ÅRSÖVERSIKT 2020

MUST

Grafisk formgivning: FM HRC Service Grafisk produktion, februari 2021
Tryck: Elanders Sverige AB

MUST ÅRSÖVERSIKT 2020

MILITÄRA UNDERRÄTTELSE- OCH SÄKERHETSTJÄNSTEN

Must presenterar här den verksamhet som bedrivits under 2020 och ger även sin syn på omvärldsutvecklingen och de säkerhetshot som riktas mot Sverige och svenska intressen.

Årsöversikten svarar mot uppdraget i Försvarsmaktens instruktion (2007:1266, 6§) där Must uppdras att varje år upprätta en översikt över den militära säkerhetstjänstens verksamhet som allmänheten kan ta del av. Must har valt att utöver detta även presentera annan verksamhet för att därigenom ge en så heltäckande bild som sekretessen medger.

FÖRSVARSMAKTEN

INNEHÅLLSFÖRTECKNING

Vision och verksamhetsidé

Musts vision

Ett säkrare Sverige i en osäker värld.

Verksamhetsidé

Must ger regeringen och Försvarsmakten unika beslutsunderlag om omvärldsutvecklingen och hot mot Sveriges säkerhet.

Must bidrar till att Försvarsmaktens förmågor utvecklas och att förbanden har en bra hot- och lägesuppfattning. Vi bidrar också till att Försvarsmakten och andra myndigheter har rätt nivå på sin säkerhet.

Must löser sina uppgifter med hög integritet och i samverkan med andra. Vi utvecklar oss kontinuerligt för att kunna möta förändrade krav.

CHEFEN MUSTS FÖRORD

Under 2020 har utvecklingen mot en mer hårdhänt maktpolitik förstärkts, globalt och i Europas grannskap. Samtidigt har den regelbaserade ordningen och förutsägbarheten försvagats. Den pågående pandemin har accelererat dessa trender och Must bedömer att risken för att Sverige utsätts för kraftfulla påtryckningar är förhöjd i denna miljö.

Den antagonistiska hotbilden mot Sverige är idag samtidigt politisk, ekonomisk och militär – inte "antingen eller". Den har således blivit både bredare och mer komplex. Det handlar om yttre hot, som allt oftare manifesteras även i den inre säkerheten. Hoten riktas mot Sveriges försvarsförmåga, välstånd och demokrati. Hybrida, dolda och förnekbara metoder blir allt vanligare.

Den militära aktiviteten i Sveriges närområde har fortsatt att öka i intensitet och har blivit alltmer kvalificerad. Trenden att se ekonomi och teknologi som strategiska verktyg förstärks. Länder som Ryssland och Kina har en bred verktygslåda för att främja sina statliga intressen, och god förmåga till samordning. Underrättelseverksamheten mot Försvarsmakten och Sverige är omfattande.

I denna verklighet verkar Must som den civila och militära underrättelsetjänst, och den militära säkerhetstjänst, som arbetar med de yttre hoten mot Sveriges säkerhet – oavsett vilka de är. När jag summerar Musts verksamhet under 2020 är jag stolt över att kunna konstatera att vi, tillsammans med våra nationella och internationella samarbetspartner, kunnat fullgöra det uppdrag vi fått av våra uppdragsgivare regeringen och Försvarsmakten.

Must ska kunna verka under alla olika omständigheter. Tack vare medarbetarnas anpassningsförmåga och kreativitet har vi under 2020, trots de begränsningar som covid-19-pandemin medfört, kunnat lösa våra uppgifter med bibehållen kraft och kvalitet.

Riksdagens inriktningsbeslut för ett starkare totalförsvar innebär en ytterligare ambitionsökning för Must. Det ger oss förutsättningar men ställer också krav på att fortsätta utveckla och anpassa Musts verksamhet i takt med omvärldsförändringarna så att vi på bästa sätt kan stödja Försvarsmaktens tillväxt.

Must bidrar till att stärka Sveriges samlade förmåga att möta en mer komplex hotbild. Under 2020 har det gällt till exempel cybersäkerhet, psykologiskt försvar, utländska direktinvesteringar och elektronisk kommunikation. Vi bidrar till ett starkare säkerhetsskydd i totalförsvaret och hela samhället. Att bidra till framtagning och implementering av ny lagstiftning är en del av detta.

Vi fortsätter att skapa tekniska förutsättningar för Must i en miljö där hantering av stordata, IT-utveckling, cyberhot, informationssäkerhet och AI är central.

Jag är också glad över att Must under 2020 fick möjlighet att blicka tillbaka på en viktig del av vårt historiska arv. Genom Armémuseums utställning "I rikets hemliga tjänst" och uppsättandet av minnesplaketter där C-byrån hade kontor hedrade vi inte minst de kvinnor, men även de män, som arbetade i verksamheten under andra världskriget.

Min förhoppning är att denna årsöversikt ska ge en bild av Musts verksamhet och vår syn på omvärldsläget och de yttre hoten. Men även av hur vi anpassar Must för att också framöver effektivt kunna fullgöra vårt uppdrag: att bidra till ett säkrare Sverige i en osäker omvärld.

Lena Hallin | Chef för Militära underrättelse- och säkerhetstjänsten

Militära underrättelse- och säkerhetstjänsten i korthet

- Must bedriver försvarsunderrättelseverksamhet och militär underrättelse- och säkerhetstjänst.
- Musts försvarsunderrättelseverksamhet bedrivs till stöd för svensk utrikes-, försvars- och säkerhetspolitik samt i övrigt för kartläggning av yttre hot mot Sverige.
- Must förebygger, upptäcker och motverkar säkerhetshot som riktas mot Försvarsmakten och dess intressen i Sverige och utomlands.
- Must är en del av Försvarsmakten och inriktas både av överbefälhavaren och av regeringen.
- Chefen för Must lyder direkt under överbefälhavaren. Chefen för Must är också Försvarsmaktens säkerhetsskyddschef och ansvarar för underrättelse- och säkerhetsfunktionen i Försvarsmakten.
- Att samverka nationellt och internationellt är avgörande för att kunna hantera nuvarande och framtida utmaningar.
- Musts verksamhet regleras av lagar och regler och granskas löpande av oberoende organ.

Inget påverkar den globala geopolitiska och geoekonomiska utvecklingen mer än hur rivaliteten mellan Kina och USA utvecklas.

SVERIGE OCH OMVÄRLDEN

OMVÄRLDSUTVECKLINGEN

Det globala säkerhetspolitiska läget är instabilt och konfliktfyllt. Pandemin orsakar i många samhällen en social och ekonomisk skörhet, som får långsiktiga följder. De viktigaste trenderna i omvärlden som påverkar Sveriges säkerhet har dock inte ändrat riktning under pandemin, utan snarare förstärkts.

Världspolitiken präglas mer än på länge av maktpolitik och den starkes rätt. Tillbakagången för demokrati, folkrätt, rustningskontroll och multilateralism har fortsatt. Både den multilaterala, regelbaserade världsordningen och den europeiska säkerhetsordningen, som varit grundpelare för internationell och svensk säkerhet under lång tid, är allvarligt försvagade.

Det säkerhetspolitiska läget utmärks i stället av en hårdnande rivalitet mellan stormakterna – i första hand mellan USA, Kina och Ryssland. Denna utspelas globalt och omfattar idag mer eller mindre alla strategiska sektorer.

De militära maktmedlen är fortsatt centrala. Ekonomi och teknologi används av stormakterna allt oftare som säkerhetspolitiska verktyg och ses som integrerade delar av den nationella säkerheten. Den politiska systemrivaliteten blir en mer framträdande konfliktdimension.

Kina och Ryssland utmanar på olika sätt USA:s ledande ställning i världspolitiken, enskilt och gemensamt. Vårt närområde är av militärstrategiskt intresse för Ryssland och USA, som båda har fortsatt att utöka sina militära aktiviteter där.

Kina har ett ökat strategiskt intresse av Arktis och av tillgång till svensk högteknologi för både civila och militära ändamål.

Inget påverkar den globala geopolitiska och geoekonomiska utvecklingen mer än hur rivaliteten mellan Kina och USA utvecklas. Ländernas försämrade relationer tycks leda mot en ökad ekonomisk och teknologisk särkoppling, och mot en närmare sammankoppling av säkerheten i Europa och Asien.

Konflikternas karaktär fortsätter att förändras. De utspelas idag på många arenor, med en bred uppsättning av verktyg och ofta med snabbt skiftande intensitet. Verkan kan ske oberoende av geografiskt avstånd genom exempelvis ekonomiska medel, cyber- och påverkansoperationer.

Sveriges säkerhet påverkas också av sammanhållningen och handlingskraften inom EU och Nato, liksom i våra viktigaste samarbetsländer. Ryssland och Kina agerar för att skapa eller utnyttja splittring inom och mellan västländerna. Den nya amerikanska administrationen har understrukit sin vilja att stärka och utveckla USA:s allianser och samarbete främst med andra demokratiska stater.

Den försvagade multilaterala och regelbaserade världsordningen gör det svårare att möta globala hot som klimatförändringen, den ekonomiska tillbakagången och pandemin, samt att. upprätthålla internationell rustningskontroll och icke-spridning.

Det blir också svårare att uppträda enat för att hantera regionala konflikter. Det är en av flera underliggande orsaker till att säkerheten under 2020 försämrades i länder som Afghanistan, Irak och Mali, där Försvarsmakten deltar i fredsfrämjande insatser. Terrorism, svaga stater och gränsöverskridande kriminalitet förblir ett hot mot stabiliteten i många regioner.

EN BREDDAD OCH ALLTMER KOMPLEX HOTBILD

Must bedömer att hotbilden mot Sverige blir bredare och allt mer komplex. Den är idag samtidigt politisk, ekonomisk och militär. Det görs också allt fler kopplingar mellan olika områden. Till exempel används ekonomiska påtryckningar för att uppnå politiska mål.

Hoten kan ha flera samtidiga syften och skada Sveriges försvarsförmåga, ekonomiska välstånd och det oberoende beslutsfattandet i vårt demokratiska samhälle. Det handlar om yttre hot som allt oftare manifesteras även i den inre säkerheten.

Kvalificerade statliga aktörer söker sårbarheter brett i vårt öppna och digitaliserade samhälle. De gör ingen skillnad mellan civilt och militärt, eller mellan offentligt och privat. De utnyttjar luckor i vår organisation, lagstiftning och samverkan.

Stormakter som Ryssland och Kina genomför antagonistiska aktiviteter riktade mot svenska intressen. Båda länderna kan använda sig av hela spektret av samhällets resurser för att nå sina målsättningar och har en god förmåga att samordna olika medel. De ryska och kinesiska underrättelse- och säkerhetstjänsterna är centrala och resursstarka aktörer.

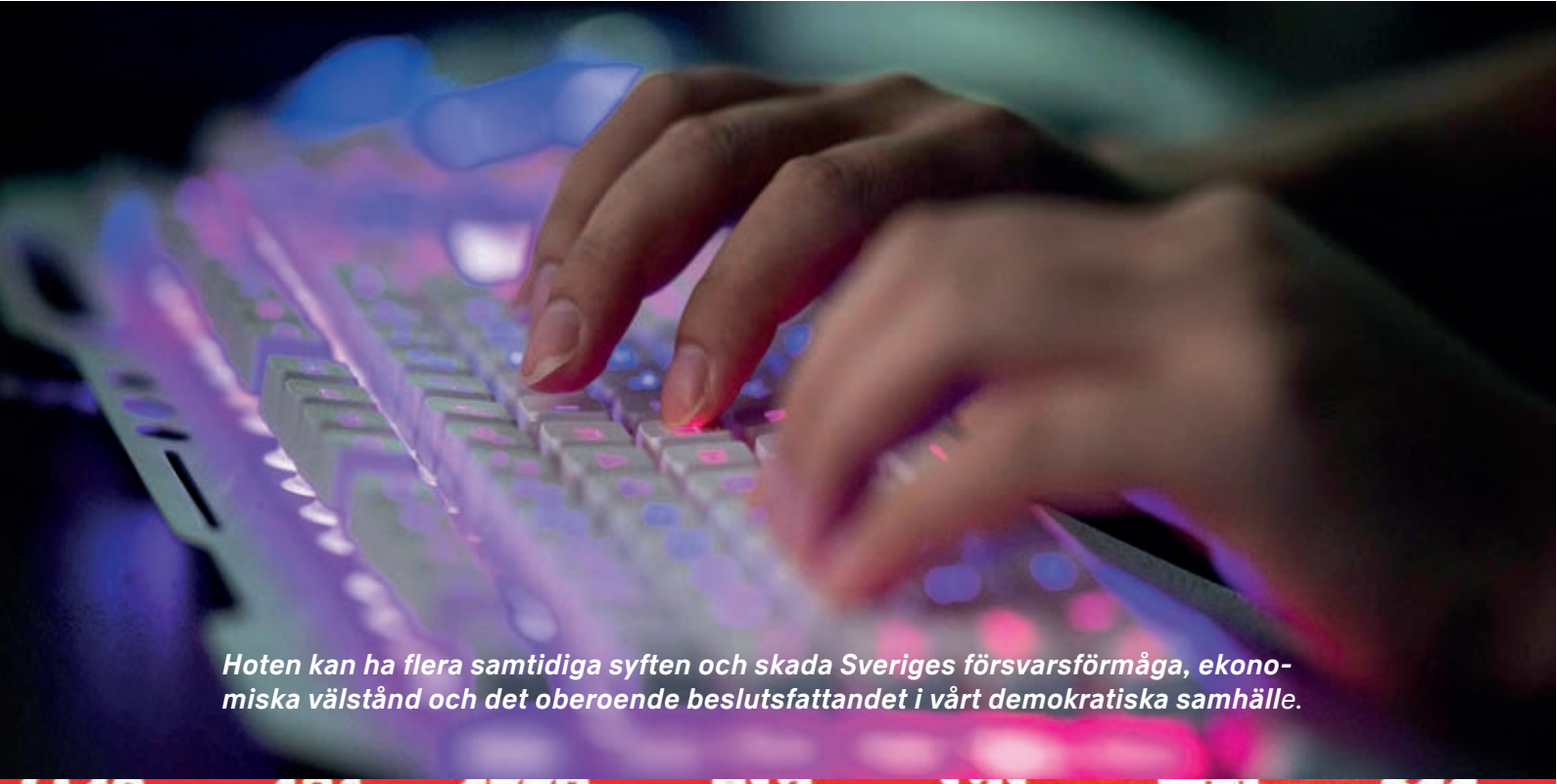
Ett väpnat angrepp mot Sverige kan inte uteslutas och utgör den dimensionerande hotbilden för Försvarsmakten. De militära eller politiska hoten mot Sverige ersätts inte av hoten mot svensk ekonomi, teknologi och infrastruktur. Det handlar inte om ”antingen eller” utan om ”både och”.

Många av hoten kan förekomma i hela konfliktskalan – från fred till kris och krig – och de är inte linjära. Metoderna är ofta förnekbara, dolda och tvetydiga. Instrumenten spänner från cyberangrepp till påverkansoperationer, utnyttjande av ekonomiska beroenden och våldsanvändning.

Främmande makts åtgärder här och nu kan utgöra ett allvarligt hot mot vår handlingsfrihet i kris eller krig. Exempelvis söker man insteg i digital eller fysisk samhällskritisk infrastruktur som man vill kunna lamslå om man skulle anse det ändamålsenligt – för politiska påtryckningar i fred, demoraliserande samhällspåverkan i en kris eller för att skada vårt totalförsvar i krig.

De senaste årens utveckling visar att agerandet även i fredstid kan innefatta våldsanvändning, som till exempel i förgiftningen av den ryska oppositionspolitikern Navalnyj med det sovjetutvecklade nervgiftet Novitjok. Det har även förekommit ett antal mord och mordförsök på europeisk mark som med varierande grad av säkerhet kan kopplas till främmande underrättelse- och säkerhetstjänster.

Must bedömer sammanfattningsvis att risken har ökat för att små eller medelstora länder som Sverige ska utsättas för kraftfulla påtryckningar. Samtidigt blir hotbilden mot Sverige bredare och alltmer komplex. Den utmanar många invanda föreställningar om konflikternas natur. Det är mot bakgrund av detta som beskrivningen av länder och regioner i denna årsöversikt ska läsas.



Hoten kan ha flera samtidiga syften och skada Sveriges försvarsförmåga, ekonomiska välstånd och det oberoende beslutsfattandet i vårt demokratiska samhälle.

SVERIGES NÄROMRÅDE

Sveriges närområde påverkas av en mer konfliktfylld global säkerhetspolitisk miljö och av en hårdnad konkurrens mellan stormakterna. Vid sidan av Rysslands och USA:s fortsatta intressen i närområdet ökar även Kinas strategiska närvaro, främst i Arktis.

De militära huvudaktörerna i Sveriges närområde är Nato och Ryssland, vars säkerhetspolitiska och militärstrategiska intressen här står emot varandra. Intressena är oförändrade och till stor del oförenliga. Den militära verksamheten bedöms därför fortsätta i minst samma omfattning som nu.

Den militära aktiviteten i närområdet – i Östersjöregionen, Barents hav och Nordatlanten – har fortsatt att öka i både intensitet och komplexitet. Under 2019 och 2020 har den varit den högsta sedan slutet av kalla kriget, men ligger under den tidens nivåer.

Den ryska militära verksamheten i närområdet har gradvis ökat, från en låg utgångspunkt, sedan Vladimir Putin blev president 2000. Främst som en reaktion efter Rysslands illegala annektering av Krim 2014 har även västs militära närvaro och övningsverksamhet ökat. Det finns en växelverkan mellan de ryska och västliga aktiviteterna.

Den militära verksamheten i vårt närområde syftar främst till att vara avskräckande och förmågehöjande. Med en hög nivå av militär aktivitet finns det alltid en risk för incidenter eller missbedömningar. Aktörerna stärker också sin underrättelseinhämtning för att förbättra sin strategiska förvarning eller för att kunna vidta förberedande åtgärder i händelse av kris eller krig.

Rysslands tröskel för att använda militära medel har sänkts över tid. Förnekbara icke-militära medel är det ryska huvudalternativet för att uppnå sina säkerhetspolitiska målsättningar gentemot Nato- och EU-länder, men Ryssland strävar efter att kunna säkerställa militär handlingsfrihet gentemot Nato i händelse av väpnad konflikt i svenskt närområde.

I en konflikt skulle Ryssland sannolikt inledningsvis ha en regional överlägsenhet gentemot Nato. Men samtidigt upplever Ryssland sig vara instängt i Östersjön vars inlopp kan kontrolleras av Nato-länder. Den ryska handlingsfriheten skulle försämras vid en förstärkning av Nato i Östersjöområdet och Ryssland skulle agera för att motverka en sådan utveckling.

Ryssland strävar i växande omfattning också efter att förbättra sin militära förmåga att verka på Nordatlanten. Syftet är att kunna förhindra transport av förstärkningar från USA till Europa i händelse av kris eller krig, och därmed bevara sin handlingsfrihet i Östersjöregionen och Barents hav.

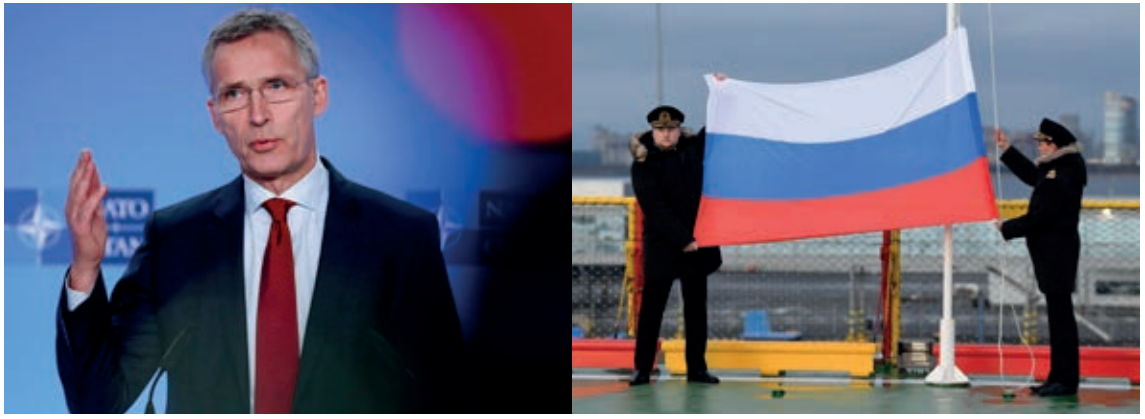
Militärstrategiska skäl ligger också till grund för Rysslands oro över utvecklingen i Belarus, tillsammans med risken för att ett okontrollerat maktskifte där även skulle kunna påverka regimstabiliteten i Ryssland. Tillgång till Belarus territorium är viktigt för Rysslands strategiska djup och för Kaliningrads försörjningssäkerhet.

Nato upprätthåller gemensam luftövervakning i de baltiska staterna och närvaro med fyra multilaterala stridsgrupper i Estland, Lettland, Litauen och Polen. Inte minst USA uppträder med kvalificerade flyg- och marinstridskrafter i Östersjöregionen och Barents hav.

Den viktigaste icke-militära konfliktytan i Östersjöregionen är Nordstream II, vars slutförande skulle förbättra Rysslands strategiska position och vars förhindrande skulle slå hårt mot ryska politiska och ekonomiska intressen. Under 2020 införde USA nya sanktioner mot projektet.

Liksom USA och Ryssland har även Kina ökande intressen i Nordatlanten och Arktis men även rörande Sverige per se. Arktis är viktigt för Kinas globala ambitioner, såväl säkerhetspolitiskt som ekonomiskt. Arktis kan erbjuda en ny transportled för Kina, som vill påverka regionens infrastruktur inom ramen för Belt and Road Initiative. Färöarna, Island och Grönland är av ökande intresse för flera stormakter.

Kinas säkerhetspolitiska intresse för Sverige handlar främst om att få tillgång till infrastruktur och högteknologi för civila och militära syften, genom handel, uppköp eller underrättelseverksamhet. Ryssland och Kina förväntas fortsätta att fördjupa sitt samarbete. Detta kan påverka även Sveriges närområde, liksom USA:s fortsatta förväntan att dess allierade och partner tar ett ökat ansvar för Europas säkerhet. USA betraktar Ryssland som ett allvarligt hot, men Kina som sin främsta säkerhetspolitiska utmanare. En ökad amerikansk tyngdpunktsförskjutning mot Asien är trolig.



De militära huvudaktörerna i Sveriges närområde är Nato och Ryssland, vars säkerhetspolitiska och militärstrategiska intressen här står emot varandra.

Ryssland har förmåga att agera snabbt och att opportunistiskt ta vara på möjligheter som dyker upp för att stärka sitt internationella inflytande.

RYSSLAND

Rysslands agerande under en längre tid har orsakat ett försämrat säkerhetspolitiskt läge i Sveriges närområde och i Europa som helhet. Det innefattar den illegala annekteringen av Krim 2014 och den pågående destabiliseringen av östra Ukraina. Ryssland agerande mot bland annat Ukraina, Georgien och Syrien visar att landet har en låg tröskel för militär våldsanvändning.

Rysslands centrala målsättningar är regimstabilitet och att stärka landets ställning som autonom stormakt. Ryssland eftersträvar en europeisk säkerhetsordning som erkänner landets rätt till en intressesfär där framför allt grannländer som Belarus, Ukraina, Moldavien och Georgien ingår. Såväl inom Ryssland som i vissa av dess grannländer finns tecken på en ökande social oro och instabilitet.

Militärstrategiska överväganden väger tungt i ryskt politiskt beslutsfattande. Ryssland ser USA:s och Natos samlade militära förmåga som den dimensionerande motståndaren och betraktar åtgärder som stärker dessa aktörers militärstrategiska förutsättningar som ett hot. 2016 stödde rysk säkerhetstjänst ett försök till kuppförsök i Montenegro inför landets Nato-tillträde.

Ryssland har förmåga att agera snabbt och att opportunistiskt ta vara på möjligheter som dyker upp för att stärka sitt internationella inflytande. Etablerandet av en rysk fredsbevarande styrka i Nagorno-Karabach är ett exempel på detta från 2020, då diplomatiska och militära medel samspelade.

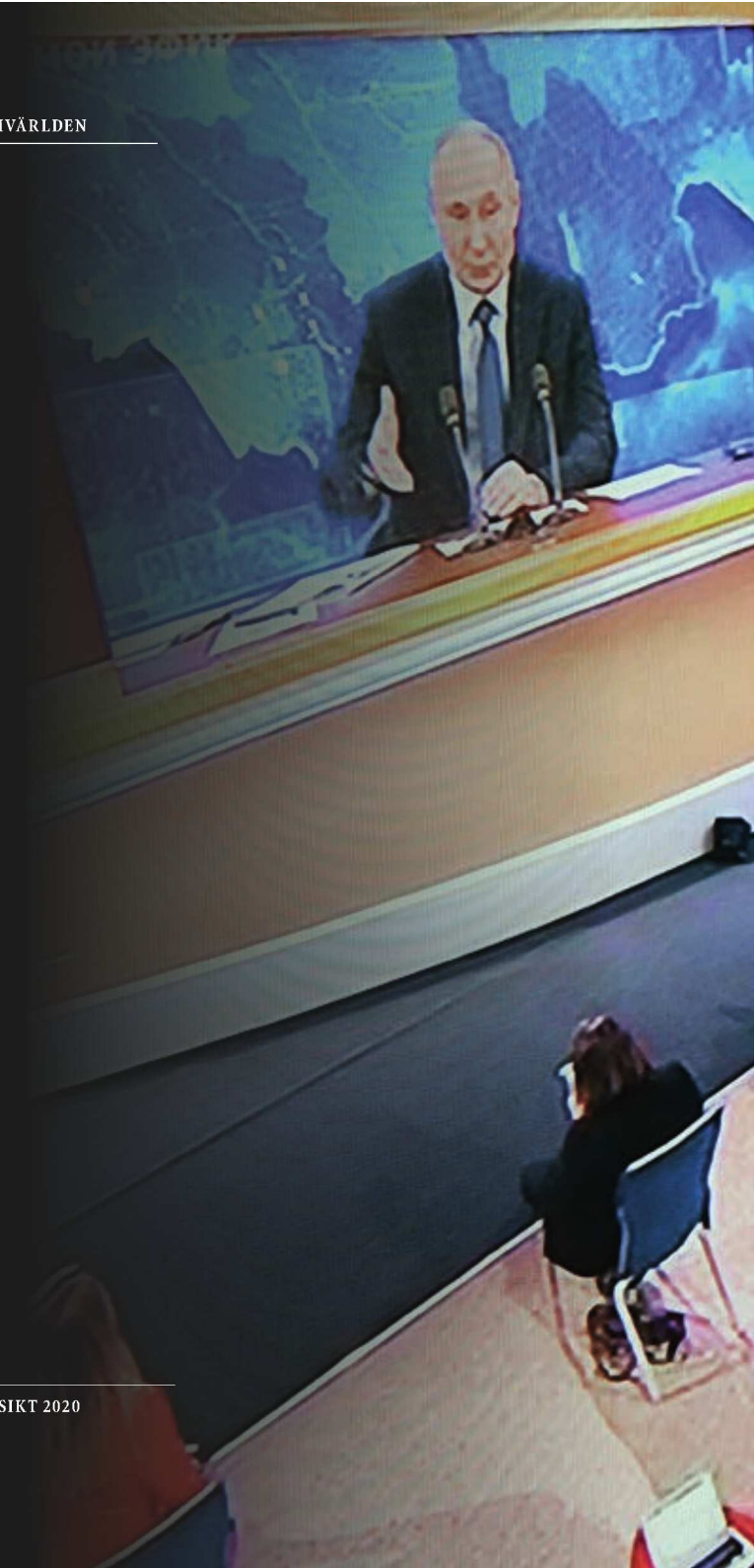
Ryssland har en god förmåga att samordnat använda en stor bredd av icke-militära och militära medel, ofta dolt och förnekbart. Man skapar eller utnyttjar splittring inom ett land eller mellan länder, inte minst för att försvaga EU och Nato, för att kunna utöva påtryckningar eller verka destabiliserande och nå de egna målen. Rysslands förmåga till påverkans- och cyberoperationer är ett viktigt verktyg i den hybrida och icke-linjära verktygslådan. Påverkansförsök pågår löpande.

De ryska maktmedlen omfattade under 2020 militär verksamhet i Libyen och Centralafrikanska republiken genom en privat firma med nära koppling till staten. Den uppmärksammade förgiftningen av Aleksej Navalnyj med det kemiska stridsmedlet Novitjok är ett annat exempel på rysk våldsanvändning. I likhet med förgiftningarna av Aleksander Litvinenko (2006) och Sergej Skripal och hans dotter Julia Skripal (2018) riskerades hänsynslöst även många andra människors liv.

Den ryska militärreformen och beväpningsprogrammet fortsätter. Av statsfinansiella skäl har takten sänkts något, men de militära utgifterna förblir högt prioriterade. Rysslands militära förmåga fortsätter att öka fram till 2025 tack vare redan gjorda investeringar, framför allt inom ramen för beväpningsprogrammet från 2008.

Förmågan till insats med kärnvapen har fortsatt högst prioritet inom den ryska militära förmågeutvecklingen. Kärnvapeninnehavet syftar till strategisk avskräckning och anses vara centralt för Rysslands ställning som stormakt. Ryssland har moderniserat både de strategiska och taktiska kärnvapnen, och genomför regelbundet kärnvapenövningar.

Efter kärnvapen prioriteras kvalificerat luftförsvar. Framgångsrika satsningar har också gjorts de senaste åren för att bygga upp en förmåga till konventionell bekämpning med hög precision på långa avstånd. Under de närmaste åren kommer Ryssland dessutom att lägga resurser på att utveckla sina ledningssystem.



Rysslands centrala målsättningar är regimstabilitet och att stärka landets ställning som autonom stormakt.

Valet av Joseph Biden till USA:s president och Kamala Harris till vicepresident markerar en förändring i synen på amerikansk maktutövning och USA:s roll i världen.

USA

Valet av Joseph Biden till USA:s president och Kamala Harris till vicepresident markerar en förändring i synen på amerikansk maktutövning och USA:s roll i världen. Samtidigt innebär det till stor del kontinuitet i de militärstrategiska prioriteringarna.

Mot bakgrund av den starka polariseringen i det amerikanska samhället och den pågående pandemin är det Must bedömning att den nya administrationen kommer att behöva prioritera den inrikespolitiska agendan. Den väntas därför i hög grad betrakta USA:s internationella intressen genom ett inrikespolitiskt prisma.

På sikt kan också pandemins ekonomiska efterverkningar, i kombination med en period av höga budgetunderskott och ökade krav på inrikespolitiska utgiftsökningar, komma att påverka både USA:s globala engagemang och framtida försvarsutgifter.

Mot denna bakgrund kommer USA fortsatt att förvänta sig att dess allierade och partner tar ett större ansvar för sin egen säkerhet – militärt, politiskt och ekonomiskt. Den transatlantiska gemenskapen kommer att utgöra en av den amerikanska politikens hörnstenar. Biden-administrationen är entydig i sitt stöd till EU och Nato, inklusive alliansens försvarsförpliktelser.

De amerikanska nationella säkerhets- och försvarsstrategierna från 2017 och 2018 utgår från en global konkurrens mellan stormakterna. I denna kontext utgör Kina det främsta militära, ekonomiska och teknologiska hotet. Den strategiska konkurrensen med Kina tilltar och USA förväntas att lägga en allt större vikt vid Stillahavsområdet. Ryssland betraktas som ett regionalt säkerhetspolitiskt hot som har en global inverkan genom sina kärnvapen, och som kan påverka USA med asymmetriska medel som cyberattacker och påverkansoperationer.

Vid sidan av Kina och Ryssland ser USA också Iran och Nordkorea, samt frågor som cyber och terrorism som utmaningar mot den egna säkerheten. Den nya administrationen väntas också lägga en större vikt vid frågor som klimathotet, multilateralism och demokratins ställning i världen.

USA kommer fortsatt att vara den ledande aktören i det internationella systemet. USA:s inflytande bygger på så väl ”hård” som ”mjuk” makt. Den hårda makten utgår från kärnvapen och på att USA är världens i övrigt starkaste militärmakt med global räckvidd, samt ett omfattande allianssystem. Den mjuka makten grundar sig på landets ekonomiska och teknologiska position, dess traditionella omfamnande av demokratiska värderingar och starka populärkulturella inflytande. Bidenadministrationen avser stärka USA:s allianser och demokratiska värderingar som fundament för säkerhetspolitiken.

USA fortsätter att vara militärtekniskt ledande. Den framtida förmågeutvecklingen präglas av en global styrkeprojektion inom alla domäner inklusive rymd- och cyberområdet. Betydande ansträngningar görs för att återta förmågan att strida mot en kvalificerad statlig motståndare. Amerikansk strävan är fortsatt att minska den permanenta militära närvaron utanför kontinentala USA till förmån för temporär eller rotationsnärvaro i syfte att verka avhållande eller som känselspröt i olika regioner.

USA kommer fortsatt att vara den ledande aktören i det internationella systemet. USA:s inflytande bygger på så väl ”hård” som ”mjuk” makt.


ULA

KINA

Kinas fortsatta framväxt har stor inverkan på det internationella systemet, och alltmer även på Sveriges säkerhetspolitiska miljö. Kina har världens näst största ekonomi och försvarsbudget. Landet utnyttjar med allt större självförtroende en stor bredd av maktmedel för att främja sina intressen.

Sedan 2012 går det kinesiska kommunistpartiet i en alltmer auktoritär riktning. Det övergripande målet är att bevara partiets maktinnehav. Hög ekonomisk tillväxt står i fokus, men också nationell samhörighet och stolthet.

Kinas syn på säkerhet omfattar nästan alla samhällsområden och landet hävdar dessa breda säkerhetspolitiska intressen med allt större eftertryck. Under 2020 fortsatte repressionen av oliktänkande och av vissa etniska grupper, till exempel uigurer, och Kina stärkte sitt grepp om Hongkong. Militära styrkedemonstrationer skedde nära Taiwan och i Sydkinesiska sjön. Skärmytslingar ägde rum vid gränsen mot Indien och starka ekonomiska påtryckningar riktades mot Australien.

Stora resurser, inklusive påverkansoperationer, lades på att framställa Kinas hantering av covid 19-pandemin som lyckad och solidarisk, och på att vinna strategiska insteg i vissa länder. Den kinesiska så kallade ”wolf warrior-diplomatin” användes offensivt.

Kina verkar systematiskt för att förändra det internationella systemet i en för landet gynnsam riktning. Den liberala världsordningen och USA som ledande makt utmanas. Konkurrensen med USA omfattar alla strategiska domäner. I centrum står tillgång till högteknologi, som anses central för framtida ekonomiska och militära maktförhållanden.

Kinas mål är att bli självförsörjande till 2025 inom nyckelteknologier och all försvarsindustri. Kinas långtgående civil-militära integration och sömlösa förbindelser mellan stat, parti och näringsliv är unik. Dess lagstiftning ålägger alla medborgare, företag och organisationer att bistå underrättelse- och säkerhetsmyndigheterna. Högteknologi anskaffas genom handel, uppköp eller underrättelseverksamhet. Högteknologiska länder som Sverige är av intresse i detta sammanhang.

Belt and Road Initiative (BRI) är strukturen för Kinas strategiska expansion. BRI innebär en utveckling av globala transportsystem och infrastruktur på ett sätt som maximerar Kinas nytta och inflytande. BRI omfattar allt från hamnar och landtransport till telekom och utvinning av naturresurser. Kina har utnyttjat beroenden inom BRI för politiska, ekonomiska och ibland militära syften.

Arktis är av ökande vikt för Kinas globala ambitioner, såväl ekonomiskt som säkerhetspolitiskt. Arktis skulle kunna erbjuda ett komplement till förbindelser över Indiska Oceanen, som idag är en

avgörande livsnerv för Kina. Kina bedriver därför en omfattande verksamhet för att påverka den framtida utvecklingen av infrastruktur, transportleder och resursutvinning i Arktis. Dessa intressen sträcker sig också till Norden.

Alla Kinas försvarsgrenar genomgår en snabb och omfattande modernisering. Kinas krigsmakt ska ges en större roll i landets utrikes- och säkerhetspolitik i takt med att Kina blir en starkare global aktör. Kinas globala ambitioner understryks av att marinens utveckling är högt prioriterad, liksom cyber- och rymddomänerna.

Kina utnyttjar med allt större självförtroende en stor bredd av maktmedel för att främja sina intressen.

EUROPA

Den europeiska säkerhetsordningen är idag allvarligt försvagad. Främst undergrävs den av Rysslands försök att med kraftfulla medel påverka andra länders säkerhetspolitiska vägval. Den europeiska säkerheten försvagas även av en fortsatt urholkning av konventionell och strategisk rustningskontroll.

Pandemin utgjorde under 2020 ett nytt hot mot EU:s sammanhållning och ekonomiska stabilitet. När pandemin bröt ut agerade EU:s medlemsstater först mindre samordnat, något externa aktörer utnyttjade för att skapa och förstärka skiljelinjer inom unionen. Efter hand har EU-länderna gemensamt kommit överens om åtgärder för ekonomisk återhämtning vilket har visat på unionens handlingsförmåga.

EU:s grannskap är instabilt, inte minst i dess östliga riktning. Under 2020 fortsatte de väpnade konflikterna i östra Ukraina, Syrien och Libyen, och dessutom tillkom kriget i Nagorno-Karabach, den massiva repressionen i Belarus och spänningarna i östra Medelhavet, liksom en ökande social och politisk oro i ytterligare länder.

EU och Nato upprätthåller tvåspårspolitiken, och Nato fortsätter sin avskräckning gentemot Ryssland. För några medlemsländer är dock terrorism och sönderfallande stater i syd mer påtagliga hot. Under 2021 kommer Nato att se över sitt strategiska koncept.

Natos och EU:s sammanhållning prövas bland annat av Turkiets agerande i unionens grannskap och militära samarbete med Ryssland. I några fall under 2020 spillde detta över även på andra säkerhetspolitiska frågor och försenade ett gemensamt agerande.

Kinas betydelse för europeisk säkerhet ökar tydligt och synen på Kina har blivit mer samstämmig inom EU. Det innefattar en ökad samsyn om att ekonomiska och infrastrukturella beroenden av Kina också kan medföra allvarliga sårbarheter.

Både Nato och EU lägger större vikt på ökad samhällelig robusthet för att möta en hybrid och komplex hotbild. I en tid av geoekonomisk konkurrens förstärker EU sin förmåga att kunna hävda sina ekonomiska och teknologiska intressen. Hösten 2020 införde EU nya sanktioner mot Ryssland som svar på cyberangrepp och på förgiftningen av den ryske oppositionspolitikern Alexej Navalny.

EU:s förmåga som säkerhetspolitisk aktör påverkas av unionens framtida relation till Storbritannien. Frankrike är den mest kapabla försvarspolitiska aktören inom unionen, men landet agerar vid behov även utanför dess ram, medan Tyskland främst betonar Natos och EU:s sammanhållning.

EU signalerade i slutet av året ett intresse till USA att intensifiera de politiska och ekonomiska relationerna. Bidenadministrationen väntas ha en mycket positiv syn på Nato och EU. Dessutom har Biden höga förväntningar på transatlantiskt samarbete både i europeiska och globala säkerhetsfrågor.

Asiatisk och europeiska säkerhet kan förväntas kopplas ihop än närmare.

I Europa och västvärlden ökar antalet attentat och attentatsplaner med en våldsbejakande högerextrem motivbild. I avgränsade nätforum förstärks sympatisörers världsbild och nya anhängare rekryteras. En ökad polarisering i öppna demokratiska samhällen är även i linje med vissa statliga aktörers intressen.

Kinas betydelse för europeisk säkerhet ökar tydligt och synen på Kina har blivit mer samstämmig inom EU.

MELLANÖSTERN

Läget i Mellanöstern har under 2020 präglats av politisk turbulens, väpnade konflikter samt vissa mellanstatliga närmanden och överenskommelser. Regimer som saknar folklig förankring, utbredd korruption och fattigdom, bidrar till en konstant grogrund för uppror och instabilitet. Konflikter i Syrien, Irak och Jemen fortsätter att utkämpas av väpnade aktörer med stöd från rivaliserande regionala stormakter som Turkiet, Iran och Saudiarabien.

Mellanöstern präglas också av global rivalitet, där den amerikanska närvaron och inflytandet utmanas av främst ryska – men allt mer även av kinesiska – insteg. Covid-19 har slagit hårt mot många länder i regionen där sjukvården är undermålig och den ekonomiska utvecklingen redan innan pandemin var negativ.

I Syrien råder dödläge mellan de olika parterna och en politisk lösning på konflikten är avlägsen. I Jemen bedriver FN skytteldiplomati samtidigt som den väpnade konflikten pågår med fortsatt intensitet. Det politiska läget i Irak fortsätter att präglas av maktkamper och korruption, samtidigt som det folkliga missnöjet växer.

Konflikten mellan USA och Iran eskalerade i början av 2020 till en mycket hög nivå, något som särskilt märktes i Irak. Spänningen minskade något i takt med att det amerikanska presidentvalet i oktober närmade sig. I Libanon har den politiska och ekonomiska krisen förvärrats så till den grad att den nationella stabiliteten möjligen hotas på sikt.

USA har under 2020 medlat fram överenskommelser om att normalisera relationerna mellan Israel och fyra arabländer; Förenade Arabemiraten, Bahrain, Sudan och Marocko. I slutet av 2020 positionerade sig olika aktörer inför tillträdet av den nya amerikanska administrationen, som signalerat intresse att återinträda i kärnenergiavtalet med Iran.

Efter stora förluster fokuserar Daesh i Syrien och Irak på långsiktig överlevnad och tillväxt, men organisationen utgör fortsatt ett hot genom mer decentraliserade attacker. Daeshs ledarskap strävar efter att ge vägledning och stöd till sina undergrupperingar i Mellanöstern, Centralasien och Afrika.

Läget i Mellanöstern har under 2020 präglats av politisk turbulens, väpnade konflikter samt vissa mellanstatliga närmanden och överenskommelser.

AFRIKA

I Afrika har spridningen av covid-19 under 2020 fått en ekonomisk påverkan på såväl nationell som lokal nivå som kan bli långsiktigt delstabiliserande.

Vid sidan av de direkta hälsoeffekterna har även de ekonomiska konsekvenserna av pandemin fått en allvarlig påverkan på liv och hälsa runt om i Afrika.

Regionens militärregimer kan komma att bli än mer repressiva i sina försök att stävja denna utveckling. Inblandningen av externa aktörer i konflikten i Libyen har fortsatt under 2020. I Mali har utvecklingen gått i negativ riktning där oroligheterna under året varit koncentrerade till de centrala och norra delarna av landet, med tyngdpunkt till gränsområdet mellan Mali, Burkina Faso och Niger. Våldsbejakande islamistiska grupperingar i Sahel med lojalitet till Daesh och al-Qaida har under året ökat sin förmåga. Statskuppen och efterföljande sanktioner har medfört en spänd och osäker period för säkerhetsläget i landet utifrån ett säkerhetspolitiskt perspektiv.

Afrikas horn har erfarit stora politiska förändringar de senaste åren som gett nya regeringar i exempelvis Sudan och Etiopien. Inbördeskriget i Etiopien som utbröt under hösten 2020 har regionaliserats och innefattar även grannländerna Eritrea och Sudan såväl som lokala miliser. Regionen är alltjämt instabil och centrala frågor kring vattenförsörjning och markfördelning driver på både politiska konflikter och migration. Militariseringen av Röda havet bidrar samtidigt till ett ökat intresse för regionen hos externa aktörer, vilkas engagemang inte sällan bidrar till ökad polarisering och instabilitet. I Somalia fortsätter det strategiska dödläget i kriget mellan den somaliska regeringen och al-Shabaab.

I Stora sjöområdet är situationen stabil men fylld av konflikter, humanitära kriser och ökande våld. Externa aktörer fortsätter ha en avgörande roll i de vägval som görs och de möjligheter som ges.

I Centralafrikanska republiken slutade året med omfattande oroligheter och väpnat våld kopplat till presidentvalet.

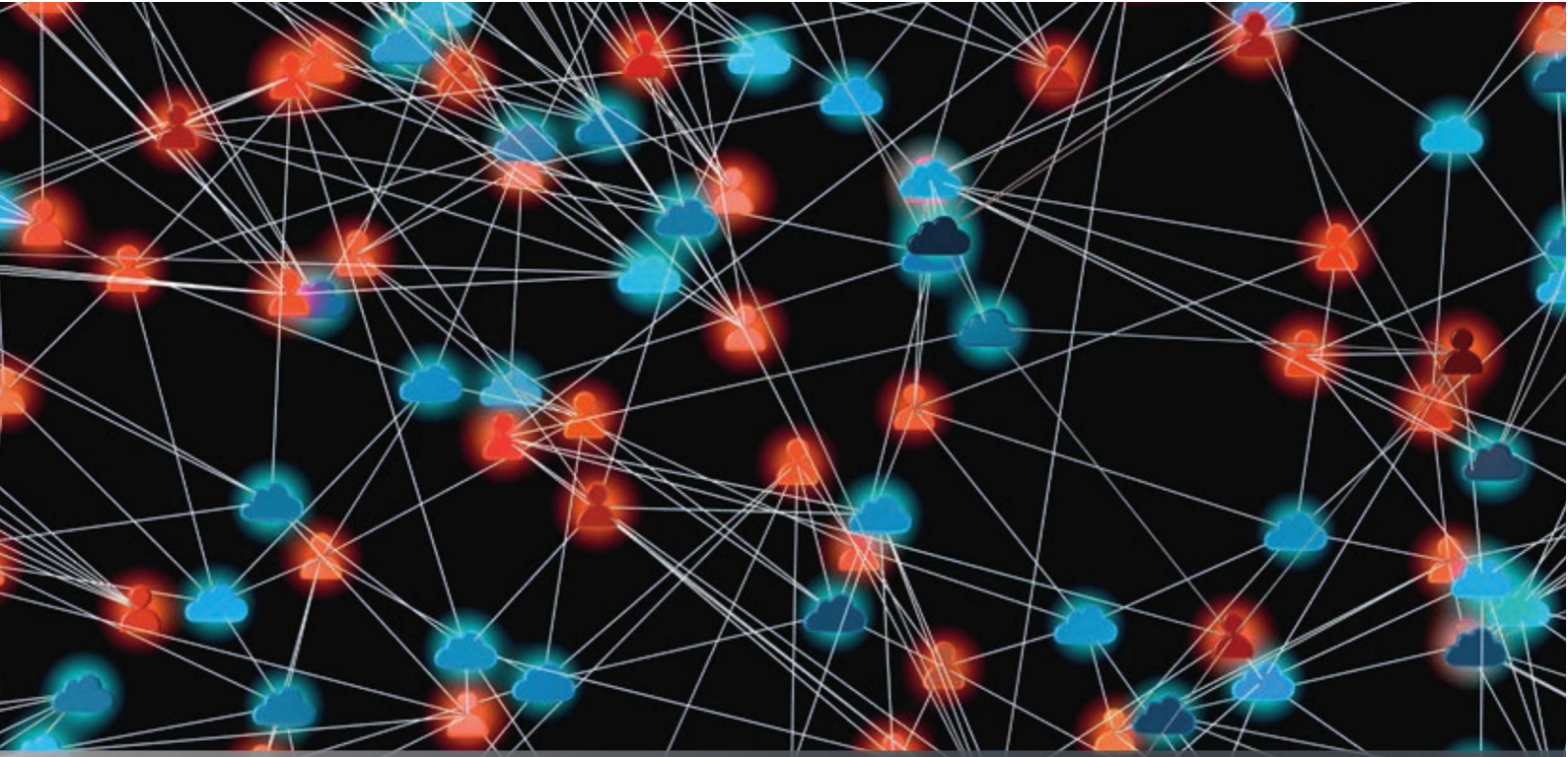
Möjligheter att lösa uppkomna regionala konflikter i södra Afrika minskar delvis till följd av att Sydafrikas interna utmaningar ökar och externa förmåga minskar. Daeshs ökade aktivitet i sydöstra Afrika och kontakterna mellan nätverk i olika länder utgör ett regionalt säkerhetsproblem.

En försämrad säkerhetssituation, klimatförändringar, terrorism och ett minskande demokratiskt utrymme i allt fler länder ger upphov till väpnade konflikter och flyktingströmmar.

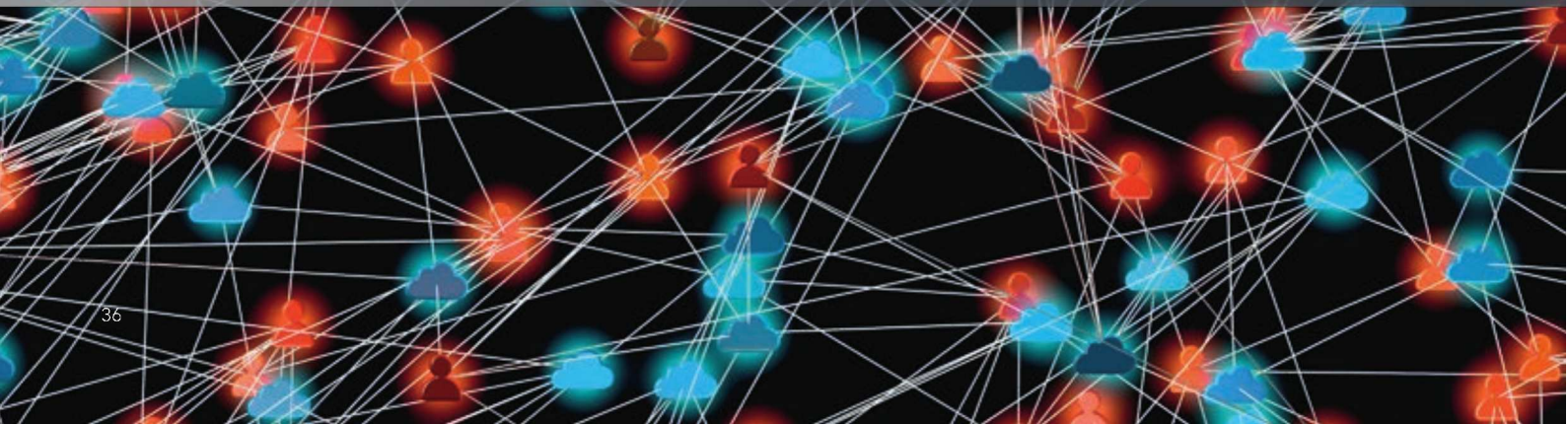
Hotbilden mot Sverige i tio punkter

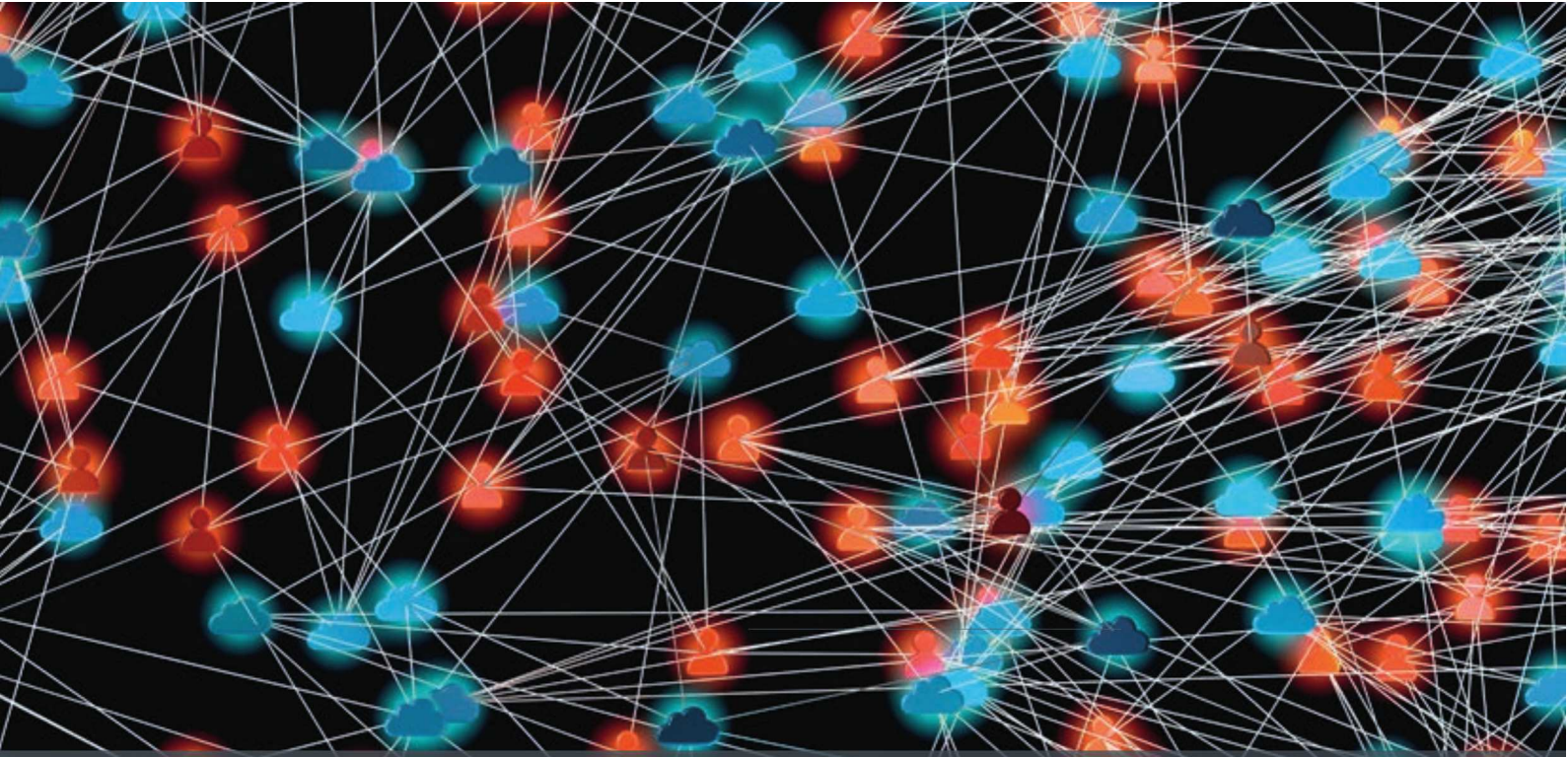
Hotbilden mot Sverige påverkas av en snabbt föränderlig omvärld med allt fler konfliktytor. Den består av en bred och alltmer komplex uppsättning hot. Hoten utmanar många traditionella föreställningar om konflikters natur och om gränserna mellan militärt och civilt, cyber och fysiska domäner, krig och fred, och mellan vår yttre och inre säkerhet. Länder som Ryssland och Kina kan samordnat utnyttja hela spektret av sitt samhälles resurser för att nå sina målsättningar.

- **En försvagad internationell ordning**. Under 2020 har utvecklingen mot en mer hårdhänt maktpolitik förstärkts, globalt och i Europas grannskap. Must bedömer att risken i denna miljö är förhöjd både för konflikter som indirekt påverkar Sverige och för att Sverige utsätts för kraftfulla påtryckningar.
- **En breddad hotbild.** Hotbilden mot Sverige är idag samtidigt politisk, ekonomisk och militär. Det handlar inte om ”antingen eller” utan om ”både och”. Det är två sidor av samma mynt att ett väpnat angrepp mot Sverige inte kan uteslutas och att yttre hot allt oftare manifesteras i vår inre säkerhet.
- **En mer komplex hotbild.** Must ser allt fler kopplingar mellan olika hotområden och att antagonister verkar med samordnade paket av åtgärder. Till komplexiteten hör att ett enskilt antagonistiskt agerande kan ha flera samtidiga syften och riktas mot vår säkerhet, vårt välstånd och vår demokrati.
- **Dolda, förnekbara och tvetydiga metoder.** Motståndaren vill inte att vi ska upptäcka ett antagonistiskt agerande i tid eller veta vem som ligger bakom. Två exempel på sådana metoder är cyber- och påverkansoperationer. Man vill försvåra vårt beslutsfattande och försvaga vår tro på vår egen förmåga.
- **Icke-linjära hot i alla konfliktnivåer.** Många av hoten förekommer i såväl fred som kris och krig. Om främmande makt under kalla kriget hade en strömbrytare, så arbetar man idag med en dimmer för att höja eller sänka konfliktnivån. Hoten är alltså inte linjära.
- **Ett väpnat angrepp kan inte uteslutas.** Rysslands agerande över tid har orsakat ett försämrat säkerhetsläge i Sveriges närområde. Den militära aktiviteten i närområdet har fortsatt att öka i omfattning och i komplexitet. Huvudsyftet är ömsesidig avskräckning och kapacitetsuppbyggnad.
- **Samhällskritisk infrastruktur ett centralt mål.** Främmande makt strävar målmedvetet efter insteg i vår digitala och fysiska infrastruktur. Syftet kan vara att använda dessa för politisk påverkan i fred, för att skapa oro i ett krisläge, eller för att försvåra våra försvarsansträningar i krig.
- **Ekonomi och teknologi.** Stormakterna ser allt mer teknologi och ekonomi som integrerade delar av sin nationella säkerhet. För ett högteknologiskt och exportberoende land som Sverige kan trenden medföra hot mot vår konkurrenskraft, vår försvarsförmåga och vårt självständiga beslutsfattande.
- **Högt hot från främmande underrättelseverksamhet.** De ryska och kinesiska underrättelse- och säkerhetstjänsterna är centrala och resursstarka aktörer. Must bedömer att hotet från främmande underrättelseverksamhet fortsatt är förhöjt.
- **Våldsanvändning i fred.** Ryssland bär ansvar för en rad våldsdåd i Europa de senaste åren, till exempel i Salisbury 2018, i Berlin 2019 och i Omsk 2020. Aktörer inom den ryska staten var inblandade i ett mordförsök i Gävle under 2020, enligt tingsrättens dom (som när detta skrivs har överklagats).

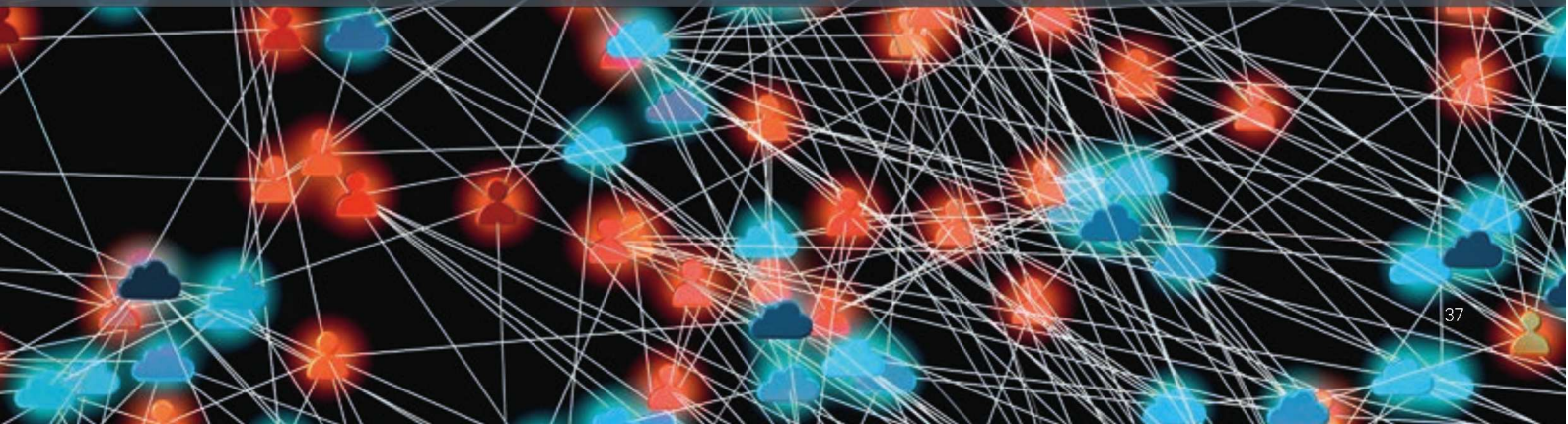


Must som den civila och militära underrättelsetjänst, och den militära säkerhetstjänst, som arbetar med de yttre hoten mot Sveriges säkerhet – oavsett vilka de är.





MUSTS UPPDRAG OCH VERKSAMHET



MUSTS UPPDRAG OCH VERKSAMHET

Must bedriver försvarsunderrättelseverksamhet och militär underrättelse- och säkerhetstjänst där uppdraget är att identifiera och analysera de yttre hot som riktas mot Sverige och svenska intressen. Verksamheten syftar till att ge underlag till stöd för svensk utrikes-, försvars- och säkerhetspolitik och i övrigt kartlägga yttre hot mot Sverige, samt att förebygga, upptäcka och motverka de säkerhetshot som riktas mot Försvarsmakten och dess intressen i Sverige och utomlands.

Musts verksamhet regleras av lagar och förordningar samt av årliga inriktningar från regeringen och överbefälhavaren. Musts verksamhet fyller en viktig roll i Sveriges försvars- och krisberedskap och ger Sverige förutsättningar att föra en självständig utrikes-, försvars- och säkerhetspolitik. Genom att leda och utveckla funktionen underrättelse- och säkerhetstjänst inom Försvarsmakten bidrar Must till ett starkare försvar.

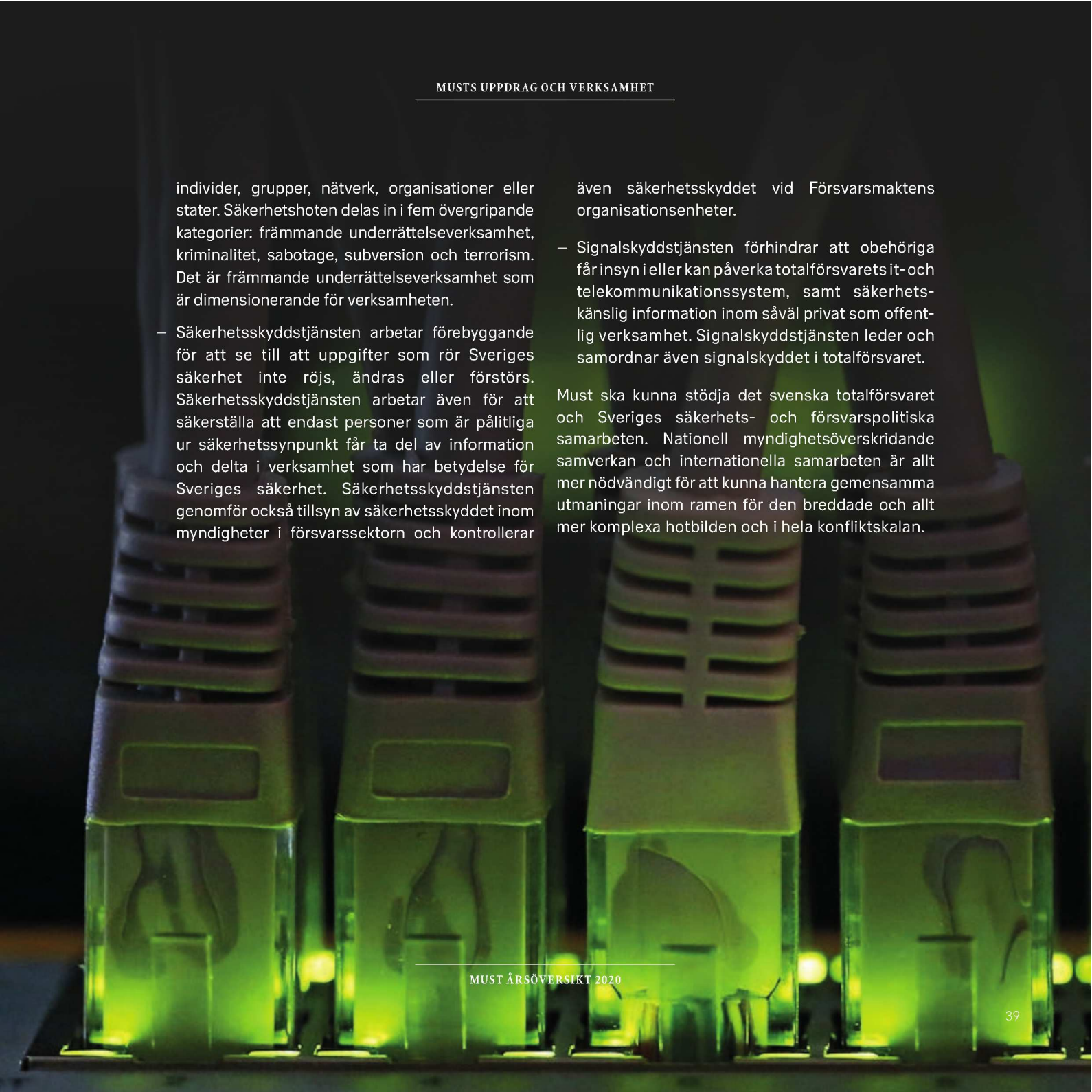
De delar av Must som arbetar med underrättelsetjänst inhämtar, bearbetar, analyserar och delger information och bedömningar om olika aktörers avsikter och förmågor. Must följer både den säkerhetspolitiska och militära utvecklingen i närområdet, Försvarsmaktens insatsområden och utvecklingen i andra regioner som är av betydelse för svensk utrikes-, säkerhets- och försvarspolitik. Must följer också gränsöverskridande fenomen och förmågor som direkt eller indirekt påverkar Sveriges säkerhet och svenska ställningstaganden. Must är därmed både en civil och en militär underrättelse- och säkerhetstjänst.

Merparten av underrättelsetjänstens analyser och bedömningar görs som stöd till regeringen enligt regeringens inriktning. Underlagen syftar till att stödja beslutsfattande och stärka lägesuppfattningen, primärt vid utrikes- och försvarsdepartementen. Mot bakgrund av att dagens hotbild är både bredare och mer komplex behöver även fler intressenter i regeringskansliet, direkt eller indirekt, få tillgång till Musts analyser och bedömningar.

Vidare bidrar Must med kunskap och personal till Försvarsmaktens internationella militära operationer. Musts verksamhet ger även stöd till Försvarsmaktens långsiktiga förmågeutveckling, försvarsplanering och operativa planering. I Musts uppdrag ingår även att leda och samordna Sveriges försvarsattachéer.

Den militära säkerhetstjänstens uppgift är att förebygga, upptäcka och motverka säkerhetshot som riktas mot Försvarsmakten och dess intressen i Sverige och utomlands samt mot försvarssektorns skyddsvärden. Verksamheten bedrivs inom tre huvudsakliga verksamhetsområden:

– Säkerhetsunderrättelsetjänsten klarlägger den säkerhetshotande verksamhetens omfattning, inriktning, medel och metoder samt motverkar desamma. Med säkerhetshot menas hot från



individer, grupper, nätverk, organisationer eller stater. Säkerhetshoten delas in i fem övergripande kategorier: främmande underrättelseverksamhet, kriminalitet, sabotage, subversion och terrorism. Det är främmande underrättelseverksamhet som är dimensionerande för verksamheten.

– Säkerhetsskyddstjänsten arbetar förebyggande för att se till att uppgifter som rör Sveriges säkerhet inte röjs, ändras eller förstörs. Säkerhetsskyddstjänsten arbetar även för att säkerställa att endast personer som är pålitliga ur säkerhetssynpunkt får ta del av information och delta i verksamhet som har betydelse för Sveriges säkerhet. Säkerhetsskyddstjänsten genomför också tillsyn av säkerhetsskyddet inom myndigheter i försvarssektorn och kontrollerar även säkerhetsskyddet vid Försvarsmaktens organisationsenheter.

– Signalskyddstjänsten förhindrar att obehöriga får insyn i eller kan påverka totalförsvarets it- och telekommunikationssystem, samt säkerhetskänslig information inom såväl privat som offentlig verksamhet. Signalskyddstjänsten leder och samordnar även signalskyddet i totalförsvaret.

Must ska kunna stödja det svenska totalförsvaret och Sveriges säkerhets- och försvarspolitiska samarbeten. Nationell myndighetsöverskridande samverkan och internationella samarbeten är allt mer nödvändigt för att kunna hantera gemensamma utmaningar inom ramen för den breddade och allt mer komplexa hotbilden och i hela konfliktskalan.

SVERIGE BEHÖVER EN STARK UNDERRÄTTELSE- OCH SÄKERHETSTJÄNST

Tillsammans höjer vi garden – Must, FRA och Säkerhetspolisen

Samverkan har inte tagit paus under pandemin. Visst har det vidtagits åtgärder – handsprit, munskydd och plexiglasskärmar har blivit vardag. Och vissa möten sker på krypterad videokonferens. Men annars fortlöper arbetet precis som vanligt och cheferna för Must, FRA och Säkerhetspolisen träffas löpande och känner varandra väl.

– Det kommer naturligt när vi träffas så pass ofta och i så viktiga frågor, säger Lena Hallin, chef för Must. Den breddade och allt mer komplexa hotbilden tar inte hänsyn till våra administrativa gränser, snarare tvärtom. Motståndaren försöker ständigt hitta luckor i vår lagstiftning eller på annat sätt utnyttja otydligheter i myndighetsansvar.

Klas Friberg, chef för Säkerhetspolisen, konstaterar att Sveriges säkerhet är en gemensam angelägenhet och poängterar:

Björn Lyrvall, generaldirektör för FRA, Lena Hallin, chef för Must, och Klas Friberg, chef för Säkerhetspolisen, möts ofta för samverkan i både aktuella och långsiktiga frågor..

– Vi har ett säkerhetsläge som innebär att fler behöver göra mer. Det breddade hotet måste mötas på bred front. Såväl den strategiska politiska nivån, våra myndigheter som näringslivet behöver prioritera säkerhet högre.

Ett företagsuppköp kan affärsmässigt vara helt legitimt. Men det kan också vara ett sätt att få tillgång till samhällskritisk infrastruktur som i sin tur kan utnyttjas för politiska påtryckningar i fred, samhällspåverkan i kris eller för att skada Sverige i krig.

Detta är ett exempel på den breddade och allt mer komplexa hotbild Sverige har att hantera. Tillvägagångssätten är avancerade och hotaktörerna använder sig av hela spektret av sina samhällens resurser och de har en väl utvecklad förmåga att samordna olika medel.

Det är i ljuset av detta som den fördjupade samverkan mellan Säkerhetspolisen, FRA och Försvarsmakten ska ses.

Björn Lyrvall, generaldirektör för FRA poängterar att cyberarenan blir allt viktigare för de stater som vill skada Sverige.

– Den snabba teknikutvecklingen skapar inte bara möjligheter, utan innebär även sårbarheter som måste hanteras. Och det är genom utbyte av information vi kan höja garden.

Det nya Nationella cybersäkerhetscentret där ytterligare fyra myndigheter ingår är ett exempel på den fördjupade samverkan inom cyberdomänen.

Men FRA:s signalspaning är bredare än så och en mycket viktig informationskälla för både Säkerhetspolisen och Försvarsmakten, eller som Lena Hallin uttrycker det:

– FRA:s inhämtning och rapportering i kombination med vår egen underrättelseinhämtning ger avgörande information när vi lägger pusslet om den hotbild som Sverige är utsatt för. Det här kretsloppet av information mellan FRA, Säkerhetspolisen och Must är ovärderligt för Sveriges säkerhet.

Samverkan i all ära. Samtidigt framhåller de tre myndighetscheferna gemensamt hur viktigt det är att varje myndighet samtidigt bibehåller sin integritet.

– Stuprör behövs även om hängrännorna både kan stärkas och breddas. Att dela information får aldrig ske slentrianmässigt säger Björn Lyrvall.

Klas Friberg menar att det är viktigt att komma ihåg att viss information inte heller ska delas mellan myndigheterna, utan det är rätt information som ska delas.

– Vi har olika lagstiftning att förhålla oss till och det är en styrka. Det håller oss alerta, bidrar till en sund konkurrens och stärker ett kritiskt förhållningssätt. Det är sällan svart eller vitt, och underrättelse- och säkerhetstjänst handlar mycket om att hantera osäkerheter för att kunna bedöma hot och risk. Ett nära samarbete med bibehållen integritet stärker Sveriges oberoende och säkerhet, säger Lena Hallin.

STÄLLFÖRETRÄDE CHEF FÖR MUST: HÖGA KRAV PÅ MUSTS ANPASSNINGSFÖRMÅGA

Daniel Olsson är ställföreträdande chef för Must. Han betonar att de snabba omvärldsförändringarna och den sammansatta hotbilden ställer höga krav på den militära underrättelse- och säkerhetstjänstens anpassningsförmåga.

– Musts verksamhet utgår alltid från hotbilden och förändras i takt med den. Kärnan i vårt uppdrag är att kartlägga yttre hot mot Sverige, oavsett var och hur dessa materialiseras.

– Vi måste tidigt förstå hur grundläggande geopolitiska och teknologiska förändringar kan påverka hotbilden. Och i en kris ska vi växla tempo och kraftsamla för att möta uppdragsgivarnas behov. Det är en skarp verksamhet för Sveriges säkerhet.

Pandemin, utvecklingen i Belarus och kriget i Nagorno-Karabach är exempel på kriser som krävt en snabb anpassning av Must under 2020, liksom uppbyggnaden av Musts förmåga att tillämpa den nya lagen om elektronisk kommunikation som trädde i kraft 1 januari 2020.

– Den unika expertis som Musts personal har byggt upp under lång tid är en nationell tillgång. Vi är bra på att använda den flexibelt och vi kan dansa med det oväntade när det behövs.

Daniel Olsson konstaterar att samtidigt som ett väpnat angrepp inte kan uteslutas, så kommer de yttre hoten mot Sverige allt oftare till uttryck även i den inre säkerheten.

– Hotbilden ställer allt högre krav på oss att arbeta sömlöst och integrerat. Det gäller både internt inom Must och i vårt samarbete med aktörer i alla delar av samhället.

Det finns antagonistiska aktörer som samordnat kan dra på resurser från alla delar av sitt samhälle för att uppnå sina mål. De försöker utnyttja luckor i svensk samordning, organisation och lagstiftning.

Daniel Olsson, Ställföreträdande chef Must.

– När tvetydighet och förnekbarhet är angriparens strategi är det viktigare än någonsin att vi kan pussla samman den kunskap som finns inom både underrättelse- och säkerhetstjänsten till en så tydlig helhetsbild som möjligt.

För att kunna göra det måste Must delge underrättelser till en bredare krets av mottagare än tidigare och samtidigt hämta in kunskap om incidenter och säkerhetshot från fler samhällsaktörer.

– Våra uppdragsgivare i regeringen och Försvarsmakten hanterar komplexa och svåra beslutssituationer. Must kan sällan ta bort osäkerheterna, men vi hjälper till att minska dem.

Daniel Olsson betonar vikten av en samlad nationell ansats för att möta de alltmer komplexa hoten och att Must är aktivt för att stärka Sveriges samlade förmåga.

– Kunskap är vår första försvarslinje. Våra underrättelser hjälper andra att kunna vidta åtgärder som höjer tröskeln för en angripare, både militärt och civilt.

Många av hoten kan riktas mot Sverige i såväl fred som kris och krig. Det utmanar traditionella föreställningar om olika konflikternas karaktär. Antagonistiska aktörer använder idag bildligt talat en dimmer, för att snabbt kunna skruva upp och ned konfliktnivån.

– Ett väpnat angrepp är det allvarligaste hotet, men de troligaste angreppen är hybrida och ickelinjära. Must anpassar sin verksamhet för att kunna hantera hela den skalan. Vi kartlägger och motverkar hybrida hot mot Sverige varje dag.

Utveckling handlar inte bara handlar om förutseende och bättre samarbeten, utan också om organisationens kultur. Underrättelsehistorien saknar inte varnande exempel på politisk opportunism, grupptänkande eller oförmåga att granska invanda föreställningar.

– Integritet och konsekvensneutralitet är A och O för Must. Vi måste alltid lyfta fram också osäkerheter och motsägelser, och vara de första att ifrågasätta våra tidigare bedömningar.

Försvarsmakten är en del av det nya nationella cybersäkerhetscentret som ska stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige.

UNDERRÄTTELSE- OCH SÄKERHETSTJÄNST ÄR EN LAGSPORT

NATIONELLT SAMARBETE – GRÄNSÖVERSKRIDANDE HOT KRÄVER GRÄNSÖVERSKRIDANDE SAMVERKAN

Under året har det nationella samarbetet utvecklats ytterligare. Must företräder Försvarsmakten som medlem i flera externa samverkansorgan och samarbeten.

För att möta en breddad och allt mer komplex hotbild är samverkan på bred front mellan myndigheter, men också med näringslivet, ännu viktigare än tidigare. Must samverkar med ett stort antal myndigheter varav Säkerhetspolisen och Försvarets radioanstalt (FRA) har en särställning.

Alla myndigheter har skilda ansvar och expertområden men bara genom att arbeta tillsammans går det att förebygga, upptäcka och motverka säkerhetshoten effektivt och göra det svårt för en motståndare. Detta oavsett om det gäller att följa den utrikes-, försvars- eller säkerhetspolitiska utvecklingen.

Samverkan är extra viktigt när det kommer till de så kallade hybrida eller icke-linjära hoten. Det kan röra sig om allt från otillbörlig påverkan, cyberangrepp och värvning av agenter till försök att tillskansa sig teknik med olagliga metoder eller uppgifter om olika aktörers intentioner och ställningstagande.

Några exempel på mer formaliserade samverkansforum är NCT (Nationellt centrum för terrorhotbedömningar) och det nystartade nationella cybersäkerhetscentret.

Nationellt cybersäkerhetscenter ska stärka motståndskraften mot cyberangrepp

Den snabba teknikutvecklingen och en breddad och allt mer komplex hotbild har skapat sårbarheter som kräver ett samordnat agerande inom cyberområdet och en stärkt offentlig/privat samverkan. Mot den bakgrunden beslutade därför regeringen den 10 december att inrätta ett nationellt center för cybersäkerhet.

I centret ingår utöver Försvarsmakten (Must och Försvarsmaktens CIO-avdelning) även Försvarets radioanstalt (FRA), Myndigheten för samhällsskydd och beredskap (MSB) och Säkerhetspolisen. Centret kommer även ha en nära samverkan med Försvarets materielverk (FMV), Polismyndigheten och Post- och telestyrelsen (PTS) som också ska ges möjlighet att medverka i centrets verksamhet.

Det övergripande målet enligt regeringen är att med cybersäkerhetscentret stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige. Samverkan med privata och offentliga aktörer ska utgöra en central del av uppdraget i syfte att stärka cybersäkerheten i samhället.

Redan innan inrättandet av centret publicerades två myndighetsgemensamma rapporter för att

uppmärksamma cyberhotet och sprida kunskap om säkerhetsskyddsåtgärder. Den ena rapporten beskriver cybersäkerhetsrelaterade hot och genom exempel från verkligheten och den andra ger rekommendationer om hur man praktiskt går tillväga för att bygga en säkrare IT-miljö.

Centret signalerar en tydlig nationell ansats och det kommer fullt utbyggt att stärka förutsättningarna för att möta den nya hotbilden och ytterligare stärka den goda myndighetssamverkan som finns idag. Centret kommer att skapa mervärden genom att bland annat förmedla råd och stöd avseende hot, sårbarheter och risker för samhället i sin helhet samtidigt som det direkt kommer att bidra till Försvarsmaktens ordinarie uppgifter inom cyberområdet.

Det ska emellertid understrykas att ett center inte löser allt. Att skydda sig mot cyberangrepp från kvalificerade aktörer är en nationell angelägenhet, och alla samhällets aktörer måste hjälpas åt.

Läs mer om Nationellt cybersäkerhetscenter:
www.cfcs.se

Lagarbete stärker skyddet för det svenska 5G-nätet

Ett 5G-nät som går att lita på. Det har varit ledstjärnan i förarbetet till den utauktionering av 3,5 och 2,3 GHz-banden som förbereddes under hösten 2020 och som Must varit en del av.

Många samhällsfunktioner kommer att vara uppkopplade mot 5G-nätet. Det skapar möjligheter, men också stora sårbarheter som måste hanteras.

5G kommer att ha en avgörande inverkan på hela samhällsutvecklingen. Miljontals verksamheter och apparater kommer inom de närmaste åren att vara uppkopplade mot internet, så kallat sakernas internet (internet of things).

Denna utveckling är positiv, men det finns risker som måste hanteras. För att Sverige ska kunna digitaliseras är säkerheten helt avgörande. Det måste gå att lita på att information i nätet – liksom själva nätet – inte styrs, manipuleras eller missbrukas av utomstående.

Regeringen har gjort bedömningen att 5G-nätet ska betraktas som säkerhetskänslig verksamhet med stor betydelse för Sveriges säkerhet.

Som en följd av detta infördes en förändring i lagen om elektronisk kommunikation (LEK) i 1 januari 2020. Den innebär att Post- och telestyrelsen (PTS) har skyldighet att samråda med Försvarsmakten och Säkerhetspolisen för att bedöma om radioanvändningen skulle kunna orsaka skada för Sveriges säkerhet.

För att tydliggöra hur elektroniska kommunikationsnät ska utformas så att det uppfyller det skydd som är nödvändigt har Must och Säkerhetspolisen under året bidragit med kunskap om säkerhetshotande verksamhet.

Därutöver har ett antal principer tagits fram. De handlar bland annat om att nätet ska fungera även om anslutningar till utlandet bryts och att det ska utformas så otillåten kartläggning av tjänster, kapacitet, lokalisering och användare förhindras. De handlar även om att säkerställa att information i nätet inte kan styras, manipuleras eller göras otillgängligt av utomstående aktörer.

Sammantaget handlar det om att identifiera och minimera risker som kan uppstå längre fram när 5G-nätet är utbyggt. En aktör med fel avsikter men med kontroll över 5G-nätet skulle kunna orsaka stor skada för Sveriges säkerhet.

Diskussionen om säkerheten i 5G-näten är just nu aktuell i ett flertal länder. Musts bedömning av säkerhetshoten mot Sverige är dock helt oberoende av andra aktörer eller de beslut andra länder fattat. Det är Sveriges nationella säkerhet som är i fokus.

Nationellt centrum för terrorhotbedömning

Vid Nationellt centrum för terrorhotbedömning (NCT), som är en permanent arbetsgrupp med personal från Must, Säkerhetspolisen och FRA har samarbetet ytterligare fördjupats. Under året har ett gemensamt it-system införts vilket ytterligare kommer att stärka analyskraften och effektiviteten.

NCT:s uppgift är att göra strategiska bedömningar av terrorhotet mot Sverige och svenska intressen utomlands på kort och lång sikt. NCT gör även analyser av händelser, trender och omvärldsutveckling med koppling till terrorism som berör eller kan komma att beröra Sverige och svenska intressen.

Bedömningarna delges delar av Regeringskansliet samt myndigheter som ingår i Samverkansrådet mot terrorism och syftar till att ge tidig förvarning

om förändringar som kan påverka hotbilden mot Sverige och svenska intressen och som kan kräva åtgärder. Samarbetet ger större möjligheter att ta tillvara den samlade kompetensen som finns vid Must, Säkerhetspolisen och FRA.

INTERNATIONELL SAMVERKAN

Att samarbeta internationellt är en naturlig del för underrättelse- och säkerhetstjänster, i syfte att stärka gemensam förmåga att bedöma och förutse komplexa säkerhetspolitiska händelser, på både kort och lång sikt. Att hjälpa och få hjälp är fundamentet i det internationella samarbetet och Must behöver en välfungerande och god relation till sina motparter.

Att samarbeta och dela med sig av kunskap, nya perspektiv och bedömningar till utländska underrättelse- och säkerhetstjänster och deras experter ger ett mervärde för både Must och dess motparter och bidrar till att Must kan delge unika underlag till sina uppdragsgivare.

Att bidra till multilaterala samarbeten är av stor vikt för Must och stärker Sveriges roll i EU och världen.

Musts medarbetare, med i många fall unika kompetenser, är en högt värderad partner internationellt. Must samarbetar både inom utveckling av nya förmågor, inom specifika bearbetningsområden samt inom projekt för exempelvis ökad rekrytering och teknikutveckling.

Att fortsätta utveckla och bidra till de multilaterala samarbetena som exempelvis finns inom EU är av stor vikt för Must, både när det gäller att delge underrättelser och kunskap och genom bemanning av analytiker och stabsofficerare. Det stärker Sveriges roll i EU. Att bedöma och förutse hur säkerhetsutvecklingen utvecklas i Europas intresseområden gör att EU förbättrar förmågan till gemensamt agerande och stärker därmed EU.

MUSTS STÖD TILL INTERNATIONELLA INSATSER

Musts förbandsdel Nationella underrättelseenheten (NUE) ansvarar för Musts stöd till Försvarsmaktens internationella operationer. Inför, under och efter en militär operation stödjer Must med underrättelser och säkerhetshotbedömningar på alla nivåer – från stridsfältet till politisk nivå.

Must sänder ut personal från NUE till insatsområdena för att stödja svenska och multinationella chefer. Must gör hotbedömningar mot Försvarsmaktens skyddsvärden och bedömningar avseende utvecklingen av konflikterna som stöd till genomförandet av den svenska säkerhetspolitiken och till Försvarsmaktens planering.

Musts underlag har under 2020 bidragit till en rad olika nationella avdömningar och beslut, till exempel vad gäller fortsatt utveckling av Försvarsmaktens styrkebidrag och hur personal ska agera ur säkerhetssynpunkt i insatsområdena.

Under 2020 har NUE haft personal i bland annat Irak, Somalia, Mali, Afghanistan och Centralafrikanska republiken. NUE:s deltagande i olika internationella insatser ger synergieffekter då till exempel terrorgrupperna Daesh och al Qaida är aktiva i flera av insatsområdena. Under 2020 har information inhämtad i ett område kunnat bekräfta en hypotes Must haft i ett annat område vilket lett till bättre underlag för beslut inom både Regeringskansliet och Försvarsmakten.

Svenska soldater i Mali under förberedelser och ordergivning inför en kommande patrull

FÖRSVARSATTACHÉVERKSAMHETEN

Sveriges försvarsattachéer utgör en viktig tillgång för Sveriges utrikes-, säkerhets- och försvarspolitik. Attachéerna representerar Sverige och Försvarsmakten och bidrar genom sitt arbete till väl fungerande relationer och samarbeten mellan Sverige och andra länder. Attachéernas kunskap om de länder de arbetar i och den öppna informationsinhämtning som de bedriver stärker även Musts förmåga att göra bedömningar och bidra till tidig förvarning.

Försvarsattachéer är officerare med gedigen erfarenhet från olika delar av Försvarsmakten. De erfarenheter som attachéerna får under tjänstgöringstiden är värdefulla och efter avslutad tjänst kan dessa erfarenheter bidra till Försvarsmaktens utveckling. Därför ser Must gärna att en attachétjänstgöring sker i mitten av karriären.

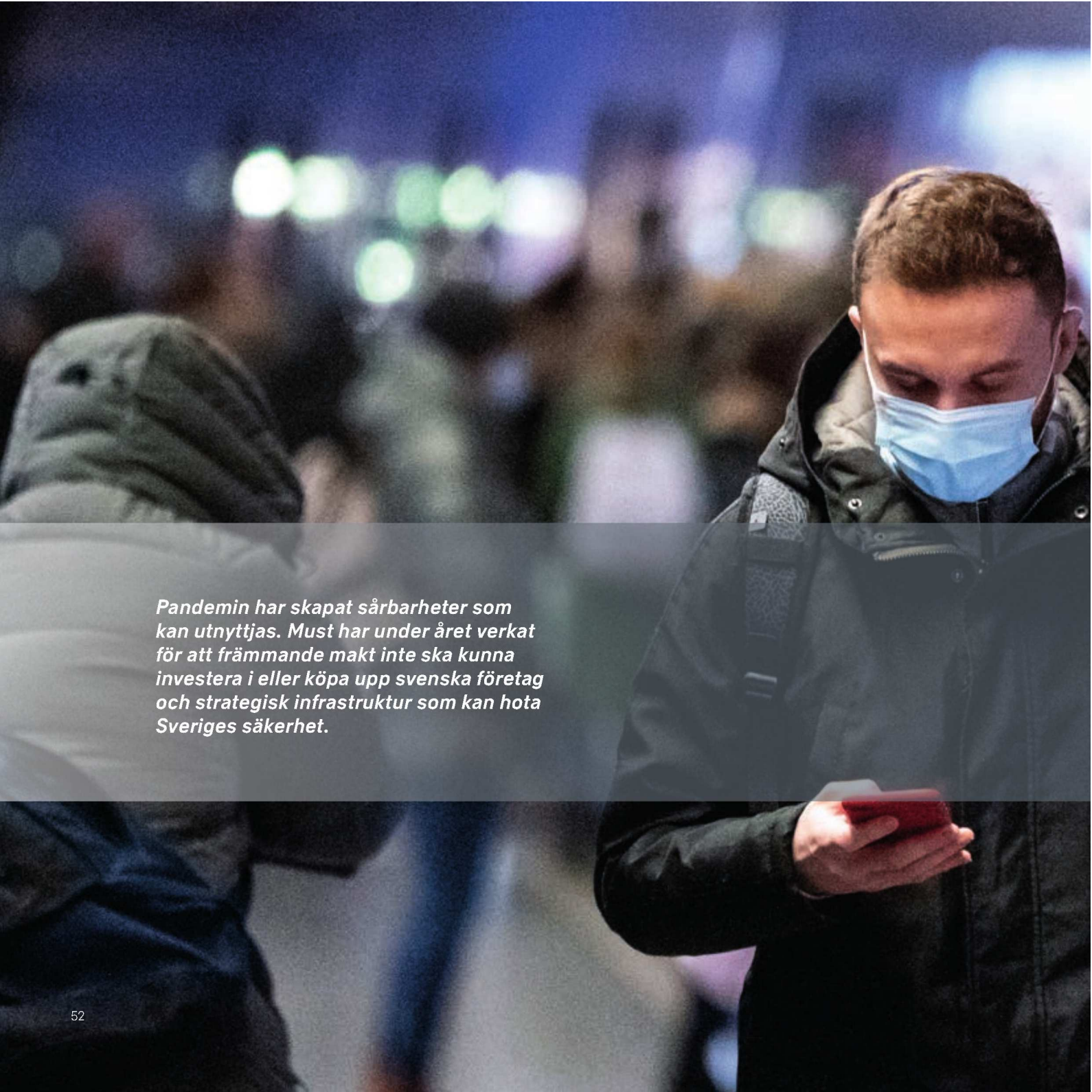
En försvarsattachés uppgifter omfattar öppen informationsinhämtning som innebär att följa och bedöma den försvarsrelaterade utvecklingen i landet och rapportera om denna. En försvarsattaché ska även stödja till exempel vid bilaterala möten, förberedelser för gemensamma operationer och övningar. Försvarsavdelningarna är samlokaliserade med ambassaderna i respektive land. Ett nära samarbete med ambassadören och övriga delar av den svenska ambassaden är av stor betydelse för attachéns arbete. Attachén är också rådgivare åt ambassadören i militära frågor.

I uppdraget som försvarsattaché ingår även att biträda svenska myndigheter och företag i frågor som berör materielsamarbeten och exportstöd. Attachén stödjer även företrädare för det svenska totalförsvaret i samband med besök.

Försvarsattachéorganisationen omfattar 26 försvarsavdelningar med 30 försvarsattachéer och tre resande försvarsattachéer.

En försvarsavdelning kan ha ett eller flera länder sidoackrediterade. Sammantaget är Försvarsmakten på detta sätt representerad i 65 länder.

Försvarsattachéerna lyder under ÖB och chefen för Must.



Pandemin har skapat sårbarheter som kan utnyttjas. Must har under året verkat för att främmande makt inte ska kunna investera i eller köpa upp svenska företag och strategisk infrastruktur som kan hota Sveriges säkerhet.

MILITÄRA SÄKERHETS-TJÄNSTEN UNDER 2020

MILITÄRA SÄKERHETSTJÄNSTEN UNDER 2020

Militära säkerhetstjänsten kan se tillbaka på ett annorlunda och intensivt år där pandemin ytterligare har visat på behovet av ett väl utvecklat säkerhetsskydd.

Hotet från främmande underrättelsetjänster är högt – fyra på en femgradig skala – omfattande och pågår här och nu.

Främmande makt ägnar sig åt närmanden, informationsinhämtning och påverkan i och mot Sverige och Försvarsmakten. Framförallt allt är det de ryska och kinesiska underrättelse- och säkerhetstjänsterna som är centrala hotaktörer, i egen kapacitet och via ombud.

Inhämtning genom tekniska hjälpmedel är ett allvarligt och konkret hot mot Försvarsmakten och Försvarsmaktens intressen. Både Ryssland och Kina har en mycket god förmåga att utföra komplexa dator- och nätverksoperationer exempelvis cyberattacker och intrång i it-system. Verksamheten bedrivs metodiskt, långsiktigt och i industriell skala. Under de senaste åren har Kinas sedan tidigare goda cyberförmåga ökat ytterligare, både kvalitativt och kvantitativt.

Den information som hotaktörerna vill komma åt finns ofta lagrad digitalt och teknisk inhämtning så som, till exempel signalspaning och cyberattacker, är därför både personal- och kostnadseffektivt.

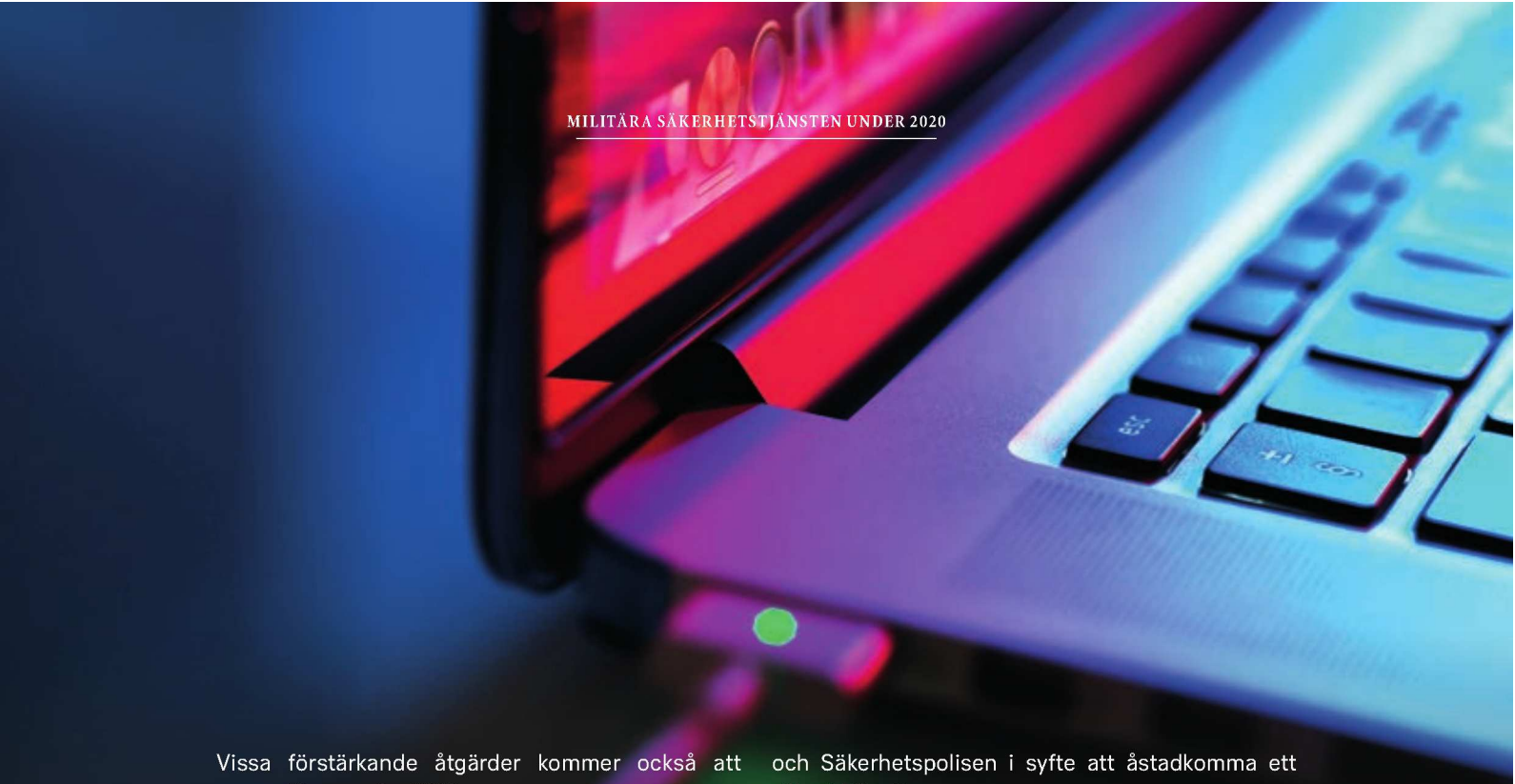
Rekognosering av Försvarsmaktens IT-system sker regelbundet, både från enskilda och kvalificerade, statliga aktörer. Teknisk inhämtning sker även mot industrin och Försvarsmaktens leverantörer i syfte att hitta den svagaste länken för att komma åt försvarsrelaterad information.

Hotaktörerna är inte bara intresserade av att komma över säkerhetskänslig information. Ett minst lika stort, och ökande hot, är intrången och kartläggningen av vår it-infrastruktur som syftar till att kunna förvanska information eller slå ut samhällsviktig infrastruktur om behov uppstår.

För att möta den förhöjda säkerhetshotbilden har Must och den militära säkerhetstjänsten arbetat aktivt på en mängd områden och åtgärder. Den 1 juni infördes en rekommendation för all personal att undvika resor till Ryssland, Kina och Iran. Syftet är att skydda medarbetarna mot säkerhetshot och att skydda Försvarsmaktens skyddsvärden.

Pandemin har skapat oro för att främmande makt ska ta tillfället i akt och investera i eller köpa upp svenska företag och strategisk infrastruktur som kan hota Sveriges säkerhet. Här har Must bidragit till att hitta lösningar och från 1 januari 2021 krävs samråd från Must och Säkerhetspolisen innan överlåtelse av säkerhetskänslig verksamhet får ske.

Under året har säkerhetstjänsten också deltagit i en översyn av de regelverk och styrningar som gäller för säkerhetsprövning, rekrytering och anställning. Översynen har visat att reglerna är tillräckliga, men att de ständigt måste kontrolleras och följas upp.



Vissa förstärkande åtgärder kommer också att genomföras under 2021.

Sedan 1 januari 2021 finns det första reglementet i säkerhetstjänst på plats. Det är en milstolpe i arbetet med att omsätta säkerhetsskyddslagen från 2018. Reglementet tydliggör vad som gäller internt inom myndigheten och kompletterar bland annat Försvarsmaktens föreskrifter om säkerhetsskydd liksom säkerhetsskyddsförordningen.

Den breddade och allt komplexare hotbilden måste mötas med en bred ansats där samhällsaktörer allt mer jobbar tillsammans. En stor del av året har präglats av myndighetssamverkan. Ett gott exempel är det arbete som säkerhetstjänsten bedrivit tillsammans med Post- och telestyrelsen (PTS) och Säkerhetspolisen i syfte att åstadkomma ett säkert 5G-nät.

Ett omfattande arbete med att motverka kartläggning av skyddsobjekt har också pågått under året. Ett antal individer har dömts till fängelse, skyddstillsyn och böter och fler rättsprocesser är att vänta under 2021.

Detta är ett antal av de öppna åtgärder och aktiviteter som den militära säkerhetstjänsten har bidragit med under året. På kommande sidor följer en beskrivning av olika säkerhetshotande aktiviteter som främmande underrättelse- och säkerhetstjänster kan rikta mot Försvarsmakten och dess intressen som sedan åtföljs av en beskrivning av säkerhetshöjande motåtgärder.

SPECIALTJÄNSTER MED HÖG RISKBENÄGENHET

De senaste åren har ett antal säkerhetshotande händelser uppdagats och offentliggjorts där Ryssland och dess specialtjänster varit bakomliggande aktörer. Exempel på detta är teknisk inhämtning, mord och mordförsök på andra staters territorium samt försök att påverka nationella val i andra länder. Detta visar att riskbenägenheten hos de ryska underrättelse- och säkerhetstjänsterna är hög, när målet är prioriterat.

De ryska underrättelse- och säkerhetstjänsterna – GRU, FSB och SVR (se faktaruta) – har en lång tradition av att bedriva kvalificerad underrättelsetjänst. De har mandat att infiltrera utländska organisationer som bedriver underrättelsetjänst eller säkerhetshotande verksamhet riktad mot Ryssland. Enligt rysk lag får de även bedriva underrättelseverksamhet utomlands genom både öppna och hemliga metoder.

Målsättningen är att försörja den ryska statsledningen med underrättelser, att stötta landets utveckling inom olika områden, bedriva påverkan och i övrigt bidra till att främja de säkerhetspolitiska målsättningarna.

GRU, SVR och FSB bedriver ett systematiskt underrättelsearbete mot utländska mål i Ryssland. Verksamheten disponerar omfattande resurser och det är sannolikt att försvarsmaktspersonal som återkommande reser till Ryssland, oavsett vart, riskerar att bli mål för de ryska underrättelse- och säkerhetstjänsternas verksamhet.

De ryska underrättelse- och säkerhetstjänsternas har två huvudspår för sin verksamhet utomlands; vilka benämns ”legal” respektive ”illegal”. Det handlar inte om huruvida verksamheten är laglig eller inte – all rysk underrättelseverksamhet är tillåten enligt rysk lag – utan om den identitet som underrättelseofficeren använder sig av utomlands.

I ”legalt” hänseende uppträder underrättelseofficeren under sin riktiga identitet, i det ”illegala” under falsk identitet, oftast också med en annan nationalitet. De förstnämnda återfinns främst vid de ryska diplomatiska beskickningarna, det vill säga ambassader, handelsrepresentationer och konsulat. På de flesta ryska ambassader och på vissa konsulat finns representanter från GRU och SVR.

Systemen med falska och riktiga identiteter förekommer parallellt och underrättelsemålen är till största del desamma. Skillnaden är att den illegala är svårare att upptäcka.

Riskbenägenheten hos de ryska underrättelse- och specialtjänsterna är hög när målet är prioriterat.

FAKTA

De ryska underrättelse- och säkerhetstjänsterna

De ryska specialtjänsterna GRU, SVR och FSB har delvis överlappande uppdrag. Exempelvis har GRU i uppdrag att inhämta underrättelser inom det ”militärteknologiska området” och SVR inom det ”vetenskapliga-tekniska området”. FSB ska inhämta underrättelser i syfte att ”öka den Ryska federationens vetenskapliga-tekniska kapacitet”.

GRU – Rysslands militära underrättelsetjänst

GRU:s uppdrag är att inhämta och analysera underrättelser på strategisk och operativ nivå, leda specialförbandsverksamhet och delta i påverkansoperationer. Underrättelseinhämtningen riktas både mot militära och civila områden. Ryska militärattachéavdelningar vid ambassaderna lyder under GRU.

FSB – Rysslands säkerhets- och underrättelsetjänst

FSB:s uppdrag omfattar kontraspionage, kontraterrorism, utrikes underrättelseverksamhet, gränstjänst, påverkansoperationer, informationssäkerhet och motverkan av kriminalitet. FSB är att betrakta som en militär organisation, då den har militära lydnadsförhållanden och väpnade förband för specialoperationer trots att den inte lyder under försvarsministeriet.

SVR – Rysslands utrikesunderrättelsetjänst

SVR är framförallt en underrättelsetjänst som inhämtar mot politiska mål, vetenskap och teknik samt deltar i påverkansoperationer. Uppdraget omfattar också kontraspionage och kontraterrorism utanför Rysslands gränser. Även SVR är att betrakta som en militär organisation, trots att den inte lyder under försvarsministeriet och nästan alltid uppträder civilt , då den har militära lydnadsförhållanden och väpnade förband för specialoperationer.

De kinesiska underrättelse- och säkerhetstjänsterna

MSS (Ministry of State Security), MID (Military Intelligence Department) och SSF (Strategic Support Force) är centrala delar av kommunistpartiets säkerhetsapparat. Tillsammans med organisationer som är ansvariga för påverkansaktiviteter bedriver de mångsidig, kvalificerad verksamhet utomlands och i Kina. Denna verksamhet riktas bland annat mot Sverige och svenska intressen.

MSS – Kinas primära civila underrättelsetjänst

MSS uppdrag är att inhämta underrättelser om bland annat politik, teknik och säkerhet. MSS bedriver en omfattande verksamhet mot utländska medborgare som befinner sig i Kina.

MID – Kinas militära underrättelsetjänst

MID:s uppdrag är att inhämta och bearbeta underrättelser på strategisk och operativ nivå. Organisationen leder Kinas försvarsattachéverksamhet.

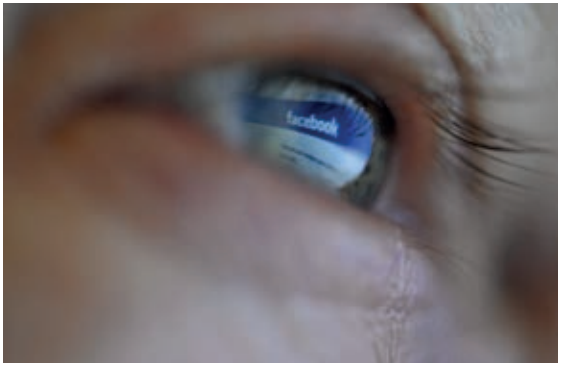
SSF – Kinas militära tekniska underrättelsetjänst

SSF ansvarar för kinesiska försvarsmaktens förmågor inom dator- och nätverksoperationer, signalspaning, rymd och anti-rymd.

KONTAKTTAGNING FRÅN FRÄMMANDE MAKT

Den omfattande tekniska inhämtningen innebär inte att behovet av att värva mänskliga källor har minskat. Försvarsmaktsanställdas riskbeteenden och sårbarheter kartläggs kontinuerligt, både i sociala medier och i andra sammanhang. Syftet är att hämta in information som kan användas för att närma sig, trakassera eller utpressa personer för att komma åt efterfrågad information eller för att skapa andra typer av accesser.

Kontakttagning eller närmanden utförs exempelvis av underrättelseofficerare från främmande makt som reser in i Sverige med falsk identitet eller under täckbefattningar, det vill säga påhittade befattningar. För att undgå upptäckt kan dessa underrättelseofficerare begära visum till ett annat land i Schengenområdet än det de har för avsikt att genomföra operationer i. Kontaktförsök kan även genomföras utomlands, då den som utsätts är betydligt mer sårbar än på hemmaplan. I samband med besök i länder med stark säkerhetsapparat – som exempelvis Ryssland, Kina och Iran – riskerar försvarsmaktspersonal liksom annan personal inom försvarssektorn, att bli utsatt för kartläggning, övervakning, trakasserier, misskreditering eller närmanden från specialtjänsterna. Därför har Försvarsmakten beslutat att rekommendera anställda att undvika resor till Ryssland, Kina och Iran.



Försvarsmaktsanställdas riskbeteenden och sårbarheter kartläggs kontinuerligt, både i sociala medier och i andra sammanhang.

De ryska säkerhets- och underrättelsetjänsterna placerar även ut underrättelseofficerare med täckmantel i specifika företag och organisationer. Syftet är att på ett till synes legitimt sätt inhämta efterfrågad information och eftersom inhämtningen sker i det fördolda är den svår att upptäcka.

Förutom företag utnyttjas även statliga organisationer som exempelvis universitet, politiska och ekonomiska samverkansorganisationer samt icke-statliga organisationer. Ett annat sätt att tillskansa sig information är genom så kallade täckföretag. De används ofta för teknikanskaffning i syfte att på ett dolt sätt anskaffa teknik till egen industri.

Men inhämtning sker inte bara i det fördolda. Även officiell samverkan med rysk militär kan utgöra inhämtningstillfällen. All rysk internationell militär samverkan koordineras inom det ryska försvarsdepartementet. De ryska underrättelse- och

säkerhetstjänsterna finns således alltid med i bilden vilket måste beaktas då Försvarsmakten samverkar med rysk militär.

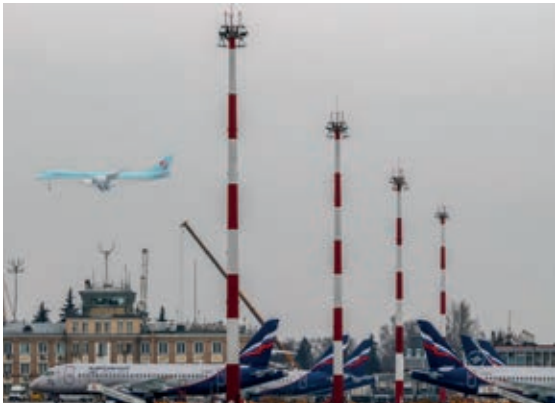
All privat kontakt mellan ryska militärer och representanter för andra länders militärer är förbjuden enligt rysk lag. Om ryska militära företrädare tar kontakt är de antingen sanktionerade av högre chef eller också begår den kontaktsökande ett regelbrott.

Förhållandet ser likadant ut för anställda i en rad andra branscher i Ryssland som anses vara vitala ur säkerhetssynpunkt, bland annat forskningsområdet. Detta innebär att många former av civil samverkan med Ryssland är komplicerad ur ett säkerhetsperspektiv. Även civil samverkan med Kina kan innebära säkerhetsrisker.

NY RESEREKOMMENDATION SKA SKYDDA FÖRSVARSMAKTENS PERSONAL

Den 1 juni 2020 införde Försvarsmakten en rekommendation för all personal att undvika resor till Ryssland, Kina och Iran. Syftet är att skydda medarbetarna mot säkerhetshot och att skydda Försvarsmaktens skyddsvärden.

På senare år har antalet incidenter där försvarsmaktsanställda råkat illa ut i samband med resor ökat. Främmande makts underrättelse- och säkerhetstjänster har blivit mer aggressiva i sina metoder. Individer inom totalförsvaret, däribland försvarsmaktsanställda, har blivit intagna till förhör, utsatts för närmanden, övervakats eller trakasserats. Det



En ny reserekommendation ska skydda Försvarsmaktens medarbetare mot säkerhetshot.

kan finnas flera olika syften med detta tillvägagångssätt, varav ett kan vara att sätta press på enskilda individer för att i förlängningen få dem att utföra tjänster.

Alla medarbetare i Försvarsmakten betraktas som skyddsvärda, oavsett befattning eller arbetsuppgifter. Det beror på att alla har, kan ha eller vet vem som har tillgång till skyddsvärd information. Försvarsmaktsanställda är extra sårbara på bortaplan, eftersom utländska underrättelse- och säkerhetstjänster har mycket större befogenheter när de genomför operationer i hemlandet.

Personal som omfattas av de nya reserekommendationerna är all tidvis och kontinuerligt tjänstgörande personal, hemvärnssoldater, frivillig personal, officersaspiranter och värnpliktiga under

grundutbildning. Rekommendationen gäller såväl privata resor som tjänsteresor eftersom hotet mot den enskilde är detsamma oavsett vilken typ av resa det handlar om.

Om resor till dessa länder ändå sker ska kontinuerligt tjänstgörande personal i förväg anmäla resan till sin lokala säkerhetsorganisation. Syftet är att stödja och förbereda medarbetarna på de risker som finns och vilka åtgärder som går att vidta för att minska dessa.

Exempel

Under 2020 reser en grupp svenskar, med koppling till försvaret, till Ryssland. Under vistelsen upptäcker de att de övervakas relativt öppet.

De som följer efter dem gör ingen hemlighet av att de finns i närheten.

Vid hemresan blir de stoppade i tullen. De får sitt handbagage noggrant genomsökt, men inga överträdelser mot tullbestämmelserna kan konstateras och gruppen får passera.

Efter tullkontrollen vinkar den ryska säkerhetstjänsten in dem till enskilda förhör. Det är uppenbart att de är väntade eftersom det redan finns svenska tolkar på plats.

De får sitta i varsitt rum utan möjlighet att kommunicera med varandra och uppfattar att det som sägs misstolkas och vänds emot dem.

En mängd frågor ställs, bland annat om syftet med resan. En av individerna meddelas – felaktigt – att denne har lämnat oriktiga uppgifter i sin visumansökan, vilket är ett lagbrott.

Under ett av förhören kommer en okänd person in i ett av förhörsrummen och hämtar individens pass och boardingkort. Han meddelas även att hans väska återigen ska sökas igenom.

De får sitta i varsitt rum utan möjlighet att kommunicera med varandra och uppfattar att det som sägs misstolkas och vänds emot dem.

Efter långa förhör släpps individerna och kan fortsätta sin resa hemåt.

GEDIGEN SÄKERHETSPRÖVNING SKA TRYGGA FÖRSVARSMAKTEN

Varje år säkerhetsprövar Försvarsmakten tusentals människor. Både nyanställd personal och de som byter befattning inom myndigheten prövas i en omfattande process. Därutöver sker en regelbunden uppföljning av alla som deltar i verksamheten.

Under året har Försvarsmakten på regeringens uppdrag sett över de regelverk och styrningar som gäller för säkerhetsprövning, rekrytering och anställning. Bedömningen är att reglerna är tillräckliga, men att de ständigt måste kontrolleras och följas upp. Vissa förstärkande åtgärder kommer också att genomföras under 2021.

I princip alla som arbetar i Försvarsmakten säkerhetsprövas. Det görs för att den personal som ska delta i säkerhetskänslig verksamhet eller ta del av säkerhetsskyddsklassificerad information måste vara pålitlig och lojal. Lika viktigt är att inte ha några sårbarheter som påverkar deltagandet i verksamheten. Om känslig information hamnar i fel händer riskerar det att försämra försvarsförmågan. Dessutom kan det ha negativ inverkan på förhållandet till Försvarsmaktens viktiga samarbetspartner, såväl nationellt som internationellt.

Ett spelberoende är en sårbarhet som kan påverka privatekonomin. Sårbarhet är tillsammans med lojalitet och pålitlighet något som bedöms vid en säkerhetsprövning.

Pålitlighet, lojalitet och sårbarhet

Att vara pålitlig innebär att man kan lita på det en person säger och gör. Pålitligheten kan påverkas av exempelvis drogberoende eller om personen är dömd för brott. Det kan också handla om att en individ är oaktsam eller har dåligt omdöme. Att följa de regler som finns är också ett uttryck för pålitlighet.

Den som är opålitlig kan också vara sårbar, till exempel genom att ljuga om vissa förhållanden. Främmande makt eller andra aktörer kan utnyttja detta för att komma åt hemlig information, till exempel genom att erbjuda ekonomisk kompensation i utbyte mot gentjänster eller genom att hota med att avslöja sådant som individen inte vill ska komma fram. En person kan även bedömas som pålitlig och lojal men ändå vara sårbar om denne exempelvis har stora skulder.

Lojalitet handlar om att vara lojal mot Sveriges säkerhet och nationella oberoende.

Försvarsmakten ställer höga krav på all personal. Inledningsvis genomgår därför de som ska placeras

i säkerhetsklass en omfattande grundutredning som genomförs på den organisationsenhet individen ska arbeta. Därefter sker en uppföljande säkerhetsprövning under hela anställningstiden, främst genom återkommande samtal med närmaste chef.

Kraven är inte desamma för alla. Ju mer information en individ har tillgång till, desto större skulle skadeverkningarna kunna bli om den hamnade i fel händer. Därför genomför Säkerhetskontoret på Must en mer omfattande säkerhetsprövning av de högsta cheferna i Försvarsmakten, det vill säga alla chefer med kommendör/överstes grad och civila motsvarigheter.

Vid säkerhetsprövning tas referenser, men majoriteten av den information som värderas i säkerhetsprövningen kommer från individen själv, till exempel betyg, intyg och den information som delges vid intervjuer. I den översyn av säkerhetsprövningsprocessen som skett under året har det framkommit att rutinerna för kontroll av verifierade och vidimerade betyg och intyg behöver följas upp på ett tydligare sätt.

Just nu ser Försvarsmakten över hur säkerhetsorganisationen och HR kan jobba ännu bättre ihop för att säkerställa att regler och tillämpning av säkerhetsprövningen går i takt. Säkerhetsprövningarna håller hög kvalitet, men inget system är hundraprocentigt. Försvarsmakten eftersträvar heller inte ett system där varje aspekt av de anställdas liv kartläggs. Strävan är att hålla en balans mellan Försvarsmaktens krav och individens fri- och rättigheter. De senare är precis de värden Försvarsmakten är satt att försvara.

INTRÅNG KAN GE FÄNGELSE — SKÄRPTA STRAFF FÖR KARTLÄGGNING AV SKYDDSOBJEKT

Under senare år har antalet anmälningar om tillträdesbrott ökat. Under 2020 har det förekommit ett antal rättsprocesser både mot individer som tagit sig in på skyddsobjekt utan tillstånd och som ägnat sig åt kartläggning av ett stort antal skyddsobjekt. Fler rättsprocesser är att vänta under 2021.

I januari dömdes en person till ett års fängelse efter att ha dokumenterat, fotograferat och inhämtat uppgifter om 36 skyddsobjekt samt spridit en del av informationen som är av stor betydelse för Sveriges säkerhet. Domen överklagades av åklagaren och under våren fastställdes domen av hovrätten.

I maj dömdes en annan person till åtta månaders fängelse för grov obehörig befattning med hemlig uppgift efter att ha lagrat information om 37 försvarsanläggningar i en dator. Enligt Försvarsmakten skulle ett röjande av de hemliga uppgifterna för främmande makt innebära betydande men för Sveriges säkerhet. Domen överklagades till hovrätten som höjde domen till ett års fängelse.

I slutet av året väcktes ytterligare ett åtal med samma rubricering. Personen misstänks för att ha spridit hemliga och känsliga uppgifter om sju försvarsanläggningar på ett hemligt nätforum. Domstolsförhandling sker under våren 2021.

Tre individer åtalades för brott mot skyddslagen efter att olovligen ha tagit sig in på en militäranläggning. De tre dömdes till villkorlig dom, något åklagaren har överklagat.

Många av de individer som ägnar sig åt den här typen av verksamhet är så kallat militärt överintresserade personer som lägger ner mycket tid på att samla in och sprida information om militäranläggningar. Genom digitala medier kan de kopiera stora mängder information och snabbt distribuera den via internet. Men att ägna sig åt kartläggning av militäranläggningar är ett mycket allvarligt brott och individer som gör det äventyrar både sin egen och Sveriges säkerhet.

2019 skärptes påföljden för överträdelsebrott i skyddslagen. Maxstraffet är numera två års fängelse. Kartläggning av militära skyddsobjekt eller innehav av material som andra anskaffat genom kartläggning betraktas nu som ett så kallat artbrott. Det är en juridisk term som innebär att det i regel är fängelse som ska utdömas oavsett straffvärde. Detta står i stark kontrast till de påföljder som tidigare utdömts och skickar därför en tydlig signal om brottets allvar.

Att kartlägga och sprida information om skyddsobjekt är olagligt. Den insikten gjorde de individer som under 2020 dömdes för grov obehörig befattning med hemlig uppgift.

Skyddsobjekt är anläggningar, byggnader och områden som behöver ges ett särskilt skydd eftersom de är av stor betydelse för försvaret av Sverige. De är även till för att skydda allmänheten från skador som kan uppstå från militär verksamhet. I takt med upprustningen av totalförsvaret har de blivit allt viktigare.

Genom att kartlägga, samla och sprida information om skyddsobjekt kan individer gå främmande makts ärenden – ibland utan att veta om det. Främmande makt lägger ner stora resurser på att kartlägga svenska militära och civila skyddsobjekt, ett arbete som tyvärr underlättas genom den verksamhet som de här individerna genomför.

ÖKAT ANSVAR INOM SIGNALSKYDD

Med den nya säkerhetsskyddslagen och tillhörande förordning har Försvarsmakten fått ett utökat ansvar inom signalskydd. Den stora skillnaden är att alla verksamhetsutövare som bedriver säkerhetskänslig verksamhet, det vill säga verksamhet av betydelse för Sveriges säkerhet, nu omfattas. Det innebär att alla aktörer som kommunicerar säkerhetsskyddsklassificerad information måste använda signalskydd som är godkänt av Försvarsmakten på förbindelser som kan avlyssnas av obehöriga. Detta gäller numera både offentlig och privat verksamhet vilket kommer att stärka säkerhetsskyddet i hela samhället.

Frågor om signalskydd kan ställas till signalskydd@mil.se

MUST TAR HÖJD FÖR KVANTDATORHOTET

Vissa menar att storskaliga kvantdatorer kommer att vända upp och ner på hela samhället. Andra menar att sådana aldrig kommer att bli verklighet. Oavsett vilket tar Musts säkerhetskontor redan idag höjd för att totalförsvarets kryptosystem ska kunna stå emot potentiella hot från framtida storskaliga kvantdatorer. Det handlar om kryptosystem som ska kunna skydda svensk sekretessbelagd information flera decennier in i framtiden.

Kvantdatorn har funnits som begrepp under mer än 30 års tid och gradvis börjar nu teorierna att realiseras. Under senare år har det skett stora framsteg inom kvantteknologiforskningen, något som på sikt skulle kunna revolutionera bland annat kryptologiområdet.

Kvantdatorer är en särskild typ av datorer som till skillnad från dagens klassiska datorer använder kvantmekaniska fenomen för att utföra beräkningar. Vissa specifika matematiska problem, som skulle ta dagens klassiska datorer ogörligt lång tid att lösa med de idag bästa kända algoritmerna, skulle med en storskalig kvantdators hjälp kunna lösas på kort tid.

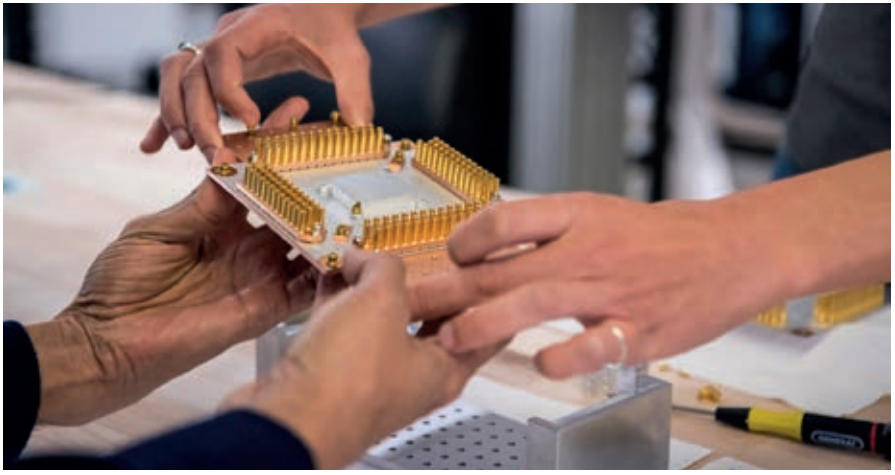
Några av de matematiska problem som kvantdatorer löser effektivt utgör själva grunden i de kryptosystem som idag används i de flesta av dagens kommersiella kryptosystem. Kvantdatorer skulle alltså relativt enkelt kunna knäcka dagens kryptosystem, vilket innebär att systemen måste bytas ut.

Sedan flera år tillbaka deltar medarbetare vid Säkerhetkontoret i forskning som rör kvantdatoralgoritmer för kryptoanalys och kvantdatorsäkra klassiska kryptosystem. Det handlar om att kunna bedöma säkerheten i dagens asymmetriska kryptosystem för att kunna ta fram olika kvantdatorsäkra alternativ.

Det är avgörande att redan i ett tidigt skede bygga in skydd mot kvantdatorer i kryptosystemen. Därför dimensionerar Försvarsmakten också redan idag merparten av totalförsvarets kryptosystem utifrån kvantdatorhotet.

De system som används för sekretesskydd måste dessutom bytas ut med god framförhållning. Om uppgifter som krypteras idag omfattas av sekretess i 25 års tid, måste dagens kryptosystem förbli omöjliga att forcera under de kommande 25 åren. Det innebär i princip att merparten av totalförsvarets kryptosystem måste vara kvantdatorsäkra redan nu.

Kvantdatorutvecklingen innebär att kartan för den asymmetriska kommersiella kryptologin sannolikt kommer att behöva ritas om i närtid. Sverige ligger tillsammans med några andra länder i framkant inom kvantdatorområdet. Säkerhetskontoret följer den här utvecklingen, och då särskilt de standardiseringsprocesser och andra ansträngningar som pågår internationellt. Ambitionen är att bidra till att ta fram nya säkra publika standarder som kan komma både Försvarsmakten, totalförsvaret och det svenska civilsamhället till del.



Must tar höjd för att totalförsvarets kryptosystem ska kunna stå emot potentiella hot från framtida storskaliga kvantdatorer.

Granskningen av Must

Musts verksamhet regleras av lagar och regler och vår verksamhet granskas löpande av oberoende insyns- och kontrollorgan.

Granskning av myndigheter sker i olika omfattning och på olika sätt beroende på verksamhet. Musts verksamhet är av sin natur omgärdad av sträng sekretess av hänsyn till Sveriges säkerhet och förhållandet till främmande makt vilket försvårar öppenhet och medborgerlig insyn. Must strävar emellertid efter största möjliga öppenhet och statsmakten har genom regering och Riksdag successivt förstärkt kontrollmekanismerna under de senaste decennierna.

Kontroll- och inspektionsverksamheten utgör ett effektivt komplement till en direkt medborgerlig insyn. Därtill utgör granskningen samtidigt ett stöd för Must eftersom de tillför viktiga juridiska perspektiv på verksamheten. Granskningarna bidrar på så vis med en trygghet att Must håller sig inom ramen för lagar och förordningar. Granskningarna föregås alltid av ett omfattande förberedelsearbete i syfte att ge granskande myndigheter så bra underlag som möjligt.

Statens inspektion för försvarsunderrättelseverksamheten

Statens inspektion för försvarsunderrättelseverksamheten (Siun) granskar Must kontinuerligt över året. Under 2020 har Must granskats med avseende om verksamheten bedrivits i enlighet med lagen om försvarsunderrättelseverksamhet. Granskningarna har bland annat omfattat viss inhämtning som Försvarsmakten bedriver med särskilda metoder och att Musts rapportering följer den inriktning som är bestämd. Utöver det har Siun även granskat att Försvarsmaktens personuppgiftsbehandling utförs enligt lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Siun har under 2020 även granskat Musts principer för rekrytering och utbildning. Mer information om granskningarna finns att återfinna på Siun:s hemsida (www.siun.se)

Integritetsskyddsmyndigheten (tidigare Datainspektionen)

Även Integritetsskyddsmyndigheten (IMY) kontrollerar att Must följer Lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt även den allmänna personuppgiftslagen (www.imy.se)

Riksrevisionen

Musts ekonomiska redovisning och efterlevnad av uppställda förvaltningskrav granskas av Riksrevisionen och genom försvarsmaktsinterna processer. Mer information finns på www.riksrevisionen.se

Dialog med uppdragsgivarna

En kontinuerlig dialog med Regeringskansliet, främst med Enheten för samordning av försvarsunderrättelsefrågor (Sund) på Försvarsdepartementet, säkerställer att Musts produktion motsvarar regeringens förväntningar. Motsvarande dialoger sker med övriga staber och ledningar i Högkvarteret för att säkerställa överbefälhavarens beställningar och långsiktiga behov.

Övrigt om granskning

Även granskarna granskas. Riksrevisionen genomförde en granskning av Siun 2015 *”Kontrollen av försvarsunderrättelse-verksamheten – RiR 2015:2”*. I sina slutsatser skriver Riksrevisionen:

”Riksrevisionens övergripande slutsats är att kontrollmyndigheten, Statens inspektion för försvarsunderrättelseverksamheten, har fått förutsättningar för att kunna bedriva kontrollverksamheten på ett effektivt sätt. Riksrevisionens slutsats är också att Siun utför de uppgifter myndigheten har enligt lagar och förordningar.

Riksrevisionens granskning visar att försvarsunderrättelsemyndigheterna tar Siuns synpunkter på allvar och genomför åtgärder i enlighet med Siuns beslut.”

STRATEGISK UTVECKLING

Kompetensförsörjning, informationshantering och teknik som drivkraft för underrättelse- och säkerhetstjänst.

Digitaliseringen har lett både till kortade beslutstider och ett överflöd av information. Ett informationsflöde som är en blandning av fakta, lögner, osäkerheter och motsägelser från fler och fler källor. Detta är inget nytt för en underrättelse- och säkerhetstjänst men mängden av information och den ökande hastigheten kräver nya metoder och förhållningssätt i allt från källutvärdering, bearbetning och analys till hur slutprodukten paketeras för mottagare av underrättelser och information.

Must utvecklar kontinuerligt sin förmåga till strategisk förvarning, att uthålligt kunna följa säkerhetspolitiska kriser, bedriva en effektiv militär säkerhetstjänst och genomföra omvärldsbevakning. Den föränderliga hotbilden hanteras genom en ständig utveckling och anpassning av samarbeten, både internt inom Försvarsmakten liksom med försvarsunderrättelsemyndigheterna, Säkerhetspolisen och övriga relevanta aktörer.

När Sverige bygger ett starkare nationellt försvar ställs det ökade krav på tillgängliga underrättelser och anpassade beslutsunderlag både vad avser en aktuell lägesuppfattning och framtida hot.

Nationellt försvar och en breddad och komplex hotbild ställer både gamla (kända) och nya (till del okända) krav på vår anpassningsförmåga, vår teknik, våra metoder och på våra medarbetares och ledares kompetenser.

Kompetensförsörjning

Det är stor konkurrens på arbetsmarknaden och Must fokuserar därför på att löpande utveckla och förbättra förutsättningarna att bibehålla och utveckla sitt starka humankapital. Målsättningen är att attrahera och behålla de bästa talangerna.

Förtroende och kvalitet är helt avgörande för vår verksamhet eftersom vår styrka är ligger i medarbetarnas omdöme, skicklighet och unika kompetens. Detta arbete har över tid byggt upp en stark gemenskap och det finns en dokumenterad stolthet över att arbeta vid Must.

Informationshantering

Must hanterar dagligen stora informationsmängder med höga krav på säkerhet. Informationshanteringen måste gå i takt med den snabba teknikutvecklingen inom bland annat artificiell intelligens och 5G. Must arbetar därför oavbrutet med att bli bättre på att nyttja informationsmiljön för att till exempel hitta mönster i stora informationsmängder eller att skapa nya tjänster, applikationer och bearbetningsverktyg åt användarna.

Ny teknik och nya metoder är en förutsättning för en modern försvarsunderrättelseverksamhet och nästa generations militära underrättelse- och säkerhetstjänst. För att utveckla förmågorna samarbetar Must både nationellt och internationellt, driver egna

utvecklingsprojekt och beställer forskning inom teknik- och informationsområdet. Forsknings- och studieresultaten används därmed för att stärka den egna förmågan men även för att bygga ett starkare nationellt försvar – tillsammans.

FOREWORD BY THE HEAD OF THE MILITARY INTELLIGENCE AND SECURITY SERVICE

In 2020, the trend towards harsher power politics intensified both globally and on Europe's borders. At the same time, there has been a weakening of the rule-based order and predictability. The ongoing pandemic has accelerated these tendencies and the Swedish Military Intelligence and Security Service (MUST) assesses that there is an enhanced risk of Sweden being subjected to strong pressure in this environment.

The hostile threat scenario Sweden is facing is at the same time political, economic and military – not "either or". As such, the threat has become broader and more complex. It involves external threats, which increasingly are manifested in internal security. The threats are aimed at the Swedish defence capability, prosperity and democracy. Hybrid, covert and deniable methods are now commonplace.

Military activities in the vicinity of Sweden have continued to increase in intensity and have become ever more advanced. The current tendency to view economy and technology as strategic tools has been reinforced. Countries like Russia and China have a have a wide-ranging of tools at their disposal to promote national interests. They also have good coordination capabilities. Intelligence activities aimed at Sweden and the Swedish Armed Forces are extensive.

This is the reality in which MUST operates in its dual roles as Sweden's both civilian and military intelligence service and military security service. As I summarise MUST's operations over the past year, I am proud to conclude that we – together with our national and international partners – have been able to fulfil the mission we received from the Swedish government and the Swedish Armed Forces.

The Military Intelligence and Security Service must be able to operate in any condition. Thanks to our staff's flexibility and creativity, we have been able to carry out our duties while maintaining high standards despite the challenges brought on by the pandemic in 2020.

The direction given by the Swedish Parliament's to reinforce the total defence means that MUST will continue to raise the level of ambition. It provides us with opportunities, but it also requires us to continue to develop and adapt MUST's operations to the pace of the changes around us so that we can support the growth of the Armed Forces to the best of our capabilities.

MUST contributes to strengthening Sweden's overall capacity to face a more complex threat environment. In 2020, measures covered cyber security, psychological defence, foreign direct investments and electronic communications. We help strengthening the security of the Armed Forces and Swedish society as a whole. Contributing to the advancement and implementation of new legislation is part of these efforts.

We continue to further develop the technological platforms necessary for MUST to operate and compete in an environment where the management of

big data, IT developmentz, cyber threats, information security and AI is vital.

I am delighted that MUST had the opportunity to revisit an important part of our legacy in 2020. Through the Army Museum´s exhibition "In the nation's secret service" and the unveiling of commemorative plaques where the so-called 'C Bureau' once was we honoured not least the women but also the men who worked there during the Second World War.

I hope this annual report will provide an overview of the operations of the Military Intelligence and Security Service as well as our view of the evolving security environment and the external threats Sweden is facing. But I also hope it demonstrates how we are adapting to guarantee that we will be able to continue to fulfil our mission: to help strengthening Sweden's national security in an uncertain world.

Lena Hallin | Director of the Swedish Military Intelligence and Seurity Service (MUST)

BILDER

Sid 6, 42, 49, 53, 63, 66, 71: Försvarsmakten
Sid 8: Jimmy Croona, Combat Camera, Försvarsmakten
Sid 10: Andy Wong, TT
Sid 15 (överst): Nicolas Asfouri/TT
Sid 15 (underst): Kazuhiro Nogi/TT
Sid 17 (vänster): Stephanie Lecocq/TT
Sid 17 (höger): Alexei Nikolsky/Russian Presidential Press and Information Office/TASS/Sipa USA/TT
Sid 18: Anatoliy Zhdanov/Polaris/TT
Sid 20: Dmitry Dukhanin/TT
Sid 22: Evan Vucci/AP Photo/TT
Sid 25: Paul Hennessy/Zuma Press/TT
Sid 27 (överst): Zhang Jingang/Costfoto/TT
Sid 27 (underst): Wang Jianfeng/Costfoto/TT
Sid 29: Chine Nouvelle/SIPA/Shutterstock/TT
Sid 30: Khaled Abdullah/TT
Sid 33: Nariman El-Mofty/AP/TT
Sid 34: Lev Fedoseyev/ITAR-TASS/TT
Sid 36: Christoph Burgstedt/Science Photo Library
Sid 39: Alessandro Bianchi/Reuters/TT
Sid 40: Magnus Glans/Svartpunkt AB
Sid 45: Kacper Pempel/Reuters/TT
Sid 47, 52: Johan Nilsson/TT
Sid 50: Oscar Larsson/Försvarsmakten
Sid 55: Andrew Brookes/Alamy Stock Photo/TT
Sid 56: Shamil Zhumatov/Reuters/TT
Sid 58: Antti Aimo-Koivisto/Lehtikuva/SCANPIX/TT
Sid 59: Leonid Faerberg/SOPA Images/Shutterstock/TT
Sid 61: Karin Wesslén/TT
Sid 65: Reuters/TT

Ett säkrare Sverige i en osäker värld

FÖRSVARSMAKTEN

107 85 Stockholm, tel 08-788 75 00
www.forsvarsmakten.se