2024-05-27

Version: 0.18

Hans Thorsen Lamm

hans@lammda.se

REMISSVAR

Till: Försvarsdepartementet

Att: Visnja Raguz

fo.remissvar@regeringskansliet.se

visnja.raguz@regeringskansliet.se

Remissvar över delbetänkandet:

Nya regler om cybersäkerhet (SOU 2024:18) (FÖ2024/00496)

Sammanfattning

Vi stödjer införandet av en lag för att upprätthålla hög cybersäkerhet, men vi anser att förslagets exkludering av försvarssektorn i betänkandet bör omprövas. Erfarenheterna från konflikten i Ukraina belyser vikten av multipla användningsområden där civila produkter framgångsrikt använts militärt. I försvarsministerns rapport om strategisk försvarsinnovation framgår det att utvecklingen till övervägande del har drivits av den civila sektorn.

Förslaget inkluderar forskning som en separat sektor vilket är problematiskt. Vid konferensen "Hur ska Sverige hantera forskning med civila och militära tillämpningar?" arrangerad av Ingenjörsvetenskapsakademin lyftes frågan. Forskning inom civila sektorer har redan omfattande lagstiftning på plats. Ytterligare reglering inom de civila sektorerna kan leda till att resurser överförs till sluten militär forskning där spridningseffekterna till det civila samhället sannolikt är mindre.

Ukraina har sedan annekteringen av Krim byggt upp egen kompetens för hur befintliga civila produkter kan användas militärt. Denna kompetens kommer vara mycket eftertraktad även civilt. Översatt till svenska förhållanden utgörs dessa kompetenskluster av hemvärn, yrkeshögskolor och driftiga entreprenörer i samverkan. Betänkandet i dess nuvarande form anser vi motverkar tillkomsten av dessa kluster.

Den statiska indelningen av högkritiska och andra kritiska sektorer saknar anpassning till dual-use. En indelning som reflekterar multipla användningsområden öppnar upp för samordning, vilket i sin tur främjar innovation. Erfarenheterna från Ukraina understryker vikten av att kreativt använda befintliga kommersiella komponenter, produkter samt tjänster för att skapa motståndskraft.

I detta svar så kommer betänkandets riskbaserade modell appliceras på ett hot där civila produkter modifierats för att attackera militära vapensystem.

Vi föreslår integration av militära tillämpningar i form av multipla användningsområden i de föreslagna sektorerna.

Övriga synpunkter

Rubriken är hämtad från MSB:s remissvar där de efterlyser samordning med totalförsvaret.

Detta dokument innehåller kommentarer på betänkandet i form av understrukna anteckningar i slutet av vissa rubriker. Vidare behandlas problematiken kring avgränsningen mellan det civila och det militära.

Sverige har en historia där dynamit, kullager och Boforskanoner haft stor påverkan på andra världskriget. Med detta i åtanke tillämpar detta remissvar taktiker från cyberkrigföring, såsom påverkan på leveranskedjor och överbelastningsattacker.

Händelserna i Ukraina och Mellanöstern har mycket gemensamt, vilket ger en intressant möjlighet att analysera komplexiteten i hur vapensystem nu skapas genom kreativ anpassning av civil teknologi.

Ett fiktivt men realistiskt scenario används för att applicera den riskbaserade modellen från NIS2-betänkandet i ett militärt sammanhang. Det som ska skyddas är stridsflygplan, hotet utgörs av civil teknologi modifierat för militärt bruk. Vidare föreslås en enkel åtgärdsplan.

Sverige är mycket beroende av Kina när det gäller leveranskedjor för elektrifiering. Tyskland hade ett liknande beroende av rysk gas.

En högt prioriterad civil sektor är finans, som på eget initiativ har kontaktat det nationella cybersäkerhetscentret vilket tillhör försvaret. Detta nämndes vid Dagens Industris konferens "Cybersäkerhet 2024". Civilministern presenterade även en bild som bekräftade att det nationella cybersäkerhetscentret är en prioritet. Presentationen från MSB:s generaldirektör verkade inte vara helt i linje med detta.

De geopolitiska allianserna för handel mappar mycket dåligt med de militära. Om syftet med lagen är att skapa resiliens inom cybersäkerhet så är kommer exkluderingen av försvaret göra det mycket svårt att genomföra.

Vi föreslår att militära och civila myndigheterna inkluderar multipla användingsområden i de scenarion som ligger till grund för riskanalys.

Dual use

I betänkandet nämns termen militär och dual use endast en gång, och det är i samband med rymden. På Försvarsmaktens hemsida kan man läsa: "Det aktiva försvaret innefattar hela totalförsvaret, inklusive både militära och civila delar." Med totalförsvaret avses land, sjö, luft, rymd samt cyber.

I försvarsministerns informationsmaterial, daterat januari 2024, framgår det tydligt att beroendet av innovationskraften i den civila industrin är betydande. "Ömsesidigt stärka innovation inom både det militära och civila området som bidrar till Sveriges försvarsförmåga, innovationskraft, ökad konkurrenskraft och stärkt säkerhet."

Insikten om hur det militära integreras med det civila har blivit mycket tydlig i samband med pågående konflikter. Det vore därför önskvärt om denna realitet även återspeglades i det slutgiltiga förslaget.

Vi föreslår att den övergripande exkludering av den militära sektorn istället ersättas med regulatoriska sandlådor för relevanta sektorer.

Nato

Solidariteten inom Nato förutsätter att varje enskild medlemsstat uppfyller de krav på krigsduglighet, inklusive uthållighet och robusthet, som ställs på det militära försvaret och på det övriga samhällets förmåga att stödja krigsansträngningen.

Enligt Natos strategiska koncept från 2022 kan en eller flera skadliga cyberaktiviteter nå nivån av väpnat angrepp och leda Nordatlantiska rådet till att åberopa artikel 5.

Sverige har gentemot NATO en skyldighet att försvara internetansluten kritisk infrastruktur mot inkommande cyberattacker. Beträffande utgående cyberattacker så har Ryssland signalerat att ett cyberangrepp riktat mot kritiskt viktiga objekt som påverkar deras nukleära svarsförmågan negativt kan utgöra skäl för rysk användning av kärnvapen.

En cyberattack kan initieras via överlagrade krypterade nätverk såsom TOR, där en angripare befinner sig utanför Sverige, men nyttjar en så kallad exit nod ansuten till en svensk IP-adress. En attack kan då riktas mot inhemsk kritisk infrastruktur, men även nyttjas för att attackera rysk infrastruktur. I båda fall så är IP-adressen knuten till Sverige.

Via TOR-nätverket så går det även att köpa en överbelastningsattack som en tjänst. Inte sällan är det stora mängder uppkopplade Internet-of-thing enheter som kontrolleras av en krimimell organisation

De flesta köpcenter erbjuder gratis trådlös internet anslutning, kombinerat med integritetsinställningar så är det i princip omöjligt att spåra angriparen.

Tekniskt sätt så är det enkelt att lösa med hjälp av registrering av allt och alla som skall anslutas till Internet, men detta kan vara i strid med EU:s grundläggande lagar om personlig integritet. "*Everyone has the right to the protection of personal data concerning them*".

Sverige och USA har nyligen initierat en dialog om samarbete med USA om att skydda mänskliga rättigheter online.

Både ingående och utgående cyberangrepp kan enligt Nato och Ryssland räknas som ett väpnat angrepp och därmed leda till en krigsförklaring. Myndigheter som har det yttersta ansvaret har enligt betänkandet lägre sanktionsavgift vilket kan påverka förebyggande åtgärder.

Tillsyn

Post och telestyrelsen (PTS) har idag ansvar för tillsyn inom digital infrastruktur. Enligt betänkandet kommer vissa delar av lagen om elektronisk kommunikation (LEK) kommer att flyttas över till NIS2, det finns även skrivningar om toppdomänlagen (2006:24) vilken för övrigt involverar finansdepartementet. Toppdomänlagens paragraf 14 handlar om versamhet i krig och fred. Attacker mot toppdomäner ingår i cyberkrigföring där gränsen mellan krig och fred är mycket otydlig. Det finns en vag skrivning om att regeringen får meddela de föreskrifter som behövs med hänsyn till landets försvar eller säkerhet i övrigt. I händelse av krig så är Sveriges toppdomän sannolikt ett mål.

Utrustning som ansluts till internet i syfte att förse elnätet med lagring bör begära tillsyn både hos Post och Telestyrelsen samt Energimyndigheten. En cyberattack riktad mot en växelriktare som är uppkopplad till en personbil kan både användas vid cyberattacker, men även få allvarliga konsekvenser för stabiliteten i elnätet.

MSB har i sitt remissvar (MSB 2024-03843-4) identifierat liknande överlapp avseende tillsyn

Vi anser att förslaget kommer leda till svåra och kostsamma tolkningar av vilka tillsynsmyndigheter som gäller i enskilda fall.

Forskning inom dual-use

Ett nytt område i NIS2-direktivet är forskning, där utbildningsinstitutioner undantas från direktivets tillämpningsområde. Medlemsstaterna kan välja att inkludera dem.

Högskolor som bedriver forskning omfattas redan idag av många lagar, såsom Offentlighets- och sekretesslagen, Dataskyddslagen, Kamerabevakningslagen, Etikprövningslagen, Biobankslagen, Upphovsrättslagen, Patentlagen, Säkerhetsskyddsförordningen samt Arkivlagen.

Forskning som bedrivs inom försvarssektorn omfattas av säkerhetsskyddsförordning, där det ställs högre krav på personer att få tillgång till information och resurser. Vidare måste personer genomgå kontroll avseende pålitlighet.

I ett brev från SAAB till Utbildningsdepartementet framgår det: "*Till följd av minskad statlig forskning inom försvarsområdet har Saab alltmer förlitat sig på civila forskningsfinansiärer, exempelvis EU och Vinnova, samt genom egenfinansiering. Dock är de låga nivåerna på militär forskning ohållbara för nationen på längre sikt.*"

Genom att integrera dual-use i betänkandet bör samarbetet förenklas. Vi har även initierat en arbetsgrupp inom säkra leveranskedjor inom ramen för den svenska Cybernoden, som drivs av RISE på uppdrag av MSB och finansieras av Vinnova.

Syftet med Cybernoden är att bilda virtuella konsortier bestående av fyra olika typer av aktörer för att gemensamt söka medel från EU:s olika program. Den kompetensdatabas som hanterar matchning mellan medlemmarnas specialiteter och aktuella utlysningar speglar inte de möjligheter som nu finns med Sveriges inträde i NATO.

De industriella kluster som formats runt dåtidens innovation och samarbete med försvaret skiljer sig mycket från den innovations-struktur som EU nu definierat. Från spontana och problemorienterade kluster så kommer forskning i EU

ske i en hiearkisk struktur med innehåll och tidsmässiga avgränsningar. Det liknar mer den planekonomi som tillämpades i det forna Sovjet. Då svenska Alfa-Laval levererade separatorer till ryska kunder, så returnerades produkterna eftersom teknisk utveckling reducerade vikten, företaget fick då fylla bly i fundamenten, eftersom industriproduktion mättes i ton och inte antal enheter. Att mäta innovation efter hur mycket pengar som avsätts till detta kan därför vara missvisande.

I ett remissvar Ds 2023:34 Statsrådsberedningen, SB PM 2021:1 går att läsa.

Försvarsföretagen som är verksamma i Sverige är med sin egen forskning och tekniska kompetens viktiga aktörer och länkar mellan totalförsvaret och de civila och internationella FoU-miljöerna.

Det är allt svårare att dra en tydlig linje mellan civil forskning och utveckling och forskning och utveckling för totalförsvaret, inte minst när det gäller nya och framväxande tekniker.

Försvarsmakten, Försvarets materielverk (FMV) och Myndigheten för samhällsskydd och beredskap (MSB) är de största offentliga finansiärerna av FoU inom totalförsvarsområdet.

Enligt försvarsuppfinningslagen är det patentverkets ansvar att plocka ut ansökningar som försvaret ska pröva för behovet av sekretess och skicka dem till FMV. Uppfinnaren/sökanden kan då aldrig bli ansvarig för sekretessbrott.

Innovation handlar om att utveckla och införa nya idéer eller lösningar, forskning är processen att generera ny kunskap och förståelse, utveckling är processen att ta en idé till praktisk användning, och entreprenörskap är processen att identifiera och utnyttja affärsmöjligheter för att skapa värde och driva tillväxt.

Då företagshemlig och militär forskning finansieras med statliga medel från Vinnova, kan det bromsa civil innovation. SAAB har tilldelats en tredjedel av budgeten för utlysningen "Cybersäkerhet för avancerad industriell digitalisering" av Vinnova för ett projekt inom leveranskedjor med öppen källkod. Trots detta har SAAB valt att inte delta i arbetet. En anledning kan vara bristen på en regulatorisk sandlåda som krävs för dual-use. Andra orsaker kan vara säkerhetsklassning och krav på svenskt medborgarskap för deltagarna.

MSB har förutom det övergripande ansvaret för samtliga tillsynsmyndigheter även tilldelats uppgiften att fördela medel från EU. I detta uppdrag så skall forskningen samordnas vilket kan bli problematiskt då varje land skall driva egna instanser inom ramen för cybersäkerhet. Erfarenheterna från Ukraina visar att mycket av den motståndskraft som nu stoppar angriparen är att resultat av innovativa ändringar av civila produkter.

EU:s andel av världsekonomin jämfört med USA har minskat under de senaste årtiondena, vidare så hade Sverige lägst tillväxt under 2023 av alla EU-länder.

Vi anser att det formerna för samarbete mellan civila och militära aktörer inom multipla användningsområden bör definieras utifrån identifierade problem från pågående militära konflikter.

Utbildning inom dual use

2019 skrev SAAB till Utbildningsdepartementet:

”*Sverige ska vara en ledande kunskapsnation, där högkvalitativ forskning, högre utbildning och innovation leder till samhällets utveckling och välfärd, näringslivets konkurrenskraft och svarar mot de samhällsutmaningar vi står inför, både i Sverige och globalt.*”

Yrkeshögskolor omfattas inte av betänkandet, vilket bör omprövas med tanke på dual-use. Det som kännetecknar denna typ av utbildning är den starka kopplingen till industrin. Anpassning av befintlig civil teknologi för militära syften kräver sällan högskolekompetens. De som studerar har i många fall yrkeslivserfarenhet.

Den snabba utvecklingen av autonoma system i Ukraina har skett på relativt kort tid och är därmed inte ett resultat av forskning. Det handlare snarare om att anpassa kommersiellt tillgänglig teknik för militära syften.

Via yrkeshögskolan erbjuds ett tjugotal program med inriktning på cybersäkerhet. Yrkeshögskolor som verkar inom cybersäkerhet borde ha försvaret representerat i sina ledningsgrupper.

Det finns även privata aktörer som erbjuder utbildning inom cybersäkerhet. Dessa kurser är oftast mycket intensiva med kort varaktighet. Då de sker utan statlig finansiering klassificeras utbildningen som tjänst vilket gör det svårt att kartlägga omfattningen.

Efter pandemin så har distansarbete etablerat sig, vilket även påverkar utbildningar. Traditionell utbildning som leds från ett klassrum av en lärare (fysiskt och synkront lärande) är i numera ersatta av självstudier på distans (virtuella och asynkrona). En konsekvens är att den svenska marknaden för digital utbildning är nu tillgänglig för utländska aktörer vilket medför att detta segment är hårt utsatt. Då cybersäkerhet befinner sig i ständig utveckling är kostnaden mycket hög för att hålla ett svenskt material aktuellt.

USA har mindre inslag av statlig finansiering i sitt utbildningssystem, vilket gör att både företag och enskilda individer vänder sig till privata aktörer. Dessa kan på mycket kort tid erbjuda en kurs där det finns behov, vilket inte är fallet då det sker via svenska myndigheter. Det kan ta upp till arton månader från att det uppstår ett behov av en viss kompetens, tills dess att utbildningen är på plats.

För komplexa och uppkopplade system så kommer flera regelverk involveras såsom Cybersecurity Resilience Act, vilken i sin tur ställer krav på leveranskedjor. Dessa kedjor borde knytas hårdare till utbildningsbehovet.

Den offentliga konkurensen i kombination med det som erbjuds via internet medför att det är mycket svårt att erbjuda grundläggande utbildning inom cybersäkerhet. För en yrkeshögskola så krävs mycket praktiska moment vilket i sin tur kräver tillgång till datacenter. Ersättningen för heltidsstudier understiger i vissa fall kostnaden för att köpa resurser i ett svenskt datacenter.

Vad gäller offentligt ägda bolag finns en särskild regel om förbud mot offentlig säljverksamhet i konkurrenslagen. Den innebär att staten inte får sälja tjänster på ett sätt som begränsar konkurrensen på marknaden. Enligt en färsk undersökning från konkurrensverket så upplever en fjärdedel av de privata företagen konkurrens från den offentliga sektorn.

Amerikanska datacenter har etablerat sig i Sverige på grund av subventionerad energi. I samband med detta så har även det statliga bolaget RISE ansvaret för ett av detta center. Ett annat center som förvaltas av RISE är cyberrange där man erbjuder utbildning och konsultation som i många fall konkurrerar med fristående aktörer.

Det digitala samhället är beroende av öppen källkod, som i sin tur är beroende av få personer. Begreppet platform är därför missvisande, en bättre beskrivning är en omvänd pyramid. Det svenska projektet curl är ett oberoende projekt som med mindre än tio personer förser miljarder användare med funktionalitet. Den senaste incidenten handlade om ett stödjande projekt som under lång tid infiltrerats i syfte att skapa bakdörrar in i miljontals datorer. Den databas som i princip hela världen använder för att hantera kända sårbarheter sköts av mindre än trettio personer i USA.

För att få lönsamhet inom utbildning krävs breda utbildningar riktade mot företagsledning. För att lösa problemen med säkerheten krävs smala kurser på distans där betalningsbeviljan är mycket låg.

Ukraina har under två år utbildat cirka tio tusen drönarpiloter. Kunskap om att bygga egna drönare startades redan 2014 när Krimhalvön ockuperades.

Med hjälp av frivilliga krafter och donationer så har genomförandet skett mycket snabbt. Då det finns mycket synergier mellan civila och militära tillämpningar så lämpar sig detta mycket väl för dual-use. Erfarenheterna från Ukraina visar att mindre drönare är viktiga för spaningsuppdrag. Då de är mycket utsatta så är det en stor fördel om civil teknologi kan nyttjas. Krav och erfarenheter mellan det militära och det civila kan med fördelas utväxlas om detta sker inom ramen för hemvärn/civilförsvar.

Förutsättningarna för att bedriva utbildning inom cybersäkerhet i konkurrens med staten bör ses över.

Delar av det svenska utbildningssystem bör knytas till leveranskedjorna för bättre följsamhet och kort återkoppling.

Säkerhet och / eller regelefterlevnad

Betänkandet värnar om det fria kunskapssökandet och den fria kunskapsspridningen, men det måste ske inom rättsliga ramar.

I en tid präglad av fred, ekonomisk tillväxt och optimism har stora nedskärningar skett inom Försvarsmakten och övriga försvarsmyndigheter. Mellan 2009 och 2022 minskade anslagen till försvaret med en procent av BNP. Med inträdet i NATO måste detta öka från dagens 1,2 till 2,0 procent.

I betänkandet har ett antal myndigheter uppskattat kostnaden för att bygga upp kompetens kring NIS2. Det är svårt att bedöma det totala behovet, men de regleringar som snart träder i kraft återspeglas i den breda skalan av utbildningar/seminarier riktade till företagsledning avseende NIS2.

I fredstid är fokus på regelefterlevnad inte detsamma som säkerhet. I krigstid är säkerhet viktigare än regelefterlevnad. Ett exempel kan vara att låta drönare stiga till höjder som överstiger de fredstida reglerna för att via spaning täcka ett större område och därigenom öka tidsfristen för egna soldater att uppsöka skydd. Att strikt följa reglerna som gäller i fred innebär att spaningsuppdraget försämras och soldater riskerar skador eftersom regeluppfyllnad prioriteras.

Ansvarig chef för det datacenter som nyligen drabbades av en allvarlig incident försvarade sig i media med orden: “*It-säkerheten brast inte*.”

Oavsett hur många som utbildas och anställs inom cybersäkerhet kan fokus på regelefterlevnad leda till bristfällig säkerhet

Genom att integrera det militära och civila (vilken i praktiken redan är en realitet) där så är lämpligt så uppstår spridningseffekter i båda riktningar.

Vi anser att försvarsindustrin bör integreras i förslaget för att få mer fokus på säkerhet, då detta även underlättar regelefterlevnad avseende cybersäkerhet

Personkontroll

Energimyndigheten som enligt direktivet faller inom en högkritisk sektor har nyligen anställt en person som på sociala medier är aktivt inom en radikal klimatrörelse ska omfattats av denna kontroll. En person med rötter i en diktatur, men med svenskt medborgarskap kan arresteras och pressas på information vid besök i sitt forna hemland. Vidare finns det andra sektorer såsom polis och rättsväsende där infiltration har skett och förväntas öka i framtiden.

Vi anser att försvarsindustrin bör integreras i förslaget för att få mer fokus på säkerhet.

Klassificering av dual use

EU

Leveranskedjor och handel

Idén att bilda EU uppstod efter två krig i Europa med fokus på tillväxt och en gemensam inre marknad. År 1991 etablerades en gemensam utrikes- och säkerhetspolitik, vilken ytterligare förstärktes 1999. Närmare samarbete med NATO påbörjades omkring 2002. Arbetet med att utforma riktlinjer för hantering av cyberhot påbörjades 2018, och några år senare avsattes medel för att stärka Ukrainas försvar med vapen efter konflikten mellan Ukraina och Ryssland, vilket ledde till ökat fokus på försvar.

Den tydliga gränsen mellan krig och fred som existerade vid EU:s grundande är inte längre lika skarp. Cyberattacker utgör en väsentlig del av modern krigföring och sker dessutom kontinuerligt. Civila resurser används i konflikter för att utmatta och överbelasta motståndaren. Exempelvis har Sverige valt att installera elmätare från Kina, och en betydande del av vindkraftsproduktionen ägs av kinesiska intressen. Tysklands beslut att ersätta kärnkraft med rysk naturgas ifrågasätts idag, särskilt med tanke på att leverantören Gazprom sedan 2007 har en egen militär arme´. Den tidigare föreställningen om att handel främjar fred har ifrågasatts mot bakgrund av dessa utvecklingar.

Problemet med multipla användningsområden har identifierats och och finns beskrivet i en rapport från 2023.

- Introducing new items on the EU control list to close the gaps in controls that may be created by blockage of the decision-making process within multilateral regimes by certain of their members
- Bringing forward the evaluation of the current Dual-Use Regulation to the beginning of 2025
- Creating a high-level forum to discuss export control developments and foster a common EU position
- Improving the coordination of Member States' National Control Lists ahead of their adoption (through a voluntary approach)

Finansiering

Sveriges statsminister skrev tillsammans med 14 andra regeringschefer till Europeiska Investings Banken (EIB) ett brev där de påpekade legala begränsningarna med dual-use. EIB har för övrigt aviserat finansiering med 8 miljarder euro för forskning och innovation. I denna utlysning understryker man vikten av att få spridningseffekter till små företag där ekosystem uppstår.

Inspektionen för Strategiska Produkter

Inspektionen för strategiska produkter kontrollerar Sveriges export av vapen och produkter som kan användas såväl i civil verksamhet som för försvarsändamål. ISP övervakar också bestämmelserna i FN:s konvention om förbud mot kemiska vapen.

PDA förordningen

Denna är att resultat av Europaparlamentets arbete (EU 2021/821) och den senaste versionen är daterad 20:e maj 2021, dvs innan konflikten i Ukraina.

“upprättande av en unionsordning för kontroll av export, förmedling, transitering och överföring av samt tekniskt bistånd för produkter med dubbla användningsområden”

”Obemannade luftfarkoster” (”UAV”), obemannade ”luftskepp” samt därtill hörande utrustning och komponenter”

Inkluderar ett system/en mekanism för aerosolspridning med större kapacitet än 20 liter.

Generalklausulen Catch-all

I vissa fall kan inspektionen för strategiska produkter tillämpa en regel som omfattar programvara, teknologi, produkten i sin helhet eller ingående komponenter. Autonoma system baserade på öppen och civil teknologi kan relativt enkel anpassas för militär slutanvändning. Ofta sker det genom att autonomt system kompletteras med annan civil teknologi från fastighets och industriautomation. I klausulen klassas ett vapenbärande system för missil, och dessa laster ska vara kemisk, biologisk eller kärnladdning.

Utmaningar

Var i livscykel skapas militär programvara?

Programvara för motorstyrning av förbränningsmotorer utvecklas av aktörer inom transportsektorn, där slutanvändaren saknar möjlighet att ändra dess funktionalitet. Erfarenheterna från "Dieselgate", där en tysk leverantör av bilar drabbades av sanktioner, visar det tydliga sambandet mellan en producent och många slutkunder.

Programvara för mobiltelefoner utgör en del av system där många tillverkare erbjuder olika funktioner till många slutkunder via en marknadsplats. En mobiltelefon har ett underliggande operativsystem som kan uppdateras efter leverans. Dessutom ställer EU:s Cybersecurity Resilience Act krav på att produkter som säljs på den inre marknaden ska kunna få mjukvarukorrigeringar. Uppdatering av mjukvara på distans involverar även NIS2. De applikationer som körs ovanpå ett operativsystem måste också underhållas, vilket lägger till ytterligare en nivå av komplexitet.

Programvara för hemautomation riktar sig till en bred grupp av slutanvändare, där kraven på enkelhet är höga. Det är vanligt förekommande att slutanvändare kan skapa funktionalitet direkt med hjälp av grafiska verktyg.

I det sistnämnda fallet blir den militärt strategiska funktionen aktuell när en redan klassificerad produkt ändras av slutanvändaren. Den programvara som slutanvändaren använder kan i sin tur vara möjlig att ladda ner efter leverans.

Sammantaget är det mycket svårt att applicera en statisk modell för klassificering av system på en dynamisk verklighet.

Var i monteringen blir en produkt militär?

En större drönare avsedd för användning inom jordbruket kan falla under exportrestriktioner, särskilt om den har stor lastkapacitet och kan sprida vätska över skogar och åkrar. I så fall är det troligt att den omfattas av PDA-förordningen och därmed exportrestriktioner. Ingående komponenter såsom batterier i samma drönare omfattas förmodligen inte av detta. Ryssland utnyttjar detta genom att importera enskilda komponenter för att sedan integrera dem inom landet

Ukraina

– Det är viktigt att vi systematiskt drar lärdomar av kriget i Ukraina för att stärka vårt eget totalförsvar. Det omfattar också att utvärdera hur svensk och västlig materiel har klarat stridssituationer, säger försvarsminister Pål Jonson.

Den utrustning som tillhandahålls till Ukraina—inklusive luftvärn, självgående haubitsar, stridsfordon, stridsvagnar, sovjetiska stridsflygplan från Polen och Slovakien, och senast löftet om F-16 stridsflygplan från USA:s allierade—kommer att behöva underhållas och förses med bränsle, och en del av detta stöd kräver en betydande logistisk infrastruktur. Alla avancerade västliga system som nu finns i Ukrainas ägo kommer att göra lite för att förskjuta balansen till landets fördel om de fastnar bakom linjerna och väntar på delar och bränsle eller lämnas utan kvalificerad personal för att underhålla dem. Växande underhålls- och supportutmaningar, inklusive bristen på reservdelar och bränsle, kommer att påverka tidslinjerna för ytterligare leveranser av avancerad västlig militärutrustning. Även om det är väsentligt att träna ukrainska soldater att använda Leopards, Challengers eller Abrams, är det lika viktigt att träna underhålls- och förvaltningspersonal som behövs för att hålla dessa stridsvagnar igång. Liknande överväganden kommer att utmana beredskapen för F-16. Utmaningen med logistik för Ukraina är verklig och omedelbar. Effekten på slagfältet av dessa system kommer att bero på tillgången på delar, ammunition och bränsle. Planer på att leverera dessa system till Ukraina måste ta hänsyn till utmaningen med att få dem dit de behöver vara, när de behöver vara där.

Lärdomarna av att utsättas för moderna GPS styrda raketer har resulterat i att Ryssland nu övergått från stora centrala ammonutionsdepåer till många mindre, vidare så kan inte längre väst förlita sig på GPS.

Ryssland har tillgång till tre gånger fler granater är vad Ukraina har, vilket utnyttjas genom att tvinga Ukraina att tömma sin arsenal av dyrbara missiler för att skjuta ner ålderdomliga inkommande granater. När dessa är slut så övergår man till moderna glidbomber.

Artelligranater är dyra att tillverka, trotylen måste gjutas för utstå den kraftiga rotation som krävs för att få hög precision. I Syrien användes så kallade tunnbomber, vilket i princip är ett oljefat fyllt med dynamit och metallskrot.

Här använder båda sidor drönare med IR-kameror och vapenlast. Det är mycket sannolikt att Sverige måste få in detta i försvaret i form av dual-use. Autonoma system från Ukraina kommer därför belysas ur ett NIS2 perspektiv.

Utvecklingsmodell.

I Ukraina så sker ibland beställning av försvarsteknologi via sociala medier. Exempel nedan från LinkedIn där man utifrån ett riktigt problem. Bolaget bakom förfrågan erbjuder även hjälp med att driftsätta lösningen.

Brave1 is looking for interceptor drone developers

Russian reconnaissance drones Orlan, SuperCam or ZALA over the front line are eyes for Russian artillery and strike UAVs. We should find a solution to shoot such drones down without wasting air defense supply. Therefore, we are looking for developers and engineers capable of creating such products.

Key development requirements:

•shoot down targets at a speed of 100-150 km/h at an altitude of 1,500 meters.

The solution must demonstrate how:

•the interceptor receives preliminary information about the target from the detection system
•takes off, finds a target and starts chasing
•hits the enemy drone by itself

If there is a ready-made solution, fill out the form: https://lnkd.in/eHVxTVrG

And what's next? If your solution meets the requirements, the Brave1 cluster will reach out and help develop the drone.

Get involved in development, apply to Brave1 and strengthen the Ukrainian military.

Autonoma system till havs

Små sjöburna robotar är svåra att upptäcka på grund av bruset från vattenytan. Lösningen har utvecklats på mycket kort tid av ett agilt kompetenskluster. Ett av designkriterierna var att systemet skulle vara enkelt att transportera på en vanlig båttrailer.

Enligt betänkandet kommer företag som tillverkar släpfordon att klassificeras enligt europeisk näringsgrensstandard som huvudgrupp 29. Dessa släpvagnar kan även ingå i vapensystem där de används för att transportera sjöburna robotar till lämpliga platser. Dessa robotar kan i sig drivas av civila produkter, såsom drivlinan från en Jetski.

Eventuella brister med sådana robotar kompenseras genom att de används i kluster nära målet, vilket överbelastar försvarets kapacitet. FMV har via sin portal begärt in förslag på en prototyp med en liknande lösning.

För att möjliggöra militär användning av släpfordon krävs kännedom om tillverkare och typ av släpvagn, vilket måste vara offentligt tillgängligt enligt lag. Informationen om användningen av släpvagnen kan dock klassificeras som sekretessbelagd med stöd av tillägg i NIS2-direktivet.

Autonoma system i luften

Luftburna obemannade farkoster är komplexa. En tillverkare kan leverera samma hårdvara, men mjukvaran definierar användningsområdet, såsom inom skogsbruk, brandbekämpning och försvar. Över tid kommer ett och samma system att användas inom olika sektorer. Beroende på sektorns vikt eller kriticitet kommer olika krav att ställas. Förutom kraven som nämns i NIS2 kan det även finnas specifika bransch- och regionala krav som tillverkaren måste beakta. Ett av argumenten för multipla användningsområden är att kostnaden för att införskaffa, underhålla och förnya systemet kan bäras av det civila under fredstid. De merkostnader som uppstår för att systemet även ska uppfylla kraven för militärt bruk är då mindre än kostnaden för att underhålla ett renodlat militärt system.

Sverige

Utvecklingsmodell

Försvarsmaktens materielverk (FMV) spelar en viktig roll i Sveriges försvarsförmåga genom att ansvara för utveckling, inköp, underhåll och avveckling av försvarsmateriel. Dess roll är avgörande för att säkerställa att Sveriges vapensystem är effektiva, moderna och anpassade för att möta de säkerhetshot som landet står inför.

Materielverket kan leda eller delta i forsknings- och utvecklingsprojekt för att skapa nya vapensystem eller förbättra befintliga system. Detta kan inkludera samarbete med både nationella och internationella företag, universitet och forskningsinstitut.

Materielverket ansvarar för att genomföra upphandlingar och inköp av försvarsmateriel, inklusive vapensystem och andra försvarsrelaterade produkter. Det kan innebära att man förhandlar avtal med försvarsindustrin och andra leverantörer för att säkerställa att Sverige får tillgång till den bästa möjliga utrustningen.

Efter att vapensystemen har inköpts är det materielverkets ansvar att se till att de underhålls och hålls i drift. Det kan inkludera planering och genomförande av underhållsinsatser, reservdelsförsörjning och teknisk support för användarna.

Materielverket kan erbjuda teknisk support och utbildning till försvarspersonal som använder vapensystemen. Det kan innefatta utbildning i användning, underhåll och reparation av utrustningen.

På FMV:s hemsida begärs in förslag på en obemannad farkost 24FMVU722, förmodlingen inspirerad av det som Ukraina använt mot den ryska flottan. Detta är intressant då FMV normalt lägger beställningar på stora helhetslösningar.

Dynamit och Bofors kanoner

Få svenskutvecklade produkter har blivit så omskrivna och fått en så stor historisk betydelse som Boforskanonen 40 mm. Den har beskrivits som ett av de vapen som kom att avgöra utgången av andra världskriget. Den första martinugnen togs i bruk av Bofors 1878, och en betydelsefull milstolpe inträffade den 16 augusti 1879, då Bofors tillverkade det första heltäta gjutstålet för eldrör – först i världen. Alfred Nobel köpte sedan hela AB BoforsGullspång och kanonverkstäderna började utvidgas.

Den 25 november 1928 fick Bofors i uppdrag av Marinförvaltningen att utveckla ett nytt specialvapen för luftvärn: en 40 mm kanon. Förebilden var en engelsk kanon som hade testats i Sverige under en tid. Efter fem års arbete var världens första helautomatiska kanon färdig att tas i bruk 1934. Utvecklingen av Bofors 40 mm krävde cirka 30 000 konstruktionsarbetstimmar och blev en stor nyhet i en tid då hotet från luften var på allas läppar. Det blev sannolikt en av vapenhistoriens mest uppmärksammade produkter någonsin. Bofors presenterade först en halvautomatisk kanon med kapacitet att avfyra 250 skott på fem minuter.

Den var snabb, träffsäker och stabil, kunde förflyttas på väg i olika hastigheter och kunde ta sig fram i ojämn terräng. Tiden för transport till skjutning var kortare än för någon annan pjäs, och ammunitionen var överlägsen i både verkan och funktionssäkerhet. De första kontakterna mellan Bofors och USA knöts 1938. I USA blev

Boforskanonen en integrerad del av försvaret, och licensproduktion startades främst på Chrysler Corporation i Detroit. Totalt uppskattas Chrysler ha tillverkat cirka 60 000 pjäser och över 120 000 eldrör.

Trots sina framgångar visade Boforskanonen sig vara otillräcklig i kampen mot de nya flygplanen med jetmotorer. Beslut togs 1979 om avveckling av Bofors ståldivision, och 1986 lämnade det sista eldröret fabriken i Karlsskoga. År 1991 slogs Bofors samman med FFV, Förenade Fabriksverken från Eskilstuna, och det nya namnet blev Swedish Ordnance inom Celsius-koncernen. År 2000 köpte försvarskoncernen SAAB-gruppen upp Celsius, och den del av företaget som ägnade sig åt kanoner och artilleriammunition såldes till det amerikanska företaget United Defense. Från Celsius andra bolag, Saab Dynamics, Bofors Missiles och Bofors Carl Gustaf, bildades Saab Bofors Dynamics, som ingår i SAAB-gruppen.

2014 upphörde all mekanisk bearbetning i kanonverkstadens gamla lokaler.

Saabs MSHORAD är en fordonsintegrerad lösning som används för motverka och neutralisera hot i luften, såsom obemannade flygande farkoster (UAV:er) och bepansrade helikoptrar. Systemet består av en mobil radarenhet och en mobil eldenhet som sedan kopplas samman med ett ledningssystem.

Stridsfordon

Hägglunds, med sitt ursprung i Örnsköldsvik, Sverige, är en företagshistoria som sträcker sig över mer än ett sekel. Det grundades ursprungligen 1899 som ett sågverk och träförädlingsföretag. Under 1940-talet började Hägglunds att tillverka skogsmaskiner och blev känt för sin kompetens inom terrängfordon.

Under årens lopp diversifierade Hägglunds sin verksamhet och började även producera andra fordon och system för militära ändamål, inklusive stridsfordon och artillerisystem.

Företaget har blivit en ledande global aktör inom försvarsindustrin med hela 80 procent av sin produktion som exporteras. Företaget är sedan 2004 en del av den brittisk-amerikanska jätten BAE Systems, en av världens största försvarsföretag med 90 000 anställda världen över. De senaste betydande beställningarna av CV90, stridsfordonet som för närvarande används i Ukraina, har kommit från Slovakien och Tjeckien. Tillsammans har dessa två länder beställt nästan 400 stridsfordon till ett sammanlagt värde på nära 40 miljarder kronor.

Stridsflygplan

Sveriges historia med stridsflygplan sträcker sig över flera årtionden och har präglats av teknologisk innovation och internationellt samarbete. Det började på 1950-talet med Saab 29 Tunnan, landets första stridsflygplan med jetmotor. Tunnan var banbrytande för sin tid och spelade en viktig roll i den svenska flygvapnets modernisering.

Frågan om det svenska militärflygets framtid hade oupphörligt diskuterats under slutet av 1970-talet. Skulle man fortsätta att producera egenutvecklade plan till höga kostnader? Eller var det bättre att licenstillverka eller rentav

köpa in från andra länder? De senare alternativen riskerade, menade många, att utarma den tekniska kompetensen i Sverige, samtidigt som industrin skulle förlora tusentals arbetstillfällen. En del av det man utvecklar är dock väldigt militärspecifikt, och är svårt att överföra till den civila industrin. Stridsflygplan är inget bra exempel på dual-use.

Efter att Saab presenterat en paketlösning som kunde växla mellan jakt, attack och spaning bildades 1980 industrigruppen JAS, som utöver Saab bestod av Volvo flygmotor, LM Ericsson och Svenska Radio AB.

I början av 2000-talet lanserades Saab JAS 39 Gripen, den senaste och mest avancerade iterationen av svenska stridsflygplan.

Sydafrika blev den första utländska köparen av Gripen och affären inkluderade omfattande motköpsåtgärder för att främja sydafrikansk industriell utveckling. Liknande avtal gjordes också med Brasilien när de köpte Gripen för att modernisera sitt flygvapen. Det kan finnas säkerhetspolitiska risker då ett av Sveriges viktigaste vapen har levererats till länder som nu närmar sig Kina och Ryssland.

Då Schweiziska folket 2014 röstade nej till att köpa 22 Gripenplan stod Sverige utanför Nato. Medfinansieringen om 23 miljarder uteblev, men då Sverige är ett stort land till ytan så beslöts det att JAS var viktigt. Nato har dock utfört löpande utvärderingar av Sveriges försvarsförmåga inom ramen för ”Planning and Review Process”, innehållet i dessa är dock sekretessbelagda.

När det kommer till konflikten i Ukraina har flyg inte spelat en avgörande roll på samma sätt som markstriderna. Luftstridskrafterna har främst använts för underrättelse, övervakning och att stödja marktrupperna snarare än att dominera luftrummet.

Med Sveriges inträde i NATO så kan det vara problematiskt när så många andra länder valt F16 som är en av mest producerade stridsflygplanen i modern tid (ca 5000 plan). Motsvarande siffra för JAS är knappt 300, och för Eurofighter ca 600. En stor kostnad för detta vapensystem är reservdelsförsörjning samt utbildning av piloter.

Det svenska flygvapnet har endast fem baser, vilket gör att dem sårbara. Ryssland ändrade sin strategi för ammunitionslager efter att ha blivit beskjutna av det moderna vapensystem.

Inom ramen för NATO så kommer 21 medlemsländer gemensamt bygga ”European Sky Shield Initiative” inspirerat av den Iron Dome som skyddar Israel mot fientliga missilier och drönare. I detta projekt så kommer drönare vara mycket centralt för att skydda EU:s gräns från Norge till Polen. Olika typer av drönare kommer tillsamms bilda en så kallad ”Drone wall”.

Krigsviktiga komponenter

Kullager

Under 1930-talet hade SKF 70 % av världsexporten av kul- och rullager. Eftar att Tyskland minerat havet utanför Skagerack så dominerades exporten till Tyskland där rullningslager var en krigsviktig insatsvara. Samtidigt begränsades exporten kraftigt till USA och Storbritannien.

När de allierade ville ha insyn i bolagets affärer ansåg Utrikesdepartementet som då ansvarade för exporten av SKF:s produkter det nödvändigt att redovisa en betydande sänkning av exporten till axelmakterna. Till de tyska sändebuden kunde dock UD visa att minskningen var marginell.

Generatorer

1915 levererade dåvarade ASEA, sex av världens största genereratorer till tungvattenanläggningen i norska Rjukan, under kriget uppstod problem med dessa. Då anläggningen ingick i det tyska kärnvapenprojektet beslöt ledningen för ASEA att bara vidta provisoriska åtgärder, inte åtgärda de grundläggande problemen.

Stegmotorer

Nedläggningen av Huskvarna-fabriken en direkt och märkbar påverkan på försvarsindustrins förmåga att tillverka och erhålla viktiga komponenter, såsom drivkretsar för stegmotorer. Detta understryker beroendet mellan den civila och militära sektorn när det gäller tillverkning och försörjningskedjor, samt behovet av att hantera sådana händelser med försiktighet och att ha strategier för att hantera eventuella försörjningsavbrott.

IR-kameror

Under 1960-talet började AGA utveckla den första kommersiella värmekameran. Deras innovation tillät användare att se och mäta temperaturer på avstånd med hjälp av infraröd teknik. Denna teknik revolutionerade inspektion och underhåll inom industrier som petrokemi, elproduktion och byggbranschen.

Under tiden spreds användningen av värmekameror till olika applikationer och marknader över hela världen. Ett amerikanskt företag, FLIR Systems (ursprungligen grundat som Systems Corporation of America 1978), var en av de ledande aktörerna inom detta område. FLIR förvärvade teknik, patent och expertis från AGA.

Idag används värmekameror för en mängd olika ändamål, från att detektera energiläckage i byggnader till att övervaka industriella processer och till och med för räddningsinsatser och militära ändamål. AGA:s och FLIR:s bidrag till utvecklingen av denna teknik har varit avgörande för dess framgång och popularitet.
Inom militären används IR-kameror, eller värmekameror, för en mängd olika ändamål på grund av deras förmåga att upptäcka och visualisera värmesignaturer. Här är några sätt IR-kameror används militärt:

Övervakning och spaning: Militära enheter använder IR-kameror för att övervaka och spana över områden, särskilt under nattförhållanden eller när siktet är begränsat på grund av dimma, rök eller andra hinder. Genom att upptäcka värme från fordon, människor eller andra föremål kan militären skapa en bild av situationen på marken.

Måligenkänning: IR-kameror möjliggör måligenkänning genom att detektera och skilja mellan olika värmesignaturer. Detta är användbart för att skilja mellan vänliga och fiendens styrkor samt för att identifiera specifika mål för riktade attacker.

Underrättelse, spaning och övervakning (ISR)**:** IR-kameror används ofta som en del av underrättelse-, spanings- och övervakningsplattformar, inklusive drönare, flygplan och satelliter. Dessa kameror kan skanna stora områden och snabbt upptäcka aktivitet eller förflyttningar som är av intresse för militären.

Målriktning för vapensystem**:** IR-kameror kan integreras med vapensystem för att hjälpa till med målriktningen. Detta kan inkludera luftvärnsmissiler, attackhelikoptrar och andra vapenplattformar som behöver noggrann riktning för att träffa sina mål.

Nattoperationer: Eftersom IR-kameror kan fungera i mörker, ger de militära enheter möjlighet att genomföra nattoperationer med ökad effektivitet och säkerhet. Detta är särskilt viktigt för specialstyrkor och andra enheter som kan behöva operera i fiendeligt territorium under täckning av mörker.

Flygmotorer

I början av 1930 bildades Nohab Flygmotorfabriker, övergick till att heta Volvo Aero för att sedan säljas till den brittiska industrikoncernen GKN 2012.

Volvo Aero försåg sedan starten försvaret med motorer. Det sista exemplet var motorn till det svenska stridsflygplanet Gripen. Det tekniska kunnandet som erhållits från utvecklingen av militära flygmotorer kunde användas i uppbyggandet av expansiva civila flygprojekt. Åren 2000-2010 hade Volvo Aero en genomsnittlig tillväxt på den civila verksamheten med 9% om året. Bolaget är även verksamt inom gasturbiner.

Finansiering

Det är svårt att kartlägga finansieringen av cybersäkerhet ur ett dual-use perspektiv.

Försvaret

Det finns ett ändringsbeslut (Fö2024/00616) till försvarets regleringsbrev där ett antal arbetspaket indikerar vilka prioteringar som görs. Cybersäkerhet förekommer i flera sammahang och med olika belopp. Under rubriken ”Försvar och samhällets krisberedskap” så avsätts 625 tkr till tillsyn av cybersäkerhetscertifiering samt 465 tkr till evaluering och certifiering av IT-säkerhetsprodukter. Direkta utgifter för materialanskaffning omfattar som jämförelse 140 950 tkr.

Civilsamhället

Cybernoden

Eftersom Saab är medlem och även presenterade sina lärdomar av ett Vinnova finansierat projekt så faller det inom kategorin. Cybernoden har sedean starten 2020 erhållit 14.5 MSEK sedan starten, vilket innebär en årlig budget på ca 3 MSEK. För att uppnå målen förutsätts att medlemmarna bildar virtuella konsortier i syfte att söka medel från EU.

Cybercampus

Detta initiativ drivs av KTH och Försvaret i gemenskap, med ungefär samma inriktning som cybernoden. Budget är för 2024 24 miljoner , men kommer ökas till 40 följande år.

Centrum för cyberförsvar och informationssäkerhet

Centret ska förutom utbilda cybersoldater, även bedriva forskning inom området såsom kryptereringsalgoritmer som klarar hot för kvantdatorer.

Budgeten är 47 miljoner, där försvaret står för 42 miljoner.

Nationellt cybersäkerhetscenter

En nationell plattform för samverkan och informationsutbyte med privata och offentliga aktörer inom cybersäkerhetsområdet.

Budget för 2024 är 120 miljoner där medel avsätts från FRA, Försvarmakten, Säkerhetspolisen samt MSB.

Extra finansiering

Vid en pressträff den 11:e April 2024 så meddelande regeringen att 60 miljoner kommer avsättas till cybersäkerhet, varav 20 av dessa allokeras till MSB.

Kommentarer

Vid CDIS-konferensen 22 April 2024 så redogjorde Lidingö Stad sina kostnader för den IT-attack de utsattes för. Direkta kostnader i samband med incidenten uppskattades till cirka 1 MSEK, främst i form av övertid för egen personal. För att undvika liknade incidenter stärktes skyddet, men till en kostnad av 1 MSEK / år. Denna incident drabbade dock endast IT-system. I presentationen så nämndes den högkritiska sektorn vatten och avlopp som var helt isolerad från internet. Då vattenförsörjningen är beroende av el, och denna i sin tur av internet anslutna stödtjänster så är det rimligt att att anta att Lidingö stad måste budgetera för att stärka cybersäkerhet så att inte el och därmed vatten slås ut vid nästa attack.

Kostnaden för att integrera Sveriges energisystem med internet borde karläggas och matchas mot det stöd som erbjuds inom ramen för de ovan nämnda cybercentrum som etablerats.

Geopolitik och leveranskedjor

Sverige köper vindkraftverk från Kina för att kompensera bortfallet från sin kärnkraft. De civila leveranskedjorna som EU skapat mappar mycket dåligt med de militära alianserna.

Ryssland får mycket hjälp med att utveckla vapensystem från Kina och Iran. Ukaina stöds militärt mestadels av NATO.

BRICS är handelsorganisation som fått sitt namn efter Brasilien, Ryssland, Indien, Kina samt Sydafrika Nyligen så inkluderades även Iran.

I den moderna globaliserade världen är det allt svårare att dra en klar gräns mellan det civila och militära när det gäller leveranskedjor och försäljning av komplexa försvarssystem. Under det kalla kriget var det tydligt vilka länder som var de huvudsakliga kontrahenterna, men idag kan formandet av den strategiska miljön ske med en mängd olika metoder och verktyg, ofta i samband med globaliseringen, digitaliseringen och utvecklingen av informationsteknologin.

Kraven på spårbarhet i leveranskedjorna kommer sannolikt att skärpas när produkter från civila sektorn också kan användas för militära ändamål. Vinnova har genom sina olika program redan finansierat projekt inom försvarsindustrin som syftar till att öka spårbarheten och säkerheten i leveranskedjor. Detta öppnar också upp möjligheter att dela resultat och innovationer med den civila sektorn, vilket kan gynna båda sidor.

Kina och EU skiljer sig åt i sina strategier när det kommer till att dominera områden som kommunikation och drönare. Kinas strategi präglas ofta av mycket långsiktiga planer och en vilja att uppnå dominans inom dessa områden genom olika metoder, inklusive ekonomiska subventioner.

Uppdraget från EU att låta medlemsländerna själva utforma NIS2 (Network and Information Security) skulle förmodligen ha sett annorlunda ut om man då hade haft insikter om hur dual-use-teknologi påverkade krigsföringen i Ukraina. Genom att integrera dual-use-aspekter i betänkandet underlättas även finansieringen av projekt, vilket möjliggör att produkter och tjänster utformas med dual-use i åtanke från början.

Regulatoriska sandlådor

Svenska myndigheter inom civila sektorer lyder enligt grundlagen under offentlighetsprincipen, där inkomna handlingar blir offentliga som huvudregel, det finns dock undantag. Försvaret och andra myndigheter tillhör dock en sektor som tillämpar sekretess.

Enligt Försvarsmakten ska kostnaderna för en angripare bli mycket höga. Vilka kostnader specificeras dock inte, men nyttjanden av civila produkter vid angrepp respektive försvar påverkar kalkylen. Vid försvar så har Ukraina nyttjat både civila och militära produkter och system. Den sex mil långa ryska militär kolonnen på väg till Kiev stoppades av endast ett trettiotal soldater utrustade med fyrhjulingar och drönare. Attacken mot Israel inkluderade civila produkter, dock i så stor omfattning att det militära försvaret överbelastades.

Med stora resurser så kommer kriget bli utdraget, då tenderar strategin att handla om utmattning. Här är det en klar fördel om civila produkter kan användas då dessa är mycket billigare. Rysslands försvarsminister är numera en ekonom.

Utmattning och överbelastning är exempel på taktiker där civil teknologi kan stödja försvaret.

Strategiska komponenter i dual-use

Det finns mycket stora synergier mellan civila och militära drönare. Både vad det gäller produkter och hur dessa nyttjas. Den civila marknaden domineras av kinesiska DJI som har 70 procent av världsmarknaden, vilket resulterat att många svenska myndigheter valt DJI som leverantörer. EU: s “Drone strategy 2.0” formulerades innan Ukraina kriget och har stora ambitioner men saknar de resurser Kina har.

Kinas önskan att bli en teknologisk supermakt i den så kallade fjärde industriella revolutionen som just nu pågår. Den rör utvecklingen av artificiell intelligens, robotteknik och "sakernas internet". Om den digitala satsningen faller väl ut kommer Kinas internationella prestige att växa avsevärt samtidigt som ekonomin och den politiska och militära kapaciteten stärks.

Sedan 2015 intensifierades planerna att ställa om Kinas tillverkningsindustri till mer avancerad, högteknologisk produktion.

I USA använder man drönare inom jordbruket, då dessa är försedda med kamera och positioneringen bedömdes risken att Kina kunde kartlägga de silos där långdistansmissiler placerats.

Vissa aktörer i Sverige använder likt Ukraina öppen teknologi för att bygga drönare. Ett samarbete med Ukraina hade sannolikt gagnat båda länder, inte minst inom leveranskedjor.

Europeiska unionens råd beslutade 2023 om nya regler för att främja gemensam upphandling inom EU:s försvarsindustri

Entreprenörer och underleverantörer måste vara etablerade och ha sina strukturer för verkställande ledning i EU eller ett associerat land och får inte kontrolleras av ett icke-associerat tredjeland. 65 % av slutprodukternas komponenter måste ha sitt ursprung i EU eller ett associerat land. Detta kan vara problematiskt när det kommer till strategiska komponenter för autonoma system.

Under 1990-talet var cirka 11 000 företag i Sverige registrerade som krigsviktiga-företag, varav 250 krävde statsfinansiering för att säkerställa en godtagbar leveranssäkerhet och tillgänglighet av de aktuella produkterna eller tjänsterna i kris eller i krig. Försvarsberedningen bedömer därför att ett återupprättat system med k-företag är nödvändigt för ett trovärdigt totalförsvar.

För att Sverige skall kunna bygga egna drönare är vi idagsläget mycket beroende av teknologi från Kina, antingen saknar vi råvaror eller kunskap.

Motorer för autonoma system

Tillgång till jordartsmetaller är en förutsättning för att erbjuda de högs specialiserade motorer som ingår i drönare. 2010 fick världen ett smakprov på riskerna, när Japan bordade en kinesisk fiskebåt och tillfångatog kaptenen. Snart minskade den kinesiska exporten av metaller till den japanska elektronikindustrin. Förutom de geopolitiska aspekterna så dominerar Kina marknaden för denna typ av motorer, där en enskild aktör innehar över 200 patent. Sverige har nyligen hittat stora förekomster av viktiga metaller, men saknar kompetens och patenten för att förädla dessa tillgångar.

Energikällor för autonoma system

De rapporter som beskriver marknaden och dess aktörer är låsta bakom betalväggar, och ligger utanför ramen för ett remissvar. En snabb överblick över vad som erbjuds på den svenska marknaden indikerar dominans från Kina.

Batterier som tas fram i norra Sverige av aktörer som Northvolt har en produktion främst riktad mot energilager samt person och lastbilar.

Här föreslår vi att europeisk näringsgrensstandard indikerar strategiska (krigsviktiga) komponenter lämpade för multipla användningsområden.

Mjukvara för autonoma system

Ett modernt operativsystem består av tiotals miljoner rader komplex källkod, tillsammans med olika verktyg och bibliotek. Öppen källkod integreras i de flesta kommersiella system och konsumeras oftast genom aggregering. Det svenska projektet curl har under 25 år spridits till miljarder enheter. Tack vare den omfattande spridningen och donationer kan högkvalitativ programvara erbjudas gratis. En ny utgåva släpps varannan månad, där både felkorrigeringar och ny funktionalitet distribueras. Vissa fel kan påverka säkerheten och kallas enligt betänkandet för sårbarheter, vilka nämns 175 gånger i texten. Sårbarheter ska enligt direktivet övervakas och analyseras. En utmaning med analysen är att den kräver djupgående domänkunskap, och denna kunskap är knuten till de tusentals projekt som skiljer sig åt när det gäller val av utvecklingsprocesser och stödsystem. Förslaget innebär en form av inventarieförteckning över de mjukvaror som ska övervakas, vilket nu benämns som Software-bill-of-material. Då EU:s strategi för cybersäkerhet spänner över många dokument som är bristfälligt koordinerade så publicerades nyligen ett nytt dokument, Cyber Resilience Act Requirements Standards Mapping, som beskriver relationen dessa. Även detta har brister då NIS2 inte nämns, en positiv observation är att det tidigare vaga begreppet "products with digital elements" nu kan mappas mot en amerikansk industristandard "Cyclone/DX".

Här föreslår vi att förslaget bör utformas så att sårbarheter bättre kan knytas till en inventarieförteckning av mjukvarukomponenter.

Strategisk

Funktionalitet som är central måste identifieras, det är även viktigt att det går att underhålla mjukvaran under dess livstid. I denna remiss så har autonoma system valts som exempel för att konkretisera dual use.

Inom den civila marknaden så används antingen leverantörsspecifik eller öppen mjukvara. Då senare har stor spridning inom segmentet av de som bygger egna drönare för hobbybruk. Det går för övrigt att beställa kompletta system helt baserad på öppen teknologi. Tyvärr så medför spridningen att den används både vid attacken av Israel den 7:e september samt vid försvaret av Ukraina i den två år långa konflikten.

Det krävs dock kunskap för att kalibrera algoritmerna för varje kombination av propeller, motor samt ram. Det är snarare denna kunskap som är strategisk, då projektet är tillgängligt för i princip vem som helst att använda.

Kritisk

Programvara avsedd för kryptering möjliggör användning av publika nätverk och extern lagringsmedia. I händelse av en sårbarenhet så kan läckage av personliga data uppstå, vidare kan det uppstå skada och driftstopp. Efter en större incident 2014 (https://en.wikipedia.org/wiki/Heartbleed) där en enskild utvecklare ansvarade för nästan all krypterad internettrafik. Idag sörjer organisationen OpenSSF för att förebygga liknande incidenter inträffar. Det var initialt en del diskussioner runt oviljan att finansiera detta projekt.

*Seeing the time taken to catch this simple error in a simple feature from a "**critical**" dependency, Kaminsky fears numerous future vulnerabilities if nothing is done. When Heartbleed was discovered, OpenSSL was maintained by a handful of volunteers, only one of whom worked full time*

Stödjande

Enligt den mest rigorösa säkerhetsstandarden "Common Criteria" definieras stödjande funktionalitet på de funktioner och mekanismer som en IT-produkt har för att underlätta säkerhetsfunktioner och uppfylla specifika säkerhetskrav.

Nyligen upptäckte en ensam utvecklare att en så kallad bakdörr avsiktligt hade planterats i ett projekt som stödjer ett annat kritiskt projekt för fjärråtkomst. Personerna bakom detta projekt har troligtvis lagt ned år på det, och det var mycket nära att den skadliga koden installerades på miljontals datorer i produktion.

Detta är mycket allvarligt, då denna kategori av mjukvara varken är strategisk eller kritisk. De projekt som driver utvecklingen är förmodligen underfinansierade, vilket underlättar för en eller flera illasinnade utvecklare kan bygga upp förtroende för att senare plantera in en skadlig kod.

Här föreslår vi att förslaget bör utformas så att beroenden till stödjande programvaror inkluderas i den analys som CSIRT förväntas göra

Strategiska kompetenser

Den öppna programvara som är fritt tillgänglig kräver kompetens för att kunna anpassa för militära syften.

Kalmanfilter

Det finns två typer av styrningar, dels för att stabilisera drönaren, dels den styrning som är kopplad till själva uppdraget. Uppdraget kan bestå i att följa ett fördefinierat mönster i syfte att besprutning av åker/skog. Stabilisering handlar om mycket korta återkopplingar som även driver drönar i rätt riktning och höjd.

Signalbehandling av videoströmmar

Det är mycket sannolikt att positioneringskällan slås ut, då måste alternativ positionering aktiveras. Genom att drönaren har terrängkartor och olika typer av kameror kan uppdraget genomföras utan stöd från rymdens satelliter.

Systemarkitektur

Civila drönare är billiga och kan användas i kluster i syfte att överbelasta dyrbara motmedel. Infrastruktur för laddning av batterier, hämta last mm kan integreras med andra system. Det krävs även kunskap om de protokoll som används inom NATO för att integrera civila dröna i militära system. Cybersäkerhet är en integrerad del av en systemarkitektur.

Artificiell intelligens

USA har mycket AI men ingen reglering, för EU gäller det omvända. Ur ett dual-use perspektiv kan det vara svårt att definiera var gränsen går mellan linjär algebra och AI. Israel beskylls för att nyttja ”AI-systemet” Lavender i kriget mot Hamas, vilket förnekas av Israels försvarsmakt vilka å sin sida hävdar att det endast är en traditionell databas. Det som driver AI-teknologin är de mycket kraftiga grafik acceleratorna som bäddat för språkmodeller samt generativ AI. De stora aktörerna erbjuder dock likartade tjänster såsom Bart och Chat-GPT som gratis. Energiförbrukningen globalt beräknas uppgå årligen till minst 100 Terawatt timmar. Då EU lider av energifattigdom så kommer detta kombinerat med regleringar hämma utvecklingen. En sökning på Lavender gav nedanstående svar, vilket ger en indikation på hur globaliseringen nu upphör.

451: Unavailable due to legal reasons

We recognize you are attempting to access this website from a country belonging to the European Economic Area (EEA) including the EU which enforces the General Data Protection Regulation (GDPR) and therefore access cannot be granted at this time. For any issues, contact bookkeeping@mcduffieprogress.com or call 706-595-1601.

Det finns dock en separat reglering inom EU för AI, så detta ligger utanför NIS2-betänkandet.

Utbildning av drönarpiloter

I en störd radiomiljö kan fiberoptik nyttjas så att en drönare styras på avstånd. Kombinationen av AI och en människa kommer under en överskådlig tid vara bättre än fullständigt autonoma system. Människans förmåga att anpassa sig, kan vara avgörande i en oförutsedd situation. Med drönare som kan styras på distans så riskeras inte människor.

Här föreslår vi att strategiska kunskaper identifieras, och att det integreras i befintliga utbildningar.

Strategiska resurser

Test av autonoma system

Drönarcentrum i Västervik skapades för att främja en regulatorisk sandlåda, Mycket arbete är nedlagt, inte minst av lokala entreprenörer. Det erbjuds möjlighet för kunder att testa autonoma system i en miljö som inkluderar vatten, skog samt öppet landskap. Tyvärr saknas långsiktig finansiering för att driva centret.

Datacenter

ICE Datacenter i Luleå har en stor potential att stödja digitalisering. Idag är det relativt få personer som nyttjar anläggningen jämfört med vad som utlovades 2016. Delar av detta center borde kunna allokeras till att utveckla molnbaserade stödtjänster för drönare. Denna resurs borde även kunna stödja utbildning, där många aktörer framför allt inom yrkeshögskolorna av kostnadsskäl tvingas använda amerikanska molntjänster. De statliga innovationsnoder som etablerats borde kunna erbjuda mindre företag resurser, på samma sätt som amerikanska erbjuder gratis datorkraft både för studenter och nystartade bolag. Articifiell intelligens är mycket energikrävande, då de flesta använder en och samma teknologi så kan en avgörande faktor vara tillgången till billig elektricitet.

Energi

Sverige hade under tjugo år tillgång till billig och planerbar energi. Den radiella distributionen med synkrona genereratorer från vatten och kärnkraft skapade hög tillgänglighet. I samband med övergång från planerbar till icke planerbara energi källor uppstår ett behov av att långt ut i elnätet kunna styra, producera samt lagra energi. Då Sveriges stämnät står i förbindelse med närliggande länder så byggs det upp ett internationellt system där elektroniska kontrakt styr internetansluten kundplacerad utrustning.

Erfarenheter från EU-projektet Interflex som bland annat drivs i södra Sverige visar att det är mycket stora utmaningar med stadsnät i så kallad ö-drift. Förutom otillräcklig kapacitet för lagring, så uppstår det även andra tekniska utmaningar, såsom cyberhot. Ur ett prestandaperspektiv så bör batterier placeras inomhus, men sett ur brandperspektiv så bör det placeras utanför fastigheten. Liknande problem finns även med solpaneler. RISE har i sin rapport ”Innovativa elsystem i byggnader – konsekvenser för brandsäkerhet från 2019” belyst problematiken.

Det äldre stabila energisystemet som Sverige nu lämnar var enklare och kunde fungera utan internet. Med det energisystem som nu är under storskalig uppbyggnad kommer det krävas flera tillsynsmyndigheter enligt betänkandet. Andra kritiska sektorer såsom dricksvatten beror av pumpar vilka i sin tur drivs av el. På så sätt skapas komplexa beroenden. Det biologiska virus som drabbade Brasilien kom från myggor som lade ägg i öppna kärl. Dessa kärl var nödvändiga för att lagra dricksvatten då pumparna slutade fungera. Den kundplacerade infrastruktur som krävs för de nya stödtjänsterna är hårt prispressad och kommer i många fall från Kina. Förutom stödtjänster så är det mycket vanligt att moderna värmepumpar och laddboxar levereras med en molntjänst vilken kan styras från en mobiltelefon. Erfarenheterna från Holland visar att cyberangrepp är vanliga för denna typ av

tjänst. Sett ut ett dual-use perspektiv och artikel 5 ur Natofördraget så är Sverige skyldiga att skydda högkritisk infrastruktur. Då dessa system är komplexa så träder även andra regleringar in såsom EU:s Cybersecerity Resilience Act (CRA).

Förutom el så krävs det även stabil fjärrvärme för uppvärming.

EU har nyligen identifierat geotermisk energi som ett intressant komplement till övriga energikällor. Utvecklingen leds av USA som i sina öknar testar olika teknologier, däribland mikrovågor med mycket hög energi för att penetrera kristallina bergarter.

Värme från jordens inre har en potential att förse mänskligheten med fossilfri värme och el under överskådlig tid. På så sätt skulle energisystemet i Sverige kunna återgå till en enkel och radiell modell. Med Carbon Capture and Storage (CCS) så kan syntetiskt bränsle erbjudas på befintliga bensinstationer utan att nettoutsläppen ökar. Då energidensiteten är cirka femtio gånger högre i flytande bränsle än i batterier så minskar behovet av att stärka det lokala elnätet.

Genom att bygga ett elnät som är enkelt och stabilt krävs ingen styrning över internet avseende stödtjänster. Kostnaden för att implementera stödtjänster, samt underhåll av en komplicerad infrastruktur kommer både bli dyrt och sårbart. Ett från internet isolerat elnät kommer även stärka motståndskraften i andra sektorer som är beroende av energiförsörjning.

Här föreslår vi att berörda myndigheter samarbetar och stödjer privata initiativa för att bygga upp kunskap runt geotermi.

Riskanalys

Ett centralt moment in betänkandet är riskanalys, i princip handlar det om att identifiera **vad som skall skyddas**, **vilka är hote**n och därefter upprätta en **åtgärdsplan**. Med utgångspunkt på Sveriges befintliga försvar och erfarenheterna från Ukrania så kommer överbelastning och ekonomisk utmattning appliceras, vilket är vanligt förekommande taktiker inom cyberkrigföring.

Texten nedan är publicerad från försvarsmaktens hemsida.

Kriget i Ukraina har aktualiserat behovet av snabb teknik- och taktikanpassning mot fienden. Dessutom är utvecklingen av kommersiella produkter ledande inom flera segment.

Om vi vill uppnå ett högt tempo i förmågebyggandet med nya teknologier, krävs ett pragmatiskt och integrerat myndighetssamarbete, men också tillsammans med industrin samt universitet och högskolor.

Det finns stora likheter mellan överbelastningsattacker i cyberrymden och för land och luft. Nedanstående text från en sökning på Internet efter attacken från Iran mot Israel.

"Meaning that you have an array of different aerial munitions — cruise missiles, ballistic missiles, drones — and they're all launched either in waves or in such a way that the timing overwhelms air defense."

För att kunna jämföra militär och civil teknologi ur ett överbelastning / utmattningsperspektiv så måste ekonomi appliceras.

Vad skall skyddas

Inom det militära är det viktigt att över tid försvara ett geografisk avgränsat område. Genom att dominera luftrummet så kan man uppnå detta. Sverige har därför en flotta om cirka 200 stridsflygplan, som uppskattat var och en kostar cirka 500 miljoner. Samtliga flygplan representerar då ett värde av 100 miljader.

Vad skall vi skydda oss mot

Iran har försett Ryssland med drönare vilka drivs med jetmotor, de kan fyras av från en modifierad fraktcontainer vilken rymmer fem jetdrönare. Containern monteras sedan på en lastbil som har förmåga att tippa flaket. Genom att i fredstid förbereda en attack så undgås de varningssystem som normalt detekterar något som närmas sig vår yttre gräns. Jetmotorn ger drönaren en mycket hög hastighet, vilket är utmanande för ett artellerisystem. Det kommer krävas någon form av missil för att slå ut en inkommande drönare. Ett rimligt antagande är att angriparen kommer nyttja tio drönare för varje mål. Det skulle då räcka med 400 lastbilar med varsin container som var och en bär fem drönare. Om angreppet sker innan krigsförklaring så förmodas det att drönarna kan nyttja sattelit för navigering. Om så inte är fallet så måste drönaren ha kameror som läser av terrängen för att hitta målet.

Det finns många tunga lastbilar i Sverige. En angripare kan sannolikt genom stöld komma i besittning av några. Någon anpassningen kommer inte krävas då den militära lasten är i form av en fraktcontainer. Vi antar att fem containers med fjärrkontroll placeras ut av en och samma person. Det skulle då räcka med 80 personer. Samma personer kan även förbereda attacken genom att montera drönare som smugglats in i landet under varuklasser som i dagsläget inte är krigsviktiga.

Erfarenheterna från sexdagars kriget visar att stridsflygplan är mycket sårbara då de inte är i luften. Israel inledde med en förebyggande attack och drog stor fördel av överraskningsmomentet.

En budget för denna typ av attack handlar om att åttio personer integreras i samhället, antag att det kostar 500.000 / år och person för den angripande parten under fem år. Kostnaden för personal uppgår då till 200 miljoner. Till detta kommer material i form drönare , containers och lastbilar vilket vi antar kostar 400 miljoner. Totalkostnaden skulle då uppgå till 600 miljoner.

Hur skall vi skydda oss

Förenta Nationerna (FN) följer en modell där varje nation representeras, vilket rimmar illa dagens konflikter som handlar om inbördeskrig, terrorism och krig via ombud. Den vedergällning som Israel utförde efter Irans attack

avfyrades dessutom innifrån Iran, vilket innebär att alla som bor i Iran inte sympatiserar med regimen. Det antas att det går att hitta knappt hundra svenska medborgare som väljer att ansluta sig till en attack.

En viktigt komponent i anfallet är modifierade fraktcontainers. Då dessa ofta används som verktygsbodar, transport av dyrbara varor, förses de ofta med elektroniska spårtjänster. Den utrustning som monteras i containern kan utökas med nya funktioner såsom transponder där vägtullar och polisbilar elektroniskt kan samla in rörelsemönster i syfte att detektera avvikelser. Då tullen kontrollerar inkommande trafik så kan en transponder monteras på containern, och även plomberas för att knytas till denna.

I anslutning till skyddsobjekt så kan ballonger med kameror även kommunicera med transponders. Då Sverige består av mycket skog så kan de drönare som idag nyttjas inom skogsbruket för att sprida gödningsmedel förses med nya funktioner av typen övervakning, men även bära någon form av vapensystem i händelse av en attack.

I direkt anslutning till skyddsobjektet så krävs det ett mycket snabbt system för att slå ut en inkommande drönare. Med inträdet i Nato så antas Sverige få tillgång till kraftfulla laserkanoner, vilka har en effekt om ca 100 kilowatt. För att slå ut en drönare så måste lasern belysa målet under ett antal sekunder för att åstadkomma den hetta som krävs för att slå ut drönaren.

Kostnaden för skyddet kan i vissa delas med civila tillämpningar. Ballonger för övervakning kan förses med IR-kamera och detektera skogsbrand, drönare avsedda för att sprida näring kan då bekämpa bränder i ett tidigt skede. Samma drönare kan även förses med vapensystem för att eliminera en container innan dess innehåll avfyrats.

Spårsändare för containers används redan idag, dessa kan i samråd med leverantörerna modifieras så att de ingår i totalförsvaret. Det kan även finnas intresse från tull och polis för att få bättre kontroll hur kriminella använder containers för smuggling av narkotika samt stöldgods.

Laserkanorer är dyra att köpa in, men väl på plats så är kostnaden endast tre dollar för att eliminera ett mål.

Åtgärdsplan

Det ovan beskrivna hotet bygger på en enkel strategi, genomförd med ombyggda kommersiella komponenter. Den stora utmaningen ligger i ansvarsfördelningen mellan Sveriges drygt 400 myndigheter. Kanske krävs det en prototyp där hotet realiseras utan förluster i form av material och människoliv.

Syftet med prototypen är att bygga upp kunskap om hotbilden avseende hastighet för drönare, tid för drönare att nå målet mm, data samlas in för att sedan användas för modellering.

Modellerna kan sedan ligga till grund för att appliceras i andra sammanhang, t.ex skydd av kärnkraftverk.

Andra hot mot flygvapnet

Transportstyrelsen

2017 så läckte transportstyrelsen uppgifter om alla svenskar som har flygcertifikat och deras hemadresser. Läckaget var en konsekvens att att utlokalisera driften av registret i syfta att spara pengar. Samtliga svenska stridspiloter, som

har ett civilt flygcertifikat, finns med i läckan. Det framgår av Säpos förundersökning. I förundersökningen framkommer det också att chefer på Transportstyrelsen beordrade personalen att godkänna tekniker från Tjeckien som inte hade genomgått någon svensk säkerhetskontroll och som det inte ens fanns något födelsedatum på.

Luftvärn

Mål i luften

Under de senaste årtiondena har utvecklingen inom luftvärnsystem gjort stora framsteg, vilket har utmanat traditionella strategier som starkt fokuserat på stridsflygplan som kärnan i luftkampen. Med avancerade luftvärnssystem som är både effektiva och kostnadseffektiva har stridsflygplanens roll gradvis förändrats och deras betydelse minskat av flera skäl.

Moderna luftvärnssystem kan arbeta med avancerade sensorer och datoriserade algoritmer för att snabbt identifiera och bekämpa hot, vilket minskar behovet av ständig bemanning och ökar deras reaktionsförmåga.

På hög höjd så är flyget utsatt för missiler, på låg höjd så utgörs faran av handburna vapensystem.

För kortare avstånd så kan en kraftig laser låsa på ett flygplan och alstra mycket hetta så att detta skadas.

Mål på marken

Det finns olika typer av missiler till moderna luftvärnssystem. Mindre bomber kan avfyras med en raket vilken kan nå mål på marken mycket långt bort.

Slutsats

Dynamit är ett mycket bra exempel på ”dual-use”, då det kan användas både för att spränga tunnlar för kollektivtrafik, men även ingå i vapensystem. Kombinerat med stål så kunde Sverige försörja de allierade med kanorer. Samma svenska stål ingick även i kullager som såldes till båda sidor i kriget. Kunskapen och leveranskedjorna var då nationella. De kluster som byggdes runt tekniken skapade grunden till industrialiseringen i Sverige.

Lagen handlar om säkerhet i cyberrymden, vilket är en gråzon mellan krig och fred. I denna gråzon så skall både civila och militära organisationer ansluta maskiner och människor.

En del av det vi importerar kan modifieras och då nyttjas i primitiva vapensystem. Då dessa primitiva system brukas i stor omfattning så liknar det en överbelastningsattackar där vinnaren är den som kommer undan till lägsta pris. Detta svar innehåller ett scenario där assymetrisk krigföring ger en angriparen en fördel.

NIS2 lagen speglar EU:s oförmåga att befatta sig med försvarssektorn. Cyberrymden är en mycket problematisk domän eftersom komplexa leveranskedjor för mjukvara inkluderas. En cyberattack kan räknas som en krigshandling och utlösa artikel 5 i Natos regelverk.

Bristen på billig och planerbar energi, driver utvecklingen av energieffektivisering, vilket i sin tur kräver styrning av elnätet.

De resurser som skall styras såsom laddstolpar är ofta integrerade med molntjänster för laddning då elen är billig. Dessa molntjänster utgör attackytor vilket kan slå ut energisystem på grund av högt och plötsligt effektbehov.

Den finansiering som nu riktar sig mot dual-use är inte i samklang med den exkludering av försvarssektorn som betänkandet innehåller.

Källor och referenser

Detta remissvar syftar till att lyfta frågan om de utmaningar som uppstår då två idag isolerade sektorer skall verka i enlighet med försvarsministerns ambitioner om att innovation inom försvaret skall bidra till tillväxt inom det civila.

Remissvaret speglar författarens erfarenheter från utbildning och innovation inom cybersäkerhet.

Önskas det fullständiga underlaget med externa källor så kontakta författaren.

hans@lammda.se