Den privat-offentliga samverkan i cyberdomänen behöver accelerera

av Richard Oehme

Résumé

This article argues that public-private collaboration in the cyber domain must accelerate to meet current and emerging security challenges. Despite a decade of debate and a government inquiry into the private sector's role in total defense, Sweden still lacks a clear and functional collaboration model. Weak public–private cooperation increases vulnerability to cyber-related disruptions and undermines total defense capability. Drawing on the author's long experience from both sectors, the article identifies six interconnected prerequisites for effective cooperation: legal conditions, shared benefits, trust, structured frameworks, everyday operational collaboration, and technical enablers. It highlights persistent legal misconceptions, the importance of mutual value, and the need for leadership-backed, standardized methods for information sharing. The article concludes that Sweden must urgently strengthen cross-sector collaboration at national, regional, and local levels to build a resilient cyber defense in an increasingly hostile digital environment.

UNDER DET SENASTE årtiondet har frågan om privat-offentlig samverkan (POS) varit föremål för omfattande diskussion. Det har även genomförts en statlig utredning som analyserat näringslivets roll inom totalförsvaret (SOU 2019:51). Trots detta har arbetet inte resulterat i en tydlig modell för samverkan. Detta är problematiskt eftersom en bristfälligt fungerande POS riskerar att försvaga vår förmåga att upprätthålla samhällsviktiga funktioner bland annat vid allvarliga cyberrelaterade störningar, och i förlängningen en försämrad totalförsvarsförmåga.

I dagens digitaliserade och uppkopplade samhälle, där huvuddelen av all samhällsviktig verksamhet bedrivs inom den privata sektorn, är det avgörande att det offentliga och det privata utvecklar ett betydligt närmare och mer strukturerat samarbete. Här behöver det offentliga, ytterst lagstiftarna, skapa bättre förutsättningar för detta genom att undanröja onödiga hinder och ge tydligare ramar som gör det enklare, tryggare och mer effektivt för aktörer att samverka. Mycket kan dock göras omgående utan att invänta nya regelverk.

Ett centralt ingångsvärde som påverkar förutsättningarna för ett samarbete mellan primärt det offentliga och näringslivet, är om det finns en skyldighet enligt författning att rapportera information till en myndighet eller statligt bolag, såsom exempelvis enligt lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. När en sådan skyldighet finns uppstår något annorlunda förutsättningar för de aktörer som berörs av skyldigheten. Men även i denna typ av ”relation” är det väsentligt att säkerställa

den gemensamma nyttan, då det kommer att bidra till effektiviteten i samverkan och rapporteringen. Ytterligare en utmaning är om det finns element av tillsyn i relationen mellan det offentliga och näringslivsaktörerna, men även här bör det gå att hitta modeller för samverkan som främjar det gemensamma säkerhetsarbetet.

Med dessa utgångspunkter följer här några reflektioner kring POS byggt på författarens erfarenheter från offentlig och privat verksamhet de senaste decennierna. Fokus är cybersäkerhet, men mycket kan även tillämpas på andra områden. Vad som sedan är centrala områden för en god POS varierar utifrån erfarenheter och perspektiv, men för min del ser jag dessa sex områden som väsentliga:

- legala förutsättningar
- gemensam nytta
- förtroende
- ramar och metoder för samarbete
- fungerande samarbete i vardagen
- tekniska förutsättningar.

Dessa områden är nära sammanlänkade och beroende av varandra, vilket innebär att brister inom ett område riskerar att få negativa konsekvenser för de andra.

Legala förutsättningar

De juridiska ramarna för samverkan upplevs ofta som hinder för närmare informationsutbyte, ibland helt i onödan. Det finns seglivade föreställningar, som att *”det offentliga kan inte skydda vår information”* eller *”det går inte att dela hemlig information med näringslivet”*. Ofta saknas en grundlig rättslig analys bakom dessa slutsatser och det är inte ovanligt att möjliga vägar till samverkan förbises.

En framåtlutad juridisk granskning kan ofta identifiera lösningar. Avgörande frågor är om informationen omfattas av sekretess, och i så fall vilken typ. Två relevanta sekretessgrunder i Offentlighets- och sekretesslagen (OSL) 2009:400 är 18 kap. §8, som gäller säkerhets- eller bevakningsåtgärder, samt affärssekretess. Om informationen omfattas av försvarssekretess (OSL 15 kap. §2) krävs särskilda hanteringsregler som godkänts av säkerhetsmyndigheter.

> *Genom avtal kan parterna på förhand reglera hur informationsutbyte och samarbete ska ske, vilket skapar förutsägbarhet och trygghet.*

Även civilrättslig sekretess och tystnadsplikt kan försvåra delning av information med det offentliga, särskilt om motsvarande skydd inte finns på myndighetssidan. Om sekretessen inte är absolut, ligger det ofta på myndigheten att göra en bedömning, där presumtionen är offentlighet. Detta kan skapa osäkerhet och leda till att information inte delas, trots att det hade varit juridiskt möjligt.

Avtal kan vara ett effektivt verktyg för att tydliggöra formerna för POS. Genom avtal kan parterna på förhand reglera hur informationsutbyte och samarbete ska ske, vilket skapar förutsägbarhet och trygghet. Ett annat hinder är att vissa myndigheter inte ser samverkan med näringslivet som en del av sitt uppdrag. Om detta perspektiv saknas på ledningsnivå kan det påverka juristers och tjänstemäns bedömningar och i praktiken försvåra informationsutbyte och samverkan.

Gemensam nytta

För att ett samarbete ska fungera krävs att alla parter ser en tydlig och konkret nytta. Frågan *”What’s in it for me?”* är central och måste besvaras för varje deltagande aktör.

Om nyttan inte är tydlig riskerar engagemanget att avta och samarbetet att urholkas.

Ett gemensamt erkännande av nyttan – gärna formaliserat genom en överenskommelse eller dokumentation – är viktigt för att säkerställa spårbarhet och för att förankra samverkan i organisationernas olika nivåer. Detta gäller även när samarbetet sker inom ramen för en lagstadgad skyldighet, som exempelvis enligt lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Samverkan innebär alltid en alternativkostnad. Den mest uppenbara är arbetstid, det vill säga – resurser som annars kunnat användas för annan verksamhet. För näringslivet innebär detta ofta att tiden för samverkan tas från arbete som har direkt påverkan på lönsamheten. Därutöver kan det tillkomma kostnader för teknik och system som krävs för att möjliggöra säker informationsdelning, särskilt om det rör skyddsvärd eller säkerhetsskyddsklassificerad information.

Ett väl fungerande samarbete förutsätter realistiska förväntningar. Det är viktigt att diskutera och enas om frågor som: Vad kan och får delas? Måste man få tillbaka exakt det man lämnar, eller kan värdet ligga i annan form av återkoppling? Hur viktig är tidsaspekten – ska information delas omedelbart eller kan det ske med viss fördröjning? Svaren påverkar både metod och struktur för samverkan.

Förtroende

Förtroende är den grundläggande byggstenen för all effektiv samverkan. Utan förtroende sker ingen, eller endast mycket begränsad, informationsdelning – oavsett vilka formella överenskommelser som finns.

Förtroende byggs över tid genom konsekvent och transparent agerande, och det kan snabbt raseras vid bristande efterlevnad av överenskomna regler eller vid missbruk av delad information. Förtroende måste finnas på alla nivåer i organisationerna – strategisk (ledning), operativ (mellanchefer) och taktisk (genomförandechefer, specialister och tekniker). Om någon av dessa nivåer saknar tilltro till processen riskerar samarbetet att förlora i värde.

> *Förtroende byggs över tid genom konsekvent och transparent agerande*

I samverkansforum med flera aktörer blir det särskilt viktigt att alla accepterar de fastställda ramarna och metoderna. När personer byts ut behöver nya deltagare snabbt introduceras till gällande regler och arbetssätt för att undvika att förtroendet urholkas och strukturen försvagas.

Ramar och metoder för samarbete

Många framgångsrika samarbeten har startats genom enskilda eldsjälars initiativ. Dessa drivkrafter är värdefulla, men långsiktigt hållbara strukturer kräver förankring på ledningsnivå i samtliga deltagande organisationer. Utan tydligt stöd från högsta ledningen riskerar samarbetet att bli ytligt och sårbart för personalförändringar.

För att samverkan ska fungera över tid måste parterna enas om tydliga metoder och regler för informationsdelning. Detta omfattar både vad som ska delas – exempelvis färdiga rapporter, varningar eller tekniska indikatorer på intrång – och hur det ska delas, såsom skriftliga rapporter, muntliga avstämningar eller återkommande möten. Det är även avgörande att fastställa hur informationen får spridas inom respektive

organisation och om, samt i vilken form, den får vidarebefordras till andra aktörer. I vissa fall kan det vara nödvändigt att anonymisera eller bearbeta uppgifterna innan vidare spridning.

Tydliga hanteringsregler måste bygga på en juridiskt hållbar grund. Ett välkänt verktyg inom cybersäkerhetsområdet är trafikljusprotokollet (Traffic Light Protocol, TLP), som på ett enkelt sätt anger hur information får spridas och till vem. Genom att använda TLP skapas en gemensam förståelse som minskar risken för missförstånd och skyddar känsliga uppgifter.

Fungerande samarbete i vardagen

Även med starka strukturer och tydliga avtal måste samarbetet underhållas i det dagliga arbetet. Regelbunden interaktion är avgörande för att bygga relationer och upprätthålla förtroende. Att försöka starta ett samarbete först vid en kris är sällan framgångsrikt. Därför bör samverkan ske kontinuerligt, och där det inte är möjligt bör den åtminstone övas regelbundet så att processerna är väl inarbetade när behovet uppstår.

Förutsättningarna skiljer sig åt mellan operativ och icke-operativ samverkan. Operativ samverkan innebär ofta hantering av känslig, ibland sekretessbelagd, information som måste delas snabbt. Detta ställer höga krav på både teknik och rutiner. Icke-operativa forum, som träffas exempelvis 6–10 gånger per år för att utbyta erfarenheter, har andra krav och kan vara enklare att etablera och underhålla.

Tekniska förutsättningar

Tekniken är särskilt viktig för operativ samverkan, där brist på godkända lösningar kan bli ett avgörande hinder. Det är inte ovanligt att organisationer tar till icke-godkända lösningar – så kallad ”skugg-IT” – för att kunna dela information, vilket medför risker. Godkända och anpassade tekniska plattformar är därför en nyckelfaktor för framgång.

> *De åtgärder som vidtas måste omfatta alla nivåer – nationell, regional och lokal.*

För den offentliga sektorn gäller att varje myndighet, region eller kommun själv måste godkänna den teknik och de informationsflöden som används. Processen blir enklare om det redan finns en lösning som godkänts av en annan aktör. Om informationen är säkerhetsskyddsklassificerad krävs dessutom kryptosystem godkända av Försvarsmakten. Myndigheten för samhällsskydd och beredskap (MSB) kan besluta om tilldelning av signalskydd för den civila sektorn, medan Försvarsmakten ansvarar för motsvarande stöd till aktörer som samverkar med det militära försvaret.

Avslutande reflektion

Möjligheterna att förbättra den privat-offentliga samverkan är redan idag betydande, och det är angeläget att agera skyndsamt. De åtgärder som vidtas måste omfatta alla nivåer – nationell, regional och lokal – för att säkerställa en robust och motståndskraftig struktur. Samverkan bör inte begränsas till enskilda sektorer; sektorsövergripande samarbete är avgörande för att möta dagens och morgondagens hot- och riskbild.

Energi-, telekommunikations- och banksektorn har redan etablerat starka samarbeten inom sina respektive områden och med centrala myndigheter. Nu är det dags att fler branscher, såsom hälso- och sjukvården, transportsektorn och hamnverksamheter, tar

en mer aktiv roll. Att arbeta i isolerade silos är inte längre hållbart – cybersäkerhet måste bli en gemensam prioritet. Det krävs även ett skifte där vi stärker de regionala strukturerna – genom samarbete mellan regioner, länsstyrelser och näringslivet – samt lokalt, där kommuner och lokala företag behöver ta en mer aktiv roll inom ramen för den nya strukturen för civilt försvar. Att skjuta på detta arbete innebär att vi utsätter oss för ökade risker i en tid där hot- och riskbilden snabbt förändras till det sämre.

I en alltmer digitaliserad värld, där sårbarheter kan utnyttjas brett och konsekvenserna bli omfattande, är en sak tydlig: ensam är inte stark. Endast genom en breddad och tvärsektoriell samverkan kan vi bygga en långsiktigt, robust och hållbar säkerhet som står emot framtidens hot.

Författaren är Senior managementkonsult vid Knowit AB med fokus på samhällssäkerhets- och cybersäkerhetsfrågor.