Lunds universitet
Statsvetenskapliga institutionen

UNDA23
VT 2024
Handledare: Tony Ingesson

Att upptäcka ryska illegalister

- Utmaningar och konsekvenser för ett kontraspionage

Johan Dahlström
Björn Wallinius

Abstract

Illegals have been a tool of Russia's intelligence service since 1922. Directorate S is one of Russia's intelligence service's most secret parts, and responsible for the illegals program. Few have insight into the activities and little are known about it. In order for a state's counterintelligence to be able to deal with a security threat, the security threat must first be identified, and this is where illegals pose a challenge. Given the changed security policy situation, with war in Europe and a broader area of conflict between Russia and the West, there is an increased relevance and topicality in studying the factors for Russia's use of illegalists based on counterespionage and detection. This study aims to investigate what consequences Russia's use of illegals can have for a state's counterintelligence regarding detection of illegals. Three different cases between 1952 – 2010 are analyzed, from the first indication of anomaly, to the discovery and up to the end of the investigation.

KEYWORDS: illegals, counterintelligence, event of concern

Antal ord: 9963

Innehållsförteckning

1 Inledning

Ryssland har använt sig av illegalister för underrättelseinhämtning sedan början av 1920-talets Sovjetunionen[1]. Under denna period var diplomatiska beskickningar i andra länder begränsade och det krävdes andra metoder för att inhämta underrättelser. Således är verksamheten ett arv från en tid med avsaknad av konsulär representation. Illegalist kan härledas till det ryska ordet för illegal (“нелегал”) och beskriver en person som befinner sig illegalt i ett annat land[2]. Illegalister är således en typisk rysk företeelse inom underrättelsetjänst och sträcker sig över 100 år tillbaka i tiden.

Den 27 juni 2010 greps tio individer på olika platser i USA misstänkta för att ha etablerat sig och verkat djupt inne i det amerikanska samhället, åtta av dem under falsk identitet och utan officiell anknytning till Ryssland.[3] De tio gripna hade under lång tid levt sina liv i USA, flera av dem som amerikanska medborgare där deras egna barn i vissa fall saknat kännedom om deras bakgrund.[4] När FBI presenterade den tio år långa operationen som Operation Ghost stories stod det klart att fallen gav en unik inblick i ett nutida avslöjande av rysk illegalistverksamhet. Fallet visar att illegalistverksamhet fortsatt används av rysk underrättelseverksamhet och är således något som kan anses äga såväl en historisk som nutida relevans och aktualitet för såväl forskningen som för en stats kontraspionage.

I studien undersöks vilka metoder för upptäckt ett kontraspionage historiskt har använt sig av i upptäckten av illegalister. Genom att analysera tidigare fall och samtidigt studera aktuell forskning rörande illegalistverksamhet och dess karaktäristika visar studien på en del av de utmaningar som illegalistverksamhet innebär för ett kontraspionage.

---

[1] Kevin Riehle, Wilson Center, 2023, *The History and Continuing Relevance of Soviet Bloc Illegal Intelligence Operatives*
https://www.wilsoncenter.org/blog-post/history-and-continuing-relevance-soviet-bloc-illegal-intelligence-operatives [hämtad 2024-05-22]

[2] Riehle, Wilson Center, *The History and Continuing Relevance of Soviet Bloc Illegal Intelligence Operatives*

[3] James M. Olson. *To catch a spy, The art of counterintelligence*, (USA: Georgetown university press, 2021), s. 24-25.

[4] Gordon Corera, *Russians among us – Sleeper Cells and the Hunt for Putin's Agents*, London, (UK: William Collins, 2020), s. 62.

1.1 Problemformulering

En illegalist är en särskilt utbildad och tränad underrättelseofficer vars uppdrag är att, på främmande stats territorium, etablera sig som inhemsk medborgare och under lång tid och utan några som helst kopplingar till ursprungslandet instrueras av och rapportera till ursprungslandets underrättelsetjänst.[5] Illegalister använder sig traditionellt sett av särskilda metoder för att undvika upptäckt.[6] Aktiva illegalister som uttryck för en främmande stats underrättelseverksamhet kan därför, likt andra former av spionage, utgöra ett säkerhetshot för den berörda staten.

Med ett förändrat säkerhetspolitiskt omvärldsläge med krig i Europa och en bredare konfliktyta mellan Ryssland och väst[7] finns en relevans och aktualitet i att studera de för Ryssland aktuella metoderna för underrättelseinhämtning och påverkansoperationer. Särskilt då det finns tendenser att Ryssland, i takt med tilltagande internationell isolering och minskad konsulär representation, i större utsträckning kan komma att använda sig av såväl nya som gamla beprövade metoder.[8]

För att kunna agera mot potentiella säkerhetshot gäller i allmänhet att de först måste definieras och registreras, alltså identifieras eller upptäckas.[9] Illegalistverksamhet som sofistikerad inhämtningsmetod[10] med falska identiteter, rigorösa legender och en långsiktig och trovärdig etablering i samhället[11] kan därmed antas försvåra kontraspionagets arbete.[12]

---

[5] Kevin P. Riehle. Russia's intelligence illegals program: an enduring asset, *Intelligence and National Security,* 35:3, 2020, s. 385.

[6] Riehle, 2020, s. 394.

[7] Säkerhetspolisen 2023/2024. Lägesbild Kontraspionage – Sänkt tröskel hos främmande makt. *SÄPO*. https://sakerhetspolisen.se/om-sakerhetspolisen/publikationer/sakerhetspolisens-arsberattelse/sakerhetspolisen-2023-2024/verksamhetens-lagesbilder/lagesbild-kontraspionage.html (Hämtad 2024-26)

[8] ibid.

[9] Hank Prunckun. Counterintelligence – Theory and practice, uppl. 2, London, UK: Rowman & Littlefield, 2019, s. 47.

[10] Riehle, 2020, s. 390.

[11] ibid., s. 385.

[12] Prunckun, 2019, s. 48.

1.2 Syfte och frågeställning

1.2.1 Syfte

Som en del av en stats säkerhetsskydds- och kontraspionagearbete är det av vikt för verksamheten att kunna upptäcka de säkerhetshot den är ålagd att hantera. Studien avser undersöka vilka konsekvenser Rysslands användande av illegalister kan få för en stats kontraspionage avseende upptäckt av illegalistverksamhet.

1.2.2 Frågeställning

Hur påverkar Rysslands användande av illegalister förutsättningarna för ett kontraspionage att upptäcka illegalistverksamhet?

2 Bakgrund

2.1 Begreppsöversikt

2.1.1 Illegalister, underrättelseofficerare och agenter

För underrättelseinhämtning i form av human intelligence eller HUMINT, görs det i forskningen skillnad på underrättelseofficerare med offentlig täckmantel respektive de utan offentlig täckmantel.[13] En vanlig form av officiell täckmantel är utsända underrättelseofficerare arbetande som ambassadpersonal, som därmed innehar diplomatisk immunitet. Den andra formen, underrättelseofficerare utan officiell täckmantel, saknar officiell koppling till hemlandets statsapparat och agerar utan rättsligt skydd.[14] I båda dessa fall är underrättelseofficerarens identitet och ursprungliga nationalitet inte dold eller falsk.[15]

En illegalist definieras traditionellt som en underrättelseofficerare som, under falsk identitet, verkar utomlands utan någon som helst koppling till varken Ryssland eller några av dess organisationer eller institutioner.[16] Därmed saknar en illegalist, i likhet med en underrättelseofficer med inofficiell täckmantel, diplomatiskt straffrättsligt skydd. Den nya identiteten kompletteras med en omfattande alternativ livshistoria, en legend.[17]

Den individ som av underrättelseofficerare rekryteras för att inhämta information å underrättelseofficerarens, och därmed den bakomliggande organisationens vägnar, benämns ofta som agent. Agenten hanteras av den rekryterande underrättelseofficeraren eller av annan individ och benämns hanterare.[18]

2.1.2 Kontraspionage

Kontraspionagets uppdrag liknar den ordinarie underrättelseverksamhetens med skillnaden att den förra har en motståndares underrättelseverksamhet som

[13] Prunckun, 2019, s. 20-21.
[14] ibid.
[15] Riehle, 2020, s. 385.
[16] ibid.
[17] Edward Lucas. The Spycraft Revolution : Changes in technology, politics, and business are all transforming espionage, *Foreign Policy.* Issue 232, 2019, s. 23.
[18] Prunckun, 2019, s. 21.

målobjekt.[19] Hank Prunckun menar att counterintelligence kan beskrivas både som den aktivitet som utförs men också den producerade underrättelseprodukten.[20] I en svensk kontext skulle counterintelligence kunna anses innefatta såväl säkerhetsskyddstjänsten som kontraspionaget.[21] Fortsättningsvis i studien ämnar vi företrädesvis använda oss av begreppet kontraspionage som ett gemensamt begrepp istället för att använda både säkerhetsskyddstjänst och kontraspionage.

2.2 Tidigare forskning

2.2.1 Kontraspionage och upptäckt

Kontraspionage som beskrivet ovan är ingen enhetlig definition om vilken det råder en vetenskaplig konsensus. I artikeln "Towards a theory of CI – What are we talking about when we talk about counterintelligence?" sammanställer John Ehrman ett flertal förslag på hur begreppet ska definieras. De i artikeln redogjorda förslagen representeras av bland annat USAs regering och före detta KGB officeren Vasilij Mitrokhin. Förslagen på definition skiljer sig åt men har, trots olika ursprung, liknande drag.[22] Ehrman själv föreslår följande definition: "Counterintelligence is the study of the organization and behavior of the intelligence services of foreign states and entities, and the application of the resulting knowledge"[23]. Blake W. Mobley definierar i sin forskning counterintelligence som den process som utgörs av en grupps aktiviteter, analyser och beslutsfattande som genomförs i syfte att skydda den egna verksamhetens handlingar, personal och planer.[24]

Hank Prunckun beskriver counterintelligence i termer av defensivt respektive offensivt arbete, där det defensiva arbetet i huvudsak avskräcker och upptäcker säkerhetshot. Prunckun menar att upptäckten av en händelse, eller "event of concern" som han kallar det, är en central utgångspunkt för arbetet inom counterintelligence.[25] Det offensiva arbetet inkluderar också upptäckt men framförallt vilseledning och neutralisering av säkerhetshot.[26] Ehrman å sin sida

[19] Prunckun, 2019, s. 25.
[20] ibid.
[21] Säkerhetspolisen. Säkerhetspolisens uppdrag. *SÄPO*. https://sakerhetspolisen.se/om-sakerhetspolisen/sakerhetspolisens-uppdrag.html (Hämtad 2024-05-26)
[22] John Ehrman. Toward a Theory of CI – What are we talking about when we talk about counter-intelligence? *Studies in Intelligence* Vol. 53 No. 2 (2009), s. 7.
[23] Ehrman, 2009, s. 6.
[24] Blake W. Mobley. *Terrorism and counterintelligence : how terrorist groups elude detection.* (New York: Columbia University Press, 2012), s. 8.
[25] Prunckun, 2019, s. 47.
[26] ibid., s. 25.

menar att gränsen mellan offensivt och defensivt arbete är flytande och att även en offensiv åtgärd som penetration av en motståndares säkerhetstjänst kan ses som defensiv om den exempelvis syftar till att avslöja en spion inom den egna verksamheten.[27]

När Ehrman definierar tillämpad counterintelligence menar han att det finns tre olika typer av operationer som kan användas för att samla in information om en motståndares underrättelseverksamhet.[28] Det kan ske genom penetrering av motståndarens underrättelseverksamhet, genom dubbeloperationer med hjälp av dubbelagenter samt via ett systematiskt utredningsarbete.[29]

2.2.2 Försvårande av upptäckt

För att kunna bedriva sin illegalistverksamhet är det av naturliga skäl avgörande för illegalister huruvida de kan förbli dolda. Inom forskningen är det i synnerhet två begrepp som beskriver hur aktörer agerar för att missrikta eller vilseleda en motståndares perception om den egna verksamheten eller dess aktiviteter. Begreppen från engelskans denial respektive deception kan översättas till att förneka respektive vilseleda. James J. Wirtz menar i sin forskning att förneka motståndaren bygger på sekretess och hemlighållande i form av att dölja observerbara faktorer kopplade till en operations planering, förberedelser eller genomförande.[30] Blake W. Mobley resonerar på ett liknande sätt men beskriver förnekandet av information i två steg: ett grundläggande förnekande och ett anpassat förnekande.[31] Det grundläggande förnekandet utgörs av ett mer allmänt säkerhetsskyddsarbete, ibland sett som ett defensivt arbete där allmänna åtgärder vidtas.[32] Det anpassade förnekandet, menar Mobley, utgår istället från underrättelseinformation och kunskap om motståndarens beteende och resurser där den egna verksamheten skyddas genom anpassning efter motståndarens metoder.[33]

Det andra begreppet, vilseledning, beskriver Wirtz kan ta sig väldigt olika uttryck men innebär att vilseledande information presenteras eller åtgärder genomförs vilka har till syfte att vilseleda motståndaren, till exempel genom falska dokument.[34] Mobley beskriver i sin forskning vilseledning som hemlig manipulation

[27] Ehrman, 2009, s. 16.
[28] ibid., s. 15.
[29] ibid..
[30] James J. Wirtz. Hiding in Plain Sight: Denial, Deception, and the Non-State Actor, *The SAIS Review,* Vol. 24, No. 3, 2008, 55-63, s. 56.
[31] Mobley, 2012, s. 11.
[32] ibid., s. 8.
[33] ibid., s. 9.
[34] Wirtz, 2008, s. 57.

och menar att denna är den mest sofistikerade metoden vilken bygger på en aktörs grundläggande och anpassade förnekande, med andra ord används kunskap om motståndarens motåtgärder för att penetrera densamma.[35]

2.2.3 Illegalister och underrättelseverksamhet

Inom forskningen om ryska illegalister får Kevin P. Riehle anses vara framstående inom ett annars begränsat forskningsfält. I sin artikel "Russia's intelligence illegals program: an enduring asset" beskriver han illegalistverksamhetens historiska betydelse för Ryssland och konstaterar att Ryssland har fortsatt att använda sig av illegalister som verktyg för underrättelseverksamheten trots både historiska motgångar och framgångar. Riehle ställer sig frågan hur Rysslands illegalistprogram ser ut idag och drar slutsatserna att programmet är fortsatt effektivt och att använda illegalister som metod äger en fortsatt relevans Detta trots den digitala och teknologiska utvecklingen med exempelvis biometri och ansiktsigenkänning.[36]

En grundläggande funktion för ett illegalistprogram är att verka som en plattform för fortsatt inhämtning även under internationella kriser, exempelvis när diplomatiska förbindelser bryts.[37] [38] Riehle hänvisar i sin artikel till uttalanden från bland andra Vladimir Putin och andra representanter för den ryska staten och underrättelsetjänsten där de med heroiska beskrivningar hedrar forna och nutida illegalister för deras uppoffringar och insatser.[39] I sin forskning konstaterar Riehle att illegalisterna dock inte enbart finns till som en långsiktig strategisk försäkring vid försämrade internationella relationer. Han menar att de även kan utgöra en aktiv roll rörande informationsinhämtning och olika typer av påverkansförsök. En annan central uppgift de har är att identifiera och bedöma individer utifrån deras potential och förutsättning att rekryteras som agenter.[40] Riehles redogörelse för illegalisternas verksamhet innebär att illegalisterna utför inhämtning i enlighet med den klassiska definitionen av underrättelseverksamhet men även en typ av hemliga operationer via påverkansförsök samt en uthållig förberedelse till hemliga operationer via en vilande beredskap.

Till skillnad mot Riehle argumenterar den tidigare chefen för CIA, James M. Olson, för illegalisternas begränsade effekt och menar att det inte bevisats att

[35] Mobley, 2012, s. 10.
[36] Riehle, 2020, s. 396.
[37] ibid., s. 395.
[38] ibid., s. 387.
[39] ibid., s. 388.
[40] ibid., s. 396.

illegalisterna har åstadkommit något av värde då han menar att syftet med deras infiltration och etablering i det amerikanska samhället saknar förklaring. Han menar att verksamheten saknar rationalitet och snarare beror på Vladimir Putins besatthet av USA än som uttryck för effektiv underrättelseverksamhet.[41] Till skillnad från exempelvis Riehle, som får anses representera den vetenskapliga delen av ämnet underrättelsevetenskap, representerar James M. Olson den andra delen, professionen.

2.3 Sammanfattning bakgrund och tidigare forskning

Illegalister används för underrättelseverksamhet inom Rysslands underrättelsetjänst och arbetar under falsk identitet som en underrättelseofficerare, utan diplomatisk täckmantel. Uppgiften att upptäcka illegalister karaktäriseras av illegalisternas sofistikerade metoder som används i syfte att förneka motståndaren information och därmed försvåra upptäckt. Upptäckten kan ske genom tre olika typer av kontraspionageoperationer, penetrering av motståndarens underrättelseverksamhet, dubbeloperationer med hjälp av dubbelagenter samt via ett systematiskt utredningsarbete[42]. Arbetet kan beskrivas som defensivt eller offensivt där det defensiva arbetet traditionellt avskräcker och upptäcker säkerhetshot[43]. Det offensiva arbetet, kontraspionaget, inkluderar också upptäckt men även vilseledning och neutralisering av säkerhetshot.

[41] Olson, 2021, s. 25-26.
[42] Prunckun, 2019, s. 47.
[43] Ehrman, 2009, s. 15.

3 Teori

3.1 Upptäckt – Theory of Counterintelligence

Hank Prunckun beskriver i sin *Theory of counterintelligence* fem steg med hjälp av vilka processen i kontraspionagets arbete kan studeras. Utifrån teorin kan således processen av upptäckt delas upp och studeras i fem olika skeenden.

I sin definition av begreppet upptäckt menar Prunckun att det handlar om att registrera en händelse där händelsen utgörs av ett intrång – eller försök till ett intrång – med syftet att tillgodogöra sig konfidentiell information.[44] Prunckun beskriver att just upptäckten av ett säkerhetshot kan hänföras till såväl de defensiva som de offensiva delarna av kontraspionagets arbete.[45] Detta beror på att ett säkerhetshot dels kan upptäckas i den defensiva verksamheten, exempelvis ett intrång i ett system eller en anomali i någon annan typ av uppföljande säkerhetsarbete.[46] Att upptäckandet delvis också ska ses ur ett offensivt perspektiv menar Prunckun beror bland annat på att det finns ett aktivt, offensivt arbete i att fortsätta sökandet efter den initiala upptäckten.[47] Därmed spelar begreppet över gränserna mellan defensivt och offensivt arbete och sammanbinder dem. Prunckuns teori tar i första hand sikte på information som mål för en angripares underrättelseverksamhet. Det teoretiska ramverket kring upptäckt som en del av Prunckuns teori, vilar på fem premisser[48].

1. Identifiering av händelsen
2. Identifiera inblandade individ-/er.
3. Identifiera inblandade individ-/ers organisatoriska tillhörighet
4. Identifiera inblandade individ-/ers nuvarande position
5. Säkra information som bekräftar att identifierade individ-/er varit delaktiga i händelsen.

[44] Prunckun, 2019, s. 47.
[45] ibid., s. 43.
[46] ibid., s. 47.
[47] ibid., s. 51.
[48] ibid., s. 47.

3.1.1 Identifiering av händelsen

Kärnan i det teoretiska ramverket för upptäckt är själva händelsen som ska upptäckas. Prunckun kallar denna händelse "the event of concern", vilken kan förklaras som en potentiellt säkerhetshotande händelse. En händelse av sådan art kan utgöras av en mängd olika typer av händelser i olika kontexter. Det handlar om att identifiera händelsen, vilket kan ske genom exempelvis tekniska hjälpmedel, varningssystem eller mänskliga observationer.[49] För att kunna identifiera en potentiellt säkerhetshotande händelse i form av någon typ av agerande ligger det också i sakens natur att veta vad som är säkerhetshotande och skyddsvärt.

3.1.2 Identifiera inblandade individ-/er

För att möjliggöra en fullständig skadebedömning av en upptäckt händelse där konfidentiell information förlorats eller riskerar att förloras är det nödvändigt att identifiera den eller de individer som fått tillgång till informationen.[50]

3.1.3 Identifiera inblandade individ-/ers organisatoriska tillhörighet

Denna uppgift är starkt sammankopplad med att identifiera individen eller individerna i sig och grundar sig i underrättelseverksamhetens kärnverksamhet. Det vill säga att insamlad data och information sammanställs och analyseras till en underrättelseprodukt. Således finns vanligen en uppdragsgivare, tillika mottagare av informationen och det är denna som den organisatoriska tillhörigheten syftar på. Ensamagerande individer anses ovanligt, men även om de agerar ensamma är deras syfte och mål vanligen att vidareförmedla informationen till en organisation eller stat. För att kunna förstå skadeverkningar och utföra en korrekt skadebedömning är det viktigt att veta vem som är den slutliga mottagaren av underrättelse-informationen.[51]

[49] Prunckun, 2019, s. 47.
[50] ibid.
[51] ibid., 48.

3.1.4 Identifiera inblandade individ-/ers nuvarande position

Genom att, via namn eller signalement, veta vem eller vilka individer man letar efter ökar sannolikheten att finna dem.[52] Detta steg syftar således till att geografiskt lokalisera de inblandade individerna, i syfte att bedriva fortsatt verksamhet.

3.1.5 Säkra information som bekräftar att identifierade individ-/er varit delaktiga i händelsen.

Målet med en kontraspionageoperation av detta slag menar Prunckun är att få kunskap om vad som inträffat, vem som utfört det inträffade, var det har inträffat, när det inträffat, varför det inträffat och hur det har inträffat. Detta har likheter med forensiskt arbete och bevissäkring i exempelvis en förundersökning. Till skillnad mot förundersökningar i brottmål är inte alltid uppdraget för ett kontraspionage att väcka åtal, istället kan informationen även användas för att tjäna andra offensiva åtgärder såsom vilseledning eller annan påverkan.[53]

Avslutningsvis menar Prunckun med sin teori att en motståndares vilja och förmåga att bedriva inhämtning påverkas av effektiviteten hos den attackerade aktörens kontraspionage. Om motståndaren trots ett effektivt kontraspionage hos den attackerade aktören väljer att fortsätta med sina aktiviteter, kräver det att motståndaren blir mer sofistikerad i sina metoder alternativt accepterar större konsekvenser och färre fördelar.

3.2 Kontraspionageoperationer – Towards a theory of counterintelligence

John Ehrman definierar, i vad han beskriver som ett teoretiskt ramverk i arbetet mot en teori, tre typer av operationer som kan användas inom kontraspionage för att få information om en motståndares underrättelseverksamhet och dess underrättelseinhämtning. De tre typerna av operationer utgörs av, penetration, dubbelagenter samt ett systematiskt utredningsarbete[54] och används i studien för att analysera och jämföra upptäckt av illegalistverksamhet. De tre olika typerna av operationer definierar i analysen varje enskilt steg i den process som beskrivits

[52] Prunckun, 2019, s. 48.
[53] ibid.
[54] Ehrman, 2009, s. 15.

utifrån Prunckuns teori. Det vill säga vilken typ av operation användes för upptäckten i respektive steg i Prunckuns tidigare beskrivna process?

3.2.1 Penetration

En operation som bygger på penetration innebär att en individ, exempelvis en officer eller anställd inom en motståndares underrättelseverksamhet, är rekryterad och kan således ge tillgång till information direkt inifrån motståndarens verksamhet. Denna typ av operation är att anse som den mest värdefulla då källan kan ha direkt tillgång till värdefull information. Även individer med lägre rang eller längre ner i hierarkin kan ha tillgång till indirekt information som även med mindre detaljrikedom kan bidra till värdefull kunskap och information att arbeta vidare på.[55] Förenklat kan en penetration ses ur ett *inifrånperspektiv* där källan har mer eller mindre direkt tillgång till informationen.

3.2.2 Dubbelagenter

Ett annat sätt att genomföra en operation är försöka rekrytera en av motståndarens agenter eller genom en så kallad "dangle", där en agent från den ena sidan används som ett lockbete och erbjuder information i syfte att bli rekryterad som agent av motståndaren.[56] En sådan operation benämns på svenska som en dubbeloperation[57] och kan ge viss information om en motståndares underrättelseverksamhet. Nackdelen är att agenten i normalfallet endast har tillgång till sporadisk information från ett *utifrånperspektiv* då denne inte är i kärnan av verksamheten utan agerar på uppdrag av den. En annan nackdel är att båda alternativen kräver att agenten förses med tillräckligt värdefull information för att anses vara pålitlig och värdefull.[58] Generellt sett anses fördelarna hos denna typ av operationer inte väga upp mot de nyss nämnda nackdelarna och anses därmed vara mindre motiverade.[59]

[55] Ehrman, 2009, s. 15.
[56] Ehrman, 2009, s. 15-16.
[57] Nylander, Bengt och Lars Korsell. *Det som inte berättats: Säpo & kontraspionaget*, (Litauen: Medströms bokförlag, 2021), s. 99.
[58] Ehrman, 2009, s.16.
[59] Ehrman, 2009, s.16.

3.2.3 Systematiskt utredningsarbete

Det som närmast kan beskrivas som ett självinitierat riktat arbete är det som Ehrman i sitt ramverk beskriver som en operation som "works systematically in a particular location to identify a target service's officers and then, through access agents or physical and technical surveillance, to uncover their activities and contacts"[60]. En operation av denna karaktär anses väldigt resurskrävande och tidsödande då det dels handlar om att identifiera underrättelseofficerare för att möjliggöra kartläggning av dem, men också den eventuella rekryteringen och hanteringen av agenter. Resursåtgången tenderar dessutom att tillta i händelse av framgång i inhämtningen och Ehrman menar att denna typ av operationer är ovanliga.[61] Om en operation av detta slag blir framgångsrik avseende identifiering och kartläggning avseende underrättelseofficerare och deras kontakter innebär det dock stora fördelar i form av en realtidsuppföljning av motståndarens pågående aktiviteter och dess modus operandi. Det kan också ge andra möjligheter, exempelvis att använda sig av insamlad och analyserad information och använda den till att initiera tidigare nämnda operationer i form av mer offensiva metoder som dubbelagenter eller "dangles".

3.3 Sammanfattning teoretiskt ramverk

Två olika teoretiska ramverk redogörs för under teoriavsnittet. Det ena, Hank Prunckuns teori, beskriver upptäckten som en process i fem steg. Detta kan förenklat beskrivas som upptäckt av händelsen som sådan, individerna som utfört verksamheten, deras organisatoriska tillhörighet, deras nuvarande geografiska position samt en utredning i form av bevissäkring. Det andra teoretiska ramverket är den del av John Ehrmans forskning där han beskriver tre olika operationer med hjälp av vilka ett kontraspionage kan bedriva sitt arbete, oavsett om den benämns defensiv eller offensiv. De tre olika operationerna är användandet av penetration, dubbelagenter eller ett systematiskt utredningsarbete.

[60] Ehrman, 2009, s.16.
[61] ibid.

4 Metod

I denna studie avser vi undersöka vilka konsekvenser Rysslands användande av illegalister kan få för en stats kontraspionage avseende upptäckt av illegalistverksamhet. Detta kommer att studeras genom analys av fallstudier i tre fall där illegalister har varit en del av underrättelseinhämtningen. Akademiskt material inom ämnet underrättelsevetenskap samt facklitteratur specifikt inom ämnet illegalister har sedan använts i analysen av dessa tre fallstudier.

Den vetenskapsteoretiska grunden baseras i studien på kritisk realism som är en blandning av idén om att kunskap skapas genom att studera verkligheten men med inslag av konstruktivism.[62] Kritisk realism är en vetenskaplig utgångspunkt där avsikten är att utforska de delar som orsakar sociala händelser. Med andra ord är den vetenskapsteoretiska ingången att utgångspunkten är att det finns en observerbar verklighet som går att erhålla kunskap om men att den data vi använder för insamlandet ses ur ett kritiskt perspektiv då den är beroende av de teorier som används.[63] Inom statsvetenskap kan kritisk realism användas för att studera sociala kontexter skapade av människan.

4.1 Fallstudie som metod

Fallstudier kan generellt beskrivas som en metod för att besvara forskningsfrågor som *hur* och *varför*.[64] Fallstudier är studier som inte är iscensatta situationer eller skeenden som är speciellt framtagna för forskning. Fallet som studeras är vanligtvis någonting historiskt eller pågående. Christopher Lamont menar att själva definitionen av en fallstudie har en stark koppling till målet med en studie, där det kan finnas flera olika definitioner.[65] Lamont menar att fallstudier kan ses som en händelse med ett slut medan andra anser att fallstudien är en ingående studie av en specifik historisk händelse över tid, syftande att förstå andra liknande

[62]Kristina Boréus och Göran Bergström. *Textens mening och makt: metodbok i samhällsvetenskaplig text- och diskursanalys,* uppl. 4, (Lund: Studentlitteratur, 2021), s. 27.
[63] ibid., s. 27.
[64] Jan Teorell och Torsten Svensson. *Att fråga och att svara - Samhällsvetenskaplig metod,* (Slovenien: Liber, 2007), s. 27.
[65] Christopher Lamont. *Research Methods in International Relations*, uppl. 2. (United Kingdom: SAGE publications, 2022), s. 213.

händelser.[66] Den sistnämnda kan sedan användas för att utveckla nya generaliserbara förklaringsmodeller för andra händelser. Runa Patel och Bo Davidsson definierar fallstudier som en metod som används inom statsvetenskapen för att studera en avgränsad grupp eller grupper med avsikt att, utifrån ett helhetsperspektiv, förklara förändringar.[67] Johannes Lindvall definierar fallstudier som ”empiriska undersökningar av enskilda stater, kommuner, organisationer, politiska partier, val, revolutioner, individer eller andra enheter”.[68] Tommy Jensen och Johan Sandström anger att det som karakteriserar fallstudien är dess ambition att pröva samtida företeelser i dess kontext när gränserna mellan företeelser och kontext är otydliga.[69] Vidare anger Jensen och Sandström att fallstudien är att föredra när ”en företeelse är både komplex och beroende av sitt sammanhang”.[70] Vidare anger författarna att fallstudien är en studie av flerdimensionella händelser i ett för studien specifikt sammanhang.[71] Fallstudier kan därför användas som ett verktyg för att upptäcka kausalitet och dess komplexitet ur ett historiskt perspektiv.

Analysmetod för studiens inomfallsstudier har varit processpårning. Processpårning är en metod för inomfallsstudier där man fokuserar på hela processen från början till slut.[72] Processpårning valdes då metoden är ett verktyg för att analysera processer för att hitta orsaker till händelser.

4.2 Metoddiskussion

Fallstudier har kritiserats för att inte generera generaliserbara teorier. Detta medför att det finns ett antal centrala faktorer som man bör ta hänsyn till vid utformningen av en fallstudie för att undvika de mest uppenbara fallgroparna. Den första av dessa är att undvika studier med endast ett fall. Fallstudier har även stött på kritik från, i första hand, forskare inom positivism. Kritiken är riktad mot att fallstudier inte alltid syftar till att skapa generaliserbar kunskap för att besvara liknande forskningsfrågor.[73] Generaliserbarheten är begränsad till teoretiska påståenden och det saknas därför möjlighet att skapa allmängiltiga teoretiska modeller genom metoden och resultaten från fallstudier kan inte betraktas som fullkomliga. Jensen

[66] Lamont, 2022, s. 212.
[67] Runa Patel & Bo Davidson. *Forskningsmetodikens grunder: att planera, genomföra och rapportera en undersökning*, (Lund: Studentlitteratur, 1991), s.76.
[68] Johannes Lindvall. Fallstudiestrategier, *Statsvetenskaplig tidskrift*, Vol 109, No. 3, 2007, s. 207.
[69] Tommy Jensen & Johan Sandström. *Fallstudier*, uppl. 1, (Lund: Studentlitteratur, 2016), s. 42.
[70] ibid., s. 42.
[71] ibid., s. 42.
[72] Lamont, 2022, s. 212.
[73] ibid., s. 213.

och Sandström menar att det krävs en tydlig strategi för att genomföra fallstudien för att inte riskera att empiriskt färga forskningsresultaten utifrån den personliga uppfattningen.[74] Forskaren riskerar annars att frångå det objektiva förhållningssättet i förhållande till studieobjektet och inta en mer subjektiv hållning, vilket äventyrar resultaten och hela studien. Generaliserbarheten är begränsad till teoretiska påståenden och det saknas därför möjlighet att skapa allmängiltiga teoretiska modeller genom metoden.[75] Resultaten kan därför inte betraktas som fullkomliga då dessa studier inte är iscensatta situationer eller skeenden där forskaren kan justera variabler för att sedan utvärdera effekten av justeringen.[76]

4.3 Operationalisering

Processpårning har använts som metod för inomfallsstudier. Analysen av fallen har en minsta gemensam nämnare i samtliga fall vilket är *händelsen.* Vi avser att definiera *händelsen* som tidpunkten där kontraspionaget identifierar en anomali och upptäckten när kontraspionaget går från att utreda en anomali till att identifiera en illegalistverksamhet. I samtliga tre fall har analysen av fallen således utgått från *händelsen* som lett till *upptäckten* där en utredning av illegalister påbörjats. För att visualisera analysen av varje fall skapades en tabell som utgår från Prunckuns fem olika steg från händelsen till upptäckt och vidare till utredning. Prunckuns fem steg ger svar på frågor som; vilken organisation tillhör illegalisterna och var befinner de sig geografiskt. Prunkuns fem steg jämförs sedan mot Ehrmans tre olika typer av operationer för upptäckt genom kontraspionage. Ehrmans teori ger svar på frågor som; hur man arbetade för att upptäcka illegalister och utreda illegalistverksamhet. Avslutningsvis sammanställs de tre fallen med syftet att se skillnader och likheter vilka sedan ligger till grund för slutsatserna.

Genom att kombinera de två teoretiska ramverken skapas ett verktyg för att undersöka upptäckt av illegalistverksamhet som en process ur ett kontraspionage-perspektiv. I processen är händelsen central och beskriver startpunkten för processen av upptäckt. Processen av upptäckt övergår flytande till ett utredningsarbete där en bevissäkring genomförs. Genom att kombinera de två teoretiska ramverken skapas möjligheten att, utifrån materialet, identifiera vilken

[74] Jensen & Sandström, 2016, s. 42.
[75] Martyn Denscombe. *The Good Research Guide for Small Scale Research Projects*, uppl. 4, (Buckingham: Open University Press 2010), s. 63.
[76] ibid.

operationstyp som varit aktuell för kontraspionaget under respektive steg i processen.

4.4 Material

Forskning inom området kontraspionage och upptäckt av illegalister är inte vanligt förekommande, vilket innebär vissa begränsningar i forskningsmaterial och teorier. Den forskning som finns är relaterad till Ryssland vilket också får anses vara en anledning till att just Ryssland studeras. De tre fall som har valts ut är resultatet av en gallringsprocess utifrån population över geografisk spridning, dokumenterat avslöjande samt fall över tid. Population valdes som kriterium men studien begränsas av tillgängligt material utanför den anglosaxiska sfären. Dokumenterat avslöjande valdes för att undvika fall som bygger på indicier eller rykten om upptäckt och därmed möjliga att studera vetenskapligt. Fallen är spridda över perioden 1953 - 2010 för att undersöka eventuella förändringar i modus operandi kopplat till brukandet av illegalister över tid.

Till grund för fallstudien ligger tre facklitterära böcker, den första är “Undercover - My Secret Life and Tangled Allegiances as a KGB Spy in America”. Den andra är “Dead Doubles” av Barnes, Trevor och den tredje är “Russian among us” av Corera, Gordon. “Dead Doubles” och “Russians among us” är detaljrika och citerade av bland annat Kevin P. Riehle. “Deep undercover” är en självbiografi skriven av en medförfattare, Coloma, Cindy men det saknas citering från akademiska artiklar. Sammantaget anses “Dead Doubles” och “Russian among us” hålla en opartisk, detaljrik beskrivning av fallen medan Deep undercover får anses vara något svagare utifrån en akademisk kvalitet. Det sistnämnda anses vägas upp av de detaljerade beskrivningar som boken ger av hur en illegalist rekryterades och tränades under kalla krigets sista år.

I fallet som rör Portland spy ring finns flera illegalister varav den mest framträdande och sammanhållande är föremål för studien. Detta motiveras av att det var genom denna illegalist som illegalistverksamheten i sig slutligen upptäcktes. I boken “Russians among us” ges detaljerade beskrivningar av flera fall av illegalister. Utifrån dessa fall har ett fall särskilt valts ut då fallet visar på flera likheter med övriga fall samtidigt som fallet visade på en metodutveckling i vissa delar och därmed relevant för frågeställningen. Därmed är inte fallet representativt för Operation ghost stories som helhet även om många likheter finns. I fallet Jack Barsky utgår litteraturen från den specifika individen och inga andra illegalister identifierades.

5 Resultat och analys

Analysen är uppbyggd utifrån de tre fallen där vart och ett är föremål för en inomfallsstudie genom processpårning utifrån vad som tidigare beskrivits under metod- respektive teoriavsnitt. Analysen av respektive fall inleds med en sammanfattning där fallet beskrivs i löpande text vilken sammanfattats utifrån den litteratur som ligger till grund för studien i det specifika fallet. I sammanfattningen ges läsaren en översikt och en övergripande förståelse för fallet. I anslutning till respektive sammanfattning presenteras en tabell för översikt över analysresultatet i respektive inomfallsstudie. Därefter presenteras analysen av materialet i detalj utifrån de fem premisserna för upptäckt där operationstyp definieras och analyseras. Slutligen genomförs en sammanställning mellan fallen där likheter och olikheter analyseras i syfte att generera underlag för slutsatser.

5.1 Fall 1 - Gordon Lonsdale

5.1.1 Sammanfattning

Portland spy ring var en spionring som var verksam i Storbritannien mellan åren 1953–1961, där ett av målen var att komma över kunskap om den brittiska marinens nya atomdrivna ubåt, HMS Dreadnought. I spionringen fanns bland annat den ryska illegalisten och underrättelseofficeren Konon Molody, alias Gordon Lonsdale. Som illegalist hanterade Lonsdale den brittiska spionen och marinofficeren, Harry Houghton. Houghton påbörjade sin spionkarriär under tjänstgöring i Polen, där han arbetade som handläggare till militärattachén i Warszawa mellan åren juli 1951 till oktober 1952.[77] Under perioden i Polen anklagades han av sin dåvarande fru att för att misshandla henne samt erbjuda hemlig information till personer som informationen inte var avsedd för. Detta var information som skickades vidare till MI5 men som inte föranledde någon åtgärd.[78] Houghton hade alkoholproblem, vilket resulterade i att han skickades hem till Storbritannien där han placerades vid Underwater Detection Establishment (UDE) på ön Portland, Storbritannien.[79]

[77] Trevor Barnes. Dead Doubles: *The Extraordinary Worldwide Hunt for One of the Cold War's Most Notorious Spy Rings,* (United Kingdom: Weidenfeld & Nicolson, 2021), s. 26.
[78] ibid., s. 53.
[79] ibid., s. 40.

Houghton rekryterade sekreteraren, Ethel Gee som snart skulle hjälpa honom komma åt hemliga uppgifter på UDE.[80]

Den amerikanska ambassadören i Bern, Schweiz, mottog 1958 ett brev undertecknat ”Heckenschütze”, krypskytt på svenska. Personen erbjöd sig att skicka hemlig information till CIA. “Heckenschütze” avslöjade att den brittiska underrättelsetjänsten var infiltrerad av två spioner, där en av dem arbetade inom den brittiska flottan och hade tjänstgjort i Polen.[81] Den sistnämnda hade ett namn som påminde om ‘Huppkener’, ‘Happkener’ eller ‘Huppenkort’ vilket ledde till Harry Houghton, Ethel Gee och Gordon Lonsdale. Avlyssning av kortvågsradion avslöjade senare hur Lonsdale hanterade paret Houghton och Gee.[82]

Genom spaning på Lonsdale visade det sig att han besökte en bank med en väska och banken blev föremål för en inofficiell husrannsakan. Bankfacket visade sig innehålla flera föremål, vilka blev bevis för Lonsdales verksamhet. Bland annat en cigarettändare med ett lönnfack som innehöll en lapp med flera adresser i London, vilka antogs vara platser för dead drops.[83] Ytterligare spaning på Lonsdale ledde MI5 till paret Peter och Helen Kroger, alias Morris och Lona Cohen, två illegalister från USA som arbetade för Lonsdale. Gripandet i januari 1961 markerade slutet på en tio år lång period av spioneri där det skulle visa sig att två av aktörerna inom Portland spy ring även deltagit i spionaget mot Manhattanprojektet och lämnat ut ritningar på USAs första atombomb till Ryssland.[84] I den efterföljande domen dömdes de inblandade i spionringen till långa fängelsestraff.[85]

[80] Barnes, 2021, s. 267.
[81] ibid., s. 26.
[82] ibid., s. 37.
[83] ibid., s. 102
[84] ibid., s. 253.
[85] ibid., s. 191.

Översikt av operationalisering i fallet Gordon Lonsdale		Ehrmans teoretiska ramverk för kontraspionageoperationer		
		Penetration	**Dubbelagenter**	**Systematiskt utredningsarbete**
		Inifrånperspektiv	*Utifrånperspektiv*	
Prunckuns teoretiska ramverk, fem premisser om upptäckt	**1. Identifiering av händelsen**	Heckenschutze avslöjade spion (Houghton).		
	2. Identifiera inblandade individer			Spaning för att hitta kontakt och identifiera övriga i spionringen.
	3. Identifiera inblandade individers organisatoriska tillhörighet			Avlyssning av Lonsdale gav att han kontrollerade Houghtons. Spaning på Lonsdale gav paret Kroger. Brev med adresser. (Krogers)
	4. Identifiera inblandade individers geografiska position			Spaning på Houghton gav Molody. Spaning på Lonsdale ger Krogers.
	5. Säkra information som bekräftar att identifierade individer varit delaktiga i händelsen			Husrannsakan på bank kopplade Lonsdale till händelse. Husrannsakan hos Krogers kopplade Krogers med Lonsdale via brev på ryska.

Tabell 1:1

5.1.2 Identifiering av händelsen

Händelsen som leder till upptäckten av illegalisten identifieras som tillfället när brittiska underrättelsetjänsten tipsades av amerikanska CIA att det fanns två spioner i Storbritannien där en av dem arbetade inom den brittiska flottan. Källan var den polska "Heckenschutze" som formellt arbetade för polska underrättelsetjänsten men som försåg amerikanska CIA/FBI med information. Heckenschutze angav att spionen inom flottan hade ett namn som påminde om 'Huppkener', 'Happkener' eller 'Huppenkort' vilket ledde misstankarna mot Harry Houghton.[86]

[86] Barnes, 2021, s. 26.

Heckenschutze anses uppfylla kriterierna för en penetration enligt Ehrmans teori utifrån en bedömning att han hade tillgång till informationen från ett inifrånperspektiv.[87] Dock hade han enbart tillgång till information om en spion inom brittiska marinen men inte om någon illegalist vilket kan tyda på en mindre central position. Heckenschutzes information är direkt kopplad till den senare upptäckten av illegalisten och definieras därför som händelsen i enlighet med Prunckuns teori.[88]

5.1.3 Identifiera inblandade individer

Den spaning som MI5 genomförde mot Houghton resulterade i att de registrerade en registreringsskylt tillhörande en av de personer som Houghton mötte. Registreringsskylten på bilen som mannen från mötet använde för att köra från platsen gav namnet Gordon Lonsdale.[89] MI5 misstänkte dock från början av utredningen att Lonsdale hade en sammanhållande roll i kontakten med Ryssland och de initierade därför spaning på Lonsdale. Spaningen ledde dem till paret Helen och Peter Kroger, två personer som sedan visade sig vara ett amerikanskt par vid namn Lona och Morris Cohen. Gordon Lonsdale och paret Cohen anses per definition vara illegalister då dessa har skapade legender[90] samt verkar utan någon koppling till en nation eller några av dess organisationer eller institutioner[91].

5.1.4 Identifiera inblandade individers organisatoriska tillhörighet

Vidare spaning på Lonsdale ledde till ett bankfack som disponerades av Lonsdale. Den husrannsakan som genomfördes i bankfacket bekräftade att Gordon Lonsdale i själva verket var rysk illegalist. Beviset var ett antal chiffernycklar för blankettchiffer som användes för att avkoda radiomeddelanden via kortvågsradio.[92] Fortsatt avlyssning och spaning ledde MI5 till paret Kroger. Vid genomsökning av Helen Krogers handväska fann MI5 en lapp med adresser som kunde kopplas till de adresser som Lonsdale förvarade i sitt bankfack. I handväskan fanns också ett brev från Lonsdale till hans familj i Ryssland. Brevet utgör även det ett bevis för koppling till Ryssland men det knyter inte Kroger till en specifik organisationstillhörighet.[93]

[87] Ehrman, 2009, s. 15.
[88] Prunckun, 2019, s. 47.
[89] Barnes, 2021, s. 37.
[90] Riehle, 2020, s. 392.
[91] ibid., 2020, s. 385.
[92] Barnes, 2021, s. 73.
[93] ibid., s. 104.

5.1.5 Identifiera inblandade individers geografiska position

MI5 inleder spaning på Houghton som i sin tur gav Lonsdale. Upptäckten försvårades då Lonsdale flyttade omkring.[94] Spaning på Lonsdale resulterade slutligen att man kunde lokalisera Lona och Morris Cohens bostad.

5.1.6 Säkra information som bekräftar att identifierade individer varit delaktiga i händelsen

Genom avlyssning av Lonsdale fick kontraspionaget information om vem, när hur och var gällande illegalistverksamheten. Genom ett systematiskt utredningsarbete kunde kontraspionaget få realtidsinformation om motståndaren men också dess modus operandi.[95] Tiden efter avslöjandet innehöll en rad utredningstekniska åtgärder i form av spaning och avlyssning av både Houghton och Lonsdale för att säkra bevis.

De utredningstekniska åtgärder som vidtogs bestod av att dokumentera vilka som var inblandade och förstå vilken typ av information som spionerna kommit över samt förstå hur de kommunicerade mellan varandra. Avlyssning av Lonsdale avslöjade att kontakten med Ryssland genomfördes via kortvågsradio där Lonsdale fick instruktioner. Dessa radiosändningar avkodades med hjälp av chiffernycklar från husrannsakan i bankfacket. I Krogers handväska påträffades privata brev, författade med hjälp av microdots, på ryska mellan Lonsdale och hans familj i Ryssland.[96] Fallet Portland spy ring är ett exempel när åtgärden blir att avvakta för att vänta ut mer information för att säkra individer som varit delaktiga i händelsen. Vidare erbjuder det systematiska utredningsarbetet ny information som gör att man börjar förstå spionringens modus operandi.

[94] Barnes, 2021, s. 73.
[95] ibid.
[96] Barnes, 2021, s. 104.

5.2 Fall 2 - Jack Barsky

5.2.1 Sammanfattning

Albert Dittrich, alias Jack Philip Barsky är en före detta illegalist från Östtyskland som var aktiv i USA mellan 1973 - 1988.[97] Han approcherades av vad han senare uppfattade som östtyska Stasi 1970 i sitt hem, initialt med löfte om ett arbete på Carl Zeiss men blev under samma samtal erbjuden att arbeta för ”staten”.[98] Mötet blev början på en resa med målet att bosätta sig i USA som illegalist. Dittrich utbildades i olika steg från 1969 tills dess att han slutligen skickades till USA 1978 där hans uppdrag var att infiltrera olika typer av tankesmedjor i USA. Utbildningen startade i Berlin 1973[99] med att Dittrich utbildades i kortvågsradio och morsekod, kryptografi, hemlig skrift samt fotografi.[100] Dittrich utbildades även i fysiska möten, dead drops, att upptäcka övervakning samt övriga färdigheter som krävdes för att leva i väst.[101] 1976 träffade Dittrich paret Kroger, de två illegalister som ingått i Portland spy ring. Paret Kroger hjälpte Dittrich att förbereda sig för sitt uppdrag.[102] 1978 skapades legenden för den nya identiteten, Jack Barsky, en pojke som avlidit 1955, tio år gammal och som återuppstått[103].

Genom envägskommunikation i form av krypterade radiosändningar över kortvågsradio kommunicerade Moskva med Jack Barsky. Under sin tid i USA blandades instruktioner och uppdrag med exempelvis nyheten om att Barsky blivit pappa till en son i Tyskland.[104] Avrapporteringen från Barsky till Moskva skedde istället via dead drops eller kodade brev[105].

Barskys mål under tiden i USA var att bygga relationer med inflytelserika personer, bland annat med det specifika målet att komma nära personer som stod nära och förstod sig på president Ronald Reagan.[106] Barsky beskriver även aktiva operationer där han bland annat använts som en mellanhand vid hantering av särskilt känsliga agenter.[107] I december 1988 meddelade KGB via kortvågsradio att den

[97] Jack Barsky. *Deep Undercover: My Secret Life and Tangled Allegiances as a KGB Spy in America,* (New York: Tyndale House Publishers Inc, 2017), s. 278.
[98] ibid., s. 68-69.
[99] ibid., s. 94.
[100] ibid., s. 98-99.
[101] ibid., s. 100-101.
[102] ibid., s. 134.
[103] ibid., s. 154.
[104] ibid., s. 204.
[105] ibid.
[106] ibid., s. 222.
[107] ibid., s. 234.

falska identiteten Jack Barsky misstänktes vara röjd och han ombads att förbereda sig för att lämna USA[108]. Istället stannade han kvar i USA bland annat under förevändningen att han fått AIDS i syfte att inte vara önskvärd i Sovjetunionen.[109]

I början av 90-talet uppstod en kris mellan Barsky och hans fru Penelope. Vid ett av deras samtal i hemmet avslöjade Barsky för Penelope att han arbetat för Ryssland och att han levt under falsk identitet i USA under en lång tid.[110] Vad han inte visste var att FBI hade installerat avlyssningsutrustning i deras hem inom ramen för den utredning som inletts mot honom 1993[111] efter information från Vasilij Mitrohkins avhopp 1992[112]. Mitrohkin som arbetat som arkivarie på KGBs första direktorat hade först kontaktat CIA men blivit avvisad och vände sig därefter till Storbritanniens ambassad i Riga vilka tillslut genom MI6 organiserade hans avhopp. Mitrohkin hade med sig sex väskor med underrättelserapporter vilka han under åren förvarat nedgrävda i trädgården, väskorna innehöll över 3500 rapporter vilka delades ut till 36 olika länder.[113] Trots att Barsky avslutat sitt arbete för Sovjetunionen och KGB redan 1988 så var det först nu som FBI på riktigt visste att de hade rätt person[114]. FBI kontaktade Barsky i maj 1997 genom ett fordonsstopp[115] varpå ett samarbete inleddes.

[108] Barsky, 2017, s. 247.
[109] ibid., s. 252.
[110] ibid., s. 265.
[111] Barsky, 2017, s. 279.
[112] Corera, 2020, s. 45-46.
[113] ibid.
[114] ibid., s. 265.
[115] ibid., s. 269.

Översikt av operationalisering i fallet Jack Barsky.		Ehrmans teoretiska ramverk för kontraspionageoperationer		
		Penetration	**Dubbelagenter**	**Systematiskt utredningsarbete**
		Inifrånperspektiv	*Utifrånperspektiv*	
Prunckuns teoretiska ramverk, fem premisser om upptäckt	**1. Identifiering av händelsen**	1992 lämnade Vasilij Mitrokhin över dokument med namn på ryska illegalister.		
	2. Identifiera inblandade individer	Mitrokhins anteckningar innehöll namnet Jack Barsky. Kodnamn: Dieter		
	3. Identifiera inblandade individers organisatoriska tillhörighet	Vasilij Mitrokhin gav information om ryska illegalister till MI6 som delades med USA.		
	4. Identifiera inblandade individers geografiska position			Utredningsarbete av FBI genom inre- och yttre spaning.
	5. Säkra information som bekräftar att identifierade individer varit delaktiga i händelsen			Avlyssning av Barsky´s bostad. Utrednings-arbete från FBI via inre- och yttre spaning. FBI köpte och flyttade in i grannhuset.

Tabell 1:2

5.2.2 Identifiering av händelsen

Den händelse som identifierats i fallet som leder till upptäckt av illegalisten är ögonblicket då FBI analyserade det från MI6 mottagna materialet, ursprungligen från Vasilij Mitrohkin. Mitrohkin hade dock bara haft tillgång till materialet fram till och med 1984.[116] Det var på detta sätt en potentiellt säkerhetshotande händelse initialt upptäcktes i fallet, en händelse som utgjordes av en potentiell illegalistverksamhet i form av en aktiv illegalist.

[116] Barsky, 2017, s. 279.

Då Mitrohkin överlämnat uppgifterna först efter sitt avhopp uppfyller han inte direkt kriterierna för en rekryterad individ på insidan i enlighet med Ehrmans teori om penetration. Däremot är hans tidigare informationstillgång att likställa med penetrationen utifrån att han, liksom en rekryterad person på insidan, haft direkt tillgång till informationen från ett inifrånperspektiv[117], dessutom med en synnerligen central position. Med reservation för att informationen kunde varit daterad och därmed saknat operationellt värde kan ändå Mitrohkins överlämnande av information likställas med en penetration. Mitrokhin hoppade enligt Barsky av redan 1991[118], Corera menar att det var 1992[119], men utredningen mot Barsky påbörjades först på hösten 1993[120]. Tilläggas kan göras att FBI bara fem månader innan Barsky ansökte om ett socialförsäkringskort hade stängt ned ett system som skulle varna för individer under trettio år som gjorde ansökningar. Systemet hade enligt FBI stängts ned på grund av uteblivna resultat[121]. Detta kan ses som ett missat tillfälle för upptäckt av händelsen av illegalistverksamheten där upptäckten skulle kunnat gjorts med en traditionell, defensiv metod.

5.2.3 Identifiera inblandade individer

I Mitrohkins material fanns en notering om en illegalist på den amerikanska östkusten vid namn Jack Barsky. Det framgick att Jack Barsky hade kodnamnet Dieter samt att det enligt Mitrohkin fanns nio volymer om Dieter i arkivet.[122] Genom Mitrohkins penetration av KGB fick FBI inte bara händelsen i form av potentiellt omfattande aktiv illegalistverksamhet, de fick även ett namn på en amerikan vid namn Jack Barsky som någonstans på östkusten levde som illegalist.[123] Upptäckten av individen Jack Barsky som illegalist var således information direkt från penetrationen. I fallet identifierades inga ytterligare individer som kunde knytas till illegalistverksamheten.

[117] Ehrman, 2009, s. 15.
[118] Barsky, 2017, s. 279
[119] Corera, 2020, s. 46.
[120] Barsky, 2017, s. 279.
[121] ibid., s. 279-280.
[122] ibid., s. 279.
[123] ibid.

5.2.4 Identifiera inblandade individers organisatoriska tillhörighet

Penetrationen genom en före detta sovjetisk arkivarie[124] får antas ha inneburit en direkt information om den organisatoriska tillhörigheten. Den avslöjade illegalisten var således den sovjetiska underrättelsetjänsten KGB:s resurs.

5.2.5 Identifiera inblandade individers geografiska position

Genom penetrationen fick FBI namnet Jack Barsky tillsammans med en lågupplöst positionsangivelse i form av USAs östkust. Namnet Jack Barsky var inte så vanligt förekommande och det gick således snabbt för FBI att lokalisera Jack Barsky och påbörja det systematiska utredningsarbetet.[125]

5.2.6 Säkra information som bekräftar att identifierade individer varit delaktiga i händelsen

För att utreda huruvida Jack Barsky var den illegalist som den upptäckta händelsen antydde fortsatte FBIs systematiska utredningsarbete. En viktig fråga att besvara var Jack Barskys operativa status. FBI misstänkte att han kunde vara en sovande agent varför ett resurskrävande och försiktigt arbete tog sin början.[126] FBI köpte bland annat grannfastigheten till Barskys hus i vilken två personer anställda på FBI flyttade in, på detta sätt kunde de effektivt övervaka Barsky.[127] Dessutom installerades avlyssningsutrustning i Barskys hem. Vid en tidpunkt under tiden som avlyssningsutrustningen var installerad avslöjade Barsky för sin fru att han arbetat för Sovjetunionen.[128] När FBI 1997 tog kontakt med Barsky genomfördes inte ett gripande, aktionen kan snarare beskrivas som en kontakt vilken initierades av att man stoppade Barskys bil med honom som ensam förare.[129] Ett samarbete inleddes i vilket Barsky för FBI redogjorde för sina tidigare förehavanden och sin metodik. På detta sätt blev Barskys bandade erkännande som en del av det systematiska utredningsarbetet startskottet på ett fortsatt utredningsarbete genom samarbete syftande till att förstå illegalistverksamhetens metoder och tillvägagångssätt.[130] I

[124] Barsky, 2017, s. 279.
[125] ibid.
[126] ibid., s. 280.
[127] ibid.
[128] ibid.
[129] ibid., s. 269.
[130] ibid., s. 276-277.

detta fall väcktes aldrig åtal, istället kunde insamlade bevis för delaktighet användas för att inkassera ytterligare kunskap och erfarenheter i syfte att bättre förstå sin motståndare.

5.3 Fall 3 – Richard Murphy

5.3.1 Sammanfattning

Ghost stories var en hemlig operation som utredde ryska illegalister och drevs av FBI i USA från omkring år 2000[131] till 2010[132]. Operationen är speciell på många sätt men den sticker ut på en punkt; illegalister förefaller inte varit ute efter hemligheter – de var ute efter att identifiera personer som potentiellt skulle kunna rekryteras som agenter[133], även kallat "spotting and assessing"[134]. Rysslands illegalister i USA skulle senare avslöjas offentligt 2010 som ett resultat av en penetration av SVR. Penetrationen var möjlig genom en rekrytering av Alexander Poteyev som sannolikt rekryterades 1999 i New York[135] även om FBI och CIA inte själva velat kommentera Poteyevs eventuella roll i avslöjandena.[136] Poteyev lämnade ut namn på illegalister från och med år 2000.[137] Under 2005 följde FBI upp ett tips där Richard Murphy och hans fru Cynthia Hopkins misstänktes vara illegalister. Under en husrannsakan fann de flera disketter som visade sig innehålla ett program för att dölja meddelanden i bilder, en form av steganografi.[138] Programmet krävde flera disketter för att fungera men visade på en utveckling inom krypteringstekniken för att skicka meddelanden.

I början av 2000-talet inträdde en annan rysk person som aldrig dolde sin ryska bakgrund i det amerikanska samhället. Anna Kuschenko, dotter till en officer inom SVR, hade rest till London där hon träffade Alex Chapman, en brittisk medborgare i 20-årsåldern.[139] Anna gifte sig med Alex 2002 och blev Anna Chapman.[140] Anna Chapman reste ofta mellan USA och Storbritannien där hon umgicks med en rad

[131] Corera, 2020, s. 84.
[132] ibid. s. 1.
[133] ibid., s. 105.
[134] ibid., s. 122.
[135] ibid., s. 76.
[136] ibid., s. 69.
[137] ibid., s. 82, 84.
[138] ibid., s. 101.
[139] ibid., s. 139.
[140] ibid., s. 138

inflytelserika personer.[141] Kuschenko var en ny typ av illegalist som FBI namngav som ”agent” eftersom de rekryterats av SVR.[142]

Under samma period inträdde även Pavel Kapustin, alias Christopher Metsos, Mikhail Kutsik, alias Michael Zottoli och Natalia Pereverzeva. FBI hade redan uppgifter om dem genom tips från Poteyev i Moskva. Kapustin hanterade dead drops och pengar för illegalister runt om i världen, i en verksamhet där även Zottoli och Pereverzeva ingick.[143] Kommunikation genomfördes i hög grad genom samtal med andra illegalister som sedan stämde träff med hanteraren, Metsos. Under 2010 greps illegalisterna i USA och Alexander Poteyev flydde från USA till Ryssland. Inget åtal väcktes, istället verkställdes en fångutväxling med Ryssland i juli 2010.[144]

[141] Corera, 2020, s. 138-139.
[142] ibid., s. 144.
[143] ibid., s. 186.
[144] ibid., s. 296.

Översikt av operationalisering i fallet Richard Murphy		Ehrmans teoretiska ramverk för kontraspionageoperationer		
		Penetration	**Dubbelagenter**	**Systematiskt utredningsarbete**
		Inifrånperspektiv	***Utifrånperspektiv***	
Prunckuns teoretiska ramverk, fem premisser om upptäckt	**1. Identifiering av händelsen**	Poteyev började lämna ut information från år 2000.		
	2. Identifiera inblandade individer	Poteyev försåg FBI med namn på illegalister i USA. Heathfield följdes redan 2000		Genom utredningsarbete är det möjligt att exempelvis Kutsik avslöjats via spaning.
	3. Identifiera inblandade individers organisatoriska tillhörighet	Poteyev som rysk källa försåg FBI med information om illegalister i USA.		Eventuellt avslöjades Kutsik:s täckmantel av hans alias.
	4. Identifiera inblandade individers geografiska position			Löpande utredningsarbete av FBI.
	5. Säkra information som bekräftar att identifierade individer varit delaktiga i händelsen			Lokalisering genom spaning och avlyssning.

Tabell 1:3

5.3.2 Identifiering av händelsen

Händelsen som föranledde upptäckten identifieras som informationen om illegalistverksamhet FBI erhöll genom penetration där källan, Alexander Poteyev var placerad i direktorat S på SVR i Moskva. Poteyev var ett resultat av en rekrytering som ägde rum runt 1999 i New York där han då var placerad.[145] Vid tillfället för FBIs rekrytering visste de att han skulle avancera inom SVR till en senior position där han var en av tre som hade möjlighet att läsa akter om illegalister i USA.[146] I egenskap av

[145] Corera, 2020, s. 78.
[146] ibid., s. 79.

sin nya position påbörjade Poteyev lämna ut namn på illegalister från och med år 2000 vilket skulle leda USA till upptäckten av illegalisterna.[147]

5.3.3 Identifiera inblandade individer

Ghost stories bestod av tio olika illegalister som avslöjats av Poteyev där FBI spanade på flera av dem samtidigt. Under 2002 spanade FBI på illegalisten Vladimir Guryev, alias Richard Murphy, när han åt lunch med en annan person som sedan skulle visa sig vara Metsos. Metsos var en äldre illegalist som föreföll ha fungerat som sambandsperson som även supporterade illegalister, bland annat i USA.[148] 2004 avlyssnade FBI när Murphy samtalade med Mikhail Kutsik. Samtalet ledde till att Zottoli reste till New York där han mötte upp med Murphy, mötet representerade första gången FBI observerade att två illegalister träffades fysiskt.[149]

5.3.4 Identifiera inblandade individers organisatoriska tillhörighet

Poteyev var orsaken till att flera av illegalisternas organisatoriska tillhörighet avslöjades men det finns också tecken på att exempelvis Kapustin kan ha avslöjats genom kontakt med Murphy och Zottoli. FBI använde under operationen en mängd olika tekniker, bland annat för övervakning av telefonsamtal, e-postmeddelanden, kontroll av bankregister, dold videoövervakning av offentliga platser, hotellrum och fysisk spaning.[150] Övervakningen fungerade dels som en källa för ny information men avlyssning och spaning bekräftade också misstankar om vilken organisation de tillhörde.

5.3.5 Identifiera inblandade individers geografiska position

Det framgår inte i utredningen hur FBI kommit över illegalisternas position och studien har därför utgått från att FBIs utredningsarbete gav positionen på illegalister. I annat fall skulle Poteyev löpande delat deras legender och adresser med FBI. Poteyevs utsatthet i form av en aktiv placering i SVR kan dock tänkas tala emot vad som mer eller mindre skulle likna en realtidsrapportering.

[147] ibid., s. 82, 84.
[148] ibid., s. 182.
[149] ibid., s. 187.
[150] ibid., s. 96.

5.3.6 Säkra information som bekräftar att identifierade individer varit delaktiga i händelsen

FBI sammanställde bevisen för illegalisterna från början av operation Ghost stories vilket medförde att de hade ett mycket gott bevisläge. Lägenheten som Murphy använde sig av var avlyssnad och där fick FBI information om bland annat utmaningar inom kommunikation som Murphy påtalade för SVR. SVR använde sig även av en egen programvara för att extrahera, dekryptera och läsa data från bilder med kodade meddelanden.[151] Murphy tyckte om att fotografera blommor vilket visade sig vara en täckmantel för att dölja meddelanden i bilder genom steganografi.

5.4 Sammanställning av fallen

5.4.1 Identifiering av händelsen

Vad gäller illegalister visar analysen att deras uppgifter ofta bestod av påverkan och en form av "spotting and assessing" där verksamheten utifrån en sofistikerad legend bedrivits från en position fullt integrerad och etablerad i samhället.[152] Detta bidrar till att anomalier och avvikande beteenden som är grunden för teorin om upptäckt ofta saknas i det, för en illegalist, dagliga operativa arbetet. Det ska dock tilläggas att illegalister också genomför andra uppgifter, som att agera som mellanhand för känsliga möten eller i undantagsfall också själva hantera agenter vilket Lonsdale[153] och Barsky[154] ger exempel på.

I fallen har händelsen i samtliga fall utgjorts av information inifrån Ryssland eller Sovjetunionens underrättelseapparaturer och dess tentakler. Informationen har varit värdefull även om detaljrikedomen har skiftat. I exempelvis fallet Gordon Lonsdale erhölls endast bristfällig information om spionen Houghton, således behövde ett systematiskt utredningsarbete bedrivas i alla steg för upptäckt av illegalisterna. I fallet Jack Barsky å andra sidan, gav penetrationen genom en centralt placerad källa flera steg av upptäckten av illegalisten parallellt med upptäckten av händelsen. I fallet Gordon Lonsdale har vi identifierat källan "Heckenschutze" som en penetration då vi utifrån materialet har bedömt att denne arbetat inne i den polska underrättelsetjänsten och därmed haft information inifrån verksamheten om än

[151] Corera, 2020, s. 104.
[152] ibid., s. 105.
[153] Barnes, 2021, s. 37.
[154] Barsky, 2017 s. 234.

perifert. Det faktum att "Heckenschutze" inte gav direkt information om illegalister men ändå gav värdefull information om verksamheten är överensstämmande med Ehrmans teoretiska ramverk där han menar att en penetration kan vara effektiv även om penetrationen sker på en lägre nivå i systemet.[155] Om "Heckenschutze" skulle definieras som dubbelagent, utifrån en diskussion om otydligheter huruvida han befunnit sig mer utanför än inuti verksamheten, skulle även det kunna förklara hans begränsade informationstillgång enligt Ehrmans teoretiska ramverk. Ehrman menar att dubbelagenter i normalfallet enbart tillför sporadisk information, de styr inte själva sin tillgång på information.[156]

Inte i något av de tre fallen har materialet klart visat att händelsen som lett till upptäckt av illegalister initierats av det systematiska utredningsarbetet. I fallet Jack Barsky finns dock exempel på defensiva metoder i form av övervakningssystem som hade kunnat upptäcka anomalier om systemen varit aktiva. Händelsen där Barsky som yngre än trettio år sökte om ett socialförsäkringskort[157] skulle kunna utgjort en händelse som, om den hade registrerats, potentiellt hade kunnat bidragit till tidigare upptäckt.

Illegalisterna har dock bedrivit vissa aktiviteter som haft en direkt koppling till deras uppdrag. Dessa aktiviteter kan i enlighet med fallen ovan spåras till kommunikation av såväl teknisk som fysisk natur och kan ses som aktiviteter som, om de registrerats som en säkerhetshotande händelse, kunde ha lett till upptäckten. Utöver den krypterade envägskommunikationen fanns ett behov att rapportera tillbaka till Moskva vilket skett genom olika sofistikerade metoder där bland annat överlämningar via dead drops eller fysiska möten har använts.[158] Gemensamt för dessa metoder är att de karaktäriseras av sofistikerade metoder för försvårande av upptäckt. I enlighet med vad Wirtz beskriver som förnekande av information[159] och Mobley som ett anpassat förnekande[160] användes exempelvis inte bara krypterade radiosändningar, illegalisterna har även undvikit att sända och därmed minskat utgående radiotrafik. Med detta sagt var inte sändande trafik helt frånvarande, kortvariga sändningar med "microburst", en form av komprimerad sändning via kortvåg, förekom.[161]

[155] Ehrman, 2009, s.15.
[156] ibid.
[157] Barsky, 2017, s. 279-280.
[158] ibid., s. 204.
[159] Wirtz, 2008, s. 56.
[160] Mobley, 2012, s. 11.
[161] Corera, 2020, s. 90

5.4.2 Identifiera inblandade individer

Identifieringen av individer som ingått i illegalistverksamheten skiljer sig åt mellan fallen. I fallet Jack Barsky identifierades endast illegalisten men ett systematiskt utredningsarbete utfördes bland annat i syfte att identifiera potentiellt fler individer. Illegalisten Gordon Lonsdale, men även paret Kroger, identifierades via ett systematiskt utredningsarbete efter en händelse som inte direkt var kopplad till illegalistverksamhet. I fallet Richard Murphy är det enligt litteraturen sannolikt att det var Poteyev som avslöjade likväl honom som övriga illegalister och att det var anledningen till att Murphy var under övervakning år 2002.[162] Om penetrationen genom Poteyev gav identifieringen på samtliga illegalister i Operation Ghost stories går inte att utläsa ur materialet men klart är att FBI genomförde ett omfattande systematiskt utredningsarbete som bland annat innefattar avlyssning av Richard Murphys samtal till illegalisten Michael Zottoli.[163] Samtalet ledde till ett möte mellan dem varpå det systematiska utredningsarbetet potentiellt hade kunnat fungera för att identifiera illegalisterna.

Den grad av sofistikering av sekretess som illegalisterna erhållit genom skapandet av legender[164] har historiskt varit en framgångsrik metod då det hjälpt illegalisterna att smälta in i samhället[165]. Riehle påtalar dock i sin forskning att anpassning av illegalistverksamheten visat sig i samband med gripandet av illegalister 2010 i Operation ghost stories. Två av dessa individer verkade under sin riktiga identitet som ryska medborgare men utan officiell koppling till ryska staten, de hanterades som illegalister och använde sig av metoder typiska för illegalister.[166] Riehle menar att Ryssland kan vara på väg att omdefiniera illegalistbegreppet till att innefatta individer med officiellt rysk bakgrund.[167] En sådan metodutveckling skulle innebära mindre komplicerade legender men skulle också kräva mindre resurser exempelvis i minskat behov att träna bort rysk accent och den ryska bakgrunden.[168]

Illegalister kan rekryteras ur två olika pooler: infödda ryssar och icke infödda ryssar. Infödda ryssar har, i jämförelse med icke infödda ryssar, påvisat en högre grad av lojalitet[169] samtidigt som de kräver mer utbildning och träning för att kunna genomföra uppdraget. Fördelen med icke-infödda ryssar är att skapandet av en legend kan vara enklare då delar av den verkliga bakgrunden kan användas, men den

[162] ibid., s. 182.
[163] Corera, 2020, s. 187.
[164] Riehle, 2020, s. 392.
[165] ibid., s. 385.
[166] ibid., s. 394.
[167] ibid., s. 396.
[168] ibid., s. 394.
[169] Riehle, 2020, s. 393.

stora fördelen är att dessa individer inte nödvändigtvis behöver tränas i nya kulturer, sedvänjor och språk för att passa in.[170]

I fallen har illegalisterna som studerats haft legender, en sofistikerad metod som gått ut på att återanvända identiteter genom att förfalska födelseattester från individer som avlidit i tidig ålder. Kring dessa legender har sedan en rigorös legend byggts upp där en form av levnadsbeskrivning upprättats. Användandet av legender och förfalskningen av födelseattester är en form av vilseledning i enlighet med Wirtz teori[171], en vilseledning som Mobley beskriver som en form av hemlig manipulation[172]. Dessa åtgärder ämnar försvåra upptäckten vid såväl inresa som vid vistelsen i landet. Corera påpekar de nya utmaningar illegalistverksamheten ställs inför med teknikutveckling av exempelvis biometri men också i form av elektroniska databaser där information om individer sparats och sammanställts. Denna utveckling tog fart först efter 11 september 2001 vilket betydde att legender för Richard Murphy och flera av de andra i Operation ghost stories hann skapas innan. Undantaget är två av dem, varav en är Anna Chapman, som kom till USA först 2006. Skillnaden är att Chapman arbetade under sin verkliga ryska identitet.[173]

5.4.3 Identifiera inblandade individers organisatoriska tillhörighet

I såväl fallet Jack Barsky som Richard Murphy kom informationen genom penetrationer vars ursprung var känt, den sovjetiska/ryska underrättelsetjänsten. Således kan de inblandade individernas organisatoriska tillhörighet anses vara tidigt kända för kontraspionagets verksamhet. I fallet Gordon Lonsdale var den organisatoriska tillhörigheten inte känd. Den organisatoriska tillhörigheten verkar snarare ha upptäckts genom ett systematiskt utredningsarbete där MI6 under en husrannsakan hos paret Kroger fann brev på ryska. Dessutom lyckades GCHQ avlyssna trafiken från Moskva till Lonsdale vilket också påvisade den organisatoriska tillhörigheten.[174]

[170] ibid., s. 394.
[171] Wirtz, 2008, s. 57.
[172] Mobley, 2012, s. 10.
[173] Riehle, 2020, s. 389.
[174] Barnes, 2021, s. 73.

5.4.4 Identifiera inblandade individers geografiska position

Inte i något av fallen finns det information som direkt tyder på att penetrationerna levererat realtidsinformation gällande aktuell geografisk position för inblandade illegalister. Denna information har kontraspionaget i respektive fall tillgodogjort sig genom systematiskt utredningsarbete i form av olika inre och yttre utredningsåtgärder, exempelvis i fallet Jack Barsky där man utifrån namnet hittade en person med samma namn bosatt på en adress varpå man sedan inledde övervakning.[175] Detta är ett tydligt tecken på det systematiska utredningsarbetets styrkor i form av realtidsuppföljning samtidigt som det tydligt pekar på en av penetrationens begränsningar – att ge information i realtid. Denna begränsning blir ännu mer tydlig i fallet där tiden från avhoppet tills dess att kontraspionagets agerade räknades i år snarare än i dagar.

5.4.5 Säkra information som bekräftar att identifierade individer varit delaktiga i händelsen

Vad denna informationsinsamling och insamlande av bevis ska syfta till kan skilja sig från fall till fall. I fallet Jack Barsky användes informationen från Barskys erkännande som ett bevis för hans roll som illegalist och blev startpunkten för det samarbete som följde. Genom samarbetet fick FBI en inblick i den metodik som Barsky som illegalist använt sig av. Vid ett tillfälle pekade Barsky ut en plats han långt tidigare använt för dead drop, på platsen låg det paket som han gömt femton år tidigare kvar.[176] Barsky åtalades aldrig, som en följd av hans samarbete och ärlighet tilläts han och familjen att stanna i USA på legitima grunder och med rena register.[177]

I fallet Gordon Lonsdale ledde det systematiska utredningsarbetet till väckt åtal för spioneri där utredningen och bevissäkringen ledde till fällande domar med för Lonsdale ett långt fängelsestraff.[178] Genom utredningsarbetet kunde kontraspionaget med hjälp av en mindre bit information nysta upp en illegalistverskamhet genom ett systematiskt utredningsarbete. Fallet visar tydligt på fördelarna med det systematiska utredningsarbetet som operationstyp där kontraspionaget får en realtidsuppföljning av illegalistverksamheten och dess modus operandi.

I Operation Ghost stories, där särskilt illegalisten Richard Murphy studerats, ledde det omfattande, tio år långa, systematiska utredningsarbetet till en

[175] Barsky, 2917, s. 279.
[176] Barsky, 2017, s. 276.
[177] ibid., s. 277.
[178] Barnes, 2021, s. 191.

fångutväxling med Ryssland.[179] Utredningen bestod av ett omfattande material där en noggrann kartläggning av individerna och deras förehavanden ägde rum. Många olika metoder användes i kartläggningen, såväl tekniska som fysiska i form av spaning. Med tio avslöjade illegalister satt USA med ett trumfkort. Genom att hota att åtala illegalisterna och därmed väcka än större publicitet hade de ett övertag i de vidare förhandlingarna[180] i utväxlingen som ägde rum i Wien i juli 2010.[181]

[179] Corera, 2020, s. 293.
[180] ibid., s. 278.
[181] ibid., s. 293.

6 Slutsatser

Syftet med studien har varit att undersöka vilka konsekvenser Rysslands användande av illegalister kan få för en stats kontraspionage avseende upptäckt av illegalistverksamhet med frågeställningen; Hur påverkar Rysslands användande av illegalister förutsättningarna för ett kontraspionage att upptäcka illegalistverksamhet?

Kort sammanfattning av slutsatser:

1. Resultaten visar på svårigheten för kontraspionaget att, genom systematiskt utredningsarbete, identifiera den säkerhetshotande händelsen vid illegalistverksamhet. Istället visar resultaten på att händelsen har upptäckts genom penetration.
2. Penetration, ibland beskriven som offensiv metod, i kombination med systematiskt utredningsarbete, ibland beskrivet som defensiv metod, förefaller vara den mest effektiva metoden för att upptäcka ett nätverk av illegalister.
3. Studien visar på en problematisering av Prunckuns teori om upptäckt där händelsen som initierar upptäckt enligt Prunckun utgår från en förlust av konfidentiell information.
4. Svårigheterna är kopplade till illegalistverkamhetens karaktäristiska metodik där sofistikerade metoder för undvikande av upptäckt. Framträdande delar i denna metodik är att vara integrerad i det angripna samhället samtidigt som avvikande beteenden, som av kontraspionaget kan uppfattas som anomalier, undviks.

Huvudsakligen visar studien på svårigheter för ett kontraspionage att utifrån ett systematiskt utredningsarbete identifiera en händelse som utgörs av en sofistikerad infiltration och integration med syfte “spotting and assessing”. Prunckuns teori om upptäckt där händelsen främst utgår från en förlust av konfidentiell information visar på studiens centrala upptäckt och påvisar ett behov av fortsatt forskning vad gäller upptäckt av illegalistverksamhet ett konkret hot saknas. Samtidigt visar studien, exempelvis i fallet Gordon Lonsdale, att det funnits tillfällen då indikationer på säkerhetshotande verksamhet varit uppenbara men där kontraspionaget inte uppfattat

händelsen. I sådana fall hade ett effektivare säkerhetsskyddsarbete möjligtvis kunnat tidigarelägga registrering av händelsen och därmed tidpunkten för upptäckt.

En centralt placerad penetration kan medföra en potentiell resursbesparing för kontraspionaget då fler steg av upptäckt erhålls samtidigt som avslöjandet. Det systematiska utredningsarbetet har också på ett annat plan visat sig ha en direkt påverkan på kontraspionagets arbete. Till skillnad mot utredningar som rör underrättelseofficerare med officiell täckmantel finns vid utredning av illegalister ett incitament till noggrann bevissäkring för en eventuell framtida rättsprocess, eller förhandling. De tre olika alternativen att använda resultatet av utredningsarbetet på ger möjligheter till politisk handlingsfrihet. Utifrån detta menar vi att ett omfattande utredningsarbete blir aktuellt i fall där illegalister medverkar.

Fallstudien visar att Ryssland har använt sig av illegalister under den studerade tidsperioden och att arbets- och kommunikationsmetoder fortsatt vara tämligen statiska under perioden men den har samtidigt belyst frågor om metodik och motiv. Riehle menar i sin artikel att Ryssland genom operatörer som Anna Kuschenko vid 2010 var på väg att omdefiniera begreppet illegalister att innefatta även individer med rysk bakgrund. Hur förändras Riehles tes om en förenkling av legender om ryska medborgare i väst möts med större skepticism som en följd av Rysslands förda säkerhetspolitik? Vidare finns ett behov av ytterligare forskning på området illegalister kopplat till det förändrade säkerhetsläget där forskningen skulle kunna bidra med att försöka förstå motiven till användandet av illegalister efter 2010. Det saknas idag forskning på målen med illegalistverksamheten med fokus på förändring. Detta går att koppla till fallet med Jack Barsky där målet med hans verksamhet beskrivs som otydligt.

Avslutningsvis visar resultaten att Prunckuns och Ehrmans teorier går att kombinera för att förklara hur Rysslands användning av illegalister påverkar kontraspionaget men det finns utrymme för vidare forskning. Det saknas idag en teori som utifrån upptäckt av illegalistverksamhet kombinerar de delar av Prunckuns teori om händelsen[182] som leder till upptäckten med Ehrmans modell för operationer inom kontraspionage[183]. En sådan teori skulle kunna vara ett verktyg för analys av illegalistfall för att utveckla kontraspionagets utmaningar i relation till illegalister.

[182] Prunckun, 2019, s. 47.
[183] Ehrman, 2009, s.15.

7 Referensförteckning

Barnes, Trevor. *Dead Doubles: The Extraordinary Worldwide Hunt for One of the Cold War's Most Notorious Spy Rings,* (United Kingdom: Weidenfeld & Nicolson, 2021).

Barsky, Jack. *Deep Undercover: My Secret Life and Tangled Allegiances as a KGB Spy in America,* (New York: Tyndale House Publishers Inc, 2017).

Boréus, Kristina & Bergström, Göran. *Textens mening och makt: metodbok i samhällsvetenskaplig text- och diskursanalys,* uppl 4, (Lund: Studentlitteratur, 2005).

Corera, Gordon. *Russians among us, Sleeper Cells and the Hunt for Putin's Agents,* (London: William Collins, 2020).

Denscombe, M. *The Good Research Guide for Small Scale Research Projects* (4th ed.). (Buckingham: Open University Press 2010).

Ehrman, John. Toward a Theory of CI – What are we talking about when we talk about counterintelligence? *Studies in Intelligence,* vol. 53, nr. 2, 2009.

Jensen, Tommy & Sandström, Johan, *Fallstudier*, uppl. 1, (Lund: Studentlitteratur, 2016).

Lamont, Christopher, *Research Methods in International Relations*, uppl. 2. (United Kingdom: SAGE publications, 2022).

Lindvall, Johannes. Fallstudiestrategier, *Statsvetenskaplig tidskrift*, vol. 109, nr. 3, 2007.

Lucas, Edward. The Spycraft Revolution : Changes in technology, politics, and business are all transforming espionage, *Foreign Policy.* nr. 232, 2019.

Mobley, Blake W. *Terrorism and counterintelligence : how terrorist groups elude detection.* (New York: Columbia University Press, 2012).

Nylander, Bengt och Lars Korsell. *Det som inte berättats: Säpo & kontraspionaget*, (Stockholm: Medströms bokförlag, 2021).

Olson, James M. *To catch a spy, The art of counterintelligence*, (USA: Georgetown university press, 2021).

Patel, Runa. & Davidson, Bo. *Forskningsmetodikens grunder: att planera, genomföra och rapportera en undersökning*, (Lund: Studentlitteratur, 1991).

Prunckun, Hank. *Counterintelligence – Theory and practice*, uppl. 2, (London, UK: Rowman & Littlefield, 2019).

Riehle, Kevin P. Russia's intelligence illegals program: an enduring asset, *Intelligence and National Security,* vol. 35, nr. 3, 2020, 385-402.

Riehle, Kevin P. Wilson Center, 2023, *The History and Continuing Relevance of Soviet Bloc Illegal Intelligence Operatives*
https://www.wilsoncenter.org/blog-post/history-and-continuing-relevance-soviet-bloc-illegal-intelligence-operatives [hämtad 2024-05-22]

Säkerhetspolisen 2023/2024. *Lägesbild Kontraspionage – Sänkt tröskel hos främmande makt.* SÄPO. https://sakerhetspolisen.se/om-sakerhetspolisen/publikationer/sakerhetspolisens-arsberattelse/sakerhetspolisen-2023-2024/verksamhetens-lagesbilder/lagesbild-kontraspionage.html [hämtad 2024-26]

Säkerhetspolisen. *Säkerhetspolisens uppdrag.* SÄPO. https://sakerhetspolisen.se/om-sakerhetspolisen/sakerhetspolisens-uppdrag.html [hämtad 2024-05-26]

Teorell, Jan & Svensson, Torsten , *Att fråga och att svara - Samhällsvetenskaplig metod,* (Slovenien: Liber, 2007), s. 27.

Wirtz, James J. "Hiding in Plain Sight: Denial, Deception, and the Non-State Actor", *The SAIS Review,* vol. 24, nr, 3, 2008, s. 55-63.