SOFF
Säkerhets- och försvarsföretagen

# Cyberförsvarsforskning

## ”Vilka teknikutvecklingsområden bör vara prioriterade för att nå en hög teknikmognadsgrad i Sverige?”

En rapport om efterfrågan samt det offentliga utbudet av forskning- och teknikutvecklingsprojekt och program på nationell, EU och Nato-nivå.

**Forskning är avgörande för internationell framgång och konkurrenskraft**

**Sverige** är idag en av de mest innovativa länderna i världen, men trots det halkar vi efter i cybersäkerhet[1]. Gapet mellan innovation och säkerhet medför samtidigt stora säkerhetspolitiska risker.

För att skydda Försvarsmaktens system, samhällets funktioner och näringslivet krävs därför ett effektivt och ändamålsenligt cyberförsvar samt en fungerande cybersäkerhet som utvecklas i linje med behov och den digitala transformationen av samhället. Ny teknik behöver därför integreras och kompetens attraheras för att Sverige ska kunna fylla gapet mellan digitalisering och cybersäkerhet och samtidigt inte falla efter i den digitala utvecklingen där användaren är säker.

**Säkerhets- och försvarsföretagen (SOFF)** ser ett behov av forsknings- och utvecklingsprogram där det offentliga och näringslivet delar på risker och kostnader och där vinster gynnar konkurrenskraft på kort sikt genom att öppna dörrar och stärka attraktiviteten. Långsiktigt är vetenskap och ny teknik i cyberområdet en viktig förutsättning för att bibehålla en långsiktigt internationell konkurrenskraft och ta del av internationella samarbeten.

För att nå en högre cyberförsvarsförmåga så är forskningen det första steget för att förstå hur teknologin kan utvecklas**.** SOFF menar att forskningsresultaten måste omsättas i tillämpningar och att tillämpningarna får avsättning på marknaden. När forskningsresultaten omsätts i tillämpningar och avsätts på marknaden så blir det lönsamt för företagen att investera mer i forskning och teknikutveckling.

Det bör understrykas att utvecklingssatsningar inte kan ersätta forskningssatsningar och omvänt kan ej forskningssatsningar kompensera för uteblivna utvecklingsuppdrag. Anledningen är för att Sverige ska ha tillgång till såväl spetskunskap som teknisk förmåga behövs då en balans mellan forskning och utveckling.

**Vår internationella framgång och konkurrenskraft** avgörs av den strategiska riktningen inom forskning och innovation**.** SOFF:s rapport om den europeiska försvarsfonden visar att Sverige är ett högteknologiskt land vars tillväxt och arbetstillfällen är beroende av

[1] Global Cybersecurity Index | Database for Institutional Comparisons in Economies. (n.d.). Hämtad 12 Juni 2021, från https://dice.ifo.de/en/node/317818

handel med andra länder, och den kompetens som finns hos våra företag och anställda. Mer än 1,2 miljoner människor i Sverige är sysselsatta inom produktion av exportberoende produkter samtidigt som svensk export står för nästan hälften av Sveriges samlade bruttonationalprodukt.

**Marknaden** styr den produkt som efterfrågas. Därför är det viktigt för företagen att fortsatt vara relevanta och redo att tillgodose de behoven som efterfrågas för stärkt internationell konkurrenskraft. I praktiken innebär detta att svenska företag redan har förvärvat den kunskapen eller produkt som efterfrågas av ett utländskt företag eller stat vid tillfället den efterfrågas. Det är då viktigt att det i ett tidigt stadie finns incitament att investera i FoU, för det är sedan avgörande för vilken position som Sverige kommer ha i framtiden.

Sedan, för att företagens egna investeringar ska öka krävs det att företagen får kvalitativ och kvantitativ information om de resonemang och tankar som finns hos kunderna. Utmaningen är att den typen av information oftast är känslig och, i staters perspektiv, kanske en fråga om nationell säkerhet. Däremot kan ett internationellt samarbete medföra en ökad tillgång till den kunskapen samt få tillgång till data och information som är avgörande för ökad konkurrenskraft. Även här spelar tidiga investeringar i FoU en viktig roll för svenskt deltagande i internationella forskningsprojekt.

**Behoven för teknik i området cyberförsvar och cybersäkerhet ökar i världen.** De internationella möjligheterna för företag är stora. SOFF menar att ett internationellt samarbete leder till tillgången av en större marknad som i sin tur ökar cyberförmågan i Sverige genom att aktörer delar kunskap. Den förvärvade kunskapen bidrar företag med samt blir en integrerad del i upprätthållandet av Försvarsmaktens operativa förmåga och försörjningstrygghet på såväl kort som lång sikt.

**Cyberområdet prioriteras alltmer på både statlig, EU och Nato-nivå.** Vi ser att cyber blir en alltmer integrerad domän i alla verksamheter och den accelererande digitaliseringen av samhällen ställer större krav på säkerhetskontroller. I tillägg kräver försvarsverksamheter alltmer sofistikerad teknik som kan försvara mot antagonistiska angrepp i cyberdomänen. SOFF har därför skapat en kartläggning av alla dessa initiativ för att hålla oss à jour med vilka initiativ som finns att engageras i.

**SOFF:s Kartläggning av FoT-initiativ: Utbud och efterfrågan**

Cyberförsvarsgruppen har för 2021 prioriterat att bevaka vad som sker inom området för forskning och utveckling i cyberdomänen. Denna rapport är en del i arbetet. Två typer av kartläggningar har skapats inför denna rapport, en kartläggning av *utbudet* i form av pågående FoT-projekt på nationell, EU och Nato nivå samt en kartläggning av *efterfrågan* hos SOFFs medlemmar. Sammanställningen för dessa två kartläggningar om *utbud* och *efterfrågan* presenteras i rapporten tillsammans med en initial analys. Respondenter i denna enkät är medlemmar engagerade i Cyberförsvarsgruppen.

I denna kartläggning har vi utgått från begreppen: *cyberförsvar, cybersäkerhet, IT-säkerhet, säkerhet i informationssystem, informationssäkerhet, datasäkerhet och robusta system.* Detta är vedertagna begrepp inom området och valda för att kunna göra en avgränsning. Det kan säkerligen finnas fler projekt som tangerar området, men här har vi valt att göra vår avgränsning. En reflektion är att det försvårar att finna information inom forskningsområdet när så många olika begrepp används.

## Kartläggningar

## Utbud

Denna kartläggning visar resultatet för utbudet för FoT-initiativ på nationell, EU och Nato nivå. I följande fil ser ni vilka projekt och initiativ som har dykt upp under undersökningen. Vi kommer även referera till denna fil i följande analys. Totalt visar 60 nationella initiativ eller pågående projekt, 25 EU projekt och 8 på Nato nivå som bedöms vara relevant. Presentationen av data är sorterade från tidigaste startdatum till senaste. För de nyare initiativen se därför längre ned i listan.

Nedan kommer resultatet presenteras på nationell, EU och Nato nivå. Resultatet från nationell nivå är presenterade utifrån vilken aktör som har högst antal projekt av det totala, de listade 60 initiativen motsvarar därför 100% av resultatet i utbudet. Notera även att projekt och initiativ är listade i ett och samma dokument och behöver nödvändigtvis inte mena att de kan kategoriseras med varandra.

### Nationell nivå

Vi ser i kartläggningen att det är få medlemsföretag som är koordinatorer. I tillägg, visar även resultatet att det finns mycket få samarbeten som följer ”trippelhelix-modellen”[2].

Resultatet visar även att det finns en omfattande aktivitet i det som bedöms relatera till cybersäkerhet- och cyberförsvarsforskning. Däremot är få av dessa samarbeten FoT-samarbeten genomförda i samarbete med industrin. Slutsatsen är därför att den insamlade data visar på att det finns en omfattande aktivitet för FoT, men ett lägre antal Trippelhelix-modellinitiativ.

Vinnova är den myndighet som står som för finansieringen av ca 41% av alla kartlagda FoT-initiativ. Under senare tid har Vinnova investerat 73 miljoner kronor i 16 projekt i syfte att stärka cybersäkerheten för avancerad industriell digitalisering. Projektens sammanlagda budget är 133 miljoner kronor och projekten pågår i 12–24 månader. Insatsen är en del i programmet Avancerad digitalisering, ett samarbete med bland annat ABB, Ericsson, Saab och Teknikföretagen. I detta resultat ser vi initiativ enligt Trippelhelix-modellen.

För kännedom kan företag följa Vinnovas utlysningar, framför allt de inom ramen för ”*Genomförbarhetsstudier digital säkerhet och digital infrastruktur*”. Utlysningen sker flera gånger per år i området digital säkerhet och digital infrastruktur och syftar till att

[2] Benämning på när aktörer från näringsliv, akademi och offentlig sektor samverkar för att skapa innovation.

stärka svenska aktörers möjligheter till internationell uppkoppling. Denna utlysning syftar till att öka antalet internationella projekt där svenska parter ingår som deltagare eller som koordinatorer.

Myndigheten för samhällsskydd och beredskap (MSB) står för 20% av finansieringen i resultatet. Alla utlysningar av forskningsmedel finns i deras publicerade forskningsplaner. Resultatet visar inget samarbete enligt Trippelhelix-modellen. Tillsammans med Försvarsmakten finansieras även Centrum för cyberförsvar och informationssäkerhet (CDIS) för Kungliga Tekniska Högskolan är koordinatorer.

Utbudet på nationell nivå visar även att Stiftelsen för Strategisk forskning (SSF) främst riktar sin finansiering till forskning inom akademin, men de har en av de mest omfattande investeringarna i cybersäkerhetsforskning i Sverige. I listan står SSF för ca 13% av all finansiering. Möjligheter för industrin att samarbeta finns, men de får enskilt vända sig till projektledaren för det finansierade projektet.

Det som bedöms relevant för cyberförsvarsområdet är SSF:s strategiska investering i cybersäkerhetsprogrammet (300 miljoner kronor) och även delar om 6G-kommunikation inom Computer and Hardware for ICT (CHI) och Future Software Systems (FuSS). Projekten inom cybersäkerhetsprogrammet bedriver i huvudsak grundläggande forskning (TRL 2–5) inom framför allt IoT-säkerhet. Ett exempel på SSF projekt som bedöms vara intressant för cyberförsvarsforskning är Programområde *Cyber Security* och projekt ”0046 KLAS Cybersäkra reglerade system”.

**EU nivå**

När vi tittar på svenskt deltagande på EU nivå ser vi att följande aktörer medverkar i projekt och EU-samarbeten: RISE och KTH.

Kartläggningen av utbudet visar inte all den aktivitet som utvecklar och formar de nya FoT-initiativen inom EU ramprogrammen Horisont Europa och The Digital Europe Programme (DIGITAL). Denna text syftar till att ta upp den information som inte kan läsas från data i filen.

I skrivandets stund ligger cybersäkerhet fortfarande inom ramen för Horisont 2020 programmet. Planen är att det succesivt ska över till ramprogrammet Horisont Europa. Inom Horisont Europa ligger Cybersäkerhet i kluster 3 (Civil Security for Society), sedan i kluster 3 finns cybersäkerhet som den 4:de destinationen ”Increased Cybersecurity” med delmålen:

- Strengthened EU cybersecurity capacities; More resilient digital infrastructures, systems and processes; Increased software, hardware and supply chain security; Reinforced awareness and a common cyber security management and culture.

Cybersäkerhetsforskning finns även i destination 6 ”Strengthened Security Research and Innovation” där man avsatt en budget på totalt 16 miljarder Euro fördelade på fem olika forskningsprogramområden.

För finansiering av cybersäkerhets- eller cyberförsvarsforskningsprojekt till EU så rekommenderar Vinnova att koppla de till följande policyområden av EU’s Strategi: ”*Futureproof security environment*” och ”*Tackling evolving Threats”,* på så sätt stärker man sin position i ansökan.

För ramprogrammet Digital Europe är cybersäkerhet en prioritering, men riktar sig mer till innovationer än forskning. De offentliga prioriteringarna i DIGITAL är “Strengthening cybersecurity coordination between Member States tools and data infrastructures” och “Support the wide deployment of the cybersecurity capacities across the economy”. Läs mer här.

Huvudorganet för cybersäkerhet i EU är Directorate-General for Communications Networks, Content and Technology (DG *Connect*) som ansvarar för cybersäkerhet och leder det europeiska centret.

**Nato nivå**

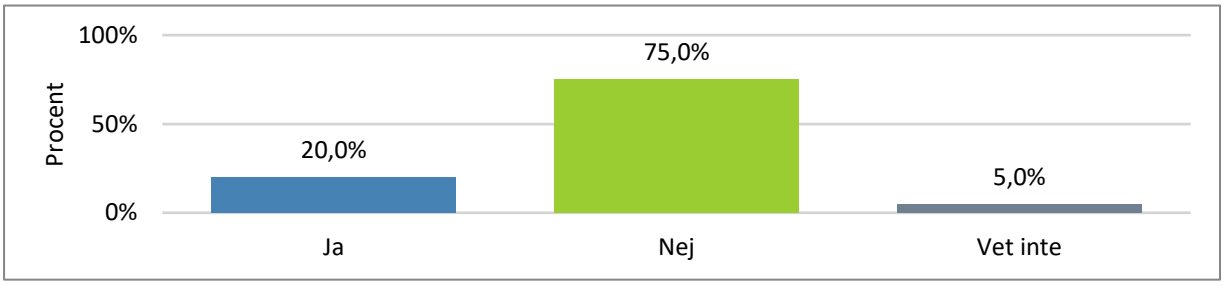
SOFF är utsedda av regeringen att representera Sverige i dess styrelse samt vara kontaktnod för de utlysningar Nato gör inom ramen för NIAG. Nyligen aviserade Nato att de kommer att satsa ett antal miljarder dollar på innovationsprogram med fokus på omvälvande teknologier. Genom Sveriges partnerskapsroll med Nato får företag i Sverige delta i de flesta programmen. Här finns med andra ord goda möjligheter för SOFF:s medlemsföretag att delta och ta plats i flertalet intressanta studier.

Resultatet visar de pågående IST projekt på Nato nivå. För mer information, kontakta kansliet.

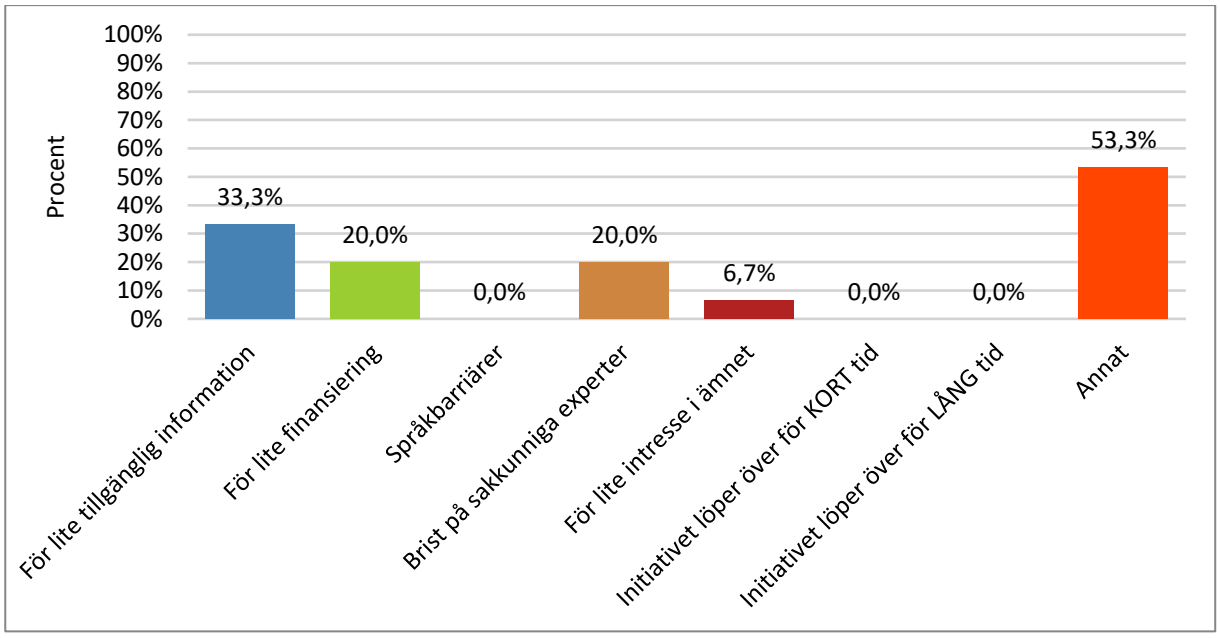
## Efterfrågan

SOFF genomförde den 17 maj till 6 juni 2021 en enkätundersökning bland företagen och detta resultat presenterar deras behov för FoT-initiativ.

**1) Under de senaste 5 åren, har ditt företag engagerat sig i ett FoT-initiativ inom cybersäkerhet eller cyberförsvar som varit offentligt finansierat?**



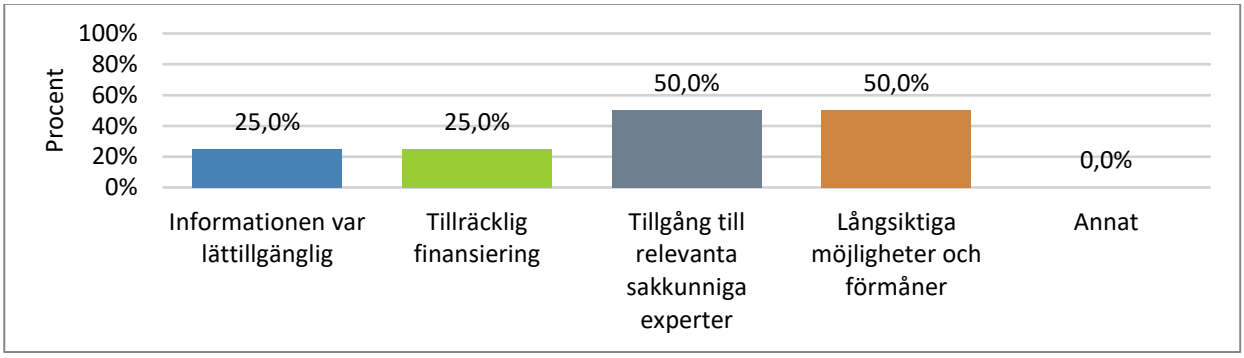

**2) Vilken av följande faktorer är den främsta anledningen till varför ni valt att INTE engagera er i?**




Det finns en majoritet bland medlemsföretagen som under de senaste 5 åren *inte engagerat sig* i ett offentligt finansierat FoT-initiativ. Anledningarna till att företagen inte engagerat sig varierar, men av resultatet framgår det att det funnits för lite tillgänglig information; för lite finansiering; brist på sakkunniga experter och för lite

intresse i FoT-initiativets ämne. En större grupp svarade av andra anledningar än dom angivna.

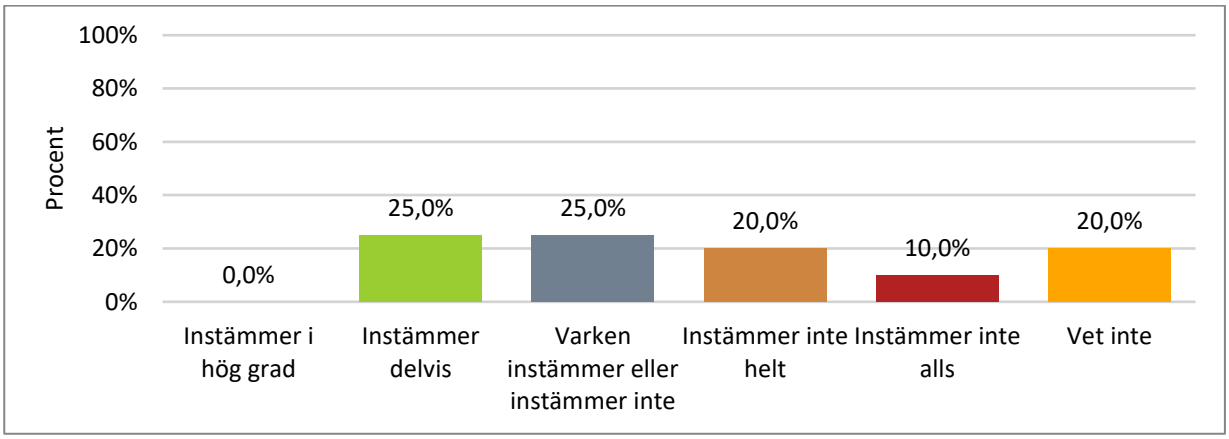
**3) Vilka av följande faktorer är den främsta anledningen till att ni har valt att engagera er?**



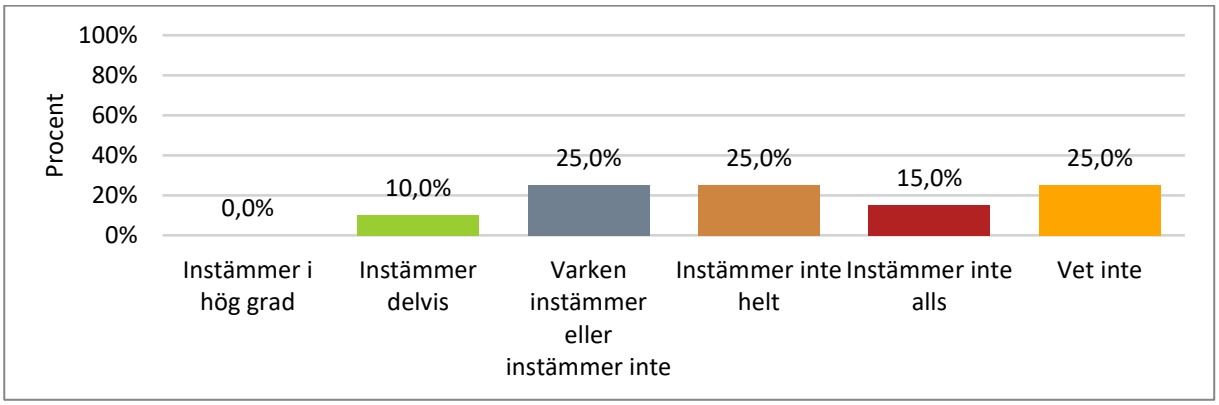

Av de 20 % företag som har engagerat sig så har tillgång till relevanta sakkunniga experter och långsiktiga möjliga förmåner varit avgörande faktorer. Det som är intressant är att för 25% av företagen fanns det förutsättningarna för engagemang såsom tillgänglig information och tillräcklig finansiering.

Det låga engagemanget bland företagen på FoT-initiativ kan ha flera orsaker. Frågan nedan ställdes för att identifiera ifall anledningen till ett lågt/högt engagemang berodde på informationen om FoT-initiativs tillgänglighet och tydlighet. Resultatet nedan visar hur företagen hittar och till vilken grad som informationen på nationell och internationell nivå går att förstå.

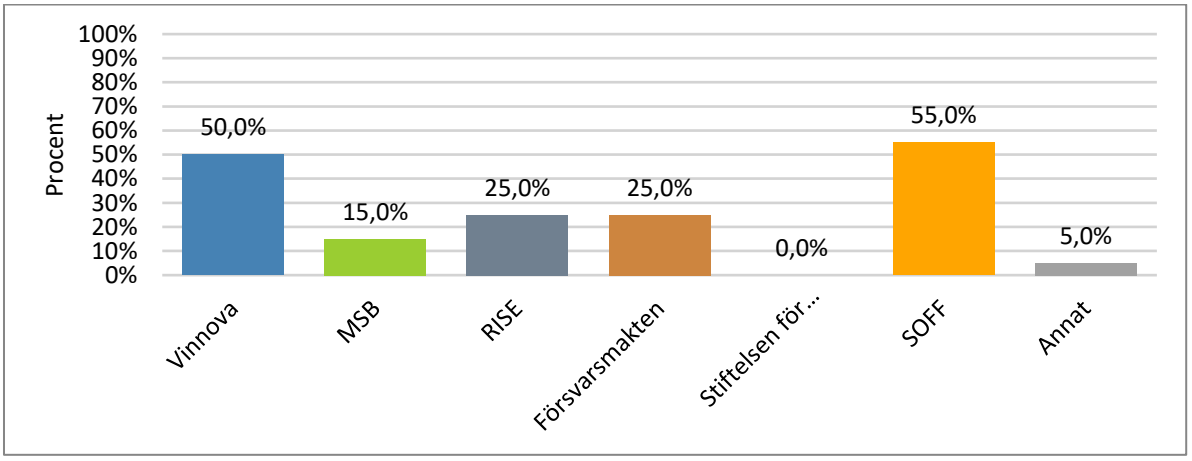
**4) Påstående: Informationen som publiceras om FoT-initiativ i området cybersäkerhet och cyberförsvar på NATIONELL nivå är lätt att förstå**



**5) Påstående: Informationen som publiceras om FoT-initiativ i området cybersäkerhet och cyberförsvar på INTERNATIONELL nivå är lätt att förstå**




**6) Hur hittar ni information om NATIONELLA FoT-initiativ i området cybersäkerhet och cyberförsvar?**



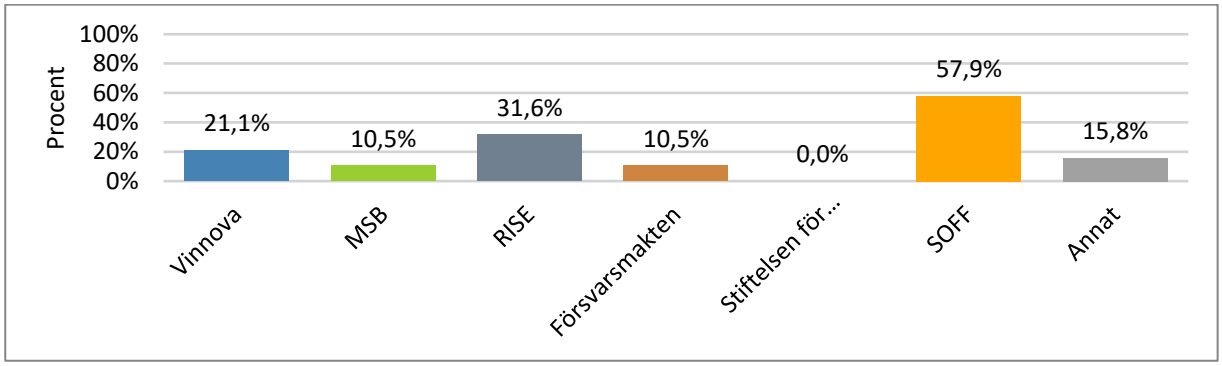

Företagen hittar information om nationella FoT-initiativ genom Vinnova och SOFF. Något som sticker ut är att 20% av alla som svarade SOFF hade endast SOFF som svarsalternativ.
SOFF har av resultatet att tyda för 20% av företagen en betydande roll i att kommunicera FoT-initiativ på nationell nivå till företagen, vilket kan bero på att det är svårt för företag att navigera sig rätt inom den nisch som cybersäkerhet utgör.

RISE, Försvarsmakten och MSB är också betydande aktörer för hur företagen hittar information om FoT-Initativ. Undersökningen visar att RISE också är en aktör som

bedriver det som kan bedömas vara forskningsprojekt både inom den svenska noden för att accelerera innovation och forskning inom cybersäkerhet samt RISE Cyber Range. Noden koordineras av RISE och arbetet genomförs i arbetsgrupper och RISE Cyber Range är en testbädd för utbildning, test och verifiering av produkter och tjänster.

Innovationsnoden driver flera arbetsgrupper inom olika områden för att underlätta identifiering av kompetenser. Idag har innovationsnoden ca 80 medlemmar där fler av SOFF medlemsföretag återfinns.

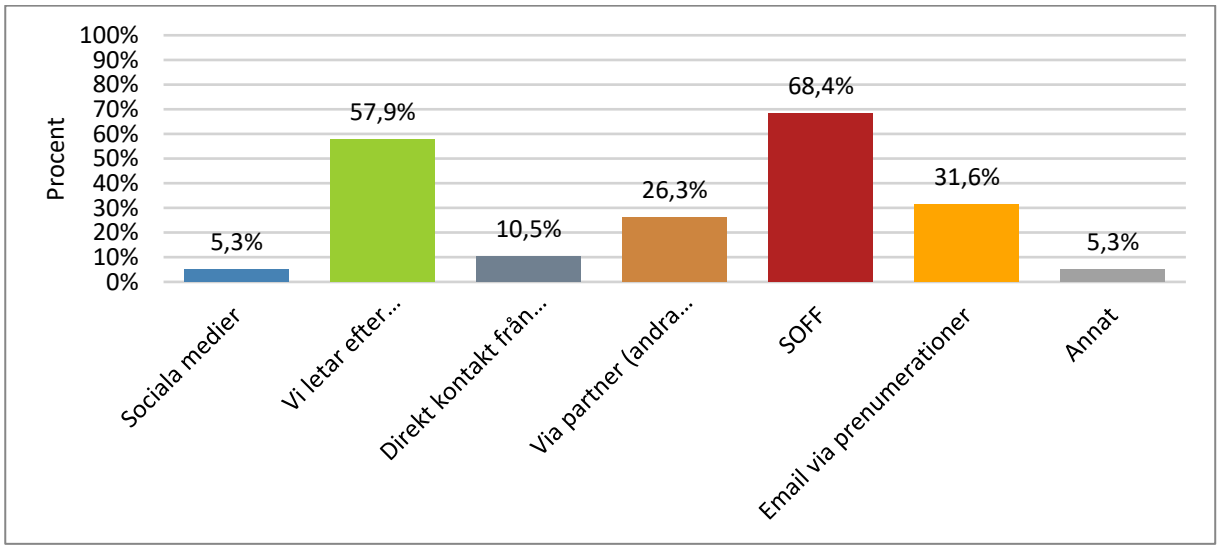
**7) Hur hittar ni information om INTERNATIONELLA FoT-initiativ i området cybersäkerhet och cyberförsvar?**




Likaså visar det sig att SOFF har en roll i att informera företagen om internationella FoT-initativ, hela 35% av de som svarade hade endast SOFF som svarsalternativ. Sannolikt beror detta på att SOFF, vid sidan av EU:s ramprogram, har särskilt fokus och resurser på den verksamhet som bedrivs inom Europeiska försvarsfonden, Nato och Europeiska försvarsbyrån (EDA).

För att identifiera viktiga informationskanaler för hur Företagen hittar FoT-initiativ ställde vi följande fråga:

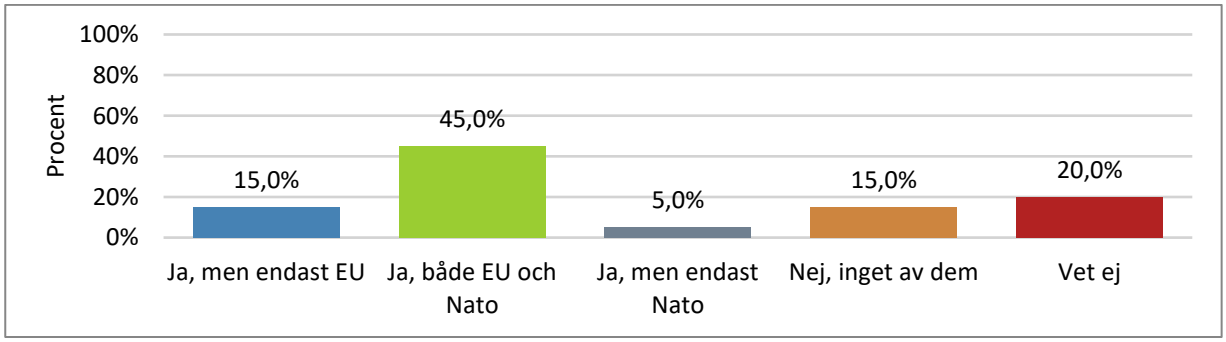
**8) Genom vilka kommunikationskanaler får ni information om FoT-initiativ? Kryssa i svar**




Detta resultat förstärker antagandet om att SOFF är en viktig kommunikationskanal för majoriteten av företagen för 25% av företagen svarade att SOFF är den enda kommunikationskanal för information som företagen nyttjade.

I detta resultat ser vi även att företagen letar efter FoT-initiativen på egen hand, men att andra kontaktytor som via partner och direkt kontakt även spelar en större roll. 75% av företagen som engagerat sig i FoT-initativ på nationell nivå har svarat att de hittat information via Vinnova och 50% svarade SOFF.

**9) Önskar ni som företag engagera er i fler FoT-samarbeten på INTERNATIONELL nivå?**

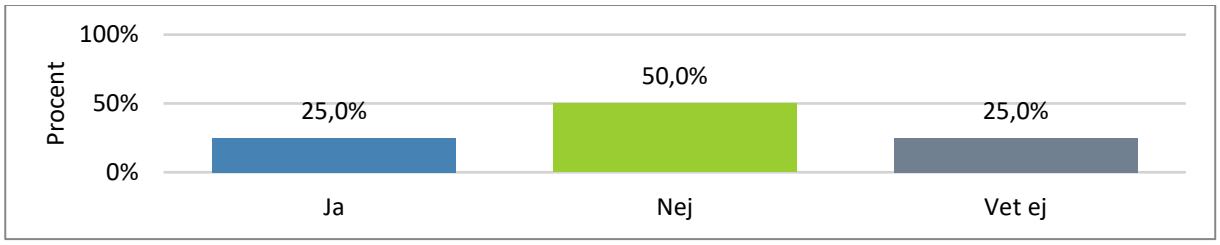



Det finns ett intresse bland respondenterna att engagera sig i FoT-samarbeten på internationell nivå. 65% svarade att de önskar att på en eller flera internationella nivåer

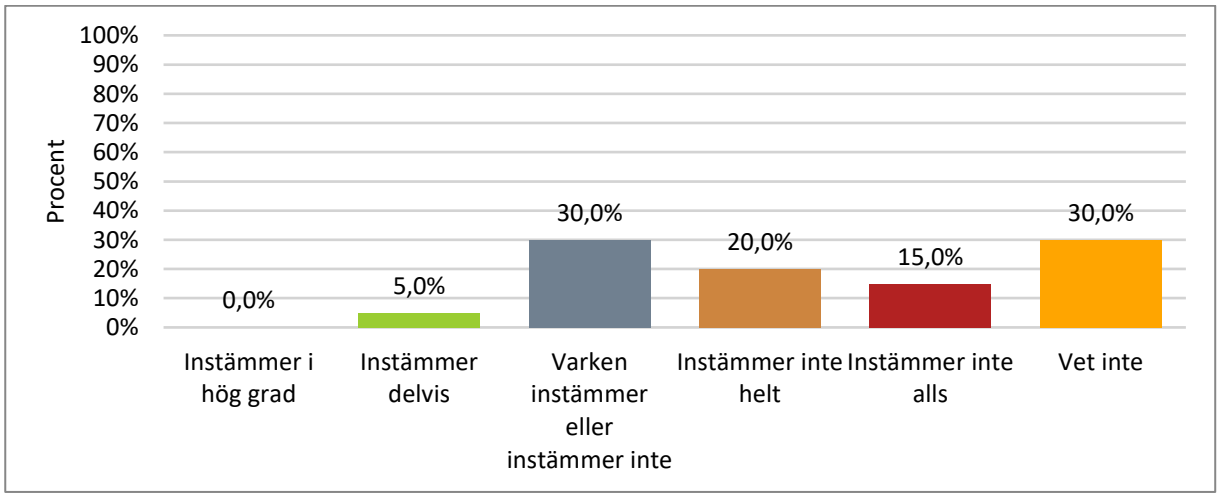
engagera sig i samarbete, varav 20% inte vet. Detta resultat visar därför på att viljan och engagemang finns hos företagen för ett internationellt samarbete.

Ett initiativ på EU-nivå som är intressant att bevaka är Europeiska Försvarsfonden, EDF. Se SOFF rapport och lanseringssamtal om EDF för mer information.

**10) Under de senaste 5 åren, har ditt företag engagerat sig i ett FoT-initiativ i området cybersäkerhet eller cyberförsvar som varit helt eller delvis finansierat av en INTERNATIONELL organisation (T.ex. EU eller Nato)?**



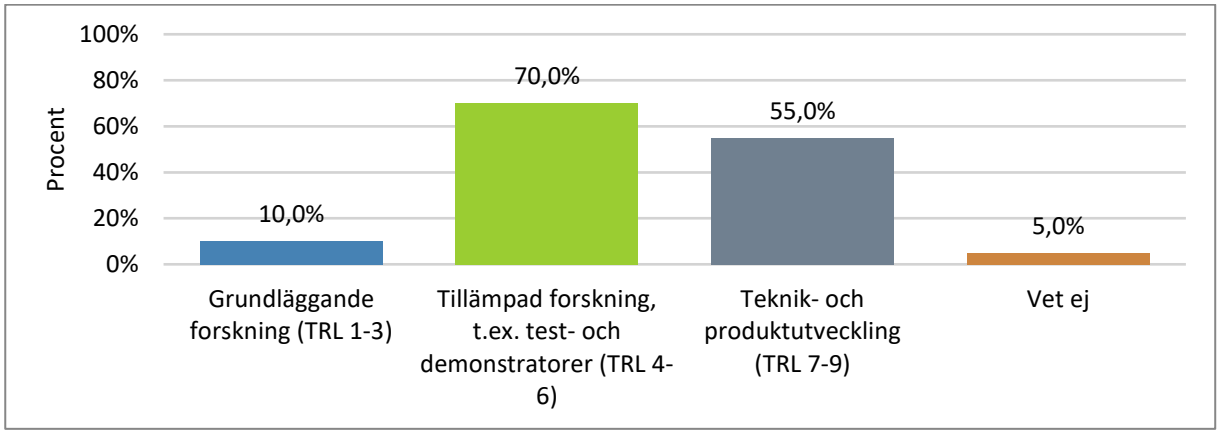

**11) Påstående: Informationen om hur vi som företag kan söka medel från EU:s ramprogram Horisont Europa, Europeiska försvarsfonden och Digital Europa är lätt att förstå**



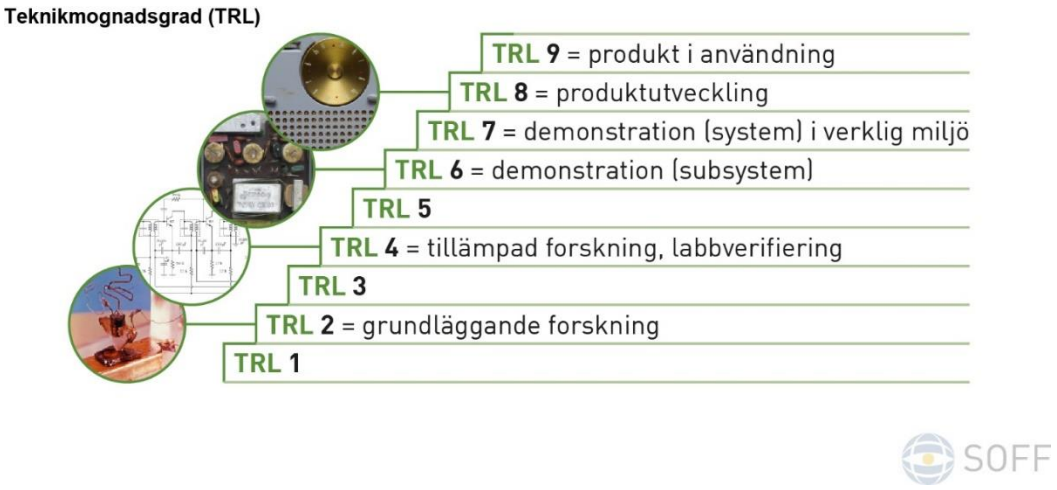

65% av företagen önskar engagera sig i fler FoT-samarbeten på internationell nivå, samtidigt visar resultatet i tabelldiagrammet ovan att informationen på både nationell och internationell nivå är svår för företagen att förstå. Det finns ett intresse bland företagen att engagera sig i FoT-initiativ på Internationell nivå, men informationen om ramprogrammen är svår att förstå.

En mindre grupp 35% önskar inte delta och kan inte fatta ett sådant beslut vid undersökningens tillfälle. Av de företagen som engagerat sig på EU nivå har 50% svarat att de finner information om internationella FoT-initativ via RISE, 50% via SOFF. Som ni även kan se i kartläggningen av *utbudet* så sticker RISE ut med ett högt deltagande i internationella konsortier.

**12) Vilket FoT-område tycker du bör vara prioritering för att nå en hög teknikmognadsgrad i cyberförsvarsområdet i Sverige? Kyssa i ditt svar.**




Majoriteten av företagen anser att tillämpad forskning och teknik- och produktutveckling bör prioriteras för att nå en hög cyberförsvars teknikmognadsgrad i Sverige. Kartläggningen visar att det är ett flertal projekt som är över TRL 3, men få forskningsprojekt finns inom TRL 7-9.



**Slutligen, företagen önskar se fler initiativ inom (listade i ordning som svaren kom in):**

- Threat intelligence
- Offensive Cyber Security
- Tillämpad forskning inom AI för cybersäkerhet.
- Utveckling av mjukvara kan bedöma ett systems preventiva/förebyggande åtgärder
- Autonoma anfall och försvarssystem.
- Implementering av säkerhetsfunktioner och verifiering av säkerhetsfunktioner
- Riskhantering
- Hur skulle ett .GOV nätverk för molntjänster kunna fungera i Sverige?
- Tillämpad kryptoteknik
- Demonstrator angående hur cyberdata kan hanteras säkert och hur data kan delas mellan olika organisationer/myndigheter för att skapa förutsättningar för ett gemensamt operativt arbete och inte enkom policyarbete.

**Slutsats**

*Möter utbudet efterfrågan?* Vetenskap och ny teknik i cyberområdet är en förutsättning för att bibehålla en långsiktig internationell konkurrenskraft och för att Sverige ska få ta del av internationella samarbeten. Försvarsföretagen är kunskapsintensiva och Sverige är ett av de mest innovativa länderna i världen, men vi behöver stärka cyberförsvars- och cybersäkerhetsförmågan genom att utbyta kunskap på nationell och internationell nivå.

Undersökningen för *utbudet* visar att det finns få projekt som samarbetar enligt Trippelhelix-modellen, där det sker en samverkan mellan näringsliv, universitet/högskola och offentlig sektor. Samtidigt visar *efterfrågan* att det finns ett stort intresse hos företagen att engagera sig i FoT-initiativ. De främsta anledningarna till att företagen valt att engagera sig har varit för att det funnits tillgång till relevanta sakkunniga experter, långsiktiga möjligheter och förmåner.

Anledningarna till att företag valt att inte engagera sig har varit flera, bland annat för att det finns för lite information, för lite finansiering och brist på sakkunniga experter. Enkätundersökningen visade även att informationen som finns tillgänglig om FoT-initiativ på nationell och internationell nivå var till större del svår att förstå. Samtidigt visade det sig finnas ett stort intresse bland företagen att engagera sig i FoT-initiativ.

**”Vilka teknikutvecklingsområden bör vara prioriterade för att nå en hög teknikmognadsgrad i Sverige?”**

Majoriteten av företagen anser att tillämpad forskning och teknik- och produktutveckling bör prioriteras för att nå en hög teknikmognadsgrad inom cyberförsvarsområdet i Sverige. Kartläggningen av utbudet visar att det är ett flertal projekt som är TRL 3, men få projekt finns inom TRL 7–9.

SOFF menar att forskningsresultaten måste omsättas i tillämpningar och att tillämpningarna får avsättning på marknaden. När forskningsresultaten omsätts i tillämpningar och avsätts på marknaden så blir det lönsamt för företagen att investera mer i forskning och teknikutveckling.

**Workshop: Slutsatser**

Slutsatserna i denna rapport har nu diskuterats i en workshop där 30 representanter från akademi, SOFF medlemsföretag och myndigheter deltog. Tillsammans diskuterade vi hur vi kan skapa förutsättningar för forskningssamarbeten enligt trippelhelix modellen, samt hur vi genom samarbete stärker både vår cyberförsvarsförmåga och konkurrenskraft i FoT.

Förslagen från workshopen presenteras nedan.

1. **Hur ska vi sammanfoga våra olika tidshorisonter?**
   Små- till medelstora företag har ofta inte samma långsiktiga tidshorisont och tillgängliga resurser och medel som akademin och det offentliga.
   För att möta våra tidshorisonter så är några av de förslag som presenterades av grupperna följande:

   **a)** Utforma forskningsprojekt med en tydlig och kortsiktig tidshorisont, anledningen är för att till exempel 1,5 år kan upplevas som lång tid för ett företag.

   **b)** Utlysta forskningsprojekt bör ha en mer specifik inriktning som kan ge snabbare återkoppling.

2. **Hur kan vi engagera fler företag i nationella och internationella FoT-projekt?**

   **Nationell nivå**
   Att skriva en projektansökan är för många företag en riskfylld process. Processen tar ofta tid och företagen behöver avsätta resurser för ansökan. Dessutom är det inte alltid en garanti att en projektansökan går igenom, och i de fallen där ansökan går igenom, så är det oftast oklart vilken avkastning som företagen kan räkna med på investeringen (ROI). Riskerna i samband med ansökningsprocessen kan i sin tur leda till att många företag avstår från att engagera sig i att ansöka om ett utlyst projekt eller samarbete. För att engagera fler företag i FoT-projekt på nationell nivå framkom följande förslag:

   **a)** Företag kan söka Vinnovas planeringsbidrag som utlyses på deras hemsida.

   **b)** Ett förslag till de organisationer som utlyser FoT-projekt, för att engagera fler företag är det viktigt att beakta ROI.

**c)** I projektutlysningen tydliggör vilka kostnader som är relaterade till projektet i ett tidigt stadie.

**d)** Möt företagens efterfrågan genom att utlysa fler projekt på en högre TRL nivå, åtminstone demonstrator nivå.

**Internationell nivå**

Företagen har ett behov och ett intresse att samverka på EU-nivå. Workshopens representanter belyste alla de utmaningarna som är kopplade till EU:s komplexa processer och att det tar tid att förstå hur de fungerar. Värdet ligger därför i samverkanseffekten, där vi alla kan dra nytta av allas insatser, bädda för framtiden och bygga kunskap tillsammans. En utmaning är att Sverige ofta kommer in sent i utformningen av utlysningarna för forskningsprojekt på EU-nivå. Det innebär att forskningsprojekten och utformningen av utbudet inte är alltid är anpassat till den svenska marknaden.
För att engagera fler företag på den internationella nivån presenterades följande förslag:

**a)** Sverige behöver bli mer proaktiva och formativa på EU-nivå, där vi är med och formar forskningsprojekten i ett tidigt skede. På så sätt blir forskningsprojekten mer intressanta att engagera sig i för att de är anpassade till den svenska marknaden och behov.

3. **Hur kan kommunikationen förbättras för en effektivare samverkan?**

För att engagera sig i FoT-initiativ på nationell-, EU- och NATO-nivå behöver först informationen om de utlysta initiativen nå fram till företagen på ett lättförståeligt sätt. Sedan, det behöver bli tydligare för företagen om vem som de ska kontakta och när om de önskar engagera sig i FoT-initiativ. Under workshopen kom det fram ett flertal förslag på vem som företagen kan vända sig till. I Sverige kan företagen om de önskar att fördjupa sig mer i FoT-projekt på nationell och internationell nivå kontakta organisationerna RISE genom sin verksamhet Cybernode, Vinnova, Stiftelsen för Strategisk Forskning (SSF), Myndigheten för samhällsskydd och beredskap (MSB), Kungliga tekniska högskolan (KTH) genom sina kanslier, Försvarets materielverk (FMV) och SOFF.

I tillägg för att nå en effektiv samverkan behöver utlysningarna smalas ned. Företagen upplever att utlysningarna ofta är breda och behöver definieras av

deltagande aktörer. Kommunikationen behöver därför bli tydligare i utlysningarna. Följande förslag presenterades:

**a)** Smala ned utlysningarna och gör de mer specifika i forskningsuppdragens formulering och uppgift.

**b)** Förtydliga vilka projekt där cybersäkerhet ingår, även om det inte är projektets huvudsyfte.

**c)** Skapa översättningsprocesser och gör det lättare att överföra kunskapen från grundforskning till tillämpning.

**d)** Gör forskningsdata mer tillgänglig till företagen.

En summering av workshopen är att det finns en konsensus om att vi tillsammans skapar värde genom samverkan. **Forskning är avgörande för internationell framgång och konkurrenskraft** och samverkanseffekten gör att vi tillsammans skapar konkurrenskraft i cybersäkerhet- och cyberförsvarsforskning på internationell nivå. Utmaningen ligger i de komplexa EU-processerna, men att myndigheter, akademi och företag tillsammans kan skapa värde genom att bygga kunskap tillsammans.