Lunds Universitet
Statsvetenskapliga Institutionen
Handledare Johan Matz

UNDA23, VT2022

Kriminella organisationers counterintelligence

En fallstudie om Södertäljenätverket

Joakim Johannesson

Abstrakt

Kriminella organisationers användning av counterintelligence är relativt outforskad inom underrättelsevetenskapen, och de studier som gjorts inom området handlar om terroristgrupper eller kriminella grupper i icke-demokratiska stater med svaga institutioner. Denna uppsats utgår från Södertäljenätverket som ett fall av en kriminell organisation i en demokratisk stat med starka institutioner och undersöker hur dess organisationsstruktur, kontrollerade territorium och folkliga stöd påverkat dess förmåga att bedriva counterintelligence. Uppsatsen undersöker också vilka taktiker för counterintelligence som organisationen använt.

Resultatet säger att organisationsstrukturen och frånvaron av folkligt stöd minskat organisationens förmåga att bedriva counterintelligence, medan den gagnats av dess kontrollerade territorium. Södertäljenätverket har brukat ett flertal taktiker för counterintelligence, varav de flesta är av typen basic denial.

Nyckelord: *Kontraunderrättelsetjänst, Counterintelligence, Criminal Counterintelligence*
Antal ord: 8458

Inledning

Studiet av underrättelseorganisationer utgår ofta från ett tävlingsförfarande på lika villkor: Statliga, utrikesfokuserade underrättelsetjänster tävlar om att skaffa strategisk information om andra staters förehavanden, samtidigt som dessa andra staters inhemska säkerhetstjänst skyddar de egna intressena från de konkurrerande staternas underrättelseinhämtning. Detta mellanstatliga underrättelsespel är dock inte nödvändigtvis representativt för allt underrättelsearbete. Även icke-statliga aktörer såsom mellanstatliga organ, privata företag och terroristorganisationer bedriver underrättelseinhämtning och analys mot andra aktörer, likväl som säkerhetstjänst för att hemlighålla skyddsvärd information. Den här formen av underrättelsespel, under mer assymetriska förhållanden, är dock ett område som är nära på outforskat inom underrättelsevetenskapen. De undersökningar som har gjorts av counterintelligence inom kriminella organisationer har främst skett inom en kontext av svaga icke-demokratiska stater, där dessa grupper haft utrymme att bygga upp en omfattande organisationsstruktur. Denna uppsats ämnar att förklara hur kriminella organisationer i en demokratisk stat med starka statliga institutioner bedriver counterintelligence mot underrättelseinhämtning och analys från andra kriminella organisationer och brottsbekämpande myndigheter. Genom större förståelse för hur kriminella organisationers counterintelligence fungerar kan brottsbekämpande myndigheters underrättelsearbete förbättras och kriminella organisationer mer framgångsrikt bekämpas.

Syfte och frågeställningar

I detta avsnitt presenteras uppsatsens syfte och vilket forskningsproblem den ämnar lösa, tillsammans med uppsatsens frågeställningar.

Syfte

Syftet med uppsatsen är att undersöka hur kriminella organisationer i demokratiska stater med starka statliga institutioner använder sig av counterintelligence. Uppsatsen utgår från resultatet av tidigare studier av terroristgrupper och kriminella organisationer i främst svaga icke-demokratiska stater, som visar att sådana grupper gagnas i sitt counterintelligence-arbete av en kompartmentaliserad organisationsstruktur, av att ha ett folkligt stöd och av att kontrollera ett territorium. Dessa tidigare studier visar också att de undersökta grupperna använder sig av ett flertal olika taktiker för att bedriva counterintelligence. Det är troligt att samma resultat inte kan appliceras i en demokratisk stat med starka statliga institutioner där en kriminell organisation inte bör kunna vara etablerad som ett parallellt samhällssystem någon längre tid.

Den svenska kriminella organisationen Södertäljenätverket studeras för att undersöka vilka taktiker för counterintelligence som en kriminell organisation i en demokratisk stat med starka statliga institutioner använder sig av. Likaså används Södertäljenätverket som fall för att undersöka om organisationsstruktur, folkligt stöd och kontroll av territorium är faktorer som påverkar hur väl en kriminell organisation i en demokratisk stat med starka statliga institutioner kan bedriva counterintelligence.

Frågeställningar

Frågeställningarna och deras utformning är centrala för en uppsats. Utifrån ett forskningsproblem kan olika frågor definieras, och forskarens uppgift är att definiera frågor som motsvarar forskningsproblemet på bästa sätt. De frågeställningar som denna uppsats syftar till att besvara är

- *Hur har Södertäljenätverkets organisationsstruktur påverkat dess förmåga att bedriva counterintelligence?*

- *Har Södertäljenätverket kontrollerat ett territorium, och har det isåfall påverkat dess förmåga att bedriva counterintelligence?*
- *Hur har Södertäljenätverkets folkliga stöd påverkat dess förmåga att bedriva counterintelligence?*
- *Vilka taktiker för att bedriva counterintelligence har Södertäljenätverket använt?*

Gentry (2016, 466) menar att det för forskningsfältets skull är önskvärt med en utvidgning av studiet av underrättelseanalys, så att forskningen omfattar även underrättelsearbete som inte är centrerat kring statliga organisationer. Genom att besvara dessa fyra frågeställningar, ökas förståelsen för hur counterintelligence används inom kriminella organisationer. Detta bidrar också till en större förståelse för underrättelse- och counterintelligence-arbete i stort.

Teori

I kapitlet förklaras först uppsatsens användning av begreppet counterintelligence, för att sedan redogöra för tidigare forskning inom området.

Counterintelligence

Inom uppsatsen används det engelska begreppet counterintelligence. Anledningen till att ett engelskt begrepp används är att det inte finns en vedertagen svensk översättning, och heller inte en översättning som fångar alla aspekter av ordet. För att förstå hur ordet har använts följer nedan två försök att definiera vad counterintelligence är.

Wettering (2000, 266-289) menar att counterintelligence ska fylla tre funktioner: att skydda hemlig information, att motarbeta främmande staters underrättelseinhämtning, och att avslöja inhemska spioner.

van Cleave (2007, 2) säger att counterintelligence ska identifiera, bedöma, neutralisera och utnyttja underrättelseverksamhet utförd av främmande stater, terroristgrupper och andra aktörer vars mål är att åsamka skada. Hon menar också att själva syftet med counterintelligence är att konfrontera och bekämpa motståndaren.

Wetterings definition trycker på att counterintelligence syftar till att försvara och hemlighålla skyddsvärd information, medan Van Cleaves definition tydliggör att counterintelligence även kan vara offensiv och användas för att slå mot motståndaren. Härav följer den definition av fenomenet som kommer användas inom uppsatsen - nämligen att counterintelligence är verksamhet som syftar till att

-hemlighålla information som skulle kunna innebära skada om en motståndare inhämtade den,
-avslöja och utnyttja försök till en pågående underrättelseinhämtning från en motståndare.

Denna definition innefattar de mer defensivt orienterade åtgärder som Wettering avser samtidigt som den inte exkluderar sådana offensiva åtgärder som van Cleave menar är syftet med counterintelligence.

Counterintelligence omfattar enligt uppsatsens definition också viss underrättelseverksamhet, syftande till att förstå hur motståndarens underrättelsetjänst bedrivs. Informationen kan analyseras varefter resultatet kan ligga till grund för att utforma egna motåtgärder, defensiva likväl som offensiva.

Det bör noteras att alla säkerhetshöjande åtgärder som kriminella grupper ägnar sig åt knappast främst är avsedda att skydda mot underrättelseinhämtning. Sådana aktörer har inte bara ett intresse av att hemlighålla information för att undvika upptäckt eller underrättelseinhämtning men också för att minska tillgången till hållbar bevisning i den händelse att de ställs inför rätta för sina brott. När åtgärder som kan förstås som counterintelligence också kan tolkas ha ett annat syfte, har de likväl bedömts vara counterintelligence inom ramen för denna uppsats. Anledningen till detta är att åtgärdens uttalade syfte, om ett sådant ens funnits, är ointressant - om den fyller *funktionen* av counterintelligence, bör den undersökas inom ramen för detta fenomen. Det är dock viktigt att förstå att en åtgärd som skyddar en grupp från att dömas i domstol inte nödvändigtvis är framgångsrik ur counterintelligence-synpunkt. Detta eftersom en polisiär underrättelsetjänst, eller en kriminell motståndare, inte har samma höga krav på att fastställa fakta som en domstol har för att kunna agera på dem. Underrättelseinformation som kommer till polisens kännedom kan exempelvis användas för ytterligare utrednings- eller brottsförebyggande åtgärder även om den inte är av sådan dignitet att den skulle leda till en fällande dom i domstol. Förutom att brottsbekämpande myndigheter kan använda information med en högre grad av osäkerhet, är det rimligt att tro att även kriminella motståndare skulle kunna agera på uppgifter som inte skulle leda till fällande dom i domstol.

Tidigare forskning

Tidigare forskning kring underrättelsearbete och counterintelligence fokuserar främst på hur statliga organisationer bedriver detta arbete. Av de studier som undersöker icke-statliga aktörer ur ett underrättelseperspektiv avser majoriteten beskriva hur dessa aktörer bedriver underrättelsetjänst, och då främst insamling och analys.

Det finns dock ett litet antal studier som undersökt hur icke-statliga aktörer använder counterintelligence. Av dessa fokuserar merparten på terroristgrupper och andra väpnade aktivistgrupper.

Wege (2012, 772-779) har undersökt Hizbollahs bruk av counterintelligence sedan dess födelse 1982 och menar att counterintelligence varit en kritisk faktor för organisationens överlevnad. Enligt Wege har Hizbollah en counterintelligence-organisation uppdelad i en undergrupp med fokus mot den interna säkerheten och en undergrupp med fokus på den externa. Infiltration av de libanesiska och amerikanska underrättelsetjänsterna, likväl som av andra militanta grupper i Libanon, lyfts fram som viktiga element för organisationens underrättelseinhämtning. Med hänsyn till att Hizbollah verkar från

Libanon, som är en relativt demokratisk stat (Freedom House 2022), är dessa resultat särskilt intressanta för uppsatsen.

Ilardi (2010, 9-17) beskriver hur Irländska republikanska armén (IRA) bedrev counterintelligence-arbete för att skydda sig mot brittisk underrättelseinhämtning. IRA anpassade sin organisations- och operationsstruktur utifrån en uppfattad hotbild. Sådana anpassningar omfattade att IRA omorganiserade sig från en bataljonsliknande struktur till en cellindelning, likväl som att man utbildade sina medlemmar i counterintelligence-arbete och i motståndarens underrättelse- och förhörsmetoder. Denna studies resultat är intressant för uppsatsens syfte, eftersom den avhandlar en konfliktförande grupp i en demokratisk stat.

Mobley undersöker ett flertal terrororganisationer och drar slutsatsen att dessa grupper gagnas i sitt counterintelligence-arbete av en kompartmentaliserad organisationsstruktur, av folkligt stöd och av att inneha ett kontrollerat territorium. (Mobley 2012, 229-242)

Gentry och Spencer har undersökt colombianska FARC:s counterintelligence-arbete och menar att gruppen inte drev någon central counterintelligence-funktion, utan att det istället var officerare i de stridande förbanden som hade ansvaret att bedriva counterintelligence. Gruppen förlitade sig också i hög grad på radio- och datorkommunikation som kunde avlyssnas av den colombianska staten. Man tycks heller inte ha lyckats upptäcka och förhindra avhopp från gruppen i särskilt hög grad, vilket lett till att ett stort antal avhoppare kunnat bidra med underrättelseinformation till staten. (Gentry och Spencer 2010, 468-471)

Dessa studier utfördes på organisationer vars målsättning varit att skaffa sig politisk makt och kontroll över ett geografiskt territorium. Inom kriminella organisationer är den främsta drivkraften vanligen att tjäna pengar, och även om det också kan finnas strategiska fördelar med att vinna politisk makt och att kontrollera ett territorium är de sällan målbilden för dessa grupper. Sådana skillnader i målsättning kan inte förbises när counterintelligence hos olika icke-statliga aktörer undersöks, då de påverkar vilken verksamhet organisationerna utför och hur de utför den.

Mobley och Ray har undersökt det colombianska före detta narkotikasyndikatet Calikartellens counterintelligence-verksamhet, och de slår fast att kartellen bedrev en sofistikerad counterintelligence-organisation med stor handlingskapacitet. Kartellens verksamhet hotades såväl av Colombias myndigheter som av den rivaliserande Medellinkartellen, och dess fortlevnad krävde avancerad counterintelligence. Calikartellen investerade därför stora resurser i staden Calis infrastruktur och välfärd likväl som att man donerade pengar till lokala medier för att förbättra sitt anseende hos lokalbefolkningen. Genom att organisationen var förankrad i Cali kunde man utföra bakgrundskontroll på medlemmar men även genom att lokalbefolkningen vidarebefordrade

underrättelseinformation till kartellen. Vidare skaffade man sig avancerad teknisk utrustning för underrättelse- och counterintelligence-arbete. Ett exempel på detta är att man skaffade ett eget signalspaningsplan som sedan användes för att lokalisera Medellinkartellens agenter i Cali. (Mobley och Ray 2019, 33-42)

Teoretiskt ramverk

Mobley och Rays undersökning av Calikartellen är den enda studie som undersökt ett kriminellt nätverk utan de omvälvande politiska ambitioner som terroristorganisationer förknippas med. Ett kriminellt nätverk har inte samma essentiella behov av publicitet och kan därmed agera utifrån andra ramar. Det är rimligt att anta att denna skillnad innebär en skillnad också i hur dessa två olika typer av grupper organiserar sig och utför counterintelligence.

Calikartellen agerade i Colombia under 1970-1990-talen. Dess motståndare bestod delvis av andra kriminella nätverk men dess främsta motståndare var den colombianska staten. Staten var dels inte stark nog för att effektivt bekämpa Calikartellen, den hade inte stöd i Calis lokalbefolkning och korruptionen var hög. Alla dessa faktorer förbättrade Calikartellens möjligheter att bedriva counterintelligence mot staten. Samtidigt begränsades inte Colombias myndigheter av den hårda styrningen av våldsmonopolet som en demokratisk stat med låg korruption gör. Detta bör ha inverkat negativt på Calikartellens möjlighet att bedriva counterintelligence.

Sammantaget utgör dessa faktorer en betydande skillnad mot en demokratisk stat med låg korruption därför att kriminella organisationer inte på samma sätt bör kunna etablera sig som en integrerad del av samhället, och i vart fall inte överleva som sådana någon längre tid.

Det här kan innebära att counterintelligence-arbetets organisation och utförande i Calikartellen inte är fullt representativt för hur samma arbete utförs i en kriminell organisation utanför Colombia. De slutsatser som Wege, Ilardi och Mobley och Ray föreslår kan dock ligga till grund för att undersöka fenomenet counterintelligence inom kriminella organisationer i starka demokratiska stater.

Mobley föreslår alltså kompartmentaliserad organisationsstruktur, folkligt stöd och kontroll av ett geografiskt territorium som viktiga faktorer för terroristgruppers counterintelligence. Ilardis resultat understöder tesen om att organisationens utformning är viktig för dess förmåga att bedriva counterintelligence. Resultaten av Ilardis studie, som utfördes på Irländska republikanska armén, visar att organisationsutformning kan vara en relevant faktor att undersöka i kontexten av demokratiska stater med starka statliga

institutioner. Samtliga av de uppräknade faktorerna är intressanta och möjliga att undersöka inom ramen för denna uppsats syfte.

Taktiker för counterintelligence kan beskrivas antingen i sin helhet, eller brytas ner i enskilda taktiker för att kunna analysera vilka taktiker som brukas framgångsrikt, brukas felaktigt eller inte brukas alls. Mobley (2012, 8-12) använder ett ramverk där terroristgruppers användning av counterintelligence kan klassificeras som en av fyra typer:

- *Basic denial* innefattar säkerhetsåtgärder som är ämnade att förhindra att skyddsvärd information ska kunna delas från gruppen till motståndaren, men som inte är specifikt utformade efter motståndarens metoder för inhämtning.

- *Adaptive denial* innebär säkerhetsåtgärder som är särskilt designade för att motverka en motståndares metoder för inhämtning. Dessa metoder är alltså anpassade utifrån en analys av motståndarens inhämtningsarbete.

- *Maladaptive denial* används för att beteckna säkerhetsåtgärder som utformats särskilt för att skydda mot en motståndares metoder för inhämtning, men som i själva verket resulterar i minskad säkerhet mot dem.

- *Covert manipulation* är den mest raffinerade typen av counterintelligence, som leder till att motståndaren leds att få en missvisande bild av gruppens beteenden, medlemmar och planer.

Terroristgrupper använder dessa strategier för counterintelligence med avsikt att skydda sig mot riktad underrättelseverksamhet från motståndaren, men också för att förhindra att skyddsvärd information kommer till civilbefolkningens eller medias känno. (Mobley 2012, 8-12)

Precis som terroristgrupper måste hemlighålla viss verksamhet måste kriminella grupper också göra det. Mobleys system för att klassificera olika typer av counterintelligence kan appliceras också på kriminella grupper utan att någon anpassning behöver göras. Det gör ramverket lämpligt för denna uppsats, och det kommer därför att användas för att klassificera olika typer av taktiker för counterintelligence när resultatet analyseras.

Metod

I detta kapitel förklaras uppsatsens metod och material tillsammans med vilka begränsningar det valda tillvägagångssättet innebär.

Fallstudie

Då den tidigare forskningen på området är mycket begränsad, finns inga tillgängliga databaser kring kriminella nätverk och deras användning av counterintelligence. Att sammanställa en sådan, och undersöka det källmaterial som detta skulle medföra, skulle vara alltför omfångsrikt för denna uppsats. Därför återstår att studera ett eller flera fall för att hitta bevis för kriminella gruppers användning av counterintelligence. Valet av en sådan fallstudie som tillvägagångssätt skulle innebära att uppsatsen brukar kvalitativ metod. Johannessen m.fl. (2019, 15-16) menar att just den kvalitativ metoden är särskilt lämpad för att undersöka ämnen som inte tidigare är utforskade i större utsträckning.

Syftet med en fallstudie är att använda ett enskilt fall av ett fenomen för att illustrera fenomenet i stort. Fallet är dock ett eget system inom fenomenet. Alvehus (2019, 79) beskriver detta som att "en spänning mellan unicitet och generalitet ligger alltså inbyggd i själva idén om "'fallet'." Detta är en inneboende egenskap hos fallstudien som dock inte innebär att dess resultat är mindre tillförlitliga, så länge de förstås i den kontext fallet tillhör.

Val av fall

Valet av analysobjekt är centralt i en fallstudie, och får konsekvenser i utfallet av undersökningen. Särskilt i en studie med ett enda analysobjekt blir resultatet påverkat av det enskilda fallets egenskaper.

I denna uppsats studeras Södertäljenätverkets användning av counterintelligence. Södertäljenätverket utgör ett fall av organiserad brottslighet i modern tid. En av de främsta fördelarna med att studera detta fall är det stora källmaterial som finns tillgängligt. Nätverket har omskrivits flitigt i media och böcker samtidigt som det även finns ett antal domar mot dess medlemmar att studera.

Olika fall kan också innebära olika svårighetsgrader för att bekräfta eller avfärda en teori eller hypotes. Lamont (2022, 252) ställer upp motsatsparet *mest-troligt* och *minst-troligt*, där mest-troligt innebär ett fall där man förväntar sig goda förutsättningar för att finna det fenomen man söker. Minst-troligt innebär motsatsen, alltså ett fall där man bedömer att förutsättningarna för att hitta det eftersökta fenomenet är som minst.

Ett mest-troligt-tillvägagångssätt kan vara användbart för att pröva en otestad teori, medan en minst-troligt med fördel kan utgöra ett svårt fall för att pröva en etablerad teori. Södertäljenätverket som fall utgör här en typ av mest-troligt-fall. Det är troligt att en kriminell organisation med sådan omfattande brottslig verksamhet använt sig av ett flertal taktiker för att bedriva counterintelligence.

Generaliserbarhet

Då en fallstudie använder sig av ett enskilt exempel för att illustrera ett fenomen som helhet, måste frågan ställas hur generaliserbart fallet faktiskt är. Ju mer detta studerade fall liknar normaltypen av fenomenet som ska studeras, desto mer generaliserbart är fallet (Teorell och Svensson 2007, 68-69). Genom att välja ett analysobjekt som är representativt kan alltså fler och säkrare slutsatser dras i resultatfasen. När inga tidigare studier av ett fenomen existerar bör istället fallet väljas för att det anses representativt utifrån andra parametrar.

Som kriminell organisation i en demokratisk stat med starka statliga institutioner utgör inte Södertäljenätverket något atypiskt fall, utan kan anses vara representativt för ett fall av det fenomen som det utgör.

Material

Till grund för uppsatsen ligger ett källmaterial bestående av facklitteratur och nyhetsartiklar. I viss utsträckning har också domar kommit att användas för att styrka andra källors påståenden. Naturligtvis hade det varit önskvärt att enbart förstahandskällor använts, för att minska risken för feltolkningar och efterhandskonstruktioner. Förundersökningsprotokoll hade varit en utmärkt förstahandskälla för att undersöka Södertäljenätverkets användning av counterintelligence. Uppsatsens omfattning medger dock inte en så djupgående undersökning av källmaterialet - exempelvis omfattande en förundersökning inför ett stort åtal mot Södertäljenätverket 2012 mer än 68000 sidor material (Kayhan 2017, 280).

För insamling av relevanta nyhetsartiklar har sökströngen “södertäljenätverket” använts i sökmotorn Retriever Mediearkivet, som indexerar svenska tidskrifter. Resultatet har sedan granskats efter relevant material, varefter de artiklar som uppfattats relevanta för undersökningen granskats efter material som är applicerbart för att besvara uppsatsens frågeställningar. Två böcker har också inkluderats i materialet; Ann Törnkvists *Följ fucking order: Liv och död i skuggan av Södertäljemaffian* och Baris Kayhans *Nätverket: Södertäljemaffians uppgång och fall*. Dessa böcker utgör skönlitteratur, men är skrivna på basis av ett stort och väl refererat källmaterial. Böckerna har behandlats på samma sätt som nyhetsartiklarna, med genomläsning och granskning efter relevant material.

Detta tillvägagångssätt innebär att en stor mängd text måste granskas manuellt. Naturligtvis hade det varit önskvärt att bruka en automatiserad process, exempelvis med hjälp av fler specifika söksträngar. Detta är dock inte möjligt då de metoder för counterintelligence som uppsatsen undersöker kan rymmas inom praktiskt taget vilket annat förehavande som helst. Specifika söksträngar ger därför ett resultat som är mycket litet i omfång, och exkluderar material som skulle vara av vikt för undersökningen. Den metod som istället brukas i uppsatsen innebär att materialet blir mer omfattande och att relevant material ändå riskerar att falla bort i sållningsprocessen. Denna sökmetod framstår dock som klart fördelaktig jämfört med den nämnda automatiska metoden.

Förutom att avgränsas till ett specifikt fall måste också en tidsperiod för undersökningen definieras. Inom uppsatsen avgränsas den undersökta tidsperioden till åren 2009-2021. Detta omfattar en relativt lång period från att Södertäljenätverket först började omskrivas i media, i samband med tre omskrivna mord 2009 och 2010, vilket ger möjlighet att följa organisationens counterintelligence-arbete över tid. Tidsperioden är utformad för att omfatta en så lång period och därigenom så mycket data som möjligt samtidigt som den ska rymmas inom uppsatsens ramar.

Källkritik

Det har redan konstaterats att andrahandskällor måste användas för att begränsa källmaterialets omfång. Andrahandskällor riskerar att ge en missvisande bild av ett ämne eftersom det påverkas av en författares egen förståelse och ämne, såväl som av hur författaren presenterar det. För att motverka detta har uppgifter kontrollerats mot varandra i den utsträckning det har varit möjligt. Det material som har inkluderats i uppsatsen har bedömts som tillförlitligt och objektivt.

Analys

I detta avsnitt presenteras först fallet Södertäljenätverket närmare. Därefter följer en genomgång av dess organisationsstruktur, kontrollerade territorium, folkliga stöd och användning av counterintelligence. Dessa faktorer analyseras för att förstå om de bidragit till fördelar för organisationens counterintelligence-förmåga.

Södertäljenätverket

Södertäljenätverket är ett kriminellt nätverk koncentrerat i Södertälje. Nätverket etablerades under det tidiga 1990- eller 2000-talet och blev nationellt omtalat efter ett antal uppmärksammade mord under åren 2009-2010, då man låg i konflikt med Södertäljeavdelningen av X-team, motorcykelklubben Bandidos underklubb. Ett flertal medlemmar av Södertäljenätverket dömdes till fängelsestraff efter ett dubbelmord på en illegal spelklubb 2010, vilket utgjorde en del i den nämnda konflikten med Bandidos och X-team. (Rodziewicz 2017)

Åren efter denna rättegång markerade en period av minskad aktivitet hos Södertäljenätverket, då ett flertal ledande personer avtjänade fängelsestraff. 2019 uttalade dock södertäljepolisen att nätverket åter vuxit till sig, om än inte till de nivåer man sett innan 2010. (Fallenius, 2019)

Nätverkets verksamhet omfattar bland annat narkotikabrott, svart låneverksamhet, utpressning och indrivning, enligt en polisrapport. (Malmgren, 2020b) Denna verksamhet har främst bedrivits inom den assyrisk/syrianska folkgruppen i Södertälje, inom ramarna för vad polisen beskrivit som ett parallellsamhälle (Wolters, 2020). Också medlemmarna i Södertäljenätverket tillhör till stor del den assyrisk/syrianska folkgruppen och har ofta band sinsemellan genom att ha vuxit upp tillsammans men också genom släktskap. Nätverket har god tillgång till vapen och medlemmarna är enligt polisens tidigare särskilda insatschef Gunnar Appelgren mycket våldsbenägna. (Ternert 2011)

Organisationsstruktur

Södertäljenätverket hade vid tidpunkten för de uppmärksammade morden 2010 en hierarkisk organisationsstruktur med en obestridlig ledare på plats i Södertälje. (Svea hovrätt dom 2014-09-01 i mål nr. B 8076-13, 50-51)

Under honom fanns sedan ett antal personer med tilldelade roller och uppgifter. Under denna andra nivå har en tredje nivå med yngre medlemmar i sin tur funnits. (Södertälje tingsrätt dom 2013-08-29 i mål nr. B2376-12, 105)

När ledaren greps och sedermera häktades 2010 hade ledarskapet kunnat bytas ut, antingen till en konkurrent om positionen eller till en ställföreträdare som sympatiserade med ledaren. Istället har nätverket säkerställt att man ska kunna kommunicera med ledaren även under hans häktes- och anstaltsvistelse. Från Kronobergshäktet visade han upp papperslappar med instruktioner genom fönstret i sin cell, som sen registrerades av nätverksmedlemmar med kikare på gatan utanför (Tagesson 2011, Södertälje tingsrätt dom 2013-08-29 i mål nr. B2376-12, 103).

Även under ledarens anstaltsvistelse har Kriminalvården flaggat för att han fortsätter att styra nätverket inifrån anstalten. 2017 drogs ett av hans telefontillstånd in efter att han gett order om en rad uppgifter och affärer till en bekant via Kriminalvårdens telefonsystem för intagna. Myndigheten bedömde att detta var ett sätt för honom att fortsätta styra nätverket trots att han suttit frihetsberövad. (Selåker Hangasmaa 2017)

Trots detta fortsatte ledaren styra Södertäljenätverket via telefonsamtal med sina föräldrar, vilket ledde till att även dessa telefontillstånd återkallades 2021. (Sjölin 2021)

Även en av ledaren kusiner ingår i nätverket och dömdes för inblandning i dubbelmordet 2010. Kusinen dömdes dock till ett kortare straff än ledaren, och har sedan frigivningen haft en roll som framstår som ställföreträdande ledare. Han dömdes därefter till fängelse vilket tycks ha försvagat nätverkets ställning i Södertälje. I upptakten till detta har polisen, som känt till kusinens roll, haft honom under övervakning. (Granström 2021a)

Polisen bedömde 2021 att kusinens roll inom nätverket varit hotad av en yngre falang (Granström 2021a). Denna grupp av yngre medlemmar har bland annat sprängt en äldre medlems bil och stulit vapen från de mer etablerade nätverksmedlemmarna. Enligt Södertäljes polischef handlar detta om oenigheter kring gruppens struktur och fördelning av intäkter. (Wierup 2021, 6)

En hierarkisk organisationsstruktur medger att en eller flera ledare samordnar organisationens verksamhet. Om de gör detta framgångsrikt kan det leda till ett bättre styrt counterintelligence-arbete. Det innebär också en risk, när all viktig verksamhet måste beordras från eller förankras med ledningen. Om dessa ledarpersoner är kända av polisen kan de sättas under övervakning. En kriminell organisation med denna struktur hamnar därför i en utsatt position när ledarpersoner bevakas.

Södertäljenätverket är till viss del exponerad för den risk som en hierarkisk organisationsdesign innebär, och var särskilt sårbar under det tidiga 2010-talet då man upplevde konsekvenserna av att dess ledarskikt frihetsberövades. I samband med återväxten av nätverket senare under 2010-talet har man därför implementerat en sidostruktur i

organisationen. Denna sidogrupp tycks ha ansvar för tvätt och förvaltning av organisationens pengar. De medlemmar som är inblandade i denna verksamhet är inte inblandade i den kriminella verksamhet som handlar om narkotikaaffärer och indrivning. Istället kretsar den i hög grad kring fastighetsaffärer. Fastighetsaffärerna och pengatvätten som sker genom dem möjliggörs genom goda relationer med mäklare och banktjänstemän. (Hellekant 2021, 4; Malmgren 2020a)

Det finns relativt lite tillgänglig information om denna parallellorganisation och dess verksamhet. Hur styrningen mellan de två delarna fungerar är också okänt. Det faktum att man lyft ut fastighetsaffärer och pengatvätt från de tungt kriminellt belastade medlemmarna i huvudorganisationen tyder dock på att man medvetet kompartmentaliserat organisationen.

Kompartmentalisering innebär visserligen en högre säkerhet för de enskilda verksamhetsdelarna, men försvårar central styrning. Om inre stridigheter som ägt rum runt 2020 går att spåra till den nya organisationsstruktur som växt fram är dock inte möjligt att säga.

Kontrollerat territorium

Kontrollerat territorium kan vid första anblick verka som en faktor som är enkel att mäta. I realiteten finns en rad avvägningar att göra vid en bedömning av huruvida en organisation kontrollerar ett territorium. En person, organisation eller stat kan sällan säga sig ha fullständig kontroll över ett territorium. Både externa och interna processer kommer leda till en varierande nivå av kontroll över ett territorium över tid. I begreppet inbegrips också någon sorts kontroll över de människor som bor eller befinner sig i territoriet, som på samma sätt kan variera. I begreppet omfattas alltså både geografiska områden, de människor som rör sig där och de aktiviteter som dessa människor företar i området.

I Södertäljenätverkets fall så har man aldrig kontrollerat ett territorium i sådan mån att brottsbekämpande myndigheter inte kunnat agera i området. Polisen har kunnat verka i hela Södertälje, och ingripa mot medlemmar i Södertäljenätverket.

Det är dock tydligt att nätverket haft viss kontroll över personerna i området och inskränkt deras handlingsutrymmen. Under utredningen av dubbelmordet 2010 är det ett återkommande tema att polisen inte effektivt kunnat utföra sitt arbete eftersom att invånare och potentiella vittnen inte vill eller vågar prata med polisen. (Baas och Siksjö 2010; Björklund 2010)

Denna ovilja att prata med polisen har troligen en tvådelad grund. Personer som är välvilligt inställda till nätverket talar inte med polisen för att skydda organisationen. Det kan grunda sig i att man känner medlemmar eller har fördelar av att befinna sig i nätverkets

närhet, exempelvis genom kriminella affärer. Personer som är ovänligt inställda till Södertäljenätverket kan förmås att inte tala utifrån den hotbild som uppstår mot någon som vittnar mot eller lämnar uppgifter kring organisationen. De skulle personligen ha vinning av att avslöja skyddsvärd information men är av säkerhetsskäl oförmögna att själva göra det.

Kontrollen som en kriminell organisation innehar över ett territorium utmanas inte bara av staten och dess brottsbekämpande myndigheter men också av andra kriminella organisationer. I likhet med brottsbekämpande myndigheter utgör konkurrerande kriminella organisationer yttre faktorer som kan inverka negativt på counterintelligence. Det kan ske genom direkta attacker på nätverket, vilket minskar dess kapacitet att bedriva counterintelligence, eller genom att konflikten tvingar organisationen att bedriva aktiviteter som man av säkerhetsskäl annars inte skulle bedriva.

Hos Södertäljenätverket exemplifieras detta av konflikten med X-team som kulminerade med dubbelmordet 2010. De två organisationerna verkade båda i Södertälje med en inbördes rivalitet genom konkurrensen om narkotikahandeln och beskyddarverksamheten i staden. Konkurrensen ledde så småningom till mer eller mindre öppna drabbningar dem emellan, tills X-teams ledare och hans bror mördades på en illegal spelklubb 2010. Efter detta lämnade X-team staden, och Södertäljenätverket tog plats som den ledande kriminella organisationen, med ensamrätt på narkotikahandel och beskyddarverksamhet. (Granström 2010)

Konflikten mellan organisationerna kan sägas ha inverkat negativt på Södertäljenätverkets förmåga att bedriva counterintelligence. I takt med att våldsanvändningen har eskalerat har det också varit svårare att hemlighålla den kriminella verksamhet man sysslat med, och när det sedermera kulminerar i mord har detta kommit till polisens kännedom och utretts. Det kan inte ha varit oväntat för Södertäljenätverket att detta skulle ske, men man har gjort bedömningen att det har varit viktigare att öka kontrollen över den kriminella verksamheten i Södertälje än att hålla verksamheten hemlig. På lång sikt innebar dock dubbelmordet att X-team lämnade Södertälje och att Södertäljenätverket åstadkom en ökad kontroll över territoriet. Man har därmed uppnått en viss långsiktig vinst även ur ett counterintelligence-perspektiv, samtidigt som denna vinst gjordes till en stor kostnad då ett flertal högt uppsatta medlemmar dömdes för inblandning i morden.

Folkligt stöd

Folkligt stöd kan innebära positiva effekter för en kriminell organisations counterintelligence exempelvis genom att vittnen är mindre benägna att berätta om eller anmäla

organisationens förehavanden och genom att utomstående förser en kriminell organisation med information om brottsbekämpande myndigheters och konkurrerande kriminella organisationers verksamhet i området.

I Södertäljenätverkets fall har det förekommit få exempel där organisationen kan uppvisa något folkligt stöd. Som tidigare nämnts under avsnittet om kontrollerat territorium så har det funnits en problematik med att få utomstående att vittna mot eller lämna information om nätverket. Den här oviljan att vittna kan dock inte härledas till något stöd för organisationen utan bottnar i en rädsla för att utsättas för repressalier mot den som delar information med brottsbekämpande myndigheter.

I de fall där organisationens medlemmar hjälpts av utomstående rör det sig om direkta familjemedlemmar, som att kusinens flickvän vid ett tillfälle undanröjer bevis för att skydda honom (Kayhan 2018, 110-111).

Att medlemmar ibland fått någon typ av stöd från familjemedlemmar är dock inte att betrakta som att det funnits något större folkligt stöd för organisationen. I övrigt har inget framkommit i materialet som kan tolkas som folkligt stöd för Södertäljenätverket och dess verksamhet.

Basic denial

Majoriteten av Södertäljenätverkets användning av counterintelligence kan klassificeras som olika former av basic denial. Basic denial är, precis som namnet antyder, den enklaste formen av counterintelligence-åtgärder. Detta innebär dock inte nödvändigtvis att det är okomplicerat för en organisation att implementera dem. Att upprätthålla basic denial-åtgärder kräver ofta ansträngning från gruppmedlemmarna, och slarv kan leda till att åtgärden antingen utförs förgäves, eller rentav att organisationen invaggas i en falsk trygghet.

En grundläggande kategori av basic denial är den som syftar till att skydda en organisations kommunikation. Om brottsbekämpande myndigheter eller konkurrerande brottsliga organisationer kunde läsa eller avlyssna kommunikation kunde man på förhand få kännedom om bland annat planerade brott och organisationens struktur. Skydd mot sådan inhämtning kan göras genom användning av exempelvis chiffer och koder eller intrapersonell kommunikation utan tekniska hjälpmedel som är möjliga att övervaka.

Inom Södertäljenätverket har kodord använts i vissa sammanhang. När ledaren kommunicerade med organisationen inifrån anstalten var detta med medvetenhet om att han kunde vara avlyssnad av Kriminalvården. Han har därför använt koduttryck för att hemlighålla kommunikationens innebörd. I Kriminalvårdens beslut att återkalla ledarens

telefontillstånd för att förhindra att han fortsätter styra nätverket kan man läsa att myndigheten inte kan tyda alla de koder som använts, vilket betyder att denna åtgärd har brukats med åtminstone viss framgång. (Selåker Hangasmaa 2017)

Övervakning av brottsbekämpande myndigheter är ett av de främsta underrättelsehoten mot kriminella aktörer. Om de övervakas kan myndigheterna samla information om deras brottsliga verksamhet och i värsta fall gripa dem på bar gärning. För att undvika fysisk spaning har åtminstone en medlem i Södertäljenätverket, ledarens kusin, varit folkbokförd på en annan adress än den han faktiskt bott på. Polisen har dock trots detta lyckats spana mot honom, och utreda var han bott. (Granström 2021a, 8)

Detta är en mycket billig säkerhetshöjande åtgärd, som dock troligen inte haft särskilt stor avkastning. Polisens spanare har lyckats finna kusinen trots att han varit folkbokförd på annan adress. För att minimera denna risk skulle aktörerna tvingas byta adress med mycket större regelbundenhet, eller rentav aldrig återvända till en tidigare bostad. Det här skulle dock kräva mycket större resurser. Det finns trots detta ingen anledning att tro att åtgärden varit kontraproduktiv, varför den är att klassificera som basic denial.

En ytterligare underrättelserisk hos medlemmarnas kommunikation är den risk som uppstår när man av någon anledning pratar med en representant för de brottsbekämpande myndigheterna. Detta kan ske i både informella samtal och i formella förhör. Utifrån hur medlemmen kommunicerar kan detta innebära en risk för att skyddsvärd information kommer motståndaren tillhanda, men det kan också innebära en möjlighet att vilseleda densamme genom lämnandet av falska uppgifter. Att vilseleda motståndaren kräver dock ett skickligt utförande. Uppgifterna måste framstå som trovärdiga och någon ytterligare källa bör kunna styrka de falska uppgifterna. Vilseledning av det här slaget vore att klassificera som covert manipulation.

Inom kriminella kretsar strävar man ofta inte efter att lyckas vilseleda polisen utan nöjer sig med att inte dela med sig av skyddsvärd information. Det enklaste sättet att utföra detta är helt enkelt att vara tyst när man pratar med poliser. Av juridiska skäl är det naturligtvis viktigt särskilt under förhör, men av counterintelligence-skäl är det viktigt i alla kontakter med polisen.

Inom Södertäljenätverket har det inte funnits en tydlig och efterlevd regel om att aldrig prata med polisen. Tvärtom förekommer det både i informella och informella sammanhang att man pratar med poliser, även om man ofta varit fåordig. Vid vissa förhör har medlemmar dock helt vägrat att uttala sig. (Kayhan 2017, 188, 198; Törnqvist 2018, 170, 180)

Detta tillvägagångssätt bör generellt kunna sägas vara till en kriminell organisations nackdel, eftersom alla uttalanden innebär en risk för att dela med sig av skyddsvärd

information samtidigt som möjligheterna att lyckas vilseleda polisen generellt är små. Vilseledning som metod är helt enkelt för svårt, och fallgroparna för många.

Basic denial-metoder har i övrigt använts relativt regelbundet av medlemmar i Södertäljenätverket. Det rör sig då om metoder som har en låg kostnad i form av tid och resurser, men som ändå kan antas ha ett visst skyddsvärde. Exempel på detta är att man möts ansikte mot ansikte för att diskutera känsliga frågor istället för att diskutera dem via eventuellt avlyssnade telefoner. När man träffats för att genomföra sådana möten har man dessutom ofta stängt av sina medhavda telefoner, antagligen för att undvika att man avlyssnas trots att mobiltelefonen inte är i samtalsläge. Andra åtgärder med hänvikt på fysiskt skydd är att man drar för gardinerna i det rum man befinner sig för att undvika fysisk spaning och att montera övervakningsutrustning. (Kayhan 2017, 168, 175, 186, 250)

Generellt kan det antas att användningen av sådana enkla basic denial-åtgärder gagnat Södertäljenätverkets säkerhet, särskilt som kostnaden för dem alltså är låga. Man tycks dock inte ha räknat med möjligheten att de platser man valt att träffas på är avlyssnade, utan bara de mobiler man burit. Under utredningen av dubbelmordet 2010 kunde därför polisen vid tillfällen avlyssna konversationer som skedde i medlemmarnas bilar, där man ibland lyckats installera avlyssningsutrustning. (Kayhan 2017, 208-209)

Adaptive denial

Risken för att av misstag dela information under kontakter med brottsbekämpande myndigheter har nämnts under avsnittet kring basic denial. Det konstaterades att en metod för att undvika detta är att i samtliga kontakter med dessa myndigheter vägra uttala sig. Som tidigare nämnts motverkade IRA den här risken för att dela skyddsvärd information genom att utbilda sina medlemmar i vilka förhörsmetoder de kunde komma att mötas av om de greps. Även inom kriminella organisationer vore det möjligt att förbereda medlemmarna på att bli förhörda utan att avslöja skyddsvärd information eller låta sig påverkas av polisens förhörsmetoder. Sådan utbildning vore att klassificera som adaptive denial.

Under utredningen av dubbelmordet 2010 satt en ung medlem av Södertäljenätverket häktad misstänkt för inblandning i brottet. Medlemmen hade förberett mopeder som skulle användas för gärningsmannens flykt från brottsplatsen. Kayhan (2018, 201-202) beskriver att den unge medlemmen först är kaxig och ljuger under de tidiga förhören med honom. Hans inställning förändras dock när han inser att han utnyttjats av nätverket, och han börjar ge utredarna information om brottet. Denna information är kritisk för att senare kunna fälla ett antal nätverksmedlemmar för morden.

Det är troligt att Södertäljenätverket inte förberett medlemmen för polisens förhörsmetoder och inför vikten av att att stå anklagad för det brott han var häktad för. Om en enskild medlem inte förväntas klara att undanhålla skyddsvärd information från brottsbekämpande myndigheter, bör den medlemmen heller inte delges sådan information. Detta fall illustrerar att Södertäljenätverket misslyckats i att förbereda sina medlemmar på att bli utsatta för förhör, och att man misslyckats med att undanhålla skyddsvärd information från medlemmar som inte kan hemlighålla den.

Användningen av mobiltelefoner utgör en risk för underrättelseinhämtning från brottsbekämpande myndigheter. Det kan ske genom avlyssning av mobilkommunikationen såväl som övervakning av telefonernas geografiska position.

Den geografiska övervakningen är en risk som Södertäljenätverkets medlemmar tagit fasta på. Man har ofta stängt av sina mobiltelefoner inför ett stundande brott för att undvika att telefonerna binder dem till brottsplatsen. (Kayhan 2017, 130, 149)

Att systematiskt stänga av sina mobiltelefoner inför ett nära förestående brott vore dock ett mönster som polisen skulle kunna övervaka, och tolka som en anledning att ingripa. Det finns dock inga tecken på att man i Södertäljenätverkets fall skulle ha utsatt organisationen för en sådan mönsteranalys. Oavsett om detta berott på att polisen inte valt att bruka denna teknik eller om Södertäljenätverket motverkat denna risk så är användningen av metoden att klassificera som adaptive denial. Metoden som sådan ligger dock i gränslandet för att bli kontraproduktiv beroende på hur den används.

Maladaptive denial

Det har redan nämnts att Södertäljenätverket brukat kodspråk för att hemlighålla delar av sin kommunikation. Att bruka ledarens namn i samtal med andra har exempelvis varit förbjudet. Istället har man använt kodnamn, till exempel al-Taweel, arabiska för “den långe”. (Törnkvist 2018, 81.)

Den här användningen av kodnamn kan dock ha som följd av att man tillåter sig att kommunicera öppet i tron att innehållet är skyddat av kodspråket. Det är uppenbart att polisen känt till vem som stod bakom exempelvis namnet al-Taweel, varför användning av denna form av counterintelligence får anses vara kontraproduktivt.

Användandet av egna namn eller kända täcknamn utgör alltså en risk för underrättelseinhämtning, varför det bör undvikas. Det är känt att kriminella ibland registrerar egendom såsom bilar i andras namn, så kallade målvakter. Målvaktens syfte är då att dölja vem som är den egentlige ägaren eller brukaren av bilen.

2021 inträffade en bisarr variant av målvaktsmetoden i Södertälje. En södertäljebo mottog ett brev från Transportstyrelsen om att han registrerats som ägare till en bil. Snart började mannen också motta parkeringsböter, då samma bil stod felparkerad. Mannen kontaktade en skrotfirma för att forsla bort bilen, men när man kom för att hämta den upptäckte man att den var en förvaringsplats för vapen. Polisen hittade så småningom tre pistoler och en mobiltelefon. Med hjälp av fingeravtryck kunde man koppla telefonen till en man i Södertäljenätverket. En av pistolerna kunde kopplas till en skjutning i Stockholm några dagar tidigare. (Granström, 2021b)

Bilen hade använts som vapengömma och registrerats på en utomstående person. Användandet av en målvakt förutsätter dock att personen som registrerats som ägare antingen är införstådd med och har godkänt uppdraget, eller av någon anledning är oförmögen att förhindra det. I detta fall borde man ha förstått att en utomstående måste reagera både mot att registreras som ägare på en bil man inte vill kännas vid, och att betala parkeringsböter för samma bil. Att informationen snart kommer komma till polisens kännedom verkar då logiskt. Polisen kan välja att ställa bilen under övervakning, vilket hade kunnat leda till både underrättelseinhämtning eller ingripanden mot Södertäljenätverket. Denna åtgärds utformning framstår därför som slarvig och kontraproduktiv, och den klassificeras därför här som maladaptive denial.

Generellt sett tenderar inte kriminella organisationers counterintelligence vara föremål för mediebevakning. Ett undantag har varit användandet av krypterade så kallade EncroChat-telefoner. EncroChat användes av kriminella aktörer för att kunna kommunicera sinsemellan utan risk att brottsbekämpande myndigheter läste innehållet.

Via EncroChat kommunicerade kriminella aktörer därför ohämmat kring brottslighet då man uppfattade att man var skyddad från övervakning. Detta skulle leda till stora konsekvenser för användarna när fransk polis 2020 lyckades tillgängliggöra chattarnas innehåll. (Polisen, 2021, 3)

EncroChat-telefoner har fysiskt kunnat kopplas till individer redan innan den franska polisen knäckte tjänstens kryptering 2020. Detta eftersom sådana telefoner, i likhet med andra mobiltelefoner, använder sig av ett sim-kort med ett individuellt IMEI-nummer. Om en person påträffats med en telefon och ett visst sim-kort har man på så sätt kunnat koppla ihop individen med IMEI-numret. Det är dock inte olagligt att inneha en sådan telefon, och då man inte kunnat utläsa vad en viss användare kommunicerat har underrättelsevärdet av denna information inte varit särskilt högt. När polisen 2020 plötsligt kunnat koppla ihop IMEI-nummer och användarnamn med deras chattloggar, har också underrättelsevärdet höjts markant.

Även inom Södertäljenätverket användes EncroChat för att kommunicera kring brottsplanering mellan medlemmar, och med medlemmar av andra kriminella

organisationer. Man har brukat ett andra lager av skydd, nämligen genom att bruka täcknamn för personer i konversationerna. Detta har dock skett på ett slarvigt sätt då vissa användare kopplat kända täck- eller smeknamn till andra användare i sina kontaktlistor (Södertälje tingsrätt dom 2021-07-05 i mål nr. B2559-20, 22-23). I övrigt har man tillåtit sig att kommunicera relativt ohämmat.

2020 dömdes två medlemmar av Södertäljenätverket till långa fängelsestraff för narkotikabrott. En av de dömde var ledarens kusin, som konstaterats haft en ledande roll i organisationen då ledaren varit frihetsberövad. Som grund för domen ligger att de två personerna kopplats till EncroChat-användare och deras chattloggar. (Södertälje tingsrätt dom 2021-07-05 i mål nr. B2559-20, 19-22)

EncroChat utgör ett intressant exempel på användandet av counterintelligence inom Södertäljenätverket, men också inom kriminella organisationer i stort. Skyddet har varit starkt, och tekniken har brukats i flera år utan att kunna läsas av myndigheterna. Under den tiden har alltså EncroChat utgjort ett gott skydd för organisationens kommunikation. Man har dock inte tillräckligt skyddat sig mot eventualiteten att krypteringen skulle komma att knäckas, och därför varit exponerad för risk när det så småningom skedde.

Södertälje tingsrätt (dom 2021-07-05 i mål nr. B2559-20, 22) slår fast att både en EncroChat-telefon och dess tillhörande abonnemang är dyra att införskaffa och inneha. Bara abonnemanget kostade runt 30 000 kronor per år. Det är därför en kostsam skyddsåtgärd man skaffat, vilket innebär att man ändå värderar detta skydd relativt högt. Det är dock nödvändigt att notera att samtidigt som EncroChat inneburit en counterintelligence-åtgärd så har det också varit en möjliggörare av kriminella affärer, eftersom det fungerat som ett socialt nätverk för kriminella aktörer. De stora summor man betalat för användandet kan därför inte enbart motiveras utifrån vilket skyddsvärde åtgärden haft.

EncroChat-affären är dock inte första gången som Södertäljenätverket exponeras för underrättelseinhämtning genom sättet man kommunicerar via mobiltelefoner. Under utredningen kring dubbelmordet 2010 upptäcker polisens analytiker ett mönster i telefontrafiken i Södertälje som ska bli en av de viktigaste pusselbitarna för att knyta brottet till Södertäljenätverket. Organisationen har begått ett fatalt misstag när man försökt skydda sin mobilkommunikation.

Grunden till detta counterintelligence-misslyckande är att man använt två mobiltelefoner med oregistrerade kontantkort för att kommunicera under förberedandet av dubbelmordet. Den ena mobiltelefonen har brukats av kusinen, som är den som kommer begå morden. Den andra mobiltelefonen har befunnit sig hos en medhjälpare som haft de två tilltänkta offren under uppsikt. Detta i sig är inte anmärkningsvärt. Att kriminella begår spaning inför ett viktigt brott är naturligt, och att bruka oregistrerade kontantkort för att underlätta spaningen är inte ett ovanligt tillvägagångssätt. Problemet ligger i att även om

kontantkorten i sig inte är registrerade, tillhörde de en serie av kontantkort som kan kopplas till Södertäljenätverket. Förklaringen till detta låg i att operatören Comviq delat ut gratis simkort i Södertälje Centrum någon gång innan brottet. Någon nätverksmedlem hade då tagit tillfället i akt att skaffa ett lager av oregistrerade kontantkort för framtida bruk, och dessa distribuerades så småningom inom nätverket. Ett antal av korten hittades exempelvis vid en husrannsakan av ledarens bil, och kunde därför med stor säkerhet knytas till honom och Södertäljenätverket. (Kayhan 2017, 211-214; Svea hovrätt dom 2014-09-01 i mål nr. B 8076-13, 64-65)

Förutom att det redan var känt för polisen att Södertäljenätverket hade tillgång till kontantkort i denna nummerserie, kunde man också koppla inköpet av de två mobiltelefonerna till en nätverksmedlem. Dessa köptes tillsammans med två värdebevis (för att överföra pengar till kontantkorten)(Kayhan 2017, 211-214).

Förutom dessa faktorer, fanns en ytterligare faktor som band nätverket till mobiltelefonerna. De användes aldrig mer efter dubbelmordet, men trots det laddades ett av simkorten med pengar via ett annat simkort. Detta genom en tjänst som möjliggjorde att man sände pengar sinsemellan. Det simkort som överfört pengar till en av mordtelefonerna tillhörde kusinen, som troligen gjort det av misstag när han skulle överföra pengar till en annan nätverksmedlem med ett telefonnummer ur samma nummerserie. (Kayhan 2017, 216-217)

Användandet av anonyma mobiltelefoner vore i sig ett effektivt verktyg för counterintelligence. Det ställer dock krav på utförandet. I det ovan nämnda exemplet begicks ett flertal misstag, som framstår som slarv. Medlemmarna borde ha noterat att man brukade flera telefonnummer som var närmast snarlika och att det vore en stor risk om dessa telefonnummer kom till polisens kännedom. Att kusinen överför pengar till ett av de telefonnummer som använts vid morden knyter honom direkt till brottet trots att det är ett misstag som enkelt hade kunnat undvikas.

Covert manipulation

Covert manipulation är den mest sofistikerade kategorin av counterintelligence-åtgärder, som syftar till att ge motståndarens en missvisande bild av en aktörs aktivitet. I sin mest förfinade form utgår covert manipulation från en noggrann analys av motståndarens inhämtnings- och analysmetoder för att vilseleda denne i en särskild riktning. Om detta lyckas kan man få motståndaren att dra fel slutsatser i underrättelsefrågor. Framgångsrikt använd kan alltså denna åtgärd leda till stora skador för motståndarens underrättelsetjänst.

All form av covert manipulation behöver dock inte vara lika sofistikerad. I analysen av Södertäljenätverket förekommer bara ett exempel på att man ska ha använt denna typ av åtgärd. Det skedde när ett antal medlemmar av nätverket samlades för att attackera en person som flörtat med en medlems flickvän. Under tiden som dessa medlemmar beskjuter personens bil befinner sig deras mobiltelefoner hos en medhjälpare som kört långt från brottsplatsen. Där ringer han och skickar meddelanden från mobiltelefonerna för att skapa en falsk bild av att personerna befunnit sig på platsen. (Kayhan 2017, 168.)

I detta fall är det oklart om åtgärden hade någon inverkan på polisens analys av deras förehavanden. Det framstår dock som troligt att en liknande åtgärd, utförd med något större noggrannhet, med framgång hade kunnat vilseleda polisen.

Även om det fastställts att Södertäljenätverket har förgreningar in i näringslivet och civilsamhället i staden, har det inte framkommit någon anledning att tro att man kunnat utnyttja dessa förbindelser för att bedriva covert manipulation.

Sammantaget kan det sägas att covert manipulation inte nödvändigtvis kräver stora resurser för att utföras, med det kräver viss analys och planering. Frånvaron av sådana åtgärder inom Södertäljenätverkets användning av counterintelligence tyder på att man föredrar att bruka mindre raffinerade säkerhetshöjande åtgärder.

Slutsatser och diskussion

I detta avsnitt besvaras uppsatsens frågeställningar. Efter detta följer en kortare diskussion kring möjliga slutsatser och förslag på framtida forskning.

Slutsatser

Uppsatsen ämnar att besvara fyra frågeställningar, som redovisas en och en tillsammans med sina svar här nedan.

Hur har Södertäljenätverkets organisationsstruktur påverkat dess förmåga att bedriva counterintelligence?

Uppsatsen visar att Södertäljenätverkets organisationsstruktur förändrats över tid. Runt 2010 hade organisationen en strikt hierarkisk struktur som var sårbar för brottsbekämpande myndigheters angrepp. Efter att ett flertal viktiga medlemmar gripits byggde man upp en parallell organisation med uppgift att förvalta gruppens tillgångar. Syftet med denna kompartmentalisering tycks ha varit att förbättra Södertäljenätverkets förmåga att behålla sina ekonomiska tillgångar genom att öppet kriminella medlemmar inte har ansvar för att förvalta stora förmögenheter. Det finns dock inget i materialet som visar på att denna nya kompartmentaliserade organisationsstruktur lett till en förbättrad counterintelligence-förmåga. Organisationen är fortfarande toppstyrd, även om den nu också omfattar en sidoorganisation. Södertäljenätverkets organisationsstruktur innebär fortfarande en risk för organisationen då dess ledarskikt är känt för polisen, vilket tillåter ledarna att ställas under övervakning. Södertäljenätverkets hierarkiska organisationsstruktur exponerar gruppen för sårbarheter som hade undvikits i en grupp med en mer kompartmentaliserad organisationsstruktur.

Har Södertäljenätverket kontrollerat ett territorium, och har det isåfall påverkat dess förmåga att bedriva counterintelligence?

Undersökningen visar att Södertäljenätverket åtnjutit viss kontroll över ett territorium i Södertälje. Gruppen har inte haft en sådan kontroll att brottsbekämpande myndigheter inte kunnat agera i området, men man har uppvisat ett sådant våldskapital att boende varit ovilliga att agera uppgiftslämnare till myndigheterna. Detta bör ha varit mycket fördelaktigt för gruppens förmåga att bedriva counterintelligence. Man utmanades i sin

kontroll över området av den kriminella organisationen X-team, men gick vinnande ur konflikten. Att man lyckats etablera sig som den ledande kriminella aktören i Södertälje innebär att man kan bedriva sin verksamhet på sina egna villkor, samtidigt som det innebär en ökad operationell säkerhet då man inte riskerar att hamna i öppna drabbningar med andra kriminella organisationer. Sammantaget innebär detta att Södertäljenätverkets kontrollerade territorium ger organisationen en fördel i dess counterintelligence-förmåga.

Hur har Södertäljenätverkets folkliga stöd påverkat dess förmåga att bedriva counterintelligence?

Resultatet visar att Södertäljenätverket inte åtnjutit något större folkligt stöd. Att boende i Södertälje undvikit att dela information om organisationen med brottsbekämpande myndigheter kan härledas till det våldskapital som man uppvisat, och hotbilden som uppstår mot den som vittnar mot gruppen. Det är dock troligt att ett utbrett folkligt stöd hade gagnat Södertäljenätverkets counterintelligence-förmåga, exempelvis genom att lokalbefolkningen bidragit med underrättelseuppgifter till organisationen. Det har dock inte framkommit uppgifter om att avsaknaden av folkligt stöd lett till negativa effekter på organisationens counterintelligence-förmåga. Södertäljenätverkets avsaknad av folkligt stöd bör alltså inte ha påverkat organisationens förmåga att bedriva counterintelligence.

Vilka taktiker för att bedriva counterintelligence har Södertäljenätverket använt?

I materialet framkommer att Södertäljenätverket använt ett flertal taktiker för att bedriva counterintelligence. Man har främst brukat mindre resurskrävande basic denial-åtgärder samtidigt som adaptive denial-åtgärder har förekommit i en mindre utsträckning. Bara ett fall av covert manipulation har identifierats. Vid tillfällen har man ägnat sig åt maladaptive denial, då främst kopplat till kommunikation via mobiltelefoni som inte varit tillräckligt skyddad mot polisens underrättelseinhämtning.

Diskussion

Inom undersökningen har organisationsstruktur, kontrollerat territorium och folkligt stöd antagits vara faktorer som är relevanta att studera för att bedöma counterintelligence-förmågan hos kriminella nätverk i demokratiska stater med starka institutioner.

I Södertäljenätverkets fall har organisationsstrukturens omstrukturering inte förändrat dess förmåga att bedriva counterintelligence i och med att man behållit delar av en hierarkisk struktur. Det är möjligt att kriminella organisationer med målsättningen att generera maximala inkomster inte kan organiseras som celler, utan alltid kommer att vara centralstyrda i någon form. Kompartmentaliserad organisationsstruktur vore då inte en särskilt relevant faktor att undersöka för att bedöma sådana organisationers counterintelligence-förmåga.

Eftersom inga belägg för något större folkligt stöd för Södertäljenätverket och dess verksamhet kunnat finnas, har denna faktors relevans inte kunnat bedömas. En fallstudie av en kriminell organisation med högt folkligt stöd vore nödvändig för att fastslå om faktorn bör appliceras även på kriminella nätverk i demokratiska stater med starka institutioner. Det är möjligt att det är svårare för kriminella organisationer i demokratiska stater med starka institutioner att bygga upp ett stort folkligt stöd, eftersom man i motsats till exempelvis Calikartellen inte erbjuder lokalbefolkningen fördelar som inte staten kan erbjuda.

Att Södertäljenätverkets counterintelligence-förmåga haft en fördel av dess kontrollerade territorium får dock anses vara bekräftat. Denna faktor bör betraktas som relevant i denna typ av undersökning även inom kontexten demokratiska stater med starka institutioner.

Det har fastslagits att Södertäljenätverket använt ett flertal taktiker för counterintelligence. Att man främst ägnar sig åt basic denial kan spegla en kultur där strategiskt säkerhetsarbete inte är högt prioriterat. Det är dock möjligt att taktiker som brukats framgångsrikt inte förekommer i källmaterialet, då de inte kommit till utomståendes kännedom. Mer forskning behövs för att bedöma om den bild som presenterats här är generaliserbar.

Att undersöka de punkter som ovan föreslås för framtida forskning bör dock inte begränsas till akademisk forskning. Även brottsbekämpande myndigheters underrättelsetjänster skulle kunna ställa upp och testa hypoteser kring de faktorer som undersökts inom ramen för denna uppsats. Resultatet av en sådan undersökning skulle innebära en ökad förståelse av bruket av counterintelligence hos kriminella organisationer även inom underrättelsetjänsterna.

Referenser

Alvehus, Johan. 2019. *Skriva uppsats med kvalitativ metod: En handbok*. Andra uppl. Stockholm, Liber.

Baas, David och Siksjö, Daniel. 2010. Polisen: Det var en hämnd. *Expressen*, 2010-07-02, 11.

Björklund, Anders. 2010. Jakten på mördarna: Polisen knackade dörr - många vågar inte berätta något. *Länstidningen Södertälje*, 2010-07-03.

Fallenius, Karin. 2019. Polisen: Södertäljenätverket växer sig starkare. *SVT Nyheter*, 2019-10-30. https://www.svt.se/nyheter/lokalt/sodertalje/polisen-sodertaljenatverket-vaxer-sig-starkare (Hämtad 2022-05-15)

Freedom House. 2022. *Lebanon: Freedom in the World 2022 Country Report*. https://freedomhouse.org/country/lebanon/freedom-world/2022 (Hämtad 2022-05-17)

Gentry, John A. 2016. Toward A Theory of Non-State Actors' Intelligence. *Intelligence and National Security*, vol. 31:4, 465-489.

Gentry, John A. och Spencer, David E. 2010. Colombia's FARC: A Portrait of Insurgent Intelligence. *Intelligence and National Security*, vol. 25:4, 453-478.

Granström, Torbjörn. 2021a. Den yngre falangen tar över narkotikamarknaden. *Länstidningen Södertälje*. 2021-07-22, 4-5.

Granström, Torbjörn. 2021b. Kriminella skrev bilen på Södertäljebo – och använde den som vapendepå. *Länstidningen Södertälje*. 2021-03-29. https://www.lt.se/2021-03-29/kriminella-skrev-bilen-pa-sodertaljebo--och-anvande-den-som-vapendepa (Hämtad 2022-05-13)

Granström, Torbjörn. 2010. Maktbalansen rubbad efter dubbelmordet. *Länstidningen Södertälje*. 2010-11-17.

Hellekant, Johan. Polisen: Mäklare ser mellan fingrarna i svarta bostadsaffärer. *SvD Näringsliv*, 2021-10-07, 3-4.

Ilardi, Gaetano Joe. 2010. Irish Republican Army Counterintelligence. *International Journal of Intelligence and Counterintelligence*, vol. 23:1, 1-26.

Johannessen, Asbjørn, Tufte, Per Arne och Christoffersen, Line. 2019. *Introduktion till samhällsvetenskaplig metod*. Andra uppl. Stockholm, Liber.

Kayhan, Baris. 2017. *Nätverket: Södertäljemaffians uppgång och fall*. Stockholm, Norstedts.

Lamont, Christopher. 2022. *Research Methods in International Relations*. 2:a uppl. London, Sage.

Malmgren, Kim. 2020a. Polisens hemliga rapport: Så styr nätverket Södertälje. *Expressen*, 2020-09-18. https://www.expressen.se/nyheter/krim/polisens-hemliga-rapport-sa-styr-natverket-sodertalje/ (Hämtad 2022-05-14)

Malmgren, Kim. 2020b. Mördare misstänks ha beordrat stormning av klubb i Stockholm. *Expressen*, 2021-08-01. https://www.expressen.se/nyheter/krim/mordare-misstanks-ha-beordrat-stormning-av-klubb-i-stockholm/ (Hämtad 2022-05-13)

Mobley, Blake W. 2012. *Terrorism and Counterintelligence: How Terrorist Groups Elude Detection*. New York: Columbia University Press

Mobley, Blake W. och Ray, Timothy. 2019. The Cali Cartel and Counterintelligence. *International Journal of Intelligence and Counterintelligence*, vol. 32:1, 30-53.

Polisen, 2021. *Lärdomar av Encrochat - Analysprojekt Robinson*. Polisen, Nationella Operativa Avdelningen.

Rodziewicz, Li. 2017. Södertäljenätverket: ”Som utländsk maffia”. *Expressen*, 2017-10-30. https://www.expressen.se/nyheter/brottscentralen/sodertaljenatverket-som-utlandsk-maffia/ (Hämtad 2022-05-15)

Selåker Hangasmaa, Karin. 2017. Maffialedaren Khouris hemliga koder från fängelset. *Expressen*, 2017-12-03, 12.

Sjölin, Jacob. 2021. Kriminalvården misstänker - styr nätverket från fängelset. *Länstidningen Södertälje*. 2021-11-23, 8.

Tagesson, Eric. 2011. Gängledaren visade meddelanden till kumpanerna från häktesfönstret. *Aftonbladet*, 2011-11-17. https://www.aftonbladet.se/nyheter/a/MgjgmM/gangledaren-visade-meddelanden-till-kumpanerna-fran-haktesfonstret (Hämtad 2022-05-13)

Teorell, Jan och Svensson, Torsten. 2007. *Att fråga och att svara. Samhällsvetenskaplig metod*. Malmö, Liber.

Ternert, Erik. 2011. Vi dömde trots offrens rädda tystnad. *Länstidningen Södertälje*, 2011-12-30.

Törnkvist, Ann. 2018. *Följ fucking order: Liv och död i skuggan av Södertäljemaffian*. Stockholm, Mondial.

Van Cleave, Michelle. 2007. Strategic Counterintelligence - What Is It and What Should We Do About It? *Studies in Intelligence*, vol. 51:2.

Wege, Carl Anthony. 2012. Hizballah's Counterintelligence Apparatus. *International Journal of Intelligence and Counterintelligence*, vol. 25:4, 771-785.

Wettering, Frederick L. 2000. Counterintelligence: The Broken Triad. *International Journal of Intelligence and Counterintelligence*, vol. 13:3, 265-300.

Wierup, Lasse. 2021. Solskenshistorien var falsk - maffian lämnade aldrig stan. *Dagens Nyheter*. 2021-06-05, 6-7.

Wolters, Staffan. 2020. Det här står i polisens hemliga klanrapport. *Upsala Nya Tidning*, 2020-12-13.