FÖR(SVARA) SVERIGE – I TIDEN

52 reformer för en digital, global och osäker era

En rapport av Wilma Eriksson Kocsis

INNEHÅLLSFÖRTECKNING

SAMMANFATTNING

- Begreppet ”totalförsvar” kan beskrivas som all den verksamhet som behövs för att förbereda Sverige inför krig.[1]

- En återkommande analys av svenskt försvar är att vår motståndskraft, enkelt förklarat som styrkan och kapaciteten i försvarets motstånd, måste stärkas. En del av detta är att höja tröskeleffekten. Tröskeleffekten innebär att vi har en militär förmåga som är så pass god att den skapar en tröskel hög nog att avskräcka angripare från att attackera.[2] Enligt Försvarsmakten är en god tröskeleffekt kärnan i ett starkare försvar.

DET SVENSKA CYBERFÖRSVARET

- Sverige är ett av världens mest digitaliserade länder, men ett av de sämre när det gäller cybersäkerhet och -försvar. Våra myndigheter har sågats för sin informationssäkerhet och våra kommuner är i särklass sämst i landet på cybersäkerhet. Samtidigt vittnar näringslivet, som också utsätts för cyberattacker understödda av främmande makt, om att de saknar stöd från politiskt håll.

- Vår cybersäkerhet är i dag fördelad på fyra departement och åtta myndigheter. Dessa krävs ständigt på djupare samordning, men så länge de saknar direktiv och mandat kommer arbetet att stå still. Sverige behöver en konkret cyberstrategi, en krisenhet under statsministern och ett sanktionssystem för de leverantörer av samhällsviktiga tjänster som bryter mot säkerhetsskyddslagen. Vi måste också bidra till arbetet med EU:s redan framgångsrika cyberdiplomati, samt utveckla en alldeles egen.

- Riksrevisionen uppmanar regeringen till en tydligare styrning av cybersäkerheten. Ett problem är att när våra myndigheter inte lyder direkt under regeringens ministrar går det heller inte att utkräva ansvar av dem. Sveriges förbud mot ministerstyre ger myndigheter mandat att agera mot regeringens vilja, och politiker möjlighet att undslippa ansvar i frågor som rör rikets säkerhet. För att förbättra Sveriges cybersäkerhet bör vi införa ministerstyre.

- I takt med att det digitala blir en allt större del av den moderna krigföringen är det viktigt att det svenska försvaret hänger med. Vi behöver inrätta cyberförsvaret som en egen försvarsgren, inkorporera mer artificiell intelligens i försvaret och inrätta ett cyberhemvärn.

- De stelbenta kraven på fysisk förmåga för att få genomföra värnplikt måste också luckras upp. På så sätt kan fler individer erbjuda sin kompetens till försvaret, vilket kan resultera i fler cybersoldater.

DET MILITÄRA FÖRSVARET

- Parallellt med att cyberhotet ökar gör även det militära hotet detsamma. Sveriges militära försvar har nedprioriterats allt mer sedan kalla krigets slut. Detta påverkar hur vi måste gå till väga när Försvarsmakten rustas upp.

---

1 SFS (1992:1403). *Om totalförsvar och höjd beredskap.*

2 Försvarsmakten. Visionen. *Försvarsmakten*. https://www.forsvarsmakten.se/sv/om-forsvarsmakten/varderingar-och-vision/vision/ (Hämtad 2021-07-04)

- En av Försvarsmaktens största utmaningar är, och kommer fortsatt att vara, personalförsörjningen. I dag lämnar gruppbefäl, soldater och sjömän sin tjänst för tidigt för att det ska vara hållbart för försvaret. Då den vanligaste anledningen till avslutad tjänstgöring är övergång till studier bör Försvarsmakten införa fler studieekonomiska incitament för att få tjänstgörande att stanna kvar tillräckligt länge. En möjlighet vore att Försvarsmakten betalar av en andel av studielånet för den som tjänstgjort en längre tid än genomsnittet.

- Internationella samarbeten är av yttersta vikt för Sverige. Det är beklagligt och fel att Sveriges nuvarande regering inte vill se samarbeten som kräver ömsesidiga försvarsgarantier. När vi nu bygger upp ett försvar som gör oss beroende av andra länders hjälp måste vi också kunna räkna med dessa länders stöd i händelse av krig. Sverige behöver verka för en försvarsallians med Finland, precis som vi också ska sträva mot fler samarbeten grundade på garantier om stöd i händelse av krig.

- Sveriges deltagande i internationella insatser har ett stort värde. Genom dessa kan vi försvara grundläggande värderingar internationellt, samtidigt som vi har möjlighet att träna våra förmågor i praktiken. Men i en tid där vårt nationella försvar är i stort behov av resurser behöver internationellt deltagande ständigt utvärderas. Sverige måste prioritera upprustandet av det egna försvaret före deltagandet i internationella insatser under en tid framöver. Vi har dock fortfarande en skyldighet att stå på motsatt sida gentemot skurkstater och minska mänskligt lidande ute i världen. Därför måste svensk försvarsindustris försäljning av vapen till diktaturer upphöra, en gång för alla.

- Trots dessa nya prioriteringar behöver Sverige ändå ha frihet nog att agera när det verkligen gäller. I dag krävs ett mandat från FN:s säkerhetsråd för att Sveriges riksdag ens ska rösta om deltagande i en internationell insats. Att förlita sig på säkerhetsrådets omdöme är att låta stormakter hindra oss från att agera självständigt. Ryssland och Kina ska inte få bestämma när det är okej för Sverige att hjälpa de som behöver hjälp. Kravet på ett FN-mandat för svenskt deltagande i internationella insatser bör avskaffas.

INTRODUKTION

När det gäller svensk försvarspolitik har de politiska skyttegravarna blivit allt för grunda. Ibland kan man till och med undra om det grävts någon skyttegrav, där det ska föras någon debatt, överhuvudtaget. Det svenska försvaret är inte huvudpunkten i ett modernt Almedalstal och väljare får mest ta del av bestämda ”ja” eller ”nej”-utrop gällande Nato och allmän värnplikt. Regeringar fälls inte, precis som att januariavtal inte heller rivs upp, med anledning av en försvarsmakt i kris och för lite i anslag. Att Sveriges säkerhetsläge under lång tid har försämrats, samtidigt som vi i mångt och mycket står oförberedda, tycks varken fånga politisk vind eller den breda allmänhetens uppmärksamhet.

Visst kan försvarspolitik, vid första anblick, kännas både komplicerat och avskräckande. Det finns mängder av åsikter gällande vilka bataljoner som behöver prioriteras och precis vilka verktyg stridsflyg bör utrustas med. Men vad som därför är viktigt att minnas är att frågan om det svenska försvaret egentligen handlar om allas liv eller död. Försvarspolitiken är värnandet av fred, demokrati, jämställdhet och de grundläggande värderingar som gör just Sverige värt att försvara. Det handlar om vilka skyldigheter vi har gentemot vårt eget land, såväl som vilket ansvar vi har gentemot omvärlden. Det är allvar.

Det vore oseriöst att påstå att nuvarande svensk försvarsförmåga kan garantera landets säkerhet. Vi har en för liten försvarsmakt, brist på soldater som vill stanna i försvaret tillräckligt länge och ett säkerhetsläge där det inte alls går att utesluta att Sverige utsätts för väpnat angrepp. Svaret på varför vi hamnat här har delvis att göra med en naivitet efter kalla krigets slut – en tro om att de stora konflikternas tid var över utvecklades till en historielöshet som sedan kom att leda till forcerade avvecklingar och nedskärningar. Rapportens ena del har således ambitionen att identifiera de problem som finns i Sveriges militära försvar i dag, samt att ge förslag på lösningar in i framtiden.

En viktig aspekt av dagens försvars- och säkerhetsarbete är också att en stor del äger rum på den digitala arenan. Stater och grupperingar som tidigare tänjt på gränser genom kränkningar av territorium med stridsflyg och ubåtar kan nu göra detsamma genom intrång i digital infrastruktur. I Sverige inträffar cyberattacker redan nu i stor skala.

Att vara en högdigitaliserad stat med bristande cybersäkerhet får konsekvenser på försvar och säkerhet. Sveriges cybersäkerhet bedöms vara den näst sämsta bland våra nordiska och baltiska grannar, röra sig på botten i europeiska mått och bara ligga snäppet över medel ute i världen. Att vår höga digitaliseringsgrad kombineras med en förhållandevis låg säkerhet sticker ut i västvärlden. Gapet mellan svensk digitaliseringsnivå och cybersäkerhet är lika stort som det i Namibia, Mongoliet eller Libyen.

I fråga om svensk cybersäkerhet och -försvar har även näringslivet en viktig roll att spela. Ett färskt exempel på dess sårbarhet går att se i den cyberattack som livsmedelskedjan Coop drabbades av under den gångna sommaren. Attackens omfattning tvingade nästan 800 butiker runt om i landet att hålla stängt i flera dagars tid. Om fler livsmedelsbutiker, eller andra leverantörer av samhällsviktig verksamhet, slås ut samtidigt tar det inte lång tid innan samhället märkbart bryts ner.

De luckor som finns inom svensk cybersäkerhet och -försvar kommer att utnyttjas av fientliga aktörer även i framtiden. Hotet som detta innebär måste uppmärksammas. Just därför lägger rapportens första del extra stor vikt vid svenskt försvar i den digitala krigszonen.

I dag avgör försvarspolitik inte en valrörelse. Men den kan, och borde så göra, redan i morgon. Detta är ett försiktigt försök till förberedelse inför en sådan framtid.

DET SVENSKA CYBERFÖRSVARET

Syftet med cyberattacker och IT-intrång mot Sverige kan vara att få tillgång till information om svenska intressen, såsom forskning, säkerhetspolitiska avsikter, företagsplaner och samhällsviktig verksamhet.[3] Cyberattacker kan också användas för att sabotera kritisk infrastruktur, eller som ett första verktyg vid ett militärt angrepp.[4] Konsekvenserna av ett framgångsrikt intrång kan bli stora; så till den grad att det går att likställa allvarliga cyberangrepp med en väpnad attack.[5]

Ett illustrativt exempel är vad som händer om en fientlig aktör slår ut Sveriges elförsörjning. Vattentillförseln upphör fort och endast öppna spisar och kaminer kan generera värme, vilket gör att vatten riskerar att frysa fast i rören samtidigt som inomhustemperaturen sjunker.[6] Butiker behöver stänga eftersom tele- och datakommunikationen påverkas och kortbetalningsdosor och uttagningsautomater slutar att fungera.[7] Strömavbrottet släcker trafikljusen och man kan inte tanka bilen på en bensinmack. Både tåg och kollektivtrafik stannar. Tids nog går det inte heller att använda mobiltelefoni eller datorer. Efter två dygn kommer samhällsviktiga institutioner ha svårt att överhuvudtaget bedriva verksamhet.[8] Ljuset slocknar.

SVERIGE: ETT DIGITALISERAT MEN CYBERSVAGT LAND?

Sverige klassas som ett av världens mest digitaliserade länder, med vana att hamna i absoluta toppen av internationella digitaliseringsindex och mätningar av digital konkurrenskraft.[9] Med den bekräftade digitala kapaciteten är det anmärkningsvärt att Sverige ändå tycks ha halkat efter när det gäller cybersäkerhet och -försvar.

I National Cyber Security Index (NCSI), ett estniskt index som mäter länders krisberedskap, cybersäkerhet och försvar, hamnade Sverige på plats 42 globalt år 2020.[10] Finland och Danmark återfanns på åttonde respektive tolfte plats på samma lista.[11] De kriterier och indikatorer där de svenska resultaten är som lägst rör lagstiftning gällande cybersäkerhet och -försvar, skydd av samhällsviktig infrastruktur och bidragande till global cybersäkerhet.[12]

HOTBILDEN MOT SVERIGE: EN GRÅTONAD KRIGSFÖRING

Enligt den militära underrättelse- och säkerhetstjänsten, Must, är hotbilden mot Sverige präglad av politisk, militär och ekonomisk karaktär.[13] Faktumet att dessa hot sammanvävts med varandra beror på den tekniska utvecklingen. Angreppssätten kan bland annat ta sig uttryck i form av cyberangrepp och påverkansoperationer.[14] Metoderna är, enligt Must, dolda, tvetydiga och möjliga att förneka. Deras syfte är att försvåra beslutsfattande och att försvaga Sveriges tro på sin egen förmåga.[15] Eftersom fienden helst vill gå under radarn och inte bli upptäckt är cyber- och påverkansoperationer effektiva.[16]

---

3 Skrivelse 2016/17:213. *Nationell strategi för samhällets informations- och cybersäkerhet.*
4 Ibid.
5 Ibid.
6 Thomsen, Dante. Vad vet du om strömavbrott? Så här påverkas du och Sverige- timme för timme. SVT Nyheter. https://www.svt.se (Hämtad 2021-06-27)
7 Ibid.
8 Ibid.
9 IMD World Competitiveness Center. *IMD World Digital Competetiveness Ranking 2020*. Institute for Management Development, 2020. (Hämtad 2021-04-23).
10 National Cyber Security Index. Index. *e-Governance Academy Foundation.* 2021. https://ncsi.ega.ee (Hämtad 2021-02-14).
11 Ibid.
12 Skrivelse 2016/17:213.
13 Försvarsmakten. *Must årsöversikt 2020*. 2021. https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/rapporter/must-arsoversikt-2020.pdf (Hämtad 2021-06-06)
14 Ibid.
15 Ibid.
16 Ibid.

Säpo beskriver att digitaliseringen av samhällsviktig infrastruktur utgör en sårbarhet för svensk säkerhetskänslig verksamhet.[17] De identifierar samtidigt runt 15 främmande stater som redan i dagsläget bedriver olovlig underrättelseinhämtning och påverkansoperationer mot Sverige, däribland Ryssland och Kina.[18] Det är också dessa två länder Säpo pekat ut som de mest allvarliga hoten för svensk säkerhet, med anledning av deras cyber- och industrispionage, desinformationskampanjer och påverkansoperationer.[19]

Försvarets radioanstalt, FRA, uppmäter att Sverige utsätts för tiotusentals cyberattacker varje månad.[20] Angreppsmetoderna kan vara allt från att forcera fram lösenord från läckta databaser, angrepp via virusbärande e-postutskick (phishing), serverattacker och angrepp mot mobila enheter för att kunna lyssna av och hämta information från dem.[21] [22]

RYSSLAND OCH KINA

Den ökade militära aktiviteten i Sveriges närområde har lett till att länder, främst Ryssland, stärkt sin underrättelseinhämtning för att kunna vidta förberedande åtgärder i händelse av kris eller krig.[23] Den ryska förmågan att utföra påverkans- och cyberoperationer bedöms vara både god och ett återkommande fenomen.[24]

Under de senaste åren har även Kina flyttat fram sina positioner i Europa. Vi kan se deras strategiska närvaro ta form i vårt närområde, speciellt kring Arktis där Kina är intresserade av att etablera nya transportleder och förbindelser.[25] [26] Initiativet Ett bälte, en väg (BRI) är grunden för den expansion som den kinesiska staten bedriver, och landet utnyttjar andra länders beroendeförhållanden gentemot dem för att åstadkomma politiska, ekonomiska och militära mål inom initiativets ram.[27]

Det kinesiska målet att bli självförsörjande inom nyckelteknologier och all försvarsindustri till år 2025 är något som också påverkar Sverige, en högteknologisk stat av intresse.[28] I enlighet med Kinas statskapitalistiska system görs dessutom ingen distinktion mellan offentlig och privat verksamhet, utan både svenska myndigheter och svensk teknikindustri bedöms utgöra måltavlor inom strategin.[29] [30] Det finns alltså anledning att misstänka att den tekniska kompetens och utveckling som skett i Kina kan härledas, åtminstone delvis, till landets industrispionage och datastöld.[31]

UT I GRÅZONEN

Cyberhotet kan beskrivas som en del av gråzonsproblematiken, det gränsland mellan krig och fred som fientliga krafter medvetet utnyttjar. Fienden har som strategi att agera så nära gränsen för upptäckt som möjligt för att på så sätt kunna vilseleda och överraska den angripna staten.[32] Det här är ett sätt för en fientlig stat att uppnå politiska målsättningar utan att använda de traditionella militära maktmedel som vi vanligtvis klassar som attack och angrepp. Den främmande makten agerar alltså inom våra regler och lagar, ofta under täckmantel av näringsliv och civilsamhälle. Bland metoderna inom gråzonen ingår påver-

17 Säkerhetspolisen. *Säkerhetspolisens årsbok 2019*. 2020. https://www.sakerhetspolisen.se (Hämtad 2021-02-14)
18 Säkerhetspolisen. *Hotbild mot säkerhetskänslig verksamhet*. 2019. https://www.sakerhetspolisen.se (Hämtad 2021-02-14)
19 Säkerhetspolisen. *Säkerhetspolisens årsbok 2020*. 2021. https://www.sakerhetspolisen.se (Hämtad 2021-02-14)
20 Weigel, Björn. *Digitaliseringens baksida: cyberhotets komponenter och konsekvenser*. Frivärld, 2018. (Hämtad 2021-06-05)
21 FRA, Försvarsmakten, MSB, Polisen, Säpo. *Cybersäkerhet i Sverige: Hot, metoder, brister och beroenden*. 2020. https://www.msb.se (Hämtad 2021-06-05)
22 Ibid.
23 Försvarsmakten. *Must årsöversikt 2020*. 2021
24 Ibid.
25 Ibid.
26 Ibid.
27 Ibid.
28 Ibid.
29 Sundbom, Henrik. Informationspåverkan – näringslivet som mål och medel. I *Gråzon*, Katarina Tracz (red.), 69–85. Stockholm: Frivärld, 2021.
30 FRA. *Årsrapport 2017*. FRA, 2017. https://www.fra.se (Hämtad 2021-06-10)
31 Sundbom, Henrik. Informationspåverkan – näringslivet som mål och medel. Gråzon.
32 Ds 2017:66. *Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025*.

kansoperationer, cyberattacker, industrispionage och strategiska uppköp.[33] [34]

Gråzonsproblematiken går hand i hand med icke-linjär krigföring: en strategi där icke-militära aktioner används både i fred och konflikt. Medan den klassiskt linjära och militära krigföringen har som syfte att utplåna motståndaren genom krig finns den icke-linjära krigföringen till för att påverka densamma.[35] Icke-linjär krigföring har i decennier varit en del av rysk militärdoktrin. När väst tenderar att se på gråzonen och icke-linjära medel som ett sätt att undvika krig ser Ryssland på metoderna som en del av krigföringen och använder dem systematiskt.[36]

EXEMPEL PÅ GRÅZONEN: FALLET LYSEKIL

2017 fick Lysekils kommun ett mycket lukrativt erbjudande av ett kinesiskt konsortium. Konsortiet, vars ledning hade nära kopplingar till Kinas kommunistiska parti och militär, ville i kommunen bygga Nordens största hamn med tillhörande vägar, järnväg och en bro.[37] Utöver infrastruktur utlovades också investeringar i lokala skolor, sjukhus och inom äldrevården. Enligt Sveriges radio rörde sig erbjudandet i sin helhet om belopp i miljardklassen.[38] Det kinesiska konsortiet i fråga leddes av Sunbase International Holdings, ett företag som samtidigt ägde alla de 18 markområden i Hong Kong som användes av kinesisk militär.[39]

Lysekil valde att fortskrida med det kinesiska erbjudandet. Jan-Olof Johansson (S), kommunstyrelsens ordförande i Lysekil, uttalade i radio att han inte alls höll med om att det fanns en risk att den kinesiska staten skulle komma att utnyttja hamnen, trots att det aldrig gjorts någon prövning gällande hur investeringen skulle påverka Sveriges säkerhet.[40] Att varken dåvarande utrikesminister Margot Wallström, försvarsminister Peter Hultqvist eller statsminister Stefan Löfven kunde göra något, annat än att möjligtvis varna för den försvars- och säkerhetspolitiska risken, beror på att ett sådant beslut bryter mot varje kommuns rätt till självbestämmande.[41] Värt att nämna är dock att ingen av de nämnda ministrarna sa ett ord om saken.

I slutändan var det omfattande protester som fick idén om ett kinesiskt hamnbygge att dö. Men det skedde inte för att kommunstyrelsen i Lysekil valde att lyssna på folket och besluta så som de önskade, utan för att konsortiet drog sig ur på grund av all negativ medial uppmärksamhet som riktats mot dem.[42]

DEN SVENSKA CYBERSÄKERHETEN

RIKSREVISIONENS SÅGNING

År 2016 granskade Riksrevisionen nio myndigheters arbete med informationssäkerhet.[43] Granskningens samtliga myndigheter, däribland Migrationsverket och Försäkringskassan, bedömdes driva ett för dåligt arbete för att uppfylla de säkerhetskrav som ställs på dem.[44] Riksrevisionen kritiserade regeringen för att inte ge myndigheterna förutsättningar för att bedriva ett godtagbart säkerhetsarbete. [45] Vad som krävdes, enligt Riksrevisionen, var starkare regeringsstyrning av regelverket för informationssäkerhet. Med det skulle myndighe-

33 Ds 2017:66
34 Hökmark, Gunnar. Den grå zonen. I *Gråzon*, Katarina Tracz (red.), 6–38. Stockholm: Frivärld, 2021.
35 Ds 2017:66
36 Ibid.
37 Sundling, Janne. Protester stoppar Kinas miljardhamn i Lysekil. *Fokus.* 2018-01-31. https://www.fokus.se/2018/01/protester-stoppar-kinas-miljardhamn-lysekil/ (Hämtad 2021-06-11)
38 Olsson, Jojje. Sanningen bakom Kinas miljardinvestering i Lysekil. *Fokus*. 2017-12-21. https://www.fokus.se/2017/12/sanningen-bakom-kinas-miljardinvestering-lysekil/ (Hämtad 2021-06-11)
39 Ibid.
40 Ibid.
41 Ibid.
42 Sundling, Janne. Protester stoppar Kinas miljardhamn i Lysekil. *Fokus.*
43 Skrivelse 2016/17:42. *Riksrevisionens rapport om informationssäkerhetsarbete på nio myndigheter.*
44 Ibid.
45 Ibid.

terna kunna prioritera sitt arbete på området.[46]

En annan kritik från revisionen var att det saknades uppgifter om kostnader för informationssäkerhet, både på myndighetsnivå och inom statsförvaltningen i sin helhet. På grund av det blev det omöjligt för Riksrevisionen att analysera säkerhetsarbetets kostnadseffektivitet.[47] Än i dag, ungefär sex år senare, är kostnaderna för detta inte kända.

MYNDIGHETERS FÖRVALTNINGSKULTUR

Sverige har ett avskalat regeringskansli, under vilket det står starka och självständiga myndigheter. Regeringen får visserligen styra hur myndigheterna arbetar, men inte hur de tolkar lagarna eller fattar beslut i enskilda ärenden.[48] [49] Medan en VD i ett privat företag fattar beslut och står till svars för dessa gentemot sin styrelse, är motsvarande styre från en minister över en myndighet förbjudet enligt lag. Sverige saknar, med andra ord, ministerstyre. Den enskilda ministern har i teorin ganska lite att säga till om gällande myndigheternas hantering av lagar och enskilda ärenden.

KOMMUNER: INDEXET

2017 genomfördes en undersökning av IT-rådgivarna Radar Ecosystem Specialist. Undersökningen gick ut på att mäta olika branschers arbete med cybersäkerhet. Resultatet för varje bransch vägdes sedan mot de risker som finns inom deras respektive områden.

Här framkom det tydligt att Sveriges kommuner är i särklass sämst på cybersäkerhet. Deras cybersäkerhetsarbete är outvecklat, trots hög riskprofil och hantering av känslig medborgarinformation.[50]

- 50 procent av kommunernas svarande uppgav att deras digitala strategi ej var i samspel med deras övergripande säkerhetsstrategi.
- 70 procent av kommunerna uppdaterade sin säkerhetspolicy/strategi mer sällan än vartannat år.
- 50 procent av kommunerna saknade organiserad utbildning i cybersäkerhet.
- 70 procent av kommunerna hade inte ett implementerat regelverk för att hantera förebyggande säkerhetsarbete.
- Kommuner var överrepresenterade i svaren som uppgav att man inte gör någon analys av skyddsvärda tillgångar överhuvudtaget.
- 80 procent av kommunerna hade ambitionen att kunna återställa sin drift först 36 timmar efter svårt cyberangrepp.

NÄRINGSLIV: MED EKONOMI SOM MOTIV OCH HOT

Som tidigare nämnts drabbas inte bara myndigheter och statsapparaten av cyberangrepp, utan även näringslivet är utsatt. Ett färskt exempel är den cyberattack som slog ut Coop i juli 2021. Efter en internationell attack riktad mot den IT-leverantör som tillhandahåller Coops kassasystem tvingades närmare 800 butiker att hålla stängt.[51] Hackergruppen som påstod sig ligga bakom, ryska Revil, krävde sedan 600 miljoner kronor för att öppna upp servrarna.[52] Det är visserligen lätt att se på händelsen som ett olyckligt missöde, eller bara en smäll för en aktör på den privata marknaden, men attacker som dessa kan få konsekvenser för den svenska säkerheten i stort. Slås flera butikskedjor ut samtidigt hotas Sveri-

46 Ibid.
47 Ibid.
48 RF 12. kap 2-3 §§
49 Regeringskansliet. Myndigheterna. *Regeringskansliet.* https://www.regeringen.se/ (Hämtad 2021-06-15)
50 Radar Ecosystem Specialists. *Svenskt IT säkerhetsindex 2.0: En undersökning i samarbete med Advenica, Dataföreningen, SIG Security och Christer Magnusson, doktor informationssäkerhet Stockholms universitet*. Radar Ecosystem Specialists, 2017.
51 Magnusson, Mattias, Fahlman, Fredrik och Mellgren, Fredrik. Kassahaveri på Coop efter utpressningsattack. *SvD*. 2021-07-03. https://www.svd.se/it-attack-mot-coops-kassasystem (Hämtad 2021-07-07).
52 Träff, Matilda/ TT. Hackade Coop: kräver 600 miljoner. *SvD*. 2021-07-05. https://www.svd.se/coop-har-polisanmalt-it-attacken (Hämtad 2021-07-07).

ges livsmedelsförsörjning fort, vilket i sin tur riskerar att både skapa kaos och få samhället att brytas ner.

Ytterligare en aspekt av hur cyberangrepp riskutsätter svensk ekonomi och svenska företag är stöld av immateriella rättigheter (på engelska: ”*intellectual property*”, förkortat IP). IP-stöld kan bland annat innebära att patent, forskningsresultat och industrihemligheter stjäls av statligt sponsrade hackergrupper för att främja ekonomisk och militärindustriell utveckling i den egna staten.[53]

Även om det saknas exakta uppskattningar för just Sverige beräknas EU förlora runt 55 miljarder euro årligen på grund av cyberspionage.[54] Den årliga förlusten USA gör på IP-stöld rör sig om uppemot 600 miljarder dollar per år.[55] USA pekar ut Kina som den primära IP-antagonisten, en bild som också delas av EU-kommissionen.[56] [57] I Kinas 10-årsplan, *Made in China 2025*, uppmuntras kinesiska bolag att investera i utlandet (och i synnerhet inom kritisk infrastruktur) för att komma över just IP.[58] [59]

I en undersökning av Svenskt Näringsliv berättar några av Sveriges största företag att de utsätts för cyberbrottslighet på daglig basis. Inte ett enda av dessa företag beskriver den svenska statens förmåga att skydda företagen i positiva ordalag. I stället används uttryck som ”*enormt dålig*”, ”*lika med noll*” och att frågan ”*faller mellan stolarna*” .[60]

SVERIGES NATIONELLA CYBERSTRATEGI: ÄNNU ETT DOKUMENT TILL HÖGEN?

Den senaste (och första) cyberstrategi som Sverige har är från 2016. I den betonas att svenskt cybersäkerhet och -försvar kräver koordinering av kompetenser.[61] [62] För säkerhetspolitiska ändamål behöver Sverige förbättra sin förmåga att förebygga, upptäcka och hantera cyberattacker. Sverige behöver också öka bekämpningen av IT-relaterad brottslighet och stärka det internationella samarbetet.[63]

Cyberstrategin föreslår en nationell modell för säkerhetsarbete. Denna ska leda till bättre samordning av svensk cybersäkerhet.[64] Modellen ska höja lägstanivån för informationssäkerheten i Sverige, men regeringen riktar primärt in sig på statliga myndigheter.[65] Den utelämnar således Sveriges kommuner, de som presenterats som sämst i klassen på de frågor som denna strategi ska behandla. Likaså har näringslivet ställts utanför strategins räckvidd.

Utöver ovan nämnda brister saknar strategin bindande status, mätbara målsättningar och konkreta metoder för att nå fram till de uppsatta målen. Det är svårt att se hur regeringens cyberstrategi använts under de gångna åren. Det är till och med svårt att avgöra om den använts överhuvudtaget.

---

53 Ds 2019:8. Försvarsberedningen. *Värnkraft - Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025*.

54 Lee-Makiyama, Hosuk. *Stealing Thunder: Cloud, IoT and 5G will Change the Strategic Paradigm for Protecting European Commercial Interests. Will Cyber Espionage be Allowed to Hold Europe Back in the Global Race for Industrial Competitiveness?* European Centre for International Political Economy, 2018. https://ecipe.org/publications/stealing-thunder/ (Hämtad 2021-06-10)

55 The National Bureau of Asian Research. *Update to the IP Commission Report*. 2017. https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf (Hämtad 2021-06-11)

56 Ibid.

57 Europeiska kommissionen. *Commission Staff Working Document: Report on the protection and enforcement of intellectual property rights in third countries*. 2021. https://trade.ec.europa.eu/doclib/docs/2021/april/tradoc_159553.pdf (Hämtad 2021-06-11)

58 Tracz, Katarina. Cyberhotet och säkerhetsskulden. I *Gråzon*, Katarina Tracz (red.), 85–98. Stockholm: Frivärld, 2021.

59 Lentz, Carl. Made in China 2025 ska ge högteknologiskt övertag. *Utrikesmagasinet*. 2019-03-14. https://www.ui.se/utrikesmagasinet/analyser/2019/mars/made-in-china-2025-ska-ge-hogteknologiskt-overtag/ (Hämtad 2021-06-10)

60 Svenskt näringsliv. *Företagen och IT-säkerheten – hotbilder, motåtgärder och behov*. 2021. https://www.svensktnaringsliv.se/ (Hämtad 2021-07-04)

61 Ds 2017:66

62 Skrivelse 2016/17:213

63 Ibid.

64 Ibid.

65 Ibid.

VAD SÄGER ANSVARIGA MYNDIGHETER?

FRA, Försvarsmakten, MSB, Polisen och Säpo beskriver i en gemensam rapport att arbetet med cybersäkerheten går ”trögt”. Vad som görs räcker inte i förhållande till de hot Sverige står inför, menar de.[66]

Myndigheterna påvisar att det finns återkommande brister i samhällets säkerhetsarbete. Det kan handla om lågt engagemang och otydlig ansvarsfördelning i säkerhetsfrågor, dåliga riskanalyser, luckor i regler och att säkerhetsåtgärder inte genomförs.

En annan påtaglig risk är den kompetensbrist som finns inom cybersäkerhet. Det svenska tekniska kunnandet är högt, men det saknas tillräcklig kompetens inom cybersäkerhet för att kunna möta det behov som finns. Kompetensbristen kan i sin tur förklara varför myndigheter inte arbetar systematiskt med att identifiera sina skyddsvärden, uppkomsten av säkerhetsincidenter och varför det så ofta är bristande krav på cybersäkerhet när verksamheter genomför upphandlingar. År 2022 bedöms underskottet av spetskompetens inom cybersäkerhet ligga på cirka 70 000 personer enbart i Sverige.[67]

DET NATIONELLA CENTRET FÖR CYBERSÄKERHET

År 2020 beslutade regeringen att FRA, Försvarsmakten, MSB och Säpo ska inrätta ett nationellt cybersäkerhetscenter. Syftet är att stärka Sveriges förmåga att förebygga, upptäcka och hantera cyberhot.[68] [69]

Genom centret ska myndigheterna koordinera hanteringen av cyberangrepp och förmedla råd om hot, sårbarheter och risker. Det ska också utgöra en plattform för samverkan mellan privata och offentliga aktörer inom cybersäkerhetsområdet. Denna samverkan uppges vara central, men vilka målgrupper eller områden som kommer att omfattas har ännu inte presenterats.[70]

INCIDENTRAPPORTERING FÖR STATLIGA MYNDIGHETER

En IT-incident beskrivs av MSB som ”*en oönskad och oplanerad IT-relaterad händelse som kan påverka säkerheten i organisationens eller samhällets informationshantering och som kan innebära en störning i organisationens förmåga att bedriva sin verksamhet*”.[71]

År 2020 rapporterades 286 incidentrapporter från statliga myndigheter – ett antal som ligger på samma nivå som föregående tre år. Den vanligaste incidenten har varit ”handhavandefel”, näst vanligaste ”angrepp” och tredje vanligaste ”störning i mjuk- eller hårdvara”.[72] I 36 procent av dessa incidentrapporter angav berörd myndighet att incidenten haft ”stor” eller ”mycket stor” konsekvens.[73] Med tanke på hur myndigheternas cybersäkerhetsarbete kritiserats för sina brister kan man argumentera för att en utsatt myndighets egen konsekvensanalys inte säger mycket alls om cybersäkerhetens status.

Att kommuner inte omfattas av MSB:s incidentrapportering påverkar onekligen myndighetens förmåga att ge en fullskalig lägesbild av Sveriges säkerhet. MSB:s statistik på detta

66 FRA, Försvarsmakten, MSB, Polisen, Säpo. *Cybersäkerhet i Sverige: Hot, metoder, brister och beroenden*. 2020
67 Ibid.
68 Regeringskansliet. Regeringen inrättar ett nationellt cybersäkerhetscenter. *Regeringskansliet*. 2020. https://www.regeringen.se/pressmeddelanden/2020/12/regeringen-inrattar-ett-nationellt-cybersakerhetscenter/ (Hämtad 2021-06-13)
69 Fö2019/01330 *Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter.*
70 Nationellt cybersäkerhetscenter. Frågor och svar om cybersäkerhetscentret. *FMV, FRA, Försvarsmakten, MSB, Polisen, PTS, Säpo.* https://www.cfcs.se/fragor-och-svar/ (Hämtad 2021-06-13)
71 MSB. It-incidentrapportering för statliga myndigheter. *MSB*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/it-incidentrapportering-for-statliga-myndigheter/ (Hämtad 2021-06-07)
72 MSB. Statliga myndigheters it-incidentrapportering 2020. *MSB*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/it-incidentrapportering-for-statliga-myndigheter/it-incidentrapportering-2020/ (Hämtad 2021-06-07)
73 MSB, *Statliga myndigheters it-incidentrapportering 2020: utmaningar för en säker och robust informationshantering.* MSB. 2021. https://rib.msb.se/filer/pdf/29488.pdf (Hämtad 2021-06-07)

område är alltså i bästa fall meningslös, och i värsta fall missvisande.

För övrigt är det värt att notera att de statsunderstödda angrepp som upptäckts främst rört sig om underrättelseinhämtning och spionage, men också om förberedelser för sabotage. Cyberangrepp sker så dolt som möjligt för att försvåra spårning och förhindra attribution, det vill säga att angriparen knyts till aktionen och således kan pekas ut offentligt. På grund av det upptäcks sällan angrepp genom säkerhetssystem eller incidentrapportering, utan via signalspaning och kartläggande sensorer.[74]

NIS-DIREKTIVET: INCIDENTRAPPORTERING FÖR LEVERANTÖRER AV SAMHÄLLSVIKTIGA TJÄNSTER

I enlighet med EU:s NIS-direktiv så ska även leverantörer av samhällsviktiga tjänster arbeta med incidentrapporter.[75] [76] NIS-reglerna innebär att leverantörer inom samhällsviktiga tjänster, såsom exempelvis energi och transport, ska arbeta systematiskt med informationssäkerhet. Reglerna omfattar också leverantörer inom digital infrastruktur.

I Sverige har NIS-direktivet implementerats genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Den leverantör som varken anmäler, vidtar säkerhetsåtgärder eller rapporterar incidenter som inträffat tvingas betala en sanktionsavgift.[77]

Om leverantören av en samhällsviktig tjänst är ett småföretag saknar det skyldigheter under NIS-direktivet. EU har nämligen en gräns på att leverantörers årsomsättning ska vara över 10 miljoner euro och ha minst 50 anställda för att omfattas av kraven.[78]

SÄKERHETSSKYDDSLAGEN

Sveriges säkerhetsskyddslag gäller för utövare av säkerhetskänslig verksamhet.[79] Här ingår krav på säkerhetsanalys, säkerhetsprövning av den som ska anställas i säkerhetskänslig verksamhet och krav på tystnadsplikt.[80]

Problemet med säkerhetsskyddslagen är att det saknas statlig befogenhet att besluta om sanktionsavgifter för den verksamhet som inte följer lagen. Detta är en klar kontrast mot de konsekvenser som uppstår vid överträdelser i det nyss nämnda NIS-direktivet, där det finns ett etablerat sanktionssystem.

STATSRÅDSBEREDNINGENS KRISENHET

Regeringskansliet utgörs av tre pelare: departementen, deras förvaltningar och Statsrådsberedningen. Just Statsrådsberedningen inrättades under Tage Erlanders tid och kan beskrivas som ett departement specifikt till för statsministern. Det består av flera kanslier, däribland statministerns eget, ett för samordning och det nyligen inrättade säkerhetspolitiska rådet.[81] Statsrådsberedningens huvudsakliga uppgift är att leda och samordna arbetet i Regeringskansliet.[82]

Under Alliansens tid i regeringsställning 2006–2014 inrättades Kansliet för krishantering vid Statsrådsberedningen. Kansliet, med 40 anställda, var en konstant bemannad krisenhet

74 Ds 2019:8. Försvarsberedningen.
75 Europaparlamentets och Rådets Direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen och Direktiv 2016/1148 (EUT L 194/1 19.7.2016), s. 22.
76 MSB. *Statliga myndigheters it-incidentrapportering 2020*. 2021.

77 SFS 2018:1174. *Informationssäkerhet för samhällsviktiga och digitala tjänster.*
78 MSB. NIS-direktivet. *MSB*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/ (Hämtad 2021-06-07)
79 SFS 2018:585. *Säkerhetsskyddslag*. 1 kap. 1 §
80 SFS 2018:585. 2 kap. 1 §, 3 kap. 1 § och 5 kap. 2 §
81 Regeringskansliet. Statsrådsberedningens organisation. *Regeringskansliet*. 2021-06-23. https://www.regeringen.se/sveriges-regering/statsradsberedningen/statsradsberedningen-organisation/ (Hämtad 2021-06-12).
82 Regeringskansliet. Statsrådsberedningen. *Regeringskansliet.* https://www.regeringen.se/ (Hämtad 2021-06-12)

med uppdrag att slå larm och samordna vid en eventuell kris.[83] Dess struktur baserades på Katastrofkommissionens rekommendationer efter tsunamikatastrofen 2004. Kommissionen framhöll att en krisenhet behövde inrättas, och att dess ledning bör ha direkt tillgång till statsministern för att snabbt få mandat att agera i kris.[84]

En granskning publicerad av Dagens Nyheter visar dock att statsminister Stefan Löfven hösten 2014 flyttade över kansliet för krishantering till justitiedepartementet[85]. Numera ansvarar inrikesminister Mikael Damberg för krisledningen, trots att inrikesministern (och för den delen också justitieministern) saknar de centrala befogenheter som kansliet för krishantering byggde på från första början. Många av de kritiska beslut som kan komma att efterfrågas av krisenheten är det bara statsministern som har befogenhet att fatta.

83 Carlsson, Mattias och Holmström, Mikael. Stefan Löfven lyfte bort ansvaret från sig själv. *DN*. 2015-12-22. (Hämtad 2021-06-10)
84 Ibid.
85 Ibid.

DET SVENSKA CYBERFÖRSVARET

FRA:s och Försvarsmaktens gemensamma definition av cyberförsvar är *”en nations eller annan aktörs samlade förmågor och åtgärder, såväl offensiva som defensiva, till skydd för dess kritiska samhällsfunktioner samt förmågan att försvara sig mot kvalificerade angrepp”*.[86]

Cyberförsvaret leds primärt av Försvarsmakten och är anpassat för högre konfliktnivåer, men ska även ha kapacitet att verka i fredstid och i kris.[87] Allmänheten saknar tillgång till detaljerad information gällande vilka medel och metoder som används i Sveriges aktiva cyberförsvar.[88] Vad som offentliggjorts är dock att det i huvudsak är en kombination av:

- **Förebyggande åtgärder**, såsom säkerhetsgranskning och rådgivning gällande begränsning av en motståndares attack eller skadeverkning.[89]
- **Underrättelse- och nätverksinhämtning**, för att samla information och kartlägga motståndarens identitet, nätverk, information och datorer.[90]
- **Defensiva operationer,** vilket innebär försvarandet av informationssystem, däribland elektroniska kommunikationsnät, för att förhindra motståndare att påverka information, informationssystem, datorer eller nätverk.[91]
- **Offensiva operationer,** vilket är att förhindra motståndaren att använda sina system, eller tvinga densamma att avbryta en attack mot de svenska.[92]

IKFN-FÖRORDNINGEN

IKFN-förordningen är de regler Försvarsmakten står under då svenskt territorium kränks av utländsk militär i fredstid.[93] [94] Förordningen beskriver att Försvarsmakten ska upptäcka och avvisa kränkningar av svenskt territorium samt ingripa vid överträdelser av tillträdesförordningen. När det kan fastslås att utländsk militär befinner sig på, och samtidigt kränker, svenskt territorium har Försvarsmakten skyldighet att agera.[95]

Notera att IKFN-förordningen upphör att gälla om regeringen förklarar att Sverige är i krig. I dessa fall är det de regelverk som verkar under krigsfara och krig som i stället träder i kraft.[96] [97]

CYBERSOLDAT

Försvarsmakten har sedan 2020 en värnpliktig grundutbildning (GU) med fokus på cyberförsvar.[98] I GU cybersoldat ingår en militär grundutbildning (GMU) och en cyberförsvarsutbildning i samarbete med Kungliga Tekniska Högskolan (KTH).[99] Ett arbete som cybersoldat inkluderar att analysera cyberhot, omvärldsbevakning och att bedriva logganalys på

86 Ds 2017:66
87 Försvarsmakten. Cyberförsvar. *Försvarsmakten.* https://www.forsvarsmakten.se/sv/var-verksamhet/det-har-gor-forsvarsmakten/cyberforsvar/ (Hämtad 2021-06-21).
88 Zouave, Erik. *Aktiva operationer på cyberdomänen: Folkrättslig normativ utveckling*. FOI, 2019.
89 Ds 2017:66
90 Ds 2017:66
91 Försvarsmakten. Cyberförsvar. *Försvarsmakten.* https://www.forsvarsmakten.se/sv/var-verksamhet/det-har-gor-forsvarsmakten/cyberforsvar/
92 Ibid.
93 IKFN är en förkortning för ”ingripanden vid kränkningar av Sveriges territorium under fred och neutralitet, m.m.”
94 SFS 1982:756. *Om Försvarsmaktens ingripanden vid kränkningar av Sveriges territorium under fred och neutralitet m.m. (IKFN-förordning).*
95 Nordgren Christensen, Annika. Planering i gråzonen. I *Gråzon*, Katarina Tracz (red.), 53–69. Stockholm: Frivärld, 2021.
96 SFS 1982:756
97 MSB. *Gemensamma grunder för samverkan och ledning vid samhällsstörningar*. MSB, 2018. https://rib.msb.se/filer/pdf/28738.pdf (Hämtad 2021-06-13)
98 Försvarsmakten. Cyberförsvar. *Försvarsmakten.* https://www.forsvarsmakten.se/sv/var-verksamhet/det-har-gor-forsvarsmakten/cyberforsvar/
99 Ibid.

drift- och säkerhetsloggar.[100]

Den som vill genomföra GU cybersoldat måste först klara av mönstringsunderlaget hos Plikt- och prövningsverket, som varje 18-åring inlämnar via ett webbformulär. Frågorna i formuläret motiveras med att grundutbildning med värnplikt är både fysiskt och psykiskt krävande. Därför är det viktigt att inte ha några skador, sjukdomar eller andra hälsotillstånd som antingen förvärras eller utsätter andra för en risk.[101] Baserat på uppgifterna i mönstringsunderlaget bedömer sedan Plikt- och prövningsverket vilka som kallas till mönstring. Vid mönstringen ingår bland annat ett styrketest och ett fysiskt arbetsprov som genomförs på en testcykel vars belastning ökar gradvis.

Resultaten på fysisk (men även mental) kapacitet i kombination med en allmän hälsokontroll vägs sedan ihop för att bedöma den mönstrandes tjänstbarhet. Om den mönstrande klassas som tjänstbar kallas denne till en utökad mönstring. Först då genomförs specifika tester för cybersoldatsutbildningen.[102]

ARTIFICIELL INTELLIGENS (AI)

AI kan enkelt beskrivas som när ett datorsystem resonerar och självständigt agerar korrekt utifrån information och tidigare erfarenhet.[103]

Trots att AI inte är specifikt framtaget för militära syften, kan det användas med sådan intention. Under cyberattacker är ett välfungerande AI-system en stor fördel: systemet kan nämligen bearbeta stora mängder data medan det samtidigt analyserar och finner mönstret i informationen den hittar.[104] Därefter klarar AI-systemet att agera självständigt eller leverera analys, beslutsunderlag och rekommendation till mänskliga beslutsfattare.[105] Den största fördelen är att det går fort.

Inga tillgängliga dokument, styrningsbrev eller budgetar tyder på att AI inkorporeras i svenskt försvar i någon större utsträckning.

100 Försvarsmakten. Cybersoldat. *Försvarsmakten.* https://jobb.forsvarsmakten.se/sv/utbildning/befattningsguiden/gu-befattningar/cybersoldat/ (Hämtad 2021-06-13)
101 Plikt- och prövningsverket. Mönstringsunderlaget. Plikt- och prövningsverket. 2021. https://pliktverket.se/monstring-och-varnplikt/monstring/monstringsunderlaget (Hämtad 2021-06-13).
102 Försvarsmakten. Cybersoldat. *Försvarsmakten.* https://jobb.forsvarsmakten.se/sv/utbildning/befattningsguiden/gu-befattningar/cybersoldat/
103 Andersson, Christer, Gustavi, Tove och Karasalo, Maja. *Artificiell intelligens – möjligheter och utmaningar för Sveriges nationella säkerhet*. FOI, 2019.
104 Ibid.
105 Ibid.

EN INTERNATIONELL UTBLICK

DEN FORMBARA CYBERRYMDEN

Utvecklingen av de regler, lagar och normer som ska gälla i cyberrymden är långt ifrån klar. Det råder ingen enighet om staters rätt till självförsvar i händelse av en cyberattack, eller vilka motåtgärder som är tillåtna att vidta. Det saknas också en allmänt accepterad gräns för när en cyberattack är så pass allvarlig att den kan klassas som våldsanvändning (vilket i sin tur aktiverar ett FN-lands rätt till självförsvar).[106] [107] [108] Vi saknar dessutom bindande lagar och konventioner gällande militära cyberoperationer.

Svensk försvars- och säkerhetspolitik utgår från att skydda grundläggande rättigheter, samt att värna en världsordning grundad i folkrätten[109]. Hur de två utgångspunkterna ska anpassas specifikt till cyberförsvaret är inte bestämt, mer än att det ska göras i ”*enlighet med folkrättens legala principer*”.[110] Till skillnad från exempelvis Finland har Sverige inte offentliggjort sina nationella ståndpunkter om folkrätt i cybermiljö.[111] Det är alltså okänt om Försvarsmakten, regeringen eller någon annan relevant del av det svenska totalförsvaret har en tydlig utgångspunkt som de arbetar efter.

FN

FN anses vara viktiga i arbetet med cyberregelverk, då det ofta är genom FN som internationellt bindande dokument kan upprättas.[112] Vid FN:s kontor för nedrustningsfrågor finns en expertgrupp med fokus på cyberfrågor. Arbetet ska resultera i årliga rapporter och resolutioner på området, men på grund av gruppens oförmåga att nå konsensus har rapporterna uteblivit vid ett flertal tillfällen.[113]

Däremot har FN lyckats kartlägga staters syn på cyberteknologi och militär användning.[114] Här framkommer en tydlig enighet om att folkrätt gäller även inom cyberdomänen.[115] När det gäller militärt agerande i cyberdomänen upplever sig dock stater sakna internationell vägledning. De vet inte hur regleringen av mänskliga rättigheter ser ut, eller hur krigslagar och principen om suveränitet ska anpassas.[116] [117]

EU

Europeiska kommissionens senaste cyberstrategi (2020) pekar på riskerna med att EU saknar en kollektiv lägesbild av cyberhotet.[118] Det sker ingen systematisk informations- och incidentrapportering på EU-nivå. I händelse av en gränsöverskridande cyberattack eller kris saknas samverkan medlemsstater sinsemellan, såväl som mellan medlemsstater och EU:s olika organ.[119] [120]

I strategin från 2020 föreslår kommissionen bland annat:

106 FN. *Charter of the United nations and Statute och the International Court of Justice*. FN, 1945.
107 Ibid.
108 Utrikesministeriet. Finland publicerade sina ståndpunkter om folkrätt i cybermiljön. *Utrikesministeriet.* 2020-10-15. https://um.fi/nyheter/-/asset_publisher/GRSnUwaHDPv5/content/suomi-julkisti-n-c3-a4kemyksens-c3-a4-kansainv-c3-a4lisest-c3-a4-oikeudesta-kyberymp-c3-a4rist-c3-b6ss-c3-a4 (Hämtad 2021-06-13).
109 Folkrätt: de regler och principer som reglerar hur stater och andra internationella aktörer ska samarbete och agera gentemot varandra, enligt regeringen.
110 Zouave, Erik. *Aktiva operationer på cyberdomänen: Folkrättslig normativ utveckling*. FOI, 2019.
111 Utrikesministeriet. Finland publicerade sina ståndpunkter om folkrätt i cybermiljön. *Utrikesministeriet.* 2020-10-15.
112 Zouave, Erik. *Aktiva operationer på cyberdomänen: Folkrättslig normativ utveckling*. FOI, 2019.
113 Ibid.
114 Ibid.
115 Ibid.
116 Suveränitet: staters oberoende från andra staters ingripande
117 Zouave, Erik. *Aktiva operationer på cyberdomänen: Folkrättslig normativ utveckling*. FOI,
118 Europeiska kommissionen. *The EU's Cyber Strategy for the Digital Decade*. Bryssel: Europeiska kommissionen, 2020-12-16. (Hämtad 2021-06-13)
119 Ibid.
120 Ibid.

- **En gemensam cybersköld.** Förslaget är att bygga operativa säkerhetscenter genom EU för att stötta redan existerande center med träning och kompetensutveckling, såväl som att etablera nya.[121]
- **En gemensam cyberenhet.** Enheten föreslås bli en plattform för samarbete mellan EU-länders cybersäkerhetsenheter. Extra fokus ska ligga på operativ koordinering vid gränsöverskridande attack.[122]
- **En utvecklad cyberdiplomati.** EU har sedan tidigare ett regelverk som gör att ekonomiska resurser tillhörande den person, stat eller grupp som begått en allvarlig cyberattack kan frysas.[123] I strategin föreslås detta regelverk utvecklas vidare.[124] EU ska, som en del av detta, också konkretisera hur cyberattacker mot kritisk infrastruktur, demokratiska institutioner och IP-stölder ska bemötas mer effektivt. Därutöver planeras cyberdiplomatin att bli bättre på att attribuera cyberattacker, och samarbetet med internationella partner (exempelvis Nato) ska stärkas.[125]
- **Ett mer kapabelt cyberförsvar.** En granskning av nuvarande cyberförsvarspolicy ska presenteras och cyberrymden ska fortsätta ses som en arena där EU genomför försvarsoperationer. Vidare ska cyberförsvarets samverkan i frågor som rör rymdindustri och civilt försvar utvecklas.

I kommissionens rapport om hur arbetet med strategin fortskridit under det senaste året redovisas de olika komponenterna var för sig.[126] Rapporten kan sammanfattas med att processen till en början gått ut på att skapa planer och påbörja diskussioner medlemsstater sinsemellan inför strategins fortsatta implementering.[127] Det lär således dröja tills, som allra tidigast, 2022 innan det går att utvärdera strategin i praktiken.

NATO

Nato beskriver sitt cyberförsvar som en huvudsaklig uppgift. Cyberrymden klassas som en domän som ska ha ett Nato-försvar likvärdigt det som finns i luften, på marken och i vattnet. Det innebär också att organisationens kollektiva försvar kan aktiveras även i händelse av en allvarlig cyberattack.[128] År 2016 avlade dessutom Natos medlemsstater en ed om att förstärka sina respektive cyberförsvar.[129]

Nato har en dygnet runt-tillgänglig cyberförsvarssupport för sina medlemsstater, samt ett ”Rapid Reaction”-team som kan aktiveras och rycka ut för att skydda Natoländers nätverk.[130] Utryckningsteamet ska ha kapacitet att svara och lösa en cyberincident inom det första dygnet.[131] Den icke-medlemsstat som önskar få hjälp från Natos cyberenhet måste först få en förfrågan godkänd av Nordatlantiska rådet.[132]

Nato genomför regelbundna övningar i cyberförsvar, såsom årliga Cyber Coalition Exercise, i vilken Sverige deltagit.[133] Det är också Nato som, inom ramen för sitt cyberför-

121 Ibid.
122 Ibid.
123 *Rådets förordning (EU) 2019/796 av den 17 maj 2019 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater*. Europeiska unionens officiella tidning, 2019. https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX-:32019R0796&from=EN (Hämtad 2021-06-13)
124 Europeiska kommissionen. *The EU's Cyber Strategy for the Digital Decade*.
125 Ibid.
126 Europeiska kommissionen. *Rapport om genomförandet av EU:s strategi för cybersäkerhet för ett digitalt decennium*. Bryssel: 2021. https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=JOIN:2021:14:FIN&from=EN (Hämtad 2021-09-09)
127 Ibid.
128 Minárik, Tomáš. NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. *The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/* (Hämtad 2021-06-13).
129 Nato. Cyber Defence Pledge. *Nato*. 2016. https://www.nato.int/cps/en/natohq/official_texts_133177.htm (Hämtad 2021-06-13).
130 Nato. NATO Cyber Defence. *Nato*. 2016. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf (Hämtad 2021-06-13).
131 Nato. NATO Rapid Reaction Team to fight cyber attack. *Nato.* 2012. https://www.nato.int/cps/en/natolive/news_85161.htm (Hämtad 2020-06-13)
132 Ibid.
133 Nato announces start of Cyber Coalition exercise. *Army Technology*. 2020-11-17. https://www.army-technology.com/news/nato-announces-start-of-cyber-coalition-exercise/ (Hämtad 2020-06-13)

svarsarbete, tagit fram en av de mest omfattande akademiska publikationerna gällande cyberförsvar och folkrätt: Tallinnmanualen.[134] Manualen är inte juridiskt bindande, men då internationella överenskommelser kring cyberförsvar saknas har den ofta använts som referens.[135]

134 Zouave, Erik. *Aktiva operationer på cyberdomänen: Folkrättslig normativ utveckling*. FOI, 2019.
135 Ds 2017:66, s. 114.

FRAMTIDENS CYBERFÖRSVAR: REFORMFÖRSLAG

VEM STYR DEN HÄR BÅTEN?

I dag går det inte att säga att Sverige har en klarlagd, primär aktör ansvarig för cybersäkerhet och cyberförsvar. Direktiven spretar åt olika håll, samtidigt som ”samordning” och ”koordination” slängs ut i luften till den grad att det nästan ter sig ironiskt. Krav på mer samarbete måste också omsättas till faktiska resultat, och det måste bli tydligt vad som gäller när det är allvar. Sverige behöver en nationell plan för vad som ska göras i händelse av en storskalig kris, likaväl som en krisplan som berör cyberattacker och dess specifika konsekvenser.

- **Inrätta en samlad nationell plan i händelse av kris och en krisplan specifikt utformad för storskaliga cyberattacker.**

Cyberstrategin som togs fram 2016 och ligger på bordet än i dag är varken en rekommendation eller bindande gentemot någon aktör. Det har gjort den tandlös. Här lyser dessutom kommunerna – Sveriges kanske svagaste cyberlänk – med sin frånvaro och problemen med IP-stölder och cyberspionage tas upp utan någon idé om åtgärd. Regeringen skriver gång på gång om vad som är viktigt, men utan att väga upp all denna vikt med konkreta förslag eller ekonomiska medel. Myndigheter kan samordna i all oändlighet, men utan direktiv och mandat kan de inte nå särskilt långt.

- **Ta fram en ny cyberstrategi**

Cybersäkerheten är en fråga som fördelas på hela fyra departement och åtta myndigheter. Det är positivt att fyra av dessa myndigheter nu bildar ett cybersäkerhetscenter. Problemet är att centret fortfarande inte gett Sverige en nationell myndighet, departement eller minister med mandat att agera. Samordning av kompetens är visserligen viktigt, men det måste finnas någon som har det sista ordet när det verkligen gäller. Det är speciellt viktigt vid attacker och kriser, när myndigheter inte har tid att nå konsensus kring beslut.

- **Inrätta en primär nationell aktör inom cybersäkerheten**

GLÖM INTE STATSMINISTERN!

I slutändan styrs inte Sverige av myndigheter och deras samordnande grupperingar, utan av en ytterst ansvarig: statsministern. Därför är det oroande att den nuvarande Statsrådsberedningen är organiserad så att akuta krissituationer som ska hanteras på högsta nivå istället skjuts bort. Att Sveriges statsminister saknar en egen krisledningsenhet försvagar landet.

- **Återinför den centrala krisledningsenheten i Statsrådsberedningen**

Regering och statsminister måste komma närmare myndigheter och departement i frågan om cybersäkerhet. En cybersäkerhetschef direkt underställd statsministern med uppgift att agera knytpunkt mellan parterna i cybersäkerhetsfrågan vore en konkret åtgärd för ökad samordning.[136]

- **Inrätta en cybersäkerhetschef i Statsrådsberedningen**

136 Nicander, Lars. ”Nu behövs en koordinator för cybersäkerheten”. *DN.* 2017-07-21. https://www.dn.se/debatt/nu-behovs-en-koordinator-for-cybersakerheten/ (Hämtad 2021-06-15).

TYDLIGARE MINISTERANSVAR

En återkommande kritik, bland annat från Riksrevisionen, är att regeringen måste bli tydligare i sin myndighetsstyrning. En bromskloss är dock den svenska förvaltningsstrukturen som sätter allt för långtgående gränser för hur denna styrning får och inte får gå till. Doktor Lars Nicander, enhetschef för asymmetriska hot- och terrorismstudier vid Försvarshögskolan, beskriver att en anledning till att informationssäkerheten i Sverige inte kommit längre beror på landets förvaltningsstruktur.[137] Nicander beskriver att just bristen på ministerstyre ger enskilda myndigheter ett ordentligt informationsövertag gentemot Regeringskansliet, och att detta medför obalans.

Utöver denna obalans föreligger också risken att förbudet mot ministerstyre får ministrar att dribbla bort sitt eget ansvar och, i värsta fall, gömma sig bakom sina myndigheter. År 2012 avslöjades det att Sverige planerade att hjälpa Saudiarabien att bygga en vapenfabrik. Då skyllde dåvarande försvarsminister Sten Tolgfors på FOI, myndigheten under honom, och det blev genast svårt att avgöra var ansvaret skulle vila.[138]

Sveriges förbud mot ministerstyre är tämligen unikt; majoriteten av demokratiska länder styrs tillåter ministerstyre, inklusive våra grannar Norge och Danmark.[139] Så länge en minister inte har ansvar för myndighetsbeslut är det svårt att utkräva fullt ansvar från våra högst uppsatta politiker. Detta är en brist, inte minst när det gäller frågor som rör rikets säkerhet. Sverige bör införa ministerstyre.

- **Inför ministerstyre**

EN OVETANDE RIKSDAG?

Ett annat problem i det politiska ansvarsutkrävandet är riksdagens minimala roll i statens säkerhets- och krisarbete. Begränsade möjligheter till ansvar riskerar också att färre politiker känner skyldighet till detsamma. På så sätt tillåts cybersäkerheten fortsatt vara en nedprioriterad fråga i politiken.

Här kan USA tjäna som förebild. Landets senat har nämligen ett utskott för militär underrättelse. *U.S. Senate Select Committee on Intelligence*, SSCI, har i uppgift att övervaka amerikansk underrättelseinhämtning och överlämna lagstiftningsförslag på området. SSCI ska också granska den amerikanska underrättelseaktiviteten och säkerställa att den är i enlighet med lagen och den amerikanska konstitutionen.[140] Utskottet består av 15 senatorer, 8 från majoriteten och 7 från minoriteten. Fördelningen är konstant och inte anpassad efter senatens partiproportioner i ett försök att värna om underrättelsefrågans partineutrala natur.[141] De senatorer som är en del av utskottet får utökad tillgång till annars sekretessbelagt material, såsom budget, metoder och faktisk underrättelseinhämtning.[142]

- **Inrätta ett specialutskott i riksdagen som behandlar underrättelse- och cyberfrågor**

HOTEN I GRÅZONEN

Exemplet med hamnen i Lysekil är inte unikt, utan är en del av en strategi som tillämpas av Kina och Ryssland runtom i världen. Ingenting tyder på att försök av detta slag kommer

137 Ibid.
138 Detta har hänt: Vapenfabriken i Saudiarabien. *Sveriges radio*. 2013-03-11. https://sverigesradio.se/artikel/5017387 (Hämtad 2021-06-16)

139 Utrikesdepartementet. *Danmark – Mänskliga rättigheter, demokrati och rättstatens principer: situationen per den 30 juni 2018.* 2018. https://www.regeringen.se/ (Hämtad 2021-06-15)
140 U.S. Senate Select Committee on Intelligence. Overview of the Senate Select Committee on Intelligence Responsibility and Activites. *U.S. Senate Select Committee on Intelligence.* https://www.intelligence.senate.gov/about (Hämtad 2021-06-16)
141 Ibid.
142 Ibid.

att minska och Sveriges styrningsstruktur utgör då en svaghet för motståndaren att utnyttja.

Till skillnad från länder som Storbritannien, USA och Kanada saknar Sverige en central instans som granskar säkerheten i utländska investeringar. Inte heller tillåter vårt starka kommunala självstyre, i kombination med förbudet mot ministerstyre, att en minister går in och avbryter en utländsk investering som utgör en fara. För att kunna avvärja hot som säkerhetspolitiskt riskabla uppköp och investeringar är det fullt rimligt att det kommunala självstyret begränsas i frågor som rör Sveriges säkerhet.

- **Begränsa det kommunala självstyret i frågor som rör rikets säkerhet**

MYNDIGHETER, INCIDENTETER OCH SÄKERHETSSKYDDSLAG

Att NIS-leverantörerna måste ha fler än 50 anställda och en årsomsättning på över 10 miljoner euro är dåliga mått för vilka som ska täckas av incidentrapportering, då det säger väldigt lite om de konsekvenser ett cyberangrepp har på samhället i stort. Bättre vore om kriterierna prioriterade det antal kunder leverantörerna når ut till. På så sätt får MSB en överblick av hur stort område som slås ut vid ett storskaligt cyberangrepp.

- **Omvärdera kriterierna för incidentrapportering så att de primärt täcker antalet påverkade kunder, snarare än anställda och omsättning**

Den nya säkerhetslagen ställer onekligen krav på upphandling, kontroll av säkerhetsskydd och inför flera viktiga skyldigheter, men så länge det saknas ett system för sanktionsavgifter kommer lagen inte att tas på allvar.

- **Inför ett sanktionssystem för de leverantörer som inte lever upp till säkerhetsskyddslagen**

CYBER OCH NÄRINGSLIV

Statsunderstödda aktörer gör sällan skillnad på offentlig och privat sektor när de agerar i gråzonen. Ändå saknas konkreta förslag för samverkan mellan svensk offentlighet och näringslivet i Sveriges cyberstrategi.

Det nationella centret för cybersäkerhet har som mål att stödja näringslivet på lång sikt, men att inte inkludera näringslivet från början kan sluta med att näringslivet inte inkluderas alls. Denna struktur blir en kultur som sedan institutionaliseras i centret, i enlighet med vad Teknikföretagen påpekat.[143] Om det nationella centret ska kunna stödja näringslivet när det är färdigutvecklat måste näringslivet vara en del av centret från första början. På sikt borde dessutom vissa branschorganisationer och företag ges platser direkt i centret, något som redan är verklighet i Norge.[144]

Det nationella centret kan bli mötesplatsen för privat och offentlig cybersäkerhet, och att här inrätta ett nationellt cybersäkerhetsråd där bådadera ingår vore lämpligt.[145]

- **Låt näringslivet ingå som en del av det nationella cybercentret.**
- **Inrätta ett nationellt cybersäkerhetsråd där både näringsliv och offentlig sektor ingår.**

Svenska staten har ansvar att skydda och stödja svenska företag, om inte annat för att fö-

143 Säkerhets- och försvarsföretagen och Teknikföretagen. Näringslivets syn på Sveriges kommande nationella cybersäkerhetscenter. *Säkerhets- och försvarsföretagen och Teknikföretagen.* 2020-04-23. https://www.teknikforetagen.se/globalassets/news/inspel/2020/naringslivets-syn-pa-sveriges-kommande-nationella-cybersakerhetscenter.pdf (Hämtad 2021-06-17)

144 Ibid.

145 Tracz, Katarina. Cyberhotet och säkerhetsskulden. I *Gråzon*, Katarina Tracz (red.).

retagen ska vara konkurrenskraftiga och, på längre sikt, undvika företagsflykter. Att hjälpa företag med cybersäkerhet kan innebära att presentera omfattande hot- och riskbilder som näringslivet kan ta del av och förhålla sig till.

- **Presentera hot- och riskbilder inom cybersäkerhet och gråzonsproblematik för näringsliv och allmänhet att ta del av.**

EU och USA utgör en tredjedel av världens ekonomi och är utsatta för kostsamma IP-stölder och industrispionage.[146] Om dessa stormakter tar fram en gemensam strategi för cyberrelaterad brottslighet kan det påverka Kina, den huvudsakliga statsaktören inom dessa typer av brott.[147]

- **Verka för en gemensam strategi mellan USA och EU gällande cyberrelaterad brottslighet.**

CYBERFÖRSVAR

I en tid där cyberrymden prioriteras allt mer behöver Sverige röra sig åt rätt håll. Det svenska försvaret består i dag av tre försvarsgrenar: armén, marinen och flygvapnet. Dessa kännetecknas av egna verksamhetsområden med specifika uppgifter, samt helt egna förband. Flera länder har etablerat cyberförsvaret som en egen försvarsgren, däribland Norge.[148] Över tid bör även Sverige etablera cyberförsvaret som en egen gren, och därmed likställa det med de tre områden försvaret fokuserar på sedan tidigare.

- **Etablera cyberförsvaret som en egen försvarsgren.**

Idén om att skapa en hög tröskeleffekt i totalförsvaret kan ses på som en vågskål som ska balanseras jämnt ut. Åstadkommer Sverige en hög tröskeleffekt i vårt cyberförsvar på bekostnad av det militära kommer skålarna hamna i obalans och resultatet bli en låg militär tröskel och avskräckningsförmåga. Detsamma gäller självklart också om vi har en hög militär tröskel och en låg inom cyberförsvar. Totalförsvarets civila och militära komponenter måste alltså vara samstämmiga och i takt med varandra, annars förlorar de sin kraft. Därför är det problematiskt att de ligger separerade från varandra i Regeringskansliet. Det civila försvaret, som skjutits över till justitiedepartementet, bör föras tillbaka under försvarsdepartementet och där stå parallellt med vårt militära försvar.

- **Återinrätta ansvaret för det civila försvaret till försvarsdepartementet.**

Precis som Annika Nordgren Christensen, tidigare ledamot av Försvarsberedningen, påpekat vore det oklokt att, i upprustningen av det civila försvaret, förbise den gråzonsproblematik som allt oftare präglar den svenska hotbilden.[149] Gråzonskompetensen, däribland cyberangrepp, måste byggas in i civilförsvarets upprustning.

- **Inkludera gråzonskompetens i upprustningen av det civila försvaret.**

Med hjälp av AI skulle Försvarsmakten kunna förbättra sin kvalité och effektivitet när det kommer till analyser av data och komplexa underrättelseoperationer. I det civila försvaret hade ett AI-system haft förmågan att notera avvikelser tidigt. AI hade, bland annat, kunnat varna om avvikelser i nätverkstrafik, vilket är ett tecken på cyberattack mot exempelvis el- eller vattenförsörjningen.[150]

146 Eurostat. China, US and EU are the largest economies in the world. *Eurostat*. 2020-05-19. https://ec.europa.eu/eurostat/documents/portlet_file_entry/2995521/2-19052020-BP-EN.pdf/bb14f7f9-fc26-8aa1-60d4-7c2b509dda8e (Hämtad 2021-06-18)
147 Tracz, Katarina. Cyberhotet och säkerhetsskulden. I *Gråzon*, Katarina Tracz (red.).
148 Forsvaret. Organisasjon. *Forsvoret.* https://www.forsvaret.no/om-forsvaret/organisasjon (Hämtad 2021-06-12).
149 Nordgren Christensen, Annika. Planering i gråzonen. I *Gråzon*, Katarina Tracz (red.).
150 Andersson, Christer, Gustavi, Tove och Karasalo, Maja. *Artificiell intelligens – möjligheter och utmaningar för Sveriges nationel-*

- **Inkorporera mer AI i Försvarsmakten, i cyberoperationer och i det civila försvaret.**

CYBERKOMPETENSEN: SOLDATER OCH HEMVÄRN

Cybersoldater i Försvarsmakten krävs redan i dag, och det behövs säkerligen fler i morgon. En potentiell cybersoldat riskerar dock att aldrig nå fram till Försvarsmakten på grund av de stelbenta krav som ställs på personer för att överhuvudtaget klassas som tjänstbara. Vissa av de mest kvalificerade för att bli cybersoldater kan sållas ut från mönstring redan vid den första, formulärsbaserade fasen, hindrade av knäproblem eller annat som hämmar fysisk kapacitet.

Försvarsmakten beskriver själva att det viktigaste inte är att en cybersoldat kan ”springa fort” eller ”lyfta tungt”, utan kompetenser såsom analytisk och logisk förmåga. Problemet är att det krävs just fysiska förutsättningar för att komma till de tester där man får uppvisa de förmågor som GU cybersoldat kräver. Den kompetens som Försvarsmakten verkligen behöver riskerar därför att aldrig fångas upp.

Mycket tyder på att de fysiska kraven beror på att en värnpliktsutbildning också innefattar en militär grundutbildning, GMU, som innehåller fysiskt krävande uppgifter. Frågan är dock om det är värt att alla potentiella cybersoldater måste klara en standardiserad GMU när problemen med personalförsörjningen i Försvarsmakten är så pass omfattande. En fysiskt anpassad GMU för cybersoldater, eller undantag från dess genomförande, borde inte vara ett problem – speciellt inte i förhållande till den kompetensvinst det kan innebära.

Ur ett perspektiv som strikt ser till att förbättra och utöka Sveriges cyberförsvar går det inte att påstå att det är viktigt att en cybersoldat kan sitta x minuter på en belastad cykel, eller springa tillräckligt många mil. Om Försvarsmakten luckrade upp regler om fysisk förmåga för tjänstbarhet skulle detta öppna för fler att kunna, och vilja, genomföra en värnplikt som cybersoldat (såväl som andra värnpliktsutbildningar som egentligen inte kräver fysisk förmåga). Det vore ett steg mot ett starkare försvar.

- **Luckra upp de fysiska kraven för att få genomföra specifika värnpliktsutbildningar och gör det enklare för fler att bli cybersoldater.**

Estland klassas som ett av världens främsta länder inom cyberförsvar. Ett försvarsområde som gör landet tämligen unikt är att de har etablerat ett cyberhemvärn: Küberkaitse üksus.[151] Det estniska hemvärnet beskrivs bestå av cyberspecialister, individer med vilja att bidra till försvaret och specialister på juridiska och ekonomiska aspekter av cybersäkerhet.[152]

Det svenska hemvärnet är uppdelat i olika förband som skyddar och stödjer samhället vid kris.[153] Tjänstgörande är frivilligt och de flesta hemvärnssoldater har tidigare genomfört värnplikt eller militär grundutbildning, men vissa saknar militär erfarenhet. I dag har Sverige inget hemvärnsförband specialiserat på cyber. För att bredda det svenska cyberförsvaret borde detta förändras.

- **Etablera ett cyberhemvärn.**

---

la säkerhet. FOI, 2019.

151 Nordlund, Linda. Estlands utrikesminister: Varje krig kommer ha cyberdimension. *SVD*. 2017-02-04. https://www.svd.se/varje-krig-kommer-att-ha-en-cyberdimension (Hämtad 2021-06-17).

152 Kaitselit. Estonian Defence Leauge’s Cyber Unit. *Estonian Defence League*. https://www.kaitseliit.ee/en/cyber-unit (Hämtad 2021-06-17).

153 Försvarsmakten. Hemvärnet. *Försvarsmakten*. https://www.forsvarsmakten.se/sv/var-verksamhet/det-har-gor-forsvarsmakten/hemvarnet/ (Hämtad 2021-06-17).

NAME AND SHAME: ATTRIBUTION OCH IKFN-FÖRORDNINGEN

IKFN-förordningen gäller under fred och neutralitet, och just därför är den högst relevant i en tid då gråzonen utnyttjas allt mer. Först när förordningen sätts i spel kan Försvarsmakten avvärja kränkning av vårt territorium. Huvudansvaret slutar då att vila på våra civila myndigheter.[154] För att IKFN överhuvudtaget ska träda i kraft krävs det att angriparens identitet går att fastställa. Därför måste Sverige prioritera arbetet med att attribuera, det vill säga hitta och identifiera, angripare som rör sig i gråzonen.

- **Prioritera försvarets förmåga till attribution av statsunderstödda angripare.**

IKFN-förordningen täcker inte Sveriges cyberdomän, detta då den inte ingår i definitionen av svenskt territorium. I en tid där digitala hot blir allt större måste Sveriges syn på territoriella gränser hänga med. Cyberdomänen bör klassas som en del av svenskt territorium, och IKFN-förordningen utvidgas därefter.

- **Inkludera cyberdomänen som en del av svenskt territorium.**

Eftersom det svenska rättsväsendet inte kan åtala gärningsmän bakom utländska cyberattacker behövs alternativa metoder för att hävda oss mot angripare. Om en cyberattack mot Sverige utförs av en statlig aktör måste det få konsekvenser, politiska såväl som diplomatiska. Sverige behöver utveckla en egen attributionsstrategi, samt bidra till utvecklingen av EU:s redan framgångsrika cyberdiplomati.

- **Etablera en svensk cyberdiplomati i händelse av attackerande statsaktörer.**
- **Verka vidare för utvecklad cyberdiplomati inom EU.**

EN CYBERFÖRSVARSDOKTRIN

Att Sverige ska ha ett cyberförsvar tycks så gott som alla vara eniga om, men *hur* cyberförsvaret ska agera är däremot inte lika klart. När cyberförsvarets offensiva och defensiva förmågor vidareutvecklas behöver vi staka ut de principer som gäller när dessa förmågor används. För att kunna svara på frågor som *när* och *var* cyberförsvaret ska användas krävs en svensk cyberförsvarsdoktrin.

- **Etablera en svensk cyberförsvarsdoktrin.**

Att de internationella forumen inte etablerat samtal och nått enighet får inte hindra Sverige från att säga var vi står. En svensk cyberförsvarsdoktrin skulle leda till en självständig och konkret syn på cyberförsvar på global nivå. Den skulle också tydliggöra våra prioriteringar i det internationella samfundet. Sverige bör presentera den cyberförsvarsstrategi som formats nationellt för att på så sätt bidra internationellt.

- **Offentliggör den svenska cyberförsvarsdoktrinen internationellt.**

INTERNATIONELLA SAMARBETEN

EU-ambitioner om att samordna hotbilder, ha gemensamma krisplaner vid cyberangrepp och en operativ förmåga är positivt. För ett sådant omfattande, och säkerligen kostsamt, arbete måste Sverige våga gå in med krav på att uppsatta mål också uppfylls. Vi bör stötta och driva på i EU:s cyberförsvarsarbete, men utan att se på det som ett substitut för ett mycket nödvändigt arbete på hemmaplan.

- **Stötta EU:s planer på en gemensam cybersköld och cyberenhet.**

154 Nordgren Christensen, Annika. Planering i gråzonen. I *Gråzon*, Katarina Tracz (red.).

Sverige gör rätt i att fortsätta träna tillsammans med Nato i deras *cyber range*, så länge det fortsätter att öka vår egen förmåga. Att Nato dessutom klassar cyberdomänen som en del av varje stats territorium är attraktivt, speciellt sett ur det svenska behovet av att stärka avskräckningsförmågan. På cyberförsvarsfronten finns det alltså fördelar att hämta genom ett medlemskap, men mer om det senare.

- **Delta i internationella övningar inriktade på cyberförsvarsförmågan.**

DET MILITÄRA FÖRSVARET

Trots att cyberattacker är ett av framtidens mest påtagliga hot kommer det militära hotet att bestå även framöver. Det största hotet i vårt närområde, Ryssland, visar på fortsatt aggression mot sin omgivning. Rysslands militära förmåga beräknas dessutom öka de kommande tio åren.[155] Sveriges försvarsberedning konstaterar att ett väpnat angrepp mot Sverige inte kan uteslutas. Samtidigt bedöms vår krigsorganisation vara begränsad på grund av en underdimensionerad volym och struktur.[156]

ETT SVENSKT FÖRSVAR, ETT BORTGLÖMT FÖRSVAR?

Siffrorna talar tydligt om hur svenskt försvar prioriterats av våra politiker. FOI har tagit fram en överblick av Sveriges officiella försvarsutgifter mellan 1900 och 2019, med siffror justerade till 2019 års prisnivå. Vad som går att utläsa är att försvarsutgifterna, av naturliga skäl, prioriterats mest under de båda världskrigen samt under kalla kriget. Efter Berlinmurens fall år 1989 höll sig försvarsutgifterna någorlunda stabila fram till millennieskiftet då de började minska. När man, utöver detta, ser på försvarsutgifter som andel av Sveriges BNP har det varit en ständigt sjunkande trend sedan mitten av 1960-talet.[157]

En iakttagelse som i mångt och mycket bekräftar bilden av försvarspolitiken som åsidosatt och nedprioriterat görs av Erik Lagersten, kommendör i Försvarsmaktens reserv och tidigare informationsdirektör i Försvarsmakten. I SVD skriver Lagersten att svenska regeringar och Försvarsmakten ständigt tenderar att planera för att minsta möjliga ansats i fred kommer att få maximalt möjligt utfall i krig.[158] Ett illustrerande exempel han använder är hur regeringsinstruktioner och ekonomiska förutsättningar mellan 2008 och 2015 tvingade fram lättrörliga militära förband på Gotland. Tanken var att de militära förbanden, i stället för en fast närvaro, först vid eskalerande hot skulle skickas ut för placering på ön – en hållning helt inkompatibel med rysk militärstrategi.[159]

Målbilden för Sveriges försvar lades om efter kalla kriget. Försvarsmakten gick från att fokusera på uppgiften att skydda Sverige från invasion till att bli en ledande nation i internationella insatser. När Ryssland inledde sitt krig mot Georgien 2008 hade Sverige därför avvecklat en stor del av den konventionella militären.[160] Kriget utbröt dessutom, och mycket ironiskt, samma år som Försvarsmakten fått i uppgift att skala bort hela 2,8 miljarder kronor från den svenska materielplaneringen.[161] De prognoser som gjorts om det svenska säkerhetsläget visade sig vara fel.

Försvarsmakten påtalar att de är i behov av högre prioritering än i dag. I sin årsrapport för 2020 beskriver de att en stor del av myndighetens markmateriel, såsom stridsfordon och olika robotar, är ålderstigen och kräver stora resurser för att ens hållas fungerande.[162] Gammal markmateriel leder till ökade reparationskostnader som, i sin tur, påverkar Försvarsmaktens möjlighet att bedriva den grundläggande verksamheten. Det påverkar de svenska krigsförbanden negativt. I rapporten beskriver Försvarsmakten även att förbandens mobiliseringsförmågor må ha utvecklats, men gjort så från en så pass låg nivå att den ännu inte uppnår myndighetens mål. Återigen ser vi tecken på den bristande prioritet som präglat

155 Ds 2019:8.
156 Ibid
157 Alozious, Juuko. Sveriges försvarsutgifter 1900-2022. FOI, 2020.
158 Lagersten, Erik. Självklart borde Sverige ingå en försvarsallians med Finland. *SVD*. 2020-01-13. https://www.svd.se/sjalvklart-borde-sverige-inga-en-forsvarsallians-med-finland (Hämtad 2021-06-20)
159 Ibid.
160 Claesson, Michael. Försvarsmakten i dag. I *Sveriges försvarspolitik – En antologi*, Zebulon Carlander och Oscar Karlflo (red.), 54-89. Stockholm: Ekerlids Förlag, 2020.
161 Ibid.
162 Försvarsmakten. *Försvarsmaktens årsredovisning 2020*. Försvarsmakten, 2021

försvaret under en längre tid.

DEN TERRITORIELLA HOTBILDEN MOT SVERIGE

STÄNDIGT DETTA RYSSLAND

Enligt Must har den militära aktiviteten i svenskt närområde fortsatt att öka både i intensitet och komplexitet.[163] Under 2019 och 2020 var den militära aktiviteten runt oss den högsta sedan slutet av kalla kriget.[164] Ryssland pekas ut som en tydlig huvudaktör, vars militära verksamhet i vårt närområde ökat sedan Putins tillträde som president år 2000. Landet bedöms ha blivit mer villigt att använda militära medel, och de strävar efter att säkerställa militär handlingsfrihet gentemot Nato.[165] Ryssland fortsätter att öka sin militära förmåga i enlighet med sin militärreform och beväpningsprogram från 2008, fastän statsfinansiella skäl sänkt takten något.[166] Den ökade ryska aktiviteten i världen, allra främst den illegala annekteringen av Krim 2014, har också lett till ökad upprustning från västländerna.[167]

FÖRSVARSMAKTENS UPPGIFT

I riksdagens mål för Försvarsmaktens operativa förmåga ingår bland annat att:

- Omedelbart möta väpnat angrepp
- Bestrida fientlig, operativ kontroll
- Uthålligt fortsätta strid
- Mobilisera krigsorganisationen under pågående angrepp och utan förberedelsetid
- Skydda kritisk verksamhet och infrastruktur
- Ge och ta emot militärt stöd till och från andra stater.[168]

Fram tills 2030 har Försvarsmakten i uppgift att i fredstid öka förmågan att:

- Upptäcka och identifiera hot mot Sverige
- Skydda egen verksamhet och infrastruktur
- Lösa krigsuppgifter med hela krigsorganisationen en vecka efter att regeringen beslutat om höjd beredskap och allmän mobilisering.[169]

TOTALFÖRSVARET 2021–2025: MOTSTÅNDSKRAFT OCH TRÖSKELEFFEKT

Då svenskt försvar nedprioriterats ekonomiskt under en längre tid innebär en stor del av uppbyggandet av svensk motståndskraft tillförandet av resurser.

I propositionen ”Totalförsvaret 2021–2025” föreslog regeringen att försvarsbudgeten skulle öka med 27 miljarder kronor under 2021–2025. Det innebar en ökning med 40 procent från tidigare försvarsbudget. Antalet värnpliktiga skulle fördubblas och uppgå till 8 000 om året. Tio år senare ska antalet tjänster i svensk krigsorganisation vara 90 000 (i jämförelse med nuvarande 60 000).[170]

TURER I FÖRSVARSBEREDNING OCH RIKSDAG

I sin slutrapport *Värnkraft (2019)* enades Försvarsberedningen, riksdagens forum för samråd inom försvarspolitiken, om både förslag och inriktning för svenskt försvar. Problem uppstod dock när Socialdemokraterna, i sista stund, vägrade binda sig till den ekonomiska ram som skulle krävas för en finansiering. Det fick de forna allianspartierna att vägra skriva under rapporten.[171] [172] Några månader senare meddelade Överbefälhavarens militära råd

163 Östersjönsregionen, Barents hav och Nordatlanten
164 Försvarsmakten. *Must årsöversikt 2020*. 2021
165 Ibid.
166 Ibid.
167 Ibid.
168 Försvarsdepartementet. *Inriktning för Försvarsmakten 2021–2025*. Regeringen, 2020
169 Ibid.
170 Prop. 2020/21:30
171 Wallberg, Peter/TT. Försvarsuppgörelse klar – tillskott på 13 miljarder. *DN*. 2020-09-18. https://www.svd.se/dn-regeringen-c-och-l-overens-om-forsvaret (Hämtad 2021-06-22)
172 Gummesson, Jonas. Öppet försvarsbråk – M hotar med att inte delta. *SVD*. 2020-02-26. https://www.svd.se/oppet-brak-om-

att bara hälften av beredningens förslag skulle kunna genomföras till 2025, och endast tre fjärdedelar fram till 2030, på grund av för litet ekonomiskt utrymme.[173]

År 2020 presenterade Centerpartiet och Liberalerna en överenskommelse med regeringen som sedan blev en del av den slutliga försvarspropositionen. I tidigare förhandlingar hade de forna alliansparterna krävt ökade anslag med 45 miljarder mellan 2026–2030, vilket i denna uppgörelse reducerats till 13 miljarder för samma period.[174] [175] Exakt hur miljarderna för åren 2026 och framåt ska finansieras sköts upp till en ny Försvarsberedning år 2023.[176] Socialdemokraterna har således inte bundit sig vid att öka anslagen. Från 2025 och framåt är alltså Sveriges upprustningsplan ofinansierad.

REKRYTERING I ETT FÖRSVAR SOM EXPANDERAR

När Försvarsmakten rustas upp avslöjas också en negativ personalutveckling. Försvarsmakten behöver öka personalmängden för att fortsätta framåt, men med tanke på de år som gått förlorade riskerar det att bli en politisk uppgift som är bra mycket svårare än att bara höja antalet värnpliktiga och hoppas på det bästa.

VÄRNPLIKTEN

DE FÖRSTA 109 ÅREN

Mellan 1901 och 1989 var det varje vuxen mans skyldighet att göra värnplikt i Sverige (och från 1994 fick kvinnor möjlighet att genomföra värnplikten på samma sätt som män).[177] På 1990-talet ändrades värnpliktslagen så att Försvarsmakten endast kallade det antal värnpliktiga som behövdes för att säkerställa krigsorganisationens (minskande) beredskap. Från mitten av 00-talet hölls värnpliktsutbildningen fortsatt igång, men då med främsta syfte att hitta frivilliga att ta anställning och delta i internationella insatser.[178] Strax därefter, år 2010, ersattes värnplikten av en frivillig militär utbildning.[179] Försvarsmaktens personalförsörjning skulle från och med då grunda sig i en modell byggd på anställda, frivilliga soldater.[180]

2010 TILL 2017

Några år efter att den allmänna värnplikten ersatts med den frivilliga militära utbildningen visade det sig att kvantiteten och kvaliteten på Försvarsmaktens bemanning av insatsorganisationen dalat. Enligt det försvarsbeslut som fattades år 2009 skulle Försvarsmakten år 2014 ha 50 000 befattningar, men den fick ett underskott på 6 000.[181]

Annika Nordgren Christensen, som år 2016 utsågs av regeringen att utreda ett svenskt personalförsörjningssystem baserat på plikt och frivillighet, beskriver att det byggts upp en utbildningsskuld inom Försvarsmakten.[182] Sedan 2010 har Försvarsmakten inte rekryterat och utbildat i de volymer som behövts.[183] Det har delvis berott på att frivilligsystemet haft för låga incitament och att man felbedömt hur lång tid anställda inom Försvarsmakten

forsvaret--hultqvist-vill-ha-ny-grupp (Hämtad 2021-06-22).

173 KU-anmälan 2020/21:36. *Försvarsminister Peter Hultqvist agerande i samband med försvarsförhandlingarna inför totalförsvarsbeslutet*.

174 Holmström, Mikael. Försvaret får mer pengar – men kritik för underfinansiering. *DN*. 2020-09-18. https://www.dn.se/sverige/forsvarsuppgorelse-klar-nytt-regemente-i-kristinehamn/ (Hämtad 2021-06-22).

175 Gummesson, Jonas. Borgerligt motbud – vill se ny brigad i Stockholm. *SVD*. 2020-05-20. https://www.svd.se/borgerligt-motbud--vill-se-ny-brigad-i-stockholm (Hämtad 2021-06-22)

176 Holmström, Mikael. Försvaret får mer pengar – men kritik för underfinansiering. *DN*. 2020-09-18.

177 Säkerhetspolitik. Historia: värnplikten. *MSB*. 2015. https://www.sakerhetspolitik.se/Forsvar/totalforsvarsplikt/Historia-Varnplikten/ (Hämtad 2021-06-22).

178 Claesson, Michael. Försvarsmakten i dag. I *Sveriges försvarspolitik – En antologi*, Zebulon Carlander och Oscar Karlflo (red.),

179 Försvarsmakten. Värnplikten genom åren. *Försvarsmakten*. https://www.forsvarsmakten.se/sv/information-och-fakta/var-historia/artiklar/varnplikt-under-109-ar/ (Hämtad 2021-06-22)

180 Claesson, Michael. Försvarsmakten i dag. I *Sveriges försvarspolitik – En antologi*, Zebulon Carlander och Oscar Karlflo (red.),

181 Försvarsmakten. Värnplikten genom åren. *Försvarsmakten*. https://www.forsvarsmakten.se/sv/information-och-fakta/var-historia/artiklar/varnplikt-under-109-ar/ (Hämtad 2021-06-22)

182 Nordgren Christensen, Annika. Personalförsörjningen. I *Sveriges försvarspolitik – En antologi*, Zebulon Carlander och Oscar Karlflo (red.), 110-129. Stockholm: Ekerlids Förlag, 2020.

183 Ibid.

stannar inom myndigheten.

SOU 2016:63 visade att Sverige, i förhållande till 2014 års nivåer, behövde rekrytera åtminstone 4 000 personer årligen för att tillgodose försvarets behov.[184] Då hade frivillighetsreformen resulterat i att snittet rekryter varit endast 2 500 per år.[185]

2017 OCH FRAMÅT

Sedan 2017 har alla 18-åriga totalförsvarspliktiga kallats till mönstring och, för dem där mönstringen gått hela vägen, vidare till värnpliktsutbildning. Regeringen bestämmer det antal värnpliktiga som ska tas ut till värnpliktsutbildning, baserat på behoven som de bedömer att Försvarsmakten har.[186]

4 900 påbörjade sin värnpliktsutbildning år 2020. Andelen som 2019/20 slutförde värnpliktsutbildningen låg på cirka 90 procent. Av dessa fortsatte 44 procent med ett engagemang i Försvarsmakten.[187]

SOLDAT- OCH OFFICERSYRKET

Parallellt med att personalförsörjningsutredningen påvisade en dyster bild av rekryteringen var inte heller redovisningen av Försvarsmaktens anställda särskilt positiv. 800 heltidstjänstgörande och 6 600 tidvis tjänstgörande gruppbefäl, soldater och sjömän (GSS) saknades för att kunna möta försvarets uppsatta målbild.[188]

I en medlemsundersökning från Officersförbundet uppgav 60 procent av officerarna och 70 procent av Försvarsmaktens gruppbefäl, soldater och sjömän att de övervägt att lämna försvaret.[189] Till absolut största del grundade sig detta i för låg lön och otillfredsställda anställningsvillkor.[190] Undersökningen visade också att 50 procent av de anställda inte trodde att deras chefer har mandat att sätta löner, och två av tre upplevde att de saknade möjlighet att påverka lönen, trots lönesamtal som genomförs.[191] Trots detta fanns ändå en positiv uppfattning om att vara anställd; 60 procent av undersökningens tillfrågade hade en positiv syn på Försvarsmakten som arbetsgivare.[192]

Genomsnittstiden för tjänstgörande gruppbefäl, soldater och sjömän var ungefär fyra år 2016. I den tidigare nämnda utredningen påpekades att denna relativt korta tjänstgöringstid behövde förlängas för att säkerställa personalförsörjningen. De tjänstgörande behöver hållas kvar med starkare incitament. Lyckas man med det, menade utredaren, skulle den operativa effekten i krigsförbanden höjas. Det skulle också minska belastningen och rekryteringskostnaderna för Försvarsmakten.[193] Anledningen till att de flesta av GSS avslutar sin tjänstgöring beror på en övergång till studier, eller vilja att övergå till studier.[194]

Försvarsmakten beskriver att utbildningarna som leder till anställning inom myndigheten är avgörande för dess personalförsörjning och organisatoriska behov.[195] Därför är det glädjande att officersprogrammet har ökat i attraktivitet de senaste sex åren. Från 2015 till 2020 har antalet sökande till officersprogrammet mer än fördubblats, och antalet re-

184 SOU 2016:63
185 Ibid.
186 SFS 1941:967. *Värnpliktslag*.
187 Försvarsmakten. *Försvarsmaktens årsredovisning 2020*. Försvarsmakten, 2021. https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/arsredovisningar/arsredovisning-2020/forsvarsmaktens-arsredovisning-2020-huvuddokument.pdf (Hämtad 2021-06-20)
188 SOU 2016:63
189 Officersförbundet, Ipsos. *Officersförbundets medlemsundersökning - Den militära personalens syn på sitt yrke och Försvarsmakten*. Officersförbundet, 2016. http://mb.cision.com/Public/3498/2039512/aa9e21eeb421dc06.pdf (Hämtad 2021-06-23)
190 Ibid.
191 Ibid.
192 Ibid.
193 SOU 2016:63 s. 167.
194 Ibid.
195 Försvarsmakten. *Försvarsmaktens årsredovisning 2020*. Försvarsmakten, 2021

gistrerade studenter har också ökat i en allt snabbare takt.[196] År 2020 erbjöds 220 av 795 sökande en plats vid officersprogrammet. I år, 2021, har över 1 000 personer sökt. Antalet erbjudna platser förväntas landa i höjd med föregående års, vilket dock är att betrakta som ett minimum i förhållande till Försvarsmaktens behov.[197]

196 Försvarshögskolan. Över 1000 sökande till Officersprogrammet. *Försvarshögskolan*. 2021. https://www.fhs.se/arkiv/nyheter/2021-02-09-over-1000-sokande-till-officersprogrammet.html
(Hämtad 2021-06-24)
197 Ibid.

INTERNATIONELLT SAMARBETE

Samarbeten och koalitioner är viktigt för Sverige, både för att utveckla kompetensen i vår egen militära styrka och för den krigsavhållande förmågan.[198] Samtidigt är det också viktigt att, i en tid där försvars- och säkerhetspolitiska hot mot Sverige ökar, säkerställa att svenska styrkor och medel används i övningar, strategier och samarbeten som går att rättfärdiga. Därför bör de försvarssamarbeten som Sverige är en del av i dag utvärderas, och i fortsättningen bör de vara inriktade på att stärka svensk säkerhet.

År 2009 röstade Sveriges riksdag igenom en egen solidaritetsförklaring om att inte förhålla sig passivt om ett EU-land eller nordiskt land angrips eller drabbas av en katastrof. Inte heller förväntas andra länder stå passiva om Sverige drabbas. Sveriges solidaritetsförklaring medför att Sverige ska verka för att kunna ge och ta emot civilt och militärt stöd från andra länder.[199] Förklaringen baseras på artikel 42.7 i Fördraget om den Europeiska Unionen, som infördes genom Lissabonfördraget. Sveriges egen solidaritetsförklaring är dock ensidig.

Trots avsaknaden av försvarsallianser bygger den svenska försvarsdoktrinen på en förväntan om utländskt stöd i händelse av angrepp.[200] För att det ska vara möjligt fordras att det ska vara praktiskt möjligt att hjälpa oss och att det ska vara mödan värt. För att möjliggöra hjälp måste också planering och övning i fredstid ske.[201] Hamnar behövs för avlastning av trupper som kommer till undsättning, en redan uttänkt ledningsstruktur gällande vilken chef, den svenska eller den utländska, som tar befäl. Vidare behövs en förberedd logistikorganisation med ammunition, sjukvårdsresurser och alla andra förnödenheter.[202]

FINLAND

Svensk-finsk försvarspolitik har en långtgående historia och har då som nu drivits fram av ett aggressivt Ryssland (eller tidigare Sovjetunion). För svensk del kan samarbetet också förklaras med att försvaret saknat resurser efter de drastiska försvarsminskningar som genomförts efter kalla krigets slut.[203] Det har varit ett måste för Sverige att samarbeta med andra parter.

Försvarsmakten beskriver att det militära samarbetet med Finland har varit högst prioriterat av alla internationella samarbeten år 2020. Under året har samarbetet fördjupats genom bland annat den lagstiftning[204] som antagits mellan länderna gällande operativt stöd. Lagen, som i stora drag går ut på att regeringen får begära militärt stöd från Finland i händelse av krig eller krigsfara (och vice versa), har ökat samarbetets förtroende och trovärdighet. Det har också möjliggjort att planering av gemensam övervakning av territoriell integritet påbörjats.[205]

År 2018 undertecknade Sverige och Finland ett samförståndsavtal om det gemensamma samarbetet. Syftet var att stärka försvarsförmågan och öka den operativa förmågan genom gemensamt agerande och resurser. Exempel på hur det har omsatts i konkreta åtgärder är upprättandet av en svensk-finsk marin stridsgrupp och att ländernas flygstridskrafter kunnat integreras vid olika övningar.[206]

198 Ds 2019: 8. *Sammanfattning*, s. 8.
199 Proposition 2008/09:140. *Ett användbart försvar.*
200 Neretnieks, Karlis. Sveriges militärstrategiska läge. I *Sveriges försvarspolitik – En antologi*, Zebulon Carlander och Oscar Karlflo (red.), 34–54. Stockholm: Ekerlids Förlag, 2020.
201 Ibid.
202 Ibid.
203 Petersson, Magnus. *Svensk-finskt försvarssamarbete då och nu.* FOI, 2021.
204 Lag (2020:782) om operativt militärt stöd mellan Sverige och Finland
205 Försvarsmakten. *Försvarsmaktens årsredovisning 2020*. Försvarsmakten, 2021
206 Petersson, Magnus. *Svensk-finskt försvarssamarbete då och nu.* FOI, 2021.

Det svensk-finska samarbetet har aldrig innehållit några försvarsgarantier.[207] Om Sverige skulle angripas kan alltså en svensk regering be om stöd från Finland, men inget av länderna har någon egentlig skyldighet gentemot den andra.

Magnus Petersson, forskare vid FOI:s enhet för säkerhetspolitik, påtalar att om krig skulle bryta ut i Östersjöregionen i dag är risken mycket stor att Sverige dras in i konflikten. Numera utgör Sverige och Finland en del av en militärgeografisk helhet, och båda ses av västländerna som en tydlig del i avskräckningen gentemot Ryssland.[208] Den handlingsfrihet som det svensk-finska samarbetet bygger på utgör en viss begränsning, beskriver Petersson. Ländernas gemensamma planering blir som ett komplement till varderas nationella planering, vilket gör att samarbetet fortfarande hålls avskilt och isolerat. En risk som Petersson också lyfter är vad som händer om avskräckningen i det svensk-finska försvarssamarbetet inte får avsedd effekt. Då kan Sverige och Finland angripas av Ryssland ändå, och dessutom riskera att stå utan stöd från både varandra och omvärlden eftersom länderna helt saknar alliansförpliktelser.

NORDEN

I Sverige finns en politisk enighet om att fördjupa det nordiska försvarssamarbetet. Utöver vårt finska samarbete har vi ingått bilaterala samarbeten med flera av våra nordiska grannar. Försvarsmakten bedriver exempelvis övningsutbyten mellan norska och svenska förband och har ett samförståndsavtal för ett försvarssamarbete med Danmark. Regeringen beskriver att det nordiska samarbetet bygger på ömsesidigt förtroende. De vill se ett så långtgående samarbete som möjligt, men enbart om det inte kräver några ömsesidiga försvarsgarantier.[209] [210]

De nordiska länderna har ett gemensamt försvarssamarbete under namnet Nordefco (Nordic Defence Cooperation). Nordefco bygger på frivillighet och länderna väljer själva vilka områden de arbetar inom.[211] Det kan innebära utbildning, övning eller internationella insatser.[212] I Nordefco finns intresse för ökat samarbete kring anskaffning av försvarsmaterielsystem. Tanken är att liknande materielsystem gör gemensamma övningar enklare. Ur ett renodlat svenskt perspektiv är detta positivt, inte minst med tanke på vår utvecklade försvarsindustri.[213]

Av de nordiska länderna är Norge, Danmark och Island medlemmar i Nato. Sverige och Finland är inte det och således saknar vi täckning av organisationens försvarsgaranti. Något annat som gör det nordiska samarbetet ännu lite svårare är det att Norge och Island inte är en del av EU. Danmark är i sin tur medlem i EU men står utanför unionens gemensamma utrikes- och säkerhetspolitik.[214] Visserligen delar de nordiska länderna i mångt och mycket historia, värderingar och gemenskap, men det går inte att tro att våra förutsättningar är identiska. Dessa skillnader gör också att flera nordiska länder ser det nordiska samarbetet som ett komplement till andra samarbeten, snarare än ett huvudsakligt sådant.[215]

207 Ibid.
208 Ibid.
209 Försvarsmakten. *Försvarsmaktens årsredovisning 2020*. Försvarsmakten, 2021
210 Regeringskansliet. Det nordiska försvarssamarbetet Nordefco. *Regeringskansliet*. https://www.regeringen.se/ (Hämtad 2021-06-23)
211 Ibid.
212 Ibid.
213 Norrevik, Sara. Internationella samarbeten. I *Sveriges försvarspolitik – En antologi*, Zebulon Carlander och Oscar Karlflo (red.), 158–182. Stockholm: Ekerlids Förlag, 2020.
214 Ibid.
215 Ibid.

EU

EU:s gemensamma säkerhets- och försvarspolitik, ESFP, är unionens försvarssamarbete.[216] ESFP innebär vissa förpliktelser, medlemsländer har till exempel en skyldighet att bistå andra medlemsländer som angrips eller utsätts för katastrof. Att Sverige inte längre kan beskrivas som fullt neutralt eller ”alliansfritt”, så som många velat föredra historiskt, är just på grund av vårt inträde i EU.

Det finns ingen permanent militär på EU-nivå. Den snabbinsatsstyrka som skapats har aldrig aktiverats eller använts på grund av låg politisk vilja.[217] Däremot budgeteras hela 13 miljarder euro i EU:s långtidsbudget för att kunna delfinansiera medlemsländers försvarsförmågor. Det sker genom den europeiska försvarsfonden, EDF.[218] Från 2021 och fram till 2027 kommer Sverige att investera fem miljarder kronor till denna europeiska delfinansiering, men det finns en risk att svensk försvarsindustri inte får ta del av någon betydande andel. EDF tillåter nämligen inte finansiering av projekt med ägare från tredjepartsländer, något som påverkar svenska försvarsindustriföretag med brittiska och amerikanska ägare.[219] Sverige är också en del av EU:s permanent strukturerade samarbete, PESCO, som drivit projekt med syfte att öka militär mobilitet mellan länderna inom materielsamarbete och cyberförsvar.[220]

22 av EU:s 27 medlemsländer är medlemmar i Nato, vars stadgar om kollektiva försvarsförpliktelser är betydligt mer långtgående än EU:s Lissabonartiklar.[221] En bidragande anledning till att Sverige har en alldeles egen solidaritetsförklaring överhuvudtaget kan härledas till att den europeiska är för vag. Denna vaghet kan kopplas till Nato-ländernas behov av en europeisk försvarsförpliktelse som är anpassad till Natos stadgar.[222] EU och Nato har ett etablerat samarbete inom ramen för försvarsförmåga, cybersäkerhet, forskning och gemensam kompetenshöjning.[223]

Efter USA lägger de samlade EU-länderna mest resurser i världen på försvar. EU-parlamentet rekommenderar sina medlemsländer att spendera minst 2 procent av BNP på sin försvarsbudget.[224] Samtidigt menar EU-parlamentet också att över 26,4 miljarder euro varje år går till spillo inom unionens försvarspolitik. Anledningen ska vara överflödiga utgifter och upphandlingshinder.[225] [226]

Med anledning av Brexit har Storbritannien lämnat EU:s försvarssamarbete. Försvarsberedningen har påtalat att Sverige bör verka för att Storbritannien förblir en del av EU:s säkerhetspolitiska gemenskap, och på så sätt också omfattas av den svenska unilaterala solidaritetsförklaringen.[227]

NATO

Försvarsmakten beskriver Sveriges samarbete med Nato som centralt för såväl vår nationella försvarsförmåga som våra militära operationer med andra länder i vårt närområde.

216 Säkerhetspolitik.se. GSFP. *MSB*. 2011. https://www.sakerhetspolitik.se/Ordlista/G/GSFP/ (Hämtad 2021-06-24)
217 Norrevik, Sara. Internationella samarbeten. I *Sveriges försvarspolitik – En antologi*, Zebulon Carlander och Oscar Karlflo (red.)
218 Ibid.
219 Ibid.
220 Lazarou, Elena och Lat¸ici, Tania. *PESCO: Ahead of the Strategic Review*. European Parliamentary research service, 2020. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652051/EPRS_BRI(2020)652051_EN.pdf (Hämtad 2021-06-24)
221 Norrevik, Sara. Internationella samarbeten. I *Sveriges försvarspolitik – En antologi*, Zebulon Carlander och Oscar Karlflo (red.)
222 Ibid.
223 European External Action Service (EEAS). *EU- NATO Cooperation.* EEAS, 2020. https://eeas.europa.eu/sites/default/files/eu_nato_factshee_november-2020-v2.pdf (Hämtad 2021-06-24)
224 Europaparlamentet. European Parliament resolution of 22 November 2016 on the European Defence Union (2016/2052(INI))
225 Europaparlamentet. Defence: MEPs push for more EU cooperation to better protect Europe. *Europaparlamentet.* 2016. https://www.europarl.europa.eu/news/en/press-room/20161117IPR51547/defence-meps-push-for-more-eu-cooperation-to-better-protect-europe (Hämtad 2021-06-24)
226 European Parliament. Infographic: Parliament wants to boost European defence by increasing cooperation. *European Parliament.* 2017. https://www.europarl.europa.eu/news/en/headlines/security/20170310STO66196/infographic-meps-want-to-boost-european-defence-by-increasing-cooperation (Hämtad 2021-06-24)
227 Ds 2019:8

I dag är Sverige ett partnerland till Nato med en status som Enhanced Opportunities Partner (EOP). Sverige har också ett avtal om värdlandsstöd vilket innebär att Sverige underlättar för Nato att verka på svenskt territorium vid övningar och militära operationer.[228]

Enligt Försvarsmakten ger Nato-samarbetet tillgång till kvalificerad utbildning- och övningsverksamhet samt standardiserings-, evaluerings- och certifieringsverksamhet. Dessa delar bidrar till Sveriges förmåga och bygger enligt myndigheten ett starkt försvar.

Nato har sedan 2017 militär närvaro i Baltikum och Polen genom sin Enhanced Forward Presence (EFP). Närvaron är defensiv och till för att skydda alliansens östra delar från ryskt angrepp. Nato beskriver att EFP delvis är till för att påminna omvärlden om att en attack mot ett alliansland är en attack mot dem samtliga. Det är en tydlig anspelning på den kollektiva försvarsgaranti som Nato-länderna erbjuder varandra i händelse av väpnat angrepp.[229]

Utöver vad som sker inom Nato har Sverige ett bilateralt samarbete med USA och en avsiktsförklaring om ökad operativ samverkan med Storbritannien.[230]

228 Norrevik, Sara. Internationella samarbeten. I *Sveriges försvarspolitik – En antologi*, Zebulon Carlander och Oscar Karlflo (red.)
229 Ministry of Foreign Affairs of the Republic of Latvia. NATO Enhanced forward Presence. M*inistry of Foreign Affairs of the Republic of Latvia*. 2021. https://www.mfa.gov.lv/en/policy/security-policy/nato-enhanced-forward-presence (Hämtad 2021-06-23)
230 Försvarsmakten. *Försvarsmaktens årsredovisning 2020*. Försvarsmakten, 2021

INTERNATIONELLA INSATSER

I dag ser Försvarsmaktens strategiska målbild för militär verksamhet i internationella insatser ut som följer:

- Att stödja värdlandets förmåga att självt omhänderta ansvaret för säkerheten i det egna landet, så att ett grundläggande skydd av civilbefolkningen kan upprätthållas.
- Att aktivt verka för att FN:s säkerhetsrådsresolution om kvinnor, fred och säkerhet implementeras.
- Att deltagande i internationella militära insatser bidrar till att bygga förmågan hos svenska krigsförband och staber.

Runt millennieskiftet bedömde våra politiker att Sveriges närområde hade en så pass låg hotbild att Försvarsmakten i stället fick direktiv om att rikta in sig på internationella insatser.[231]

Sedan sin första insats på Balkan 1999 har EU bedrivit uppemot ett fyrtiotal krishanteringsinsatser. Sverige har bidragit till dem alla, antingen med civil eller militär personal.[232] EU har sällan deltagit i skarp konflikt utan låtit antingen FN- eller Nato-ledda insatser ta det ansvaret.[233]

Nato har också bedrivit flera militära insatser som Sverige deltagit i. Bland dessa återfinns Bosnien och Hercegovina, Libyen och Afghanistan.

FN:S SÄKERHETSRÅD

Ett i nuläget viktigt organ när det handlar om internationella insatser är FN:s säkerhetsråd, det råd som beslutar huruvida internationella insatser ska genomföras och hur kriser och konflikter ska hanteras. Säkerhetsrådet består av fem permanenta medlemsstater och tio roterande medlemmar. De fem permanenta rådsmedlemmarna är USA, Storbritannien, Frankrike, Kina och Ryssland. Dessa fem sitter också på en vetorätt vid samtliga beslut, vilket möjliggör att de kan blockera beslut som inte passar dem.

Ibland händer det att säkerhetsrådet beslutar om en militär insats, men sedan uppdrar till andra organisationer, såsom Nato eller EU, att leda uppdraget. I dessa fall har insatsen fortfarande ett FN-mandat i ryggen. Det är detta FN-mandat, oavsett vem som leder insatsen, som Sveriges regering och riksdag kräver för att Sverige ska delta i en militär insats.

SVENSK VAPENEXPORT

Svensk försvarsindustri är historiskt framgångsrik, och Sverige ligger på plats 15 av världens största vapenexportsländer.[234] Enligt Inspektionen för strategiska produkter uppgick den svenska exporten av krigsmateriel till drygt 16,3 miljarder kronor år 2020.[235] 67 procent av exporten gick till EU och dess samarbetsländer, exempelvis USA, Sydkorea och Norge.

Sedan 2018 har Sverige lag på en hårdare exportkontroll av krigsmateriel, där mottagarlandets demokratiska status ska utgöra ett centralt villkor för tillståndsprövningen[236]. Tan-

231 Hugemark, Bo. Försvarets historiska utveckling. I *Sveriges försvarspolitik – En antologi*, Zebulon Carlander och Oscar Karlflo (red.), 11–34. Stockholm: Ekerlids Förlag, 2020.
232 Norrevik, Sara. Internationella samarbeten. I *Sveriges försvarspolitik – En antologi*, Zebulon Carlander och Oscar Karlflo (red.)
233 Ibid.
234 Kuimova, Alexandra, Wezeman, T. Siemon och Wezeman, D. Pieter. *Trends in International Arms Transfers, 2020*. SIPRI, 2021. https://sipri.org/sites/default/files/2021-03/fs_2103_at_2020_v2.pdf (Hämtad 2021-06-25)
235 Inspektionen för strategiska produkter. Den svenska exporten av krigsmateriel 2020. *Inspektionen för strategiska produkter.* 2021. https://isp.se/media/1478/20210318-pressmeddelande-isp.pdf (Hämtad 2021-06-25)
236 Regeringskansliet. Skärpta regler för vapenexporten. *Regeringskansliet*. 2017. https://www.regeringen.se/ (Hämtad 2021-06-25)

ken är att allvarliga och omfattande kränkningar av mänskliga rättigheter, såväl som grava brister i mottagarens demokratiska status, ska utgöra ett hinder för att få ta del av svensk vapenexport.[237]

Trots denna lagstiftning är Sveriges största exportland Förenade Arabemiraten som vi förra året exporterade till för ett värde av 3,2 miljarder.[238] En femtedel av allt som svensk försvarsindustri exporterar går därmed till en diktatur där medborgare saknar politiska rättigheter, där det rapporteras om tortyr och sharialagar tillämpas på mänskliga rättigheters bekostnad.[239] Förenade Arabemiraten är dessutom en krigförande part i Jemenkriget, den humanitära katastrof FN beskrivit som den värsta i världen.[240] I januari 2021 fick svenska Saab ett nytt kontrakt med staten för två spanings- och stridsledningsflygplan. Priset för dessa landade på runt fyra miljarder kronor per plan.[241] Att Förenade Arabemiraten köpt vapen och militär utrustning från Sverige som sedan använts i Jemen, eller möjligen Libyen, bedöms vara en reell risk. Att hitta konkreta bevis för den saken är dock svårt.[242]

Andra utomeuropeiska länder som svensk försvarsindustri exporterar till inkluderar Saudiarabien (diktaturen som är ännu en drivande part i Jemenkriget), Kuwait och Oman.[243]

237 Ibid.
238 Inspektionen för strategiska produkter. Den svenska exporten av krigsmateriel 2020. *Inspektionen för strategiska produkter.* 2021.
239 Utrikesdepartementet. *Förenade Arabemiraten – Mänskliga rättigheter, demokrati och rättstatens principer: situationen per den 30 juni 2019.* https://www.regeringen.se/ (Hämtad 2021-06-25)
240 Landguiden. Konflikten i Jemen. *Utrikespolitiska institutet.* https://www.ui.se/landguiden/konflikter/jemen/ (Hämtad 2021-06-25)
241 Saab. Saab receives follow-on contract for GlobalEye. *Saab.* 2021. https://www.saab.com/newsroom/press-releases/2021/saab-receives-follow-on-contract-for-globaleye (Hämtad 2021-06-25)
242 Olsson, Jonas. Nya vapenleveranser till Förenade Arabemiraten – trots brott mot mänskliga rättigheter. *SVT Nyheter*. 2021-03-19. https://www.svt.se/nyheter/inrikes/nya-vapenleveranser-till-forenade-arabemiraten-trots-brott-mot-manskliga-rattigheter (Hämtad 2021-06-25)
243 Inspektionen för strategiska produkter. Den svenska exporten av krigsmateriel 2020. *Inspektionen för strategiska produkter.* 2021.

FRAMTIDENS MILITÄRA FÖRSVARSPOLITIK: REFORMFÖRSLAG

Sverige står inför en svår balansgång mellan tid och förmåga. Försvaret behöver byggas upp, och det fort, men vi behöver också inse att den naivitet och politiska arrogans som i decennier präglat svensk försvarspolitik gör en ögonblicklig förbättring omöjlig. De luckor som skapats i form av kompetens-, materiel- och personalbrist kommer att ta år att täppa igen riktigt ordentligt. För sådant arbete krävs långsiktig politik, vilket förklarar varför de turer som togs i Försvarsberedningen inför den senaste försvarspropositionen är oroväckande. Att Socialdemokraterna först vägrade binda sig till en nödvändig ekonomisk ram, sedan förhandlade ner de ökade anslagen och slutligen lyckades få upprustningen från 2025 och framåt att vara ofinansierad är att förhindra försvarets långsiktiga förmåga. Det är att ta för lätt på Sveriges säkerhet och att vägra göra upp med en utveckling man i stor utsträckning bidragit till själv.

Om Sverige utropar solidaritetsförklaringar till hela EU och Norden, men samtidigt saknar infrastruktur, materiel och personal så är vi inte trovärdiga. Att ingå bilaterala avtal, kompetensutbyten eller försvarsallianser i ett sådant tillstånd ter sig orealistiskt och rätt så meningslöst för den andra berörda staten. Det är en anledning till varför Sverige måste återutveckla den infrastruktur, såsom mobiliseringsförråd och utbildningsanordningar, som försvunnit genom åren. Det materiella är grundläggande för att kunna åstadkomma en ökad militär förmåga.

- **Öka Sveriges försvarsutgifter till minst 2 procent av BNP.**
- **Säkerställ att Sverige har den logistiska förmågan som krävs för att kunna assistera utländsk hjälp i händelse av angrepp.**

PERSONALREKRYTERING

FRÅGAN OM VÄRNPLIKT

Att ha en värnplikt som tar hänsyn till individers frivillighet är positivt, men senast vårt värnpliktssystem baserades enbart på frivillighet ledde detta till en alldeles för låg andel rekryter. Dagens system kan ses på som en mellanväg värd att fortsätta gå på: Försvarsmakten ges största möjliga underlag vid rekryteringen, samtidigt som individens villighet också spelar in på beslutet om tjänstbarhet. Därför bör vi fortsätta kalla samtliga 18-åringar till mönstring, men bara kalla ett visst antal värnpliktiga till grundutbildningen. Frivilligheten kan dock bara tillgodoses så länge Sveriges försvarsbehov tillåter en sådan modell.

Ett relevant argument mot allmän värnplikt är att volymen av värnpliktiga inte är ett rättvisande mått på försvarsförmåga. En förbättrad försvarsförmåga kan däremot uppstå om värnpliktsutbildningen håller hög kvalitet och om civila med specialistkunskap lockas till Försvaret med hjälp av starka incitament.[244] Färdigutbildade värnpliktiga måste också vilja ta anställning eller ingå avtal med Försvarsmakten eller hemvärnet så att deras kompetens kan bibehållas och förvaltas. Att undersöka hur ett hemvärnsavtal görs mer attraktivt är en nödvändig åtgärd.

- **Fortsätt kalla samtliga 18-åringar totalförsvarspliktiga till mönstring.**

244 Nordgren Christensen, Annika. Personalförsörjningen. I *Sveriges försvarspolitik – En antologi*, Zebulon Carlander och Oscar Karlflo (red).

EN ANSTÄLLNING INOM FÖRSVARSMAKTEN

En av Försvarsmaktens svåraste uppgifter är att få anställda att stanna längre. Om fler gruppbefäl, soldater och sjömän (GSS) är kvar i sin anställning i mer än fyra år skulle deras kompetens bibehållas längre och utbildningskostnaderna minska. Med tanke på korrelationen mellan uppsägning som GSS och påbörjan av studier kan en lösning vara reformer av studieekonomisk karaktär.

Den statliga utredningen om personalförsörjning, SOU 2016:63, presenterade en rad av studieekonomiska incitament som aldrig förverkligades. Bland dessa ingick att Försvarsmakten skulle erbjuda hjälp med återbetalning av studielån för den individ som tjänstgjort tillräckligt länge vid myndigheteten och därefter gått vidare och fullgjort en universitets- eller högskoleutbildning. Ett annat förslag var att möjliggöra för tjänstgöring som GSS parallellt med studier. Då skulle Försvarsmakten betala en lön som motsvarar minst låneandelen av studiemedlet som studenter i vanliga fall får av CSN. Ett ytterligare förslag var att den som varit anställd i Försvarsmakten i minst sex år skulle få ett högre bidragsbelopp vid vidare studier, men med en begränsning på 120 veckor.[245]

Gemensamt för utredningens förslag är att alla går att ta del av först efter att ens tjänstgöring vid Försvarsmakten passerat den genomsnittliga anställningstiden. Detta minskar risken att incitamenten utnyttjas utan att åstadkomma den kvarhållande effekt man är ute efter. Förslagen är praktiskt genomförbara, realistiska och ställer tydliga krav på lång tjänstgöring. De har således chans att också generera goda resultat. Viktigt är dock att förslagen kompletteras med en kontrollmekanism så att utbildningen genomförs på en tillfredsställande nivå. Den som mottar dessa förmåner måste också klara sin utbildning och ta sina högskolepoäng.

- **Möjliggör för gruppbefäl, soldater och sjömän att studera inom ramen för sin tjänstgöring, med en lön motsvarande studiemedel.**
- **Låt Försvarsmakten betala tillbaka en andel av gruppbefäls, soldaters och sjömäns studielån efter en tjänstgöring över genomsnittet och en fullbordad universitetsutbildning.**

Det finns även ett stort behov att hålla kvar de GSS som inte planerar för någon vidareutbildning, utan överväger att lämna på grund av låg lön. Den ingångslön som GSS erbjuds medför att lönen förblir låg även efter ett par år i yrket, trots en löneutveckling.[246] Att Försvarsmakten inte kan erbjuda konkurrenskraftiga löner i jämförelse med likvärdiga yrken skapar onekligen en låg vilja att stanna kvar. Därför behövs en generell lönehöjning för GSS. En sådan höjning kräver också en lönehöjning för officersyrkena, detta så att vidareutbildning lönar sig även inom Försvarsmakten. En ytterligare reform för att åstadkomma kvarhållande incitament vore att skapa en succesiv bonustrappa där bonusen baseras på hur många år den anställda har tjänstgjort.

- **Höj den generella lönen för gruppbefäl, soldater och sjömän.**
- **Höj officers- och specialistofficerslönerna.**
- **Utveckla en successiv bonustrappa för gruppbefäl, soldater och sjömän, baserad på tid i tjänst.**

FLER OFFICERARE!

Det är positivt att antalet sökande till officersprogrammet ökat på senare år, men antalet antagna ligger fortfarande på ett minimum. En bidragande faktor kan vara att ett ökat antal antagna skulle kräva fler officer-specifika boenden och tillgång till kompetenta lärare.

245 I heltidsstudier skulle detta motsvara en kandidatexamen á tre år.
246 SOU 2016:63

Även detta är en resursfråga. Boendeplatser och en stram försvarsbudget får inte hindra återväxten av svenska officerare.

Om antalet studieplatser ökar vid officerprogrammet är det dock viktigt att de antagna fortsatt har en tillräckligt hög intellektuell och fysisk nivå för att lämpa sig för yrket. För att säkerställa sådan kompetens bör sökande också uppfylla en miniminivå. Exakt hur den nivån ska definieras, liksom som var den ska ligga, bestäms däremot bättre av Plikt- och prövningsverket, Försvarsmakten och Försvarshögskolan.

- **Skapa fler platser vid officersprogrammet, men inför skarpare minimumkrav för att få genomföra utbildningen.**

INTERNATIONELLT SAMARBETE

FINLAND OCH NORDEN

Vår försvarspolitiska relation med Finland är unik och dess vidareutveckling är viktig. Att regeringen inte vill se några ömsesidiga försvarsgarantier i Norden är att sätta Sverige i en utsatt position. Bygger vi försvar som gör oss beroende av andra länders hjälp måste vi också kunna räkna med deras stöd i händelse av krig. En bilateral försvarsallians med Finland, där vi säkerställer sådant stöd gentemot varandra, är ett sätt för Sverige att höja sin tröskeleffekt för angrepp. Men en försvarsallians är inte nödvändigtvis enkel. Länderna måste komma överens om försvarsalliansens utformning och enas om när (eller att) det är värt att gå ut i krig för den andra. En försvarsallians är inte heller ett garanterat skydd mot angrepp, vilket gör att Sverige måste vidta fler åtgärder för att bygga tröskeln ännu lite högre.

- **Ingå en bilateral försvarsallians med Finland.**

Samarbetet med de övriga nordiska länderna är annorlunda än det finska, framförallt på grund av de Nato-medlemskap som präglar de andra ländernas utformning av försvar och samarbeten. Precis som Karlis Neretnieks, officer och tidigare rektor för Försvarshögskolan, påtalar: Idén om att Sverige ska ingå i ett gemensamt nordiskt försvarsförbund är orealistisk då norsk och dansk säkerhet bygger på Nato.[247] För dem är samarbete med Sverige mer en bonus än en lösning, vilket självklart påverkar hur de förhåller sig till det. Att samverka inom Nordefco och genom bilaterala avtal är bra, men dessa kommer aldrig ensamt kunna åstadkomma sådana tröskelhöjningar som Sverige behöver.

- **Prioritera bilaterala, formaliserade samarbeten mellan Sverige och andra länder, speciellt med våra närmsta grannar.**
- **Sträva efter fördjupat nordiskt samarbete.**
- **Fördjupa det nordiska materielsamarbetet inom ramen för Nordefco.**

EUROPA

EU varken kan eller strävar efter att ersätta Nato. Lissabonfördragets föreskrifter om gemensamt försvar är trots allt tydligt underordnade både medlemsländernas Nato-medlemskap och val att stå neutrala.[248] Ändå är det positivt att arbetet med en unionsgemensam säkerhets- och försvarspolitik fortskrider, likaså att EU arbetar med att kunna komplettera Nato. Ett skarpt försvarspolitiskt EU måste också kunna vara en kraft att räkna med i de

247 Neretnieks, Karlis. Karlis Neretnieks: Nordiskt försvarssamarbete i stället för Nato? *SVD.* 2018-01-09. https://www.svd.se/karlis-neretnieks-nordiskt-forsvarssamarbete-i-stallet-for-nato (Hämtad 2021-06-18)

248 Europaparlamentet. “EU-armé”? Vad gör Europa för att stärka sitt försvar? *Europaparlamentet.* 2021. https://www.europarl.europa.eu/news/sv/headlines/security/20190612STO54310/eu-arme-vad-gor-europa-for-att-starka-sitt-forsvar (Hämtad 2021-06-18)

lägen då Nato inte vill eller kan leda försvarspolitiska åtaganden. Det gör det viktigt att unionen också strukturerar sig självständigt.

Att EU:s medlemsländer gör en resursförlust på över 26 miljarder euro (260 miljarder kronor) på grund av upphandlingshinder och överflödiga utgifter är både ineffektivt och försvagar idén om att EU kan ta en ledande försvarspolitisk roll. Sverige måste kontrollera till vad och var våra bidrag till ett europeiskt försvar går och säkerställa att de projekt vi deltar i är kostnadseffektiva och bidrar konkret till ett europeiskt samarbete. Kontrollen av resursförluster bör, å andra sidan, inte begränsas till enbart EU:s försvarsutgifter.

- **Ge Storbritannien en unilateral solidaritetsförklaring och uppmuntra andra EU-länder till detsamma.**
- **Verka för att EDF:s delfinansiering av medlemsländers försvarsindustrier även kan inkludera de som ägs av EU:s samarbetsländer.**
- **Ställ oss positiva till ett fördjupat försvarssamarbete i Europa.**

NATO

Nato är den försvarsorganisation som hela vår omvärld, från Ryssland till vår egen försvarsmakt, förhåller sig till. Den handlingsfrihet som Sverige erhåller genom att inte ingå i alliansen kan inte trumfa den säkerhetsgaranti, och således tröskeleffekt, vi skulle vinna av att gå med. Om vi ändå skulle angripas hade Natos hjälpinsatser varit grundade i planer och förberedelser, snarare än den improvisation som hjälpen skulle innebära utan medlemskap[249]. Medlemskapet skulle föra oss närmre våra baltiska och västnordiska grannar, såväl som Storbritannien som numera saknas inom EU:s ramar. I dag är Sverige så nära en fullvärdig medlem en stat kan bli, utan att vara just medlem. Sverige deltar i stora delar av Natos verksamhet med undantaget att vi saknar dess fullvärdiga skydd. I en skakig omvärld på väg mot en osäker framtid borde den svenska Nato-optionen vara ett självklart steg att ta.

- **Formalisera Natosamarbetet genom ett medlemskap**
- **Placera svenska trupper i Baltikum inom ramen för Natos EFP**

INTERNATIONELLA INSATSER

Ibland påstås det att FN ger legitimitet till internationell kris- och konflikthantering, men samtidigt kan högst nödvändiga insatser blockeras av rådets fem permanenta medlemmar. Att Sverige ska förlita sig på FN:s omdöme och mandat för att agera i en internationell insats är att placera oss själva i ett passivt hörn och samtycka till att styras av stormakters vilja. Kravet på FN-mandat hindrar oss från att agera moraliskt och efter eget huvud. Ryssland och Kina ska inte ha makt att kunna förhindra svenska soldater att avvärja en kris eller stödja dem som behöver stöd. FN har dessutom en återkommande historia av att agera för lite och för sent, samt att utnyttja sin immunitet för att undslippa ansvar i insatser de ansvarat för.[250] Det går att förstå viljan att se FN som en slags kvalitetsstämpel. Tyvärr är det inte så verkligheten ser ut.

- **Ta bort kravet på FN-mandat för deltagande i internationella insatser**

Svenska trupper har ibland behövt agera på lägre taktisk och strategisk nivå än sin förmåga för att anpassa sig till det större kollektiv de blivit en del av i en internationell insats. Att det ställs olika krav på färdigheter i internationella och nationella insatser är inte så konstigt. Samtidigt är det ändå viktigt att de lärdomar och erfarenheter som fås utanför Sve-

249 Neretnieks, Karlis. Karlis Neretnieks: Nordiskt försvarssamarbete i stället för Nato? *SVD.*
250 Pilkington, Ed. UN response to Haiti cholera epidemic lambasted by its own rights monitors. *The Guardian*. 2020-05-04. https://www.theguardian.com/world/2020/may/04/united-nations-un-haiti-cholera-letter-rights-monitors (Hämtad 2021-06-18)

riges gränser kultiveras även innanför dem. Det kan exempelvis handla om att chefer och befälhavare aktivt arbetar med att kunna leda utländska förband, en förmåga som behövs den dag Sverige angrips och andra länder kommer till vår hjälp (om de kommer!), eller att soldater övar på att samverka. Sverige behöver sträva efter att få med sig hem relevant erfarenhet från internationella insatser. En del i detta kan vara att allra främst prioritera deltagande i militära insatser ledda av Nato och i andra hand EU.

- **Träna svenska befäl och chefer i att kunna leda utländska trupper.**
- **Prioritera deltagande i internationella insatser som leds av Nato.**

I slutändan går inte internationella insatser ut på att främja deltagarländers egen operativa förmåga. I stället handlar det primärt om att försvara värden värda att försvara, med vapen i hand om så krävs. Givet Sveriges utgångsläge är det viktigt att göra en pragmatisk, men ändå mycket svår, avvägning. Sverige ska vara ett land som står upp för frihet, demokrati och människovärdet, men vi måste vara starka själva innan vi kan skydda andra. I de lägen där Sverige står mellan att lägga resurser på att stärka ett nästintill avvecklat nationellt försvar och utföra monotont arbete i en FN-ledd insats måste Sverige, i dag och i den närmsta framtiden, prioritera den förstnämnda uppgiften.

- **Prioritera uppbyggnaden av det nationella försvaret före deltagandet i internationella insatser.**

Att Sverige fortfarande exporterar vapen och krigsmateriel till diktaturer är oacceptabelt. Svensk försvarsindustri bör verka under en nolltolerans mot export till diktaturer. Nuvarande halvdana lagstiftning är inte tillräcklig. Att förändra detta vore att stå på demokratins och den civila befolkningens sida och att motverka mänskligt lidande på riktigt.

- **Solidaritet är inte alltid militära muskler. Svensk försvarsindustri ska inte sälja vapen till diktaturer.**

KOMMER DET ATT KOSTA FÖR MYCKET?

På slutklämmen är det alldeles rimligt att, som ekonomiskt liberalt sinnad, ställa sig frågan om allt det som föreslås i denna rapport kommer att kosta för mycket. Svaret som följer måste bli ett tydligt nej. Att försvarsanslagen behöver öka för att kunna åstadkomma ett försvar värt namnet bör det finnas en bred liberal och konservativ uppslutning kring. Till och med grundbulten i den mest libertarianska nattväktarstaten är att försvaret är en av få riktiga kärnuppgifter och att det är dit den minimala mängden skattepengar ska riktas.

När regeringar skapat ineffektiva och dyra myndigheter, hostat upp bidrag till bisarra projekt och försökt införa familjeveckor har de gjort det på bekostnad av den svenska säkerheten. År efter år, bit efter bit, har det skurits i försvaret, både från vänster och höger. Sverige behöver inte skapa ett fullvärdigt försvar med hjälp av höjda skatter, i stället behöver vi genomföra liberalkonservativa reformer under en lång tid framöver. Men exakt hur man slimmar ner en rödsvullen stat på bästa sätt får vara tema för en annan sommars rapport.

KÄLLFÖRTECKNING

LITTERATUR

Carlander, Zebulon och Karlflo, Oscar (red.). *Sveriges försvarspolitik – En antologi*. Stockholm: Ekerlids Förlag, 2020.

Tracz, Katarina (red.). *Gråzon*, Stockholm: Frivärld, 2021.

OFFENTLIGT TRYCK

Ds 2017:66. *Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025*.

Ds 2019:8. Försvarsberedningen. *Värnkraft - Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025*.

Ds 2019: 8. *Sammanfattning*.

Europaparlamentet. European Parliament resolution of 22 November 2016 on the European Defence Union (2016/2052(INI))

Europaparlamentets och Rådets Direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen och Direktiv 2016/1148 (EUT L 194/1 19.7.2016 s. 1–36), s. 22.

Europeiska kommissionen. *Commission Staff Working Document: Report on the protection and enforcement of intellectual property rights in third countries*. 2021. https://trade.ec.europa.eu/doclib/docs/2021/april/tradoc_159553.pdf (Hämtad 2021-06-11)

Europeiska kommissionen. *Rapport om genomförandet av EU:s strategi för cybersäkerhet för ett digitalt decennium*. Bryssel: 2021. https://eur-lex.europa.eu/ (Hämtad 2021-09-09)

Europeiska kommissionen. *The EU's Cyber Strategy for the Digital Decade*. Bryssel: Europeiska kommissionen, 2020-12-16. (Hämtad 2021-06-13)

FN. *Charter of the United nations and Statute och the International Court of Justice*. FN, 1945.

FRA, Försvarsmakten, MSB, Polisen, Säpo. *Cybersäkerhet i Sverige: Hot, metoder, brister och beroenden*. 2020. https://www.msb.se (Hämtad 2021-06-05)

FRA. *Årsrapport 2017*. FRA, 2017. https://www.fra.se (Hämtad 2021-06-10)

Fö2019/01330 *Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter*.

Försvarsdepartementet. *Inriktning för Försvarsmakten 2021–2025*. Regeringen, 2020.
Försvarsmakten. *Försvarsmaktens årsredovisning 2020*. Försvarsmakten, 2021. https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/arsredovisningar/arsredovisning-2020/forsvarsmaktens-arsredovisning-2020-huvuddokument.pdf (Hämtad 2021-06-20).

Försvarsmakten. *Must årsöversikt 2020*. 2021. https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/rapporter/must-arsoversikt-2020.pdf (Hämtad 2021-06-06).

Inspektionen för strategiska produkter. Den svenska exporten av krigsmateriel 2020. *Inspektionen för strategiska produkter.* 2021. https://isp.se/media/1478/20210318-pressmeddelande-isp.pdf (Hämtad 2021-06-25)

MSB. *Gemensamma grunder för samverkan och ledning vid samhällsstörningar*. MSB, 2018. https://rib.msb.se/filer/pdf/28738.pdf (Hämtad 2021-06-13)

MSB, *Statliga myndigheters it-incidentrapportering 2020: utmaningar för en säker och robust informationshantering.* MSB. 2021. https://rib.msb.se/filer/pdf/29488.pdf (Hämtad 2021-06-07)

Proposition 2008/09:140. *Ett användbart försvar.*

Proposition 2020/21:30. *Totalförsvaret 2021–2025.*

Rådets förordning (EU) 2019/796 av den 17 maj 2019 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater. Europeiska unionens officiella tidning, 2019. https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX-:32019R0796&from=EN (Hämtad 2021-06-13)

SFS 1941:967. *Värnpliktslag*.

SFS 1982:756. *Om Försvarsmaktens ingripanden vid kränkningar av Sveriges territorium under fred och neutralitet m.m. (IKFN-förordning).*

SFS 1992:1403. *Om totalförsvar och höjd beredskap.*

Skrivelse 2016/17:213. *Nationell strategi för samhällets informations- och cybersäkerhet.*

Skrivelse 2016/17:42. *Riksrevisionens rapport om informationssäkerhetsarbete på nio myndigheter.*

SFS 2018:585. *Säkerhetsskyddslag*.

SFS 2018:658. *Säkerhetsskyddsförordning*.

SFS 2018:1174. *Informationssäkerhet för samhällsviktiga och digitala tjänster.*

SFS 2020:782. *Om operativt militärt stöd mellan Sverige och Finland*

Säkerhetspolisen. *Hotbild mot säkerhetskänslig verksamhet*. 2019. https://www.sakerhetspolisen.se (Hämtad 2021-02-14)

Säkerhetspolisen. *Säkerhetspolisens årsbok 2019*. 2020. https://www.sakerhetspolisen.se (Hämtad 2021-02-14)

Säkerhetspolisen. *Säkerhetspolisens årsbok 2020*. 2021. https://www.sakerhetspolisen.se (Hämtad 2021-02-14)

RAPPORTER

Alozious, Juuko. Sveriges försvarsutgifter 1900–2022. FOI, 2020.

Andersson, Christer, Gustavi, Tove och Karasalo, Maja. *Artificiell intelligens – möjligheter och utmaningar för Sveriges nationella säkerhet*. FOI, 2019.

IMD World Competitiveness Center. IMD World Digital Competetiveness Ranking 2020. Institute for Management Development, 2020. (Hämtad 2021-04-23).

Kuimova, Alexandra, Wezeman, T. Siemon och Wezeman, D. Pieter. *Trends in International Arms Transfers, 2020*. SIPRI, 2021. https://sipri.org/sites/default/files/2021-03/fs_2103_at_2020_v2.pdf (Hämtad 2021-06-25)

Lazarou, Elena och Lat¸ici, Tania. *PESCO: Ahead of the Strategic Review*. European Parliamentary research service, 2020. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652051/EPRS_BRI(2020)652051_EN.pdf (Hämtad 2021-06-24)

Lee-Makiyama, Hosuk. *Stealing Thunder: Cloud, IoT and 5G will Change the Strategic Paradigm for Protecting European Commercial Interests. Will Cyber Espionage be Allowed to Hold Europe Back in the Global Race for Industrial Competitiveness?* European Centre for International Political Economy, 2018. https://ecipe.org/publications/stealing-thunder/ (Hämtad 2021-06-10)

Petersson, Magnus. *Svensk-finskt försvarssamarbete då och nu.* FOI, 2021.

Radar Ecosystem Specialists. *Svenskt IT säkerhetsindex 2.0: En undersökning i samarbete med Advenica, Dataföreningen, SIG Security och Christer Magnusson, doktor informationssäkerhet Stockholms universitet*. Radar Ecosystem Specialists, 2017.

Svenskt näringsliv. *Företagen och IT-säkerheten – hotbilder, motåtgärder och behov*. 2021. https://www.svensktnaringsliv.se/ (Hämtad 2021-07-04)

Säkerhets- och försvarsföretagen och Teknikföretagen. Näringslivets syn på Sveriges kommande nationella cybersäkerhetscenter. *Säkerhets- och försvarsföretagen och Teknikföretagen.* 2020-04-23. https://www.teknikforetagen.se/globalassets/news/inspel/2020/naringslivets-syn-pa-sveriges-kommande-nationella-cybersakerhetscenter.pdf (Hämtad 2021-06-17)

The National Bureau of Asian Research. *Update to the IP Commission Report*. 2017. https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf (Hämtad 2021-06-11)

Utrikesdepartementet. *Danmark – Mänskliga rättigheter, demokrati och rättstatens principer: situationen per den 30 juni 2018.* 2018. https://www.regeringen.se/ (Hämtad 2021-06-15)

Utrikesdepartementet. *Förenade Arabemiraten – Mänskliga rättigheter, demokrati och rättstatens principer: situationen per den 30 juni 2019.* https://www.regeringen.se/ (Hämtad 2021-06-25)

Weigel, Björn. *Digitaliseringens baksida: cyberhotets komponenter och konsekvenser*. Frivärld, 2018. (Hämtad 2021-06-05)

Zouave, Erik. *Aktiva operationer på cyberdomänen: Folkrättslig normativ utveckling*. FOI, 2019.

ARTIKLAR

Carlsson, Mattias och Holmström, Mikael. Stefan Löfven lyfte bort ansvaret från sig själv. *DN*. 2015-12-22. (Hämtad 2021-06-10)

Detta har hänt: Vapenfabriken i Saudiarabien. *Sveriges radio*. 2013-03-11. https://sverigesradio.se/artikel/5017387 (Hämtad 2021-06-16)

Holmström, Mikael. Försvaret får mer pengar – men kritik för underfinansiering. *DN*. 2020-09-18. https://www.dn.se/sverige/forsvarsuppgorelse-klar-nytt-regemente-i-kristinehamn/ (Hämtad 2021-06-22).

KU-anmälan 2020/21:36. *Försvarsminister Peter Hultqvist agerande i samband med försvarsförhandlingarna inför totalförsvarsbeslutet*.

Lagersten, Erik. Självklart borde Sverige ingå en försvarsallians med Finland. *SVD*. 2020-01-13. https://www.svd.se/sjalvklart-borde-sverige-inga-en-forsvarsallians-med-finland (Hämtad 2021-06-20)

Gummesson, Jonas. Borgerligt motbud – vill se ny brigad i Stockholm. *SVD*. 2020-05-20. https://www.svd.se/borgerligt-motbud--vill-se-ny-brigad-i-stockholm (Hämtad 2021-06-22)

Gummesson, Jonas. Öppet försvarsbråk – M hotar med att inte delta. *SVD*. 2020-02-26. https://www.svd.se/oppet-brak-om-forsvaret--hultqvist-vill-ha-ny-grupp (Hämtad 2021-06-22).

Magnusson, Mattias, Fahlman, Fredrik och Mellgren, Fredrik. Kassahaveri på Coop efter utpressningsattack. *SVD*. 2021-07-03. https://www.svd.se/it-attack-mot-coops-kassasystem

Neretnieks, Karlis. Karlis Neretnieks: Nordiskt försvarssamarbete i stället för Nato? *SVD.* 2018-01-09. https://www.svd.se/karlis-neretnieks-nordiskt-forsvarssamarbete-i-stallet-for-nato (Hämtad 2021-06-18)

Nicander, Lars. ”Nu behövs en koordinator för cybersäkerheten”. *DN.* 2017-07-21. https://www.dn.se/debatt/nu-behovs-en-koordinator-for-cybersakerheten/ (Hämtad 2021-06-15).

Nordlund, Linda. Estlands utrikesminister: Varje krig kommer ha cyberdimension. *SVD*. 2017-02-04. https://www.svd.se/varje-krig-kommer-att-ha-en-cyberdimension (Hämtad 2021-06-17).

Olsson, Jojje. Sanningen bakom Kinas miljardinvestering i Lysekil. *Fokus*. 2017-12-21. https://www.fokus.se/2017/12/sanningen-bakom-kinas-miljardinvestering-lysekil/ (Hämtad 2021-06-11)

Olsson, Jonas. Nya vapenleveranser till Förenade Arabemiraten – trots brott mot mänskliga rättigheter. *SVT Nyheter*. 2021-03-19. https://www.svt.se/nyheter/inrikes/nya-vapenleveranser-till-forenade-arabemiraten-trots-brott-mot-manskliga-rattigheter (Hämtad 2021-06-25)

Pilkington, Ed. UN response to Haiti cholera epidemic lambasted by its own rights monitors. *The Guardian*. 2020-05-04. https://www.theguardian.com/world/2020/may/04/united-nations-un-haiti-cholera-letter-rights-monitors (Hämtad 2021-06-18)

Sundling, Janne. Protester stoppar Kinas miljardhamn i Lysekil. *Fokus.* 2018-01-31. https://www.fokus.se/2018/01/protester-stoppar-kinas-miljardhamn-lysekil/ (Hämtad 2021-06-11)

Thomsen, Dante. Vad vet du om strömavbrott? Så här påverkas du och Sverige- timme för timme. SVT Nyheter. https://www.svt.se (Hämtad 2021-06-27)

Träff, Matilda/ TT. Hackade Coop: kräver 600 miljoner. *SVD*. 2021-07-05. https://www.svd.se/coop-har-polisanmalt-it-attacken (Hämtad 2021-07-07).

Wallberg, Peter/TT. Försvarsuppgörelse klar – tillskott på 13 miljarder. *DN.* 2020-09-18. https://www.svd.se/dn-regeringen-c-och-l-overens-om-forsvaret (Hämtad 2021-06-22)

WEBBSIDOR

European External Action Service (EEAS). *EU- NATO Cooperation.* EEAS, 2020. https://eeas.europa.eu/sites/default/files/eu_nato_factshee_november-2020-v2.pdf (Hämtad 2021-06-24)

Europaparlamentet. Defence: MEPs push for more EU cooperation to better protect Europe. *Europaparlamentet.* 2016. https://www.europarl.europa.eu/news/en/press-room/20161117IPR51547/defence-meps-push-for-more-eu-cooperation-to-better-protect-europe (Hämtad 2021-06-24)

Europaparlamentet. "EU-armé"? Vad gör Europa för att stärka sitt försvar? *Europaparlamentet.* 2021. https://www.europarl.europa.eu/news/sv/headlines/security/20190612STO54310/eu-arme-vad-gor-europa-for-att-starka-sitt-forsvar (Hämtad 2021-06-18)

Eurostat. China, US and EU are the largest economies in the world. *Eurostat*. 2020-05-19. https://ec.europa.eu/eurostat/documents/portlet_file_entry/2995521/2-19052020-BP-EN.pdf/bb14f7f9-fc26-8aa1-60d4-7c2b509dda8e (Hämtad 2021-06-18)

Forsvaret. Organisasjon. *Forsvoret.* https://www.forsvaret.no/om-forsvaret/organisasjon (Hämtad 2021-06-12).

Försvarshögskolan. Över 1000 sökande till Officersprogrammet. *Försvarshögskolan*. 2021. https://www.fhs.se/arkiv/nyheter/2021-02-09-over-1000-sokande-till-officersprogrammet.html
(Hämtad 2021-06-24)

Försvarsmakten. Cyberförsvar. *Försvarsmakten.* https://www.forsvarsmakten.se/sv/var-verksamhet/det-har-gor-forsvarsmakten/cyberforsvar/ (Hämtad 2021-06-21).

Försvarsmakten. Cybersoldat. *Försvarsmakten.* https://jobb.forsvarsmakten.se/sv/utbildning/befattningsguiden/gu-befattningar/cybersoldat/ (Hämtad 2021-06-13)

Försvarsmakten. Hemvärnet. *Försvarsmakten*. https://www.forsvarsmakten.se/sv/var-verksamhet/det-har-gor-forsvarsmakten/hemvarnet/ (Hämtad 2021-06-17).

Försvarsmakten. Visionen. *Försvarsmakten*. https://www.forsvarsmakten.se/sv/om-forsvarsmakten/varderingar-och-vision/vision/ (Hämtad 2021-07-04)

Försvarsmakten. Värnplikten genom åren. *Försvarsmakten*. https://www.forsvarsmakten.se/sv/information-och-fakta/var-historia/artiklar/varnplikt-under-109-ar/ (Hämtad 2021-06-22)

Kaitselit. Estonian Defence Leauge's Cyber Unit. *Estonian Defence League*. https://www.kaitseliit.ee/en/cyber-unit (Hämtad 2021-06-17).

Landguiden. Konflikten i Jemen. *Utrikespolitiska institutet.* https://www.ui.se/landguiden/konflikter/jemen/ (Hämtad 2021-06-25)

Lentz, Carl. Made in China 2025 ska ge högteknologiskt övertag. *Utrikesmagasinet*. 2019-03-14. https://www.ui.se/utrikesmagasinet/analyser/2019/mars/made-in-china-2025-ska-ge-hogteknologiskt-overtag/ (Hämtad 2021-06-10)

Minárik, Tomáš. NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. *The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/* (Hämtad 2021-06-13).

Ministry of Foreign Affairs of the Republic of Latvia. NATO Enhanced forward Presence. M*inistry of Foreign Affairs of the Republic of Latvia*. 2021. https://www.mfa.gov.lv/en/policy/security-policy/nato-enhanced-forward-presence (Hämtad 2021-06-23)

MSB. It-incidentrapportering för statliga myndigheter. *MSB*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/it-incidentrapportering-for-statliga-myndigheter/ (Hämtad 2021-06-07)

MSB. NIS-direktivet. *MSB*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/ (Hämtad 2021-06-07)

MSB. Statliga myndigheters it-incidentrapportering 2020. *MSB*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/it-incidentrapportering-for-statliga-myndigheter/it-incidentrapportering-2020/ (Hämtad 2021-06-07)

MSB. Totalförsvar och civilt försvar. *MSB.* https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/totalforsvar-och-civilt-forsvar/ (Hämtad 2021-07-04)

Nationellt cybersäkerhetscenter. Frågor och svar om cybersäkerhetscentret. *FMV, FRA, Försvarsmakten, MSB, Polisen, PTS, Säpo.* https://www.cfcs.se/fragor-och-svar/ (Hämtad 2021-06-13)

Nato announces start of Cyber Coalition exercise. *Army Technology*. 2020-11-17. https://www.army-technology.com/news/nato-announces-start-of-cyber-coalition-exercise/ (Hämtad 2020-06-13)

Nato. NATO Cyber Defence. *Nato*. 2016. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf (Hämtad 2021-06-13).

Nato. Cyber Defence Pledge. *Nato*. 2016. https://www.nato.int/cps/en/natohq/official_texts_133177.htm (Hämtad 2021-06-13).

Nato. NATO Rapid Reaction Team to fight cyber attack. *Nato.* 2012. https://www.nato.int/cps/en/natolive/news_85161.htm (Hämtad 2020-06-13)

Plikt- och prövningsverket. Mönstringsunderlaget. Plikt- och prövningsverket. 2021. https://pliktverket.se/monstring-och-varnplikt/monstring/monstringsunderlaget (Hämtad 2021-06-13).

Regeringskansliet. Regeringen inrättar ett nationellt cybersäkerhetscenter. *Regeringskansliet*. 2020. https://www.regeringen.se/pressmeddelanden/2020/12/regeringen-inrattar-ett-nationellt-cybersakerhetscenter/ (Hämtad 2021-06-13)

Regeringskansliet. Statsrådsberedningens organisation. *Regeringskansliet*. 2021-06-23. https://www.regeringen.se/sveriges-regering/statsradsberedningen/statsradsberedningen-organisation/ (Hämtad 2021-06-12).

Regeringskansliet. Statsrådsberedningen. *Regeringskansliet.* https://www.regeringen.se/ (Hämtad 2021-06-12)

Regeringskansliet. Det nordiska försvarssamarbetet Nordefco. *Regeringskansliet*. https://www.regeringen.se/ (Hämtad 2021-06-23)

Regeringskansliet. Myndigheterna. *Regeringskansliet.* https://www.regeringen.se/ (Hämtad 2021-06-15)

Saab. Saab receives follow-on contract for GlobalEye. *Saab.* 2021. https://www.saab.com/newsroom/press-releases/2021/saab-receives-follow-on-contract-for-globaleye (Hämtad 2021-06-25)

Säkerhetspolitik.se. GSFP. *MSB*. 2011. https://www.sakerhetspolitik.se/Ordlista/G/GSFP/ (Hämtad 2021-06-24)

U.S. Senate Select Committee on Intelligence. Overview of the Senate Select Committee on Intelligence Responsibility and Activites. *U.S. Senate Select Committee on Intelligence.* https://www.intelligence.senate.gov/about (Hämtad 2021-06-16)

Utrikesministeriet. Finland publicerade sina ståndpunkter om folkrätt i cybermiljön. *Utrikesministeriet.* 2020-10-15. https://um.fi/nyheter/-/asset_publisher/GRSnUwaHDPv5/content/suomi-julkisti-n-c3-a4kemyksens-c3-a4-kansainv-c3-a4lisest-c3-a4-oikeudesta-kyberymp-c3-a4rist-c3-b6ss-c3-a4 (Hämtad 2021-06-13).


MUF
moderata
ungdomsförbundet