande stater eller extremistiska rörelser.

I säkerhetsutredningen undersöks sådana omständigheter som kan göra en person mottaglig för påverkan eller påtryckning eller som kan påverka personens tillförlitlighet i en viss uppgift.

Skyddspolisen överväger alltid från fall till fall och i förhållande till arbetsuppgifterna om de uppgifter som framkommit i samband med utredningen är sådana att det är nödvändigt att underrätta arbetsgivaren. Exempelvis kan allvarliga ekonomiska svårigheter göra en person mottaglig för påverkansförsök.

Säkerhetsutredningen är inte bindande för arbetsgivaren. Arbetsgivaren beslutar alltid själv om informationen från Skyddspolisen påverkar till exempel en rekrytering.

Skyddspolisens år



Skyddspolisen är en säkerhets- och underrättelsetjänst som skaffar, analyserar och rapporterar unik och proaktiv underrättelseinformation till statsledningen om hot mot den nationella säkerheten. Även kontraterror, kontraspionage och att göra säkerhetsutredningar hör till Skyddspolisens arbetsfält.

Den nationella säkerheten måste skyddas varje dag på året, dygnet runt. Hela vår personal på mer än 580 anställda utför detta arbete på kontoret, ute på fältet och på webben – överallt i Finland och även utomlands. I vår sammanfattning av det gångna året presenterar sex av våra medarbetare sina tankar om sitt hektiska arbetsår.

Ilkka Hanski, chef för avdelningen för säkerhetsutredningar: "Vi har satsat på att utveckla utredningarnas kvalitet"

Också i år har avdelningen för säkerhetsutredningar haft bråttom, eftersom antalet utredningar har ökat betydligt. Ökningen har skett över en längre tid, men i år steg antalet för första gången till över etthundra tusen. Totalt gjordes omkring 115 000 utredningar.

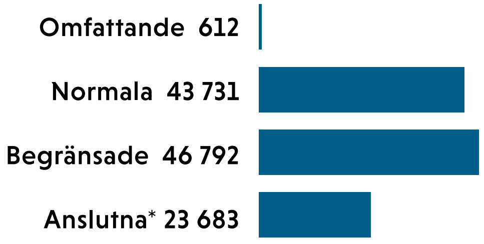
Något som har bidragit till ökningen är de senaste årens lagändringar, men vi har också själva arbetat konsekvent för att alla centrala aktörer ska omfattas av säkerhetsutredningarna. Vi har också fört dialog med de organisationer som redan omfattas av förfarandet för att säkerhetsutredningarna ska gälla alla relevanta arbetsuppgifter.

Vi har också satsat på att utveckla utredningarnas kvalitet. De utländska bindningarna utreds numera allt oftare i samband med normala säkerhetsutredningar. Utredningarna inbegriper nu också fler intervjuer.

Det tar i genomsnitt mindre tid att genomföra en säkerhetsutredning, eftersom vi har utvecklat våra egna processer. Den tid som krävs för en utredning påverkar hur låg tröskel en organisation har för att anlita oss för säkerhetsutredningar. Vårt utvecklingsarbete har gett resultat eftersom 95 procent av dem som besvarade vår kundnöjdhetsundersökning i fjol var nöjda med våra tjänster. Hela 97 procent av kunderna ansåg säkerhetsutredningarna vara viktiga för deras organisation.

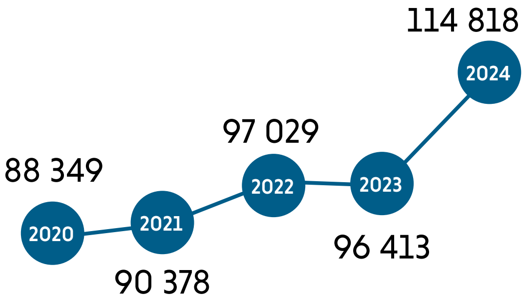
Skyddspolisens avdelning för säkerhetsutredningar ger också utlåtanden om uppehållstillstånd och om ansökningar om medborgarskap och visering. Också dessa utlåtanden har blivit fler. Genom utlåtandena kan vi bidra till att människor som hotar den nationella säkerheten inte kommer till Finland.

Säkerhetsutredningar 2024



*Det behövs inte alltid göra en ny utredning ifall en persons arbetsuppgifter ändras.

Säkerhetsutredningar totalt



Medarbetare med observationsuppgifter: "Vårt fältarbete sker där människor vistas"

Jag har jobbat flera år med observationsuppgifter inom Skyddspolisen, dvs. i kärnan av Skyddspolisens egen informationsinhämtning. Som metod för underrättelseinhämtning avser observation att en person eller grupp av personer iakttas i hemlighet när det behövs för att få viktig information och skydda den nationella säkerheten.

Skyddspolisens uppgift är att ta fram sådan unik information om den nationella säkerheten som inte finns att tillgå någon annanstans. Då är informationsinhämtning som Skyddspolisen utför själv och självständigt av central betydelse.

Vårt fältarbete sker där människor vistas. De som vi vill inhämta information om anstränger sig också för att agera proffsigt och i smyg, så även vi måste agera på samma sätt, fast bättre. Även om informationsinhämtning på webben blivit allt viktigare, finns det mycket information som fortfarande måste skaffas i den fysiska världen.

Vårt arbete är utmanande och kräver långsiktighet. En operation kan innehålla långvarig insamling av information, men de faktiska resultaten syns först flera år senare. Vi är också medvetna om att vår arbetsinsats bara är en pusselbit i den stora helheten av civil underrättelseinhämtning med många aktörer.

Även vi har haft ett exceptionellt hektiskt år. Vi har använt metoderna för underrättelseinhämtning på ett mångsidigt sätt och lyckats skaffa viktig information för den nationella säkerheten.

Det gångna året har också varit tungt för de anställda eftersom det kännetecknats av en stor arbetsmängd i kombination med ett osäkert ekonomiskt läge. Det har förekommit oro bland personalen över huruvida vårt arbete kan fortsätta i denna form när resurserna krymper. Det krävs mänskliga resurser för att Skyddspolisen ska kunna skydda samhället genom sin närvaro.

Teemu Liikkanen, chef för kontraspionage: "Vi måste hitta nya sätt att bekämpa spionage"

Jag började som chef för kontraspionage i början av september 2024. Redan innan jag började antog jag att jobbet var utmanande, men jag blev ändå överraskad av brådskan, frågornas mångfald och informationsmängden.

Det rör sig om stora saker och stort ansvar hela tiden. Spionage och påverkan mot vårt land är inte frågor som gäller enbart Skyddspolisen utan hela Finland. Det gör också arbetet intressant och givande, särskilt när man lyckas med något.

Man behöver inte fundera på om det man gör är viktigt, även om allt inte är glamour hela tiden. Precis som i allt annat expertarbetet är det mycket läsande och skrivande, många möten och många saker att sätta sig in i.

Som chef för kontraspionage försöker jag utveckla vårt arbete i alltmer proaktiv riktning. Ryssland har traditionellt använt diplomatisk täckmantel i sin personbaserade underrättelseinhämtning, men nu har det försvårats betydligt. Eftersom motparten tvingats söka nya sätt att inhämta information, måste även vi försöka hitta nya sätt att bekämpa spionage. I bästa fall vet vi vad motparten planerar innan planerna verkställs.

Eftersom omvärlden förändras och hoten är mångfasetterade måste vi utveckla vår verksamhet. Jag vill exempelvis bidra till att underlätta samarbetet mellan avdelningarna, det vill säga överbrygga gränser.

Kontraspionage hör till Skyddspolisens traditionella kärnuppgifter. Därför måste reformer göras med respekt för historien – det finns all anledning att bevara det som fungerar.

It-spanare: "Ett till synes galet lösningsförslag kan leda in på rätt spår"

Mitt arbete går ut på att samla information från olika datanät. Vårt team fungerar som en slags koncerntjänst som har specialiserat sig på att använda olika metoder för att inhämta information och underrättelser på webben.

Våra dagar varierar stort beroende på vad vi behöver skaffa information om. Den ena dagen söker vi kanske information som gäller Ryssland, medan nästa dag går i kontraterrorns tecken. Vårt team verkar inom Skyddspolisens hela verksamhetsfält, så kan jag inte säga att något tema skulle ha dominerat fjolåret. Men självfallet sysselsätter alla ekon från öst oss. Vi jobbar alltid när det behövs – webben sover inte!

Öppna källor är en viktig utgångspunkt för så gott som alla mina arbetsuppgifter. Information som finns i öppna källor kan jämföras med underrättelseinformation som samlats in med andra metoder eller exempelvis mot andra myndighetsregister. Underrättelser från öppna källor är ett utmärkt hjälpmedel när man bestämmer sig för hur de egentliga metoderna för underrättelseinhämtning ska inriktas. Vissa metoder använder vi själva, medan vi i fråga om andra stöder andra enheter inom deras kompetensområden.

Det går att göra en grov indelning av vårt team i tre kompetensområden. Vi har detektivhjärnor med polisiär bakgrund, och de är så att säga bra på att lägga pussel. Men vi behöver också experter på olika språk (exempelvis kinesiska, ryska och arabiska kan nämnas), och dessutom är it-experterna naturligtvis viktiga. Det är sällan som någon kan vara allt detta på en och samma gång.

Vi samarbetar nära med ämnesexperter och utbildar dem i användningen av öppna källor. Exempelvis kan en analytiker som specialiserat sig på Kina se på den insamlade informationen med helt andra ögon än vi.

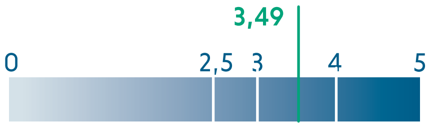
Mitt jobb är tämligen självständigt. Ingen kommer och säger hur ett jobb ska göras. Ett gott slutresultat går nämligen att nå på så många olika sätt. Men samtidigt är det stöd som teamet ger en viktig tillgång till exempel när man länge kör huvudet i väggen med ett problem. En kollega kan med fräschare ögon se något som man själv inte märker. Det är förvånande hur ofta ett till synes galet lösningsförslag som en kollega fantiserar ihop med glimten i ögat till sist kan leda in dig på rätt spår.

Man gör alltid olika tankefel inom underrättelsearbetet, och det är något som underrättelsespecialister bör vara medvetna om. Ett klassiskt tankefel som it-spanare gör är att anta att någon säkert redan vet detta, så det lönar sig inte att rapportera. I det dagliga livet har det ändå visat sig att det alltid lönar sig att säga till när man misstänker sig ha funnit något som hör till Skyddspolisens ansvarsområde. Det bästa med mitt arbete är att till och med minsta lilla korn av information teamet skaffar kan fungera som ett incitament för annan informationsinhämtning.

Ibland känns informationsinhämtning på webben som att leta efter en nål i en höstack. Eller som vi brukar säga: som att försöka hitta en okänd strandstuga på världskartan. Och vi hittar den så gott som alltid!

Förtroende och anseende

T-Media genomförde 2024 en undersökning av vilket förtroende allmänheten har för Skyddspolisen och vilket anseende myndigheten har. Den siffra som beskriver anseendet är en sammanställning av hur allmänheten bedömt Skyddspolisens arbete, förvaltning, ekonomi, ledning, ansvar, arbetsgivarbild, växelverkan och förnyelseförmåga.



0–2,5 Mycket lågt
2,5–3 Lågt
3–3,5 Måttligt
3,5–4 Högt
4–5 Mycket högt

Chef för internationella ärenden: "Internationellt samarbete är en av Skyddspolisens viktigaste kapaciteter"

De hot som påverkar Finland har blivit mer komplexa de senaste åren och även mer avlägsna kriser kan ha återverkningar hos oss. Internationella utbyten och jämförelser av information hjälper till att analysera hur hoten fungerar, hänger ihop med varandra och utvecklas. Därför blir internationella nätverk och internationellt samarbete allt viktigare i vårt arbete med avseende på underrättelseinhämtningen.

Internationellt samarbete är en av Skyddspolisens viktigaste kapaciteter. Det är ett sätt att utbyta unik information bilateralt. Den information som detta samarbete genererar är väsentlig exempelvis för att förse statsledningen med förstklassig rapportering.

Skyddspolisens internationella samarbete har blivit aktivare, vilket också märks i att korrespondensen ständigt ökar. Våra anställda jobbar med internationellt samarbete varje dag och på bred front på olika avdelningar.

Vid sidan av bilateralt informationsutbyte kan samarbetet också bedrivas på multilaterala forum, och exempelvis Nato har fört med sig ett viktigt tillskott i detta avseende. För Skyddspolisens del stärktes och etablerades Natosamarbetet ytterligare under året. Samarbetet inom alliansen är inte bara en möjlighet utan också en skyldighet, och Skyddspolisen svarar för Finlands del för frågor som gäller civil underrättelseinhämtning i enlighet med sitt ansvarsområde.

De icke-militära påverkansförsöken och hoten har tagit sig alltmer varierande former de senaste åren, vilket också märks i Natosamarbetet.

Det internationella samarbetet i vardagen är hektiskt och förändras dagligen, eftersom variablerna i den säkerhetspolitiska miljön och utrikes- och säkerhetspolitiken sällan följer exakta geografiska gränser eller tidszoner.

Internationell korrespondens

21 000

internationella meddelanden
(skickade och mottagna)

Personal

Medelålder 42,9

Personer 584

Personal med akademisk examen 72,6 %

Systemchef Susanna Kallonen: "Våra IKT-anställda kommer inte lätt undan"

Arbetet inom IKT-branschen går typiskt sett ut på att lösa svåra och komplicerade problem av teknisk och processuell natur i samarbete med olika samarbetspartner. Så kommer det också att vara på Skyddspolisen 2025.

Det svåra ekonomiska läget har varit en extra krydda i sammanhanget den senaste tiden. Trots det har vi kunnat arbeta vidare med viktiga systemutvecklingsprojekt. Det gäller bland annat projektet Inter, som startades med hjälp av EU-finansiering och går ut på att ta fram moderna verktyg och AI-egenskaper till stöd för dataanalys i Skyddspolisens centrala informationssystem.

Syftet är också att effektivisera arbetet och förbättra kvaliteten på arbetsprocesserna. Med hjälp av denna typ av utvecklingsprojekt vill vi förbättra våra analysförmågor ytterligare. Arbetet bidrar till Skyddspolisens ombildning till en underrättelsetjänst och skapar beredskap för att den datamängd som ska behandlas ökar.

Projektet har hunnit ungefär halvvägs. Tills vidare har de kvantitativa etappmålen till största delen uppnåtts, och projektet framskrider enligt tidsplanen. Bland annat har vi redan infört en arbetsyta som effektiviserar samarbetet mellan våra analytiker. Nästa steg är att ta fram AI-verktyg.

Också det omfattande it-infrastrukturarbete som Skyddspolisens nya kontorshus förutsätter har krävt betydande satsningar av vår IKT-personal när flytten till ny adress 2025 hägrar. Allt måste finnas på plats inför flytten så att systemen fungerar och vardagslunken kan fortsätta smidigt efter flytten. Även inom detta enorma projekt har våra anställda visat prov på sin utmärkta yrkeskunskap.

Vårt verksamhetsområde har sina särdrag och därför ställs det också särskilda krav när vi utvecklar våra it-system. Dessa krav medför vissa svårigheter i utvecklingsarbetet. Våra IKT-anställda kommer inte lätt undan när de ska utveckla och underhålla ett stort antal system och den bakomliggande infrastrukturen samt maskinvaran. Vi jobbar för fullt för att lyckas hålla jämna steg med den allmänna IKT-utvecklingen.

Dem vi har att tacka för att allt lyckas är vår ytterst kunniga och uthålliga IKT-personal som dag efter dag löser dessa komplexa problem och för sin del bidrar till kontinuiteten i vår organisations kärnverksamhet. ■

Finansiering som använts per räkenskapsår

(miljoner euro M€)