För säkerhets skull

Säkerhetshoten mot svenska företag

Näringslivets Säkerhetsdelegation (NSD)

Omslag: Albin Ekman/Gustav Hammarskiöld
Layout: Albin Ekman
Redigering: Karl Lallerstedt
Foto: Gustav Hammarskiöld

Tryckt 2020 hos Print in Baltic JSC
ISBN 978-91-985633-3-7

För säkerhets skull

Säkerhetshoten mot svenska företag

Förord

Säkerhetsfrågor blir allt viktigare för svenska företag, av flera skäl: den generella brottsutvecklingen i landet, digitaliseringen av samhället som skapar nya sårbarheter, och vår sammankoppling med en allt oroligare omvärld.

Den här boken är tänkt att bidra med ökad kunskap om utvecklingen, hur du som företagare bättre kan skydda ditt företag och även vad samhället i stort kan göra för att öka tryggheten.

Vår målgrupp är bred — företagare rent allmänt, men specifikt de som berörs av eller har ansvar för säkerhetsfrågor. För att göra boken mer tillgänglig och lättläst har vi valt att inte utforma den som en renodlad handbok i säkerhetsfrågor. Men det finns samtidigt en hel del referensmaterial och gott om praktiska tips. Tanken är att det är en bok som man kan komma tillbaka till flera gånger.

Att bidra till en ökad kunskap kring säkerhetsfrågor i företag är viktigt i sig — men indirekt hoppas vi också bidra till ett bättre samhälle genom att fler företag blir röster för vikten av god säkerhet i samhället. Kunskap är en förutsättning för förbättring.

Vi hoppas också att spridningen av denna bok — som är tillgänglig gratis i digital form för alla — kommer att bidra till att fler företagare väljer att engagera sig i Näringslivets Säkerhetsdelegation (NSD).

NSD har nu funnits i över 50 år och är det ledande nätverket för personer med ansvar för säkerhetsfrågor inom näringslivet. Nätverket inkluderar även representanter från offentlig sektor och i vår centrala delegation ingår bland annat cheferna för Polisen, MUST, SÄPO och MSB.

Tipsa gärna dina vänner och kollegor om denna bok, och om Svenska Säkerhetspodden där experterna som bidragit med sin kunskap till boken intervjuats.

Om ditt företag är medlem i Svenskt Näringsliv och du ansvarar för säkerhetsfrågor, anmäl dig gärna som kontaktperson till NSD. Genom att bygga ett större nätverk blir vi en starkare och viktigare röst för främjandet av säkerhetsfrågor i Sverige.

Mer information om NSD, och hur man blir kontaktperson finns här HTTPS://WWW.SVENSKTNARINGSLIV.SE/FRAGOR/NSD/.

Jag önskar dig stimulerande läsning!

Thomas Lundin,
ordförande i Näringslivets Säkerhetsdelegation

Om den här boken

När World Economic Forum presenterar sin årligen återkommande Global Competitiveness Report placerar Sverige sig konsekvent i topp. I 2019 års rapport hamnar Sverige på en hedrande åttondeplats av de 141 länder som studerats.

Ett av de områden som försämrar vår totalplacering gäller dock Security, ett mått som omfattar bl a mordstatistik, den organiserade brottslighetens omfattning och kvaliteten på polisens arbete. Där placerar vi oss inte högre än på plats 38, betydligt sämre än våra nordiska grannländer.[1]

En av de allra mest omdebatterade frågorna i Sverige på senare år gäller just brottsligheten, och hur den på ett stort antal områden ökar. Det leder till otrygghet, personligt lidande och stora samhällsekonomiska kostnader. Och som World Economic Forum sätter fingret på i sin ranking påverkar det i högsta grad även näringslivets förutsättningar.

Syftet med den här boken är att ge en aktuell överblick av hur svenska företag påverkas av olika typer av säkerhetshot. Dessa kan gälla allt från stölder och skadegörelse till organiserade bedrägerier, cyberbrott och företagsspionage.

Utöver att dessa brott drabbar företagare av kött och blod försämrar de också Sveriges konkurrenskraft. Brottslighet mot företag är därför en naturlig fråga för det svenska

näringslivet att engagera sig i. Även företag behöver kunna lita på skydd från brottslighet.

Boken bygger på intervjuer med experter av olika slag, såväl svenska och internationella forskare som säkerhetsanalytiker, branschföreträdare och representanter för polisen. De har olika perspektiv på utvecklingen, men målar alla bilden av att brottslighet är ett växande problem för svenska företag, ett problem som inte alltid tas på tillräckligt allvar.

Greger Ekman har skrivit huvuddelen av boken baserat på de ovan nämnda expertintervjuerna samt underlag som officiella rapporter och nyhetsrapportering. Intervjuerna genomfördes av Karl Lallerstedt och finns tillgängliga i de första tretton poddavsnitten av NSD:s poddserie Svenska Säkerhetspodden.

Marie Wallin har författat appendixet ”Om du utsätts för brott – en praktisk handledning för företag”. Olof Erixon har författat appendixet om ”En enkel modell för riskanalys”. Karl Lallerstedt har agerat redaktör för den slutliga texten och ansvarar för eventuella fel. Värt att notera att boken inte skall tolkas som något officiellt ställningstagande från Svenskt Näringsliv eller Näringslivets säkerhetsdelegation.

Vi vill med denna bok uppmärksamma en vardag som allt för många företag lever i, en vardag där brottslighet av olika slag utgör ett påtagligt hot mot affärer, medarbetare och kunder. Det är vår förhoppning att på detta sätt kunna öka fokus på företagens villkor när insatser mot brottsligheten diskuteras.

Karl Lallerstedt,
ansvarig för säkerhetspolicyfrågor på Svenskt Näringsliv

Fotnoter

1 http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

POLIS AVSPÄRRAT
POLICE - DO NOT CROSS

KAPITEL 1

Vad är det som händer?

Företagen och brottsligheten

Trots en lång period av högkonjunktur och låg arbetslöshet under 2010-talet är det fler som ser mörkt än ljust på framtiden.

SOM-institutet vid Göteborgs Universitet, som löpande mäter svenska folkets syn på vart Sverige är på väg. Utvecklingen åren 2012-2019 har givit en tydlig bild: allt färre tycker att Sverige utvecklas åt rätt håll, allt fler åt fel håll. I 2019 års mätning är pessimisterna drygt tre gånger så många (61 procent) som optimisterna (19 procent).[2]

Den utbredda pessimismen inför Sveriges framtid har flera förklaringar, många olika händelser och förändringar har bidragit till den syn som dominerar. En av de allra viktigaste förändringarna är brottsligheten. Få saker har diskuterats så intensivt runt svenska folkets köksbord som minskande trygghet och ökande brottslighet.

Brottsligheten tar upp allt mer utrymme i massmedias rapportering och är en dominerande fråga i den politiska debatten. Den sätter spår även på marknaden: försäkringsbolag, larm- och låsföretag och vaktbolag som erbjuder varor

och tjänster för att öka säkerheten upplever en mycket stark efterfrågan.

Den här boken handlar om vad denna ökande brottslighet består i, vilka konsekvenser den får för svenska företag och vad som kan göras åt den – av företagen själva och av ansvariga politiker. I detta första kapitel vill vi ge en överblick över problemet och dess konsekvenser. Längre fram i boken djupdyker vi i enskilda områden och i olika brottstyper.

ALLT FLER UTSÄTTS FÖR BROTT

Så som andra samhällsfrågor som diskuteras intensivt finns förstås, även vad gäller brottsligheten, olika uppfattningar om hur utvecklingen egentligen ser ut. Delar av problemet är också svårt att tolka, men den allmänna bilden får sägas vara entydig: brottsligheten och otryggheten i det svenska samhället ökar.

Den myndighet som ansvarar för att samla fakta om brottslighet, brottsbekämpning och brottsförebyggande arbete är Brottsförebyggande Rådet, Brå. Brå presenterar varje år ett antal olika studier, varav den mest övergripande är den Nationella trygghetsundersökningen (NTU). Där redovisas de övergripande resultaten från omfattande datainsamlingsarbete som 2020 omfattade 70.400 uppgiftslämnare. NTU studerar utvecklingen över tid och 2020 års rapport innefattar data för den senaste tioårsperioden.

Trenden under mätperioden är tydlig: andelen som anger att de utsatts för brott ökar. Under 2019 uppgav en dryg femtedel av de tillfrågade (22,6 procent) att de som privatpersoner utsatts för något brott under året. De brott som omfattas

är misshandel, hot, sexualbrott, personrån, fickstöld, försäljningsbedrägeri, kort-/kreditbedrägeri, trakasserier eller nätkränkning. Motsvarande andel var år 2018 23,1 procent.

De två vanligaste brotten är hot, sexualbrott, kort- och kreditbedrägerier vilket 9,2, 5,6 respektive 5,5 procent uppgav att de utsatts för under 2019. Den typ av brott mot privatpersoner som uppvisat den tydligaste ökningen över tid är sexualbrott, som ökat i varje undersökning sedan år 2012 fram till 2018, då en minskning från toppnoteringen 6,4 procent 2017 noteras. Sedan 2015 uppvisar hot och personrån en liknande utveckling.

Brottsligheten är omfattande och ökar över tid, men alla brottsoffer drabbas förstås inte på samma sätt. Tvärtom är vissa grupper betydligt mer utsatta för brott än andra. En fjärdedel (26,4 procent) av dem som utsattes för brott mot person under 2019 utsattes för fyra eller fler brott. Det motsvarar ungefär 6,0 procent av befolkningen, som alltså mer eller mindre regelbundet utsätts för brott.

Faktum är att dessa särskilt utsatta personer står för den absoluta merparten av den brottslighet som drabbar någon varje år. Av den totala andelen händelser utgjorde den upprepade brottsligheten hela nio tiondelar (90,3 procent). De som är utsatta för upprepad brottslighet är väldigt hårt drabbade. Tre av fyra brott som begås (75,1 procent) drabbar personer som utsatts fyra eller fler gånger.

Den allra mest utsatta gruppen har också en tydlig profil sett till ålder, kön, utbildning och etnisk bakgrund. Upprepad utsatthet är vanligare bland personer under 25 år, bland kvinnor, bland personer födda i Sverige med två utlandsfödda föräldrar samt bland personer med låg utbildning.

ALLT FLER KÄNNER ORO FÖR BROTT

De allra flesta – nästan fyra av fem personer – drabbas som sagt inte alls personligen av något brott utifrån Brås sätt att mäta saken varje år. Samtidigt finns en utbredd oro för att utsättas för brott. Nästan varannan tillfrågad (47 procent) oroar sig i stor utsträckning för den ökande brottsligheten.

Oro för brottslighet är ett problem på flera sätt. Dels är det naturligtvis i sig obehagligt och stressande för de människor som oroar sig för att utsättas för olika brott, även om de faktiskt inte drabbas. Dels påverkar oron människors agerande och sätt att leva på ett sätt de inte önskar, oron för brott begränsar rörelse- och handlingsfriheten även för dem som inte själva drabbas.

Ett uppmärksammat mått på detta är att tre av tio (30 procent) uppger att de känner sig mycket otrygga vid utevistelse i sitt bostadsområde kvällstid på grund av rädslan att utsättas för brott. Kvinnor oroar sig i högre utsträckning än män för att utsättas för brott i det egna bostadsområdet, 38 respektive 22 procent. Var tionde kvinna uppger att de inte lämnar hemmet kvällstid för att de är oroliga att utsättas för brott.

En av brottslighetens många skadliga effekter är att den över tid kan erodera förtroendet för rättsväsendet. Reaktionen är lätt att sätta sig in i: om staten inte kan sköta sin mest grundläggande uppgift och skydda medborgarna från brott, varför ska då medborgarna lita på staten?

Sverige har historiskt präglats av internationellt sett hög tillit, såväl mellan medborgarna som mellan medborgarna och staten. Det gäller även svenska folkets syn på rättsväsendet. Hela 49 procent av de tillfrågade i NTU uppger att de har stort förtroende för rättsväsendet. Det är en hög nivå jämfört

med många andra länder, motsvarande nivå i USA är exempelvis bara 23 procent.[3]

Ett av de många skälen till att bekämpa den växande brottsligheten är just att förhindra att den börjar erodera förtroendet för rättsväsendet. Erfarenheten visar nämligen att när en sådan nedbrytningsprocess väl börjat kan den visa sig mycket svår att stoppa. Det visar inte minst situationen i Sveriges särskilt utsatta områden.

OTRYGGHET I UTSATTA OMRÅDEN

På samma sätt som brottsligheten i Sverige drabbar människor olika hårt beroende på hur gamla de är eller deras kön eller etniska bakgrund, är också var man bor en avgörande fråga för risken att utsättas för brott av olika slag.

Det har naturligtvis alltid funnits skillnader i brottslighet mellan områden, få samhällsproblem fördelas jämnt över befolkningen och definitivt inte brottslighet. Det allvarliga är dock förekomsten av ett stort antal områden som bedöms särskilt utsatta för brottslighet och näraliggande problem, områden där det blir allt svårare ett leva ett tryggt och produktivt liv.

Sedan ett par år publicerar Polisen återkommande analyser av dessa områden. I den senaste rapporten, som presenterades 2019, listas totalt 60 utsatta områden. Av dessa klassificerar Polisen 22 områden som särskilt utsatta områden, 10 som områden i riskzonen att utvecklas till särskilt utsatta och 28 som övriga utsatta områden.[4]

Typiskt sett finns dessa områden i förorter till storstäderna Stockholm, Göteborg och Malmö, men även mindre

städer har motsvarande typer av problem. I sin klassificering av områden har Polisen tillämpat fyra kriterier:

- De boendes benägenhet att delta i rättsprocessen
- Polisens möjligheter att utföra sitt uppdrag
- Eventuella parallella samhällsstrukturer
- Extremism, främst våldsbejakande islamistisk extremism

De särskilt utsatta områdena kännetecknas av akuta och fundamentala problem på alla dessa områden. Det handlar alltså inte enbart om brottslighetens omfattning i sig, utan om hur hela den sociala miljön fungerar – eller snarare inte fungerar.

Dessa områden präglas av svag ekonomi, utbredda sociala problem och en allt djupare negativ spiral som successivt bryter ner det reguljära samhällets normer. Tilliten boende emellan är låg vilket innebär en svag förmåga till kollektivt ansvarstagande och ordningsskapande i området.

Få reagerar på det som normalt anses vara normbrytande beteenden. Det finns också en motvilja mot att vända sig till polisen, även bland dem som utsätts för brott. Detta ger i sin tur kriminella mer utrymme att öppet och ibland demonstrativt bryta mot lagen. Den öppna brottsligheten bidrar vidare i sig till att ytterligare minska benägenheten att t ex polisanmäla och vittna – det upplevs tydligt i vardagen att rättsväsendet inte fungerar.

De kriminella gängen, som har goda förutsättningar att växa i dessa områden, fyller delvis det tomrum som uppstår när civilsamhället är svagt och rättssystemet inte uppfattas fungera. Nya maktstrukturer etableras och de kriminellas inflytande i lokalsamhället ökar. Det fördjupar den redan

svaga tilliten till varandra och till rättsväsendet som finns i dessa områden.

Resursstarka individer väljer av naturliga skäl ofta att flytta ifrån sådana miljöer. Det innebär i sin tur färre goda förebilder för ungdomar och underlättar rekryteringen till de kriminella gängen eller nätverken. Dessa organisationer utövar en attraktion för pojkar och unga män som söker bekräftelse och ett socialt sammanhang, liksom skydd och säkerhet. Polisen beskriver att det i stora drag är samma grundläggande process för rekrytering av personer till jihadism som till reguljär kriminalitet.

Där kriminella gäng och organisationer har en stark ställning kan så kallade parallella samhällsstrukturer uppstå. Det innebär att kriminella sammanslutningar är med och sätter normerna för vad som är accepterat inom ett visst område, och även tillämpar ett slags privat rättsskipning för dem som bryter mot reglerna.

Detta parallella rättssystem gäller inte bara vid brottslighet utan även vid vad det reguljära rättssystemet kallar civilrätt. Personliga konflikter, verkliga eller inbillade oförrätter, otrohet och äktenskapsproblem handläggs ”privat” utan inblandning av polis och domstolar. De normer som gäller inom de parallella rättssystemen förs vidare till nya generationer inom familjer och släkter.

Det lokala näringslivet i dessa områden drabbas mycket hårt av den organiserade brottsligheten, många företagare är i praktiken rättslösa. Dels kan de utpressas att lämna ifrån sig pengar genom traditionell s k beskyddarverksamhet. Men dels förekommer också att den organiserade kriminaliteten med hot om våld tvingar till sig kontroll över företag som

används som legal fasad för bedrägerier och annan ekonomisk brottslighet.

Systematiska stölder är ett återkommande problem för butiker och butiksnäringen i särskilt utsatta områden. Det stora våldskapital som gängmedlemmarna äger medför att de, utan risk att polisanmälas, i praktiken kan ta varor utan att betala. Företagare kan även med hot om våld tvingas sälja illegal alkohol och tobak eller upplåta sina lokaler för lagerhållning av stöldgods och narkotika.

Den parallella samhällsstrukturen gör att kriminella organisationer kan etablera illegal konkurrens gentemot den reguljära näringsverksamheten.

Ett exempel är att erbjuda illegal låneverksamhet och försäljning av varor som är insmugglade, oskattade, icke godkända, piratkopierade eller stulna. Det finns i vissa av dessa områden även en illegal hyresmarknad, där gängen erbjuder sig att mot betalning eller genomförda tjänster ordna bostäder som de i sin tur kan ha tvingat till sig.

Sammantaget kan de särskilt utsatta områdena beskrivas som miljöer där det reguljära rättsväsendet har mycket svårt att verka. Istället tar kriminella organisationer gradvis över allt fler av de uppgifter som normalt sett sköts av det legitima näringslivet eller det lokala civilsamhället.

HUR PÅVERKAS FÖRETAGEN AV BROTTSLIGHETEN?

Av naturliga skäl handlar diskussionen om brottslighetens konsekvenser framförallt om privatpersoners situation. Alla kan sätta sig in i hur det måste vara att inte känna sig trygg om man rör sig ute på kvällen eller ens i sitt eget hem. Men

brottsligheten har högst konkreta effekter även på svenska företag.

Längre fram tittar vi närmare på hur företag i olika branscher påverkas av olika typer av brottslighet, men låt oss börja med att på ett övergripande plan studera hur brottslighet påverkar svenska företag.

I en undersökning[5] bland Svenskt Näringslivs medlemsföretag uppger nästan sex av tio (56 procent) företag att brottsligheten är ett problem för dem och deras verksamhet. En lika stor andel uppger att de har utsatts för brott under de senaste två åren.

Det vanligast förekommande brottet var stölder, som drabbat 33 procent av företagen. Men även inbrott, bedrägerier och skadegörelse var vanligt förekommande. Ungefär vart femte företag har de senaste två åren drabbats av denna typ av brottslighet.

Mörkertalet i den officiella brottsstatistiken är stort då långt ifrån alla brott anmäls. Endast hälften av företagen som utsatts för brott anmäler alla brott de utsatts för, många gånger avstår man från att anmäla. Nästan vart femte företag anmäler över huvud taget aldrig brott de utsatts för. Den viktigaste anledningen till att en polisanmälan inte görs är att den drabbade företagaren inte tror att en sådan skulle leda till någonting.

Tendensen att inte anmäla brott man utsätts för betyder dock inte att företagen misstror polisen generellt. Tvärtom har företag i allmänhet stort förtroende för polisen. Svenskt Näringslivs undersökning visar att två av tre företag (67 procent) har mycket eller ganska stort förtroende för polisen, endast sex procent uppger att de helt saknar förtroende.

Faktum är att företagare, trots att de så ofta utsätts för brott, har större förtroende för polisen än vad svenska folket i allmänhet har. Drygt hälften av den tillfrågade allmänheten uppgav att de hade stort förtroende för polisen, jämfört alltså med nästan två av tre företagare.

Samtidigt är det nog så allvarligt att vart tjugonde företag uppger sig helt sakna förtroende för polisen. Företagare är ålagda att följa mängder av lagar och regler, att rapportera uppgifter till myndigheter, att hantera sina anställdas skatteinbetalningar etc. De måste helt enkelt noga följa lagen, då behöver de kunna lita på att polisen säkerställer att andra också gör det.

BROTTSLIGHETENS KOSTNADER I NIVÅ MED KOSTNADEN FÖR RÄTTSVÄSENDET

Som vi kommer att gå närmare in på får brottsligheten flera typer av negativa konsekvenser för företagen. Den mest uppenbara är dock att den kostar företagen mycket stora pengar varje år.

När Svenskt Näringsliv låtit företagen uppskatta de direkta kostnaderna av brottslighet summerar det till närmare 50 miljarder kronor per år (genomsnittet av de uppskattade årskostnaderna 2018 och 2020).[6] Det är i närheten av kostnaden för rättsväsendet i Sverige. Den totala kostnaden för samhället är dock betydligt högre än så. De närmare 50 miljarderna innefattar inte brottslighet riktad mot privatpersoner eller offentlig sektor, inte heller är de indirekta kostnaderna för samhället medräknade.

Stölder är den typ av brott som ger upphov till de allra största kostnaderna, det som kostar mest efter detta är skadegörelse, följt av inbrott. Den ekonomiska skada brottsligheten ger upphov till försämrar företagens lönsamhet på ett högst påtagligt sätt. Den bransch som är hårdast drabbad är handeln.

Det är viktigt att då påpeka att kostnaderna i Svenskt Näringslivs undersökning endast gäller just de direkta kostnaderna för stulna varor, skadegörelse på egendom, bedrägerier etc. Till detta ska läggas indirekta kostnader som åsamkas företagen i andra led.

Företag som regelbundet drabbas av brottslighet kan som en konsekvens av detta få försämrat rykte och ett skadat varumärke. Det får negativa konsekvenser för kund- och leverantörsrelationer, för rekryteringen av nya medarbetare, för tillgången på lokaler att hyra, för möjligheten att beviljas krediter eller teckna försäkringar etc.

Piratkopiering och varumärkesförfalskning är en form av brottslighet som inte märks på samma sätt som andra former av stöld. Men konsekvenserna av denna kriminalitet är kostnader på över 17 miljarder kronor för svenska företag och över 7 000 förlorade arbetstillfällen. Två procent av den totala årliga försäljningen av svensktillverkade varor, motsvarande 28 miljarder kronor, beräknas vara förfalskade.[7]

Det finns två kategorier av piratkopior. ”Äkta kopior” som kunden är medveten om är kopior av originalprodukter, så som billiga varianter av reservdelar eller märkeskläder. Den andra kategorin är rena förfalskningar av originalprodukterna som köps i god tro.

Sverige som har en innovativ, exportinriktad ekonomi med ett högt förädlingsvärde är särskilt utsatt för intrång i immateriella rättigheter, så som patent och registrerade varumärken. Det värdemässigt överlägset största intrånget sker inom produktkategorierna motorfordon och maskiner, industriell utrustning. 20 procent – var femte – bilreservdel som säljs i Sverige beräknas vara en förfalskning. Den enskilt största källan av piratkopior är Kina.

En annan form av brottslighet som blivit ett tilltagande problem är IT-relaterade brott som datastölder, cyberbedrägerier och utpressning. En del av cyberattackerna är statsfinansierade och det är i princip omöjligt för enskilda bolag att skydda sig mot dessa attacker vars syften kan vara industrispionage.

Samtidigt är det viktigt att känna till att även företag omfattas av Säkerhetsskyddslagen (2018:585). Enligt denna har alla verksamheter ett ansvar att *”planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.”*[8]

Företagens kostnader för att skydda sin verksamhet mot brott ökar. Inte minst ökar kostnaderna för att skydda IT-system mot intrång. Av Svenskt Näringslivs undersökning[9] framgår att drygt åtta av tio (82 procent) av de företag som de senaste två åren utsatts för brott vidtagit åtgärder för att skydda sig mot ytterligare brott.

Brottsligheten tvingar företag att satsa allt större summor på larm och lås, kameraövervakning, säkerhetsvakter etc. Även detta är kostnader företagen inte skulle haft om inte brottsligheten var så hög.

Det är svårt att uppskatta företagens kostnader för att skydda sig mot brott. En indikation är dock den stadigt växande marknaden för säkerhetsföretag av olika slag. Sedan år 2014 har antalet anställda i företag som ingår i organisationen Säkerhetsföretagen ökat med mer än en femtedel, från ca. 22 000 till 27 000 anställda.[10] De tjänster som dessa företag erbjuder motsvarar dock bara en del av den totala kostnaden för företagens säkerhet.

Vart tredje företag i Svenskt Näringslivs undersökning uppger att det är en utmaning att bedriva verksamhet som vanligt med tanke på brottsligheten. Detta är ett mönster som går igen i hela landet men läget är mest akut i storstädernas utsatta förorter. Svenskt Näringslivs lokala företagsklimatundersökning 2020 visade också att minskad brottslighet och ökad trygghet var det enskilt mest prioriterade området bland över 30 000 svarande företag.

I en undersökning som Stockholms Handelskammare låtit genomföra uppger ett av fyra företag i utsatta områden utanför Stockholm att brottslighet är det enskilt största problemet i deras verksamhet. Var femte företagare uppger att de känner sig ganska eller mycket otrygga i sina egna affärslokaler. En knapp tiondel överväger att flytta verksamheten ifrån området på grund av den höga brottsligheten.[11] I dessa områden är brottslighetens hot mot näringslivet existentiellt.

BROTTSLIGHETENS LÅNGSIKTIGA KONSEKVENSER

Risken att utsättas för brott har blivit ett allt mer akut problem för dem som bor i de särskilt utsatta områdena i de större städernas förorter.

Kriminella strukturer har i flera fall blivit så etablerade att den reguljära trygghetsinfrastrukturen inte längre fungerar tillfredsställande. Kriminella nätverk och organiserad brottslighet fyller ut tomrummet som lämnas av civilsamhället och rättsväsendet.

Det samma gäller företagens utsatthet. Brottsligheten skapar otrygghet för ägare och personal, förstör företagens tillväxtmöjligheter och ger upphov till stora kostnader. Generellt har många företag runtomkring i landet denna typ av problem.

Mer specifikt är brottsligheten i flera av de utsatta områdena ett omedelbart hot mot den fortsatta företagsamheten i dessa miljöer. Vissa företagare tvingas dra slutsatsen att det helt enkelt inte går att verka i dessa områden. Om företagen lämnar försämras områdets status ytterligare och framtiden blir dystrare för dem som bor där.

Brottslighet mot företag har även långsiktiga effekter som är än mer destruktiva och på sikt farliga för samhällsutvecklingen i stort. På flera sätt utgör den ett mer fundamentalt hot mot samhället.

För att dessa områden ska kunna utvecklas på ett positivt sätt är det av avgörande betydelse att de företag som fortfarande verkar där kan finnas kvar, växa och anställa fler medarbetare. Och på sikt att fler företag kan etableras i dessa miljöer. Utan ett välmående näringsliv kommer de utsatta områdena att sjunka allt djupare i utsatthet.

Centralt för bekämpningen av brott är att det finns tillräckligt många poliser och övriga utredare. Det innebär att Polismyndigheten måste lyckas med att behålla de poliser man har och rekrytera nya. Mycket tyder på att det blivit

svårare att rekrytera poliser i tillräcklig takt.[12] De ökade kraven brottsligheten ställer på polisen innebär i sin tur en ökad press på åklagarmyndigheten, domstolarna och kriminalvårdens kapacitet att hantera alla ärenden.

Eurostats (2016)[13] sammanställning över polistätheten inom EU visar att Sverige, med 203 poliser per 100 000 invånare, ligger 37 procent under snittet på 324 poliser inom unionen. 2019 uppgick antalet poliser till 20 423[14], vilket motsvarar knappt 198 poliser per 100 000 invånare baserat på en befolkning om 10,33 miljoner (2019)[15]. Trots att antalet polisanställda aldrig varit fler har antalet poliser per capita sjunkit eftersom befolkningen ökat.

I Eurostats sammanställning har Sverige tillsammans med Danmark (186) och Finland (137) lägst polistäthet inom EU. Stora medlemsländer som Tyskland (297) och Frankrike (326) har omkring 50 procent fler poliser per capita.

Tillräckliga polisresurser och en förstärkning av hela rättskedjan är grunden för brottsbekämpningen. Den ökade mängden tung kriminalitet och dödliga skjutningar tar stora resurser i anspråk som innebär att rättsväsendet tvingas göra prioriteringar som riskerar att få allvarliga långsiktiga konsekvenser.

Tyvärr har det visat sig att mängdbrott så som ringa stölder, som ofta begås av unga förövare, är ingångar till gradvis grövre kriminalitet. Att brottsutredningar läggs ned eller avskrivs direkt ger kriminella en tidig anvisning om att de kan komma undan med brott. Samtidigt som de butiksinnehavare och företagare som drabbas av ideliga stölder tolkar låga uppklarandegrader som att samhället har gett upp eller inte bryr sig om brottsoffren.

De lågprioriterade mängdbrotten står för lejonparten av de mångmiljardbelopp som brottligheten kostar företagen årligen. Kostnaderna för privatpersoner och samhälle tillkommer.[16]

Sammanfattning

→ En stor del av svenska folket utsätts varje år för brott av olika slag. Enligt statistik från Brå har över en femtedel av svenska folket utsatts för någon form av brott senaste året.

→ De vanligaste brotten är hot, trakasserier och sexualbrott. Vissa brott, som t ex bilinbrott, har minskat markant, men många andra typer av brott ökar.

→ Utsattheten för brott är mycket ojämnt fördelad i samhället, en liten del av befolkningen utsätts för en stor andel av brotten. Tre av fyra brott som begås drabbar personer som utsatts för brott fyra gånger eller fler.

→ Polisen klassar 22 bostadsområden i Sverige som särskilt utsatta. I dessa områden är de boende ofta ovilliga att medverka i rättsprocesser, brott anmäls sällan och polisen har svårt att utföra sitt arbete. Kriminella gäng tar över allt mer av civilsamhällets och rättsväsendets uppgifter. Allt fler företag i dessa områden tvingas flytta eller lägga ner sin verksamhet.

→ Enligt en undersökning Svenskt Näringsliv låtit göra uppger sex av tio svenska företag att brottsligheten är ett problem för deras verksamhet, lika många har utsatts för brott de senaste två åren.

→ Brottsligheten innebär stora kostnader för företagen. Bara de direkta kostnaderna i form av stölder, skadegörelse, bedrägerier etc. uppgår till närmare 50 miljarder kronor per år. Det är inte långt ifrån kostnaden för hela Sveriges rättsväsende.

→ Intrång i immateriella rättigheter som patent och registrerade varumärken kostar svenska företag över 17 miljarder kronor och 7 000 arbetstillfällen årligen. Handeln med piratkopior av svenska produkter omsätter över 28 miljarder kronor varje år, något som drabbar den innovativa exportinriktade svenska ekonomin hårt.

→ Till de direkta kostnaderna ska läggas indirekta kostnader i form av skadade varumärken, svårigheter att t ex rekrytera, beviljas lån eller teckna försäkringar. Dessutom tvingas svenska företag varje år satsa stora summor för att skydda sig från brott, även dessa kostnader ligger utanför de närmare 50 miljarderna.

→ De långsiktiga konsekvenserna av brott mot företag kan på sikt hota hela samhällsutvecklingen. Tilliten i samhället bryts ner, förtroendet för rättsväsendet försvagas och tilltron till demokratins förmåga att skydda medborgarna undermineras. Att medborgarna upplever att staten inte förmår leverera trygghet är en ny företeelse i Sverige som riskerar att få långtgående konsekvenser.

→ Historiskt har Sverige haft en låg brottslighet och en hög tillit både mellan medborgare och mellan medborgare och samhälle. Tilliten har underlättat att driva affärsverksamheter vilket givit den svenska ekonomin en konkurrensfördel. Ökande brottslighet och minskande tillit är inte bra för affärerna.

→ Polistätheten i Sverige är högre än i Finland och Danmark men mer än en tredjedel lägre än den genomsnittliga polistätheten inom EU.

→ Även relativt lindriga brott kostar företagen och samhället tiotals miljarder kronor årligen. Krafttag mot denna inkörsport mot grövre kriminalitet är viktigt för att bekämpa den ökande brottsligheten. Det är en viktig signal från samhället att det inte är praktiskt taget riskfritt att ägna sig åt småkriminalitet.

Fotnoter

2 Göteborgs universitet, SOM-institutet, Vart är Sverige på väg? Folkets syn på utvecklingen i Sverige, 2020. https://www.gu.se/sites/default/files/2020-08/287-302%20Johan%20Martinsson.pdf

3 https://news.gallup.com/poll/1597/confidence-institutions.aspx (tabell bara)

4 Polisen: Kriminell påverkan i lokalsamhället - En lägesbild för utvecklingen i utsatta områden, 2019. https://polisen.se/siteassets/dokument/ovriga_rapporter/kriminell-paverkan-i-lokalsamhallet.pdf/download?v=

5 Svenskt Näringsliv: Brottslighetens kostnader 2020, 2020. https://www.svensktnaringsliv.se/material/rapporter/brottslighetens-kostnader-2020pdf_1143423.html/BINARY/Brottslighetens%20kostnader%202020.pdf

6 Svenskt Näringsliv: Brottslighetens kostnader 2020, 2020. https://www.svensktnaringsliv.se/material/rapporter/brottslighetens-kostnader-2020pdf_1143423.html/BINARY/Brottslighetens%20kostnader%202020.pdf

7 OECD: Förfalskning och piratkopiering och den svenska ekonomin, Säkerställande att ”Made in Sweden” alltid är det, 2019. https://www.prv.se/globalassets/in-swedish/varfor-immaterialratt/forfalsk- ning-och-piratkopiering-och-den-svenska-ekonomin-2019.pdf

8 https://riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/saker- hetsskyddslag-2018585_sfs-2018-585

9 Svenskt Näringsliv, Brottslighetens kostnader 2020, 2020. https://www.svensktnaringsliv.se/material/rapporter/brottslighetens-kostnader-2020pdf_1143423.html/BINARY/Brottslighetens%20kostnader%202020.pdf

10 Säkerhetsföretagen, Säkerhetsföretagens årsrapport 2019, 2019. https://www.transportforetagen.se/globalassets/rapporter/sak/sakerhetsforeta- gens-arsrapport-2019.pdf ?ts=8d79fe2ac65ea00

11 Stockholms Handelskammaren, Kriminaliteten förgiftar företagandet i förorten, 2017. https://www.chamber.se/rapporter/kriminaliteten-forgiftar-foretagandet-i-fororten. htm

12 Sveriges radio (10 juni 2018): Polisutbildningen dabbas av avhopp – 100 stolar kan stå tomma

13 Eurostat, Police officers per 100 000 inhabitants (2019). Data från år 2016.

14 Polisen: Årsredovisning 2019, s. 94.

15 Statistiska centralbyrån: Sveriges befolkning

16 Svenskt Näringsliv, Brottslighetens kostnader 2020, 2020. https://www.svensktnaringsliv.se/material/rapporter/brottslighetens-kostnader-2020pdf_1143423.html/BINARY/Brottslighetens%20kostnader%202020.pdf

KAPITEL 2

Vem begår brotten och varför?

Bakom varje brott finns minst en gärningsman. På samma sätt som olika typer av brott drabbar olika typer av brottsoffer skiljer sig också gärningsmännens profil tydligt åt beroende på brottens karaktär. Ideologiskt motiverad eller ekonomisk brottslighet utförs exempelvis i regel av personer med en annan profil än rånare och inbrottstjuvar.

I det här kapitlet beskriver vi vad som är känt om de personer som begått eller är misstänkta för brott. Att även misstänkta, dvs inte bara dömda, personer är intressanta att studera har med just den organiserade brottsligheten att göra.

Ett av problemen med brottsligheten, som beskrivs i kapitel 1, är att benägenheten att polisanmäla brott ofta är låg. Det gäller i synnerhet brott begångna av kriminella gäng och brott som sker i de särskilt utsatta områdena. För att få en översiktlig bild av profilen hos de som begår brott kan det därför vara illustrativt att även se till de misstänkta.

I vår genomgång förekommer inga identifierade personer, men det är ändå viktigt att påpeka att alla som varit misstänkta för brott naturligtvis inte är skyldiga. Tvärtom bör de ses som oskyldiga till motsatsen är bevisad.

VAD SÄGER STATISTIKEN?

Genom den ansvariga myndigheten Brå finns i Sverige omfattande statistik kring de personer som i Sverige misstänks för brott varje år. Det är därför lätt att få en översiktlig bild av vad dessa personer har gemensamt. Tre faktorer sticker särskilt ut.

För det första är de brottsmisstänka ofta unga. Nära hälften, 45 procent, var yngre än 30 år vid tidpunkten för brottet. Antalet misstänkta per 100 000 innevånare i respektive åldersgrupp var högst i den allra yngsta gruppen, de mellan 15 och 20 år.[17]

För det andra är de som misstänks för brott till övervägande delen män.[18] 2019 var hela 79 procent av de misstänkta var män. De kvinnliga misstänkta har dessutom lite annan profil än de manliga. Dels var kvinnorna något äldre när brottet begicks, dels var det vanligare att kvinnor var misstänkta för endast ett brott.

För det tredje är personer med utländsk bakgrund överrepresenterade bland de brottsmisstänkta. Statistik om brottslighet bland personer med utländsk bakgrund uppfattas ibland som politiskt kontroversiell, sannolikt för att sådan statistik ofta används för att dra långtgående slutsatser om invandringspolitiken. Men att det finns en överrepresentation bland personer med utländsk bakgrund är ett faktum, även sedan statistiken justerats för andra bakgrundsfaktorer.[19]

ÅTERFALLSFÖRBRYTARE UTFÖR EN STOR DEL AV BROTTEN

De allra flesta människor begår inga brott alls, oavsett etnisk bakgrund, men många av dem som begår brott kommer att göra det ganska snart igen. En stor del av brotten varje år begås av personer som återfallit i brott, många efter ganska kort tid.

Brå har studerat[20] återfallsbrotten och undersökt hur många av de som lagfördes för ett brott som har återfallit i brott inom ett år under perioden 2008-2017. De preliminära siffrorna visar att återfallsförbrytare står för en stor del av brottsligheten – i genomsnitt 3,2 återfallsbrott per person inom ett år. Detta avser då endast lagförda brott, dvs brott som inte uppdagats eller inte hunnit lagföras under perioden faller utanför denna studie.

I synnerhet unga och tungt kriminellt belastade tenderar att återfalla i brott inom kort. För en genomsnittlig återfallsförbrytare tar det cirka fyra månader innan ett nytt brott begås och uppdagas. Tungt kriminellt belastade män begår nya brott betydligt fortare än så – mediantiden till första återfall är drygt två månader.

Sammantaget lagförs ungefär en av fyra (24 procent) av de dömda för ett nytt brott inom ett år – 16 procent av kvinnorna och 25 procent av männen.

Återfallsfrekvensen är generellt sett högst bland de yngsta och lägst bland de äldsta. Bland dömda personer i åldern 18-20 återföll 30 procent inom ett år, vilket kan jämföras med de dömda som är över 60 år där endast 11 procent återföll under samma period. Bland kvinnor var återfallen flest i åldersgruppen 21-39 år (20 procent), och bland män i åldersgruppen 18-20 år (33 procent).

ORGANISERAD BROTTSLIGHET I SVERIGE

En stor del av brottsligheten utförs av kriminella gäng och nätverk av olika slag. Denna typ av brottslighet har på senare år uppmärksammats allt mer, i takt med att det blivit allt mer uppenbart att organiserad brottslighet inte är ett marginellt fenomen utan ett högst påtagligt samhällsproblem. Därför kommer vi i detta kapitel att särskilt fokusera på den organiserade brottslighetens karaktär och egenskaper.

Rapporten Våldsbejakande extremism och organiserad brottslighet i Sverige är en grundlig undersökning av hur så kallade antagonistiska miljöer uppstår, upprätthålls och samspelar med varandra. Undersökningen bygger dels på intervjuer med berörda personer och dels på analys av bland annat Polisens och Säkerhetspolisens databaser.[21]

Totalt rör det sig om drygt 15 000 personer som ingår i tre huvudkategorier av kriminella strukturer: fotbollsfirmor[22], våldsbejakande extremism och organiserad brottslighet.Dessa delas i sin tur upp i tio underkategorier: nätverk, partiella organisationer[23], gatugäng, mc-gäng, maffia, fotbollsfirmor, islamister[24], autonoma, vit makt, och övriga extremister.

Personer i dessa strukturer är i regel mycket brottsaktiva, men typen av brottslighet skiljer sig delvis åt mellan de olika organisationstyperna, vilket illustreras i diagrammet nedan. De två största brottskategorierna i alla grupper är våld och narkotikabrott, men även ekonomisk brottslighet och stölder är betydande inslag.

Nätverk, partiella organisationer och MC-gäng har den största andelen narkotikabrott i sin verksamhet, medan autonom vänster och vit makt har den största andelen våldsbrott (ofta begångna mot varandra).

ALLT YNGRE PERSONER REKRYTERAS

De personer som utgör den organiserade brottsligheten är ofta påfallande unga, medelåldern är 26 år och den vanligaste åldern (typåldern) är bara 19 år. Det finns även tecken på att den organiserade brottsligheten kryper allt längre ner i åldrarna, exempelvis ökar antalet häktade barn, trots att icke straffmyndiga under 18 år endast i undantagsfall ska häktas.

Kriminalvårdens siffror för de första månaderna 2019 visar ett veckogenomsnitt på fler än 35 häktade 15-17-åringar. Det kan jämföras med 20-25 personer under samma perioder åren 2017 och 2018. Det kan tyda på att kriminaliteten i olika typer av gängmiljöer involverar allt yngre personer.[25]

Poliser som arbetar mot denna typ av brottslighet beskriver en indelning av kriminella i olika åldrar beroende på arbetsuppgift i organisationen.[26] De yngstas relation till den kriminella miljön är ofta ganska sporadisk och deras verksamhet förhållandevis enkel. Den kan bestå i t ex distribution av narkotika till missbrukare, personrån, inbrott och stölder i närområdet.

Dessa unga personers intäkter från brotten omsätts ofta snabbt i konsumtion. Inte sällan är de yngre brottslingarna impulsiva, utåtagerande och risktagande vilket gör att de tenderar att ofta exponera sig för polisen.

De äldre kriminella ingår ofta i mer fasta konstellationer och deras brott är också mer komplexa än de yngres. Då dessa personer är mer etablerade i den kriminella miljön och deras brottslighet mer avancerad samverkar de också oftare över tid och inom ett större geografiskt område. I sådana fall är etnicitet, släkt- eller vänskapsband ofta starkare sammanhållande faktorer än den geografiska platsen.

NÄSTAN UTESLUTANDE MÄN I KRIMINELLA STRUKTURER

Som nämndes tidigare var hela åtta av tio av de personer som 2019 misstänktes för brott män. Den sneda könsfördelningen är än mer uttalad vad gäller organiserad brottslighet, hela 92 procent av brotten i dessa strukturer begås av män.

Samtidigt beskriver forskarna bakom Institutet för framtidsstudier det som förvånande att andelen kvinnor i den organiserade brottsligheten inte är ännu lägre. Andelen kvinnor varierar dock kraftigt mellan de olika organisationskategorierna. Högst är andelen kvinnor i den autonoma vänstern och lägst inom fotbollsfirmorna, 18,1 respektive 0,7 procent. Näst störst andel kvinnor återfinns i den extrema islamistiska miljön, där andelen är 13,5 procent.

LÅG UTBILDNING OCH SOCIALA PROBLEM

Ett återkommande mönster hos de flesta former av organiserad brottslighet är att de personer som verkar i denna miljö har svag social ställning, däribland låg utbildning.

Sett till hela gruppen organiserade brottslingar har 46 procent gymnasiet som högsta utbildning medan endast tre procent har högskoleutbildning. Merparten av de övriga har inte slutfört gymnasiet.

En förklaring till den låga utbildningsnivån är naturligtvis att många brottslingar i dessa miljöer är så unga, de har helt enkelt inte haft möjlighet att nå en högre utbildningsnivå än grundskola. Samtidigt varierar utbildningsnivån bland personer som begår olika typer av brott, särskilt vissa ideologiskt motiverade grupper sticker ut som oftare akademiskt utbildade.

Personer i den autonoma vänstermiljön är mest välutbildade, bland dem är 20 procent högskoleutbildade. Även personer i den extrema islamistmiljön och vit makt-miljön är mer välutbildade än genomsnittet i den organiserade brottsligheten. Där har nio respektive sex procent eftergymnasial utbildning.

En problematisk uppväxtmiljö är något som förenar majoriteten av personerna i de våldsbejakande miljöerna, oberoende av vilken typ av brottslighet de medverkat i.

I studien från Institutet för framtidsstudier har uppgifter om ingripande åtgärder från Socialtjänsten riktade mot unga personer med anledning av deras uppväxtmiljö registrerats. Hela 80 procent av de kriminella i dessa grupper har som barn varit föremål för insatser såsom omhändertagande och placering utanför hemmet.

Personer som tillhör gatugäng eller s k partiella organisationer har oftare än andra organiserade brottslingar haft sociala problemen under uppväxten. Det hänger sannolikt ihop med att många i dessa grupper börjar begå brott när de är mycket unga, särskilt vålds- och narkotikabrott samt stölder.

KRIMINELLA STRUKTURER I UTSATTA OMRÅDEN

Den sociala miljö i vilken en person växer upp spelar naturligtvis stor roll för risken att senare i livet hamna i brottsregistret. Särskilt stor är risken för de barn och unga som växer upp i det som definieras som socialt utsatta.

Profilen på sådana socialt utsatta områden, som polisen definierade 2015, beskrivs mer ingående i kapitel 1. Generellt kan dock sägas att det är områden med en geografisk

koncentration av faktorer som bidrar till att öka brottsligheten. Sådana faktorer kan vara hög arbetslöshet, dåliga skolresultat och en hög andel unga.

I Polisens rapport Utsatta områden – sociala risker, kollektiv förmåga och oönskade händelser (2015)[27] definieras ett ”utsatt område” som är ett geografiskt område som karaktäriseras av låg socioekonomisk status och kriminell påverkan på lokalsamhället. Ett ”särskilt utsatt område” uppvisar samma problematik men kännetecknas också av allmän obenägenhet att delta i rättsprocessen, parallella samhällsstrukturer, våldsbejakande religiös extremism och närhet till andra utsatta områden.

Det finns flera rapporter som beskriver brottslighet och sociala problem i dessa miljöer. Brås rapport Utvecklingen i socialt utsatta områden i urban miljö 2006-2017 pekar på att kriminaliteten i dessa områden har en delvis annan karaktär än andra områden som är med i den nationella trygghetsundersökningen. Utmärkande är enligt Polisen ordningsstörningar, som buskörning, och även öppen narkotikahandel. Vidare beskrivs ofta brott i kriminella nätverk och utpressning av lokala näringsidkare som vanligt förekommande.

Bland de yngre kriminella som bor i denna typ av områden blir uppdrag som springpojkar till gängen ofta en introduktion till kriminalitet. De yngre ser upp till de äldre gängmedlemmarna, gör dem till förebilder i en miljö där de laglydiga förebilderna är mycket få. Uppdrag som att bära narkotika och hålla utkik efter polisen är lättförtjänta pengar och ger möjlighet att avancera i gänget.

Att vara knuten till ett gäng ger också status. Snabba pengar ger möjligheten att köpa märkeskläder, smycken,

bilar och liknande. I den lokala miljön ger tillhörigheten till gänget också möjlighet att ta för sig av varor i affärer utan att betala, köra med bilar och motorcyklar på gångvägar och andra förmåner som gängets egna regler ger. Att associeras med ett våldskapital ger en form av respekt som kan vara attraktiv för många unga.[28]

Den bild polisen ger av denna typ av miljöer är att de kriminella grupperingarna inte egentligen behöver ägna sig åt formell rekrytering, den går så att säga automatiskt genom att allt fler lockas till den status och de förmåner gänget kan erbjuda.[29]

En praktisk aspekt som underlättar rekryteringen är att många unga, främst killar, vistas ute på gatorna under stora delar av dygnet. Det är delvis konsekvensen av en utbredd trångboddhet, det finns helt enkelt inte plats i hemmet. Stora mängder sysslolösa unga killar på gatorna under sena kvällar är i sig en riskabel situation, men den gör det också lättare för gängen att locka nya rekryter.[30]

En del av de unga i de utsatta områdena är den första generationens kriminella i en släkt utan tidigare kriminell belastning, men ofta går kriminaliteten i arv. Två eller till och med tre generationer av kriminalitet i samma släkt är inte ovanligt. Barn till kriminella föräldrar har svårt att undvika att själva dras in i den kriminella verksamheten, dels för att föräldrarna sätter normen för hur man bör leva, och dels för att det kan finnas en förväntan på att de ska hjälpa till.

I kriminella grupper där lojaliteten med gänget i sig kombineras med släktskap och etnicitet blir det särskilt svårt för de kriminella att sluta begå brott. Samtidigt finns tendenser att närstående pressas att mer eller emot sin vilja bli en del av

den kriminella verksamheten, vilket gör det lättare att fylla luckorna när någon sitter i fängelse.[31]

En ytterligare försvårande omständighet är den utbredda fattigdomen i de utsatta områdena. Arbetslösheten är mycket hög och många familjer har svårt att klara ens de mest grundläggande utgifterna. Framgångsrika yngre kriminella kan i praktiken försörja syskon och föräldrar med sin brottslighet, vilket gör att familjen får ett intresse av att kriminaliteten fortsätter snarare än att de unga bryter sig ur den.[32]

SAMHÄLLET PÅ RETRÄTT FRÅN UTSATTA OMRÅDEN

Många företagare och boende i de särskilt utsatta områdena upplever att myndigheterna dragit sig undan och att det i sig är en viktig orsak till den växande kriminaliteten. I sin rapport Relationen till rättsväsendet i socialt utsatta områden beskriver Brå hur just det offentligas svaga närvaro är något som gör det lättare att begå brott.

I rapporten säger en tjänsteman från Skatteverket att bristen på myndighetsrepresentation innebär att kriminaliteten söker sig till området, gängen vet att det t ex inte förekommer någon kontroll av samma slag som i andra miljöer. De enda som är kvar menar tjänstemannen är socialarbetare och poliser, i övrigt håller sig myndigheterna borta från de värst utsatta områdena.

Kombinationen av svag myndighetsnärvaro och starka kriminella organisationer med stort våldskapital gör att det är få som vågar vittna eller ens polisanmäla om de utsätts för brott. En av de personer som intervjuas i Brå-rapporten summerar sin syn på saken såhär:

”Nej, gå och vittna kan jag inte göra, för du vet, de bor ju här och jag ser att polisen inte kan skydda mig … Nej, men alltså om inte jag [drabbas], så kanske barnen. Så man vågar inte riktigt.”[33]

Det är lätt att förstå att den som fruktar att ett vittnesmål kan innebära allt ifrån trakasserier till grovt våld väljer att istället tiga. Samtidigt bidrar oviljan att polisanmäla och vittna till en ond cirkel med allt vanligare och allt grövre brott, och ännu svagare vilja att medverka till polisutredningen o s v. Den låga uppklarandegraden i det stora antal gängrelaterade dödsskjutningar som främst drabbat socialt utsatta områden kan till stor del förklaras med en rädsla att själv bli brottsoffer.

I Brå-rapporten beskrivs en undersökning i två olika socialt utsatta områden, ett med fler och ett med färre skjutningar. I båda områdena uppgav 80 procent av de tillfrågade att de skulle vittna om de själva utsattes för misshandel. Däremot var skillnaden stor vad gäller om de bevittnade ett personrån. I området med färre skjutningar skulle 64 procent vittna, i området med fler skjutningar bara 43 procent. Skillnaden förklaras med att rädslan för att själv utsättas för våld är större i det senare området. Gängen skrämmer till tystnad.

I vissa områden har oviljan att vittna gått så långt att det till och med är vanligt att misstänkta, som senare visar sig oskyldiga, föredrar att sitta häktade långa perioder istället för att tala med polisen. En utredare i Järvaområdet utanför Stockholm uttrycker det såhär i SR Ekot:

”Det är ingen som pratar med polisen ute hos oss. Vi har inga vittnen. Vi har nästan inga målsägande, för

de är rädda för att medverka. De vågar inte säga vad de drabbats av till polisen, för då har de ju pratat med polisen, och det får man inte göra ute i förorten."[34]

Brott kan naturligtvis i många fall utredas även om det inte finns några vittnen eller ens målsägande. Men det gör utredningarna svårare och mer utdragna, och ställer höga krav på teknisk bevisning. Under den tiden kan de misstänkta begå nya brott.

INTERNATIONELL ORGANISERAD BROTTSLIGHET

Den inhemska organiserade brottsligheten, särskilt den som sker i de utsatta områdena, är huvudsakligen knuten till ett visst geografiskt område. De brott som begås där är ofta lokala, och saknar koppling till andra orter i Sverige. En stor del av den organiserade brottslighet som drabbar svenska företag är dock på olika sätt internationell.

Gränsöverskridande kriminalitet förutsätter kontakter med god lokalkännedom och förtroende i närmiljön. Dessutom finns redan befintlig konkurrens från andra kriminella strukturer som redan är etablerade och har den lokala förankring som krävs. Det har därför traditionellt ofta varit svårt för utländska kriminella nätverk att etablera sig i Sverige.

Omvärldstrender har dock på senare år gjort det lättare för kriminella grupperingar att göra affärer över Sveriges gränser. Internationellt sett begränsade gränskontroller och en stor andel boende med utländsk bakgrund, särskilt i vissa områden, har gjort det möjlighet att bygga upp gränsöverskridande kriminalitet.

Just förekomsten av lokala kriminella med kontakter i sina gamla hemländer har ofta varit nyckeln. Ett exempel är inflödet av illegala vapen från Balkan, där vapensmugglarnas släktförbindelser med kriminella på plats i Sverige varit viktiga. På samma sätt har stöldligor med östeuropeisk anknytning kunnat bygga upp en verksamhet där de stjäl i Sverige för att sedan snabbt sälja stöldgodset i östra Europa.[35]

De strukturer som ägnar sig åt denna typ av brottslighet kan, enkelt uttryckt, vara organiserade på två olika sätt:

1. Celler som styrs från ursprungslandet och som reser till Sverige för att under en kort tid begå specifika stölder, enligt uppdragsgivarens beställning, och frakta hem stöldgodset.
2. Kriminella i Sverige som utför stölder, ofta på uppdrag av den rysktalande organiserade brottsligheten. Detta är inte sällan en starkt hierarkisk organisationsform där de lägre nivåerna kontrolleras av de högre.

Vissa aktörer i denna typ av kriminalitet fungerar som så kallade ”ankarpersoner” och möjliggör kriminalitet genom att tillhandahålla asylhjälp, falska officiella postadresser, bostäder, fordon, lokaler för lagring av stöldgods med mera. De som utför brotten köper dessa tjänster som ett slags konsultuppdrag, för att dels öka effektiviteten i den kriminella verksamheten och dels minska upptäcktsrisken.[36]

De organiserade stölderna har på senare tid utvecklats och blivit allt mer etablerade. Deras geografiska utbredning har ökat, etableringen i Sverige har blivit mer varaktig med långsiktiga kopplingar till lokalt förankrade kriminella.

Brottsnätverken styrs ifrån hemländerna dit merparten av stöldgodset går och brottsvinsterna omsätts. Kriminaliteten är högt organiserad och utförseln av stöldgodset utförs ofta inte av de som utför stölderna.[37]

Denna typ av brott är inte längre någon marginalföreteelse. Uppskattningsvis står internationella brottsnätverk för åtminstone vartannat bostadsinbrott och ungefär 90 procent av stölderna av bilar, bildelar, båtmotorer och jordbruksmaskiner.[38]

Polisens bedömer att denna brottslighet kommer att fortgå i nuvarande omfattning eller öka de kommande två åren. Kombinationen av god efterfrågan på stöldgodset, möjlighet till stora vinster, låg risk för upptäckt och låga straff gör detta till ett tacksamt område för kriminella gäng av olika slag.

Sammanfattning

→ Statistiken visar att de brottsmisstänkta i Sverige kännetecknas av särskilt tre egenskaper: de är i regel unga och många mycket unga, de är i de allra flesta fall män och de har ofta utländsk bakgrund (särskilt svenskfödda med utlandsfödda föräldrar är överrepresenterade).

→ En stor del av brottsligheten begås av personer som redan är dömda. Ungefär en av fyra personer som dömts för brott lagförs för ett nytt brott inom ett år. Många begår flera nya brott under den perioden, i genomsnitt lagförs återfallsförbrytare för 3,2 nya brott under det första året efter påföljden.

→ Den organiserade brottsligheten är omfattande och kan se ut på olika sätt, allt från kriminella MC-gäng och maffia till fotbollsfirmor eller islamistiska extremister. Sammantaget omfattar denna brottslighet cirka 15 000 personer.

→ I kriminella strukturer av olika slag är det särskilt påtagligt att många av de brottsmisstänkta är unga (typåldern är 19 år) och män (92 procent).

→ De allra flesta som verkar i kriminella strukturer av olika slag har låg utbildning (endast 3 procent har högskoleutbildning) och många har varit föremål för socialtjänsten under sin uppväxt (80 procent har omhändertagits som barn eller placerats utanför hemmet).

→ Unga kriminella i utsatta områden utför ofta enklare tjänster åt mer erfarna medlemmar – småstölder, narkotikadistribution, hålla utkik vid inbrott etc – och får på så sätt status i området och pengar till konsumtion.

→ Vissa kriminella strukturer engagerar flera generationer i samma släkt, där barnen hjälper föräldrarna att begå brott eller undgå upptäckt. I andra fall försörjer unga kriminella istället sina laglydiga familjer vilket gör dem beroende av brottsligheten. Kopplingen till släktband gör det särskilt svårt att bryta denna typ av kriminalitet.

→ Det finns exempel på att offentliga aktörer drar sig undan från de mest utsatta miljöerna för att det inte går att verka där. Det ökar de kriminella gängens handlingsfrihet och ger dem en chans att ersätta det reguljära samhällets normer och regler med sina egna.

→ Den internationella organiserade brottsligheten har blivit allt mer etablerad i Sverige och ägnar sig framförallt åt stölder av olika slag. Internationella stöldligor bedöms ligga bakom cirka hälften av alla bostadsinbrott samt nio tiondelar av stölderna av bilar, bildelar, båtmotorer och jordbruksmaskiner.

→ Internationella stöldligor är i regel organiserade på två olika sätt: antingen ligor som reser till Sverige för att begå brott och ta med sig stöldgodset, eller lokala ligor som begår stölder på uppdrag från organisationer i sina hemländer och skickar stöldgodset dit.

→ Många internationella aktörer köper tjänster från kriminella aktörer som bistår med t ex asylhjälp, falska officiella postadresser, bostäder, fordon, lokaler för att förvara stöldgods etc.

Fotnoter

17 Brå, Kriminalstatistik 2019, Misstänkta personer, 2019. https://www.bra.se/statistik/statistik-utifran-brottstyper/ungdomsbrottslighet. html#Misstankta

18 Brå, Kriminalstatistik 2019, Misstänkta personer, 2019. https://www.bra.se/download/18.7d27ebd916ea64de530 4de45/1585639838563/Sam- manfattning_misstankta_2019.pdf

19 Brå, Nordiska studier om brottslighet bland personer med utländsk och inhemsk bakgrund, En kartläggande litteraturöversikt av publicerad forskning och statistik 2005-2019. https://www.bra.se/download/18.62c6cfa2166eca5d70eed454/1571297186393/2019_Nordiska_studier_om_brottslighet_bland_personer_med_utlandsk_och_inhemsk_bak- grund.pdf

20 Brå, Kriminalstatistik 2017, Återfall i brott preliminär statistik, 2020. https://www.bra.se/download/18.7d27ebd916ea64de53064bc5/1590651588411/Sam- manfattning_aterfall_prel_2008-2017.pdf

21 Institutet för framtidsstudier, Forskningsrapport 2018/4, Våldsbejakande extremism och organiserad brottslighet i Sverige, 2018. https://www.iffs.se/media/22498/brott_2018_4.pdf

22 Med fotbollsfirmor avses mer eller mindre välorganiserade grupper som utövar våld i olika fotbollsklubbars namn, normalt sett mot andra klubbars ”firmor” eller supporters.

23 Med partiella organisationer avses grupper som saknar formell organisation eller t ex samarbetar på ”projektbasis” inför t ex enskilda rån.

24 Begreppet ”islamist” är omdiskuterat i dessa sammanhang och syftar inte på den religiösa övertygelsen i sig utan på benägenheten att utöva våld eller begå andra brott i religionens namn.

25 https://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=7224757(2019-05-24)

26 Polisen, Utsatta områden – sociala risker, kollektiv förmåga och oönskade händelser, 2015, s. 15. https://polisen.se/siteassets/dokument/ovriga_rapporter/utsatta-omraden-socia- la-risker-kollektiv-formaga-och-oonskade-handelser.pdf

27 Polisen, Utsatta områden – sociala risker, kollektiv förmåga och oönskade händelser, 2015. https://polisen.se/siteassets/dokument/ovriga_rapporter/utsatta-omraden-socia- la-risker-kollektiv-formaga-och-oonskade-handelser.pdf

28 Polisen, Utsatta områden – sociala risker, kollektiv förmåga och oönskade händelser, 2015. https://polisen.se/siteassets/dokument/ovriga_rapporter/utsatta-omraden-socia- la-risker-kollektiv-formaga-och-oonskade-handelser.pdf, s. 15.

29 Brå, Rapport 2018:6, Relationen till rättsväsendet i socialt utsatta områden, 2018. https://www.bra.se/download/18.10aae67f160e3eba62930 67b/1521032613477/2018_6_ Relationen_till_rattsv%C3%A4sendet_i_socialt_utsatta_omr%C3%A5den.pdf

30 Ibid. s. 85.

31 Ibid. s. 136 f

32 Polisen: Utsatta områden – sociala risker, kollektiv förmåga och oönskade händelser, 2015, s. 15.

33 Brå: Relationen till rättsväsendet i socialt utsatta områden, 2018, s. 67.

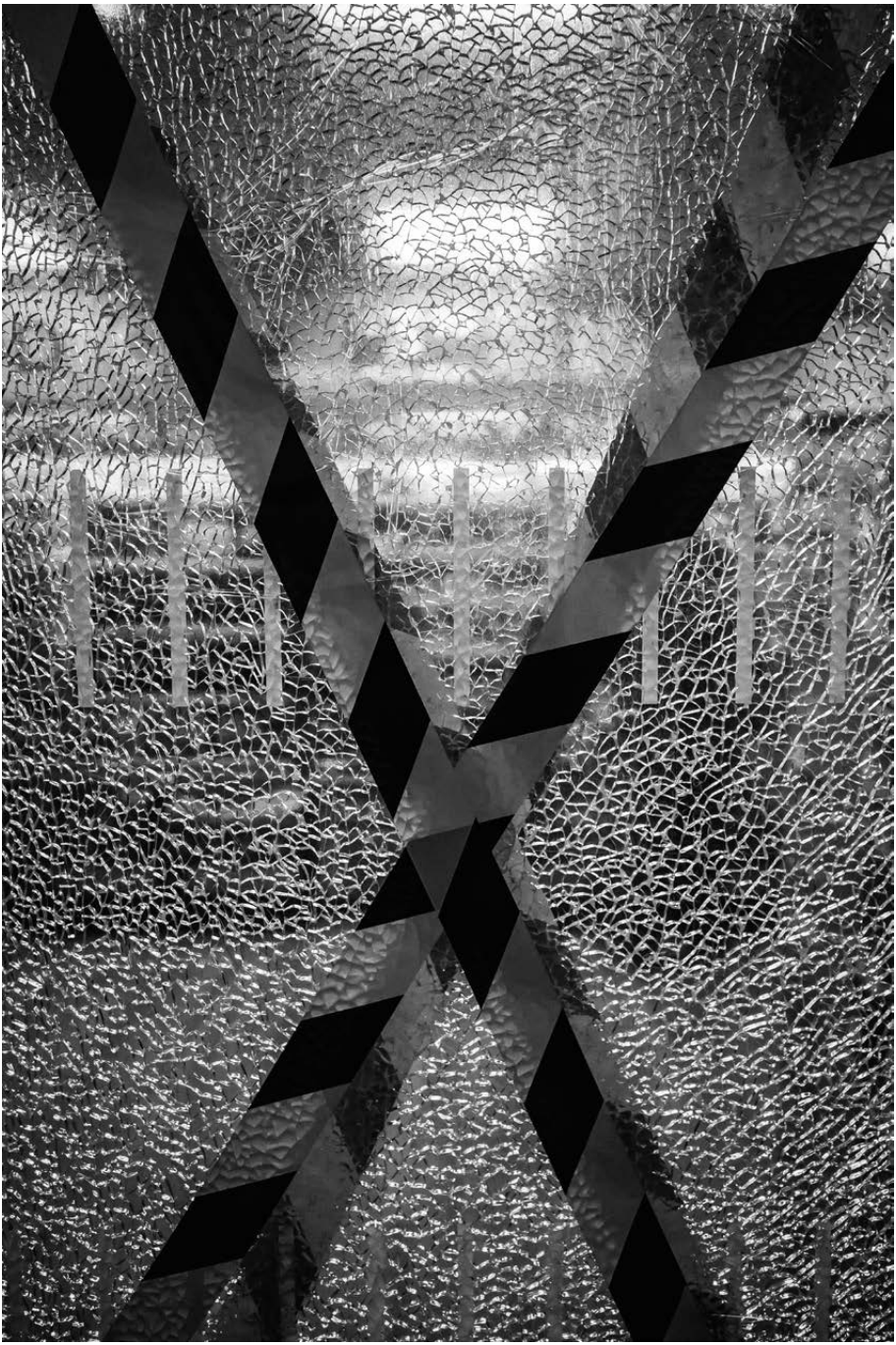
34 https://sverigesradio.se/sida/artikel.aspx?programid=909&artikel=7229580 (2019- 05-29)

35 http://www.sakerhetspolitik.se/Hot-och-risker/Organiserad-kriminalitet-/Gransoverskridande-kriminalitet/ (2019-05-24)

36 Ibid. s .4

37 Polisen, Tullverket, Kustbevakningen, Delredovisning 2 av regeringsuppdrag, Uppdrag till Polismyndigheten, Tullverket och Kustbevakningen att förstärka bekämpningen av internationella brottsnätverk som begår tillgreppsbrott i Sverige (Ju2018/00991/PO), 2019, s. 6.

38 Polisen: Internationella brottsnätverk inom organiserad tillgreppsbrottslighet Erfarenhetsberättelse 2016 - januari 2019 Öppen version, s. 3.



KAPITEL 3

Brotten som förstör livskvaliteten – mängdbrott

De allra flesta uppfattar att brottsligheten i Sverige generellt ökar, vilket också illustreras av statistiken. Men vilka brott som är de vanligaste är inte nödvändigtvis de samma som får mest uppmärksamhet i massmedia.

Terrorbrott och gängskjutningar drabbar sällan allmänheten i vardagen, även om gängskjutningarna ökat markant. De brott som drabbar vanligt folk är istället mängder av småbrott – ringa stölder, stölder, skadegörelse, störande av ordningen med mera. Mängdbrotten påverkar den upplevda känslan av trygghet och livskvalitet på ett mycket påtagligt sätt.

Mängdbrotten är särskilt allvarliga inom handeln, där hot och stölder blivit vardag i en del butiker. I vissa områden är det så illa ställt att butikerna slår igen eller flyttar till mindre brottsbelastade områden.

Att få bukt med mängdbrotten borde vara ett prioriterat mål, men en stor del av Polisens resurser går idag åt till att försöka hålla efter den allra grövsta brottsligheten. Det ger såväl småtjuvar som internationella stöldligor utrymme att bedriva sin kriminella verksamhet.

Vår förhoppning är att samhället ska komma till insikt om de stora kostnaderna i pengar, men även i förlorad trygghet, som denna brottslighet för med sig.

EN ALLVARLIG SITUATION

Sverige befinner sig idag en mycket allvarlig situation när det gäller organiserad brottslighet och mängdbrott. Magnus Lindgren, generalsekreterare för stiftelsen Tryggare Sverige, beskriver läget såhär:

> *Vi tror lätt att utvecklingen i andra länder ser ut som den gör i Sverige. Det gör den inte. I Nederländerna finns inga områden dit Polisen inte kan rycka ut eller Posten inte kan leverera brev. I Tyskland har man inga skjutningar som de vi har. I Italien har de inga bilbränningar, Norge har färre skolbränder och Spanien har färre bomber.*

Han framhåller samtidigt at all brottslighet inte ökar. Fysiska stölder generellt visar tecken på att minska något, med undantag för båtmotorer. Cyberbedrägerier är det brott som ökat mest dramatiskt.

Trots detta begås hundratals bedrägeribrott över nätet i form av id-kapningar, bedrägerier med stulna kontokortsnummer, etc, varje dag. Mer om denna typ av brottslighet kan du läsa i kapitel *”Vem kan man lita på? – Bedrägerier i stort och smått”*.

Utvecklingen i Sverige har försämrats på bred front sedan 2014-2015 och framåt. Den nationella trygghets-

undersökningen, NTU, visar att tryggheten ökade under tio år för att sedan visa på en tydligt försämrad upplevd trygghet.

Allmänhetens upplevda trygghet påverkas i stor utsträckning av spektakulära brott som gängskjutningar och sprängningar, men också av mängdbrott eller livskvalitetsbrott och ordningsbrott. Förekomsten av grov organiserad brottslighet i ett geografiskt område har stor påverkan på den trygghet invånarna som bor där känner. Tyvärr har denna brottslighet ökat.

Bilden av brottslighetens och trygghetens utveckling varierar. Magnus Lindgren beskriver hur Tryggare Sverige i sin verksamhet fått anstränga sig för att beskriva verkligheten någorlunda korrekt. Debatten har en tendens att pendla mellan ytterligheter – antingen svartmålning eller skönmålning. Samtidigt är det ett faktum att situationen varierar stort mellan olika områden.

Faktisk brottslighet och därtill upplevd trygghet varierar i regel stort inom ett så begränsat område som en kommun. NTU har idag inte en tillräckligt hög upplösning för att man ska kunna identifiera var problemen är som störst. Tryggare Sverige har konstaterat att de kommuner och kommundelar som hade utmaningar för tio år sedan, i allmänhet, har långt mycket större utmaningar idag.

INTERNATIONELLA STÖLDLIGOR BAKOM MÅNGA BROTT

Den brottslighet som de internationella stöldligorna ägnar sig åt i Sverige är ett stort problem. Försäkringsvärdet av stulet gods uppgick år 2016 till 1,1 miljarder kronor. Stöldernas

omfattning har inte minskat. Uppskattningsvis försvinner 70-90 procent av stulna båtar och bilar ut ur landet. Motsvarande siffra för inbrottsgods uppfattas till omkring 30 procent.

Per Klingvall på Stöldskyddsföreningen understryker att det är nödvändigt att skärpa lagstiftningen.

> *Vi måste hindra kriminella från att komma in i landet och ge tullen bättre möjligheter, det kräver både befogenheter och ekonomiska resurser att kunna stoppa utförsel av misstänkt stöldgods. Inte minst måste man slå till mot så kallade ankarplatser där de kriminella ligorna lagrar stöldgods i väntan på transport ut ur landet, säger Per Klingvall.*

Det behövs också ett utökat internationellt polisiärt samarbete för att stoppa stöldligornas framfart, menar han. Stöldgods från Sverige omsätts på en marknad i andra länder. För att göra det mindre attraktivt att stjäla i Sverige behöver polisen i de andra berörda länderna försvåra omsättningen av stulna bilar, båtar mm genom att slå till mot hälare och ekobrottslingar.

GROV BROTTSLIGHET SLUKAR POLISRESURSER OCH LEDER TILL ÖKAD OTRYGGHET

All brottslighet ökar som sagt inte. I Sverige och Europa i stort är nivåerna historiskt låga för vissa tillgreppsbrott. Traditionella brott som bostadsinbrott är oförändrade, rentav kan en viss nedgång skönjas.

Av den brottslighet som ökar är den grova, organiserade brottsligheten allra mest allvarlig. Denna brottslighet tar stora polisiära resurser i anspråk, vilket går ut över bekämpningen av den stora mängden mindre allvarlig brottslighet, de livskvalitetsbrott som gemene man är utsatta för.

När man frågar experterna – det vill säga de som är drabbade, ofta boende i utsatta områden – hur de uppfattar brottsligheten kommer sällan terror eller organiserad brottslighet upp. Högst upp på listan står alltid klotter och skadegörelse, män som kontrollerar kvinnor, unga män som kör för fort och stör ordningen och saboterar förutsättningarna för handeln, säger Magnus Lindgren.

STORA MÖRKERTAL OCH LÅG UPPKLARINGSGRAD

Att allmänheten upplever att brottsligheten är större än vad statistiken visar och att det inte lönar sig att anmäla brott riskerar att skada förtroendet för rättssamhället och minska den upplevda tryggheten. Mörkertalet är mycket stort och behöver utredas grundligt.

Har vi en Polis som inte arbetar med mängdbrott och handlarna upptäcker att brott de utsätts för inte utreds minskar tilltron till staten. Risken ökar för att brottsutsatta företagare vänder sig till kriminella för beskydd. Detta är en mycket farlig utveckling, med stora mörkertal som aldrig retts ut, säger Magnus Lindgren.

Beskyddarverksamhet finns i Sverige men få vågar tala om det. Särskilt i utsatta områden är det svårt att få personer att tala med Polisen eftersom det kan få obehagliga konsekvenser. Magnus Lindgren menar att bättre lokalt förankrad Polis som systematiskt över tid har byggt relationer till de boende i området sannolikt skulle kunna öka chanserna att få in tips och vittnesmål från allmänheten.

Uppklaringsgraden för brott, särskilt livskvalitetsbrott, är väldigt låg i Sverige. Endast omkring två procent av de stölder som polisanmäls klaras upp. Brottsutsatta som anmäler vittnar om en uppgivenhet även inom Polisen, som trots all motvind försöker göra sitt jobb så bra som möjligt.

Många poliser upplever sitt jobb tröstlöst när kriminella som de ansträngt sig för att få lagförda slipper undan utan straff eller med låga påföljder. Till exempel när det gäller brott mot handeln betalar åtta av tio dömda gärningsmän aldrig några böter, enligt Svensk Handel.

I de fall en och samma gärningsperson misstänks för både mindre allvarliga och mer allvarliga brott samtidigt är det dessutom vanligt att anmälningarna om de mindre allvarliga brotten läggs ned. Det har att göra med att de mindre allvarliga brotten i sig inte kommer att ge någon ytterligare påverkan/effekt på straffet. Detta är en följd av reglerna om så kallad förundersökningsbegränsning.

Logiken är att om den misstänkte fälls för det grövre brottet så adderar inte de mindre brotten till straffet, som bestäms med hänsyn till det allvarligaste brottet. Detta kan upplevas som provocerande av brottsoffren.

– Den låga uppklaringsgraden påverkar brottslingarnas beteende då sannolikheten för att åka dit för ett brott är så låg.

Sverige är näst efter Danmark sämst i Europa på att klara upp stöldbrott, säger Per Geijer, säkerhetschef på branschorganisationen Svensk Handel.

Vem vill anmäla brott när det sannolikt ändå inte kommer att leda till någon fällande dom, frågar sig Per Geijer? Eller när man sett att Polisen släppt gärningspersonen direkt utanför dörren till affären?

Svensk Handel menar att antalet stölder ökar även om Brå säger att de minskar. Förklaringen är en sjunkande anmälningsbenägenhet. Statistiken visar inte all brottslighet i samhället och är långt ifrån sanningen, menar Per Geijer.

HANDELN SÄRSKILT HÅRT DRABBAD

Av landets branschorganisationer har ingen annan än Svensk Handel någon person med särskilt uppdrag att hantera stöldproblematiken – Svensk Handel har fyra. Det är i sig en illustration till hur brottsutsatt handeln är idag och hur allvarligt branschen ser på dessa frågor.

Olika butiker utsätts för brott i olika utsträckning. Alla som arbetar i butik lär dock förr eller senare komma i kontakt med brottslighet. I Svensk Handels Trygghetsbarometer-undersökningar som genomförs varje kvartal svarar de flesta av landets butiker att de någon gång under året har drabbats av brottslighet i någon form.

För de flesta som arbetar inom handeln är jobbet i butik trevligt, men för vissa är situationen mycket besvärlig. Hot, stölder och trakasserier är dagligt förekommande i vissa butiker.

Vår rekommendation är att vara försiktig när man konfronterar brottslingar, det händer att snattare är efterlysta för mord. Varans pris är ofta ganska lågt och påföljden obefintlig så det finns inte mycket positivt i vågskålen men väldigt mycket risk för den handlare som ingriper. Det skapar frustration, man vill förstås ingripa och markera mot kriminalitet. Det blir en påfrestning för medarbetarna både när de ingriper och när de inte gör det, säger Per Geijer.

Tyvärr verkar inte samhället se så allvarligt på mängdbrott, det verkar som om det är något handeln behöver bli tvungen att lära sig leva med, konstaterar Per Geijer. Det är en orimlig situation att låta hot, lindrigare våld och skadegörelse nöta ned företagare och anställda.

MATÖKNAR OCH ”NO-GO”-OMRÅDEN

Konsekvenserna av den oreda och de ökande livskvalitetsbrott som särskilt präglar utsatta områden märks tydligt i handeln. En omfattande brottslighet med allt från småstölder till hot och misshandel gör det svårt att driva butiker i vissa områden.

Till slut ger handlarna upp och lägger ned butikerna vilket driver på utvecklingen mot så kallade ”matöknar” där de boende inte har någon möjlighet att handla livsmedel i närområdet, enligt Per Geijer.

Vi ser en utveckling som går mot att stora kedjor uttryckligen väger in säkerheten i områden för

potentiell etablering. Det uppmärksammas för dåligt idag, eftersom uteblivna investeringar inte ger några rubriker. Resultatet är en långsam erodering av utbudet i dessa områden över tid. Hemelektronik, mobiltelefoner och mode kan man inhandla på längre avstånd, men att matbutikerna försvinner är extra allvarligt, säger Per Geijer.

I vissa områden är den lokala brottsbelastningen så stor att många aktörer väljer att helt enkelt inte verka där eller åka dit, menar Per Geijer.

”No-Go”-områden är en realitet, även om man periodvis har lyckats få bukt med problemen. I enstaka fall och under kortare perioder har det varit omöjligt att leverera varor till vissa områden, säger Per Geijer.

I dessa områden är det även svårt att hitta ett försäkringsbolag som vill försäkra butiker och andra företag. Lyckas man inte teckna en brandförsäkring eller ansvarsförsäkring är det svårt och riskfyllt att driva företaget. En lösning kan vara att knyta verksamheten till en branschorganisation som Svensk Handel som kan erbjuda ett försäkringsskydd.

Kriminaliteten bidrar på flera olika sätt till att företag och välbehövliga jobb drivs ut ur socialt och ekonomiskt utsatta områden där de behövs som mest. På så vis fördjupas områdenas problem och de riskerar att fastna i en ond cirkel. Den negativa utveckling som fått fäste i vissa utsatta områden är svår att bryta. De som kan flyttar ifrån de otrygga områdena till mer trygga, otryggheten polariseras.

Kriminaliteten dikterar i praktiken mycket av villkoren för näringslivet utan att allmänheten märker det, företagare i flera branscher tvingas hela tiden ta hänsyn till brottsligheten i sin vardag.

En konsekvens som gemene man förmodligen inte märker, är att butikerna tvingas anpassa sitt utbud efter vad som efterfrågas av brottslingar. För att minska risken för stölder slutar man helt enkelt sälja varor som är allt för stöldbegärliga. Detta är en utveckling som inte bara pågår i de utsatta områdena.

MÖJLIGA ORSAKER TILL DEN NEGATIVA UTVECKLINGEN

Även om den negativa utvecklingen i Sverige på kort tid varit exceptionellt stark, är Sverige inte ensamt om brottsutsatta områden. Andra länder har också problem. De franska förorterna är ökända för sin kriminalitet. I Storbritannien ökar mängden knivskärningar och syraattacker.

Cyberkriminaliteten ökar överallt, i Storbritannien är över hälften av alla anmälda brott på något sätt cyberrelaterade. Alla länder och områden har sina egna förutsättningar, men finns det några faktorer som sannolikt lägger grunden för ökad kriminalitet?

Magnus Lindgren beskriver några faktorer, eller ”tipping points” som han kallar dem, som är särskilt betydelsefulla: den fysiska utformningen av bostadsområden, centraliseringen av Polisen, gängbrottsligheten inträde, den misslyckade narkotikapolitiken och migrationskrisen 2015.

Den ökning av kriminaliteten vi sett de senaste tio åren är resultat av politiska beslut. Den nuvarande situationen är på det sättet självförvållad, den har inte bara uppstått av sig själv. Det finns klara och tydliga orsaker som lett fram till att brottsligheten och otryggheten ökat i många olika kommuner, säger Magnus Lindgren.

Magnus Lindgrens summering av faktorer bakom brottsligheten:

1. BOSTADSOMRÅDENAS UTFORMNING

Den första faktorn Magnus Lindgren pekar på är den fysiska utformningen av bostadsområden har stor betydelse för de boendes upplevda trygghet. I och med modernismens inträde på 1950- och 60-talen förändrades stadsbyggnadsmiljön.

Under lång tid byggdes städer småskaligt och integrerat med husens öppna framsidor vända mot det offentliga rummet, gator och torg, där det sociala utbytet skedde. Modernismen vände upp och ned på detta och istället byggdes vad som benämndes ABC-städer (Arbete-Boende-Centrum)[39], som en idé med stora hyreshus byggda runt lokala torg med butiker.

I praktiken fungerade detta dock inte, de boende föredrog att både arbeta, handla och tillbringa sin fritid på annan plats. Uppförandet av bostadsområden inom miljonprogrammet som i stor utsträckning saknade arbetsplatser – så kallade sovstäder – fick till följd att dessa områden blev ödsliga vid olika tidpunkter. Det sociala liv som fanns flyttade från offentliga öppna ytor till innergårdar med mindre social kontroll. På så sätt byggdes förutsättningar för otrygghet och kriminalitet.

2. CENTRALISERINGEN AV POLISEN

En annan betydelsefull faktor är enligt Magnus Lindgren det faktum att Polisen förstatligades 1965. Ungefär samtidigt började polisen lämna lokalsamhället och sedan dess har varje polisreform enligt Magnus Lindgren lett till att Polisens lokala förankring gradvis försämrats. Vid den senaste reformen 2015 centraliserades Polisen ännu mer och det lokala vakuum som uppstod har kunnat fyllas av kriminella.

3. GÄNGBROTTSLIGHETENS INTÅG

En tredje faktor som Magnus Lindgren lyfter fram är den organiserade brottslighetens etablering i Sverige. Under 1980-talet etablerade sig MC-gängen i Skåne och med dem började en kriminell infrastruktur byggas upp, ett helt ekosystem av kriminalitet.

> *Vi hade kunnat pressa tillbaka dem då, men det fanns en politisk oförmåga att hantera MC-gängen. Det fanns en del som sa att de gängen bara var motorintresserade män som borde få hålla på med sin näringsverksamhet – när de i själva verket ägnade sig åt grov kriminalitet. Den tystnadskultur som rådde då ser vi i kvadrat idag, säger Magnus Lindgren.*

4. DEN MISSLYCKADE NARKOTIKAPOLITIKEN

Sverige har omfattande problem med droger och sannolikt kommer situationen att förvärras de närmaste åren, tror Magnus Lindgren. Enligt Folkhälsoinstitutets rapporter minskar andelen svenska ungdomar som provat narkotika,

men samtidigt ökat antalet överdoser och den totala droganvändningen, inklusive tyngre droger.[40]

5. MIGRATIONSKRISEN SATTE PRESS PÅ KOMMUNERNA

Magnus Lindgren menar även att den så kallade migrationskrisen, som kulminerade 2015, bidragit till problemen. Under denna period ökade befolkningen mycket snabbt och många nyanlända kommit att bosätta sig i redan utsatta områden. Detta är en naturlig konsekvens av viljan att bo nära släktingar och landsmän, men det fördjupar också problemen i många områden.

Kommunerna har idag hårt ansträngd ekonomi och svårt att leva upp till sina åtaganden. Det innebär att de ökande sociala problemen, särskilt i de utsatta områdena där arbetslösheten är hög och utbildningsnivån är låg, blir svåra att komma till rätta med. En följd av detta är att otryggheten ökar.

ÅTGÄRDER FÖR ATT BEKÄMPA BROTTSLIGHET

En av de frågor som prioriteras högst just nu är att bekämpa kriminaliteten och otryggheten. Det finns inga enkla lösningar utan en kombination av åtgärder och initiativ kommer att behövas.

Magnus Lindgren tycker sig, genom Tryggare Sveriges arbete ute på fältet, se en betydligt större samsyn om att vi har en mycket allvarlig situation att hantera, än han gjorde för tio år sedan. Samsynen förenklar arbetet framåt.

Ur ett näringslivsperspektiv finns flera viktiga insatser som skulle kunna bidra till att vända utvecklingen, enligt experterna som intervjuats för detta kapitel.

PRIORITERA MÄNGDBROTTEN

Mängdbrotten eller livkvalitetsbrotten är isolerade inte så allvarliga men den stora mängden gör dem i längden svåra att hantera och är en viktig anledning till den ökande otryggheten i samhället.

> *Om man tänker sig att brottsligheten är en pyramid med mängdbrotten i basen och den grövsta kriminaliteten i toppen, så fokuserar samhället på toppen, trots att mängdbrotten berör fler. Vi behöver ändra inriktning och angripa mängdbrotten som gör drabbar folk i vardagen och gör att de känner sig otrygga, säger Per Geijer.*

I New York inledde man under 1980-talet så kallad ”broken window policing”, som innebar att man höll efter småbrott och visade att samhället inte hade någon tolerans för till exempel klottrare eller plankare i kollektivtrafiken. Erfarenheterna av denna metod har på flera sätt varit positiv.

> *Den här typen av gränssättande polisiär verksamhet är nödvändig. I kombination med mjukare ”community policing” som betonar den relationsbyggande lokala närvaron, säger Magnus Lindgren.*

FÖRSÄMRA FÖRUTSÄTTNINGARNA ATT BEGÅ BROTT

Brottsligheten är så omfattande i Sverige såväl som i Europa att det är naivt att tro att vi med nya lagar, fler poliser och mer resurser ska kunna arrestera oss ur problemen, framhåller Magnus Lindgren, som efterlyser ett paradigmskifte i synen på brottslighetens orsaker.

> *Vi måste förhindra att brott begås. I vårt land har det funnits en naiv uppfattning om att man begår brott för att man är fattig. Den uppfattningen är en skymf mot de 98 procent fattiga som inte begår några brott. Man begår brott därför att man kan. Genom så kallad situationell prevention kan man minska tillfällena då brott kan begås, säger Magnus Lindgren.*

Situationell prevention innebär att man systematiskt begränsar faktorer som underlättar brott, exempelvis genom fysisk utformning av platser, social kontroll, väktare, poliser, boendevärdar etc.

I Sverige har vi, enligt Magnus Lindgren, varit dåliga på att arbeta med förutsättningarna för att begå brott i den fysiska miljön. Social prevention är också verkningsfull och innebär att man försöker påverka förutsättningar i uppväxtförhållandena på ett sätt som minskar risken för att unga ska dras in i kriminalitet.

> *Vi behöver snabba åtgärder, att utbilda nya poliser tar fem år innan de gör någon skillnad, och innan domstolarna börjar tillämpa nya lagar tar det också flera*

år. Detta löser inga problem här och nu, därför ser vi negativt på utvecklingen, säger Magnus Lindgren.

”POLISIFIERA” DE UTSATTA OMRÅDENA

Polisens lokala närvaro har minskat generellt över tid, samtidigt har kriminaliteten ökat, särskilt i de utsatta områdena. Ett sätt att snabbt ”ta tillbaka” dessa områden kan vara att öka polisnärvaron.

Vi föreslår i Tryggare Sveriges åtgärdsprogram att omedelbart avsätta 3 000 poliser till de utsatta områdena. Det viktiga är den fysiska närvaron dygnet runt, även om etableringen bara är en byggbarack. Detta vet vi från militära missioner utomlands, säger Magnus Lindgren.

När den polisiära närvaron väl är etablerad blir det lättare att i senare faser engagera fastighetsägare och näringsliv genom platssamverkan för att skapa tryggare områden.

Tryggare Sverige har skapat ett oberoende kunskapscentrum för platssamverkan eftersom man anser att det är ett problem att företagen inte får vara med och ta ansvar för tryggheten i den svenska modellen. Näringslivet och kommunen är de viktigaste krafterna för att återskapa ordning efter att Polisen etablerat ordningen i ett område.

BÄTTRE STATISTISKT UNDERLAG

Bra beslut baseras på fakta. Den Nationella trygghetsundersökningen, NTU, och NTU Lokal ger inte tillräckligt bra underlag för att initiera ett kunskapsbaserat brottsbekämpande och brottsförebyggande arbete.

Brott begås alltid på en plats och den platsen behöver dokumenteras så att det är möjligt att teckna en bild av brottslighetens och otrygghetens utseende på lokal nivå, i olika kommundelar och områden. Den kunskapen finns inte tillgänglig idag.

HUR KAN FÖRETAG UNDVIKA ATT UTSÄTTAS FÖR BROTT?

Hur kan man som företagare skydda sig mot brott? En grundregel som Svensk Handel har är att företagare behöver ha ett gott försäkringsskydd och uppfylla de lagar och krav som ställs på verksamheten. Dessutom är det viktigt att inte lockas att beblanda sig med den svarta ekonomin, det ökar annars risken för att utsättas för utpressning och på sikt tvingas in i brottrelaterad verksamhet.

Att som företagare aktivt försöka öka sin egen och medarbetarnas medvetenhet om risken att utsättas för brott är en bra grund för det kontinuerliga säkerhetsarbetet. En första åtgärd kan vara att se till att det finns galler för fönstren och att se över låsen så att de är säkra samt att inga obehöriga har tillgång nycklar eller koder.

Mer komplicerat, men viktigt, är att se över företagets cybersäkerhet och informationssäkerhet i bred mening. Det kan till exempel gälla att uppdatera programvaror och hålla

ordning på vilka som har inloggningsuppgifter till systemet. Det är också viktigt att etablera säkerhetsrutiner för att undvika att medarbetare klickar på okända länkar eller lockas att göra felaktiga utbetalningar.

Det finns många brottsdrabbade företagare som man kan få stöd och råd av. Det finns ingen anledning att uppfinna hjulet på nytt, det är bättre att ta del av andras erfarenheter. Att organisera sig i företagarföreningar och branschorganisationer är ett bra sätt att stärka sig själv och dra lärdom av andra i samma situation. Branschorganisationerna ger också säkerhetsutbildningar för medlemsföretagen och samlar mycket bra information på sina hemsidor.

Hur kan du skydda dig och ditt företag?
Några av Per Klingvalls praktiska råd:

- → Tänk preventivt och installera både det fysiska och digitala skyddet efter de normer som ges ut av bland annat SSF Stöldskyddsföreningen.
- → Besök SSF Stöldskyddsföreningens webbsida och ta del av säkerhetsguiderna där. De beskriver både fysiska och digitala normer och skydd. Där finns även en helpdesk om du tror du drabbats av bedrägerier.
- → Delta i Grannsamverkan, där hjälper man varandra och det har du nytta av som företagare också.
- → Gå in på www.ssfcybersäkerhet.se och testa din grundläggande IT-säkerhet
- → Ladda ned Svensk Handels app om du tillhör handeln.
- → Polisanmäl alltid brott.

Fotnoter

39 https://sv.wikipedia.org/wiki/ABC-stad

40 https://www.folkhalsomyndigheten.se/publicerat-material/publikationsarkiv/d/den-svenska-narkotikasituationen-2019/?pub=66860


command
option

KAPITEL 4

Den som är uppkopplad är också sårbar – cyberbrott

En mycket stor del av de brott svenska företag utsätts för varje år sker utan att gärningsmännen har någon fysisk kontakt med sina offer. Cyberbrott är en bred kategori, innefattande allt ifrån sabotageaktioner till stöld av värdefull data eller narkotikaförsäljning via nätet.

För att bättre förstå denna typ av brott och hur vår digitaliserade vardag öppnar nya möjligheter för kriminella har vi intervjuat två experter på området.

Vi inleder med ”cybersäkerhetsgurun” Anne-Marie Eklund Löwinder, säkerhetschef vid Internetstiftelsen, som bland annat ansvarar för den svenska toppdomänen .se och för .nu. Hon är dessutom en av 14 personer i världen som har behörighet att generera de digitala krypteringsnycklar som krävs för att domännamnsystemet DNS (Domain Name System), och därmed själva internet, ska fungera på ett säkert sätt.

DIN DATOR KAN VARA EN ZOMBIE!

Vilka hot står då internet som sådant, och alla vi som är beroende av internet, inför? Vad är det som kan hända om inte säkerheten upprätthålls?

> *De vanligaste brottstyperna är utan tvekan olika typer av bedrägerier, men mer storskaliga hot kan också uppstå genom att stora mängder datorer kapas och används som ”zombies” i ett så kallat botnet. Datorerna bildar ett robotiserat nätverk av datorer som kan användas för att attackera olika mål. Vanligen handlar det då om överbelastningsattacker, till exempel att hundratusentals datorer besöker någon viss webbplats tills den bryter samman av belastningen, berättar Anne-Marie Eklund Löwinder.*

Det förekommer även att datorer kapas för att kaparna ska kunna använda datorkraften i ett stort antal datorer för att utvinna kryptovaluta, en process som ger en viss ersättning för att möjliggöra transaktioner med till exempel bitcoin. Det är heller inte bara datorer som kan kapas, även mobiltelefoner, webbkameror och annan utrustning kopplad till internet kan tas över om någon lyckas ta sig in i ditt system olovligen.

Det speciella med denna typ av attacker är att de personer vars datorer deltar i attackerna ofta inte har en aning om att så är fallet, de märker helt enkelt ingenting. Offren blir med andra ord verktyg för brottsligheten, samtidigt som de själva är just brottsoffer.

På senare år har flera mycket omfattande cyberattacker begåtts mot stora företag och verksamheter, på ett sätt som

demonstrerar den enorma skada denna typ av kriminalitet kan åsamka samhället. Ett av de mer spektakulära fallen var när rederikoncernen Maersk år 2017 utsattes för en attack med så kallad ransomware (kidnappningsprogramvara), som låste företagets hela IT-system.

Då Maersk, som många andra företag, är helt beroende av internet och digitala lösningar för sin verksamhet satte detta angrepp en enorm press på företaget. Maersk installerade om hela sitt nätverk, innefattande 4 000 servrar och 45 000 datorer. Detta tog tio dagar och kostade förstås stora pengar.

Maersk var länge ytterst sparsamt med att berätta om hur man gått till väga för att hantera problemet, men under World Economic Forum 2018 berättade företagets styrelseordförande Jim Hagemann Snabe om de dramatiska tio dagar när man var tvungen att hålla verksamheten igång manuellt i väntan på att IT-systemet skulle kunna tas i drift igen:

> *”Tänk er ett företag som har skepp med tio till tjugo tusen containrar på väg in i hamnen var femtonde minut, i tio dagar, samtidigt som du inte har någon IT. Det är nästan omöjligt att föreställa sig.”*[41]

Maersk uppger att man på detta sätt lyckades upprätthålla 80 procent av verksamheten under denna period, trots detta orsakade cyberattacken företaget förluster på motsvarande 3 miljarder kronor under tio dagar.

Liknande attacker har även gjorts mot stora offentliga verksamheter, berättar Anne-Marie Eklund Löwinder. För en tid sedan gjordes en motsvarande attack med ransomware mot sjukhus i Frankrike. Där utnyttjades svagheter i en

programvara som många sjukhus använde för att låsa IT-systemen och därmed stoppa verksamheten vid hela 120 sjukhus samtidigt.

I fall som detta är det uppenbart att skadan av cyberattacker inte bara är ekonomisk utan även orsakar mänskligt lidande och i förlängningen även kan resultera i dödsfall.

STORA MEN SVÅRBEDÖMDA KOSTNADER

I Svenskt Näringslivs undersökning uppskattas de direkta kostnaderna för brott mot svenska företag till närmare 50 miljarder kronor per år, varav cyberbrottslighet av olika slag uppskattas leda till jämförelsevis låga kostnader.[42] Men frågan är om detta verkligen speglar de verkliga kostnaderna?

Anne-Marie Eklund Löwinder menar att mörkertalet av flera skäl är mycket stort för denna typ av brott. Dels tar det ofta lång tid innan intrång i företags system upptäcks, även om tiden minskat något på senare år. Dels kan det vara svårt för drabbade företag att veta vilken information inkräktarna kommit åt, och därmed bedöma vilka skador attacken orsakat.

> *Det är alltid svårt att bedöma kostnader, men det vi vet är att det kostar extremt mycket pengar. Globalt sett bedöms cyberbrott kosta ungefär 600 miljarder dollar, så det är enorma belopp och en mycket lönsam affär för dem som begår brotten. Risken att åka fast är minimal och du behöver knappt använda din egen dator utan använder andras. Det är en oemotståndlig affärsmodell, helt enkelt.*

Ett ytterligare dilemma gäller företags möjligheter att försäkra sig mot angrepp av detta slag. Även företag som återkommande utsätts för stölder och andra fysiskt mer påtagliga brott kan ha svårt att teckna försäkringar, vilket beskrivs i kapitel 1. Ett grundläggande problem är just att det är mycket svårare att bedöma kostnaderna för ett dataintrång än för inbrott och stölder i företagets lokaler.

Dessutom tillkommer, enligt Eklund Löwinder, problemet att försäkringsmarknaden på detta område är ganska outvecklad.

> *Cyberförsäkringsmarknaden är inte riktigt mogen än. Om du tittar på försäkringsvillkoren så kommer du se att om försäkringsbolaget hittar minsta exempel på att du inte jobbar med säkerhet på det sätt de vill så får du ingen ersättning alls. Det kommer säkert att utvecklas med tiden, men jag tror inte vi är där ännu. Man kan t ex tänka sig att företag som har vidtagit vissa säkerhetsåtgärder, som installerat brandväggar, uppdaterat operativsystem etc får rabatt på premien.*

PRAKTISKA TIPS FÖR MER ROBUSTA SAMHÄLLSFUNKTIONER

Hur kan då stora samhällskritiska verksamheter, oavsett om de är privata företag eller offentliga verksamheter, skydda sig från denna typ av angrepp? Hur undviker vi att vårt samhälles stora beroende av internet utnyttjas för att skada oss? Hur kan våra system göras mer robusta?

Eklund Löwinder ger några handgripliga tips som kan minska utsattheten och begränsa skadan för den som ändå blir drabbad:

FÖR DET FÖRSTA att dela upp stora verksamheters nätverk i flera separata delar, skapa celler som kan isoleras från varandra så att ett angrepp inte lika lätt kan spridas sig i hela systemet.

FÖR DET ANDRA att begränsa enskilda personers behörighet till systemet, så att ingen har tillgång till precis allt utan endast det han/hon behöver för sitt arbete. På så sätt kan intrång som görs via någon enskild medarbetare inte nå hela nätverket.

FÖR DET TREDJE att genomföra regelbundna tester av verksamhetens säkerhetssystem för att visa huruvida det är möjligt för en utomstående att ta sig in i systemet.

För det fjärde samma tips som gäller för mindre företag och privatpersoner: se till att uppdatera operativsystem och virusskydd, använd säkra lösenord och en bra brandvägg.

Anne-Marie Eklund Löwinder inser att de här enorma angreppen kan skapa känslan att det är omöjligt att skydda sig, men menar att slutsatsen är den omvända: alla behöver sopa rent framför sin egen dörr och göra det bästa man kan utifrån sina förutsättningar.

> *Man ska komma ihåg att behoven ser väldigt olika ut beroende på vilken verksamhet du har. Behöver du ständig tillgänglighet, då krävs redundans* [*överskottskapacitet, red anm*] *och flera infrastrukturer. Är sekretessen viktigast, då behövs stark kryptering både för transport och lagring av data. Är riktigheten i*

informationen avgörande, ja då är det datakvalitet som borde vara i fokus.

Varje företag behöver ställa sig frågan: vad är det i vår verksamhet som vi står och faller med, vad är det värsta vi skulle kunna drabbas av? Utifrån det kan företaget göra sin riskbedömning, definiera vilka risker man är berett att leva med och vilka man absolut måste skydda sig mot.

En viktig insikt är också att varken stora eller små företag rimligen kan skydda sig mot alla risker. Skydd har också en kostnad, och vissa risker kommer att vara alldeles för dyra att skydda sig mot. Man kan ju inte lägga mer resurser på att skydda sig än värdet på det man riskerar. Då är det viktigare att man har en plan för vad man ska göra om något inträffar, menar Eklund Löwinder.

Hon menar också att många myndigheter tyvärr lägger alldeles för små resurser på sin IT-säkerhet och IT-drift, och att de därför är allt för dåligt skyddade mot angrepp.

Jag såg nyligen en siffra på att svenska myndigheter varje år lägger ungefär 1,5-2 procent av sin budget på IT och IT-drift. Motsvarande siffra i banksektorn är snarare runt 20 procent, så det är en stor skillnad. Det avspeglar förstås hur enormt beroende bankerna är av fungerande IT, men det kommer rapport efter rapport om att många myndigheter använder alldeles för dålig säkerhet och för gamla IT-miljöer. Men ändå sätter ingen ner foten och säger att detta måste fixas.

Vems är då ansvaret att IT-säkerheten blir bättre i samhällskritiska funktioner i Sverige? I slutänden är detta förstås ett politiskt ansvar, där Eklund Löwinder menar att regeringen till exempel skulle kunna ta ett betydligt större ansvar för att i regleringsbrev för olika myndigheter tydligt markera att informationssäkerhet är prioriterat och att myndigheten måste uppfylla de föreskrifter som finns från Myndigheten för samhällsskydd och beredskap (MSB).

CYBERATTACKER EN DEL AV VÄRLDSPOLITIKEN

En allt mer aktuell fråga i vår globaliserade ekonomi är hur företag ska se på leverantörer som är baserade i auktoritära stater.

På senare tid har detta diskuterats både i näringslivet och politiken. Frågan är hur man som företagare bör se på detta, ska ett företag från en auktoritär stat per automatik ses som en förlängning av regimens intressen, och vågar man då göra affärer med sådana företag?

Anne-Marie Eklund Löwinder menar att vi i praktiken inte har något annat val än att i en grundläggande mening lita på företag baserade i länder som Kina, även om det finns kända problem med cyberattacker från kinesisk sida.

> *Det finns till exempel inte chipsfabriker i särskilt många länder, så alldeles oavsett om du köper en produkt som kanske är monterad i Frankrike så kommer den sannolikt ändå att innehålla komponenter som är tillverkade i Kina.*

Hon understryker samtidigt att man bör vara medveten om att diskussioner om säkerhetspolitiska aspekter på handel – som mellan USA och Kina – ofta innehåller moment av protektionism. Som mediekonsument behöver man lära sig genomskåda vad som är reella säkerhetsproblem och vad som är försök att begränsa motpartens marknad.

Vill du veta mer om cybersäkerhet?
Några av Anne-Marie Löwinders tips:

- → Internetkunskap.se , Internetstiftelsen i Sveriges webbplats med praktiska tips om bl a källritik på nätet, cyberbrott, desinformation och integritet
- → Boken Informationssäkerhet av Per Oscarsson (Studentlitteratur 2019)
- → Boken Bli säker: IT-säkerhet för alla Av Karl Emil Nikka (Nikka Systems Sverige 2018)
- → Podden Säkerhetssnack
- → Bruce Schneiers nyhetsbrev Crypto-Gram

DARKNET – ANONYM KRIMINELL MASSMARKNAD

Vad kan då det svenska rättssystemet göra för att bekämpa denna brottslighet som rör sig fritt över gränserna och ofta inte är beroende av fysisk kontakt med sina offer? För att få en fördjupad bild av vi talat med kriminalinspektör Jan Olsson, en av Sveriges mest erfarna poliser på området.

Olsson arbetar idag på Nationellt IT-brottscentrum vid polisens Nationella operativa avdelning (NOA), har 28 års

erfarenhet som polis och det senaste decenniet inriktat sig särskilt på att kartlägga och utreda brottslighet som begås med hjälp av internet.

Till att börja med kan konstateras att den internetrelaterade kriminaliteten inte i första hand riktar sig mot företag utan mot privatpersoner, som exempelvis narkotikahandeln via Darknet. Till detta ska läggas stora mängder internetrelaterade sexualbrott mot barn som också involverar internet och i regel sker via Darknet.

Svensk polis medverkade hösten 2019 i ett stort tillslag mot en gammal bunker i Tyskland som sedan 10 år fungerat som illegal serverhall för framförallt narkotikaförsäljning men även barnpornografi och verktyg för dataintrång.[43] Denna typ av tillslag är viktiga för att slå sönder den kriminella infrastrukturen, men kräver också mycket stora resurser för att utreda, konstaterar Jan Olsson.

> *Den mängd data med bevismaterial vi får tillgång till från bara den här utredningen motsvarar 6 Tb data*[44] *per dag sju dagar i veckan. Utredningen av materialet från bara de här servrarna kommer att bli klar långt efter min pension, det tar mycket av vår tid att gå igenom sådana mängder information.*

Hur fungerar då den kriminella digitala ekonomin via Darknet? Hur kan det komma sig att brottslingar lyckas hålla sin verksamhet dold så länge? Jan Olsson beskriver hur stora delar av den kriminella ekonomin är uppbyggd kring så kallad kryptovaluta, som ger möjlighet att köpa och sälja varor och

tjänster anonymt på ett sätt som normalt sett inte är möjligt med vanliga pengar.

> *Själva köpet av valutan sker normalt sett på det öppna nätet, att köpa kryptovaluta är ju inte olagligt. Men själva försäljningsställena av det man sedan köper för sin kryptovaluta, de finns sedan på Darknet. Bland det som säljs finns bland annat narkotika, vapen, kreditkortuppgifter och skadlig kod av olika slag. Så man kan säga att Darknet är en samling marknadsplatser som möjliggör många olika typer av brottslighet.*

Olsson beskriver hur Darknet som marknadsplats är mycket sofistikerad och lyckas upprätthålla ett visst mått av förtroende mellan köpare och säljare trots att det mesta som sker är illegalt. Exempelvis finns en utvecklad kundtjänstfunktion där köparen snabbt kan få svar på frågor om varför den kod för att infiltrera banker inte fungerar som avsett och vad man ska göra för att det ska bli rätt.

Vad gäller just skadlig kod är detta en verksamhet som utvecklats från att vara något bara de allra mest tekniskt kunniga klarade av till att bli ett slags massmarknad där även kriminella med måttliga IT-kunskaper kan köpa kod som är enkel att använda för att exempelvis stjäla kortuppgifter eller göra intrång hos olika företag. Ungefär som om en inbrottstjuv skulle köpa en apparat som gör att även personer med begränsade tekniska kunskaper kan koppla ur avancerade inbrottslarm.

Den skadliga koden kan ofta även hyras, genom att man betalar för att kunna använda den i till exempel en vecka och

koden därefter slutar fungera. Att verktygen för även avancerade dataintrång har blivit så lättanvända är en viktig förklaring till att denna typ av brottslighet har växt så kraftigt på senare år.

KAPPLÖPNING MELLAN POLISEN OCH CYBERBROTTSLINGAR

Det är naturligtvis en utmaning för svensk polis att hålla jämna steg med en brottslighet som växer i takt med den tekniska utvecklingen och nya kategorier brottslingar lockas till en verksamhet de uppfattar erbjuda låg risk och snabba pengar.

Polisen har fått i uppdrag att höja IT-kompetensen hos 30 000 polisanställda, tiden är förbi då cyberbrott var något som kunde utredas av en liten grupp experter. Teknikens utveckling och användarvänlighet gör att allt fler brott på ett eller annat sätt är internetrelaterade. Utredning av elektroniska spår i datorer eller mobiltelefoner är en del av väldigt många brottsutredningar även om själva handlingarna begåtts i den fysiska världen.

De poliser som är specialiserade på denna typ av brott är ganska få, men de blir allt fler. När Nationellt IT-brottscentrum grundades 2015 jobbade 35 anställda i verksamheten, i skrivande stund har enheten växt till cirka 100 personer. Dessutom har regionala bedrägericentra byggts upp – de flesta bedrägerier är IT-brott – som ska bemannas med mellan 35 och 80 anställa i var och en av polisens sju regioner.

En särskild utmaning är att hålla jämna steg med den metodutveckling som sker i den kriminella verksamheten på IT-området.

När vi på NOA utreder brott sker det främst för att kartlägga de metoder som använts och dokumentera vad som krävs för att kunna gå i mål med utredningarna, sen ska den kunskapen föras vidare till regional nivå där det mesta av det utredande arbetet sker. Och en del enklare brott ska kunna lösas på lokal polisområdesnivå, syftet är att höja kompetensen i hela organisationen för att möta den anstormning vi ser, beskriver Jan Olsson.

Samtidigt som polisens satsning på detta område ökat kraftigt är rekrytering av tillräckligt kompetenta medarbetare till de olika tjänsterna en flaskhals. Det är inte många som har tillräckliga kunskaper för att kunna bekämpa komplexa cyberbrott, och av dem som har denna kompetens är det många som lockas till jobb i den privata sektorn där de ekonomiska villkoren ofta är bättre.

ALLT MER SPECIALISERAD, OFTA INTERNATIONELL VERKSAMHET

De cyberbrott som begås blir också allt mer specialiserade och tekniskt specialiserade. Ett exempel är användningen av så kallad ransomware (kidnappningsprogramvara), där brottslingarna blivit betydligt mer pricksäkra i vilka företag som angrips, vilka metoder som används och vilka lösensummor som begärs. Jan Olsson beskriver hur skillnaderna kan se ut i praktiken.

Förr var det vanligt att attackerna med ransomware skickades ut till massor av företag och privatpersoner och begärde låga lösensummor, till exempel motsvarande 3 000 kronor i bitcoin. Idag ser vi allt mer av det vi kallar ”spearfishing”, dvs angreppen fokuserar på företag som dels har pengar och dels är starkt beroende av sina filer. Då kan kraven på lösensumman vara kanske 10 miljoner kronor. Offren är färre idag, men den totala förtjänsten för brottslingarna är högre.

Något som också driver utvecklingen mot allt mer komplexa brott är det faktum att även stater och statsunderstödda verksamheter är aktiva på denna kriminella marknad. Dessa grupper kallas ofta APT (Advanced Persistent Threat)[45], organiserade hemliga nätverk av hackers som normalt sett jobbar på uppdrag av stater och försöker ta sig in obemärkt och ligga kvar i system under lång tid. De är då inte främst ute efter pressa någon på pengar, utan att stjäla affärshemligheter.

Enligt Jan Olsson är det också tydligt vilka länder som är ansvariga för denna typ av attacker.

Många av dem kommer från Ryssland och är i praktiken en del av GRU, Rysslands militära underrättelsetjänst. Det är ganska lätt att se. Men vi ser också attacker från grupper knutna till Nordkorea, särskilt attacker mot banker och växlingsinstitut för att helt enkelt finansiera sin vapenindustri. Det här är ofta enormt skickliga personer, som är väldigt svåra för enskilda företag att stänga ute. Om de vill in, kommer de förr eller senare att lyckas.

Att cyberbrotten ofta sker från utlandet gör dem också betydligt svårare att utreda. Jan Olsson beskriver att det är ovanligt att komplexa brott av detta slag begås av personer i Sverige. Istället är angriparna ofta baserade i länder som Sverige har ett dåligt polisiärt samarbete med.

Ett problem är att det inte är säkert att själva handlingen som utgör ett brott i Sverige, exempelvis ett dataintrång, måste vara ett brott även i Ryssland. Det gör det mycket svårare att få personer utlämnade till Sverige, även om de bevisligen har begått brott mot svenska företag.

Detta vet också de kriminella mycket väl, därför ser ryska hackers ofta till att geoblockera den kod de skapar – det vill säga göra den oanvändbar mot ryska företag. På så vis minskar risken att rysk polis intresserar sig för deras verksamhet kraftigt.

Vad ska man då tro om denna typ av brott framöver? Kommer cyberbrotten per automatik att fortsätta öka i takt med den tekniska utvecklingen? Jan Olsson tror att det kommer att ske en ökning men tror och hoppas att det sedan planar ut:

> *Det kommer naturligtvis att öka i framtiden, i takt med att tillgängligheten till internet fortsätter öka och allt fler får internettillgång via smartphones. Samtidigt tror och hoppas jag att vi når en kulmen när vi skaffar oss ett mer genomtänkt förhållningssätt till allt det vi gör på internet. Vi måste lära oss att brott via internet får väldigt konkreta fysiska konsekvenser för andra, då finns hopp om att det hela planar ut.*

Vad kan då göras för att minska svenska företags utsatthet inför denna utveckling? Vad kan vi lära av andra länder?

> *En verklig förebild är England, där det finns en stor avdelning med hälften poliser och hälften bankanställda i samma byggnad för att gemensamt kunna spåra och gripa personer som ligger bakom cyberbrott. Det är oerhört framgångsrikt. En liknande funktion finns i Nederländerna, där näringslivet är med och finansierar det brottspreventiva arbetet. Även Danmark och Norge har kommit längre än vad vi har gjort.*

Jan Olsson menar att Sverige kommit långt vad gäller att få berörda myndigheter att samarbeta, men just vad gäller relationen till näringslivet har vi en bra bit kvar. Alla har ett gemensamt intresse av att den här typen av brott minskar.

Så undviker du utpressning på nätet.
Jan Olssons praktiska tips för att avslöja ransomware:

- → Var misstänksam. Är du helt säker på att den person som kontaktar dig är den han/hon säger?
- → Ber personen dig att göra något ovanligt? En första varningsklocka.
- → Uppmanas du klicka på en länk eller ladda ner en fil? En andra varningsklocka.
- → Om du är det minsta osäker: ring och dubbelkolla (inte till numret i mailen/SMS:et, det kan vara bedragarens nummer)
- → Vill du undvika fler brottsförsök: skaffa en säkerhetslösning som sållar bort försök till ransomware

Fotnoter

41 https://techworld.idg.se/2.2524/1.696700/nonpetya-maersk

42 Svenskt Näringsliv, Brottslighetens kostnader 2020, 2020. https://www.svensktnaringsliv.se/material/rapporter/brottslighetens-kostnader-2020pdf_1143423.html/BINARY/Brottslighetens%20kostnader%202020.pdf

43 https://www.dn.se/nyheter/varlden/polisen-slog-till-mot-darknet-servrar-i-tyskland/

44 En TB (terabyte) motsvarar en miljon megabyte

45 https://en.wikipedia.org/wiki/Advanced_persistent_threat


20
EURO

KAPITEL 5

Vem kan man lita på?

Bedrägerier i stort och smått

Att människor litar på varandra är av avgörande betydelse i varje samhälle. Hög tillit är särskilt avgörande i näringslivet, för att våga göra affärer med någon måste man lita på att han eller hon kommer att hedra sin del av överenskommelsen.

I internationell jämförelse är Sverige, som konstaterades i kapitel 1, ett land där tilliten är mycket hög. Det gäller både människors tillit till stat och myndigheter, och tilliten människor emellan. Samtidigt är det dessvärre vardag för svenska företag att någon försöker lura dem.

Bedrägerier är ett av de allra vanligaste brotten som svenska företag utsätts för. I Svensk Handels Trygghetsbarometer – i en återkommande mätning bland butikschefer eller butiksansvariga för tredje kvartalet 2019 svarar drygt var femte (21 procent) av de tillfrågade utsatts för bedrägerier eller bedrägeriförsök bara den senaste veckan.[46]

Det enskilt vanligaste bedrägeriförsöket i svenska butiker är enligt denna undersökning att en kund byter ut en varas prismärkning för att få ett lägre pris, men även kortbedrägerier eller försök med stulna eller manipulerade kvitton är vanligt.

Ofta är det nog också så vi tänker oss bedrägerier mot företag: någon försöker lura till sig en vara gratis eller till ett orättmätigt lågt pris. Men detta är bara en mycket liten del av de bedrägerier som drabbar svenska företag varje år.

VÄRLDENS ÄLDSTA YRKE?

Nigel Iyer är en ledande expert på hur företag kan upptäcka och förhindra bedrägerier. Han har arbetat i 25 år som rådgivare och analytiker på området och skrivit en rad böcker på temat, senast ”How to Find Fraud and Corruption – Recipes for the Aspiring Fraud Detective”.

Han är en av grundarna av startupbolaget B4 Investigate, där han utvecklat en metod och applikation för att lättare bedöma kostnaden för bedrägerier och hur företag kan öka sin lönsamhet genom att bekämpa dem.

Nigel Iyer beskriver att bedrägerier som fenomen är ”lika vanligt som en vanlig förkylning och lika gammalt som pyramiderna”. Kanske kan man rentav säga att bedragare är världens äldsta yrke?

Iyer beskriver hur man förenklat kan tala om sju olika typer av bedrägerier mot företag:

- Leverantörer som försöker lura sina kunder
- Kunder som försöker lura sina leverantörer
- Mutor och ”kickbacks”, i ena eller andra riktningen
- Manipulation av bokföring
- Frontföretag och svarta pengar
- Stöld och bedrägeri mot företaget från anställda
- Stöld och bedrägerier från utomstående (hackers t ex)

Av flera skäl är det svårt att uppskatta kostnaden för alla dessa bedrägerier, den är ibland svår att mäta och många företag är ovilliga att polisanmäla. Iyer nämner som exempel att den brittiska regeringen uppskattat att bedrägerier i Storbritannien generellt sett motsvarar 3,6 procent av BNP. När motsvarande uppskattningar görs för företag brukar nivåerna handla om en till sju procent av omsättningen.

Samtidigt varierar utsattheten för bedrägerier naturligtvis kraftigt mellan olika branscher, bland särskilt utsatta branscher internationellt brukar nämnas t ex kapitalintensiva byggprojekt eller banker och andra finansiella företag.

I grund och botten kan man säga att bedrägerier finns överallt i samhället, men eftersom bedragare är ute efter pengar tenderar bedrägerier att vara vanligast där det finns stora summor pengar i omlopp, konstaterar Nigel Iyer.

ALLA ÄR POTENTIELLA BEDRAGARE

Vilka är det då normalt sett som ligger bakom alla dessa bedrägerier? Iyer är skeptisk till de vanligaste sätten att beskriva typiska bedragare, som han menar ofta ger en allt för ensidig bild av vem den typiska bedragaren är.

Förr i tiden, när jag började jobba med det här, talade många om att man skulle hålla utkik efter misstänkt dyra bilar på företagets parkering och att de som låg bakom bedrägerierna var psykopater som kunde kännas igen på sina personlighetsdrag. Men det där tror

jag inte alls på, de allra flesta bedragare är normala människor som rationaliserar ett olagligt beteende och själva intalar sig att vad de gör är OK.

Iyer beskriver hur beteendeforskningen visar att de allra flesta av oss, i alla fall i liten skala, är potentiella bedragare eller fuskare. Alla kan vi tänka oss att göra sådant som inte är tillåtet, för att det gynnar oss. Det handlar för de allra flesta om småsaker, som att t ex glömma att betala en tågbiljett och sedan inte göra det i efterhand heller.

En viktig insikt i arbetet mot bedrägerier är att mekanismerna är de samma när det gäller mer allvarliga situationer, vi har alla en tendens att rationalisera våra handlingar som OK. Det handlar alltså inte om att identifiera någon viss personlighetstyp, utan om att bygga rutiner och kultur i företagen som gör att otillåtet agerande kan förhindras eller upptäckas.

I sina böcker och föreläsningar talar Nigel Iyer ofta om att alla kan bli ”fraud detectives”, dvs att vi alla kan lära oss att upptäcka bedrägerier och oegentligheter. Företag där många medarbetare har ögonen öppna för sådant som verkar misstänkt kommer att klara sig bättre.

De flesta har redan förutsättningar för att upptäcka bedrägerier, det gäller bara att vara uppmärksam. Jag brukar prata om att man måste ha de röda glasögonen på, att vara lite extra uppmärksam och nyfiken på vad som sker. Motsatsen är att ha de blåa glasögonen på, och utgå från att det vi ser är OK. I privatlivet är detta ofta självklart, men som medarbetare utgår vi lätt från att sådant är någon annans ansvar.

Han menar att vi alla behöver bli bättre på att ”tänka som en tjuv”, att använda vår fantasi och fundera: hur skulle den här situationen kunna utnyttjas om någon är ute i onda syften? Vilka brister finns, som skulle kunna skapa problem för mitt företag?

Så långt den enskildes ansvar. Men vad är det viktigt för företag att tänka på för att undvika att drabbas av bedrägerier? Vad kan företagen göra? Och vilka misstag är det viktigt att undvika?

Nigel Iyer pekar också på några klassiska misstag som även mycket stora företag ibland kan göra.

FÖR DET FÖRSTA – att lita på att lagar och regler räcker. Dilemmat med detta är att ett komplext regelverk tvärtom kan innebära fler kryphål för den som vill utnyttja bolagets resurser på ett otillåtet sätt.

FÖR DET ANDRA – att lita på att bolagets revisorer ska upptäcka eventuella missförhållanden. Detta är normalt sett inte revisorernas jobb, så här finns ett stort gap i förväntningarna.

FÖR DET TREDJE – att lita på ”visselblåsare” i organisationen. Problemen behöver dock vara mycket allvarliga innan en enskild medarbetare är villig att ta en stor personlig risk och rapportera något som till en början kanske inte ens kommer att tas på allvar.

FÖRETAGSKULTUREN BÄSTA SKYDDET

Istället för att lita på att företaget är skyddat från bedrägerier genom att ”någon annan” – i eller utanför organisationen – upptäcker missförhållanden menar Iyer att detta är en

kulturell fråga som bolagets högsta ledning behöver ta på allvar. Arbetet mot bedrägerier måste bli en del av företagets kultur, inte en extern tjänst.

> *Vad som krävs är en företagskultur där det uppfattas som goda nyheter om någon i företaget har avslöjat försök till bedrägeri och agerat utifrån det. Idag är det ofta tvärtom: det uppfattas som dåliga nyheter och därför något som ledningen i det längsta skjuter ifrån sig. Det är en naturlig instinkt att inte vilja se problem, därför krävs en kultur som uppmuntrar avslöjandet av problem.*

De avgörande argumenten för att det är goda nyheter om någon upptäckt försök till bedrägeri är ekonomiska. Skador på företagets anseende och lönsamhet kan lättare förhindras om företaget upptäcker bedrägerier i tid. Trots att förekomsten av bedrägeri är ett besvärligt problem att hantera i en organisation är det förstås positivt att det avslöjas.

Även på den politiska nivån krävs en förändrad attityd och kultur, menar Nigel Iyer. Ett vanligt misstag är att politiker i västvärlden tror att deras länder är mer eller mindre fria från denna typ av problem därför att de rankas bättre än många utvecklingsländer vad gäller förekomsten av korruption etc.

> *Många beslutsfattare feltolkar Transparency Internationals Corruption Perception Index[47], och tror att den här typen av problem bara finns i fattiga länder. Ofta är det tvärtom – bedrägeri och korruption söker sig dit pengarna finns, så även om problemen är vanligare i*

många fattiga länder är det i rika länder som bedragare kommer över riktigt stora belopp.

Det är viktigt att påpeka att bedrägerier kan se väldigt olika ut och begås av väldigt olika typer av förövare. Ett allt vanligare problem även för svenska företag är kriminella organisationer som bedriver olaglig verksamhet på ett sätt som för ett otränat öga kan se helt legitimt ut.

MYNDIGHETERNA STEGET EFTER BROTTSLINGARNA

Denna typ av professionell ekonomisk brottslighet är ofta mycket svårare att upptäcka än om t ex en enskild anställd kommer på ett sätt att stoppa lite pengar i egen ficka. Och kan dessutom vara betydligt mer skadlig för företaget.

Hur går det då till? Vilka metoder använder professionella bedragare för att kunna lura till sig pengar från företag? Nigel Iyer beskriver hur en avgörande del av den organiserade brottslighetens tillvägagångssätt är att skapa s k frontföretag, dvs företag som ser legitima ut men i själva verket bara är en fasad.

Han beskriver hur de t ex kan registrera ett företag i London, som ägs av ett företag på Brittiska Jungfruöarna, som i sin tur ägs av ett företag i ett helt annat land och vars bankkonto finns i ytterligare ett annat land. Eftersom regelverket och myndigheternas befogenheter ligger så långt efter brottslingarna kan denna typ av kedjor av ägande dölja kriminaliteten i flera år innan den upptäcks.

Att komma till rätta med denna typ av avancerade kriminella strukturer förutsätter betydligt större resurser hos de

rättsvårdande myndigheterna och ett mer utvecklat samarbete över gränserna. Men Iyer pekar också på en annan metod, som kan vara nog så effektiv:

> *Ju fler ”fraud detectives” som finns i ett företag, ju fler som i sin vardag håller ögonen på sådant som verkar misstänkt, desto dyrare och svårare för brottslingarna att verka. Det är ofta mer effektivt än att försöka hålla jämna steg i lagstiftningen.*

I diskussioner om kriminalitet beskrivs svenskar emellanåt som lite naiva, som att vi inte riktigt inser allvaret och att det faktiskt finns stora kriminella organisationer som verkar i vårt land. Nigel Iyer menar tvärtom att Sverige är ett av de länder som har allra bäst förutsättningar att bekämpa bedrägerier av olika slag.

De viktigaste skälen till detta är kulturella. Den höga svenska tilliten och konsensuskulturen bidrar till att vi gärna löser problem tillsammans istället för var och en på egen hand. Och ju mer t ex medarbetare på ett företag pratar med varandra, desto större chans att försök till bedrägeri upptäcks i tid.

INTERNETBASERADE BEDRÄGERIER I SVERIGE

Hur ser då situationen ut i dagens Sverige för svenska företag vad gäller bedrägerier av olika slag? För att få en fördjupad bild av detta har vi talat med Kriminalkommissarie Jan Olsson, en av Sveriges främsta experter på bekämpning av bedrägerier av olika slag.

Han var en av grundarna av Nationellt Bedrägericentrum, och arbetar idag vid Nationella Operativa Avdelningen (NOA) vid Polisens Nationella IT-brottscenter. Han vet mer än de allra flesta om hur bedrägeribrottslighet idag ser ut och hur man bäst går till väga för att bekämpa den.

Vid Nationellt Bedrägericentrum arbetar idag ett tiotal personer med att bevaka och analysera bedrägeribrott riktade mot svenska företag och privatpersoner. Enheten utreder inte egentligen brotten utan analyserar tillvägagångssätt och aktörer, för att på så sätt stödja utredande poliser runtom i landet med kunskap både från Sverige och andra länder.

Hur ser då bedrägeribrott i Sverige typiskt sett ut? Vilken typ av brott gäller det? Jan Olsson beskriver bedrägeribrott som ett mycket brett fält, som kan innefatta ”allt från hästskojare till mycket komplexa internetbaserade bedrägerier”. Idag sker ungefär 80 procent av bedrägerierna på ett eller annat sätt med hjälp av internet.

Just den tekniska utvecklingen har gjort det lättare för brottslingar att bedriva sin verksamhet i stor skala och även lättare att undgå upptäckt. Det blir med andra ord både mer lönsamt och mindre riskfyllt att försöka lura företag och privatpersoner på pengar om det kan ske via internet än om man måste ha fysisk kontakt.

Samtidigt är Jan Olsson noga med att påpeka att det inte är tekniken i sig som skapar möjligheten till brottslighet, det är snarare i våra mänskliga behov det hela börjar.

> *Internetbaserade brott över lag är ett svar på människors behov, vi vill ha snabba betalningslösningar och ett så krångelfritt liv som möjligt. Ofta är de tekniska*

lösningarna i sig väldigt säkra, så det är vi människor som ”hackas”. Det som kallas ”social engineering”, helt enkelt att kriminella lurar människor att använda tekniken på ett sätt som möjliggör brottet.

Rent praktisk handlar det om att kriminella t ex per telefon utger sig för att vara någon annan och förmår människor att göra saker vi inte borde göra med teknikens hjälp. Alternativt att de genom falska mail eller SMS lurar människor att klicka på länkar som sedan t ex lurar av offret kortuppgifter eller planterar en skadlig kod som stjäl pengar via datorn. Tekniken är verktygen, men det som möjliggör brotten är mänsklig övertalningsförmåga.

Vilka är då de vanligaste typerna av bedrägerier i Sverige idag? Hur ser de kriminellas tillvägagångssätt ut? Jan Olsson berättar att det överlägset vanligaste brottet i denna kategori är det som kallas ”card not present”, dvs bedrägeribrott där kreditkortsnummer används på nätet av någon som inte har tillgång till det fysiska kortet och inte har rätt att använda det.

För svenska företag är detta ett stort problem, kriminella köper systematiskt varor och tjänster med hjälp av kreditkortsuppgifter de har kommit över mot kortinnehavarens vilja. Denna typ av brottslighet drabbar i slutänden just företagen, då kortföretagen normalt sett ser till att den kortinnehavare som drabbas hålls skadelös.

Alla kriminella inköp med svenska kreditkort sker förstås inte hos svenska företag, men ett stort antal företag i Sverige drabbas varje år. Dessutom tillhör de använda kortuppgifterna i sig inte bara privatpersoner utan i vissa fall företag.

Ett annat brott, som främst drabbar äldre privatpersoner, är s k ”vishing” (efter voice-fishing), där en kriminell person ringer upp och utger sig för att jobba på den kontaktades bank och försöker få personen att lämna sina inloggningsuppgifter till internetbanken.

När denna brottstyp var som allra störst stals i storleksordningen 90 miljoner kronor per månad från framförallt äldre, som ett resultat av att ett stort antal olika kriminella organisationer parallellt ägnade sig åt detta. När Polisen, i samarbete med bankerna och Bank-ID, gjorde en särskild insats mot denna ty av brott kunde tillslag göras mot sju-åtta olika kriminella organisationer.

Vilka är då de vanligaste bedrägeribrotten mot svenska företag begångna via internet? Jan Olsson beskriver hur bedrägeribrotten ofta är en del i en kedja av olika typer av brott, där företag kan drabbas i flera led.

> *Ofta är själva bedrägeriet bara den sista länken i en lång kedja av brott. Det första som sker är gigantiska dataintrång hos företag för att stjäla kreditkortsuppgifter. Nyligen hittade s k ”vita hackare” (hackare som använder sina metoder för att avslöja brott) 26 miljoner kreditkortsuppgifter till salu. Mängden kortuppgifter är så stor att brottslingarna har svårt att hinna använda alla kort innan deras giltighetstid löpt ut.*

Nästa steg, berättar Jan Olsson, är att bedragare köper kortuppgifter på Darknet, den krypterade dolda delen av internet där bl a många kriminella affärer sker. När kortuppgifterna väl används är brottsoffren dels privatpersoner som äger korten

och dels företag som luras att sälja till kriminella. Dessutom bygger som sagt alltihop på stora dataintrång hos företag.

> *Ett vanligt brott som drabbar företag är vad som brukar kallas för ”business e-mail compromised”, dvs att någon fingerar ett mejl så att det ser ut att komma från en ledande person i företaget för att få någon att t ex skicka stora utlandstransaktioner eller liknande.*

I en sådan situation manipuleras mottagaren att lita på att mejlet är äkta och göra överföringen, utan att undersöka vem mottagaren av pengarna är eller ringa upp den person som sägs vara avsändaren och dubbelkolla att uppgifterna verkligen stämmer. Återigen är verktyget tekniskt, men själva bedrägeriet bygger på mänsklig övertalningsförmåga.

> *Ett annat stort hot är det som kallas ”ransomware”, dvs någon på företaget får ett mail och luras klicka på en länk, som laddar ner skadlig kod som i sin tur låser alla filer i datorn eller i värsta fall hela företagets nätverk. Företaget tvingas sedan betala utpressarna för att få filerna upplåsta.*

Jan Olsson avråder bestämt från att betala utpressare i dessa typer av situationer, även om han har förståelse för att företag ibland ändå väljer att göra det. Problemet med att betala är dels att utpressarna därmed får bekräftat att de kan lura just detta företag på pengar, och lockas att försöka igen. Och dels därför att man bidrar till att finansiera kriminalitet, där

bedrägerierna ofta i praktiken är ett sätt att finansiera grövre brott.

Företag som utsätts för denna typ av utpressningsförsök och får sina filer låsta uppmanas dels att polisanmäla händelsen och dels att t ex besöka webbplatsen NOMORERANSOM.ORG, där ett antal stora IT-säkerhetsföretag gratis lagt upp programvara som ofta kan låsa upp filerna.

GÄRNINGSMÄN: FRÅN TONÅRINGAR TILL MC-GÄNG OCH IS-SYMPATISÖRER

Vilka är det då som begår de olika bedrägeribrotten? Enligt Jan Olsson är spännvidden bland gärningsmännen mycket stor, och mönstret ser väldigt olika ut beroende på vilken typ av bedrägerier det gäller.

> *I de enkla bedrägerierna mot privatpersoner genom stulna kortuppgifter är det vanligt med äldre tonåringar som helt enkelt vill finansiera en livsstil de inte har råd med, köpa dyra kläder etc. Den typen av gärningsmän ser sällan att de begår ett brott, de ser inga drabbade personer framför sig. Extremfallet i andra änden är tung brottslighet, ofta MC-gäng eller andra kriminella organisationer.*

Jan Olsson påminner om att bedrägerier inte bara är brott i sig utan ofta används av organiserade brottsligheten som ett enkelt sätt att finansiera annan och betydligt grövre brottslighet. Att se mellan fingrarna med bedrägerier är därför i praktiken att bidra till mycket grov brottslighet.

Aktörer som ger sig in i t ex ”vishing”-verksamhet är inte längre vanliga bedragare utan kriminella organisationer som ser att det finns stora penningflöden som de vill komma åt. De har ett stort våldskapital och använder bedrägerier för att finansiera allt från narkotikasmuggling till att skänka pengar till IS eller någon annan terrorgrupp. Det måste man tänka på när man prioriterar mellan olika brott från polisens sida.

I praktiken menar Olsson att den organiserade brottsligheten kommer att söka sig till verksamheter där tillgången på enkla pengar är stor och risken att åka fast är liten, det blir en rationell kalkyl som vilket affärsbeslut som helst.

ÖVERTRO PÅ TEKNIKEN GÖR OSS MER UTSATTA FÖR BROTT

Hur kommer det sig då att bedragare lyckas lura såväl privatpersoner som företag på så stora pengar? Hur kan det vara möjligt att människor så ofta lockas att begå misstag som kan kosta dem eller deras arbetsgivare miljontals kronor?

Jan Olsson beskriver orsakerna som en kombination av att vi ofta har en övertro på hur tekniken påverkar oss samtidigt som bedragarna med tiden har blivit mycket skickliga på att skapa just den trygghet som kan få oss att göra saker som egentligen är ytterst riskfyllda.

Vi har ett ofta märkligt förhållande till internet, som om det inte vore en del av vår värld. De flesta tycker att det på något sätt är mer ofarligt att göra saker på

internet än i den verkliga världen, och litar mer på vad som står på nätet än vad någon kanske säger. Dessutom har bedragare lärt sig att förfalska information via nätet som gör att vi upplever att vi kan lita på dem, trots att vi egentligen inte vet vilka de är.

De skickligaste bedragarna har dessutom lärt sig att när de ringer upp tilltänkta offer ska de använda ord och uttryck som ger intryck av att de verkligen ringer från t ex banken eller Polisen och att det därför är säkert att ge dem t ex dina inloggningsuppgifter till internetbanken. Om de dessutom använder sig av s k ”spoofing”, dvs fingerar det telefonnummer de ringer ifrån så de ser ut att vara den de säger blir det ännu svårare att genomskåda dem.

HUR SKYDDAR VI OSS?

Vad kan man då göra för att skydda sig eller sitt företag från att utsättas för bedrägerier av olika slag? Jan Olsson menar att det finns några enkla tips som skulle kunna minska antalet lyckade bedrägerier kraftigt.

FÖR DET FÖRSTA: lämna aldrig någonsin ut dina kortuppgifter eller ditt inlogg till internetbanken via telefon, mail eller SMS. Om banken, polisen eller någon annan behöver nå dig för att du är utsatt för dataintrång eller annat behöver de inte be om sådana uppgifter. Och de kommer inte kontakta dig per telefon i ett sådant syfte.

FÖR DET ANDRA: när du behöver ha lösenord för inloggning på olika ställen, använd en lösenordshanterare. Om du har

samma lösenord överallt blir du en tacksam måltavla, särskilt om lösenordet är lätt att lista ut.

FÖR DET TREDJE: spärra dina bank- eller kreditkort för internetköp när du inte själv använder dem. Det går inte att skydda sig mot att dina kortuppgifter stjäls från ett företag där du handlat, men om du har spärrat kortet när du inte behöver handla på internet kan en bedragare inte använda dina uppgifter.

Svenska banker ligger också, enligt Jan Olsson, ganska långt fram vad gäller att undvika kortbedrägerier och samarbetet mellan bankerna och Polisen är bättre än i de flesta andra länder.

Samtidigt uppmanar Olsson oss alla att vara vaksamma på bedrägeriförsök i vår vardag, och aldrig underskatta kreativiteten hos personer som försöker lura andra på pengar. Som exempel nämner han den i dessa sammanhang ganska populära s k ”triangelmodellen” för att lura till sig pengar utan att bli upptäckt.

Ett bedrägeri enligt denna modell kan t ex gå till på följande sätt:

1. En privatperson lägger ut en annons på nätet om att sälja t ex en kamera.
2. Bedragaren ringer säljaren, säger sig vara intresserad och affären görs upp. Bedragaren säger att pengarna förs över strax och en kompis till honom/henne sedan kommer för att hämta kameran.
3. Omedelbart därefter lägger bedragaren ut en egen annons om att sälja något betydligt med värdefullt, t ex en motorcykel, för samma summa som kameran. När

spekulanter ringer uppger bedragaren samma kontonummer som för köpet av kameran.

4. När tre personer som tror de får köpa motorcykeln har fört över pengar ringer bedragaren säljaren av kameran och säger att pengarna har förts över men att det av misstag skett tre gånger. Säljaren uppmanas sedan ge ”kompisen” som kommer för att hämta kameran den överskjutande summan kontant.
5. Bedragaren åker hem till säljaren och hämtar kameran samt de ”felaktigt” inbetalade pengarna och försvinner sedan. När de som velat köpa motorcykeln polisanmäler bedrägeriet är det enda säkra spåret kontonumret till säljaren av kameran.

Det är förstås svårt för den person som i detta exempel ville sälja en begagnad kamera att förutse vad som kan hända. Däremot illustrerar exemplet att det alltid är viktigt att vara på sin vakt och att man bör bli misstänksam om något avviker från det vanliga. I detta fall skulle de märkliga ”dubbelbetalningarna”, och att köparen vill ha mellanskillnaden kontant, ha väckt misstanke. Liksom det märkligt låga priset på motorcykeln.

Det är alltid lätt att vara efterklok, men som Nigel Iyer beskriver i början av detta kapitel är den kanske viktigaste insatsen mot bedrägerier att vara uppmärksam när något avviker från det vanliga och dubbelkolla sådant som verkar märkligt. Om någon försöker få dig att betala eller lämna ifrån dig uppgifter på ett sätt du inte är van vid, särskilt under tidspress, finns en uppenbar risk att du är utsatt för ett bedrägeriförsök.

Fotnoter

46 Svensk Handel, Trygghetsbarometern, Tredje kvartalet 2019, 2019. https://www.svenskhandel.se/globalassets/dokument/aktuellt-och-opinion/rapporter-och-foldrar/trygghetsbarometern/trygghetsbarometern-q3-2019.pdf

47 https://www.transparency.org/research/cpi/overview

KAPITEL 6

När det otänkbara händer – om utpressning, rån, kidnappning och attentat mot företag

I den här boken beskriver vi många olika typer av brott företag kan drabbas av. Dessa brott är av olika karaktär, och även om alla typer av brott är oacceptabla finns vissa som utgör ett mer akut fysiskt hot för företagaren och de anställda. I detta kapitel har vi sammanfattat de grövsta formerna av brott mot företag, inklusive sådana som hotar hela samhället.

OTILLÅTEN PÅVERKAN – UTPRESSNING

En brottskategori som har ökat kraftigt vad gäller brott mot företag är utpressning. När Brå gav ut rapporten Otillåten påverkan mot företag – En undersökning om utpressning[48], år 2012, beskrev den en tioårig ökning av utpressning i kriminalstatistiken. Även sammanställningen över anmälda brott år 2018[49] visar på en ökning jämfört med föregående år – med 291 procent. Totalt anmäldes hela 15 600 utpressningsbrott under 2018. De anmälda utpressningsbrotten minskade dock kraftigt (-38 procent) under 2019.[50]

I Svenskt Näringslivs rapport Brottslighetens kostnader (2018) framkommer att endast en procent av företagen, i den

enkätundersökning som ligger till grund för rapporten, uppgav att de utsatts för utpressning. I 2020 års utgåva av undersökningen har andelen fördubblats till två procent. Samma ökning återspeglas i andelen företag som tror att det kommer bli vanligare med utpressning i framtiden. Andelen som tror att det kommer bli vanligare med utpressning i framtiden har ökat från 11 till 20 procent.[51]

Att otillåten påverkan i form av utpressning innefattar direkt våld mot företagare är lyckligtvis ganska ovanligt. Däremot används hot om våld återkommande som påtryckningsmedel, om inte företagaren gör som de kriminella säger kommer de att utsättas för våld.

Något förenklat kan man säga att de kriminella som direkt använder våld vid sin utpressning är mindre etablerade i ”branschen”, aktörer som ägnat sig åt denna typ av brottslighet länge behöver ofta inte använda våld i någon större omfattning för att deras offer ska förstå vad som kommer att hända om de vägrar ge efter för påtryckningarna.[52]

ORGANISERAD BROTTSLIGHET

Företagare är tacksamma måltavlor för utpressning, i synnerhet om de hanterar kontanter i sin verksamhet. Särskilt olika former av organiserade brottslighet har specialiserat sig på att använda påtryckningar mot företag som ett enkelt sätt att komma över pengar till jämförelsevis låga risker.

Det kan t ex gälla traditionell så kallad beskyddarverksamhet knuten till ett visst territorium som den kriminella organisationen kan sägas kontrollera. Om inte företaget betalar

kommer det att utsättas för skadegörelse eller våld, enda sättet att slippa undan är att betala ”beskydd”.

För en företagare som har börjat betala eller gett efter för andra former av otillåten påverkan har svårt att hålla inne med betalningarna. Då vet de kriminella att företagaren är beredd att betala och risken är stor att utpressningen ska trappas upp till allt större belopp. Det är helt enkelt mycket svårt att ”köpa sig fri”, den som väl börjat betala fastnar tvärtom allt mer i de kriminellas klor.

OLIKA MOTIV BAKOM OTILLÅTEN PÅVERKAN

Det finns fler anledningar än beskyddarverksamhet från kriminella organisationer till att företagare utsätts för otillåtna påtryckningar. Brås rapport Otillåten påverkan mot företag tar upp ett antal olika möjliga motiv bakom utpressning mot företag.

KONFLIKTER OCH HÄMND

Tvister och konflikter med personer som företaget har ekonomiska förbindelser med är ibland en grogrund för utpressning. Det kan vara t ex tidigare eller nuvarande anställda, delägare eller kunder som står för utpressningen. Det förekommer även att andra företag utövar otillåten påtryckning för att stärka sin egen konkurrenssituation.

I dessa fall är det vanligt att utpressningen föranleds av ett konkret missnöje, med t ex löner, villkor eller ägarförhållanden. I det fall det är en kund som står för utpressningen kan missnöje eller tvist om pris eller kvalitet vara den

bakomliggande orsaken. Det förekommer också att kunder som inte betalar utsätts för otillåten påverkan från företag som vill driva in skulden med olagliga medel.

Näraliggande exempel gäller rena hämndmotiv, där verkliga eller upplevda oförrätter kan leda till konflikter som trappas upp genom otillåten påverkan. Lättkränkta individer kan motiveras av det som av allmänheten skulle bedömas som verkliga bagateller, exempelvis att nekas inträde till en nattklubb, och därmed gå över gränsen i sin hämnd.

Lönsamma företag och företagare som uppfattas som förmögna kan utsättas för utpressning i kriminellt vinstdelningssyfte. Går företaget bra finns risken att personer med en relation till företaget anser sig ha rätt till en del av vinsten, trots att så i praktiken inte är fallet. Det gäller särskilt om företagaren har byggt sin rikedom genom tveksamma affärer, då är risken större att man i verksamheten kommit i kontakt med personer som är kapabla att ta till olagliga metoder för att tillgodogöra sig värde.

En ytterligare faktor som kan ligga bakom utpressning och trakasserier mot företag eller företagare är ideologiskt drivet motstånd mot företagets verksamhet. Militant djurrättsaktivism har t ex legat bakom att verksamheter som innefattar animaliska produkter utsätts för sabotage och andra olagliga påtryckningar.

Särskilt minkfarmare och deras familjer har drabbats av systematiska trakasserier i det uttalade syftet att de ska tvingas lägga ned sin verksamhet. Minkfarmerna i sig har ett starkt symbolvärde, liksom pälsbutiker, inom djuraktiviströrelsen. Utpressarna har inte något uppsåt att komma över pengar i dessa fall, utan drivs av en ideologisk övertygelse

att straffa företagare som bedriver verksamhet aktivisterna uppfattas som oetisk.

Intensiteten i den militanta djuraktivismen varierar, men de senaste åren har en uppgång i antalet aktioner kunnat noteras. Till stor del har hoten och skadegörelsen riktas mot lantbrukare, vilket fått relativt stor uppmärksamhet i media.[53] Lantbrukarnas riksförbund (LRF) har presenterat data som visar att alltfler lantbrukare upplever att de utsätts för hot och trakasserier från militanta djurrättsaktivister.[54]

KONTAKTER MED KRIMINELLA ÄR EN RISKFAKTOR

Dessvärre är det inte alltid företagare som drabbas av denna typ av påtryckningar själva är alldeles oskyldiga. I vissa fall förekommer det att mindre nogräknade företagare själva anlitar kriminella för att utöva påtryckningar i tvister eller för att driva in skulder och liknande. Det kan i sin tur leda till att den som utsätts svarar med att själv anlita kriminella för att bemöta påverkansförsöket. En ond cirkel av i värsta fall eskalerande våld skapas.

Det normala i ett rättssamhälle är att den som utsätts för utpressning polisanmäler eller vidtar andra legala åtgärder för att freda sin verksamhet. Men att kontakta polisen är kanske inte alltid förstahandsalternativet för företagare som själva inte har rent mjöl i påsen.

En annan faktor som kan få vissa företagare att söka andra sätt att freda sig än de rättsliga är misstro mot myndigheternas förmåga att skydda dem. En butiksägare som gjort mängder av polisanmälningar för snatterier och annat som oftast

inte lett någonstans är det lätt att förstå att tilltron till de legala vägarna är svag.

Det företag som anlitar kriminella för att utöva påtryckningar istället för att använda de legala medel som står tillbuds tar stora risker även för egen del. De hot och andra metoder de kriminella använder riskerar att vändas mot uppdragsgivaren själv.

De kontakter de kriminella som anlitas får med sin uppdragsgivare ger ingångar till dennes företag. Risken finns att företagaren i nästa skede utsätts för utpressning av just de kriminella han/hon anlitat. Det faktum att en företagare anlitat kriminella ger också de som anlitas en hållhake på företagaren som kan användas för att tilltvinga sig tjänster eller pengar. Det drar i sin tur in företagaren i ett slags beroendeförhållande som blir allt svårare att komma ur.

Dessvärre räcker det inte att hålla sig borta från kriminella personer för att slippa drabbas av denna typ av påtryckningar. Företagare kan också tvingas att begå brott, av kriminella som vill komma åt företagets verksamhet för att exempelvis använda kontantflöden för att tvätta pengar. Brå skriver i sin rapport att de finns fall där företagaren mot sin vilja i det närmaste blivit målvakt i sitt eget företag när brottslingar tagit över tillstånd eller kontantflöden.

HOT OCH VÅLD

Hot är en annan form av otillåten påverkan som drabbar företagare och anställda. I 2019 års statistik[55] över personer misstänkta för brott misstänktes 20 347 personer för olaga hot.

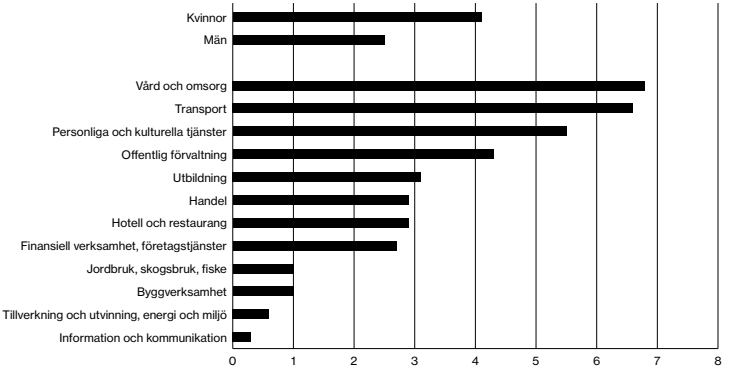
Risken att drabbas av hot och våld beror på vilken bransch man är verksam inom.

Företag som i sin verksamhet hanterar kontanter eller människor (exempelvis inom vård, service, säkerhet) är enligt Arbetsmiljöverket mer utsatta än andra typer av företag. Andra faktorer som också framhålls är kvälls- eller nattarbete, ensamarbete, bristande förmåga att lösa konflikter och verksamhet i generellt brottsbelastade miljöer.

Av SCB:s rapport Hot, våld och oro 1980-2017 (2018)[56] framgår att tre procent av de förvärvsarbetande i åldrarna 16-64 år utsattes för hot på arbetsplatsen (2016-2017). Kvinnor var mer drabbade av hot på arbetsplatsen än män, fyra respektive tre procent. Procenttal kanske inte är så talande men tre procent motsvarar 150 000 personer, som alla blivit utsatta för brott på sin arbetsplats.

Andel som någon gång under de senaste 12 månaderna har varit utsatta för hot i arbetet, fördelat efter kön respektive näringsgren. 2016–17.

Förvärvsarbetande 16–64 år



Källa: SCB, Undersökningarna av levnadsförhållanden

Allra vanligast är hot och våld på arbetsplatsen inom vård och omsorg samt transporter (i synnerhet kollektivtrafik, kan man anta). Bland dem som arbetade i dessa sektorer utsattes ungefär sju procent för våld i arbetet 2016-2017.

En oroväckande trend som också redovisas är att utsattheten för våld i arbetet fördubblats från en till två procentenheter mellan perioden 1982-1983 och 2016-2017. Motsvarande ökning för hot är hela tre gånger – från en till tre procentenheter. Återigen är procenttalen låga – de flesta drabbas lyckligtvis inte – men för ett stort antal personer är sådana händelser vardag. Det är en synnerligen allvarlig utveckling.

SÄKERHETSHÖJANDE ÅTGÄRDER ÄR KOSTSAMMA

Arbetsgivarna har huvudansvaret för medarbetarnas arbetsmiljö. Kriminaliteten medför därför stora kostnader för företagen som måste värna om medarbetarnas arbetsmiljö. Exempelvis kan företag bli tvungna att hyra in vakter under vissa tider eller öka bemanningen för att undvika ensamarbete. Kriminaliteten för med sig stora kostnader för företagen, och riskerar att gå ut över andra typer av arbetsmiljöarbete.

Alla säkerhetshöjande åtgärder behöver inte vara dyra, saker som att ändra rutiner och arbetssätt kan man göra med de resurser man har i det ordinarie arbetet. Kostnaden ökar dock snabbt när externa leverantörer anlitas för t ex larm- och väktartjänster.

Handelns kostnader för säkerhetsåtgärder, som larm, övervakningskameror och väktare, beräknas uppgå till cirka 11 miljarder kronor per år.[57] Enligt en enkätundersökning[58] som Svenskt Näringsliv genomfört (2020) hade 62 procent

av företagen vidtagit någon form av säkerhetshöjande åtgärder de senaste två åren. Motsvarande siffra bland företag som utsatts för brott under samma period var 80 procent.

Branschorganisationen Säkerhetsföretagens ökande omsättning i Sverige är en annan tydlig illustration till att landets företag har ett behov av säkerhetshöjande åtgärder, som svar på en växande kriminalitet. Mellan 2012 och 2016 ökade Säkerhetsföretagens omsättning med omkring 40 procent, till 35 miljarder kronor. Omsättningen under 2018 var gott och väl över 38 miljarder.[59] Tillväxten i säkerhetsbranschen förklaras till stor del av att utvecklingen går mot såväl fler som grövre brott där också vapen allt oftare förekommer.

HANDELN SÄRSKILT UTSATT FÖR HOT OCH VÅLD

Hot eller våld är ett allvarligt bekymmer för många företag, särskilt inom handeln. Branschorganisationen Svensk Handel genomför återkommande sin Trygghetsbarometer för att få en fördjupad förståelse av handlarnas utsatthet för brott.

Resultatet för andra kvartalet 2020[60] visar att fyra av tio handlare utsatts för brott den senaste tiden. Det är den högsta nivån sedan mätningarna startade år 2018. 41 procent av butikerna i undersökningen hade utsatts för stöld den senaste veckan. I samband med stölderna förekommer ofta också hot mot personalen. 17 procent uppgav att de hade utsatts för hot eller våld den senaste tiden vid pågående stölder.

Generellt ökar det hotfulla beteendet från besökare eller kunder i handeln. Sedan föregående kvartals Trygghetsbarometer hade andelen drabbade fördubblats och så många som

knappt var tredje handlare (31 procent) uppgav att de hade drabbats av hotfullt beteende som inte hade direkt samband med stöld eller snatteri.

Allvarligt är också att Trygghetsbarometern visar att hoten i fler än vart tredje fall (37 procent) inte anmäls. Svensk Handel förklarar den låga anmälningsbenägenheten med att rättsväsendet har en tendens att bagatellisera butiksstölderna, få brott utreds och straffen är låga. Många handlare menar att det inte är någon idé att anmäla eftersom rättsväsendet ändå inte gör något åt anmälningarna.

Våld och hot på jobbet är även ett betydande rekryteringshinder för handeln. Hot och våld på jobbet är oacceptabelt men det är inte mycket handlarna kan göra åt det om inte brotten utreds och gärningsmännen lagförs. För att trygga arbetsmiljön tvingas handeln därför att anlita egna vakter och vidta andra säkerhetshöjande åtgärder, vilket ökar kostnaderna för handlarna och i förlängningen för kunderna. Stök och bråk i affärslokalerna är också direkta negativa effekter för affärerna då potentiella kunder undviker butiker helt eller under vissa tider.

Den som hotar t ex företagare eller anställda i handeln måste göra en avvägning av hur hotet ska framställas, tomma ord är inte effektiva. Har man ett stort våldskapital att skrämmas med – t ex genom att tillhöra en välkänt kriminell organisation – kan man nöja sig med subtila hot, ordval räcker för att budskapet ska tas på allvar och uppfattas som ett hot.

Aktörer med mindre våldskapital, vars kriminella nätverk t ex är mindre välkända, kompenserar ofta detta med direkta hot om att döda eller misshandla någon, ofta förstärkt genom att vapen visas upp. Mer professionella aktörer drar sig ofta

för vapenhot då det innebär en risk för strängare straff om hotet polisanmäls.[61]

Hot som går ut på att ”avslöja” eller genera ett offer genom att offentliggöra komprometterande information förekommer också. Sociala medier som Facebook och Twitter har gett var och en tillgång till en medial plattform för att publicera nästan vilka budskap som helst. Kraften i de sociala medierna är så stor att ett hot om att framställa ett företag i dålig dager kan få så allvarliga effekter för affärerna att vissa väljer att ge efter för hoten – alldeles oavsett om det som riskeras att offentliggöras är sant eller falskt.

Men det är inte bara i handeln som hot och våld är vanligt. En annan grupp som är särskilt utsatt är vakter av olika slag. På senare tid har det, bland annat i Västerås[62], förekommit skjutningar där dörrvakter på nattklubbar varit måltavlor. Motivet för sådant våld kan ofta vara något slags hämnd för att gärningsmännen nekats inträde till den aktuella nattklubben.

Konsekvensen av den här typen av dåd blir att personer som är anställda för att upprätthålla ordningen på ett uteställe med tiden kommer att dra sig för att göra sitt jobb. Att avvisa personer som demonstrerar ett våldskapital blir något som dörrvakter och andra personer som arbetar med säkerhet vet innebär risker för våldsamma hämndaktioner. Därför finns risken att de kriminella kan fortsätta verka ostört.

Den bransch som har allra flest arbetsskadeanmälningar orsakade av våld, hot och kränkande behandling är vård och omsorg. Särskilt förekommande är anmälningar inom HVB- och LSS-boenden, dessa typer av verksamheter svarade för hela 41 procent av anmälningarna om arbetsolyckor med sjukfrånvaro orsakade av hot och våld, mellan åren 2012 och

2017. En stor andel av de anställda inom både den privata och offentliga delen av denna sektor är kvinnor.[63]

Vi nämnde tidigare att en särskild typ av trakasserier och hot riktar sig mot lantbrukare och djuruppfödare – särskilt minkfarmare. Dessa brott begås av olika grupperingar inom den militanta delen av djurrättsrörelsen. En granskning som Göteborgs-Posten har gjort visar att djurrättsaktivister ligger bakom minst 200 brott i Västsverige 2017-2019.[64]

De metoder som används är bland annat skadegörelse av produktionsanläggningar, vilket blir mycket kostsamt för företagaren. Utsläppta djur och förstörda nätkassar för fiskodling medför stora ekonomiska skador, men ofta även lidande för de som djuraktivisterna säger sig vilja skydda.

Också mer personliga påtryckningar, som telefonsamtal på nätterna, skändning av anhörigas gravar och hotfulla hembesök på gårdar, förekommer. I en del fall har hoten övergått i misshandel och till och med mordbrand. Även för denna typ av brottslighet är anmälningsfrekvensen låg, endast 40 procent av de lantbrukare som utsatts för denna typ av brott uppger att de har polisanmält det inträffade.[65]

En särskild form av trakasserier, som specifikt drabbar kvinnliga företagare eller anställda, är sexuella trakasserier av olika slag, begångna av besökare eller kunder. Inom särskilt handeln är detta ett påtagligt problem.

I samband med de s k #metoo-uppropen gjorde Expressen i samarbete med Demoskop en undersökning bland kvinnliga medarbetare i handeln som visade att hela 40 procent någon gång utsatts för sexuella övergrepp eller ovälkomna sexuella närmanden på jobbet.[66]

I mer än hälften av fallen (55 procent) uppgavs att en kund var förövaren. Detta är ett allvarligt arbetsmiljöproblem som arbetsgivarna har svårt att angripa då en butiksägare inte kan porta en person från butiken, då en butik ska vara en plats dit allmänheten har tillträde.

Både branschorganisationen Svensk Handel och facket Handelsanställdas förbund vill se lagändringar som gör det möjligt att genom ett tillfälligt tillträdesförbud porta personer som begår brott mot personalen.

RÅN

De mest allvarliga brotten, som t ex rån, drabbar lyckligtvis ganska få företag. Två procent av företagen i Svenskt Näringslivs enkät om företagens kostnader för brott uppgav att de utsatts för rån någon gång under de senaste två åren. Det är dock värt att hålla i minnet att även om två procent kan tyckas lågt så innebär det tusentals drabbade företag och anställda.[67]

Ett rån mot en butik är ett mycket allvarligt brott som innebär risk för såväl fysiska som psykiska skador för offret. Rån leder ofta till allvarliga arbetsolycksfall. Enligt AFA Försäkrings rapport Hot och våld på den svenska arbetsmarknaden (2018) berodde 21 procent av de allvarliga arbetsolycksfallen på rån.[68]

Samma rapport visar att unga oftare är drabbade av rån – hela 43 procent av antalet allvarliga arbetsolycksfall år 2016-2017, i åldrarna 16-25 år, berodde på rån. Det hänger samman med att rån är mer vanligt förekommande inom handel och restaurang, som anställer många unga. Av ungdomarna är

unga kvinnor särskilt utsatta. AFA Försäkrings rapport visar att kvinnor i åldrarna 16-25 år löper 3,7 gånger högre risk att rånas än kvinnor i genomsnitt.

Att rånas är en traumatiserande upplevelse vilket speglas i att samhällets kostnader för rån är betydligt högre än för en stöld. För en butik är rån marginellt mer kostsamt än en stöld, men för samhället är kostnaden betydande i form av vård och sjukskrivning, etc.

Bland företagen förväntar sig många att rånen kommer att bli vanligare i framtiden. Företagens förväntningar på framtiden är naturligtvis något som återspeglas i investeringsviljan för olika säkerhetshöjande insatser. Det ska heller inte underskattas att företagare som förväntar sig att oftare utsättas för rån arbetar under psykisk press vilket är mycket skadligt för deras långsiktiga hälsa.

KIDNAPPNING

Det förekommer även att företagare och deras verksamheter drabbas av ännu grövre brott än rån mot butiker eller andra lokaler. Kidnappning av företagsledare eller deras anhöriga är ett säkerhetshot som både företagsledare och företag behöver förhålla sig till. Kidnappningen av hemelektronikkedjan SIBA:s dåvarande VD och delägare Fabian Bengtson 2005 skapade en ökad medvetenhet om de mest allvarliga risker som ledande företagare löper.

Bengtssons kidnappare krävde 50 miljoner kronor i lösensumma. Idag är det troligt att kravet på lösensumman hade varit ställt i en kryptovaluta, för att underlätta kidnapparnas utväxling av offer mot lösensumma och göra det svårare att

spåra kidnapparna efteråt. Ofta har kidnappare kunnat gripas i samband med utväxlingen, om denna istället sker anonymt på nätet är chansen att komma undan betydligt större.

Den tekniska utvecklingen har dock även påverkat vilka brott kriminella grupperingar använder sig av, och generellt ökat intresset för brott som kan utföras helt på nätet. Kriminella som vill komma över ett företags pengar fokuserar idag oftare på IT-bedrägerier eller företags- och identitetskapningar snarare än VD-kidnappningar, vilket minskar hotet mot företagarnas liv och hälsa. Samtidigt förekommer kidnappningar fortfarande, och är en risk särskilt förmögna personer och deras anhöriga behöver vara vaksamma inför.

De säkerhetsföretag som arbetar med att skydda företagsledare och deras anhöriga understryker betydelsen av att försöka undvika rutiner som gör att ens rörelser under dygnet blir allt för förutsägbara.

Barn och barnbarn är också måltavlor vilket gör att det behövs en plan för att även föra dem i säkerhet om det finns en hotbild. Stora företag har i regel ett bra skydd för sina ledande anställda, vilket gör att kidnappningshoten snarare riktas mot företagsledare på mellanstora företag där de kriminella tänker sig att det kan finnas stora förmögenheter att komma åt.

PÅGÅENDE DÖDLIGT VÅLD OCH TERRORISM

Terrordådet på Drottninggatan i Stockholm den 7 april 2017, som kostade fem människor livet, visade att vårt öppna samhälle är sårbart och att dödliga terrordåd kan ske även i Sverige. Sedan dess har flera olika misstänkta förberedelser till

terrorism mot mål i Sverige upptäckts. Detta är ett högst reellt hot idag.

Trots att sannolikheten att som enskild person drabbas av en terrorattack är mycket låg så påverkas medborgarnas vardagliga beteenden av medvetenheten om att en attack faktiskt kan inträffa. I en undersökning som Novus utfört, på uppdrag av Högskolan Dalarna och Länsstyrelsen Dalarna, säger sig var femte tillfrågad ha blivit mer misstänksam mot andra personer den senaste tiden.

I samma undersökning uppger 15 procent att de undvikit stora folksamlingar som köpcenter, gågator, konserter och sportevenemang på grund av oro för terrordåd. Två av tre (65 procent) tror att problemet med extremism kommer att öka under 2020-talet.[69] Allmänhetens oro för terrordåd påverkar konsumtionsmönstren på ett sätt som drabbar företag vars lokaler eller verksamheter bygger på en stor genomströmning av potentiella kunder. Om människor är rädda för att vistas på gator och torg kommer det förstås även att innebära minskad kundtillströmning i butikerna.

Även företag och deras verksamheter kan vara måltavlor för terrorister. Samhällskritisk infrastruktur som t ex elförsörjning löper en risk att angripas både genom attacker på fysiska installationer och IT-system.

För en del företag, särskilt inom media och opinionsbildning, kan redaktioner och även enskilda medarbetare t ex profilerade skribenter bli måltavlor. Attacken mot den franska satirtidningen Charlie Hebdo 2015 och den planerade attacken mot Jyllands-Posten 2010, var båda islamistiska terroristers verk.

Dessa attacker mot medieredaktioner visar på riskerna med publicering av material som kan väcka terroristers vrede. För det fria meningsutbytet och yttrandefriheten innebär det latenta hotet om att utsättas för attentat en risk för självcensur.

Ur ett arbetsgivarperspektiv kan man tvingas att göra en avvägning mellan det publicistiska intressen och att värna medarbetarnas säkerhet. Bland medarbetarna kan terrorhotet och risken för andra trakasserier leda till självcensur, vilket allvarligt hämmar samhällsdebatten.

Antalet bombattentat där någon, företrädelsevis i ett bostadsområde, detonerar sprängladdningar har ökat kraftigt i Sverige. Under 2018 skedde 162 sprängningar.[70] Under 2019 anmäldes hela 257 sprängningar, en uppgång med 59 procent.[71] Denna utveckling bidrar starkt till en ökande otrygghet i samhället i stort, men framförallt försämras livskvaliteten och tryggheten för dem som bor i områden som drabbats.

Situationen är unik jämfört med de flesta andra länder och en parallell utveckling har skett vad gäller attacker med skjutvapen. I regel är dessa skjutningar, där ett stort antal skott avlossas på öppen gata utan hänsyn till omgivningen, gängrelaterade uppgörelser. I kapitel 2 beskriver vi mer ingående de kriminella miljöer där denna typ av brott begås.

Vad och vilka som ligger bakom de många bombdåden i Sverige har inte fått någon tillfredsställande förklaring. Uppgörelser mellan olika kriminella gäng är dock även här en sannolik förklaring. Få gärningsmän har dessutom lagförts.[72]

Den låga andelen uppklarade brott är i sig problematisk då den lär de kriminella gängen att risken att åka fast är minimal. Därför är risken stor att utvecklingen kommer att fortsätta.

Hittills har de många bombdåden som ofta utförts i bostadsområden skadat relativt få personer. Den materiella förödelsen har däremot varit omfattande och drabbar främst fastighetsföretag. Med på det sätt som beskrivs mer ingående i kapitel 1 får brottslighet också konsekvenser för samhällsutvecklingen och tilliten i stort.

Fotnoter

48 Brå, Otillåten påverkan mot företag, En undersökning om utpressning, Rapport 2012:12, 2012. https://www.bra.se/download/18.4dfe0028139b9a0cf4080001396/1371914739200/2012_12_otill_ten_p_verkan.pdf

49 Brå, Kriminalstatistik 2018, Anmälda brott, Slutlig statistik, 2019. https://www.bra.se/download/18.62c6cfa2166eca5d70e4fb6/1553761868570/Sammanfattning_anmalda_2018.pdf

50 https://www.bra.se/statistik/statistik-utifran-brottstyper/hot-och-paverkan-mot-samhallet.html

51 Svenskt Näringsliv: Brottslighetens kostnader för svenska företag (2018) och Brottslighetens kostnader 2020 (2020)

52 Brå: Otillåten påverkan, rapport 2012:12, s. 70 f.

53 https://www.svt.se/nyheter/lokalt/skane/okade-attacker-mot-lantbrukarna

54 https://www.atl.nu/lantbruk/radsla-farbonder-att-halla-sitt-yrke-hemligt/

55 Brå, Kriminalstatistik 2019, Misstänkta personer, 2019. https://www.bra.se/download/18.7d27ebd916ea64de5304de45/1585639838563/Sam- manfattning_misstankta_2019.pdf

56 SCB, Hot, våld och oro 1980-2017, 2018. https://www.scb.se/contentassets/14f8221b750440 59a52f293dfobd1f6f/le0101_2016i17_sm_lebr1802.pdf

57 http://www.ehandel.se/Handeln-lagger-11-miljarder-om-aret-pa-sakerhet,11661.html

58 Svenskt Näringsliv, Brottslighetens kostnader 2020, 2020. https://www.svensktnaringsliv.se/material/rapporter/brottslighetens-kostnader-2020pdf_1143423.html/BINARY/Brottslighetens%20kostnader%20 2020.pdf

59 Säkerhetsföretagen, Säkerhetsföretagens årsrapport 2019, 2019. https://www.transportforetagen.se/globalassets/rapporter/sak/sakerhetsforetagens-arsrapport-2019.pdf?ts=8d79fe2ac65ea00

60 Svensk Handel, Trygghetsbarometern, Andra kvartalet 2020, 2020. https://www.svenskhandel.se/globalassets/dokument/aktuellt-och-opinion/rapporter-och-foldrar/trygghetsbarometern/trygghetsbarometern-q2-2020.pdf

61 Brå, Otillåten påverkan mot företag, En undersökning om utpressning, Rapport 2012:12, 2012, s. 67. https://www.bra.se/download/18.4dfe0028139b9a0cf4080001396/1371914739200/2012_12_otill_ten_p_verkan.pdf

62 https://www.expressen.se/nyheter/krim/krogvakter-vagrade-slappa-in-kriminel- la-tva-skjutna/

63 https://www.av.se/press/arbetsmiljoverket-kraftsamlar-mot-hot-och-vald-i-arbetslivet/?hl=kraftsamling%20mot%20hot%20och%20våld%20i%20arbetslivet

64 https://www.gp.se/nyheter/gp-granskar/s%C3%A5-blev-djurr%C3%A4tt-ster- rorn-det-st%C3%B6rsta-hotet-mot-b%C3%B6nderna-1.12613185

65 https://www.atl.nu/lantbruk/polisen-skarp-insatserna-mot-hatbrotten/?_ga=2.218028371.433259887.1561542883-1020243941.1557814512

66 https://handels.se/press/debattartiklar/porta-kunder-som-utsatter-anstalda-i-butiker-for-sexuella-trakasserier/

67 Svenskt Näringsliv, Brottslighetens kostnader för svenska företag, 2018, s. 15 f. https://www.svensktnaringsliv.se/bilder_och_dokument/rapport-brottslighetens-kostnader-for-svenska-foretagpdf_1126183.html/Rapport:+Brottslighetens+kostnader+fr+svenska+fretag_1.pdf

68 AFA Försäkring, Hot och våld på den svenska arbetsmarknaden, 2018, s. 14 och 18. https://www.afaforsakring.se/globalassets/nyhetsrum/seminarier/hot-och-vald-pa-den-svenska-arbetsmarknaden/f6345-delrapport-4---hotovald.pdf

69 https://www.dagenssamhalle.se/debatt/radslan-terror-forandrar-manniskors-vardag-30085

70 https://www.bra.se/om-bra/nytt-fran-bra/arkiv/nyheter/2020-01-29-sprangningarna-okar.html

71 https://www.bra.se/om-bra/nytt-fran-bra/arkiv/nyheter/2020-01-29-sprangningar- na-okar.html

72 https://www.svd.se/nio-av-tio-sprangningar-olosta-en-stor-utmaning

KAPITEL 7

Industrispionage – ett hot mot svensk konkurrenskraft

Allt mer av företagens värde är immateriella tillgångar som är lagrade i mer eller mindre säkra IT-system. Investeringar gjorda i dessa tillgångar under mycket lång tid kan vara helt avgörande för konkurrenskraften på lång sikt. För att de konkurrensfördelar företagen skapat ska kunna upprätthållas måste de immateriella tillgångarna kunna hållas inom företaget.

Det är därför inte förvånande att olika typer av aktörer har ett intresse av att försöka stjäla denna typ av tillgångar. Detta är vad vi i dagligt tal menar med industrispionage. Idag riktar sig denna verksamhet huvudsakligen mot IT-system, men även fysiska mål förblir viktiga måltavlor.

De vanligaste målen för industrispionage är kunskap i form av forskningsresultat, produktutveckling, ritningar, mjukvara. Men även information i form av affärsstrategier och kalkyler är intressanta för olika aktörer.

Det är svårt att beräkna svenska företags kostnader för det industrispionage de drabbas av. Det är dock uppenbart att den ekonomiska skadan kan vara mycket stor. Att konkurrerande aktörer får kännedom om affärshemligheter innebär

att de kan bespara sig kostnader för produktutveckling och konkurrera med stulen teknik till lägre pris.

Industrispionage kan också innebära att svenska företag förlorar affärer därför att konkurrenterna har kännedom om vilka bud de svenska företagen kommer att lägga i upphandlingar. Information av detta slag har ett värde som kan vara svår att överblicka och därför är det mycket viktigt att företag, såväl som stat och myndigheter har ett genomtänkt arbetssätt för att stärka informationssäkerheten.

Det kan även handla om att enskilda företags anseende och trovärdighet kan skadas genom läckage av känslig information, s k doxing.

Svårigheten att sätta en prislapp på hur mycket svenska företag förlorar på grund av industrispionage skapar också ett policyproblem. Så länge den samhällsekonomiska kostnaden inte är känd, är det heller inte lätt för politiska beslutsfattare att bedöma hur angelägna insatser mot denna verksamhet är.

Det finns också ett informationsproblem som gör att mörkertalet sannolikt är betydande. Eftersom företag som drabbas ogärna talar om vad man utsatts för och vilka effekter angreppen fått vet politikerna inte riktigt vilka problemen är och hur stora de är. Det är inte heller alltid lätt för de drabbade företagen att bedöma konsekvenser och kostnader av vad de drabbats av.

VEM LIGGER BAKOM ANGREPPEN? HUR STOR ÄR SKADAN?

Alla företag som lagrar värdefull information i sina system riskerar att utsättas för industrispionage. Den värdefulla informationen kan vara forskning, mjukvara, ritningar men också kundregister och affärshemligheter som marknadsplaner, försäljningssystem och strategidokument. Hotbilden ökar med informationens värde. Banker, finansiella företag och försvarsindustrier tillhör de mest utsatta sektorerna.

Pierre Anderberg är Chief Information Security Officer på Sveriges största försvarsindustriföretag Saab och har en bakgrund inom Försvarsmakten. Han har gedigen erfarenhet av hur företag utsätts för denna typ av angrepp.

> *Företag i Sverige angrips mer eller mindre dagligen. De flesta angrepp är av enklare karaktär och går att skydda sig mot med standardiserade säkerhetsmekanismer. En mindre del av angreppen är däremot avancerade och bakom dem ligger resursstarka aktörer. För att skydda sig mot sådant krävs betydligt större resurser och kompetens, säger Pierre Anderberg*

Det finns ett stort intresse för svensk teknik bland såväl konkurrerande företag som andra stater. Medicin, vård och miljöteknik är områden där svenska företag ligger i framkant på den tekniska utvecklingen. Stora företag hanterar ofta betydande värden vilket ökar hotbilden. Det krävs stora resurser och hög säkerhet för att kunna stå emot de avancerade angrepp som statsunderstödda kan genomföra.

Johan Wiktorin är VD för säkerhetsföretaget Intil, har en bakgrund som officer och som omvärldsdirektör på revisionsfirman PwC med 25 års erfarenhet av säkerhetsarbete. Han menar att många svenska företag ofta gör alldeles för lite för att skydda de tillgångar man har från denna typ av angrepp.

Svensk tillverkningsindustri har intressant intellektuell egendom, men skyddet av denna egendom står idag inte i proportion till värdena, säger Johan Wiktorin.

En annan faktor som påverkar riskerna för industrispionage är att vi använder allt mer teknik som måste försvaras mot angrepp. Mycket begärlig data finns idag i mobiltelefoner, och inte bara i datorer inne på företagen. Det har gjort att riskerna för angrepp ökat dramatiskt de senaste fem, tio åren.

STATSUNDERSTÖDDA AKTÖRER

Teknologi och innovationer är dyrköpt intellektuell egendom som många länder inte har egen kapacitet att utveckla. Det innebär att vissa stater kan ha ett intresse av att gynna sin egen industri eller ett strategiskt intresse av att komma över värdefull teknik. Hotbilden mot försvarsindustrin kan till stor del förklaras av den militärteknologiska kapplöpningen mellan stater.

Om industrispionage visar sig fungera kommer verksamheten att fortsätta. Geopolitiska spänningar ökar även spionaget mot företag. Särskilt försvarsteknologi är intressant för länder som saknar egen kapacitet på området.

Sanktioner som hindrar teknologiskt utbyte är en bidragande förklaring till varför vissa länder bedriver industrispionage. Vissa länder begår också andra IT-brott i stor skala för att dra in pengar till statskassan. Denna typ av agerande är av naturliga skäl vanligare i länder utan demokratisk in syn i de politiska institutionerna.

Vissa stater utgör ett större hot än andra. Kina, Ryssland och Iran är länder som ofta uppges vara särskilt aktiva i fråga om industrispionage. Angreppen utförs ofta av kriminella organisationer med statlig sponsring eller i utbyte mot någon tjänst.

> *Vi måste ta industrispionage på större allvar. Kinesiska myndigheter har t ex laglig rätt att genomföra penetration på servrar i Kina utan att berätta varför, vilket svenska företag som gör affärer i Kina måste tänka på. Alla bolag med kinesiska medborgare omfattas av kinesiska lagar, även i Sverige. Det ställer högre krav på bakgrundskontroller av kinesiska medborgare, samtidigt måste kontrollerna kunna genomföras utan att diskriminera, säger Johan Wiktorin.*

Utöver aktörer med statsanknytning finns exempel på enskilda personer och organisationer som bedriver industrispionage mot svenska företag. Motiven för denna kriminella aktivitet är dock inte säkerhetspolitisk eller strategisk utan rent ekonomisk. Dessa kriminella vill tjäna pengar på den information de kommer över. Det kan antingen ske genom att de själva får affärsmässiga fördelar eller genom att de säljer informationen vidare.

DESINFORMATION OCH SMUTSKASTNINGSKAMPANJER

En verksamhet som hänger nära samman med industrispionage är olika former av desinformation. Denna typ av insatser kan t ex har till syfte att påverka marknaden och gynna de egna affärerna. Det kan ske genom smutskastningskampanjer mot konkurrerande varumärken eller spridande av marknadspåverkande desinformation i syfte att manipulera börskurser och destabilisera konkurrenters ställning på marknaden.

Snabb nyhetsförmedling och sociala medier ökar räckvidden för all typ av information, även desinformation, och underlättar den här typen av aktiviteter. Särskilt i det korta perspektivet kan det göra mycket stor skada på företag och varumärken. Det är dessutom svårt att skydda sig mot angreppen, och det mesta talar för att denna typ av aktiviteter kommer att bli allt vanligare. Svenska företag behöver en beredskap att hantera och minimera skadorna av även den här typen av attacker.

STRUKTURERAT INFORMATIONSSÄKERHETSARBETE

Angripare letar alltid efter den svagaste länken, som ett rovdjur identifierar den svagaste individen i en flock. Vad gäller industrispionage kan det t ex handla om tekniska brister som dåligt uppdaterade säkerhetssystem, men också mänskliga faktorer som slarv med lösenord. Därför är en helhetssyn på informationssäkerhet och ett integrerat säkerhetsarbete grunden för att kunna skydda företagens information.

Tekniskt blir angreppen allt mer avancerade och samtidigt enklare att utföra. Färdiga angreppssystem, designade för att utnyttja sårbarheter i IT-system, säljs som idag som produkter på den svarta marknaden. Tekniken gör att dataintrångsförsöken kan automatiseras och utföras av gärningsmän utan specialistkompetens.

Allra mest problematiskt är det ofta med statliga aktörer som kan ha kännedom om svagheter i systemen som inte är kända för andra berörda.

> *Om en angripare tar sig in i ett system är de svåra att upptäcka. Det skulle vara som att leta efter en nål i en höstack. Kända sårbarheter måste åtgärdas snabbt, men det tar tid att agera. Informationssäkerhet är som militär rustning, det är angriparsidan som har initiativet, säger Pierre Anderberg.*

Företagen har naturligtvis ansvar för att investera för att skydda sin information men staten har samtidigt en nyckelroll i att bekämpa statsunderstött industrispionage samt sammanställa och göra kompetens tillgänglig för näringslivet.

> *Statsmakterna behöver en samlad säkerhetsdoktrin för informationssäkerhet som omfattar hela samhället. Det behövs mer utbildad kompetens, högre utredningskapacitet inom Polisen. Att regeringen skjuter till pengar till ett cybersäkerhetscentrum är bra men det behövs en betydligt mer genomtänkt informationssäkerhetsdoktrin, säger Johan Wiktorin.*

INFORMATIONSSÄKERHETSKULTUREN AVGÖRANDE

Det är inte alltid tekniskt kunnande som ger det bästa skyddet mot angrepp av detta slag . Att bygga upp en säkerhetsmedveten kultur inom företagen, och en organisation som stödjer denna kultur, är nog så viktigt.

Den mänskliga faktorn är ofta en svag länk som angripare riktar in sig på för att få tillgång till ett IT-system. Ofta är den första fasen i ett angrepp att få någon på insidan att agera för att lämna ut lösenord, klicka på en länk eller öppna en bilaga som innehåller skadlig kod.

> *Försök till sådana angrepp är vanligt och om de skulle lyckas ger det ett första fotfäste inne i systemet. För de anställda kan det vara svårt att avgöra om e-posten kommer från en legitim avsändare, vi har ju massor av partners som förväntar sig kommunikation av oss, säger Pierre Anderberg.*

Företag som saknar god cyberhygien är betydligt mer utsatta. För att täppa till säkerhetsluckor i systemet är det viktigt med en god informationssäkerhetskultur i organisationen. Alla medarbetare måste vara medvetna om att företaget och de själva kan vara måltavlor, och ha grundläggande kunskap om de vanligaste typerna av angrepp. Det gäller alla funktioner inom företaget, i stort och i smått.

Personligt ansvar är viktigt för att strategidokument och rutiner ska omsättas i praktiken. Ofta gör företagen för lite för att försöka upptäcka intrångsförsök i tid. Det kan ta allt mellan tre och nio månader att göra proaktiva genomgångar av loggar, detektion av klienter i systemet, laptops, mobiler

och nätverk. Under tiden kan inkräktare hinna göra stor skada. Gamla misstag går att dra lärdom av men skadorna går sällan att reparera.

Det är särskilt svårt att få kontinuitet i arbetet om man använder sig av inhyrda konsulter. Stora företag har i regel processer för att hantera och överblicka vilka enheter som finns i ett system. Det förekommer ändå att medarbetare inte blir av med sina behörigheter när de lämnar en anställning. Även om kompetensen finns inom organisationen, vilket den i regel gör i stora företag, så varierar genomslaget i det faktiska säkerhetsarbetet – det vill säga det arbete som sätter nivån för informationssäkerheten.

> *Över tid har vi tappat lite ordning och reda. Ofta har företag administrationskonton som inte kan knytas till någon fysisk person. Samtidigt kan sådana konton ha enorma befogenheter, att exempelvis ta emot och attestera fakturor, kopplade till kontona. Likaså finns ofta oklarheter vad gäller behörigheten att koppla in hårdvaror och mjukvaror i IT-systemen, säger Johan Wiktorin.*

Lyckas man få medarbetarna att känna stolthet över att de gemensamt upprätthåller en stark säkerhet blir det mycket svårare för en angripare att komma in i systemet. Säkerhetskulturen stärks av enkla dagliga rutiner som att låsa in mobiltelefoner i skåp under viktiga möten.

Det är dels effektivt i sig och blir dessutom en påminnelse om att det finns aktörer som vill tjuvlyssna till vad som sägs i mötesrummet. Likaså är det värdefullt att föra en löpande

dialog om vad man kan tala publikt om och vad som måste stanna inom företaget eller det enskilda mötet.

INVESTERA I INFORMATIONSSÄKERHET

Medvetenhet om vikten av att ha säkra system, och en god informationssäkerhetskultur i organisationerna, varierar mellan olika företag och branscher.

I de branscher som är extra utsatta som bank, finans och försvarsindustri sätter företagen i regel av stora resurser för att hålla en hög säkerhetsnivå. En tumregel är att tio procent av IT-budgeten ska gå till säkerhet. I bank, finans och försvarsindustri är andelen avsevärt högre. I exempelvis den civila tillverkningsindustrin är investeringarna i många fall betydligt mindre. Trots att de ofta har stora mängder värdefull information har dessa företag inte alltid ett tillräckligt skydd mot industrispionage.

Grunden för ett företags säkerhetsarbete är att företagets ägare och ledning förstår riskerna och är beredda att avsätta resurser för att upprätthålla en hög säkerhetsnivå. Det går inte att nonchalera säkerhetsproblemen – de måste tas itu med genom konkreta åtgärder.

I Sverige är utbildat säkerhetsfolk en bristvara. Näringslivet rekryterar idag i stor utsträckning från myndighetssfären, men det är ofta svårt att hitta personer med tillräcklig erfarenhet. Det driver upp kostnaderna för säkerhetstjänster.

Här har staten en viktig uppgift i att se till att marknadens behov av säkerhetskompetens möts, menar Johan Wiktorin. Att förlita sig på inhyrd personal skapar inte den kontinuitet

som är önskvärd inom ett så komplext område som informationssäkerhet.

INTEGRERA SÄKERHETSARBETET

Kopplingen mellan företagens affär och informationssäkerhet är ofta inte tillräckligt tydlig idag. Det illustreras bl a av hur svårt det är att få en uppfattning om hur mycket industrispionage kostar svenska företag varje år. Företagsledningar behöver flytta säkerhetspersonerna högre upp i organisationerna.

> *Det kan vara svårt att inordna säkerhetspersonerna under IT-avdelningen, det är lättare att vara ett stöd från sidan av verksamheten. Det finns mycket att jobba med här, säger Johan Wiktorin.*

En gedigen säkerhetsskyddsanalys av företaget är grunden för en stark informationssäkerhet. Det är viktigt att inte slarva med att analysera vilken hotbild som finns och vad som ska skyddas. Detta är en naturlig del av säkerhetsexperternas arbete i företagen, men deras arbete behöver bli bättre integrerat med den affärsmässiga sidan av företagens verksamhet. Här finns ett stort behov av tydlig intern kommunikation om de gemensamma målen för säkerhetsarbetet.

Trots alla tekniska lösningar är den mänskliga faktorn avgörande för huruvida säkerhetsnivån i praktiken är hög eller låg. Om säkerhetskulturen är stark blir det mycket svårare att kringgå de tekniska säkerhetslösningarna.

Samtidigt behöver tekniska system i så stor utsträckning som möjligt designas för att minska risken för både mänskliga misstag och uppsåtliga angrepp.

ÖKA RISKMEDVETENHETEN INOM FÖRETAGET

I säkerhetsanalysen är det viktigt att väga in de särskilda risker som kan uppstå vid internationell expansion. Svenska företag är aktiva exportföretag med många affärskontakter i och resor till andra länder. Dessa resor ökar riskexponeringen, i varierande grad beroende på land och region.

Vissa resor kan innebära stora fysiska risker i form av kidnappning och utpressning. Men också risken för stölder av information på mobiler och datorer kan öka. Därför är det viktigt att tänka på att inte resa med sina skyddsvärda data.

En bra rutin är att ha särskilda resemobiler och -datorer som inte ger tillgång till skyddsvärd information om de skulle bli stulna. Under resan är det viktigt att alltid ha uppsikt över mobil och dator. Man bör även vara medveten om att det alltid innebär en potentiell risk att använda sig av ett trådlöst nätverk på resa. De kan tappas på information eller förses med skadlig mjukvara som sedan ägaren ovetandes tar med hem till företaget.

Riskerna varierar som sagt från land till land men generellt gäller det att vara på sin vakt även under resor i västländer. Säpo varnar i dessa sammanhang särskilt för Kina, Ryssland och Iran. Varningen gäller också länder och regioner där dessa har inflytande, så som Centralasien, vissa länder i Afrika eller Libanon. Ett bra stöd för planeringen av resor är

Brittiska utrikesdepartementets Foreign Travel Advice som löpande uppdaterar riskbedömningar för resor i olika länder.

Affärsresenärer och andra företagsrepresentanter är allt vanligare mål för statsunderstött industrispionage. Dessa aktörer är långsiktiga och kan bearbeta personer under lång tid, och även försöka genomföra direkta värvningar av medarbetare i svenska företag med målsättningen att få en kontakt ”på insidan”.

> *Värvningar är inte så vanligt men det förekommer i en större utsträckning än vi skulle önska, säger Johan Wiktorin.*

Värvningen är ofta en lång process i vilken främmande makt kartlägger och närmar sig personer som de bedömer mottagliga för påtryckningar eller erbjudanden.

Det kan från början verka oskyldigt. Utfästelser om kommande affärsmöjligheter kan t ex vara en ingång. Måltavlorna kan också kompromitteras på olika sätt för att sedan kunna pressas att lämna ut information. Om man som affärsresenär misstänker att man utsatts för ett värvningsförsök eller utpressning ska man kontakta Säpo när man kommit hem till Sverige.

INSIDERS – HOT INNE I FÖRETAGEN

Angripare letar som sagt alltid efter svaga länkar. Ofta är den svaga länken IT-systemet, men det finns också ett insider-hot som behöver hanteras. En stark säkerhetskultur räcker inte. Det behövs också ett personalsäkerhetskoncept som beaktar

informationssäkerhet under hela processen från rekrytering till avslutad anställning.

Insiderhot är svåra att tackla eftersom det är lätt att redan beskrivningen av denna typ av problem kan väcka misstro inom en organisation. Men i grunden måste alla medarbetare känna en trygghet i att kollegorna går att lita på.

> *För oss är det viktigt att hitta medarbetare vi kan lita på och som har en hög säkerhetsmedvenhet. De utgör en viktig del i skyddet och välutbildade, uppmärksamma medarbetare ökar vår förmåga. Våra medarbetare utbildas i och övar säkerhet regelbundet, säger Pierre Anderberg.*

Just rekryteringsprocesser blir som sagt extra känsliga när utländska medborgare är inblandade. Företag har dessutom begränsade möjligheter att på egen hand utföra bakgrundskontroller, särskilt utomlands. Säpo har här en avgörande roll för att stödja svenska företag vid känsliga rekryteringar.

TREDJEPARTSRISKER

Även om den egna organisationen har en god informationssäkerhet händer det att det slarvas i underleverantörsledet eller hos en affärspartner. Denna typ av problem är förstås särskilt problematiska både att upptäcka och skydda sig mot.

Om angreppen sker via exempelvis en underleverantör av IT-tjänster spelar den egna säkerheten mindre roll. Det kräver ytterligare resurser att säkerställa att molntjänster med mera är säkra, men det är nödvändigt.

Det finns anledning för företag att även väga in tredjepartsrisker, och sådana risker kan finnas på många olika områden. Infrastruktur som kommunikation och elförsörjning är också något som kan utsättas för påverkan. Utan el står fabriken stilla. Även här har staten ett stort ansvar för att upptäcka och avvärja säkerhetshot.

> *Investerare har starkt intresse av att lösa tillitsfrågan. Alla är beroende av tredjepartsleverantörer vad gäller både produkter och tjänster. Därför är det viktigt att bygga bort tillitsproblemet. Vi försäkrar oss om att de mjukvaror vi köper inte har bakdörrar eller andra sårbarheter, säger Pierre Anderberg.*

Även myndigheter och kommuner hanterar en stor mängd åtråvärd information och får inte glömmas bort när det gäller företagens informationssäkerhet. Även de är måltavlor för industrispionage då de lagrar känslig information om företag och i flera fall även företags hemliga information i sina system.

> *Ett konkret exempel på en tredjepartsrisk där det inte är ett företag som utgör svagheten är ett samarbete mellan ett tjeckiskt universitet och företag för en tid sedan. Universitetet hade ordnat konferenser och samtidigt visade det sig att den universitetsanställde som ordnat konferenserna sedan startat en egen firma för kinesisk-tjeckiskt samarbete, säger Johan Wiktorin.*

Det är viktigt att svenska företag är medvetna om tredjepartsriskerna oavsett om det handlar om andra företag, universitet, myndigheter, andra organisationer eller enskilda personer.

CERTIFIERING

Ett bra sätt att ta sig an säkerhetsarbetet och att hantera tredjepartsrisker är att följa de inarbetade certifieringsstandarder som finns.

För affärer på vissa marknader är olika typer av certifiering ett krav för att få delta i upphandlingen. För svenska företag som har den typen av behov är ISO 27000 en bra internationell standard som har alla grundelement på plats, menar Pierre Anderberg. USA har egna motsvarigheter och i regel behöver man följa en standard som accepteras i det land man gör affärer. Stora företag följer i regel flera certifieringsstandarder parallellt.

STATEN MÅSTE SKYDDA SVENSKA FÖRETAG

Det finns ett säkerhetspolitiskt intresse för staten Sverige att skydda svensk teknologi och konkurrenskraft. Sverige och EU behöver ge företagen bättre stöd för att motverka industrispionage. Det är inte rimlig att förvänta sig att svenska företag ska kunna stå emot angrepp från statsunderstödda aktörer på egen hand och bekostnad.

Både myndigheter och företag behöver hjälpas åt för att skydda de känsligaste tillgångarna och därför är det

viktigt med ett väl fungerande samarbete, säger Pierre Anderberg.

Staten och myndigheterna måste dessutom vara mer på sin vakt för egen del och se till att skydda sin verksamhet. Politiken har ett ansvar att se till att ställa tydliga krav på att företagen upprätthåller en hög lägstanivå på sitt skydd. Offentliga köpare bör ställa krav på att leverantörerna är säkerhetscertifierade eller uppfyller vissa kravdokument.

Kompetensförsörjning är ett annat strategiskt ansvar där staten har en viktig roll. Det behövs fler utbildade säkerhetsspecialister för att möta det hot som IT-relaterad brottslighet utgör. Polisen behöver även höja sin utredningskapacitet.

Det är viktigt att Sverige satsar på att öka sin cyberförsvarsförmåga. IT-baserade attacker är billiga att utföra och dessutom skalbara. Det gör att en i andra avseenden mindre stark statsaktör kan ha en stor förmåga att utföra attacker. Sverige måste, precis som alla andra länder, satsa på att möta cyberhotet och helst ligga i framkant av utvecklingen för att inte riskera att bli den svaga länk som det är tacksammast att angripa.

Det är bra att regeringen skjuter till pengar till cybersäkerhetscentret. Men framgången hänger på mandatet och hur de myndigheter som ska stödja centret – FRA, Säpo och MSB – agerar i praktiken. En samlande informationssäkerhetsdoktrin är nödvändig för arbete framåt.

En viktig uppgift är att samla in incidentsinformation. Det är känsligt eftersom de som angripits sällan vill medge att de utsatts för ett intrång. Företag som angrips måste kunna få råd och stöd, men det blir samtidigt en balansgång mellan vad som är statens ansvar respektive det privata näringslivets, säger Johan Wiktorin.

Vad gäller kompetensutbyte menar Wiktorin att det finns mycket att lära från Storbritannien, där GCHQ (motsvarigheten till FRA) leder ett kompetensutbytescentrum mellan offentliga och privata aktörer. Där kan konkreta råd om IT och informationssäkerhet inhämtas.

Israel tillämpar en annan modell i vilken näringsliv, akademi och försvar bildat ett informationssäkerhetskluster som sysselsätter tusentals personer. Samarbetet har lett till att Israel är ett av de främsta länderna inom cybersäkerhet. Tidigare, under kalla kriget, användes ett liknande arbetssätt i Sverige för försvarsinnovationer.

KAPITEL 8

”Allt som är lönsamt kommer att kopieras” – piratkopiering

Vissa typer av brottslighet mot företag är spektakulära och väcker stor uppmärksamhet, andra typer sker i det tysta utan att företagen själva kanske någonsin märker det. En av de största kriminella marknaderna i världen är piratkopiering, något som sker i nästan alla branscher och åsamkar svenska företag stor skada trots att vi sällan talar om det.

För att få en tydligare bild av denna jätteindustri, och vad svenska företag kan göra för att skydda sig, har vi intervjuat två av Sveriges främsta experter: Ann-Charlotte Söderlund och Peter Hedin.

Söderlund är advokat vid Gozzo Advokater och en av Sveriges allra mest rutinerade personer vad gäller frågor kring piratkopiering och skydd av immateriella rättigheter. Hon grundade Swedish Anti-Counterfeit Group 1996 och var dess ordförande fram till 2005, samt sakkunnig i EU-kommissionens Expert Group on IPR Enforcement och European Observatory on Infringements in IPR med fler uppdrag som sakkunnig.

Hedin är Patent- och registreringsverkets (PRV) Senior Enforcement Policy Advisor och har en bakgrund som expert vid bl a EU:s varumärkesmyndighet Office for Harmonisation in The Internal Market, Trademarks and Designs (OHIM). Med andra ord den svenska statens främsta expert på piratkopieringsfrågor.

ALLT FRÅN FLYGPLANSDELAR TILL BANANER

Piratkopiering är ett vitt begrepp som syftar på olika typer av otillåten kopiering, som sker utan att den som äger rättigheterna till produkternas varumärke, konstruktion eller design har gett sitt tillstånd. De kopierade produkterna säljs sedan som om de vore äkta, vilket innebär att piratkopierarna kan dra nytta av de investeringar rättighetsinnehavaren gjort utan att behöva göra de investeringar som krävs för att bygga varumärken.

I den allmänna debatten diskuteras piratkopiering sällan, och när det sker gäller diskussionen ofta digitala produkter som t ex filmer eller dataspel. Men faktum är att piratkopiering av fysiska produkter är en gigantisk marknad, och att det som kopieras är snart sagt allting som går att kopiera.

Vilken typ av produkter är det då som kopieras? Såväl Ann-Charlotte Söderlund som Peter Hedin framhåller att det i praktiken gäller alla typer av produkter som har ett värde på en marknad. Varhelst det finns ett värde i varumärke eller design riskerar man att kriminella försöker dra nytta av detta värde utan att betala för sig.

Alla produkter som har ett visst mått av framgång på marknaden kommer bli föremål för piratkopiering, så om företagen inte upptäckt någon kopiering beror det ofta på att de inte kontrollerat saken ordentligt, menar Ann-Charlotte Söderlund.

I praktiken har typen av piratkopierade produkter varierat över tid, beroende på vad som efterfrågas men också på vilka typer av aktörer som gett sig in på marknaden. Söderlund har bevakat denna typ av brottslighet mycket länge och beskriver hur typerna av produkter har växlat mellan decennierna:

Det har sett väldigt olika ut genom årtiondena. Före mitten av 80-talet piratkopierades främst lyxprodukter som klockor och handväskor. Det förekommer förstås fortfarande, men från mitten av 80-talet fram till mitten av 90-talet ökade piratkopieringen även av kläder och sportprodukter. Sedan dess kopieras i princip allting: allt från bildelar till batterier, kosmetika, tandborstar, pennor, tändare, mediciner, leksaker, parfymer, insektsmedel, ja allt möjligt.

Bland de produkter som kopieras finns även sådana som innebär uppenbara risker för konsumenterna. Peter Hedin nämner bland de värsta skräckexemplen piratkopierade bromsbelägg till bilar, som tillverkats av trä men sedan målats för att se ut som metall. Men även airbags, reservdelar till flygplan och komponenter till kärnkraftverk har kopierats olovligen med uppenbara säkerhetsrisker som följd.

Andra exempel på direkt farlig piratkopiering gäller t ex läkemedel, där den verksamma substansen kan vara mångdubbelt större än rekommenderat, insektsmedel som visar sig innehålla DDT, felaktigt konstruerade hjärtklaffar och höftledsproteser eller exempelvis livsmedel som innehåller giftiga eller starkt allergena ämnen.

Det finns egentligen ingen gräns för vilka produkter som kan bli föremål för piratkopiering. Ett av de mest udda exemplen gäller bananer, säger Peter Hedin. Bananer piratkopieras genom att falska klistermärken som anger bananernas varumärke, och kanske utger sig för att vara ekologiskt odlade, trycks upp och klistras fast på bananer av lägre kvalitet. Det illustrerar också att riskerna med piratkopiering ofta kan vara svåra att först bedöma.

> *Det kan förstås verka oskyldigt men när du köper en banan av visst märke så vet du det att den är odlad på ett säkert sätt, att de som skördat arbetat under drägliga förhållanden o s v. Den garantin har du inte alls om du köper en piratkopierad banan, så det kan vara så att du stödjer en helt annan sorts verksamhet.*

MILJARDFÖRLUSTER, KONKURSER OCH FÖRLORADE ARBETSTILLFÄLLEN

Vad kostar då piratkopieringen? Bland de drabbade företagen finns inte bara internationella lyxvarumärken, på det sätt många kanske tänker sig, utan i hög grad även svenska företag.

OECD har med hjälp av statistik från tullmyndigheter världen över tagit fram rapporten ”Förfalskning och

piratkopiering och den svenska ekonomin" (2019)[73] där man försöker kvantifiera den direkta kostnad denna typ av kriminalitet orsakar. Resultatet är häpnadsväckande.

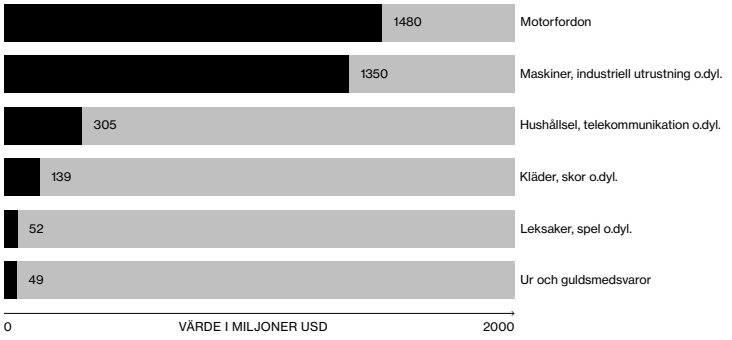
Den totala handeln med piratkopior av svenska produkter omsätter över 28 miljarder kronor varje år, vilket motsvarar ungefär två procent av hela världshandeln med svenska produkter. Den direkta förlust svenska företag drabbas av som ett resultat av detta uppgår till 17 miljarder, intäkter som hade kunnat komma svenska företag till del och hade kunnat investerats i ökad tillverkning i Sverige.

OECD uppskattar att Sverige det senast undersökta året (2016) gick miste om cirka 7 100 arbetstillfällen på grund av piratkopieringen, samtidigt som svenska staten gick miste om 7 miljarder kronor i förlorade skatteintäkter.

Det är då viktigt att påpeka att även denna detaljerade studie sannolikt underskattar problemet. Dels omfattas endast varor som handlas över gränserna, och dels ingår inte digitala produkter som är en mycket stor marknad. Till detta ska

De största produktkategorierna som är föremål för intrång i svenska immatriella rättigheter inom den globala handeln 2016 (74

Vad gäller beslagtaget värde



läggas att försök att mäta brottslighet till sin natur brukar ge underskattningar – det finns alltid ett mörkertal i form av brott som inte upptäckts.

De svenska produkter som kopieras avspeglar tydligt den svenska exportens sammansättning. Sett till värdet är de allra mest drabbade produktkategorierna delar till motorfordon samt maskiner och industriell utrustning, men även hushållsel och produkter för telekommunikation kopieras i stor utsträckning.

I vissa sektorer är dessutom andelen piratkopior mycket hög. Vad gäller t ex bilreservdelar som säljs i Sverige uppskattas hela 20 procent vara förfalskningar, medan den kosmetika och parfymer som säljs i Sverige till hela 55 procent är förfalskade. Att majoriteten av en produktkategori kan vara falsk visar hur allvarligt problemet är.

För svenska företag är piratkopieringen skadlig i flera led, och riskerar i slutänden att innebära att företag helt enkelt går under. Ann-Charlotte Söderlund beskriver hur piratkopieringen skadar företag i flera led:

> *Företagen skadas allvarligt av detta och på flera olika sätt. Dels är det förstås så att det företag vars produkter kopieras inte får avsättning för sina produkter utan kunderna köper kopior istället. Dels är ett problem att piratkopieringen konkurrerar ut mellanmarknadsprodukter som kanske inte är så exklusiva som de dyraste men gediget gjorda. Och i värsta fall blir det som med företaget Lovikkavanten som gick i konkurs på grund av att de konkurrerades ut av piratkopior av deras egna vantar.*

ÄR KONSUMENTERNA LURADE?

Att kopieringen är så oerhört omfattande och förekommer på de mest oväntade produktområden väcker en annan fråga: är de konsumenter som köper kopiorna medvetna om att detta är vad de gör, eller har de i själva verket lurats att tro att de köper originalprodukter?

I OECD-rapporten uppskattas att ungefär hälften av de piratkopierade produkter som importeras till Sverige sedan såldes till konsumenter som trodde att de köpte originalprodukter.

Ann-Charlotte Söderlund menar att det ser väldigt olika ut i olika grupper. Hon beskriver tre typexempel på konsumenter och inköpssituationer som alla drabbar företagen men där konsumenternas medvetenhet varierar.

En första grupp gäller främst unga konsumenter som regelbundet köper piratkopierade produkter och i regel inte bryr sig särskilt mycket om att de är just kopior. Ibland finns även i denna grupp en känsla av att det är rätt därför att det ändå bara drabbar globala storföretag och inte gör någon större skada.

En andra grupp är personer som generellt sett köper originalprodukter men ibland väljer kopior för att de vill ha något de inte tycker sig ha råd att köpa i original. Det gäller framförallt lyxprodukter, där konsumtionen har ett starkt imagevärde.

Och en tredje grupp är konsumenter som verkligen inte vet att de köper kopior. Här är det vanligast med produkter som är ganska anonyma, som t ex läkemedel köpta på nätet eller tvättmedel, men även situationer där det i praktiken är

omöjligt för konsumenten att kontrollera äktheten – som t ex reservdelar när bilen lämnas in på verkstad.

Söderlund menar att den låga kunskapen om vilka typer av produkter som kan vara piratkopierade är ett stort problem, men också att riskerna med att köpa piratkopior ofta underskattas av konsumenterna. De flesta förstår sannolikt risken med piratkopierade flygplansdelar eller läkemedel, men även andra produkter kan innebära risker.

> *Men även så enkla saker som kläder kan vara farliga om de är piratkopierade. Vi har höga krav på vilka kemikalier kläder får innehålla och hur garvning av läder ska gå till för att vara säkert, och sen förstås brandskydd i barnkläder etc. Där är det i praktiken omöjligt för konsumenten att skydda sig.*

Den typen av risker innebär, förutom en fara för konsumenten, också ett hot mot de företag som tillverkar de kopierade produkterna. Om något inträffar med en piratkopierad produkt är det ofta företaget som tillverkat originalet som får skulden i allmänhetens ögon.

> *Det finns många exempel på den typen av problem, det kan gälla piratkopierade mobilladdare som börjar brinna och där varumärket som tillverkat telefonerna skadas. Och om varumärkesägaren går ut och förklarar att det var en piratkopia är det många som inte ens noterar det.*

JÄTTEMARKNAD FÖR KRIMINELLA ORGANISATIONER

Många av de brott som drabbar svenska företag begås av väldigt olika typer av brottslingar – allt från privatpersoner som försöker tjäna lite pengar till grovt kriminella eller organiserad brottslighet. Vad gäller piratkopiering är mönstret tydligare: detta är en verksamhet för internationella kriminella organisationer, däribland några av världens mest ökända grupperingar.

Peter Hedin beskriver hur piratkopiering har blivit ”det perfekta brottet” för den internationella organiserade brottsligheten: vinstmarginalerna är enorma, risken att åka fast är mycket låg och för den som åker fast blir straffen sällan särskilt hårda. Han menar att det finns en lite naiv inställning till den här typen av brottslighet och att många inte förstår hur allvarlig situationen är.

> *Det är viktigt att man inser att en piratkopierad produkt inte är en enskild företeelse, utan en integrerad del av organiserad brottslighet som också sysslar med annan brottslighet som t ex penningtvätt, trafficking eller narkotikasmuggling. Det måste sättas in i ett större sammanhang för att förstå vilken typ av kriminalitet det här rör sig om.*

Faktum är att piratkopiering är en marknad värd mer än den globala narkotikasmugglingen och därför är det inte förvånande att den lockar flera av världens mest ökända brottssyndikat, som t ex maffian i Neapel och på Sicilien eller de kinesiska Triaderna. Det är i detta sammanhang ”oskyldiga” köp av piratkopierade produkter bör ses.

I vilka länder det förekommer mest tillverkning av piratkopior är enligt Peter Hedin väl känt, och de olika länders kriminella grupperingar har också specialiserat sig på olika typer produkter:

> *Det absolut vanligaste ursprungslandet är Kina, men vi ser även stora flöden från t ex Thailand och Indonesien, i Indien är det särskilt läkemedel som kopieras, i Turkiet särskilt cigaretter. Sen distribueras piratkopiorna ofta via hubbar i form av frihandelszoner som t ex Förenade Arabemiraten där transitsändningar sällan kontrolleras.*

Till dessa kedjor av illegal tillverkning och försäljning ska sedan läggas länder som fungerar som inkörsportar till den åtråvärda europeiska marknaden. Länder som särskilt brukar nämnas i detta sammanhang är t ex Bulgarien, Ungern och Rumänien. Där kan kriminella mellanhänder erbjuda en väg innanför EU:s yttre gränskontroller, och när kopiorna väl kommit dit är de mycket svåra att stoppa.

Det stora värdet på denna marknad och de resursstarka organisationer som är inblandade gör också att tillverkarna av förfalskade produktkopior ofta använder sig av ganska avancerade metoder för att undgå upptäckt. En metod som förekommer är att tillverkningen sker i lastrummet på fartyg ute på internationellt vatten, för att sedan leverera till en hamn där man vet att kontrollerna för tillfället är extra bristfälliga.

Hur ser då brottsligheten ut i Sverige? Vilka är det som ägnar sig åt import och vidareförsäljning av piratkopierade

produkter i vårt land? Peter Hedin beskriver att import av piratkopior i huvudsak sker på två olika sätt.

> *Det finns främst två olika varianter: antingen en vanlig person som beställer något på nätet från framförallt Kina, eller handlare som säljer de här produkterna – med eller utan vetskap om att det är kopior. När det gäller försäljning i butik har i regel yrkeskriminella importerat och sedan sålt till svenska butiker*

Ann-Charlotte Söderlund understryker att även seriösa handlare står för en del av importen av kopierade produkter, ofta utan att egentligen vara medvetna om det. De kanske får ett erbjudande om någon produkt till extra bra pris, lockas av att kunna höja sina marginaler och avstår – medvetet eller omedvetet – från att dubbelkolla att allt verkligen står rätt till med de produkter de erbjuds.

HUR BEKÄMPA PIRATKOPIERING?

Söderlund och Hedin ger även en samstämmig bild av hur tillverkning och försäljning av piratkopierade produkter ska kunna bekämpas. De ser framför sig tre olika behov.

För det första behöver de olika berörda myndigheterna prioritera denna typ av brott högre och även samverka bättre.

Ann-Charlotte Söderlund menar att det på senare år har skett en rejäl förbättring av hur denna typ av brott bekämpas, samtidigt som det fortfarande finns mycket kvar att göra.

Det blir bättre och bättre, när jag började jobba med det här var det ganska få som brydde sig om det. Idag har vi särskilda IP-åklagare och både Observatory och EU-kommissionen är väldigt aktiva, men de enskilda medlemsländerna måste ge det här betydligt mer uppmärksamhet.

Ett ytterligare skäl att ägna arbetet mot piratkopiering större uppmärksamhet är att denna brottslighet ofta hänger ihop med annan kriminell verksamhet. Det gäller inte bara de internationella brottssyndikatens kombination av piratkopiering, narkotikasmuggling och trafficking.

Även i mer vardagliga sammanhang kombineras piratkopiering ofta med andra brott. När Polisen exempelvis gjort tillslag mot försäljning av piratkopierad merchandise runt de stora arenorna i Stockholm, Göteborg och Malmö har även annan brottslighet kunnat stoppas.

Samtidigt beskriver både Söderlund och Hedin att Sverige, trots att vi är ett stort exportland vars produkter ofta kopieras, inte uppmärksammar detta på samma sätt som många andra länder gör. Söderlund beskriver de svenska handelsattachéerna som en nyckelgrupp.

Vissa länder som är särskilt drabbade, t ex Frankrike, har rejäla resurser för att hjälpa företag som är drabbade genom t ex särskild ”helpdesk” för företagen. Här har svenska beskickningar en hel del att lära, handelsattachéerna borde kunna göra mer.

En annan aspekt är vilka påföljder som kan dömas ut när någon grips för piratkopiering. I januari 2017 tillsattes en utredning (Dir 2017:4) angående grovt upphovsrättsintrång och grovt varumärkesintrång, i syfte att se över behovet av skärpta straff för särskilt allvarliga brott av detta slag.

När intervjun med Söderlund genomfördes (vintern 2019) har fortfarande inget lagförslag presenterats. Ett sådant vore dock ytterst angeläget, enligt Söderlund.

> *Jag tror det vore viktigt inte minst för att få omvärlden att förstå att det här är allvarliga brott. Det känns ju väldigt märkligt att straffet inte blir hårdare om det rör tusentals produkter istället för någon enstaka, det visar ju att verksamheten är betydligt mer organiserad och systematisk. Dessutom skulle Polisen få fler verktyg att använda om straffvärdet var högre.*

Ett ytterligare problem gäller att utredningen av dessa brott – på samma sätt som många andra typ av brottslighet – ofta tar mycket lång tid. Även för förhållandevis småskaliga fall av t ex försäljning av piratkopior kan utredningsarbetet ta flera år, under tiden kan brottsligheten fortsätta.

Särskilt viktigt beskrivs det att förbättra Tullens möjligheter att ingripa, ofta är det framförallt hos Tullen kunskapen om denna typ av brottslighet finns snarare än hos Polisen.

En andra viktig insats vore om företag är mer uppmärksamma, både på om de drabbas och om produkter de köper kan vara piratkopierade.

Peter Hedin beskriver att ett särskilt dilemma är att företagen ofta inte ens känner till att deras produkter är

piratkopierade. Han menar att många företag behöver bli bättre på att bevaka sina distributionskedjor, så att de har chans att upptäcka om deras produkter kopieras.

> *En orsak till att många företag inte vet att deras produkter kopieras är att de inte har anmält till tullverket att de har den produkten med det varumärket på, då är det ju väldigt osannolikt att tullen skulle stoppa en sändning. Om inte företagen beskriver detta som ett problem kommer inte staten att se problemet, så det är viktigt att företagen får upp ögonen för detta. Om man har en framgångsrik produkt är sannolikheten hög att den kommer piratkopieras förr eller senare.*

Att företag inte har anmält sina varor till tullverket kan ha olika förklaringar. En är att många företag tror att det räcker med att registrera sina immateriella rättigheter och att jobbet då är gjort. Men i praktiken är det snarare då det börjar, menar Hedin. Företag behöver aktivt hålla ögonen på att rättigheterna inte kränks, och då inte bara i sitt hemland utan i alla de länder man har något slags koppling till.

Ett ytterligare problem är att företag ofta avstår från att anmäla fall där de faktiskt vet att deras immateriella rättigheter har kränkts. Söderlund beskriver att om ägaren av ett känt konsumentvarumärke uppmärksammar att det utsatts för piratkopiering kan konsumenter avstå från att köpa originalprodukterna av rädsla att bli lurade. Därför kan det ofta vara bättre om problem av detta slag uppmärksammas av branscher gemensamt, vilket gjorts t ex i läkemedelsindustrin.

Hedin lyfter särskilt fram det digitala verktyget ACRIS, där företag enkelt kan registrera vilka varumärken och rättigheter man har samt vilken typ av problem man stött på i olika länder. Genom att där lämna vittnesmål om intrång kan företag ge EU-kommissionen ett starkare bevisunderlag i förhandlingar med tredje land.

Ett ytterligare verktyg för att försöka tvinga bort piratkopior från marknaden skulle kunna vara upphandlingar, menar Söderlund.

> *Inom EU förs t ex diskussioner om att anbudsgivare måste kunna säkerställa att det inte används några piratkopior i någon del av utförandet av uppdraget. Det tror jag kan vara en modell att fundera på.*

För enskilda företag menar Söderlund att det kan vara effektivt att använda sig av det som i USA ibland kallas ”kackerlackstrategin”, en parallell till bekämpning av skadedjur i lägenheter.

Syftet måste då inte nödvändigtvis vara att piratkopior helt försvinner från marknaden, men att göra det så besvärligt att de söker sig till andra företags produkter. Att de helt enkelt ”flyttar till grannen”. I praktiken kan det handla om att ha nolltolerans mot piratkopior, att slå till omedelbart även mot små problem. Det kan få kriminella att välja andra produkter där de kan verka mer ostört.

En tredje betydelsefull förändring vore om vi alla i egenskap av konsumenter lärde oss mer om hur den här marknaden fungerar och vad det egentligen betyder att köpa illegala kopior.

En annan aspekt som Ann-Charlotte Söderlund menar ofta glöms bort är att tillverkningen av piratkopior normalt sker på ett sätt som vi aldrig skulle acceptera för legala produkter.

> *I Sverige är vi ju väldigt medvetna om sociala villkor och miljö, men när det gäller piratkopior så har du ingen aning alls om hur tillverkningen gått till och där uppfattas det plötsligt inte som så viktigt. I praktiken blir det ofta ett sätt att finansiera miljöförstöring och barnarbete.*

Om fler konsumenter försökte tänka ett steg längre, inklusive att reflektera kring hur tillverkningen av piratkopierade produkter ser ut i praktiken, skulle det sannolikt bli svårare för de kriminella att sälja sina produkter.

Peter Hedin summerar det viktigaste som konsumenterna borde tänka på i en enkel tumregel: ”Om det verkar för bra för att vara sant så är det oftast det.”

Vad kan svenska företag göra?
Peter Hedins praktiska tips:

→ Det mest grundläggande: Se till att era varumärken är registrerade i alla länder där ni ska sälja, producera eller ha någon form av kontakt med i er verksamhet. Är inte varumärkena registrerade lokalt kan de inte skyddas.

→ Anmäl till tullverken i alla länder som era produkter kan passera och där ni har registrerat era rättigheter.

→ Använd de hjälpmedel som finns. EU:s immaterialrättsmyndighet OHIM har ett enkelt databasverktyg som nationella tull- och polismyndigheter samt Europol och andra berörda har tillgång till. Där kan företag gratis lägga in information om sina produkter, information som automatiskt översätts och skickas till berörda myndigheter.

Fotnoter

73 OECD, Förfalskning och piratkopiering och den svenska ekonomin, säkerställandet av att ”Made in Sweden” alltid är det, 2019. https://www.prv.se/globalassets/in-swedish/upphovsratt/piratkopiering/forfalskning-och-piratkopiering-och-den-svenska-ekonomin-2019.pdf

74 Ibid

KAPITEL 9

Att navigera i gråzonen mellan krig och fred

Sveriges omvärld har blivit mer osäker, och i takt med detta rustas det svenska försvaret upp. Det är främst Rysslands agerande i Europa som motiverar en förstärkning av försvarsförmågan. Näringslivet är en viktig del i det totalförsvar som nu åter håller på att byggas upp, efter nedrustningen som följde på Berlinmurens fall och Öststatskommunismens kollaps.

I spåren av Sovjetunionens upplösning försöker Ryssland att återupprätta sin ställning som stormakt. Upprustningen av den ryska militären är en viktig del av dessa ansträngningar. Till detta ska läggas de ryska underrättelse- och säkerhetstjänsternas spionerи och påverkansarbete i andra länder – däribland Sverige.

Svenska företag riskerar att bli måltavlor eller omedvetna brickor i ett större politiskt spel och måste därför vara vaksamma och stärka sitt säkerhetsarbete.

På längre sikt uppfattar dock många bedömare det kinesiska underrättelsearbetet som ett mer allvarligt hot mot Europas säkerhet. Det ryska agerandet beskrivs ofta som präglat av kortsiktig opportunism, medan det kinesiska speglar mer långsiktiga ambitioner där uppbyggandet av en

närvaro och inflytande är centralt, och exempelvis innefattar förvärv av svenska och andra europeiska företag.

Denna typ av säkerhetspolitiska hot, med en blandning av påverkansaktioner och politiska påtryckningar är en del av det så kallade hybridkriget. Detta kan beskrivas som en ständigt pågående konflikt där aktörerna utövar påverkan för att uppnå egna fördelar. Sådana fördelar innefattar allt typer av insatser som gör motståndaren svagare. Det kan t ex innefatta att underblåsa redan befintliga konflikter i ett land, förmedla desinformation eller ge stöd till extrempartier.

För Sveriges säkerhet är det nödvändigt att lära sig förstå och navigera i den gråzon som uppstått mellan vad som traditionellt uppfattas som krig och fred.

För att få en fördjupad bild av det försämrade säkerhetsläget, hybridkriget och upprustningen av totalförsvaret har vi talat med tre experter.

MARTIN ALLARD har en bakgrund inom strategisk analys i Regeringskansliet och bl a varit sekreterare i utredningen om näringslivets roll i totalförsvaret. Han är idag verksam som konsult på det globala säkerhetsföretaget 4C Strategies.

MARK GALEOTTI är hedersprofessor vid University College i London, grundare av konsultfirman Mayac Intelligence och en av världens främsta experter på rysk organiserad brottslighet. Han är även författare till böckerna *We Need To Talk About Putin* (2019), *Russian Political War* (2019) och *Vory: Den ryska supermaffian* (2018, på svenska 2019).

OSCAR JONSSON är författare till boken *The Russian Understanding of War: Blurring the Lines between War and Peace* (2019), och har en bakgrund som forskare vid Försvarshögskolan

samt vikarierande chef för den utrikes- och säkerhetspolitiska tankesmedjan Frivärld.

EN MINDRE SÄKER OMVÄRLD

RYSSLAND

Efter det kalla kriget slut och Sovjetunionens upplösning samt den efterföljande ekonomiska krisen förlorade Ryssland sin ställning som supermakt. Även om Ryssland efterträdde Sovjetunionen i FN:s säkerhetsråd och fick kontroll över Sovjetunionens kärnvapenarsenal var landet jämförelsevis svagt.

Under president Vladimir Putin har Ryssland, tack vare stora inkomster från råvaror som olja och gas, systematiskt återuppbyggt sin militära kapacitet och därmed återtagit rollen som militär stormakt. Kriget i Georgien 2008 visade också för omvärlden att man var villig att använda sina militära medel offensivt.

Det slutliga kvittot på den nygamla ryska säkerhetsdoktrinen kom i och med annekteringen av Krim-halvön och kriget i Ukraina 2014. Parallellt med det ännu pågående kriget i Ukraina har även Ryssland ett omfattande militärt engagemang till stöd för Al-Assad-regimen i Syrien.

Även i Sveriges närområde har Ryssland demonstrerat sin militärmakt. För svenskt vidkommande blev den så kallade ryska påsken år 2013, då Ryssland simulerade ett flyganfall mot svenska mål, en väckarklocka. Särskilt anmärkningsvärt var att det på långfredagen 2013 inte fanns någon beredskap

inom svenska flygvapnet att skicka upp stridsflygplan för att markera mot den ryska anflygningen.

Det säkerhetsmässiga läget på och kring Östersjön har försämrats markant och särskilt de Baltiska staterna upplever ett ökat hot från sin ryska granne. Till skillnad från Sverige och Finland är Estland, Lettland och Litauen medlemmar i NATO. Detta skyddar dock inte från de påverkansoperationer som Ryssland genomför i syfte att destabilisera och försvaga sin omgivning och relativt sett öka sin egen styrka.

KINA

Stärkt av en mycket hög och långvarig tillväxt har Kina kunnat inta en allt mer dominerande roll globalt. I första hand har grannländerna kring Sydkinesiska sjön fått erfara de ökade kinesiska territoriella anspråken, som bland annat innefattar byggandet av konstgjorda öar i havet.

Men Kina har medvetet och långsiktigt arbetat för att öka sitt inflytande i omvärlden även längre från de egna gränserna. Inte minst har kinesiskt kapital och teknik överförts till länder runt om i världen som därmed blivit allt mer beroende av Kina. Också i Europa och Sverige ökar det kinesiska inflytandet, inte minst genom strategiska företagsförvärv, en aktivitet som Totalförsvarets forskningsinstitut (FOI) följer och dokumenterar.

Kina uppges av många källor bedriva ett mycket omfattande industrispionage riktat mot försvarsindustrier och andra ledande högteknologiska företag i Sverige. Landet är på många sätt lika aktivt i Europa som Ryssland men har ett mer långsiktigt fokus och är inte lika synligt.

Mark Galeotti påpekar att även Ryssland känner av det växande Kinas ambitioner. De båda länderna har genomfört militära övningar tillsammans, vilket utåt sett tyder på goda relationer, men förutsätter gemensamma intressen och mål. Samtidigt finns stora spänningar mellan länderna.

Galeotti menar att Ryssland om ungefär tio år kommer att behöva välja om man ska alliera sig med EU mot Kina eller om man ska bli beroende av Kina.

I Washington talar man om ett hot från Ryssland-Kina men i Moskva är man mer oroade över Kina än man är i väst. Just nu behöver Ryssland dock Kina. Man kan säga att Kina för Ryssland är som klimatförändringar: ett stort problem som det är svårt att göra så mycket åt, säger Mark Galeotti.

HYBRIDKRIGET

Oscar Jonsson beskriver kärnan i den ryska uppfattningen om modern krigföring som att gränsen mellan krig och fred successivt suddas ut. Ryska militärteoretiker har noterat att den enkla svart/vita uppdelningen mellan krig och fred har blivit mindre relevant, då de icke-militära medlens effektivitet har ökat drastiskt. Ryssland anser även att Väst regelbundet utövar sådan aktivitet gentemot ryska intressen.

Att Ryssland har en offensiv strategi i dessa sammanhang går att spåra till att landets ledning upplever ett reellt hot från Väst, främst från icke-militära medel. Den arabiska våren och det uppror som då underlättades av informationsutbyte i sociala medier blev en väckarklocka för Ryssland.

För Kreml är konfrontationer på gatorna ett större hot mot den ryska statsledningens grepp om makten än en regelrätt Nato-invasion.

När det blev tydligt vilken stor kraft för förändring icke-militära aktiviteter kan utlösa ökade Ryssland sina ansträngningar för att möta dessa hot och stärka sin egen offensiva förmåga på området. Så kallade trollfabriker, som ägnar sig åt att sprida desinformation och så split på nätet, byggdes upp för att kunna utföra omfattande påverkansoperationer. Sverige och EU mobiliserar nu för att möta den påverkan som ryska och ryskfinansierade aktörer utövar.

EN NYGAMMAL MILITÄRDOKTRIN

Mark Galeotti ogillar egentligen begreppet hybridkrig, som han menar ger bilden av att det som sker skulle vara något nytt, men menar att det är bra beskrivning av en konfliktsituation som ännu inte övergått till det vi i dagligt tal kallar krig.

> *Sovjetunionen agerade på liknande sätt och sysslade med bred propaganda i stor skala, gav stöd till organisationer, påverkade och hotade personer etc. De drog sig inte heller för våld eller mord. Den stora skillnaden är att då var öst och väst olika sfärer, ekonomiskt och kulturellt, idag är vi inom samma informationssfär. Det ger andra möjligheter att agera, menar Mark Galeotti.*

Tidigare krävde en påverkansoperation ofta långa och komplicerade förberedelser under månader eller till och med år.

Det gäller exempelvis försöket att anklaga USA för att ha skapat och spridit AIDS genom ett misslyckat militärt test med biologiska stridsmedel. Då var man tvungna att plantera falsk information långt i förväg och låta den vandra igenom den internationella pressen innan den började påverka amerikanska intressen.

I dagens sammankopplade värld är denna typ av operationer betydligt lättare och snabbare att genomföra. Det innebär också att desinformationen inte behöver handla om att skapa nya konflikter. Det kan istället ofta vara snabbare och effektivare att underblåsa befintliga konflikter inom länder som det ligger i Rysslands intresse att försvaga.

SÖNDRA UTAN ATT HÄRSKA

Även om Ryssland har återuppbyggt sin militära förmåga till en imponerande kapacitet är USA och NATO totalt sett betydligt starkare. Inte minst ekonomiskt, Ryssland har trots sin storlek en ekonomi som är ungefär lika stor som Spaniens, enligt Galeotti.

Samtidigt är den ryska upprustningen inte beroende av import i någon större utsträckning, vilket gör att sanktioner sällan får effekt. Det begränsade ekonomiska beroendet av omvärlden innebär också att en svag ekonomi mätt i amerikanska dollar ger ett falskt mått på köpkraften. Det kan därför vara svårt att jämföra de ryska försvarsanslagen med andra länders.

Mark Galeotti konstaterar att Ryssland inte drivs av någon nämnvärd s k ideologiexport, till skillnad från Sovjetunionen som även rent politiskt försökte sprida kommunismen globalt.

Snarare handlar de nuvarande ryska insatserna om att återupprätta Ryssland som en stormakt med en egen inflytandesfär och veto i världspolitiken med rätt att – när man upplever ett sådant behov – ibland sätta sig över internationella spelregler för att skydda sina egna intressen.

Eftersom Västländerna med alla mått mätt är starkare förlitar sig Ryssland på s k asymmetriska aktiviteter, där man kan slå över sin egen viktklass. Allt sedan Sovjettiden har Ryssland en kompetent underrättelsetjänst med uppgift att inte bara tolka vad som händer i omvärlden, utan också aktivt påverka händelseförlopp.

Om det anses motiverat antas den ryska underrättelsetjänsten inte dra sig för mord. Ett av de mest uppmärksammade mordförsöken med kopplingar till ryska underrättelsetjänsten ägde rum i brittiska Salisbury 2018, då den ryska ex-agenten Sergej Skripal och hans dotter förgiftades med nervgift.

> *Putin förlitar sig på underrättelsetjänsten för att det är det verktyg han har. Men det finns också goda nyheter, vi känner till det mesta ryssarna är inblandade i. Vi har kontroll på deras trollfabriker och hur de jobbar för att överdriva och förgifta debatten, sprida desinformation och ”alternativa förklaringar” till händelser, beskriver Mark Galeotti.*

Risken är att vi fokuserar på de synliga påverkansoperationerna samtidigt som de osynliga pågår med samma aggressivitet som under kalla kriget. De påverkar politiker, individer och det är ett lika allvarligt hot som den öppnare påverkan och vi borde fokusera mer på den, anser Mark Galeotti.

Militär eller ekonomisk styrka är ett relativt mått. Ryssland stärks när de länder som upplevs som fiender försvagas genom osämja och interna stridigheter. När exempelvis EU:s medlemsländer inte är eniga och kan uppvisa en enad front gentemot exempelvis rysk aggression, stärks Ryssland. Ur det perspektivet är det lätt att förstå att ryska påverkansoperationer i enskilda länder är intressanta för Moskva. Små riktade insatser kan ge stor utdelning.

EN DISTRAHERAD FIENDE ÄR EN SVAG FIENDE

Ryska militärteoretiker menar att när andra medel än de traditionella militära är mer effektiva så förändrar det förståelsen av krig. Fokus ligger mer på konsekvenserna än medlen för att uppnå ett visst mål. Om politisk instabilitet kan skapas i ett land som anses vara fientligt, t ex genom att underblåsa befintliga konflikter i landet, så är det ett intressant område att satsa resurser på.

Även om effekten av den ryska inblandningen i den besvärliga Brexit-processen är svår att avgöra så är den ett tydligt exempel på hur politiska motsättningar kan försvaga eller delvis förlama ett land. Med tanke på all den politiska energi Brexit-processen tar finns inte mycket utrymme att hantera andra frågor i Storbritannien. För övriga EU tar Brexit också stort utrymme och försvagar unionen. Ett oenigt och distraherat EU gör Ryssland relativt starkare, även om den ryska situationen inte i sig har förändrats.

Ett sätt att destabilisera andra länder kan t ex vara att stötta populistpartier, oavsett var dessa befinner sig på

höger/vänster-skalan, för att deras politiska inflytande ska polarisera debatt och politik.

> *En av de mer fascinerande delarna av det pågående informationskriget är att Ryssland lyckas framstå som att de kan hjälpa både högern och vänstern samtidigt. I Italien stöds både den yttersta vänstern och yttersta högern samtidigt av Ryssland. Ryssarna är mindre intresserade av att försöka påverka val, eftersom det inte fungerar, och desto mer av att fördjupa politiska konflikter, säger Mark Galeotti.*

Att påverka en opinion är svårt. De ryska framgångarna har underlättats av att många redan haft en känsla av att media och politiker ljuger, och därför är mer mottagliga när någon sprider konspirationsteorier. Ett lågt förtroende för staten och politiker gör ett samhälle mottagligt för påverkansoperationer.

Mark Galeotti framhåller att det mest verkningsfulla vaccinet mot påverkan är att politiker och stat försäkrar sig om att stärka sin egen legitimitet och bygga förtroende mellan väljare och valda.

EN JAKT PÅ ENKLA SEGRAR

De ryska påverkansoperationer som pågår och planeras är inte nödvändigtvis delar i en större noggrant regisserad konspiration. Snarare är de resultat av opportunism och en decentraliserad underrättelsetjänst som tar egna initiativ.

Putin inspirerar, men underrättelsetjänsterna agerar själva och letar efter enkla segrar. De använder kriminella om det behövs för att påverka personer med inflytande över politiken, konstaterar Mark Galeotti.

Rysk underrättelsetjänst är flexibel så till vida att de använder de metoder och verktyg som står till förfogande för stunden. Det kan vara organiserad brottslighet, ideella organisationer eller företag som engageras, beroende på vad som behövs.

Det är inte ovanligt att organiserad brottslighet finansierar underrättelseorganisationer. Detta pragmatiska synsätt på medel och samarbetspartners ökar risken för att svenska företag och företagare dras in i underrättelseoperationer, utan att vara medvetna om det.

FÖRETAGEN ÄR OCKSÅ BRICKOR I UNDERRÄTTELSESPELET

Inget företag vill förstås bli indraget i denna typ av verksamhet, men i praktiken kan det vara svårt att hålla sig undan. Exempelvis kan en bank riskera att på olika sätt indirekt hjälpa både organiserad brottslighet och underrättelseagenter med finansiella tjänster utan att känna till det.

Det har också visat sig att företag med verksamhet i andra länder emellanåt fungerat som täckmantel för underrättelseagenter. Om en auktoritär stat skulle begära tjänster av dess företag eller medborgare finns det i praktiken mycket begränsade möjligheter att vägra att utföra tjänsterna.

Denna typ av inflytande är ofta mycket svårt att upptäcka. Snåriga bolagskonstruktioner gör det svårt för svenska

företag att veta om de företag som de gör affärer med har koppling till främmande underrättelsetjänster, eller kriminella organisationer med kopplingar till underättelsetjänst. Det kan också bli ett stort problem om det senare visar sig att man gjort affärer med ett företag som finns med på västländernas sanktionslistor.

Svenska företag och företagare är intressanta för utländska underrättelsetjänster som vill förmå företagen att använda sina affärskontakter för inflytande och olika typer av tjänster. Kontakter odlas genom mutor, korruption och erbjudanden om särskilt gynnsamma affärer. När en person väl korrumperats är grunden för framtida utpressning och fler ”tjänster” lagd.

> *Rysk underrättelsetjänst är extremt kompetent och har global räckvidd. Om man hittar nyckelpersoner som har brister som gör dem utsatta kan underrättelsetjänsten t ex lägga in något på deras datorer eller utpressa dem. De söker även upp personer som känner sig svikna och förbigångna av sina arbetsgivare och försöker muta dem, säger Oscar Jonsson.*

För att undvika att hamna i klorna på en utländsk underrättelsetjänst behöver svenska företagare vara uppmärksamma på märkliga affärsförslag och göra en noggrann due diligence (företagsbesiktning) i sina affärskontakter. Man måste också ta sitt eget säkerhetsarbete på allvar, det gäller särskilt företag som arbetar med teknologi som kan ha en militär tillämpning.

FÖRSÄMRAT SÄKERHETSLÄGE KRÄVER UPPRUSTNING

Det svenska totalförsvaret är nu åter under uppbyggnad efter den långa period av nedrustning som följde efter Sovjetunionens och Öststatskommunismens fall i början av 1990-talet. Skälen till detta är främst Rysslands aggressiva utrikespolitik och den ökade oron i omvärlden.

TOTALT FÖRSVAR

De scenarion som Sverige behöver förbereda sig på är inte i första hand en invasion av främmande makt. Sverige måste vara rustat för angrepp i flera olika dimensioner. Det gäller dels hybridkrig som beskrivs ovan, men också olika former av sabotage som t ex cyberangrepp som syftar till att slå ut strategisk infrastruktur som elförsörjning, kommunikations- och betalsystem.

Totalförsvaret är benämningen på det militära och civila försvarets sammanlagda förmåga, dvs även på en civil beredskap och förmåga som till stor del upprätthålls av näringslivets ordinarie verksamheter.

FÖRETAGENS BETYDELSE FÖR TOTALFÖRSVARET

Även angrepp mot företag kan ha säkerhetspolitiska motiv eller få säkerhetspolitiska konsekvenser. Den svenska Säkerhetsskyddslagen (2018:585) gäller ”den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd”. Denna definition omfattar uttryckligen även privata företag.[75]

Myndigheten för samhällsskydd och beredskap (MSB) och Försvarsmakten har tillsammans utarbetat en gemensam grundsyn för totalförsvaret. Denna omfattar en beskrivning av förutsättningar och politisk inriktning, identifierade behov, en handlingsplan för vägen framåt samt en gemensam syn på hotbild som utgångspunkt för planeringen. I denna beskrivning påpekas att svenska företag måste stärka sin förmåga att kunna stå emot angrepp av olika slag.

Samtidigt ligger det i statens intresse att underlätta för företagen att ta ansvar för att stå emot angrepp. Ett exempel är offentliga upphandlingar, där staten behöver väga in leverantörens förmåga att klara kriser av olika slag. Upphandlingar kan helt enkelt inte bara handla om lägsta pris utan också om leveransförmåga i krissituationer, vilket förstås kommer påverka priset.

> *Företag har inte något direkt incitament att skaffa sig en förmåga att klara sig under exempelvis tre månaders avstängning eftersom det inte är något som kunder vanligtvis efterfrågar. Det finns därför en naturlig ovilja att t ex bygga upp lager, säger Martin Allard.*

ENSKILDA FÖRETAG VIKTIGA FÖR FÖRSVARSFÖRMÅGAN

Eftersom många företag har betydelsefulla roller för totalförsvaret är det också viktigt att engagera näringslivet i försvarsförmågehöjande insatser. Det kan samtidigt innebära kostnader och i viss mån besvär för företagen. För att det ska gå att skapa engagemang och acceptans för olika åtgärder menar

Martin Allard att det krävs ett partnerskap mellan offentliga och privata aktörer, för att analysera behov och kostnader.

I en broschyr från Överstyrelsen för civil beredskap (MSB:s föregångare) i samarbete med SAF (nuvarande Svenskt Näringsliv) från mitten på 90-talet presenterades företagens åtaganden också som ett slags förmån.

– Det är nödvändigt att hitta en balanspunkt mellan åtaganden och förmåner, som t ex att få sitta med vid bordet och kunna påverka och få inblick i myndigheternas planering. Myndigheterna kan inte göra det vanliga misstaget att bara tala med varandra. De behöver inse att företagen är en viktig del i samhället, säger Martin Allard.

I en allvarlig krissituation kan totalförsvaret behöva ta företags resurser i anspråk. Det är då viktigt att företagen ersätts för sin beredskap, även man kan hävda att företagen har ett ansvar att ställa upp behöver anspråken upplevas som rimliga. Om staten ställer ohållbara krav på företagen utan att erbjuda rimlig kompensation finns en risk att försvarsförmågan sänks genom att företag helt enkelt flyttar utomlands.

Det behövs en avvägning av militärt och civilt försvar. Om Försvarsmakten tar exempelvis lastbilar i anspråk som förberedelser inför ett eventuellt förfogande innebär det en lastbil mindre som kan betjäna behoven inom det civila försvaret. Det finns en uppenbar risk att myndigheterna gör fort och fel om man inte betraktar totalförsvarets behov som en helhet, anser Martin Allard.

LÅNGSIKTIGT ARBETE ATT HÖJA FÖRSVARSFÖRMÅGAN

Regeringen beslutade 2015 att återuppta försvarsplaneringen. Efter det har mycket hänt även om ett omfattande arbete återstår. Sverige har utvecklat och fördjupat försvarssamarbeten med andra länder och ökat försvarsanslagen. Samtidigt pågår utredningar om civilförsvarslagstiftningen och sektorsansvar för myndigheter som båda är viktiga för företagen.

> *Allt kommer inte att vara fantastiskt när krisen kommer, vi behöver tio år för att bygga upp förmågan ordentligt. Men det är inte säkert att vi får tio år, kriser som de senaste årens skogsbränder uppstår regelbundet och då får man försöka lösa det med de resurser som finns, menar Oscar Jonsson.*

Det är viktigt att myndigheterna analyserar risker och förutsättningarna för att hantera olika kriser. Även om de viktigaste händelserna som påverkar vår säkerhet kan komma att vara omvärldshändelser, som vi idag inte har någon aning om kommer inträffa, så finns det många områden där Sverige faktiskt har kontroll och vi kan förbereda oss.

> *Det är viktigt med tydliga politiska ambitioner och förståelse för att uppbyggnaden av ett modernt totalförsvar är ett mycket långsiktigt arbete, som kräver uthållighet, betonar Martin Allard.*

Vill du veta mer?

- → Kier Giles bok Moscow Rules: What Drives Moscow to Confront the West
- → Podden I krig och fred
- → Försvarsmaktens serie Om kriget kommer finns på Youtube
- → MSB:s webbplats, www.msb.se

Fotnoter

75 https://riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/sa- kerhetsskyddslag-2018585_sfs-2018-585

APPENDIX

Om du utsätts för brott – en praktisk handledning för företag

Förundersökningsregler – vad du som företagare behöver veta

FÖRUNDERSÖKNINGEN

Mycket förenklat är en förundersökning ett slags projekt i straff- och processrätt som leds av en förundersökningsledare. En förundersökningsledare kan vara både en polisanställd eller en åklagare. Ärenden som bedöms vara av *icke enkel beskaffenhet* ska som huvudregel ledas av en åklagare och övriga ärenden av en anställd inom Polisen som har en särskild förundersökningsledarbehörighet. De brott som brukar benämnas ”mängdbrott” (ringa stölder i butik, övriga ringa stölder och stölder, inbrott, skadegörelser, bedrägerier, misshandlar, olaga hot o s v.) leds i de allra flesta fall av en förundersökningsledare inom Polisen.

Förundersökningen handlar om att utreda ett eller flera brott som är under s k allmänt åtal och att i det arbetet samla in och rättssäkert säkra bevisning. (Allmänt åtal, se avsnitt A nedan.) Detta arbete görs för att skapa ett underlag för

bedömningen av om brottet/brotten kommer att hålla hela vägen till åtal och fällande dom. I arbetet behöver förundersökningsledaren ha goda kunskaper om bevisvärdering för att kunna sortera bevisningen i ärendet som ”stark” eller ”svag”. Svårigheten att avgöra om bevisningen styrka varierar från fall till fall.

FÖRUNDERSÖKNINGSREGLERNA

Förundersökningsreglerna är många och komplicerade. Reglernas huvuddrag är dock enkla och värda att känna till. Rättegångsbalken är huvudlagen på området och till den lagen finns även viktiga regleringar i bl a Förundersökningskungörelsen.

I dessa rättsregler framkommer flera s k ”rättsliga principer”. En sådan, och en av de allra viktigaste, är att en förundersökning ska bedrivas objektivt. Inget får låsas fast, en förundersökningsledare får aldrig ”köra på” i ett ursprungligt spår i vilket ”det är X som är tjuven” och fastna där. Om det under den pågående förundersökningen säkras bevisning som talar för att det inte alls är X som är tjuven måste förundersökningen byta fokus.

Givetvis arbetar en förundersökningsledare med olika alternativ och vissa hypoteser om gärningspersoner kan vara mer troliga än andra, varför vissa ärenden drivs åt ett och samma håll med en misstänkt person som huvudmisstänkt. Det viktiga är dock att hela tiden vara öppen för att det inledande spåret kan vara fel och i så fall ändra kurs mot en annan misstänkt. Det är denna dynamik – med löpande säkring och värdering av bevisning – som kännetecknar en korrekt, objektiv och rättssäker förundersökning.

BEVISNING

Huruvida bevisning är ”stark” eller ”svag” (avsnitt B nedan) är förenklat uttryckt kärnan i förundersökningsarbetet. Det kan vara bra att som företagare känna till detta, för att om möjligt kunna bidra med så mycket ”stark” bevisning som möjligt vid t ex en anmälan om brott.

Att du som företagare, och i en situation som målsägande, redan vid anmälningstillfället kan berätta för Polisen att det finns en övervakningskamera på platsen, att det verkar finnas vittnen som är oberoende i förhållande till dig och annan relevant information underlättar den polisanställdes bedömning av kvaliteten på ärendet.

Om du vet vilka överväganden förundersökningsledaren kommer att behöva göra för att bedöma om det finns potential att driva ärendet vidare fram till en fällande dom kan du lämna mer värdefulla uppgifter. Vet du om vad Polisen kommer att bedöma som ”stark” och ”svag” bevisning är det också lättare att förstå om ett ärende *inte* leder vidare. Om Polisen bara tar upp en anmälan och håller ett förhör med dig som målsägande och det inte finns mer bevisning att gå på är det inte förvånande om ärendet inte leder till åtal.

FÖRUNDERSÖKNINGSBEGRÄNSNING

Ibland kan det vara svårt att förstå varför rättsväsendet lägger ned brottsutredningar, särskilt om man själv är målsägande. För att öka förståelsen och moderera förväntan på rättsväsendet behöver man känna till förundersökningsbegränsning (avsnitt C nedan).

En utredning om ringa stöld i butik kan läggas ned för att den FU-begränsas mot en misstanke om ett grövre brott som samme misstänkte person är åtalad för. Reglerna om FU-begränsning uppfattas dock inte sällan som orättvisa och får också ofta kritik från målsäganden som har svårt att acceptera att en förundersökning kan läggas ned när det finns en misstänkt. Det är bra att som brottsdrabbad känna till det regelverk som polisanställda och åklagare är styrda av.

Även beslut om FU-begränsning kan vara felaktiga. Den som är målsägande i ett ärende som läggs ned med hänvisning till FU-begränsning har rätt att begära omprövning av beslutet.

RÄTTEN ATT BEGÄRA UT HANDLINGAR OCH RÄTTEN ATT BEGÄRA OMPRÖVNING

Besluten om att lägga ned en förundersökning kan vara felaktiga, både vad gäller beslut om FU-begränsning och beslut som grundar sig på att förundersökningsledaren anser att det finns bevisproblem. Då är det också viktigt att veta hur du kan begära ut handlingar ur en förundersökning (avsnitt D nedan) och hur du kan begära en omprövning av ett beslut som du anser är felaktigt (avsnitt E nedan).

KUNSKAP GER ETT FÖRSPRÅNG GENTEMOT ANDRA MÅLSÄGANDEN

Det är tyvärr nödvändigt att som företagare ha en viss kunskap om förundersökningsreglerna. Polisens utredningsverksamhet är mycket eftersatt beträffande de s k ”mängdbrotten”.

I och med det ökar risken att beslut om att inte inleda eller lägga ned en förundersökning inte vilar på den rättssäkra grund som de ska. Att som företagare då veta om hur man begär ut handlingar och begär en omprövning av beslut om att inte utreda brott får då kvalitetssäkrande effekt på Polisens arbete.

Har du dessa verktyg kan du säkerställa din egen rättssäkerhet. Om du dessutom har kunskap om hur bevisning bedöms och säkras på bästa sätt ger det dig också bättre förutsättningar att få ditt ärende kvalitativt hanterat. Kvalitativa anmälningar med angivande av möjlig ”stark” bevisning gör det lättare för Polisen att driva förundersökningen. Bristfälliga, röriga anmälningar upprättade av en anmälare som inte känner till skillnaden av olika typer av bevisning gör inte förundersökningsarbetet lättare.

Att målsägare kan lite om förundersökningar verkar kvalitetshöjande och förbättrar rättssäkerheten både vid själva anmälningsupptagningen, liksom vid ett mottagande av beslut om en nedlagd förundersökning. Med denna kunskap får målsägaren en tydligare och starkare röst gentemot myndigheterna och kan agera mer slagkraftigt när det borde göras mer i ett ärende. Samtidigt kan kunskapen förhoppningsvis också få bort viss frustration kring de ärenden som trots allt läggs ned.

A. Brott under allmänt åtal och Polisens rapporteringsskyldighet

ALLMÄNT ÅTAL

I Sverige finns det två olika kategorier av brott – de som är under s k ”allmänt åtal” och de brott som inte är det. De allra flesta brott är under allmänt åtal och av de brott som brukar benämnas ”mängdbrott” (stölder, inbrott, skadegörelser, bedrägerier, misshandlar, olaga hot) är alla det. Detta får betydelse för vilka skyldigheter Polisen i Sverige har.

POLISENS RAPPORTERINGSSKYLDIGHET

En polismans rapporteringsskyldighet stadgas i 9 § Polislagen:

> *”När en polisman får kännedom om ett brott som hör under allmänt åtal, skall han lämna rapport om det till sin förman så snart det kan ske.*
>
> *En polisman får lämna rapporteftergift om brottet med hänsyn till omständigheterna i det särskilda fallet är obetydligt och det är uppenbart att brottet inte skulle föranleda annan påföljd än böter.”*

Om en polisman får kännedom om ett brott under allmänt åtal, ska polismannen alltså som huvudregel skriva en rapport/anmälan om detta ”så snart det kan ske”. Denna skyldighet innebär också en rättighet för invånare i Sverige att (som huvudregel) få en polisanmälan upprättad med anledning av ett brott.

OM POLISEN INTE TAR UPP EN ANMÄLAN?

Om polismannen inte tar upp en anmälan med dig som målsägande ska du be att av polismannen få en motivering i skrift till varför så inte sker.

OM POLISMANNEN HÄNVISAR TILL REGELN OM RAPPORTEFTERGIFT

Om du som målsägande inte håller med polismannen om att det brott du vill anmäla är så pass obetydligt att en rapporteftergift ska lämnas har du rätt att göra en s k missnöjesanmälan.

En sådan kan du lämna i skrift till polismannen som beslutade om rapporteftergiften. Din missnöjesanmälan kommer sedan att prövas internt inom Polisen. Är du som målsägande inte heller nöjd med det beslut som Polismyndigheten fattar har du rätt att begära att Åklagarmyndigheten ska pröva frågan.

B. Bevisning i brottmål

KRAV PÅ BEVISNING – FÖR RÄTTSSÄKERHETEN

För att någon ska kunna dömas för ett brott krävs bevis. Exempelvis räcker det inte med att en person A går till Polisen, visar sin tomma väska och påstår sig ha blivit bestulen på sin plånbok av person B. Det behövs s k ”stödbevisning” som styrker att person B verkligen tagit person A:s plånbok.

MUNTLIG OCH SKRIFTLIG BEVISNING

Person A i exemplet berättar för Polisen att det var B som tog plånboken men att platsen det skedde på, enligt A, var folktom. För A är det ”självklart” att detta har hänt och A:s berättelse, som målsägande, skriver Polisen ned i ett förhör – muntlig bevisning.

Det svenska rättsväsendet kommer dock inte att med endast detta kunna döma B för stöld, eftersom den bevisning som finns enbart baseras på en enda persons information – den drabbade själv person A:s.

”STARK” OCH ”SVAG” BEVISNING

Förenklat är den bevisning som finns i ärendet är för ”svag”, även om person A i sig är tydlig. Problemet är att det inte går att objektivt bedöma A:s uppgifter. A kan ljuga. Ärendet kan tas vidare genom att Polisen exempelvis kontrollerar om det finns någon övervakningskamera.

Då kommer en till dimension in i ärendet – ett slags objektivt vittne som typiskt sett är att se som ”stark” bevisning. Om en övervakningsfilm visar samma sak som A påstått finns det s k stödbevisning för A:s påstående och det finns anledning att eftersöka B.

Att tänka på om bevisning när brott anmäls

→ Om du själv blivit utsatt för ett brott kommer dina egna uppgifter om vad som hänt inte räcka för att någon ska kunna fällas till ansvar.

↓ Det bästa är om det finns objektiv stödbevisning, t ex:
  → Film från en övervakningskamera – och då är det viktigt att se till att filmen säkras så snabbt som möjligt i anslutning till brottet. Typiskt sett är övervakningsfilmer ”stark” bevisning.
  → Kontoutdrag från bank (t ex vid bedrägerier) är också ”stark” bevisning.

↓ Ett vittne kan både vara ”svag” och ”stark” bevisning, t ex:
  → ”Svag”: En påverkad person, en person med dålig syn, en person du känner väl och som möjligen inte är helt objektiv, en person som var upptagen med något annat under tiden.
  → ”Stark”: En nykter person, en person med perfekt syn, en helt oberoende människa som bara råkade passera, en person som hade sin totala uppmärksamhet på händelsen.

C. Förundersökningsbegränsning

FÖR EN EFFEKTIVARE HANDLÄGGNING AV BROTT

Förenklat är Förundersökningsbegränsning (FU-begränsning) ett rättsligt verktyg för att effektivisera handläggningen av brott genom hela rättskedjan (Polisen – Åklagarmyndigheten – Domstolarna). I praktiken betyder det att vissa brott inte kommer att utredas – även då det står klart vem som begått brottet och det finns ”stark” bevisning.

Vilka dessa brott är och i vilka situationer FU-begränsning sker och hur FU-begränsningar är tänkt att fungera beskrivs nedan, efter en kort genomgång av den svenska rättskedjan.

DOMSTOLARNA BESTÄMMER STRAFFET – I SVERIGE LÄGGS INTE STRAFF IHOP

I USA kan en person dömas till över hundra års fängelse. Till skillnad från i USA läggs straff inte automatiskt ihop i svensk rätt. Enligt reglerna i brottsbalken blir inte straffet dubbelt så långt om en person döms för två stölder i stället för en, eller för tio bedrägerier i stället för fem.

Ett exempel kan vara att person C står åtalad för ett eller flera grova brott, exempelvis en grov misshandel och en grov stöld, med ”stark” bevisning i båda fallen.

Troligtvis kommer då C att dömas för båda dessa grova brott. Det spelar dock ingen roll för straffets längd om C samtidigt skulle dömas för ett eller flera mindre allvarliga brott, t ex ringa stölder, bedrägerier på låga belopp eller liknande s k ”mängdbrott”. Domstolen kommer inte att ”slå ihop” straff, utan istället når domstolen ett tak för straffets längd. Det är så den svenska straffmätningen går till.

Detta brukar i media beskrivas som att vi i Sverige har straff- och mängdrabatter. Det svenska systemet med straffmätning har bedömts som nödvändigt för att strafftiderna inte ska bli orimligt långa.

Straffmätningen får effekt för polisernas och åklagarnas arbete, eftersom det inte alltid är lönt att utreda alla brott som en och samma person är misstänkt för, då det inte kommer att påverka domstolens straffmätning. Den svenska lagen ger alltså stora möjligheter att avstå från utredning och åtal mot en misstänkt för brott som inte skulle få någon eller bara liten betydelse för straffmätningen. Det är en konsekvens av FU-begränsning. Det huvudsakliga syftet med

FU-begränsning är att rättsväsendets personalresurser ska användas så effektivt som möjligt.

FÖRUTSÄTTNINGAR FÖR FU-BEGRÄNSNING

Förenklat kan man säga att det handlar om mindre allvarliga brott, de brott som ofta benämns mängdbrott och som begås av någon av följande typ av gärningsman:

1. En förstagångsförbrytare i en mindre allvarlig situation som kan beskrivas som en ”en gång ingen gång”-situation.
2. Brottsaktiva personer som är misstänkta/åtalade för grövre brott parallellt med ringare brott.

I exemplet med person C ovan, kommer C att dömas för grov misshandel och grov stöld. Det innebär att de enklare brotten, som exempelvis ringa stölder i butik, troligen inte kommer att utredas, eftersom de kommer att FU-begränsas.

Här kan ett exempel vara person D som är misstänkt för tusen bedrägerier av normalfallet – alla med ganska låga belopp om 5 000 kronor – 10 000 kronor per brott. Det finns inte en åklagare som kommer att åtala in alla dessa tusen bedrägerier, eftersom åklagaren vet att domstolen inte kommer att plussa straffen.

Istället kommer domstolen i sin straffmätning att nå ett tak för straffets längd och därefter får fler åtalade brott ingen effekt på straffets längd. Med vetskap om detta kommer inte heller Polisen att utreda tusen bedrägerier eftersom många av dem kommer att FU-begränsas. Detta trots att Polisen vet vem som begått brotten.

Reglerna om straffmätning styr domstolarnas utdömande av straff – och dessa styr i sin tur vilka brott som Polisen och Åklagarmyndigheten kommer att arbeta i och vilka brott som FU-begränsas.

FU-BEGRÄNSNINGEN EFFEKTIVITET

Tanken bakom reglerna om FU-begränsning är att göra brottsbekämpningen mer effektiv genom att polis och åklagare har möjlighet att koncentrera utredningsresurserna till de uppgifter som är mest angelägna. Utöver att styra resurserna till utredningsinsatser för att bekämpa allvarligare brottslighet bidrar FU-begränsningen till att utredningar avslutas inom rimlig tid, vilket får anses ligga i både misstänkt och målsägares intresse.

OMPRÖVNING AV BESLUT OM FU-BEGRÄNSNING

Även om FU-begränsning beslutats i ett ärende kan målsäganden anse att ärendet ska utredas. Utredningen kan återupptas efter att målsäganden begärt omprövning av beslutet om FU-begränsning. Det finns andra intressen än straffets längd som kan motivera att ett ärende ska utredas, åtalas och dömas. Bedömningar ska göras i det enskilda fallet och ett beslut om FU-begränsning kan vara felaktigt.

D. Grundläggande om rättigheterna att begära ut handlingar ur en förundersökning

OFFENTLIGHETS- OCH SEKRETESSLAGEN

Offentlighets- och sekretesslagen (2009:400) är alltför omfattande för att behandlas här men det är ändå bra att känna till något om den rätt lagen ger en målsägande att ta del av handlingar. Exempelvis har målsäganden rätt att ta del av innehåll ur ärenden som polis eller åklagare beslutat att antingen inte alls arbeta i eller att lägga ned.

NÄR POLISEN LAGT NED EN FÖRUNDERSÖKNING

Låt oss säga att du har anmält ett brott, t ex en stöld, och sedan får ett beslut om att Polisen har lagt ned förundersökningen. Antingen förstår du beslutet och tycker att det är i sin ordning. Men det kan också vara så att förundersökningen, så vitt du vet, har lagts ned utan att Polisen gjort den utredning som du anser behövs i ärendet. Alla vittnen kanske inte har hörts av Polisen.

Det kan som målsägare vara svårt att bedöma utsikterna för att en begäran om omprövning av ett beslut om nedlagd förundersökning ska leda till att förundersökningen återupptas.

RÄTTEN ATT BEGÄRA UT HANDLINGARNA

För att som målsägande få mer klarhet i vad som gjorts och inte i en förundersökning är ett första steg att begära ut de handlingar som finns i ärendet. Handlingarna ger samma lägesbild av fakta och bevisning som förundersökningsledaren hade när denne fattade beslutet om att lägga ned förundersökningen.

Handlingarna lämnas ut efter att Polisen gjort en sekretessprövning av begäran att ta del av handlingarna. Handlingar som är av betydelse för målsäganden möjligheter att tillvarata sina rättigheter ska typiskt sett lämnas ut.

Om det, baserat på de relevanta handlingarna i ärendet, finns grund för att begära en omprövning av ärendet är nästa steg att formellt begära omprövningen.

E. Rätten att begära omprövning av en nedlagd förundersökning

OMPRÖVNING AV ETT MYNDIGHETSBESLUT

Alla myndighetsbeslut går inte att klaga på. Beslut av polisanställd eller åklagare att inte inleda en förundersökning eller att lägga ned en förundersökning är beslut som målsäganden har rätt att begära en omprövning av.

Låt oss säga att du har anmält ett brott, t ex en stöld, och sedan får ett beslut om att Polisen har lagt ned förundersökningen. Antingen förstår du varför beslutet fattats och tycker att det är i sin ordning. Men det kan också vara så att förundersökningen, så vitt du vet, har lagts ned utan att Polisen gjort den utredning som du anser behövs i ärendet.

I avsnittet som handlar om rätten att begära ut handlingar (avsnitt D ovan) redogörs för hur målsägandens rätt att få tillgång till samma beslutsunderlag som den som fattade beslutet om att inte inleda förundersökning, eller att lägga ned den, hade. Efter att ha begärt ut handlingarna och fått

dem är nästa steg att göra en bedömning av om det är lönt att begära en omprövning.

BEGÄRA EN OMPRÖVNING ELLER INTE?

Målsäganden som anser sig ha goda utsikter till framgång kan begära en omprövning av aktuellt beslut direkt, enligt ovan.

Om ärendet är mer komplicerat är det i regel nödvändigt att begära ut handlingarna i ärendet för att bilda sig en uppfattning om vad som är gjort och inte i förundersökningen.

Om det, baserat på de relevanta handlingarna i ärendet, finns grund för att begära en omprövning av ärendet är nästa steg att formellt begära omprövningen.

MALL – begäran om prövning av polisbeslut/överprövning av åklagarbeslut

ORT OCH DATUM

TILL DEN INSTANS DÄR BESLUTET FATTADES (Polismyndigheten/Åklagarmyndigheten/Ekobrottsmyndigheten)

SÖKANDE – du som begär omprövning/överprövning
Namn:
Personnummer:
Adress:
E-post:
Telefonnummer:
Om ombud ska dennes namn anges och fullmakt bifogas

VILKET BESLUT VILL DU HA PRÖVAT/ÖVERPRÖVAT?
Det är viktigt att ett fullständigt ärende-/diarienummer anges. Din begäran kan annars inte prövas. Ange vilken myndighet som fattat beslutet, diarienumret för ärendet, datumet för beslutet samt namnet på handläggaren.

VILKEN ÄNDRING VILL DU HA?
Prövning/överprövning av beslut hanteras skriftligen. En begäran om prövning/överprövning ska vara tydlig och fullständig när den skickas in, annars granskas ärendet normalt inte. Det är vanligtvis inte möjligt att komplettera begäran senare. Här anger du vilken ändring av beslutet som önskas, t ex att förundersökningen ska återupptas eller att åtal ska väckas.

VARFÖR VILL DU HA ÄNDRING?
Här bör du beskriva varför du är missnöjd med beslutet. Du bör också tydligt ange om du lämnar någon information som inte har lämnats tidigare.

VILL DU LÄMNA IN NÅGRA NYA HANDLINGAR?
De ska i så fall lämnas in tillsammans med denna begäran. Handlingar som redan finns hos Polisen/Åklagarmyndigheten ska inte lämnas in.

UNDERTECKNANDE MED NAMN AV DEN SOM BEGÄR OMPRÖVNING/ÖVERPRÖVNING

APPENDIX

En enkel modell för riskanalys

Allt arbete med att hantera risker – oavsett vilken typ av verksamhet det handlar om – bör utgå från ett logiskt tänkesätt, som genomförs systematiskt, repeteras regelbundet och (om möjligt) inte ändras efter hand.

Ett vedertaget begrepp för ett sådant tänkesätt är den s k riskcykeln. Riskcykeln består av fyra huvudmoment.

- Riskanalys. Här identifierar man risker, bedömer sannolikheten för att en viss händelse ska inträffa och värderar konsekvenserna av att det sker.
- Policy. Här lägger man fast vilken skyddsnivå man vill uppnå.
- Skyddsplan. Här bestämmer man vilka åtgärder som ska vidtas för att uppnå den bestämda skyddsnivån.
- Uppföljning. Efter att man vidtagit de beslutade åtgärderna prövas om man uppnått den avsedda balansen mellan de identifierade riskerna och de genomförda skyddsåtgärderna.

Efter att detta arbete är slutfört så återupptas moment A i riskcykeln. Hur lång tid som ska förflyta mellan uppföljningen

och det förnyade riskcykelarbetet är helt och hållet beroende av organisationens behov. I ett litet företag kan det kanske gå år emellan, i ett stort företag kan riskcykeln behöva löpa med kortare mellanrum. Självfallet kan en inträffad skadehändelse föranleda att riskcykelarbetet omedelbart måste återupptas.

RISKANALYS

I riskcykelarbetet är analysen av vilka risker som kan finnas, och hur de ska bedömas, grundläggande. Det är också på detta område som många upplever de största svårigheterna. Hur ska man egentligen gå till väga? Det finns flera modeller för analysarbete av detta slag – här följer en beskrivning av en av de enklaste.

IDENTIFIERA RISKER

Varje verksamhet är i någon mening unik, men de risker som finns är i någon mening allmängiltiga. Oavsett vad man ägnar sig åt så involverar verksamheten alltid människor, material, byggnader och penningflöden. I många verksamheter finns det också betydande tillgångar i form av patent, företagshemligheter och andra immateriella tillgångar.

Människor – både i och utanför verksamheten – kan förorsaka skador genom t ex stöld (både av material och intellektuell egendom), bedrägeri, skadegörelse, brand etc. Material – oavsett om det består i utrustning eller förbrukningsvaror – kan orsaka eller bli föremål för brand, stöld, skadegörelse, lagerskador, maskinskador etc. Byggnader är utsatta

för liknande risker. Penningflöden är alltid känsliga, både för brottsliga angrepp och tekniska fel. Och nästan alla verksamheter är idag beroende av störningsfri tillgång till el och datorkraft.

I de flesta fall brukar det efter en stunds eftertanke vara ganska lätt att identifiera vilka sorts risker som finns i just den egna verksamheten. Att identifiera dem är ofta ganska enkelt, men att bedöma konsekvenserna av att en viss händelse inträffar kan vara svårare, och att värdera helheten kan vara ännu något svårare. Ett enkelt tillvägagångssätt beskrivs nedan.

VÄRDERA RISKERNA

- För varje identifierad risk sätts ett sannolikhetsvärde på 1-3. Ett värde på 1 innebär att den bedömda sannolikheten för att något ska hända är låg, medan 3 innebär att risken är hög. Om man inte kan bestämma sig för huruvida risken är låg eller hög sätts värdet till 2.
- För varje identifierad risk åsätts ett konsekvensvärde på 1-3. Ett värde på 1 innebär att den bedömda konsekvensen av att något inträffar är liten, medan 3 innebär att konsekvensen av händelsen är stor. Om man inte kan bestämma sig för huruvida konsekvensen av en händelse är stor eller liten sätts värdet till 2.
- I nästa steg summeras sannolikhetsvärdet och konsekvensvärdet för varje identifierad risk.
    A. Om summan är 2 kan risknivån anses vara acceptabel. Sannolikheten för att något ska inträffa är låg, och konsekvensen därav är liten.

B. Om summan är 3 eller 4 är risknivån oacceptabel, och saken bör åtgärdas. Exempelvis kanske sannolikheten för en viss händelse är låg, men konsekvenserna om den inträffar är stora, eller omvänt.
C. Om summan är 5 eller 6 är risknivån mycket eller katastrofalt hög. Omedelbara åtgärder krävs.

I samtliga fall måste man hålla sig strikt till den logiska modellen. Man får t ex inte låta sig påverkas i sin sannolikhetsbedömning av en viss händelse, av förhandskunskapen om att konsekvensen är stor. Inte heller får man låta vetskapen om ett lågt skyddsvärde påverka sannolikhetsbedömningen – om det t ex är stor sannolikhet för totalförlust, men skyddsvärdet är lågt så blir ändå risknivån oacceptabel och bör åtgärdas.

Riskanalysmodellen ovan är medvetet enkel och syftar att uppmuntra företag som ej ännu påbörjat ett systematiskt riskanalysarbete att påbörja ett sådant. Företag som omfattas av den nya säkerhetsskyddslagen bör ta del av den information och vägledning som finns tillgänglig på Säkerhetspolisens hemsida: HTTPS://WWW.SAKERHETSPOLISEN.SE/SAKERHETSSKYDD.HTML

Medverkande experter

MARTIN ALLARD, principalkonsult och strategisk rådgivare på det globala säkerhetsföretaget 4C Strategies, bakgrund inom strategisk analys i Regeringskansliet och har bland annat varit sekreterare i utredningen om totalförsvarets försörjningstrygghet.

PIERRE ANDERBERG, Chief Information Security Officer på Sveriges största försvarsindustriföretag Saab och har en bakgrund inom Försvarsmakten.

ANN-CHARLOTTE BJÖRK SÖDERLUND, advokat vid Gozzo Advokater med stor erfarenhet av frågor som rör piratkopiering och skydd av immateriella rättigheter, grundare av Swedish Anti-Counterfeit Group som flera uppdrag som sakkunnig på EU-nivå.

MARK GALEOTTI, hedersprofessor vid University College London, grundare av konsultfirman Mayac Intelligence och en av världens främsta experter på ryska säkerhetsfrågor och organiserad brottslighet, författare till flera böcker i ämnet bl a *We Need To Talk About Putin* (2019) och *The Vory: Russia's Super Mafia* (2018).

PER GEIJER, säkerhetschef på branschorganisationen Svensk Handel med 9 000 medlemsföretag inom parti- och detaljhandel som ger arbete åt 300 000 personer.

PETER HEDIN, Senior Enforcement Policy Advisor, Patent- och registreringsverkets (PRV) och har en bakgrund som expert vid bl a EU:s varumärkesmyndighet Office for Harmonisation in The Internal Market, Trademarks and Designs (OHIM).

NIGEL IYER, internationell bedrägeriexpert, grundare av startupbolaget B4 Investigate och författare till ett flertal böcker på området, senast *How to Find Fraud and Corruption* (2019).

OSCAR JONSSON, tidigare chef för den utrikes- och säkerhetspolitiska tankesmedjan Frivärld, bakgrund som forskare vid Försvarshögskolan, författare till boken *The Russian Understanding of War: Blurring the Lines between War and Peace* (2019).

PER KLINGVALL, rådgivningschef på SSF Stöldskyddsföreningen vars syfte är att arbeta brottsförebyggande mot fysiska och digitala vardagsbrott genom bland annat säkerhetskollen.se.

MAGNUS LINDGREN, generalsekreterare för stiftelsen Tryggare Sverige var syften är att förbättra hjälpen till brottsdrabbade och främja utvecklingen på det brottsförebyggande området.

ANNE-MARIE EKLUND LÖWINDER, Chief Information Security Officer på Internetstiftelsen, en av Sveriges främsta IT-säkerhetsexperter, bland annat medlem i MSB:s cybersäkerhetsråd och ledamot av Digitaliseringskommissionen.

JAN OLSSON, kriminalkommissarie, en av Sveriges mest erfarna poliser på bedrägerier och cybersäkerhet, verksam hos Nationellt IT-brottscentrum vid polisens Nationella operativa avdelning (NOA) .

MARIE WALLIN, jurist, tidigare åklagare som varit verksam inom polisen och undervisat vid Polishögskolan och Stockholms Universitet, grundare av Rätt Nu.

JOHAN WIKTORIN, VD för säkerhetsföretaget Intil, har en bakgrund som officer och som omvärldsdirektör på revisionsfirman PwC med 25 års erfarenhet av säkerhetsarbete.

Om Näringslivets säkerhetsdelegation (NSD)

Näringslivets säkerhetsdelegation bildades 1967 som ett initiativ från dåvarande Svenska Arbetsgivareföreningen – SAF. Verksamheten bedrivs sedan 2001 av Svenskt Näringsliv. NSD är ett nätverk av personer med säkerhetsuppgifter, främst i det privata näringslivet men också den offentliga sektorn.

Det är ett forum för idé-, erfarenhets- och kunskapsutbyte i säkerhetsfrågor. Med ”säkerhet” avses främst sådant som rör hot om yttre eller inre brottsliga angrepp, liksom totalförsvar. Verksamhetens syfte är att bidra till ett bättre säkerhets- och riskmedvetande, i företagen och hos allmänheten. Den bedrivs i sex regioner, med var sin regional ordförande stödd av en arbetsgrupp.

Arbetet stöds av Svenskt Näringsliv och en central delegation. Svenskt Näringsliv bjuder varje år in till en konferens i samband med den centrala delegationens årsmöte. För mer information se Svenskt Näringslivs hemsida:

HTTPS://WWW.SVENSKTNARINGSLIV.SE/FRAGOR/NSD/.

Referenslista

RAPPORTER

AFA FÖRSÄKRING, Hot och våld på den svenska arbetsmarknaden, 2018.

BRÅ, Otillåten påverkan mot företag, En undersökning om utpressning, Rapport 2012:12, 2012.

BRÅ, Rapport 2018:6, Relationen till rättsväsendet i socialt utsatta områden, 2018.

BRÅ, Kriminalstatistik 2018, Anmälda brott, Slutlig statistik, 2019.

BRÅ, Kriminalstatistik 2019, Misstänkta personer, 2019.

BRÅ, Nordiska studier ozm brottslighet bland personer med utländsk och inhemsk bakgrund, En kartläggande litteraturöversikt av publicerad forskning och statistik 2005-2019, 2019.

BRÅ, Kriminalstatistik 2017, Återfall i brott preliminär statistik, 2020.

BRÅ, Nationella trygghetsundersökningen 2020, 2020

BRÅ, Rapport 2018:6, Relationen till rättsväsendet i socialt utsatta områden, 2018.

INSTITUTET FÖR FRAMTIDSSTUDIER, Forskningsrapport 2018/4, Våldsbejakande extremism och organiserad brottslighet i Sverige, 2018.

GÖTEBORGS UNIVERSITET, SOM-institutet, Vart är Sverige på väg? Folkets syn på utvecklingen i Sverige, 2020.

FOLKHÄLSOMYNDIGHETEN: Den svenska narkotikasituationen 2019, 2019.

POLISEN: Internationella brottsnätverk inom organiserad tillgreppsbrottslighet Erfarenhetsberättelse 2016 - januari 2019 Öppen version, 2019.

POLISEN, Kriminell påverkan i lokalsamhället – En lägesbild för utvecklingen i utsatta områden), 2019.

POLISEN, Utsatta områden – sociala risker, kollektiv förmåga och oönskade händelser, 2015.

POLISEN, Årsredovisning 2019, 2020.

POLISEN, Tullverket, Kustbevakningen, Delredovisning 2 av regeringsuppdrag, Uppdrag till Polismyndigheten, Tullverket och Kustbevakningen att förstärka bekämpningen av internationella brottsnätverk som begår tillgreppsbrott i Sverige (Ju2018/00991/PO), 2019

SCB, Hot, våld och oro 1980-2017, 2018.

STOCKHOLMS HANDELSKAMMAREN, Kriminaliteten förgiftar företagandet i förorten, 2017.

SVENSK HANDEL, Trygghetsbarometern, Tredje kvartalet 2019, 2019.

SVENSK HANDEL, Trygghetsbarometern, Andra kvartalet 2020, 2020.

SVENSKT NÄRINGSLIV, Brottslighetens kostnader för svenska företag, 2018.

SVENSKT NÄRINGSLIV, Brottslighetens kostnader 2020, 2020.

SÄKERHETSFÖRETAGEN, Säkerhetsföretagens årsrapport 2019, 2019.

OECD, Förfalskning och piratkopiering och den svenska ekonomin, säkerställandet av att ”Made in Sweden” alltid är det, 2019.

WORLD ECONOMIC FORUM, The Global Competitiveness Report, 2019.

LÄSTIPS

IYER, NIGEL: How to Find Fraud and Corruption, Recipies for the Aspiring Fraud Detective, Routledge, 2019.

GALEOTTI, MARK: We Need To Talk About Putin, Ebury Press, 2019.

GALEOTTI, MARK: Russian Political War, Routledge, 2020.

GALEOTTI, MARK: Vory: Den ryska supermaffian, Albert Bonniers Förlag, 2019.

GILES, KIER: Moscow Rules: What Drives Moscow to Confront the West, Brookings Institution, 2018.

JONSSON, OSCAR: The Russian Understanding of War: Blurring the Lines between War and Peace, Georgetown University Press, 2019.

NIKKA, KARL EMIL: IT-säkerhet för alla, Nikka Systems Sverige, 2018.

OSCARSSON, PER: Informationssäkerhet, Studentlitteratur, 2019.

EU:S immaterialrättsmyndighet OHIM:s databasverktyg: https://euipo.europa.eu/ohimportal/sv/

INTERNETSTIFTELSEN i Sveriges webbplats med praktiska tips om bl a källritik på nätet, cyberbrott, desinformation och integritet: https://internetkunskap.se

NYHETSBREVET Crypto-Gram, utgiven av Bruce Schneier: https://www.schneier.com/crypto-gram/

SSF Stöldskyddsföreningens säkerhetsguider: https://www.stoldskyddsforeningen.se/foretag/sakerhetsguider/

SÄKERHETSNACK, IT-säkerhetspodd av Olle Segerdahl & Christoffer Jerkeby