Lunds universitet
Statsvetenskapliga institutionen

UNDA23
VT-24
Handledare: Tony Ingesson

FBI-fällan

En teorikonsumerande fallstudie av Operation Trojan Shield

Alice Dobric & Moa Markefjäll

Abstract

Skyddade av vad de kriminella trodde var ett säkert krypterat kommunikationsverktyg smeds planer för kriminella handlingar helt filterlöst. Det som brottslingarna inte visste var att krypteringsverktyget övervakades i realtid, genom ett framgångsrikt internationellt polissamarbete. I denna uppsats undersöks hur Operation Trojan Shield, OTS, framgångsrikt infiltrerat den krypterade kommunikationsplattformen ANOM. Polisens övervakning i realtid genererade en världsunik bevisinsamling. Syftet med uppsatsen är att analysera hur rättsvårdande myndigheter lyckades vilseleda och manipulera kriminellas belsutsprocesser genom den innovativa kombinationen av stingoperationer och reflexiv kontroll. Med hjälp av en teorikonsumerande fallstudie analyseras hur OTS kan exemplifiera nämnda kombination av stingoperationers metoder och principer för reflexiv kontroll, vilket ger en djupare insikt i operationens effektivitet. Studiens analys och slutsatser visar på hur traditionella strategiska metoder inom brottsbekämpning har moderniserats och kombinerats i den unika operationen. Uppsatsen fyller en kunskapslucka då operationen inte tidigare studerats i en större utsträckning.

Nyckelord: Operation Trojan Shield, reflexiv kontroll, stingoperationer
Antal ord: 9 704

Innehållsförteckning

1. Inledning

Den 7 juni 2021 sker ett internationellt synkroniserat tillslag runtom i hela världen (mål nr B 9644-21, s. 4). Det är inte förrän dagen därpå som Europol i en presskonferens avslöjar att tillslagen varit en del av den så kallade Operation Trojan Shield, OTS - ett världsunikt transnationellt samarbete i vilket de största och mest sofistikerade brottsbekämpande operationerna hittills genomförts i kampen mot krypterade kriminella aktiviteter (Europol 2021b). I en tid där kriminella organisationer desperat sökte efter krypterade kommunikationstjänster utvecklade FBI kommunikationsplattformen ANOM, vilken möjliggjorde att brottsbekämpande myndigheter i realtid och dolt kunde läsa chattar som kriminella användare skickade i tron om att de var krypterade (ibid.). Resultatet? Exceptionell framgång mot den allvarliga och organiserade brottsligheten och något som aldrig tidigare skådats inom brottsbekämpning världen över (The Justice Department 2021).

1.1 Syfte och frågeställning

För att förstå hur Operation Trojan Shield kunde bli så framgångsrik krävs en djupare analys av de strategier som användes för att manipulera kriminellas beteenden och beslutsprocess. Uppsatsen ämnar att undersöka huruvida metoder för stingoperationer och innovativa principer för reflexiv kontroll kan återfinnas i ett modernt exempel på förebyggande och bekämpning av organiserad brottslighet.

Syftet med uppsatsen är således att närma sig en djupare insikt i hur brottsbekämpande myndigheter lyckats vilseleda kriminella att använda sin egen krypterade kommunikationstjänst ANOM. Syftet undersöks utifrån följande frågeställning:

- Hur kombinerar Operation Trojan Shield stingoperationers metoder med principerna för reflexiv kontroll?

2. Bakgrund

Globalisering och människors ökade rörlighet skapar nya möjligheter för gränsöverskridande brottslighet (European Commission). Den ökade komplexiteten och omfattningen av transnationell brottslighet har skapat stora utmaningar för brottsbekämpande myndigheter. Brottsbekämpandet har avancerat och utmanar traditionella övervakningsmetoder, i exempelvis Operation Trojan Shield. Behovet av ömsesidigt samarbete mellan länder för att insamla och utbyta information, i syfte att stoppa den gränsöverskridande brottsligheten, har ökat (European Commission). Följande bakgrundsavsnitt undersöker hemliga- och preventiva tvångsmedel, hur de operationaliserats samt lagstiftningskontexter.

2.1 Hemliga- och preventiva tvångsmedel och dess operationalisering

Med begreppet "hemliga tvångsmedel" omfattas metoder som genom hemliga medel och tekniker används av rättsvårdande myndigheter för att på ett dolt sätt samla in information (Hasani 2019, s. 42). Det finns en stor mängd metoder som exempelvis kameraövervakning, rumsavlyssning, hemlig övervakning av elektronisk kommunikation, telefonavlyssning också kallat hemlig avlyssning av elektronisk kommunikation samt hemlig dataavläsning (Åklagarmyndigheten 2023). Nämnda tekniker används av myndigheter för bevisinsamling, utredning och i sin tur lagförandet av kriminell aktivitet (Hasani 2019, s. 43).

2.2 Lagstiftning kring hemliga- och preventiva tvångsmedel

De juridiska ramarna för operationalisering av hemliga tvångsmedel varierar beroende av länders egna regelverk. Det finns dock vissa internationella standarder som upprättats för att gemensamt syfta till att värna om individens rättigheter. Exempelvis finns den europeiska konventionen för beskyddandet av de mänskliga rättigheterna, artikel 8, som skyddar individens rätt till privatliv utan inskränkningar om inte annat anges i lag eller på annat sätt anses vara "nödvändiga i ett demokratiskt samhälle" (Hasani 2019, s. 47).

Regleringen av hemliga tvångsmedelsanvändning är ett ämne som under senare år diskuterats i både media men också politiskt. Hasani (2019, s. 52) exemplifierar kritik som framkommit mot tidigare kosovariska regleringar av hemliga tvångsmedel runt år 2012. Rättsexperter menade att den kosovariska lagstiftningen synliggjorde bristerna i tillämpningen av hemliga tvångsmedel då avsaknaden av betydande misstanke och domstolsprövning saknades (ibid.). Detta relaterar intressant nog till en mer nutida utveckling av regleringar kring hemliga

tvångsmedel, tidigare nämnda lagstiftning från Kosovo 2012 speglar debatten om användning av hemliga tvångsmedel utan brottsmisstankar som i Sverige nådde sin kulmen under 2023. Användningen av så kallade "preventiva tvångsmedel" utan konkreta brottsmisstankar är sedan oktober 2023 tillåtet i Sverige (Åklagarmyndigheten 2023).

2.3 Sammanfattning

Med betoning på den ökade komplexiteten i brottslighetens flexibilitet utmanas traditionell brottsbekämpning. Verktyg som hemliga- och preventiva tvångsmedel får en betydande roll i den nya innovativa brottsbekämpningen.

3. Tidigare forskning

I studiens inledande fas gjordes grundliga sökningar på huruvida Operation Trojan Shield varit föremål för akademiska analyser. Resultatet var lika unikt som operationen i sig. Uppsatsen fyller därför ett stort gap i forskningen gällande huruvida stingoperationer och reflexiv kontroll kan operationaliseras i en världsunik brottsbekämpande insats som Operation Trojan Shield. För att möjliggöra en djupare analys av Operation Trojan Shields karaktärsdrag presenteras tidigare forskning om stingoperationer, dess metoder och konsekvenser i följande avsnitt. Till följd av arbetets begränsade omfattning redogörs endast ett urval av tekniker.

3.1 Definition av stingoperationer

"Sting operations" har ingen entydig definition, men enligt Newman och Socia´s (2007, s. 3) utsago finns fyra faktorer som stingoperationer anses innehålla. För det första innehåller stingoperationer ett incitament att begå brott som antingen dirigeras eller utnyttjas av polis. För det andra innehåller operationen en eller flera måltavlor i form av möjliga lagöverträdare för specifika brottstyper. För det tredje ska operationen inkludera antingen någon typ av infiltratörer eller informatörer alternativt inkludera någon typ av vilseledning. Avslutningsvis nämner författarna det mest signifikanta baselement som ingår i stingoperationer, vid varje avslutad framgångsrik operation uppges ett "gotcha climax". Detta klimax definieras som en avslutande punkt i operationen där polisen avslöjar deras inblandning (ibid.).

För att stingoperationer ska få ett utfall för rättsväsendet måste det föreligga någon grad av ”vilja” att begå brottet hos den potentiella lagöverträdaren. Hur motiveras då de potentiella lagöverträdarna? Newman och Socia (2007, s.3) menar att ”viljan” för att begå brott som är iscensatta av polisen genom vilseledning inte nödvändigtvis är ett faktum. Författarna betonar snarare att det är manipulationen och vilseledningen som särskiljer just stingoperationer. Försvarsadvokater belyser ofta denna aspekt för att ta måltavlans agerande i försvar, det finns även argument för att stingoperationer i vissa fall kan skapa brottstillfällen för personer som annars inte skulle begå brott (Newman & Socia 2007, s.3). Newman och Socia (2007, s. 26) betonar dock att polis och rättsväsendet riktar stingoperationer mot individer där brottsmisstankar eller benägenhet att begå brott redan finns samt att bevisföringen ofta är så pass god att lagöverträdarna i många fall erkänner när de konfronteras.

3.2 Vilseledningstekniker och verktyg

Vilseledning, ett centralt inslag i stingoperationer. Som tidigare nämnt används olika typer av metoder för att skapa situationer där kriminell aktivitet kan styras och övervakas av rättsvårdande myndigheter i en iscensatt situation. I följande del av redogörelsen presenteras flera olika vilseledningstekniker och verktyg.

3.2.1 Täckmantel

Under stingoperationers utförande finns ett flertal sätt för rättsväsendets personal att smälta in i omgivningen (Newman & Socia 2007, s. 7). En del täckmantlar är så vattentäta att polisen även kan ha ett samröre med, arbeta eller bo tillsammans med de misstänkta (ibid.). Genom att agera enligt sin täckmantel syftar polisen att gripa de som gör anspråk på de olagliga aktiviteterna.

3.2.2 Professionella informatörer

Professionella informatörer är en komplicerad teknik som ofta föregås av en mycket invecklad och allvarlig brottslighet. Här används en kriminell, eller tidigare kriminell, som informatör, det är enligt Newman och Socia (2007, s. 7) till stor fördel om infiltratören redan har en etablerad roll i nätverket eller är expert på den specifika brottsligheten där informationsutbyte efterfrågas. Informatörens uppgift är att i sin dolda roll i den kriminella verksamheten förse polisen med viktig information om brottsligheten eller de kriminella individer som de i sin tur kan använda i bekämpningen av brottslighet.

3.2.3 Annonsering

Annonsering refererar till en metod där poliser använder lockande erbjudanden eller anställningsmöjligheter och därmed "annonserar ut" ett tillfälle där den potentiella lagöverträdaren kan gripas (Newman & Socia 2007, s. 8).

3.2.4 Internetbaserade metoder

Med falska webbsidor och identiteter kan polisen utnyttja internet som verktyg i stingoperationer. Med hjälp av internet får polisen närmare tillgång till en dold kommunikation mellan brottslingar och skapar därför tillfällen för bevisinsamling (Newman & Socia 2007, s. 8).

3.2.5 Övervakning

Det sista men ack så viktiga vilseledningsverktyget som behandlas i denna redogörelse är övervakning. I stingoperationer har övervakningen en väsentlig roll, dels för bevisföringens betydelse i rättsprocessen senare, men också för hur operationen ska justeras under det aktiva utförandet (Newman och Socia 2007, s. 9). Verktyg som rumsavlyssning eller telefonavlyssning har utvecklats och avancerat och anpassar sig efter den moderna brottsutvecklingen.

3.3 Syfte och mål med stingoperationer

Det arbete som föreligger stingoperationer motiveras ofta med två syften. För det första är användningen av stingoperationer fördelaktigt för utredningar (Newman och Socia 2007, s. 11). Utredningarna ger insikter om kriminell aktivitet och stingoperationernas möjliggörande av bevisinsamling anses därmed enligt Panzarella och Funk (1987, s. 1) vara unik. Som brottsbekämpande insats möjliggör stingoperationer faktorer av vilseledning och doldhet en upptäckt av brott i en större omfattning än vad som ibland förutspåtts.

För det andra syftar stingoperationer att bidra till brottsförebyggande arbete och reducerande av framtida brott (Newman och Socia 2007, s. 11). Trots att den mest uppmärksammade resultatet av en stingoperation är arresteringar och i slutändan fällande domar ger stingoperationer mer än så. Newman och Socia (ibid.) exemplifierar hur Lauderhill Police Department, LPD, använde information från en stingoperation. LPD implementerade också lärdomarna från stingoperationen i det dagliga polisarbetet för att förebygga en fortsatt drogproblematik (ibid.).

3.4 Fördelar med stingoperationer

3.4.1 Utredning och rättsligt utfall

Operationerna möjliggör bevisinsamlingen samt underlättar identifiering av nyckelpersoner eller andra verksamma i de illegala aktiviteterna vilket har lett till fler arresteringar. Newman och Socia (2007, s. 25) refererar till forskning som entydigt visar på hög frekvens av arresteringar i samband med stingoperationer. Enligt författarna tyder forskningen på att stingoperationer har en hög framgångsfrekvens i relation till fällande domar (Newman & Socia 2007, s. 26). Alla stingoperationer leder inte till åtal eller fällande dom. Men enligt författarna anses dessa operationer inte vara misslyckade i sin helhet trots detta. Exempelvis

kan avslöjandet av illegal försäljning av tjänster eller produkter ge goda förutsättningar för att under en period helt reducera alternativt förebygga framtida försäljningar (Newman & Socia 2007, s. 27).

3.4.2 Polisens image

Vid avslöjanden av stingoperationernas utfall får polismyndigheter vanligtvis medial uppmärksamhet. Newman och Socia (2007, s. 26) talar för att läsarnas annars vardagliga inställning till polisens brottsbekämpande får ett lyft och polisen tenderar att få positiva återkopplingar från allmänheten. Det gäller dock att agera strategiskt i det mediala avslöjandet av operationerna. Genom att avslöja operationen i närtid till dess genomförande uppges polisen, och media, ge läsarna en positiv bild av operationen. Detta med syfte att undvika att allmänhetens fokus förskjuts på de provokativa åtgärder som ofta föreligger i operationens initierande (ibid.).

Langworthy (1989, s. 44) menar dock att den traditionella synen på stingoperationer som endast positiv för polisens image inte ger en rättfärdig bild. Han menar att det finns många mindre krävande och riskfyllda sätt att förbättra polisens anseende bland medborgarna. Langworthy menar att avslöjandet av en stingoperation, eller tillkännagivandet av en planerad operation, kan ha brottsförebyggande och avskräckande effekter i samhället men riskerar också att utföras med oetiska metoder med rättssäkerheten i blindo (ibid.). Men genom att polisen har en god kontakt med åklagarmyndighet för att bearbeta implementeringen av lagar och regler i bevisinsamlingen. Ett sådant samarbete syftar alltså att förebygga olagliga åtgärder, som exempelvis brottsprovokation, i stingoperationer (Newman & Socia 2007, s. 26).

3.5 Begränsningar med stingoperationer

3.5.1 Återfall och ökad brottslighet

Det finns enligt författarna få vetenskapliga studier som konstaterar att det brottsförebyggande utfallet varar längre än ett år. De studier som visar på att stingoperationerna har brottsförebyggande effekter har också inkluderat andra polisiära åtgärder utan att differentiera huruvida stingoperationerna därmed är den ensamma faktorn i förebyggandet av återkommande brottslighet (Newman & Socia 2007, s. 29).

Enligt författarna finns flertalet studier som visar att stingoperationer möjligtvis kan öka den riktade brottsligheten då polisen förser aktörer med nya, konstruerade, möjligheter att begå brott (Newman & Socia 2007, s.29). Även Langworthy (1989, ss. 33-34) stämmer in i denna problematik och menar att risken för ökad brottslighet måste tas i beaktning inför en stingoperation. För att förstå argumentationen fullt ut menar Newman och Socia (2007, s. 29) att det är fördelaktigt att gå tillbaka till den grundläggande formuleringen av polisens uppdrag i samhället. Polisens uppdrag är att minska brottsligheten i samhället och därmed inte bidra med möjligheter för flera brott att begås (Newman & Socia 2007, s. 29). Författarna poängterar dock att de återfann minst en studie som med vetenskaplig bakgrund nyanserade ovanstående argumentation, och därför finns ingen stående regel som garanterar stingoperationers effekter (ibid.).

3.5.2 Etik och politik

Newman och Socia (2007, s. 30) belyser också hur väletablerade etiska och politiska ställningstaganden kan omformuleras, och även överskridas, i jakten på kriminella. Stingoperationerna blir en "katt- och råttalek" där beslutsfattare och rättsvårdande myndigheter, formulerar lögner för att få möjligheten att arrestera- och agera mot kriminell aktivitet. Panzarella och Funk (1987, s. 12) menar att det finns en överhängande risk i utförandet av stingoperationer där gränser för regelverk, etik och makt suddas ut. Detta menas kunna ha stora effekter på rättsvårdande myndigheters legitimitet (ibid.).

Polisen och allmänheten, uppges enligt Panzarella och Funk (1987, s. 146) sympatisera med att oetiska lögner i vissa fall är acceptabelt i relation till den moraliska vinsten i motiveringen av fördelarna med att kriminell aktivitet avslöjas. Langworthy (1989, s. 43) poängterar här vikten av att utreda politiska och etiska dimensioner av en stingoperations påverkan på samhället för att få en bättre bild över dess positiva kontra negativa utfall.

3.6 Sammanfattning

I tidigare forskning redogörs för definitionen av stingoperationer som konturlös. Enligt Newman och Socia (2007) finns dock fyra faktorer som stingoperationer innehåller: incitament att begår brott, måltavlor, vilseledning och "gotcha"-klimax. Stingoperationer skapar ett tillfälle för brott men förutsätter någon form av vilja att begå brott. Det har också betonats att vilseledning och manipulation kan spela en viktig roll. Operationerna används i

syfte att avslöja och förebygga brott men begränsningar som rättsäkerhetsdilemman och ökad brottslighet har också lyfts.

4. Teori

Eftersom uppsatsens frågeställning delvis utgår från teorin om reflexiv kontroll presenteras en redogörelse för teorins syfte samt ett för uppsatsen relevant utplock av tekniker. Teorin kan bidra med att förstå hur brottsbekämpande myndigheter i Operation Trojan Shield kunde kontrollera den organiserade brottsligheten genom att förmå kriminella att fatta beslut som missgynnade dem själva.

4.1 Teorin om reflexiv kontroll

Teorin om reflexiv kontroll härstammar ur sovjetisk militär doktrin (Chotikul 1986, s. 43). Reflexiv kontroll innebär ett sätt att förmedla särskilt förberedd information till en partner eller motståndare, i syfte att få denne att frivilligt fatta av leverantören önskvärda beslut (Chotikul 1986, s. 5). Den reflexiva kontrollen bygger på antagandet om att kontroll över en människa bäst utövas genom att aktivt och målmedvetet påverka och manipulera informationen denne förses med (Chotikul 1986, s. 45). Det centrala målet är att få motståndaren att känna sig förvirrad och osäker samt låta denne ha bristande kunskap (Chotikul 1986, s. 68).

Den sida med högst grad av reflexiv kontroll har störst chans att påverka sin motståndares beslutsprocess (Thomas 2004, s. 242). Graden av reflexivitet beror på flera faktorer, av vilka de viktigaste är bland annat analytisk förmåga, erfarenhet och kunskap om fienden (ibid.). Ju större förståelse för sitt mål, desto större effekt har den reflexiva kontrollen (Chotikul 1986, s. 68). För att uppnå framgångsrik reflexiv kontroll krävs studier av fiendens filter (Thomas 2004, s. 241). Filtret är det genom vilket all data om den yttre världen passerar och innefattar. Det innefattar begrepp, kunskaper, idéer och erfarenheter en baserar sina beslut på (Thomas 2004, ss. 242-243). Genom att lokalisera filtrets svagaste länk kan leverantören utnyttja denna för eget syfte (Thomas 2004, ss. 241-242).

4.2 Tekniker för reflexiv kontroll

Thomas (2004, ss. 248-249) hänvisar i sin artikel bland annat till Komov som listat följande grundläggande delar av reflexiv kontroll:

1. Distraktion, genom att skapa ett verkligt eller falskt hot mot fienders viktiga platser.
2. Informationsmättnad, genom en stor mängd motstridig information.
3. Paralysering, genom att skapa en föreställning av hot mot svaga punkter.

4. Uttröttning, genom att tvinga fiender att utföra onödiga operationer och därigenom slösa resurser.
5. Vilseledning, genom att tvinga fienden att omfördela styrkor till en hotad region.
6. Avledning, genom att övertyga fienden om att gå emot koalitioners intressen.
7. Pacificering, genom att låta fiender tro att träning pågår snarare än offensiva förberedelser och därigenom minska fienders vaksamhet.
8. Avskräckning, genom att skapa en uppfattning om överlägsen styrka.
9. Provokation, genom att tvinga fienden att vidta åtgärder som missgynnar sig själv.
10. Överbelastning, genom överdrivet stor mängd information till fiender under förberedelsefasen.
11. Alternativa förslag, genom att erbjuda information som påverkar fienden bland annat juridiskt, moraliskt eller ideologiskt.
12. Påtryckningar, genom att erbjuda information som misskrediterar ledningen.

Komkov har inte nämnt huruvida varje element kan användas individuellt eller i kombination (Hosaka 2019, s. 332). Kamphuis hävdar dock att många element kan kopplas samman och att vissa element naturligt följer implementeringen av andra (ibid.).

Thomas (2004, s. 249) hänvisar också till Chausovs listade principerna för reflexiv kontroll som en målorienterad process som:

- omfattar alla aspekter av reflexiv kontroll,
- bygger på en bild av sin motståndares kapacitet och potential,
- överensstämmer mellan mål, uppdrag, plats, tid och metoder för reflexiv kontroll samt
- modellerar förutsägelser för motståndarens åtgärder.

Teorin kommer i analysdelen att ställas mot teknikerna i Operation Trojan Shield, för att pröva huruvida reflexiv kontroll återfinns i ett brottsbekämpande sammanhang.

5. Metod och material

Metodavsnittet avser att presentera uppsatsens metod och material samt en metoddiskussion. Metodavsnittet avslutas med en redogörelse av arbetets operationalisering.

5.1 Metod

Som tidigare redovisats är uppsatsens syfte att studera hur Operation Trojan Shield kan illustrera användning av stingoperationers metoder och principerna för reflexiv kontroll. Den metodologiska ansats som anses mest lämplig är en teorikonsumerande fallstudie. En sådan studie redogör för tidigare etablerade teorier för att tolka, förstå och analysera specifika fall (Esaiasson 2017, s. 42). Genom att tillämpa teorin om reflexiv kontroll och tidigare forskning om stingoperationer på fallet OTS kan analysen förankras i teoretiska begrepp och empiriska exempel.

Teorikonsumerande forskningsdesigner varierar i generaliserbarhet efter hur syftet är formulerat (Esaiasson 2017, s. 43). Vår teorikonsumerande studie syftar inte till att uppnå en hög generaliserbarhet då vi endast undersöker ett fall. Med en medvetenhet om studiens begränsningar av generaliserbarhet och risken för att teorikonsumerande studier kan riskera övertolkning finns flera fördelar. En framträdande sådan är hur den teorikonsumerande ansatsen möjliggör en befintlig teoris prövning mot ett samtida exempel, vilket kan mena att stärka dess aktualitet (Esaiasson 2017, ss. 89-90).

En fallstudie är en forskningsdesign som avser en grundlig genomgång av ett, eller ett litet antal, specifikt fall (Gerring 2004, s. 341). En stor fördel med fallstudier är å ena sidan dess potential att djupdyka i detaljer. Å andra sidan kan fallstudier, likt ovan nämnda teorikonsumerande ansats, vara begränsade i sin generaliserbarhet då fokuset endast riktas mot, i det här fallet, en operation.

5.2 Material

Uppsatsen utgår från flera typer av material. Som grund för tidigare forskning och teori har vetenskapliga artiklar och litteratur använts som förstahandskällor för att gynna studiens centralitet och aktuella grund (Esaiasson 2017, s. 293). Fördelarna med att använda vetenskapliga artiklar är att dess teoretiska perspektiv är direkt tillämpliga i vår uppsats, vilket speglas i tidigare forskning och teori. Det ökar trovärdigheten i vår analys. Dock är det

viktigt att utifrån dessa primärkällor också noggrant uppmärksamma olika nyanser och argumentationer även om dessa inte helt överensstämmer med studiens specifika kontext.

Redogörelsen av Operation Trojan Shield har huvudsakligen baserats på information från de brottsbekämpande myndigheterna bakom operationen, men också dokument från rättsväsendet och information från myndigheters webbsidor. Informationen har jämförts i flera olika källor för att säkerställa att empirin är trovärdig.

5.3. Diskussion av forskningsdesign

I efterhand är det viktigt att återkoppla till den teorikonsumerande ansats som forskningen utgår från. En teorikonsumerande uppsats där en teori valts i inledningsfasen av ett arbete garanterar inte att teorin är tillämpbar i fallet, vilket å ena sidan skulle kunna ifrågasätta reliabiliteten i forskningen. Å andra sidan resonerade vi kring det faktum att om utfallet skulle resultera i att det inte fanns lämpliga teoretiska jämförelsepunkter så var det också ett resultat. Studiens reliabilitet och validitet ventileras i detta sammanhang i relation till huruvida tidigare forskning och teori kunnat appliceras.

Empirin grundar sig i tillförlitliga förstahandskällor, men kan ge en viss bristfällig bild av operationen. Det kan exempelvis handla om att de brottsbekämpande myndigheterna inte inkluderar kritik mot sig själva. Enligt vår bedömning är detta dock inget som påverkar våra slutsatser.

Manijikian (2013, s. 565) menar att samhällsvetare inte kan teoretisera isolerat utan påverkan av personliga och omgivningens värderingar. Det är sålunda viktigt att belysa att uppsatsens analys och slutsatser är ett resultat av tolkningar. Eftersom empirin i uppsatsen noggrant och konsekvent hänvisats till teori och tidigare forskning, kan dock någorlunda hög reliabilitet och validitet påstås uppnås.

5.4 Operationalisering

Teorin om reflexiv kontroll och den tidigare forskningen om stingoperationer nyttjas i ett kompletterande syfte för att få ett mer nyanserat svar på forskningsfrågan. Genom att bryta ner centrala begrepp och applicera dem på Operation Trojan Shield har teori och tidigare forskning operationaliserats. Begreppen har sedan använts för att analysera hur

stingoperationers metoder och reflexiv kontroll kan återfinnas i OTS. Likvärdigt har tidigare forskning om stingoperationer operationaliserats i jämförelser av vilka vilseledningstekniker som anses applicerbara i fallet.

6. Resultat

I följande redogörelse presenteras Operation Trojan Shield kronologiskt. Inledningsvis presenteras syftet med OTS och skapandet av FBI:s kommunikationstjänst ANOM, därefter för utvecklingen av ANOM, inklusive distribution och användning och slutligen för operationens utfall genom att presentera arresteringar och beslag.

6.1 Operationens framkomst

År 2017 började FBI San Diego att utreda Phantom Secure, ett företag som erbjöd krypterad kommunikation (Cheviron 2021, s. 4). Utredningen visade att den huvudsakliga kundbasen var transnationella kriminella organisationer (ibid.). Efter åtalet mot Phantom Secure fann utredarna att användarna snabbt flyttade till andra plattformar för krypterad kommunikation, såsom Sky Global och EncroChat (The Justice Department 2021). Eftersom krypterade kommunikationstjänster ger en sköld mot brottsbekämpande övervakning och upptäckt, är det en tjänst som är högt efterfrågad i kriminella sammanhang (Cheviron 2021, s. 5). FBI tog tillfället i akt att utnyttja dels det tomrum som uppstod efter nedstängningen av Phantom Secure, dels de kriminellas desperata behov av en ny krypterad kommunikationstjänst genom att rekrytera en så kallad confidental human resource, CHS (Cheviron 2021, s. 6).

CHS:en hade utvecklat en ny krypterad kommunikationstjänst, vilken FBI fick tillgång till i utbyte mot pengar och reducerat straff (Cheviron 2021, s. 6). Innan tjänsten erbjöds på marknaden byggdes en huvudnyckel in i det befintliga krypteringssystemet - en funktion som utan användarnas kännedom möjliggjorde för brottsbekämpande myndigheter att dekryptera och lagra meddelanden (Cheviron 2021, s. 7). För första gången i historien var FBI med och utvecklade en plattform för krypterad kommunikation - ANOM (The Justice Department 2021).

Operation Trojan Shield inleddes, något som kom att bli en av de mest sofistikerade brottsbekämpande insatserna hittills i kampen mot kriminell verksamhet (Europol 2021a). Målet med ANOM var att rikta in sig på global organiserad brottslighet, narkotikahandel och penningtvätt oavsett var de verkade (ibid.).

6.2 Operationens genomförande

Den CHS som rekryterades av FBI gick också med på att distribuera ANOM-enheter till sitt befintliga nätverk bestående av distributörer av krypterade kommunikationsenheter, som alla i sin tur hade direktlänkar till kriminella nätverk (Cheviron 2021, s. 6). Eftersom krypterade kommunikationsenheter finns till för att undvika brottsbekämpande upptäckt, bygger distributionen av dessa på förtroende (ibid.).

ANOM-enheterna såg utifrån ut som en vanlig smartphone, men saknade nödvändiga funktioner som GPS och email (The Justice Department 2021). Den enda praktiska användningen var krypterad kommunikation genom ANOM (mål nr B 9642-21, s. 14). Kommunikation kunde enbart ske mellan ANOM-användare och en enhet kostade motsvarande över 20 000 svenska kronor (Cheviron 2021, s. 5). På grund av enheternas begränsade funktionalitet bedömdes det osannolikt att enheterna skulle ha icke-kriminella användare (ibid.). ANOM-applikationen var dold i en kalkylatorapplikation (mål nr B 9644-21, s. 4) och först när användaren angav en hemlig PIN-kod och därefter höll ned likamed-tecknet öppnades ANOM (mål nr B 9642-21, s. 16). Om enheten undersöktes av en ovetande användare fanns det således inget som avslöjade applikationen (ibid.). På ANOM kunde användare skicka text, bilder, videor, anteckningar och korta röstmeddelanden till enskilda användare eller grupper (mål nr B 9642-21, s. 15). Avsändare, mottagare, innehåll, tid och självförstörelsetid var synligt för avsändare och mottagare (mål nr B 9642-21, s. 17) medan platsinformation enbart var synligt för de brottsbekämpande myndigheterna (ibid.).

I slutet av 2018 började CHS:en erbjuda ANOM-enheter till tre före detta Phantom Secure-distributörer med kopplingar till kriminella organisationer främst i Australien (Cheviron 2021, s. 7). ANOM marknadsfördes som “designat av kriminella för kriminella” (The Justice Department 2021) och som ett “nytt sofistikerat system med enheter som är omöjliga att dekryptera av rättsväsendet” (mål nr B 9642-21, s. 13). I ett första beta-test i Australien utnyttjades ANOM uteslutande i kriminellt syfte (The Justice Department 2021). Tillväxten av enheterna var till en början långsam men allt eftersom skedde en organisatorisk tillväxt, och i takt med ökad efterfrågan ökade även distributionen till att omfatta fler kriminella distributörer (Cheviron 2021, ss. 8-9).

Det var först ett år senare som FBI själva fick tillgång till att granska meddelandena i enlighet med Mutual Legal Assistance Treaties (Cheviron 2021, ss. 7-9), vilket möjliggör för brottsbekämpande myndigheter och åklagare att insamla bevis, information och vittnesmål utomlands i en form som är laglig i den begärande staten (United States Department of Justice 2022, s. 2). Vid samma tillfälle bjuds andra partners in i samverkan runt den tillgängliga informationen på plattformen (mål nr B 9642-21, s. 13). Operation Trojan Shield leddes av amerikanska FBI, den nederländska polisen, den svenska Polismyndigheten och Australiens federala polis (ibid.). Europol inrättade en operativ insatsstyrka, en tillfällig grupp av representanter från medlemsstaterna och Europol som bildas för ett specifikt projekt och koordinerar underrättelse- och utredningsinsatser (Europol 2022, s. 13). De samordnade det internationella brottsbekämpande samfundet, berikade informationsbilden och förde in kriminalunderrättelser i pågående operationer, och fungerade således som ett kriminalunderrättelsecentrum som underlättade utbyte av information (Europol 2021a). Med i samarbetet var också Österrike, Kanada, Danmark, Estland, Finland, Tyskland, Ungern, Litauen, Nya Zeeland, Norge, Storbritannien, Skottland och USA samt US Drug Enforcement Administration, DEA (ibid.).

År 2020 respektive 2021 nedmonterades EncroChat och Sky Global (The Justice Department 2021) - en avsiktlig och strategisk aspekt av Operation Trojan Shield (Europol 2021a). Nedmonteringarna resulterade i massiv ökning av efterfrågan på ANOM-enheter och antalet aktiva användare växte från 3 000 till 9 000 (Cheviron 2021, s. 11).

6.3 Operationens utfall

Den 7:e juni 2021 gjordes ett internationellt synkroniserat tillslag världen över av samarbetspartners i OTS (mål nr B 9644-21, s. 4). På FBI:s presskonferens samma dag betonades att dagen markerar kulmen på mer än fem år av strategiskt, innovativt och komplext utredningsarbete i syfte att störa och avveckla krypterade kommunikationstjänster (The Justice Department 2021).

Vid detta tillfälle hade totalt 11 800 ANOM-enheter använts (Cheviron 2021, s. 10), av över 300 kriminella organisationer i fler än 100 olika länder (Europol 2021a). I 18 månaders tid hade FBI, Europol och DEA utnyttjat underrättelser i realtid från de 27 miljoner meddelanden som erhållits och granskats från ANOM (Europol 2021b). Utfallet innefattade totalt över 700

husrannsakningar, drygt 800 arresteringar och fler än 100 hot mot liv som kunnat mildras (ibid.). Beslagen inkluderade över 8 ton kokain, 22 ton cannabis och cannabisharts, 2 ton syntetiska droger, 6 ton prekursorer för syntetiska droger, 250 skjutvapen, 55 lyxfordon och över 48 miljoner dollar i olika världsomspännande valutor och kryptovalutor (ibid.). Underrättelserna gav också möjlighet att störa stor kriminell verksamhet medan plattformen var aktiv (Europol 2021a). Operation Trojan Shield har beskrivits krossa allt förtroende som brottslingar kan ha för krypterade kommunikationstjänster (The Justice Department 2021).

Europol pekar ut tre lärdomar av Operation Trojan Shield. Det handlar inledningsvis om exceptionell insikt i kriminella kretsar (Europol 2021b). Det innefattar bland annat ökad kunskap om användandet av digitala verktyg, inte minst kryptering och att tjänsterna erbjuds avsiktligt för kriminella behov (Cheviron 2021, ss. 10-11). För det andra påvisar OTS att kriminella nätverk på 2000-talet är mer flexibla än vad som tidigare trotts, vilket är anledningen till varför brottsbekämpande myndigheter behöver utnyttja teknisk infrastruktur för att verka starkare och mer störande (Europol 2021b). Slutligen betonar OTS vikten av internationellt samarbete bland brottsbekämpande organ (ibid.). Den förbättrade underrättelsebilden förväntas stödja det fortsatta arbetet (Europol 2021a).

7. Analys

Följande analysavsnitt är uppdelat i två delar. Den första delen syftar till att urskilja stingoperationers karaktärsdrag i Operation Trojan Shield, varpå den efterföljande delen syftar till att urskilja principer för reflexiv kontroll i samma operation. Först härefter går att besvara hur Operation Trojan Shield kombinerar stingoperationers metoder med principerna för reflexiv kontroll, vilket görs i uppsatsens slutsatser. Att ge kontext till Operation Trojan Shield som en stingoperation möjliggör en djupare förståelse för operationens inslag av reflexiv kontroll. Följande analysdel syftar att möjliggöra en djupare insikt i uppsatsens frågeställning: *Hur kombinerar Operation Trojan Shield stingoperationers metoder med principerna för reflexiv kontroll?*

7.1 Operation Trojan Shield som stingoperation

7.1.1 Definition

Newman och Socia (2007, s. 3) utmanar den annars otydliga definitionen av stingoperationer med fyra faktorer som författarna menar att stingoperationer innehåller. Hur återfinns dessa fyra faktorer i Operation Trojan Shield?

Den första faktorn som Newman och Socia (2007, s. 3) lyfter är huruvida operationen uppmuntrar till brott arrangerat av polis. Denna återfinns i Operation Trojan Shield på flera sätt. OTS har en betydande polisiär inblandning i det aktiva skapandet, distributionen och marknadsföringen av ANOM. Ett internationellt polissamarbete utvecklade ANOM med syfte att locka kriminella till att använda appen som skulle kunna övervakas av polisen i realtid (Cheviron 2021). Användarna av ANOM antog att tjänsten var legitim och på så sätt skapade polisen ett tillfälle för brott att planeras och begås i övervakad form.

Den andra faktorn gäller måltavlorna för operationen. Newman och Socia (2007, s. 3) menar att en stingoperation ska innehålla en eller flera måltavlor, i form av grupper och individer, som tros ha förmåga att begå brott. Operation Trojan Shield bottnar i en polisiär desperation att få kontroll över den transnationella brottsligheten (The Justice Department 2021). Ett krypteringsverktyg som ANOM tillät polisen att inkludera flera olika typer av måltavlor men som alla på olika sätt var knutna till kriminella nätverk. Å enda sidan kan argumenteras för att OTS saknade specifika måltavlor då operationen omfattade ett brett spektrum av kriminella nätverk och varierande brottskapacitet. Det ska å andra sidan betonas att

operationen medvetet avstod från att begränsas till enskilda mål utan lät bevisinsamlingen styra utveckling och resultat, måltavlan begränsades därmed inte till en specifik grupp.

Faktor nummer tre gäller huruvida insatsen innehåller någon typ av infiltratör, informatör eller vilseledning (Newman & Socia 2007, s. 3). FBI och de andra samarbetsorganen brukade vilseledning med hemliga- och preventiva tvångsmedel genom att distribuera ANOM som en "säker" krypterad chattjänst. Genom vilseledningen möjliggjordes också ett eget infiltratörsskap utan behov för att ha en fysisk infiltratör på plats som begränsas både säkerhetsmässigt och fysiskt. Den digitala infiltrationen av chattarna möjliggjorde att polisen hade ögon på betydligt fler ställen än vad en fysisk infiltratör hade möjliggjort.

Den sista faktorn åsyftar "gotcha-klimaxet" som syftar till en avslutande punkt i insatsen där de inblandade myndigheternas roll avslöjas. OTS nådde sitt klimax den 7:e juni 2021 när det internationella samarbetet möjliggjorde synkroniserade tillslag mot ANOM-användare världen över. Över 800 arresteringar av misstänkta individer har redovisats. Detta mycket komplexa klimax ställde höga krav på att operationen inte fick avslöjas i förtid. Så när arresteringarna kunde göras till följd av den omfattande bevisinsamlingen markerades denna slutpunkt av ett "gotcha-klimax", polisen lyckades prestera innan insatsen avslöjades. Sammanfattningsvis kan därmed samtliga fyra av Newman och Socias (2007, s. 3) definitionsfaktorer återfinnas i OTS.

7.1.2 Operationens syfte

Som nämnt i uppsatsens tidigare forskning kännetecknas stingoperationer av två syften. Det första syftet är dess utredande faktor som ger goda förutsättningar för rättsväsendets utredningar av den kriminella aktiviteten (Newman och Socia 2007, s. 11). OTS visar explicit hur detta syfte uppfylls genom sin unika kombination av hemliga- och preventiva tvångsmedel. Genom att involvera övervakning av kommunikationsplattformen kunde både information om brott som redan begåtts eller begicks i nutid samlas in, men även information om framtida handlingar vilket genererade plats för preventiva tvångsmedel. Med hjälp av hemliga- och preventiva tvångsmedel som hemlig dataavläsning kunde de 27 miljoner meddelanden som skickats mellan ANOM-enheterna användas för att effektivt störa kriminell aktivitet (Europol 2021b), tydligast aktualiserat genom det synkroniserade tillslaget den 7:e juni 2021. Det var inte endast det fysiska begränsandet genom arresteringar som var

betydande utan också det faktum att kriminellas tillit till krypterade chattjänster med stor sannolikhet förstörts.

Det andra syftet som kännetecknar stingoperationer är dess brottsförebyggande arbete och reducering av framtida brott (Newman och Socia 2007, s.11). Huruvida brottsförebyggande stingoperationers arbete faktiskt blir är svårt att mäta. Men det finns vissa faktorer som trots detta ger en övergripande bild av hur OTS har haft en brottsförebyggande påverkan. Som nämnt ovan kan antas att kriminellas förtroende för krypterad kommunikation satts ur spel (The Justice Department 2021), detta skulle i sin tur kunna leda till att samordningen försvåras som möjligtvis kan leda till att vissa brott förebyggs. Resultatet av operationen, arresteringar, beslag och slutligen domar är i sig en förebyggande åtgärd då framtida brottslig kapacitet begränsas genom resurser.

Den förmåga som stingoperationer och i det här fallet OTS exemplifierar ger insikt i hur betydande och unik operationernas bevisinsamling kan vara. Som Panzarella och Funk (1987, s.1) betonar ger de viktiga insikter om annars dold brottslig aktivitet. Operationens utfall är fortfarande relativt färskt, därför är det svårt att fastställa konkreta exempel på efterdyningar. Men mängden underrättelser har, precis som Panzarella och Funk (ibid.) betonar, möjliggjort en djupare förståelse för brottsförebyggande arbete och dess framtid.

7.1.3 Vilseledningstekniker

Stingoperationers olika tekniker är också deras kännetecken. Tekniker som: "täckmantlar", "professionella informatörer", "annonsering", "internetbaserade metoder" och "övervakning" är ett fåtal, om än de mest framträdande, av de oändliga metoder som kan kombineras i stingoperationer. Operation Trojan Shield möjliggör en intressant fallstudie där traditionella metoder anpassats efter en digital samtid. En systematisk analys av hur dessa metoder operationaliserats i OTS kan ge en bild av operationens genomförande. Denna del av analysen syftar att belysa operationaliseringen av stingoperationers metoder.

Täckmantel och professionella informatörer

Den traditionella bilden av hur stingoperationers täckmantlar ser ut har utmanats av nya innovationer, något som operationaliserats i Operation Trojan Shield. Genom att skapa en övervakad kommunikationsplattform gav kombinationen av hemliga- och preventiva tvångsmedel polisen möjlighet att infiltrera kriminellas kommunikationer utan att riskera den

egna organisationens välbefinnande och dolda roll. OTS unika metod lyckades generera förstahandsinsikter i den ofiltrerade kommunikationen mellan kriminella när ANOM i sig verkade som en "dold agent", en täckmantel och digital professionell informatör.

Syftet med täckmantlar är att genomföra bevisinsamling och utredning med hjälp av att smälta in i miljön och observera det som tar plats för att slutligen göra anspråk och avbryta den kriminella aktiviteten (Newman & Socia 2007, s.7), likt preventiva tvångsmedel. Men användningen av täckmanteln genererade också information om brott som utförts eller utfördes i realtid vilket också ger operationen ett inslag av hemliga tvångsmedel. Kombinationen av täckmantel och informatör visar också på operationens effektivitet att integreras i kriminellas kommunikationstjänst och samtidigt tillåta den falska trygghetен för dold kommunikation att fortgå.

Annonsering

Newman och Socias (2007, s.8) redogörelse för traditionella vilseledningsverktyg betonar annonsering som en effektiv, men kritiserad, metod för att locka kriminella att delta i aktiviteter som de annars inte skulle deltagit i. I relation till OTS finns tendenser av annonsering men som också tar hänsyn till debatten om rättsäkerhetens roll när det gäller att "lura" eller "locka" in personer som annars inte skulle deltagit i de brottsliga handlingarna. Det som skiljer sig mellan den traditionella metoden och Operation Trojan Shields är det faktum att OTS inte drevs av ett lockande. Operationen möjliggjorde endast fortsatt kommunikation efter att andra kända krypterade verktyg knäckts av polis. Dessutom kan också argumenteras för att en icke-kriminell användare av ett krypterat verktyg med stor sannolikhet inte hade valt att använda ANOM då en enhet inte kunde brukas för annan än dold kommunikation och endast kommunicera med andra ANOM-enheter (Cheviron 2021, s. 5).

Internetbaserade metoder

Internetbaserade verktyg är den metod som varit mest uppmärksammad i den unika utformningen av Operation Trojan Shield. Internets revolution i samhället utnyttjades i samband med operationen för att skapa en kommunikationskanal för kriminella som med som tillät polisiär övervakning och bevisinsamling på en mycket detaljerad nivå. Internet möjliggör också en bredare insikt av det internationella perspektivet, användningen av internet gav polisen tillgång till globala kriminella nätverk och deras kommunikationer i

realtid. Innovationen av en ny operationalisering av metoden tillät den annars omfattande begränsningen av geografiska utmaningar (Newman & Socia 2007, s.8). Den teknologiska lösningen blev därmed en betydande del för operationens omfattande framgång.

Övervakning

Övervakning är en traditionell metod för stingoperationer men kan anpassas på många olika sätt och har en betydande roll för stingoperationers ofta extensiva bevisföring (Newman & Socia 2007, s. 9). I Operation Trojan Shield brukades två typer av övervakning. För det första användes traditionell övervakning, inklusive hemliga- och preventiva tvångsmedel som hemlig dataavläsning. Detta för att möjliggöra den realtidsövervakning som ledde till bevisinsamlingen i form av 27 miljoner sparade meddelanden (Europol 2021b). För det andra användes också övervakning som en ständigt utvärderande funktion för att hela tiden justera operationens tillvägagångssätt för att få det mest effektfulla utfallet. Genom att under operationens gång överväga bevisen som samlats in kunde polisen också studera hur och när operationen skulle avslöjas. OTS stora "gotcha-klimax" baserades på denna övervakning, med information om vem som skulle gripas kunde 800 arresteringar göras världen över. Övervakningen i OTS är unik och helt och hållet avgörande för de realtidsanpassningar som operationen gjorde efter nätverkens beteenden.

Sammanfattningsvis illustrerar Operation Trojan Shield hur traditionella vilseledningstekniker för stingoperationer kan förfinas med hjälp av den digitala utvecklingen och modern teknik och hur denne skapade en omfattande strategisk möjlighet att ingripa mot den organiserade brottsligheten internationellt.

7.1.4 Operationens karaktär

Följande del av analysen presenterar tidigare nämnda fördelar och begränsningar med stingoperationer, applicerat på Operation Trojan Shield.

Utredning och rättsligt utfall vs. återfall och ökad brottslighet

Stingoperationer är kända för dess möjligheter till djupgående utredningar. Newman och Socias (2007, s. 25) positiva inställning till utredningens förmåga att resultera i stora mängder arresteringar bekräftas även i Operation Trojan Shield. Genom identifikation av nyckelpersoner som också kunde bemötas med straffpåföljder, beslagtagning av stora

mängder vapen och narkotika samt större insikt i de komplexa strukturerna som de kriminella nätverken bygger på fick utredningen ett stort positivt inflytande.

Operationen har också nackdelar som måste tas på allvar. En av de mest framträdande kritikerna mot stingoperationer är dess relevans i relation till återfall och ökad brottslighet. Som Newman och Socia (2007, s. 29) betonar finns det få studier som tyder på att stingoperationers, ofta i kombination med andra insatser, brottsförebyggande-efterdyningar varar längre än ett år. Huruvida brottsligheten har minskat i relation till OTS är svårt att bedöma.

I relation till argumentationen om ökad brottslighet önskas göra en koppling till tidigare del av analysen. Som tidigare nämnt i relation till Operation Trojan Shields vilseledningstekniker är annonseringaspekten här unik. Newman och Socia (2007) samt Langworthys (1989) argumentation för ökad brottslighet i samband med operationerna kan förstås utifrån den traditionella förståelsen för annonsering, alltså problematiken och oron för personer som annars inte hade begått kriminella handlingar blandats in (Langworthy 1989, ss. 33-34). I OTS återfinns möjligtvis inte den oron i samma utsträckning, då det kan hävdas att inga lockelser användes förutom användningen av en "säker" krypteringstjänst. Att använda krypteringstjänster i sig är inte olagligt utan det är snarare innehållet som användarna skapade i ANOM som leder till brottsmisstankarna. Operationen saknar helt polisiär inblandning i form av erbjudande av fake-tjänster eller andra lockelser som traditionellt använts för att vilseleda och senare arrestera kriminella.

Polisens image vs. etik och politik

Det som ofta motiverar utförandet av dessa ofta komplicerade stingoperationer är den polisiära motivationen om en bra image (Newman och Socia 2007, s. 26). Det internationella polisiära samarbetet i Operation Trojan Shield genererade stor medial uppmärksamhet. Operationen presenterades som en framgångsrik insats mot den gränsöverskridande brottsligheten vilken kan tala för Newman och Socias (2007, s. 26) argument om att positiva medierapporter syftar till att porträttera de polisiära insatserna i ett positivt ljus. Dess tidiga offentliggörande kan också möjligtvis bekräfta Langworthys (1989, s. 44) redogörelse för det strategiska syftet med att publicera positiv information för att inte riskera att den etiska debatten tar alltför stor plats. Kritiken för huruvida rättssäkerheten äventyrats besvarades av Europol att fokus ska riktas till de positiva effekterna snarare än den etiska debatten.

Operation Trojan Shields resultat har beskrivits som exceptionell framgång mot den allvarliga och organiserade brottsligheten som aldrig tidigare skådats inom brottsbekämpning (Europol 2021b).

7.1.5 Sammanfattning

Operation Trojan Shield karaktäriserar en stingoperation genom dess signifikanta syfte och tillvägagångssätt. Operationen illustrerar ett exempel på hur en samtida stingoperation kan utformas. Trots att uppsatsen inte syftar att diskutera huruvida rättssäkert operationen genomfördes är det intressant att reflektera över hur en samtida stingoperation möts av samma karaktäristiska kritik som historiska stingoperationer. Stingoperationers användning av vilseledning är ett utmärkande kännetecken. I fortsatt del av analysen syftar till att urskilja principer för reflexiv kontroll i samma operation, för att i slutsaserna möjliggöra att besvara frågeställningen hur Operation Trojan Shield exemplifierar en kombination, och att metoder i stingoperationer på så sätt kan liknas vid strategier för reflexiv kontroll.

7.2 Användning av reflexiv kontroll i Operation Trojan Shield

För att möjliggöra besvarande av huruvida Operation Trojan Shield kombinerar stingoperationers metoder med principerna för reflexiv kontroll krävs vidare även en analys av reflexiv kontroll i OTS. Som konstateras i analysdelen ovan återfinns stingoperationers metoder för vilseledning i OTS. Vilseledning, i form av manipulation, är också ett element i tekniker för reflexiv kontroll, vilket nedan analys reflekterar kring. På så sätt möjliggörs för en djupare insikt för kombinationen i Operation Trojan Shield.

7.2.1 Manipulation av information

Som tidigare nämnt i avsnittet för teorin innebär reflexiv kontroll ett sätt att förmedla särskilt förberedd information till en partner eller motståndare, i syfte att få denne att frivilligt fatta av leverantören önskvärda beslut (Chotikul 1986, s. 5). De centrala målen är dels att få denne att känna sig förvirrad och osäker, dels att låta denne ha bristande kunskap (Chotikul 1986, s. 68). Vidare bygger den reflexiva kontrollen på antagandet om att kontroll över en annan människa bäst utövas genom att aktivt och målmedvetet påverka och manipulera informationen denne får (Chotikul 1986, s. 45).

I sammanhanget av Operation Trojan Shield erbjöds en krypterad plattform kallad ANOM (The Justice Department 2021). I spridandet av ANOM-enheter undanhölls dock en för de kriminella väsentlig information - att meddelanden kunde dekrypteras och på så sätt granskas och lagras av brottsbekämpande myndigheter (Cheviron 2021, s. 7). Den verkliga avsikten med ANOM, att rikta in sig på global organiserad brottslighet, narkotikahandel och penningtvätt oavsett var de verkar (Europol 2021a), behålls således dold, vilket möjliggjorde för FBI och internationella samarbetspartners fick tillgång till kriminella nätverks kommunikation i syfte att störa kriminell aktivitet (Europol 2021b). Ett ytterligare exempel på undanhållande av information finns att hitta i faktum att meddelandena på ANOM innehöll platsinformation, något som var osynligt för användarna men synligt för de brottsbekämpande myndigheterna bakom ANOM (mål nr B 9642-21, s. 17).

Samtidigt skapades också av brottsbekämpande myndigheter information i form av att kriminella nätverk trodde att de använde en säker, krypterad kommunikationsplattform (Europol 2021a), inte minst på grund av marknadsföringen av ANOM som "designat av kriminella för kriminella" (The Justice Department 2021) och som ett "nytt sofistikerat system med enheter som är omöjliga att dekryptera av rättsväsendet" (mål nr B 9642-21, s. 13).

Genom att på ett strategiskt sätt kontrollera de kriminellas informationsflöde och noggrant hantera vilken information de skulle få, kunde det verkliga syftet med ANOM döljas och ANOM-enheter spridas och börja användas i kriminella syften. Med utgångspunkt i att kriminella efterfrågar krypterade kommunikationstjänster för att undvika brottsbekämpande övervakning och upptäckt (Cheviron 2021, s. 5), hade kriminella med stor sannolikhet aldrig börjat använda ANOM om de haft vetenskapen att kommunikationen inte var krypterad. Manipuleringen i form av undanhållande av information kan därför sägas ha varit avgörande för Operation Trojan Shield och dess framgång vad gäller brottsbekämpning.

Ett första exempel på vilka aspekter av reflexiv kontroll som använts i Operation Trojan Shield kan därför sägas vara manipulation av information. FBI lät de kriminella ha bristande kunskap i och med dels undanhållandet av viss information, dels skapandet av falsk information. Detta ledde till att de kriminella byggde upp en falsk trygghet för ANOM, vilket i sin tur resulterade i att de kriminella beslutade att börja använda ANOM samt vara mindre försiktiga och istället mer benägna att kommunicera sina olagliga aktiviteter online. På så sätt

presenterades och undanhölls information för att få de kriminella att agera på ett sätt som gynnade brottsbekämpande myndigheter.

7.2.2 Konsten att förutsäga reaktioner

En grundläggande komponent för att framgångsrikt kunna utöva reflexiv kontroll är att ha den högre graden av reflexiv kontroll i jämförelse med sin motståndare, något som enligt Thomas (2004, s. 242) kan uppnås genom analytisk förmåga, allmän kunskap och erfarenhet samt kunskap om sin motståndare. Som tidigare nämnt i teoriavsnittet betonar även Chotikul (1986, s. 68) att effekten av den reflexiva kontrollen beror på förståelsen för sitt mål. I användandet av reflexiv kontroll utnyttjas bland annat moraliska och psykologiska faktorer, såväl som personliga egenskaper och vanor (Thomas 2004, s. 242).

I Phantom Secure-utredningen, strax före inledandet av Operation Trojan Shield, upptäcktes att den krypterade kommunikationsplattformen Phantome Secure hade en kundbas vars huvudsakliga syfte var användning av krypterad kommunikation för transnationell kriminell verksamhet (Cheviron 2021, s. 4). Efter åtalet mot Phantom Secure upptäcktes dessutom att kriminella användare snabbt letade efter andra plattformar för krypterad kommunikation (The Justice Department 2021). I samband med detta konstaterades att krypterade kommunikationstjänster är högt efterfrågade i kriminella sammanhang, på grund av dess sköld mot brottsbekämpande övervakning och upptäckt (Cheviron 2021, s. 5).

Tack vare den erhållna informationen i utredningen erhölls insikter som bidrog till att förutspå kriminellas reaktioner efter nedmonteringen av Phantom Secure. Denna typ av kunskap, eller med utgångpunkt i teorin om reflexiv kontroll - förståelse för sitt mål, kan sålunda hävdas varit betydande för Operation Trojan Shield. Om de kriminella nätverken haft högre grad av reflexiv kontroll och konsten att förutsäga de brottsbekämpande myndigheternas ambitioner att utnyttja all erhållen kunskap om krypterade kommunikationsverktyg i en operation med syfte att störa kriminell verksamhet, hade Operation Trojan Shield troligen misslyckats.

Förståelsen för sin motståndare kan också hävdas innebära de brottsbekämpande myndigheternas kunskap om de kriminellas behov utöver en enhet som erbjuder krypterad kommunikation. Detta innefattar bland annat att ANOM-enheterna utifrån såg ut som en vanlig mobiltelefon (mål nr B 9644-21, s. 4), att kommunikation enbart kunde ske mellan

ANOM-användare (Cheviron 2021, s. 5), att ANOM-applikationen var dold i enheten (mål nr B 9642-21, s. 16) samt att en enhet kostade stora summor pengar (Cheviron 2021, s. 5). Det innefattar också att meddelanden kunde skickas till en grupp ANOM-användare och att det var möjligt att skicka text såväl som bilagor (mål nr B 9642-21, s. 15).

Såvida ANOM-enheten saknat funktioner som kriminella efterfrågar, eller uppenbart avslöjat att de inte utvecklats av kriminella, hade efterfrågan troligtvis inte vuxit till att bli lika stor. Syftet med ANOM var att rikta in sig på global organiserad brottslighet, narkotikahandel och penningtvätt oavsett var de verkar (Europol 2021a). Att användarna uteslutande använde ANOM i kriminellt syfte (The Justice Department 2021) påvisar således konsten att förutsäga reaktioner.

Ett ytterligare resonemang vad gäller att förutspå de kriminellas reaktioner, går att föra kring det rätta tillfället för utvecklandet av ANOM, inklusive utnyttjandet av sårbarheter. Eftersom krypterad kommunikation per definition syftar till att undvika upptäckt, bygger distributionen av krypterade enheter på förtroende (Cheviron 2021, s. 6). FBI förutsåg att ANOM kunde växa organisatoriskt genom utnyttjandet av betrodda distributörer (Cheviron 2021, s. 7). FBI tog också tillfället i akt efter nedstängningen av Phantom Secure och utnyttjade det tomrum som uppstod i utbudet av krypterade kommunikationstjänster (Cheviron 2021, s. 6). Ur insikten att de kriminella användarna snabbt flyttade till andra plattformar för krypterad kommunikation, såsom Sky Global och EncroChat (The Justice Department 2021), förutsåg FBI att användare också skulle strömma till ANOM.

Med utgångspunkt i att huvudsyftet med reflexiv kontroll är att lokalisera filtrets svagaste länk hos sin motståndare för att sedan kunna utnyttja den för sina egna syften (Thomas 2004, s. 241), går att påstå att FBI genom studier av fiendens filter utnyttjade åtminstone två typer av sårbarheter. Det handlar dels om kriminellas förtroende för varandra, dels de kriminellas desperata behov av en ny krypterad kommunikationsplattform vid tre olika tillfällen - nedstängningen av Phantom Secure, EncroChat och Sky Global.

Ett andra exempel på vilka aspekter av reflexiv kontroll som använts i Operation Trojan Shield kan därför sägas vara brottsbekämpande myndigheters konst att förutsäga de kriminellas reaktioner. En sådan konst kräver djup förståelse av motståndaren och dess tankesätt, strategier och vanor. I utredningen av Phantom Secure erhölls en stor mängd

kunskap om krypterad kommunikation och kriminellas användning av sådana plattformar, och i distributionen av ANOM utnyttjades sårbarheter i form av kriminellas desperation av krypterad kommunikation samt förtroende för varandra. Detta resulterade i att FBI hade den högre graden av reflexiv kontroll och således kunde förmå de kriminella att inte bara börja använda, utan också kraftigt öka efterfrågan av, ANOM.

Konsten att förutsäga reaktioner kan möjligtvis även omfattas av att distributörer tog sig an uppgiften att sprida ANOM-enheter på grund av de stora vinsterna i verksamheten, samt att CHS:en delade med sig av sin nyutvecklade krypterade kommunikationstjänst i utbyte mot pengar och reducerat straff (Cheviron 2021, s. 8). Huruvida detta var förutsägelser i högre grad än förhoppningar är dock svårt att konstatera. Att det varit avgörande för genomförandet av Operation Trojan Shield är däremot ett faktum.

7.2.3 Komovs tekniker

Med utgångspunkt i att krypterade kommunikationstjänster är högt efterfrågade i kriminella sammanhang (Cheviron 2021, s. 5) kan dessa bedömas vara viktiga platser ur kriminellas perspektiv. Att brottsbekämpande myndigheter avsiktligt och strategiskt stängde ner krypterade kommunikationsplattformar som Phantom Secure, EncroChat och Sky Global (Europol 2021a) kan således tolkas som användandet av distraktion. Med distraktion menas enligt Komov skapandet av ett verkligt eller falskt hot mot fienders viktiga platser (Thomas 2004, s. 248).

Nedstängningen ledde dessutom till att de kriminella istället strömmade till ANOM-enheterna i den desperata jakten på en ny plattform för krypterad kommunikation (Cheviron 2021, s. 11). Detta kan beskrivas som att tvinga fienden att omfördela styrkor till en hotad region, samt att tvinga fienden att vidta åtgärder som missgynnar sig själva, vilket Komov hänvisar till med begreppen vilseledning respektive provokation (Thomas 2004, ss. 248-249). Att ANOM var en hotad region, och att användandet av den missgynnade de kriminella, blev inte känt förrän efter avslöjandet och det var information de brottsbekämpande myndigheterna således undanhöll.

Vidare har Operation Trojan Shield beskrivits krossa allt förtroende för krypterad kommunikation bland kriminella (The Justice Department 2021), ett uttryck i vilket det går att urskilja förhoppningar om att skapa en uppfattning om de brottsbekämpande

myndigheterna som överlägsna. Det går således att koppla till tekniken avskräckning, som innebär att skapa en uppfattning om en överlägsen styrka (Thomas 2004, s. 248). Detta kan möjligtvis även inkludera tekniken alternativa förslag, vilket är en teknik för reflexiv kontroll genom att erbjuda information som påverkar fienden bland annat moraliskt och ideologiskt (Thomas 2004, s. 249). Om kriminella inte längre ser någon nytta med sin kriminella verksamhet, eller upprepade gånger blir stoppade av brottsbekämpande myndigheter, skulle det möjligtvis kunna leda till en förändring i moralen och ideologin att begå brott. Avslöjandet av Operation Trojan Shield inkluderade också avslöjandet att en CHS gått med på att bedra sina allierade, vilket kan tänkas omfatta information som misskrediterar ledningen och det som Komov benämner som påtryckningar (Thomas 2004, s. 249). Ledningen är i det fallet högt uppsatta kriminella, och kan vara en del i att utnyttja de kriminellas sårbarhet i form av högt förtroende för varandra.

Utifrån ovan analys av vilka tekniker som går att koppla till Operation Trojan Shield, har ingen koppling hittats till teknikerna informationsmättnad, paralysering, uttröttning, avledning, pacificering eller överbelastning. Detta är således militära tekniker som inte gestaltas i brottsbekämpning, åtminstone i detta fall. Ovan analys är också ett exempel på Kamphius (Hosaka 2019, s. 332) påstående att många element av reflexiv kontroll kan kopplas samman och att vissa element naturligt följer implementeringen av andra element. Som tidigare nämnt har Komov inte resonerat kring huruvida varje element kan användas individuellt eller om flera element kan kombineras med varandra (Hosaka 2019, s. 332).

7.2.4 Chausovs principer

Vad gäller vilka av Chausovs principer för reflexiv kontroll förs följande resonemang. Baserat på att alla Komovs tekniker för reflexiv kontroll inte kan återfinnas i Operation Trojan Shield kan det inte hävdas att operationen omfattar alla typer av reflexiv kontroll, vilket är den första principen som Chausov lyfter (Thomas 2004, s. 249). Det går dock att mena på att processen i Operation Trojan Shield bygger på en bild av sin motståndares kapacitet och potential, överensstämmer mellan mål, uppdrag, plats, tid och metoder för den reflexiva kontrollen samt modellerar förutsägelser för motståndarens åtgärder.

Det som tidigare konstaterats - att brottsbekämpande myndigheter kunnat förutsäga kriminellas reaktioner genom djup förståelse av motståndaren och utnyttjande av sårbarheter, ligger till grund för att hävda att processen i Operation Trojan Shield bygger på en bild av sin

motståndares kapacitet och potential samt modellerar förutsägelser för motståndarens åtgärder. Det faktum att rätt tillfälle utnyttjats ligger till grund för att processen i operationen slutligen bygger på överensstämmelse mellan mål, uppdrag, plats och tid.

7.2.5 Lyckad reflexiv kontroll

Att den reflexiva kontrollen i Operation Trojan Shield varit framgångsrik kan konstateras baserat på flertalet faktorer. Inledningsvis hade det vid avslöjandet av operationen använts 11 800 ANOM-enheter (Cheviron 2021, s. 10) från över 300 kriminella organisationer i fler än 100 olika länder (Europol 2021a), vilket visar på utsträckningen. För det andra kunde FBI, Europol och DEA i 18 månaders tid utnyttja underrättelser i realtid från 27 miljoner meddelanden som erhållits och granskats från ANOM (Europol 2021b) och inte bara arrestera kriminella efter avslöjandet utan också störa kriminell verksamhet medan plattformen fortfarande var aktiv (Europol 2021a). För det tredje innefattade operationen flertalet viktiga beslag (Europol 2021a). Målet med ANOM, att rikta in sig på global organiserad brottslighet, narkotikahandel och penningtvätt (Europol 2021a), kan således sägas ha uppfyllts.

7.2.6 Ett långsiktigt brottsförebyggande perspektiv

Operation Trojan Shields resultat har beskrivits som exceptionell framgång mot den allvarliga och organiserade brottsligheten (Europol 2021b). Den kunskap som erhållits ger en betydelsefull insikt i kriminella kretsar och den berikade underrättelsebilden förväntas stödja det fortsatta brottsförebyggande och brottsbekämpande arbetet (ibid.). Operationen har dessutom skakat om förtroendet för krypterad kommunikation bland kriminella (Cheviron 2021, s. 11).

Målet med ANOM var som tidigare nämnt att rikta in sig på global organiserad brottslighet, narkotikahandel och penningtvätt (Europol 2021a). En kortsiktig strategi för att uppnå den typ av mål hade troligtvis kunnat åstadkommas utan Operation Trojan Shield. Genom operationen kan det snarare hävdas att långsiktiga fördelar uppnåtts. Dessa går att hitta i lärdomarna av Operation Trojan Shield, vilka handlar om erhållen kunskap om krypterad kommunikation i kriminellt syfte, insikten att brottsbekämpande myndigheter behöver utnyttja teknisk infrastruktur för att verka starkare och mer störande samt vikten av internationellt samarbete bland brottsbekämpande organ (Europol 2021b).

Från detta går att urskilja en strävan efter att skapa bestående förändringar i form av påverkan de kriminellas trygghet på lång sikt. Utövandet av den reflexiva kontrollen kan således ha verkat bestående, eller åtminstone är förhoppningen sådan. En sådan vidareutveckling av konceptet reflexiv kontroll kan tänkas vara en form av konstruktiv reflexiv kontroll, där fokus ligger på att inte bara manipulera en motståndares beslut utan också på att forma deras långsiktiga strategier på ett sätt som gynnar den som utövar kontrollen.

Huruvida denna åtgärd i ett brottsförebyggande långsiktigt perspektiv är till fördel eller nackdel för brottsbekämpande myndigheter återstår att se. Som även tidigare analyserats kan brottsbekämpande åtgärder som Operation Trojan Shield leda till att kriminella inte längre ser någon möjlighet eller vinst i organiserad brottslighet, likväl som att den ökade övervakningen kan leda till att de kriminella möjligtvis utvecklar nya strategier för att undvika upptäckt. Vad som med säkerhet kan sägas är dock att användningen av reflexiv kontroll i Operation Trojan Shield bidragit till att under en viss tid identifiera och neutralisera hot från kriminella nätverk och organiserad brottslighet, och på så sätt skakat om kriminellas förtroende för krypterade kommunikationsverktyg.

7.2.7 Sammanfattning

De tekniker av reflexiv kontroll i Operation Trojan Shield som genom ovan analys har urskiljts är manipulation av information, konsten att förutsäga reaktioner, distraktion, vilseledning, provokation samt möjligen avskräckning, alternativa förslag samt påtryckningar. Av Chausovs principer går att hitta exempel på att processen i Operation Trojan Shield bygger på en bild av sin motståndares kapacitet och potential, överensstämmer mellan mål, uppdrag, plats tid och metoder för den reflexiva kontrollen samt modellerar förutsägelser för motståndarens åtgärder. Användandet av reflexiv kontroll går bland annat hitta i att ANOM marknadsfördes som en plattform för krypterad kommunikation, när brottsbekämpande myndigheter i själva verket kunde granska kommunikationen i realtid. Det går också att hitta i sättet på vilket FBI erhöll kunskap om kriminell verksamhet och senare utnyttjade detta, inte minst genom att utnyttja ett tillfälle när de kriminella var extra sårbara.

Operation Trojan Shields stora framgångar kan tala för en lyckad reflexiv kontroll, och ur lärdomarna kan anas en strävan efter att skapa bestående förändringar i att påverka kriminellas trygghet på lång sikt.

8. Slutsatser

Slutsatserna i detta avsnitt avser att besvara uppsatsens frågeställning: *Hur kombinerar Operation Trojan Shield stingoperationers metoder med principerna för reflexiv kontroll?* Från föregående analys går att dra följande slutsatser.

En första slutsats är att Operation Trojan Shield är en stingoperation, eftersom flertalet karaktäristiska drag av en stingoperation återfinns i syftet med och tillvägagångssättet för OTS. Den samtida och sofistikerade utformningen av OTS utmanar traditionell konventionell syn på stingoperationer, vilket gör den unik.

En andra slutsats är att militära användningsområden för reflexiv kontroll återfinns i en samtida omtolkning och realisering av brottsbekämpning. De brottsbekämpande myndigheterna bakom OTS hade den högre graden av reflexiv kontroll och operationen lyckades således tack vare att de kriminella inte hade lika hög grad av reflexiv kontroll. En enkelbiljett till FBI:s fälla.

En tredje slutsats är att OTS kan påstås vara lyckad i den mening att den resulterat i bland annat bevismaterial, arresteringar världen över, förbättrad underrättelsebild samt ökad kunskap om transnationell kriminalitet såväl som krypterade kommunikationstjänster. På så sätt har operationen uppfyllt sitt mål - att rikta in sig på global organiserad brottslighet, narkotikahandel och penningtvätt. Ur ett långsiktigt brottsförebyggande perspektiv kan den reflexiva kontrollen följaktligen benämnas som konstruktiv.

En fjärde och avslutande slutsats är att analysen visar att de många likheterna mellan stingoperationers metoder och principer för reflexiv kontroll bekräftar att stingoperationer, åtminstone i OTS, förverkligar reflexiv kontroll i praktiken. Detta genom att effektivt och strategiskt kombinera vilseledning och manipulation för att vid rätt tillfälle angripa global organiserad brottslighet. Reflexiv kontroll fungerar således som en nyckelkomponent i stingoperationer för att påverka kriminellas beslutsprocess.

Källförteckning

Cheviron, Nicholas, 2021. United States District Court. https://www.justice.gov/usao-sdca/press-release/file/1402426/dl?inline [hämtad 2024-08-02]

Chotikul, Diane (1986). "The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspectives: A Preliminary Study." *Naval Postgraduate School. Monterey: California.*

Esaiasson, Peter. m.fl. 2017. *Metodpraktikan: Konsten att studera samhälle, individ och marknad.* Femte upplagan red. Stockholm: Norstedts Juridik AB.

European Commission, u.å. *Mutual legal assistance and extradition* [Elektronisk]. https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en [hämtad 2024-08-17]

Europol a, 2021. *800 criminals arrested in biggest ever law enforcement operation against encrypted communication.* [Elektronisk] https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication [hämtad 2024-06-30]

Europol b, 2021. *Press conference – Operation Trojan Shield/OTF Greenlight* [video]. https://www.youtube.com/watch?v=e443mE8l-_0 [hämtad 2024-07-10]

Europol, 2022. "The European Union Agency for Law Enforcement Cooperation". https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20in%20Brief.pdf [hämtad 2024-08-10]

Gerring, John. 2004. "What Is a Case Study and What Is It Good for?" *The American political science review.* Vol. 98, ss. 341–354.

Göteborgs tingsrätt dom 2021-12-06 i mål nr B 9644-21

Göteborgs tingsrätt dom 2021-12-23 i mål nr B 9642-21

Hasani, Fejzullah 2019. "Covert and technical surveillance measures and investigation". *Acta Universitatis Danubius Juridica*, Vol. 15. No.3. ss. 41-53.

Hosaka, Sanshiro, 2019. "Putin the 'Peacemaker'? - Russian Reflexive Control During the 2014 August Invasion of Ukraine", *Journal of Slavic Military Studies,* Vol. 32, No. 3, ss. 324-346.

Langworthy, Robert H. 1989. "Do stings control crime? An evaluation of a police fencing operation. Justice Quarterly." Vol.6, No.1. ss.27-46.

Newman, Graeme .R. & Socia, Kelly. (2007). Sting Operations. Problem-Oriented Guides for Police Response Guides Series No. 6.

Manijikian, Mary, 2013. "Positivism, post-positivism and intelligence analysis". *International Journal of Intelligence and Counterintelligence*, vol. 26, nr. 3, ss. 563 - 583.

Panzarella, Robert, & Funk, Joanna, 1987. "Police Deception Tactics and Public Consent in the United States and Great Britain." *Criminal Justice Policy Review,* Vol. 2. ss.133-143.

The Justice Department, 2021. *FBI's Encrypted Phone Platform Infiltrated Criminal Syndicates; Result is Massive Worldwide Takedown* [video]. https://www.youtube.com/watch?v=S89O0nis_ss [hämtad 2024-07-26]

Thomas, Timothy L, 2004. "Russia's Reflexive Control Theory and the Military", *Journal of Slavic Military Studies*, Vol. 17, No. 2, ss. 237-256.

United States Department of Justice, 2022. "Mutual legal assistance treaties of the United States".https://www.justice.gov/d9/pages/attachments/2022/05/04/mutual-legal-assista

nce-treaties-of-the-united-states.pdf [hämtad 2024-08-17]

Åklagarmyndigheten, 2023. *Lagen om preventiv avlyssning utvidgas.* [Elektronisk] https://www.aklagare.se/nyheter-press/aktuellt-pa-aklagarmyndigheten/lagen-om-preventiv-avlyssning-utvidgas/ [hämtad 2024-07-12]