Cyberhot inifrån?

En studie om otillåtna registerslagningar, myndighetspersonal och Natomedlemskap

Av Clara Antlöv & Julia Forssén

LUNDS UNIVERSITET
Rättssociologiska institutionen

Kandidatuppsats (RÄSK02)
Vårterminen 2024

Handledare: John Woodlock

Examinator: Patrik Olsson

Förord

Denna kandidatuppsats markerar slutet på vår tid på kandidatprogrammet i kriminologi, med inriktning rättssociologi, vid Lunds universitet. Det har varit tre lärorika år som gett oss möjligheten att bredda våra akademiska kunskaper och vår förståelse för disciplinen.

Inledningsvis vill vi rikta ett stort tack till studiens respondenter som tog sig tid och deltog i intervjuer som bidrog till spännande infallsvinklar i arbetet. Utan era insikter hade inte denna studie varit möjlig.

Vidare vill vi uttrycka en djup tacksamhet till vår handledare John Woodlock, som bidragit med stöd och hjälp under hela processen. Din expertis och ditt engagemang har varit en ständig källa till inspiration och vägledning.

Slutligen vill vi rikta ett stort tack till alla våra studiekamrater, vänner och varandra. Ni har gjort denna studietid både givande och minnesvärd. Er vänskap har varit ovärderlig.

Stort tack!

Clara Antlöv & Julia Forssén
Maj 2024, Lund

Abstract

The ever-increasing digitalization of the world sees the emergence of new threats that result in increasingly high demands on nations regarding the maintenance of national cybersecurity. Meanwhile, recent conflicts in Europe have placed Sweden in a new political security situation where, since March 2024, Swedish NATO membership is now a reality. Despite the significance of national security issues, a high frequency of unauthorized database accesses has been detected within Swedish authorities and have been subsequently dealt with through the Swedish courts. Therefore, this essay aimed to investigate this phenomenon by formulating research questions focusing on perceptions of state employed actors regarding legislation on unauthorized access, and potential implication of Sweden's NATO membership. To achieve the study's purpose, a qualitative approach was applied, consisting of eight interviews with government personnel, six of whom worked within the police authority, one in a district court, and one in the enforcement authority. The transcripts were analyzed through application of previous research and a theoretical framework consisting of legitimacy theory and new institutional theory. The study's findings indicated that the occurrence of unauthorized database accesses was expected to adversely affect the legal security and legitimacy of government agencies by reducing public trust. NATO membership was not expected to have any effects on the occurrence of unauthorized database accesses. Notwithstanding, as the threat landscape could change, respondents emphasized the importance of cooperation to strengthen Swedish cybersecurity. It was highlighted that maintaining legality and trust within government operations becomes essential in a changed security policy context.

Nyckelord: cybersäkerhet, legitimitet, myndighet, Nato, olovlig registerslagning

Antal ord: 14 702

Innehållsförteckning

1. Inledning

I det inledande avsnittet presenteras en introduktion för studiens valda ämnesområden som vidare specificeras med hjälp av en problemformulering bestående av tre nivåer. Därefter framhävs studiens syfte och frågeställningar, som följs av en motivering av undersökningens rättssociologiska relevans, och avslutningsvis ges en beskrivning av studiens avgränsningar.

1.1 Introduktion

Världen är i omvandling. Den teknologiska utvecklingen och digitaliseringen har lett fram till industriella möjligheter att förbättra levnadsstandarden hos människor världen över (Montasari 2023, s.1-2). Men fördelarna har inte kommit ensamma. Bakom dessa fördelar ligger en komplex verklighet där den snabba utvecklingen inte bara har revolutionerat vårt sätt att leva, utan också öppnat dörrar för nya former av hot och kriminalitet som utmanar den globala säkerheten (ibid.). Dagens cyberhot är således ett resultat av ett allt kraftfullare teknologiskt framträdande som tillgängliggjort nya metoder och tillvägagångssätt för aktörer med kriminella avsikter (Montasari 2024, s.2). I en tid där cyberrelaterade hot är alltmer påtagliga står nationer inför en gemensam utmaning, att anpassa strategier och policy i takt med ett allt större beroende av den nya teknologin (Kelly & Montasari 2023, s.97-99; Warner 2023, s.107).

I svensk kontext har politiska händelser satt landets säkerhet på spel då Rysslands invasion av Ukraina kastat en skugga över närområdet och frammanat omvärdering av dennes försvar (Försvarshögskolan 2023, s.71, 102-103). Med ett nyligen inrättat Natomedlemskap står Sverige inför nya utmaningar och möjligheter att stärka sitt totalförsvar, där cybersäkerhet spelar en avgörande roll (Lundin & Magnusson 2022, s.68-69). För att skydda den nationella säkerheten krävs en förståelse för det juridiska ramverk som styr bekämpning av cyberhot, och genom att utveckla och anpassa lagstiftning går det att stärka försvaret och säkra samhällsviktiga tjänster från potentiella intrång (ibid.). Däremot har tendenser i form av ett ökat antal dataintrång relaterade till svenska myndigheter (BRÅ 2022, s.32; Lindskog, Huuva, Lehtinen & Shannon 2022, s.42, 76; se bilaga 1), blottat vad som

väcker frågor om ett potentiellt, tidigare förbisett, hot (Stoddart 2022, s.353-355). Frågor om ett hot som skulle kunna utgöras av brister inom den svenska statens kärnverksamhet. Frågor om ett hot som kan komma inifrån.

1.2 Problemformulering

1.2.1 Cyberhot, ett internationellt fenomen

Cyberhotet och fenomenets globala påtaglighet, respektive tillhörande utmaningar, är idag en internationell gemensam nämnare (Montasari 2023, s.1-2), vilken förståelse för dess breda problematik förespråkar en närmare konkretisering och definiering. *National cyber security centre* (NCSC 2016) definierar cyberattacker som "försök att skada, störa eller få obehörig åtkomst till datasystem, -nätverk eller -utrustning". Cybersäkerhet definieras vidare handla om skyddet av sådana system, nätverk och utrustning, respektive den information dessa innehåller, från obehörig åtkomst eller förstörelse (ibid.). Fortsättningsvis gör Stoddart (2022, s.353-355) ansats till karaktärisering av hotaktörer kopplade till cyberangrepp, och gör här en uppdelning mellan utomstående hot respektive hot inifrån, varav hotaktörerna som angriper inifrån kan handla om underrättelseagenter som agerar infiltratörer, men inkluderar också anställda inom organisationer exempelvis.

1.2.2 Cybersäkerhet i en svensk kontext

Närtidens säkerhetspolitiska utveckling har satt det svenska totalförsvaret på prov och under dessa omständigheter blir bland annat Sveriges förmåga inom cyberområdet en kritisk punkt för den nationella säkerheten (Lundin & Magnusson 2022, s.68-69). För att minska den svenska sårbarheten för cyberangrepp och -intrång krävs en kompetenshöjning inom flera områden, däribland verksamhetsmässigt, tekniskt samt juridiskt, för att kunna bevara god funktion hos samhällsviktiga tjänster som måste kunna motstå och förebygga missgynnande skeenden för cybersäkerheten (ibid.).

1.2.3 Olovliga registerslagningar inom svenska myndigheter

För att fortsatt se till en del av den juridiska grund genom vilken upprätthållande av svensk cybersäkerhet eftersträvas, kan uppmärksamhet riktas mot den straffbestämmelse

återfunnen i 4 kap. 9 c § Brottsbalken (BrB) (SFS 1962:700) som gäller vid dataintrång. Som bakgrund för utvecklingen av lagrummet har EU:s rambeslut "Rådets rambeslut 2005/222/RIF av den 24 februari 2005 om angrepp mot informationssystem" (EUT L 69 16.03.2005) förelegat, vilket antogs av Sverige år 2004 (Prop 2003/04:164). EU:s rambeslut betonar vikten av fungerande skydd gentemot informationssystem, såsom attacker mot kritisk infrastruktur, och lyfter vidare angelägenheten om straffrättsligt försvar och internationellt samarbete (Träskman & Wennberg 2019, BrB 4:9 c s.2; Prop. 2003/04:164, s.7). Med utgångspunkt i den tidigare utvecklingen av straffbestämmelsen, anses det intressant att undersöka hur ett svenskt Natomedlemskap eventuellt kan medföra behov till ytterligare reformering av den befintliga lagstiftningen.

Efter att ha beställt domar från Sveriges tingsrätter i syfte att studera karaktären av dataintrång och dennes lagföring, identifierades olovliga registerslagningar som en av de mest behandlade gärningarna med brottsrubricering dataintrång. Bland de identifierade domarna förekom otillåtna registersökningar inom statliga myndigheter där en person blivit åtalad för dataintrång (se bilaga 1). Karaktäriserande för brottskoden är att den vanligtvis utförs av en person som genom sin yrkesroll bereder sig tillgång till information tillhandahållet ur datasystem som denna är obehörig (BRÅ 2022, s.32). Således kan dessa antas möjliggöra en förklaring genom en inkludering i den kategori av cyberhot som Stoddart (2022, s.353) menar härleds från angreppssätt inifrån. Vidare har detta, efter granskningen av domarna, uppenbarats ske inom viktiga verksamheter såsom sjukvården och Polismyndigheten, som har kritiska funktioner för samhället och således blir särskilt angelägna att skydda från intrång ur en cyberrelaterad säkerhetssynpunkt (Lundin & Magnusson 2022, s.68-69; Stoddart 2022, s.3-4).

1.3 Syfte och frågeställning

Syftet med studien är att undersöka svenskt cyberförsvar och -säkerhet samt den rättsliga kapaciteten inom området genom att se till kontexten av ett svenskt Natomedlemskap, och hur detta kan påverka Sveriges roll i upprätthållandet av nationellt cyberförsvar. Här föreslås en inriktning på svensk lagstiftning kring dataintrång, vilket efter att ha studerat

domar från Sveriges tingsrätter visats vara förekommande i form av olovliga slagningar genomförda inom myndigheter. Därmed motiveras ett inifrån-ut perspektiv där det ses till försvarspotential gentemot inhemska aktörer, till skillnad från det som generellt fått mest fokus, angrepp mot Sverige utifrån, från främmande makt (Stoddart 2022, s.353-355). Till följd av studiens syfte presenteras nedan de frågeställningar som studien förhåller sig till:

- Hur uppfattar aktörer inom svensk brottsbekämpande myndighetsverksamhet olovliga registerslagningar i relation till legitimitet och rättssäkerhet?

- Vilka förväntade rättsliga effekter tror brottsbekämpande myndighetspersonal att Sveriges Natomedlemskap kan ha på cybersäkerheten och förekomsten av olovliga registerslagningar inom myndigheter?

Brottsbekämpande myndigheter syftar på myndigheter som bland annat arbetar med att upprätthålla allmän ordning, verkställa straffpåföljder samt förebygga och bekämpa brottslighet (Integritetsmyndigheten 2023). I studien refereras aktörer inom brottsbekämpande myndigheter till anställd personal hos en sådan myndighet. Val av respondenter motiveras vidare under "5.3.1 Urval".

Legitimitet åsyftar i studien till Tylers (2022, s.761) definition av begreppet, vilken beskriver hur allmänna sociala värdeuppfattningar av en auktoritet blir avgörande för regelefterlevnad, och beskrivs vidare under rubrik "4.1 Legitimitetsteori".

Åklagarmyndigheten (u.å) beskriver rättssäkerhet som att ett land har ett rättssystem med lagar och regler som skyddar samhällets medborgare från ingrepp utöver lagens befogenhet. Denna beskrivning av begreppet används vidare i studien.

1.4 Rättssociologisk relevans

Studiens rättssociologiska relevans kan kortfattat beskrivas genom undersökningens fokus på hur subjektiva uppfattningar formar människors inställning till lagen samt hur detta kan

påverka regelefterlevnad i relation till legitimitet (Baier, Svensson & Nafstad 2018, s.74-76). För att vidare illustrera detta aktualiseras relationerna mellan rättssociologins fyra byggstenar i form av kodifierad statsrätt, rättslig praxis, sociala normer och social praxis (ibid., s.13-14).

Vid undersökning av myndighetsaktörers uppfattningar om olovlig registerslagning och dess förekomst inom myndigheter, utgörs den rättssociologiska relevansen av relationerna mellan kodifierad statsrätt och sociala normer, samt kodifierad statsrätt och social praxis (Baier, Svensson & Nafstad 2018, s.18-20). Relationerna mellan byggstenarna behandlar den formella rättens förmåga att influera normer och moral, men även det direkta handlandet, och synliggörs således i den delen av studiens syfte som ämnar se till myndighetspersoners uppfattning kring praxis kopplat till olovliga registerslagningar. I studiet av huruvida människor uppfattar gällande lagstiftning som rättmätig är begreppet *legitimitet* av stor relevans eftersom det är, utifrån ett normativt perspektiv, avgörande för hur individen väljer att följa lagen respektive inte (ibid., s.74).

När aktörernas individuella uppfattningar sedermera sätts i relation till Natomedlemskapet och alliansens potentiella innebörd för svensk rättskultur, samt synen på olovliga slagningar och berörd lagstiftning, tillförs en ytterligare dimension av rättssociologisk relevans. Här aktualiseras relationen mellan sociala normer och kodifierad statsrätt, eftersom denna relation utgör det område vilket ger täckning för studiet av människors uppfattningar om rätt handlande och dessa normers eventuella diskrepans till vad som är formaliserat i lagen (Baier, Svensson & Nafstad 2018, s.17).

1.5 Avgränsningar

Med hänsyn till studiens omfattning och tidsomfång har avgränsningar motiverats nödvändiga (Bryman 2018, s.33, 363). Initialt har en geografisk avgränsning gjorts till Sverige eftersom cybersäkerhet är ett globalt påtagligt fenomen, varav en sådan studie kräver omfattande resurser för att uppnå en större geografisk täckning. Vidare har arbetets intresse för studiet av cybersäkerhet preciserats genom att se till ett specifikt lagrum där

dataintrång fått stå i fokus. Denna avgränsning motiveras utifrån att lagstiftningen gällande dataintrång antas betydande inom ämnet eftersom lagens formalisering har grundats i strävan att uppnå ökad säkerhet för Sveriges informationssystem genom "Europaparlamentet och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF" (EUT L 218, 14.08.2013).

Fortsatt fokus på olovliga registerslagningar inom lagrummet motiveras i att dessa brott identifierades som en framträdande tendens i begärda och studerade tingsrättsdomar med brottsrubriceringen dataintrång. Vidare har granskning av dessa domar härlett avgränsning till ett fokus på olovliga slagningar inom myndigheter eftersom denna förekomst var påfallande inom brottstypen, samt då myndighetsverksamhet utgör en viktig del av den svenska staten (Regeringskansliet 2023). Fortsatt har endast uppfattningar om brottstypen hos brottsbekämpande myndighetsverksamma undersökts då dessa antogs betydande vid studiet av nationell cybersäkerhet, som i sin tur skapade relevans i kontextualiseringen med hjälp av det svenska Natomedlemskapet.

2. Bakgrund

I avsnittet för bakgrund presenteras ett djupare underlag för studiens valda forskningsområde. Inledningsvis presenteras dataintrång som brottstyp och dess bestämmelse i brottsbalken, samt olovlig registerslagning som brottskod. Därefter ges en beskrivning av Nato och Sveriges inträde i alliansen, följt av Natos riktlinjer kring cybersäkerhet och avslutningsvis ett avsnitt om det svenska totalförsvaret med särskilt fokus på myndigheternas roll inom det civila försvaret.

2.1 Dataintrång som brottstyp

Bestämmelserna kring dataintrång formuleras i 4 kap. 9 c § BrB enligt följande:

> Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.
>
> Är brottet grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art (4 kap. 9 c § BrB).

Lagrummet infördes först i brottsbalken genom att den då kallade datalagen (SFS 1973:289) ersattes med personuppgiftslagen (SFS 1998:204; Träskman & Wennberg 2019, BrB 4:9 c s.1). Det tidigare lagrummets straffbestämmelse överfördes utan ändringar, vilka sedermera saknade en mer genomgripande översyn av dator- och datarelaterade gärningar (Träskman & Wennberg 2019, BrB 4:9 c s.1). Detta resulterade vidare i en rad förslag kring reglering av oberättigade dataförfaranden vilka bidrog till utvecklandet av dagens formulering av bestämmelserna kring dataintrång. Väsentliga ändringar i straffbestämmelsen har gjorts med grund i EU:s rambeslut (EUT L 69 16.03.2005). Syftet med rambeslutet var att närma sig en harmonisering av medlemsländernas lagstiftning gällande dessa angrepp för att i sin tur kunna bidra till bättre samarbete mellan myndigheter över nationella gränser (Träskman & Wennberg 2019, BrB 4:9 c s.2; Prop. 2003/04:164, s.7). Det är i huvudsak Europarådets konvention om IT-relaterad brottslighet som varit vägledande för angivelserna i rambeslutet (Dir. 2011:98, s.7). Sverige antog rambeslutet 2004 med grund i förslag framlagt i Prop. 2003/04:164. Antagandet har sedermera härlett två ändringar i svensk lagstiftning, vilka föreslogs via Prop. 2006/07:66 respektive Prop. 2013/14:92, och som blir relevanta inslag i den utvecklingen som gett upphov till dagens straffbestämmelser om dataintrång.

I Prop. 2006/07:66 (s.1) övervägdes behovet av lagändringar med intentionen att förverkliga EU:s ramsbeslut (EUT L 69 16.03.2005) i relation till befintliga straffbestämmelser. Här identifierades ett utvidgat straffansvar som nödvändigt för Sveriges möjligheter att uppfylla det åtagna rambeslutet (Prop. 2006/07:66, s.1). Således utvidgades

dataintrångsbestämmelsen år 2007 till en omfattning där straffansvar följer den som olovligen blockerar en uppgift som är avsedd för automatiserad behandling, eller den som olovligen allvarligt stör eller hindrar användningen av en sådan uppgift (Träskman & Wennberg 2019, BrB 4:9 c s.6). Även försök och förberedelse till sådana brott medför därmed straffansvar (Prop. 2006/07:66, s.1). I Prop. 2013/14:92 framfördes vidare förslag om skärpt straff för dataintrång genom implementeringen av Europaparlamentet och rådets direktiv gällande angrepp mot informationssystem (EUT L 218, 14.08.2013), och hur en straffskärpning skulle innebära att Sverige uppfyller direktivets krav. Således föreslogs en gradering av dataintrång där en bestämmelse om grovt dataintrång inkluderades i brottsbalken (Prop. 2013/14:92). År 2014 trädde den nya bestämmelsen i kraft och blev en del av svensk rätt (SFS 2014:302), vilket utgör den senaste ändringen som gjorts i lagrummet behandlande dataintrång.

2.1.1 Olovlig registerslagning

Dataintrång är en bred brottstyp som omfattar flera kategorier av handlingar, varav olovlig registerslagning är en av dessa brottskoder tillsammans med överbelastningsattack, skadlig kod i utpressningssyfte, intrång i sociala medier och e-tjänster samt övrigt dataintrångsbrott (BRÅ 2022, s.32; Lindskog et al. 2022, s.9-10). BRÅ (2022, s.32) förklarar dataintrång genom olovlig registerslagning när en person, med tillgång till register- eller datasystem inom sin tjänst, genomför en informationssökning som överskrider den anställdes befogenhet. Om inte personen hade en anledning att söka i registret, i relation till dennes arbetsuppgifter och tjänsteutövning, är informationssökningen otillåten och kan således tolkas som dataintrång enligt 4 kap. 9 c § BrB (BRÅ 2022, s.32; Lindskog et al. 2022, s.42).

Till skillnad från andra brottskategorier inom dataintrång där det är svårt att fastställa en identitet på den som utfört handlingen, kan olovlig registerslagning oftast knytas till en skäligen misstänkt eftersom gärningspersonen vanligtvis genomför brottet på sin arbetsplats genom inloggning i arbetsplatsens IT-system (Lindskog et al. 2022, s.12). Olovliga registerslagningar förekommer inom olika verksamheter, exempelvis sjukvården, Kriminalvården, Socialtjänsten och Polismyndigheten (ibid., s.42-43). Av de polisanmälda

ärendena som Lindskog et al. (ibid., s.43) granskat gällande dataintrång, konstateras att en tredjedel av de förekommande olovliga registerslagningarna har begåtts inom Polismyndigheten.

Sandén (se Svensson 2023), som är jurist vid Polismyndigheten, framhäver att både effektiviteten och rättssäkerheten hos polisen drabbas när de upplever en tvetydighet i huruvida aktörerna får göra registerslagningar eller inte. Svensson (2023) är jurist samt redaktionschef för JUNO nyheter och belyser att domar angående dataintrång mot poliser visar på en tvetydig praxis. Författaren beskriver Polismyndighetens riktlinjer (PM 2017:4 se Svensson 2023) i form av att en sökning måste tolkas som nödvändig i relation till det arbete som ska utföras. Samtidigt är olika instanser av rätten inte eniga i hur det ska tolkas, exempelvis framhävs att tingsrätter generellt tenderat att fria på grund av den bristande beskrivningen, samtidigt som hovrätten i ett senare skede har fällt flera rättsfall som överklagats från tingsrätten (Svensson 2023).

2.2 Sverige och Nato

NATO står för *North Atlantic Treaty Organization* och är en allians med syfte att bevara fred för alliansens medlemmar (MSB 2024). Natos organisation är ett internationellt samarbete och består av dels en politisk, dels en militär del, men som gemensamt syftar till att tillgodose dess medlemmar med garanterad frihet och säkerhet (Regeringskansliet 2024a). Det Nordatlantiska fördraget består av 14 artiklar och utgör försvarsalliansens grundläggande stadga. Av fördragets artiklar framhävs artikel ett, tre och fem som särskilt viktiga (MSB 2024). Artikel ett understryker vikten av fredlig konfliktlösning, däremot anses artikel tre och fem av störst relevans för denna studie med hänvisning till dess betoning på det nationella och kollektiva försvaret och är således de enda artiklarna som beskrivs ingående. Den femte artikeln framhäver betydelsen av det kollektiva försvaret som innebär att ett utfört angrepp mot ett medlemsland inom Nato, ses som ett angrepp mot hela alliansen. Således har alla medlemsländer ett gemensamt ansvar att försvara alliansens medlemsländer (ibid.). Artikel tre i fördraget framhäver kravet på att medlemsländerna inom Nato ska ha förmåga att skydda både sig själva och bidra till det kollektiva försvaret,

vilket utöver den militära delen inom totalförsvaret även inkluderar en civil del som ställer krav på civilt försvar i form av upprätthållande av viktiga samhällsfunktioner (MSB 2024; Prop. 2022/23:73, s.14).

Efter granskning av Sveriges säkerhetsläge efter Rysslands invasion av Ukraina år 2022 gjordes en bedömning om ett försämrat säkerhetsläge som medförde säkerhetspolitiska konsekvenser för Sverige (Prop. 2022/23:74, s.8, 12). Med bakgrund av det försämrade säkerhetsläget gick Sverige med i Nato den sjunde mars år 2024, vilket medför att Sverige är en del av det nordatlantiska fördraget och dess artiklar (Regeringskansliet 2024b). Det innebär i sin tur att Sverige innehar ett solidariskt ansvar för Natos säkerhet och blir en del av alliansens operationsplanering och ska bidra med försvarsåtgärder (Prop 2022/23:74, s.24). Vidare anses Natos kompetens i att hantera cyberhot som en viktig komponent för att avskräcka brottslighet och stärka försvaret (ibid., s.17).

2.2.1 Nato och cyberförsvar

Inom Nato betonas ett ökat cyberhot, med en komplex och destruktiv karaktär, som resultat av teknikens ökade framväxt. En del av Nato innefattar således en kollektiv förmåga att stärka alliansens cyberförsvar där länderna måste förbereda sig för att bemöta kommande cyberhot (Nato 2023). Nato verkar för att allierade ska utveckla informationsutbyte mellan medlemsländerna och ett ömsesidigt stöd mellan aktörerna för att utveckla kunskap om hur länderna kan förebygga, hantera och återhämta sig från cyberattacker. Informations- och kunskapsspridning, övningar inom cyberförsvar och upplysning av bäst praxis inom området är några av de möjligheter som Nato hjälper de allierade med (ibid.).

De allierade länderna inom Nato har det primära ansvaret att nationellt upprätta stabilt cyberförsvar, men eftersom Natos medlemmar är delar av en större allians är det till alliansens fördel att Nato stödjer ländernas nationella cyberförsvar. Vidare har Nato klargjort att en eventuell cyberattack kan medföra att artikel fem aktiveras (Prop. 2022/23:74, s.15; Stoltenberg 2019, s.27). Enligt Lindstrom och Luiijf (2012, s.50) är det av stor vikt att både studera intern och extern säkerhet eftersom riskfaktorer inte

nödvändigtvis endast kommer utifrån. Vidare framhävs att en del nationer är i behov av att stärka sin interna cybersäkerhet genom en nationell säkerhetsstrategi för att således kunna stärka den externa säkerheten (ibid., s.51).

2.3 Sveriges totalförsvar

Det centrala målet för det svenska totalförsvaret är att upprätthålla god samordning och samarbetsförmåga för att möjliggöra ett så tryggt försvar som möjligt (Försvarshögskolan 2023, s.7). Totalförsvaret blir aktiverat i samband med att det fattas ett beslut om höjd beredskap från Sveriges regering, vid fredstider arbetar de berörda aktörerna med att planera och upprusta totalförsvaret (ibid., s.119, 122). Totalförsvaret består både av en militär och en civil del, där det civila försvaret omfattar bland annat statliga myndigheter, kommuner och företag som har till uppgift att exempelvis upprätthålla viktiga samhällsfunktioner, bibehålla en nödvändig försörjning och tillföra det militära försvaret stöd i största möjliga mån (ibid., s.122, 124).

Beredskapsmyndigheter är myndigheter som arbetar under regeringen och innehar ett större ansvar för specifika samhällsfunktioner i relation till totalförsvaret och krisberedskap. Exempel på några av dessa myndigheter är Polismyndigheten och Domstolsverket (Försvarshögskolan 2023, s.137-138). Bennesved, Ingemarsdotter och McWilliams (2023, s.2-3) konstaterar att det civila försvaret finansieras på en nationell nivå, således antas att den nationella civila beredskapen inte drastiskt kommer att påverkas av ett Natointräde, förutom den generellt avskräckande aspekten som antas medföra ett inträde i försvarsalliansen. Istället betonas att det med största sannolikhet kommer påverka det nordiska samarbetet för civilt försvar, vilket följaktligen kommer påverka Natos avskräckningsförmåga på längre sikt (ibid., s.4), där avskräckning syftar på tillvägagångssätt för att genom hot förhindra oönskade handlingar (Sörensen 2023, s.1).

3. Tidigare forskning

I avsnittet för tidigare forskning presenteras en litteraturöversikt med syfte att öka kunskap om den forskning som är befintlig inom ämnesområdet. Inledningsvis introduceras litteratursökningens tillvägagångssätt och därefter presenteras det valda materialet i en deskriptiv analys som följs av en tematisk analys.

3.1 Tillvägagångssätt

För att kartlägga den kunskap som finns inom ämnesområdet för studien har en litteraturöversikt genomförts. En litteraturöversikt ämnar att framhäva begrepp, teorier och sammanställningar som är relevanta inom forskningsfältet för att skapa en övergripande bild över vad som undersökts och nyttjade tillvägagångssätt (Lindstedt 2019, s.187; Hart 2018, s.3). Inledningsvis gjordes initiala sökningar på olika databaser med avsikt att få generell information om det valda ämnet för att i sin tur kunna centrera sökningen på det som uppfattades som mest relevant (Hart 2018, s.3). De slutgiltiga sökningarna gjordes sedan i databaserna LUBsearch och SCOPUS.

I förhållande till studiens syfte och frågeställning valdes sökord ut för att anpassa sökningens relevans (Lindstedt 2019, s.173). Efter initiala sökningar drogs slutsatsen att svenska ord inte gav resultat, således valdes engelska termer ut i form av: *cybersecurity*, *NATO*, *authority* och *law** med tillhörande synonymer, som slutgiltiga sökord. Genom att använda booleska operatorer som *AND* och *OR*, kunde sökningen begränsas, utvidgas och kombineras för att finna relevant material (ibid., s.175). Utöver de booleska operatorerna användes trunkering i form av *(*),* vilket medförde att sökningen gav träffar på ord som innehöll varianter av det ursprungliga ordet (ibid., s.178). Sökorden delades in fyra block där orden inom respektive block kombinerades med *OR* och sedan kombinerades de fyra blocken i en gemensam sökning med *AND*. Sökblocken presenteras i tabell 1.

Slutgiltig sökning			
Block 1	Block 2	Block 3	Block 4
Cybersecurity *Cyber security* *Data security* *datasecurity*	*NATO*	*Authority* *Authorities* *Police* *Military* *Prosecutor* *Judge* *The security police*	*law** *Legislative* *Legal*

Tabell 1. Sökord

I LUBsearch sorterades publikationerna utifrån *Peer-reviewed*, *Academic journals*, engelska som språk och tillgång via bibliotekets samling. Sökningen i LUBsearch, med valda filter, resulterade i tio resultat den 26:e mars 2024 då sökningen genomfördes. I SCOPUS fanns möjlighet att applicera fler filter för att begränsa sökningen, således begränsades sökningen till *Social science, Article, Open access*, engelska som språk och där sökorden fanns i publikationens titel eller *abstract*. Sökningen i SCOPUS resulterade i 35 sökresultat den 27:e mars 2024. Gemensamt resulterade sökningarna i LUBsearch och SCOPUS i 45 resultat. För att begränsa antalet artiklar gjordes en relevansbedömning utifrån artiklarnas *abstract* (Bryman 2018, s.144; Urinboyev, Wickenberg & Leo 2016, s.527), vilket resulterade i 29 resultat. För att minska antalet artiklar ytterligare gjordes en andra relevansbedömning utifrån artiklarnas fulltext (Bryman 2018, s.144; Urinboyev, Wickenberg & Leo 2016, s.528). Efter den andra relevansbedömningen reducerades antalet artiklar till 20 stycken.

Eftersom tidigare sökningar inte gav träffar på forskning i en svensk kontext, gjordes en ytterligare sökning i LUBsearch med *swed** som nyckelord och relaterades till *cybersecurity*, *authority* och *legitimacy,* i olika kombinationer med tillhörande synonymer, vilket gav resultat på forskning om myndighetsverksamhet i en svensk kontext. Dessa sökningar, som resulterade i två utvalda artiklar, utgör ett tillägg till studiens tidigare sökningar. Slutligen ligger därför 22 artiklar till grund för studiens tidigare forskning, vilket presenteras i en deskriptiv analys och vidareutvecklas i en tematisk analys.

3.2 Deskriptiv analys

En deskriptiv analys tillämpades i syfte att presentera en överblick av det för studien utvalda vetenskapliga underlaget (Urinboyev, Wickenberg & Leo 2016, s.522, 529). Kriterierna författare, år, språk, geografisk avgränsning samt nyckelord, har valts ut för att beskriva en översiktlig presentation av publikationernas huvudsakliga karaktärsdrag (se bilaga 2).

3.3 Tematisk analys

Den tematiska analysdelen utgörs av en form av innehållsanalys, som är en metod för att systematiskt bryta ner och kategorisera ett textinnehåll i syfte att besvara specifika forskningsfrågor (Boréus & Kohl 2018, s.50). Utifrån denna analysmetod möjliggjordes sedermera identifiering av frekvent förekommande teman i det underliggande vetenskapliga materialet som sedan kodades (Bryman 2018, s.702). Kodningen har i sin tur urskiljt begrepp och fraser vilka motsvarar översättningar på texternas identifierade teman (ibid.). Med hjälp av denna metodik identifierades, vid granskning av studiens tidigare forskning, två huvudteman i form av “Samarbete” och “Legitimitet”.

3.3.1 Samarbete

Cybersäkerhet är en flerdimensionell utmaning som sträcker sig över flera domäner och sektorer, såväl inom nationer som internationellt (Devanny, Goldoni & Medeiros 2022, s.44). Komplexiteten inom området medför att det är omöjligt att inneha kunskap som omfattar hela disciplinen (Venables 2021, s.1). För att fatta välgrundade beslut gällande cyberrelaterad säkerhet och skydd krävs sålunda en samlad ansträngning och ett

kunskapsutbyte av både nationella och internationella samarbeten (Venables 2021, s.5; Devanny, Goldoni & Medeiros 2022, s.44). Således antas olika former av partnerskap på alla nivåer vara en viktig komponent för att öka motståndförmågan gentemot cyberhotet (Semenenko, Dobrovolsky, Sliusarenko, Levchenko & Mytchenko 2023, s.193).

Napetvaridze och Chochia (2019, s.176) framför internationellt samarbete som en viktig aspekt i att skapa förståelse och kunskap kring vad som behöver anpassas i förhållande till en miljö som konstant ändras. Genom globalt samarbete och kunskapsutbyte gällande exempelvis framgångsrika insatser medkommer möjligheter att utveckla effektiva tekniker, strategier, försvarsprogram, samt stärka sina resurser inom cybermiljön (Semenenko et al. 2023, s.192; Komalasari & Mustafa 2023, s.337). Genom en internationell utformning av nya rättsområden, praxis och lösningar skapas nya policyområden (Willers 2021, s.539), vilket blir viktigt i utformandet av gemensamma strategier, tillvägagångssätt och tolkningar för att en enhetlig internationell bekämpning av cyberhot ska vara möjlig (Condrut 2023 se Semenenko et al. 2023, s.195; Devanny, Goldoni & Medeiros 2022, s.35, 41-42).

Det lyfts vidare att det däremot finns en avsaknad av internationellt samarbete för att gemensamt bygga en standard för cybersäkerhet, vilket innefattar behov av gemensamma normer för beteenden, handlingsåtgärder, utbyte av kunskap samt utveckling av en global strategi för cybersäkerhet (Shopina, Dmytro, Khrystynchenko, Zhukov & Shpenov 2020, s.985). Med asymmetriska kunskapslägen och bristande förståelse mellan stater inom den globala sfären, kompliceras sålunda beslutsprocessen rörande internationella bemötanden av cyberoperationer (Devanny, Goldoni & Medeiros 2022, s.34-35). Dessa brister i informationsdelning och internationellt normskapande försvagar den totala cybersäkerheten och ansträngningarna för att uppnå denna, och således lämnas den globala cyberarenan med en ökad sårbarhet för angrepp (Komalasari & Mustafa, s.337). Som en del av en lösning på sådan problematik lyfts fördelarna med internationella försvarsallianser såsom Nato (Gao & Chen 2022, s.699).

Ett ökat samarbete som erbjuds genom medlemskap i Nato kan förbättra förmåga och kompetens i cybersäkerhetsfrågor (Gao & Chen 2022, s.699-700; Pleta, Karasov & Jakštas 2018, s.568, 576). Detta genom att erbjuda samordning av åtgärder för cyberförsvar genom ett centralt maktmedel vilket i sin tur leder till ett effektivare skydd (Ilie, Mutulescu, Artene, Bratu & Fainsi 2011, s.440; Jacuch 2021, s.110). Cybersäkerhet är av hög prioritet inom Nato (Efthymiopoulos 2019, s.23), och medlemskapet i allianser medför möjlighet till utvecklandet av nationella säkerhetsintressen, men också delaktighet i stärkandet av de medallierade ländernas cybersäkerhet (Givens, Busch & Bersin 2018, s.14).

Att inneha position som medlemsstat i Nato innebär sålunda visst ansvar i förhållande till alliansens säkerhet och försvarsförmåga i stort, och på så sätt kan högre krav förväntas på den nationella säkerheten hos medlemsländerna (Givens, Busch & Bersin 2018, s.14). I dagens diskurser gällande cybersäkerhet går det inte att bortse från staten, individer samt föreningar eller företag som viktiga intressenter (Lobato & Kenkel 2015, s.23-24). Dessutom är statens roll inom cybersäkerhet till viss del begränsad eftersom området är en del av både den offentliga och privata sektorn. Statliga sanktioner och åtgärder för att upprätthålla cybersäkerhet kan således begränsa grundläggande fri- och rättigheter (ibid., s.38-39).

Den privata sektorn, i form av individer eller företag, belyses därför som viktiga aktörer i arbetet för att motverka cyberhoten, däremot kan de även välja att införa dem utan en vidare koppling till en statsmakt (Lonardo 2021, s.1096). Att samarbeta med den privata sektorn utgör en viktig del av långsiktiga åtgärder och är något som därför har uppmärksammats av EU-kommissionen (ibid.). Genom kommunikation och samarbete skapas förståelse för befintliga behov hos företag och kontroll av att cybersäkerhet hos företag byggs upp på korrekt sätt (Napetvaridze & Chochia 2019, s.176-177).

Tasevski (2015, s.8) föreslår vidare inrättandet av en cybersäkerhetskultur som involverar kampanjer och projekt som innefattar kunskapsspridning och utbildning. Kunskap bör även fördelaktigt spridas till professioner som arbetar inom IT, men även andra professioner som är i behov av kunskap. Således förespråkas ett ökat samarbete med utbildningsinstitut som

dels utbildar specialister, dels tar fram eller ändrar befintliga säkerhetsprogram som anpassas efter befintliga behov (Napetvaridze & Chochia 2019, s.176; Pravdiuk 2022, s.21). Genom att sprida kunskap om tekniker och förbättra samarbete mellan olika aktörer inom akademin, offentliga och privata organisationer kan följaktligen försvaret bli starkare (Lobato & Kenkel 2015, s.35; Carrapico & Farrand 2017, s.260).

3.3.2 Legitimitet

Hur staten hanterar bemötandet av cyberbrottslighet och hur bemötandet uppfattas hos befolkningen är ett ytterligare tema som återfinns i studiens valda artiklar. Inledningsvis kan den studie som Devanny, Goldoni och Medeiros (2022, s.34) genomfört, gällande svårigheterna med att främja brett godkännande av attribution i relation till effekterna med strategiska cyberoperationer, uppmärksammas. Om den egna statens förmåga inte upplevs tillräcklig i en cyberoperation kan förtroendet för statens avskräckningsförmåga minska och staten tvingas välja andra tillvägagångssätt (ibid., s.44).

Hugyik (2020, s.37-38) betonar att Natos försvarsstrategier på nationell nivå består av en militär och en civil del. För att öka det civila försvaret krävs exempelvis åtgärder i form av kunskapsspridning, ökad medvetenhet och ett bättre samarbete och utbyte mellan forskning och näringsliv (ibid.). Utbildningsprogram är vidare något som Iancu, Tuşa, Iancu, Simion, och Moise (2023, s.377) lyfter som ett sätt att åstadkomma förändring i attityder och uppförande, där denna kunskap senare kan bidra till att upprätthålla en god och hållbar miljö inom social utveckling. Genom att besitta grundliga kunskaper om rättsliga normer och beteenden som är kriminaliserade i relation till grundläggande sociala värden, skapas en förmåga att förutse brottsliga handlingar som riskerar att hota sådana värden inom cyberrymden (ibid., s.364). För att upprätthålla ett förtroende för statliga institutioner och organisationer krävs åtgärder både på makro- och mikronivå för att värna om fred, allmän ordning och tillhandahållandet av ett generellt säkerhetsskydd för samhället och dess befolkning (ibid.).

Cyberattacker från främmande makter förekommer mer frekvent, Semenenko et al. (2023, s.196) poängterar dock att attacker kan förekomma internt och behöver inte nödvändigtvis vara externa (jfr. Stoddart 2022, s.353-355). Interna hot kan kopplas till den modell som Venables (2021, s.1) presenterar med tre komponenter som syftar till att skapa förståelse kring cyberrymdens uppbyggnad, där människan har en väsentlig roll. *Human layer* är en delkomponent som betonar den funktion som människan besitter i relation till förståelse för cyberrymdens uppbyggnad och karaktär. Den mänskliga användaren kan påverkas av flera faktorer som är svåra att förhindra, däribland utpressning, nyfikenhet eller mänskliga fel (ibid., s.9). Venables (ibid.) hävdar att några av de mest framgångsrika åtgärderna mot cyberattacker är utbildning bland, samt kontroll över, den mänskliga nivån. Motiven bakom gärningsmännen kan vara allt från finansiell vinst, ideologi, religion, politik eller underhållningssyfte. Gärningspersonen kan dessutom vara en del av den utsatta interna organisationen eller en extern aktör (ibid., s.12).

Utifrån en svensk kontext diskuterar Eneman, Ljungberg, Raviola och Rolandsson (2022, s.219-220, 230) användningen av teknik med ansiktsigenkänning inom Polismyndigheten. Författarna har fokuserat på ett fall där den svenska polisen använde verktyget *Clearview AI*, vilket är ett privat företag där polisen inte haft direkt insyn i hanteringen av uppgifterna. Fallet fick mycket uppmärksamhet på grund av brott mot integritetsfrågor, vilket är en konsekvens av nya avancerade övervakningssystem (ibid., s.222, 230). Vidare framhävs en svår balansgång mellan integritet och brottsbekämpning, där polisens arbete behöver uppfattas som legitimt för att övervakningsteknik ska kunna nyttjas (ibid., s.222). Dessutom understryks att Polismyndigheten har svårt att kontrollera enskilda polisers användning av tekniken, därför poängteras värdet av organisatoriska rutiner för att utvärdera effektivitet och studera hur uppgifter hanteras (ibid., s.230).

Vidare kan framhävas att Ording, Gao och Chen (2022, s.418) identifierat flera aspekter för utvecklingen av *Information Security Policy* (ISP). ISP beskrivs som etablerade regler inom en organisation som vägleder och tillgodoser skydd över organisationens tillgångar (Whitman 2008 se Ording, Gao & Chen 2022, s.419). Studien består dels av en inledande

litteraturöversikt, dels av intervjuer med ledande säkerhetsansvariga och chefer i Sverige (Ording, Gao & Chen 2022, s.419), vilket applicerar forskningen i en svensk kontext. Resultatet av studien visar att ISP-utvecklingen påverkas av organisatoriska sammanhang, institutionella påtryckningar och sökandet efter legitimitet (ibid., s.418). Författarna lyfter fem rekommendationer i ISP-utvecklingen som kan bearbetas av verksamma aktörer i praktiken, bland annat att tydligt definiera ISP:s roll i organisationen och att se ISP som en del av en legitimitetsprocess istället för en källa till legitimitet (ibid., s.430).

3.4 Slutsatser av tidigare forskning

Sammanfattningsvis kan konstateras att cybersäkerhet utgör ett komplext område som sträcker sig över nationsgränser och mellan olika aktörer. För att hantera cyberhot på ett effektivt sätt krävs samarbete och kunskapsutbyte både på en nationell och internationell nivå. Vidare kan fastställas att bristen på förtroende och legitimitet gentemot statens bemötande av cyberhot kan påverka statens avskräckningsförmåga och hur samhället betraktar offentlig verksamhet gällande avvärjande av cyberhot och informationshantering.

Avslutningsvis kan konstateras att det föreligger en bristande mängd forskning som är relaterad till en svensk kontext i förhållande till Nato och cybersäkerhet, vilket således utgör en kunskapslucka inom fältet. Dessutom finns ytterligare en kunskapslucka inom forskning som är *peer-reviewed* och behandlar olovlig registerslagning inom myndighetsverksamhet, således är denna aspekt viktig att beakta i samband med uppsatsens analysdel. Det är dessutom av vikt att poängtera att lagstiftning i andra länder skiljer sig från Sverige, vilket medför att den tidigare forskningen är svår att direkt applicera i ett svenskt sammanhang. Däremot tolkas andra länders implementering av lag i förhållande till exempelvis Nato och EU som relevant eftersom det kan ge en inblick i hur framtiden kan se ut genom att studera andra länders praxis. Trots att den valda forskningen som utspelar sig i en svensk kontext inte behandlar olovliga registerslagningar, eller kan relateras till Nato i denna aspekt, tolkas svensk myndighetsverksamhet och hantering av legitimitetsfrågor som relevant i förhållande till studiens syfte och frågeställning för att möjliggöra svensk kontextualisering.

4. Teoretisk ansats

I följande avsnitt presenteras studiens valda teoretiska ansats, vilket i sin tur används som analytiskt verktyg i studiens analysdel för att skapa förståelse och kunskap för studiens undersökningsobjekt. Den första teoretiska ansatsen utgörs av *legitimitetsteori* och följs av *nyinstitutionell teori.*

4.1 Legitimitetsteori

Weber (1983, s.144-145) talar först om legitimitet i förhållande till dennes betydelse inom olika auktoritetssystem, och menar här att *legitimitetens* betydelse blir beroende av vilken slags *legitimitet* som auktoriteten själv gör anspråk på. För att illustrera denna tes görs en uppdelning mellan olika idealtyper inom vilka *legitimitet* får olika innebörder beroende på organisationens utformning (ibid., s.144-156). Den organisationstyp som kopplas till dagens myndighetsutövning (Månson 2007, s.74-76), är den Weber benämner som byråkratiska förvaltningsstaber, och har sedermera tilldelats säregna egenskaper. Relevant är att *legitimitetsutövning* inom dessa baseras på fastställandet av gemensamma överenskommelser som organisationens medlemmar förväntas efterleva, och vilka vidare kan vara både målrationellt respektive värderationellt grundade (Weber 1983, s.147-148).

Webers principer gällande *legitimitet* har sedermera gett upphov till en uppström av social teoriutveckling, däribland Tyler som utarbetar *legitimitetsbegreppet* utifrån sin teori om *procedural justice* (Tyler 1988, s.128-129; Sunshine & Tyler 2003, s.534-535; Tyler 2003, s.307-308; Tyler & Mentovich 2023, s.6, 9). Teorin berör studiet av människors rättviseuppfattning vid rättsliga processer och har implementerats vid studier med forskningsfrågor som berör regelefterlevnad och acceptans för rättsliga myndigheter, vilka i sin tur utgör kärnområden för förordningarna och deras rättsliga grunder (Tyler 1988, s.128-129; Tyler & Mentovich 2023, s.10). I många av de studier som anammat teorin har *legitimitet* och dess normativa faktorer visats få en betydande roll i hur denna påvisats utgöra en central grund för regelefterlevnad och acceptansen för auktoriteter (Sunshine &

Tyler 2003, s.518; Tyler 2006, s.57; Levi, Sacks & Tyler 2009, s.356-357; Meares, Tyler & Gardener 2015, ss.308-309; Tyler 2022, s.761; Tyler & Mentovich 2023, s.6-10), och således motiveras här ett fokus på det *legitimitetsbegrepp* som utformats genom studiet av *procedural justice*. Vidare påvisar dessa studier en kvantitativ tillämpning av *legitimitetens* betydelse (ibid.), vilket motiverar intresset i den utvecklade förståelse för begreppet som antas uppnås genom ett sådant kvalitativt angreppssätt som applicerats i detta arbete (se rubrik "5.1 Studiens utformning").

Denna undersöknings anammande av ett normativt perspektiv på *legitimitet* kan till en början motiveras genom hänvisning till Sunshines och Tylers (2003, s.518) studie, i vilken ett instrumentellt respektive normativt perspektiv jämförs vid undersökning av vad som leder till allmän *legitimitetsuppfattning* av polisen, och där resultatet visar på ett starkt band mellan normativitet och medborgares stöd för polisen. Utifrån undersökningens resultat bekräftas Webers (1983) respektive Tylers (2006) teser om allmänhetens reaktioner gentemot auktoriteter som förankrade i sociala värdeuppfattningar (Sunshine & Tyler 2003, s.534-535). Då denna uppsats ämnade undersöka *legitimiteten* hos främst poliser, därtill kompletterande myndighetsaktörer (se rubrik "5.3.1 Urval"), antogs därför Sunshines och Tylers (2003, s.534-535) slutsatser ge skäl för ett normativt angreppssätt till *legitimitet* i studien.

I Tylers (2006, s.165-166) redogörelse för ett normativt perspektiv inkluderas hur *legitimiteten* hos ledare står i direkt relation till regelefterlevnad. Detta område är av intresse i förhållande till studiens syfte relaterat till olovliga slagningar och brottstypens eventuella relation till *legitimitet* hos myndigheter, och således blir ett fortsatt fokus på *legitimitetsbegreppets* normativa ursprung motiverat. *Legitimitet* är ett begrepp som kan få många olika betydelser beroende på den kontext begreppet sätts i (Meares, Tyler & Gardener 2015, s.208). Denna undersökning antog *legitimitetsbegreppet* som hänvisande till bedömningen av en auktoritets handlingar som önskvärda, korrekta eller lämpliga, vilken i sin tur grundas i ett socialt konstruerat system av värderingar, övertygelser och sociala normer (Tyler 2022, s.761). Genom detta synsätt tillskrivs *legitimitet* en betydelse i hur dess

existens i tanken hos människor i ett samhälle leder till en personlig förpliktelse att lyda auktoriteter, och sålunda skapar möjligheten till en effektiv och fungerande rättsstat (ibid., s.762). Levi, Sacks och Tyler (2009, s.356-357) framhäver vidare hur denna normativa förståelse för *legitimitetsbegreppet* har en tydlig koppling till upplevd tillit och förtroende för staten, och således antas denna relevant sett till studiens syfte och dess anammande av ett rättssociologiskt perspektiv (jfr. Baier, Svensson & Nafstad 2018, s.74).

4.2 Nyinstitutionell teori

Nyinstitutionell teori, som utvecklats från den tidigare sociologiska institutionella teorin, möjliggör ett perspektiv som studerar samhällets moderna struktur och hur institutioner påverkar människors handlingssätt (Meyer 2009 se Jepperson & Meyer 2021, s.243; Engdahl & Larsson 2011, s.204). Meyer och Rowan (1977, s.340) framhäver att formella organisationsstrukturer i moderna samhällen präglas av institutionalisering. Institutionaliseringen medför att organisationer tvingas införliva nya metoder och rutiner i enlighet med rådande rationaliserade uppfattningar om organisatoriskt arbete. Genom införlivande av nya metoder och rutiner framstår organisationen som modern och rationell vilket i sin tur ökar organisationens uppfattade legitimitet, oavsett hur effektiva tillvägagångssätten är i praktiken (ibid., s.340-341).

Organisationernas sätt att upprätthålla sin anpassningsförmåga till omgivningen, framför att skapa samordning och kontroll, medför att det skapas en klyfta mellan organisationens formella struktur och det faktiska arbetet (Meyer & Rowan 1977, s.340-341). Denna differens kan relateras till begreppet *institutionaliserad myt* (ibid., s.359-360). Begreppet används för att förklara hur formella organisationer, som associeras med rationalitet, kontroll och samordning, upprätthåller sin legitimitet trots att avsikterna med organisationens handlingar inte resulterar i det som var tänkt, vilket kan beskrivas som att planering och handling uppfattas som löst sammansatta med varandra (ibid., s.340). För att organisationen ska vara bestående krävs att organisationen uppfattas som legitim både av organisationens egna medlemmar och av omgivningen runt omkring (Eriksson-Zetterquist 2009, s.68).

Inom *nyinstitutionell teori* finns i huvudsak två ytterligare begrepp som diskuteras, dessa är *organisationsfält* och *isomorfism* (Eriksson-Zetterquist, Kalling & Styhre 2015, s.295). *Organisationsfält* definierar den idé om att omgivningen både skapas av organisationer och formar sådana. Detta innebär i sin tur att alla organisationer placeras inom ett fält, vilket tillgodoser organisationen med förutsättningar att få den legitimitet de är i behov av i förhållande till kompetens och resurser för att överleva (DiMaggio & Powell 1983, s.148; Eriksson-Zetterquist, Kalling & Styhre 2015, s.296).

Isomorfism beskriver tendensen att fler organisationer börjar likna varandra för att uppfattas som rationella för att överleva, vilket således är en konsekvens av organisationsfälten (DiMaggio & Powell 1983, s.149; Eriksson-Zetterquist, Kalling & Styhre 2015, s.298). Di Maggio och Powell (1983, s.150) beskriver tre former av isomorfism: tvingande, imiterande och normativ. Tvingande *isoformism* blir förekommande när en stark organisation kräver att mindre och svagare organisationer ska förhålla sig till formella och informella regler som är gällande inom fältet (ibid.). Den andra typen av *isomorfism*, den imiterande, är framträdande när en organisation imiterar en organisation som upplevs framgångsrik när den egna organisationen inte vet hur de ska hantera specifika frågor (ibid., s.151). Den tredje och sista formen av *isomorfism* är den normativa och beskrivs genom professionalisering, där det finns en ökad tendens att anställa personal med professionell utbildning, vilket i sin tur innebär att fler har en gemensam akademisk bakgrund. Att fler har samma akademiska bakgrund är ytterligare en bidragande faktor till att organisationsstrukturen likriktas (ibid., s.152).

Eftersom denna undersökning syftade till att studera olika aktörers uppfattningar gällande olovlig registerslagning och brottstypens relation till cybersäkerhet och Sveriges inträde i Nato, ansågs studiet av organisationers tillvägagångssätt att bemöta institutionella förändringar och upprätthålla legitimitet relevant utifrån ett rättssociologiskt perspektiv (jfr. Baier, Svensson & Nafstad 2018, s.20). Begrepp i form av *institutionaliserad myt*, *organisationsfält* och *isomorfism* bedömdes relevanta för att skapa förståelse för

föreställningar som blivit en del av det rådande systemet, hur organisationen samverkar med andra institutioner inom fältet och ge möjliga förklaringar till organisationers homogenitet i relation till praxis och beteende. Således ansågs den *nyinstitutionella teorin* som ett passande komplement till *legitimitetsteorin* som tillsammans utgör studiens teoretiska ansats.

5. Metod och material

I avsnittet för metod presenteras studiens valda metod och material. Inledningsvis ges en beskrivning av studiens utformning och datainsamlingsmetod med tillvägagångssätt, vilket beskriver insamlingen av studiens empiriska material i form av intervjuer. Vidare i avsnittet beskrivs analysmetod, forskningsetiska principer och avslutningsvis framförs en diskussion gällande studiens validitet och reliabilitet.

5.1 Studiens utformning

Studien ämnade undersöka individuella uppfattningar hos aktörer inom det svenska rättsväsendet, sålunda blev en kvalitativ forskningsdesign tillämplig då en sådan karaktäriseras av att lägga större vikt vid ord än siffror (Bryman 2018, s.454-455), och betraktades således lämpad för studiens syfte, och som komplement till den befintliga kvantitativa forskningsansatsen på Tylers (2022) legitimitet. Den kvalitativa forskningstraditionen har som överordnat mål att erhålla insikter och förståelser för fenomen inkluderande situationer i personers sociala verkligheter (Dalen 2015, s.15). Mot denna bakgrund har valet av en kvalitativ ansats framför en kvantitativ gjorts. Kvantitativ forskningsdesign kan erbjuda fördelar i förhållande till replikerbarhet och generaliserbarhet, men då kvantitativa ansatser snarare har en intresseinriktning mot mätning, än mot kontextuell förståelse (Bryman 2018, s.215-217, 484), bedömdes denna metod gå emot den linje som för denna undersökning var önskvärd. Studien har utgått från en deduktiv ansats där studiens empiriska material har härletts från undersökningens

tidigare forskning och teoretiska ansatser (ibid., s.47-49), i form av legitimitetsteori och nyinstitutionell teori, som givna premisser i analysavsnittet.

5.2 Datainsamlingsmetod

Som kvalitativ metod för datainsamling tillämpades semistrukturerade intervjuer (Denscombe 2018, s.268-269). Den kvalitativa intervjun är speciellt lämplig för att få fram beskrivande information om informantens egna erfarenheter och tankar (Dalen 2015, s.14), och bedömdes således lämplig i förhållande till studiens syfte. Kvalitativa intervjuer karaktäriseras även av att vara mer flexibla då de ger intervjupersonen mer utrymme att berätta fritt, medan en kvantitativ intervju i stor utsträckning använder sig av slutna frågor och således begränsar mängden infallsvinklar som i sin tur möjliggör den förståelse som i undersökningen eftersträvades (Bryman 2018, s.257-259, 561-563).

Mot denna bakgrund ansågs även valet av semistrukturerad intervju motiverad. Detta då den semistrukturerade intervjun erbjuder flexibilitet som tillåter den intervjuade att utveckla sina idéer och ge utförliga svar (Dalen 2015, s.269). Däremot konstrueras ofta, i samband med semistrukturerade intervjuer, en lista med ämnen som ska behandlas (ibid.), vilket således tillät metoden att besvara de frågor som var nödvändiga för bemötandet av studiens frågeställningar, och bedömdes därför fördelaktig.

För att uppnå önskat resultat med hjälp av de semistrukturerade intervjuerna konstruerades en intervjuguide, som bestod av en lista av teman vilka behandlades under intervjuerna (Bryman 2018, s.563). Studiens intervjuguide (se bilaga 3) konstruerades utifrån det syfte, de frågeställningar, den tidigare forskning, samt de valda teoretiska utgångspunkterna som förelåg undersökningen. På så sätt underlättades erhållandet av svar på studiens frågeställningar, samt den tolkning som sedan gjordes utifrån det intervjupersonerna berättat (Bryman 2018, s.565-566). Eftersom intervjuerna skedde med olika aktörer inom olika brottsbekämpande myndighetsområden anpassades frågorna i förhållande till den intervjuades verksamhet och kunskapsområde.

För att testa lämpligheten i intervjufrågornas utformning utfördes en pilotintervju där studiens frågor testades samtidigt som intervjuarens egna beteende i intervjusituationen undersöktes (Bryman 2018, s.332; Dalen 2015, s.40). Pilotintervjun genomfördes med en myndighetsanställd inom Kriminalvården med erfarenhet av registerslagningar, men inkluderades inte i studiens urval.

Under intervjuerna spelades ljudet in, efter samtycke från den som intervjuades, med hjälp av en diktafon för att tillmötesgå intresset i att upprätthålla de forskningsetiska principer som vidare behandlas under rubriken "5.4 Forskningsetiska principer". Intervjuerna genomfördes via telefon, vilket motiverades utifrån studiens tidsomfång samt den geografiska spridningen mellan respondenterna (Bryman 2018, s.262). Här förekom ett övervägande av för- och nackdelar nödvändig då intervjuer via telefon reducerar möjligheten att se intervjupersonen (ibid., s.263), dock tolkades detta inte som problematiskt eftersom studien inte hade för avsikt att observera beteenden.

Intervjuerna tog mellan 30 och 50 minuter, och de avslutades med en förfrågan om möjlighet till senare återkoppling för eventuella frågor eller önskan om komplettering. Efter varje avslutad intervju genomfördes transkribering av det inspelade ljudmaterialet i syfte att erhålla en form av data som var lämpad för analys (Denscombe 2018, s.395-396).

5.2.1 Urval

Studiens empiriska material utgörs av intervjuer med åtta respondenter. De som intervjuades har rekryterats genom ett målstyrt urval i form av en kombination mellan snöbolls- och bekvämlighetsurval (Bryman 2018, s.243, 496, 504-505). Genom ett målstyrt urval väljs individer eller organisationer ut med relevans i förhållande till studiens forskningsmål (ibid., s.496). Inledningsvis ansågs ett snöbollsurval motiverat till följd av upplevd svårighet att nå respondenter genom andra tillvägagångssätt (ibid., s.505). Således kontaktades bland annat Polismyndigheten, Sveriges tingsrätter, Åklagarmyndigheten, och Försvarsmakten via e-post till myndigheternas registrator. Däremot upptäcktes ett metodproblem att få tag i respondenter som var villiga att medverka genom ett

snöbollsurval. För att lösa problemet togs beslutet att rekrytera fler deltagare genom ett bekvämlighetsurval, vilket innebar att bekanta till studiens författare kontaktades (ibid., s.243). Dessa respondenter blev tillfrågade via e-post eller sms om de var intresserade av att medverka.

De valda respondenterna motiverades utifrån förmågan att erbjuda ett varierat perspektiv på olovliga registerslagningar och dess relation till Nato. Den större andelen av respondenterna utgjordes av poliser, anledningen till detta kan hänvisas till den tendens som Lindskog et al. (2022, s.43) identifierat via BRÅ i samband med polisanmälda dataintrång, där Polismyndigheten stod för en tredjedel av de granskade ärendena. Vidare ansågs det givande med ytterligare perspektiv på brottstypen inom myndigheter där registerslagningar var förekommande, och således ansågs respondenten från Kronofogdens roll i studien motiverad. För att erhålla ett perspektiv som tillgodosåg lagstiftningen om dataintrång i praktiken, uppfattades det motiverat att intervjua en rättstillämpande aktör inom rättskipningsprocessen. I förhållande till de praktiska utövarna, som har ett användarperspektiv på rätten, ansågs ett domarperspektiv kunna bidra med ett vertikalt perspektiv som ett komplement till det horisontella (Hydén 2002, s.17). Domarperspektivet fastställer innehållet i juridiken (ibid.) och bidrog således till ett annat perspektiv jämfört med de andra myndighetsutövarna.

Poliser, domare och anställda inom Kronofogden har olika uppgifter i samhället, men har gemensamt att de arbetar med olika typer av brottsbekämpande myndighetsverksamhet. Exempelvis arbetar Polismyndigheten med att förebygga och utreda brottslighet, domare arbetar med juridiska bedömningar i brott- och tvistemål och Kronofogden arbetar med att driva in betalningar i samhället och motverka brottslighet (Polisen 2023; Sveriges Domstolar 2022; Kronofogden u.å.). Således ansågs det motiverat att nyttja begreppet *brottsbekämpande myndighetsverksamhet* i studiens frågeställningar för att specificera studiens inriktning.

5.3 Analysmetod

Kvalitativ forskning har den gemensamma nämnaren att analysmetoden innehar ett tolkande angreppssätt (Dalen 2015, s.18). Den tolkning som för studien blev adekvat härstammande ur hermeneutiken då ett sådant angreppssätt innebär betoning på förståelse och tolkning med syfte att nå ett djupare meningsinnehåll (ibid., s.18-19). För att uppnå detta blev det en nödvändighet att sätta identifierade budskap i ett sammanhang eller i en helhet (ibid.), vilket i denna undersökning utfördes med en tillämpning av den tidigare forskningen och de teoretiska ansatserna.

Det insamlade empiriska materialet genomgick en kodningsprocess i samband med analysen. Kodning av kvalitativa data går ut på att söka kategorier som kan sammanföra och organisera det föreliggande materialet på nya sätt, för att på så vis möjliggöra förståelse för vad informanterna har berättat (Dalen 2015, s.78). Den analysmetod som användes för detta ändamål är den tematiska innehållsanalysen (Bryman 2018, s.702). Analysmetoden gick ut på eftersökning och identifiering av teman i det transkriberade materialet, vilka sedan kopplades till studiens syfte och frågeställningar (ibid., s.704). Respektive tema som observerades i undersökningens empiri utgjorde sedermera varsin rubrik i analysavsnittet, under vilka relevant data sammanställdes och operationaliserades utifrån studiens syfte.

5.4 Forskningsetiska principer

Till följd av studiens karaktär där myndighetspersoner tillfrågades om sin yrkesroll och deras personliga uppfattningar, har etiska överväganden gjorts i relation till de forskningsetiska principer som Vetenskapsrådet (2017) framställt. De fyra huvudkraven, informations-, samtyckes-, konfidentialitets- och nyttjandekravet, har alla beaktats vid studiens utformning (Lindstedt 2019, s.51).

Genom att respondenterna fick ta del av en informations- och samtyckesblankett (se bilaga 4) innehållande information om studiens syfte, intervjuns innebörd och tillvägagångssätt, deras frivilliga medverkan och rätt att avsluta denna utan att behöva ange skäl, säkerställdes

således informationskravet. Kravet innebär att de som medverkar får information om syftet med studien samt vad deras medverkan innebär (Lindstedt 2019, s.51). Dessutom säkerställdes samtyckeskravet genom att deltagarna fick information om sin bestämmanderätt gällande sin medverkan, men även genom att deltagarna lämnade en muntlig bekräftelse på att de tagit del av informationen i blanketten, och ett informerat samtycke till sin medverkan och att ljudet spelades in under intervjun (ibid., s.52). Initialt hade studien för avsikt att få skriftligt samtycke från de intervjuade, men eftersom blanketten skickades digitalt fanns det tekniska svårigheter med signering av dokumentet vilket gjorde att muntligt samtycke ansågs tillräckligt.

För att uppnå konfidentialitetskravet, i form av att behandla uppgifter som kan identifiera personer med största möjliga konfidentialitet (Lindstedt 2019, s.52-53), har namnen på de intervjuade pseudonymiserats till "Intervjuperson A", "Intervjuperson B", "Intervjuperson C" och så vidare. I fall där personerna haft en mycket specifik befattning inom myndigheten och meddelat de exakta antal år som personen arbetat inom myndigheten, har denna information valts bort. Ljudinspelningarna vid intervjuerna genomfördes dessutom med hjälp av en diktafon, vilket således medförde att ljudfilen lagrades lokalt och inte sparades i något moln som skulle riskera att obehöriga kunde ta del av filen. Efter att filen transkriberats för hand, raderades ljudfilen. Avslutningsvis har nyttjandekravet tillgodosetts genom att de insamlade uppgifterna enbart användes till studiens ändamål (ibid., s.55), vilket även respondenterna informerades om genom studiens informations- och samtyckesblankett.

5.5 Reliabilitet och validitet

Reliabilitet beskriver huruvida en undersökning kan genomföras på nytt och ge samma resultat, samtidigt som validitet handlar om hur väl det konstaterade resultatet kan relateras till undersökningens avsiktliga studieobjekt (Bryman 2018, s.72, 465). Initialt kan extern reliabilitet respektive validitet nämnas. Den externa reliabiliteten handlar om i vilken omfattning studien kan replikeras, medan extern validitet handlar om forskarens möjlighet till att generalisera resultatet (ibid., s.465-466). För denna undersökning är både den externa

reliabiliteten samt validiteten bristande, dels genom komplikation att upprepa studien eftersom de intervjuade kan uttrycka sig annorlunda vid olika tillfällen, dels genom studiens kvalitativa fokus på de åtta respondenternas tolkning av dataintrång och dess relation till Nato.

Vidare beskriver intern reliabilitet den utsträckning som forskare, vid tillfällen där det finns fler än en forskare, tolkar situationer och begrepp på ett gemensamt sätt. Intern validitet handlar istället om hur slutsatserna som forskaren genererat har god koppling till studiens undersökningsmetoder och observationer (Bryman 2018, s.465). Här kan konstateras att den interna reliabiliteten har förstärkts genom att uppsatsförfattarna fört en genomgående diskussion sinsemellan under arbetets gång och således uppnått konsensus i alla uppsatsens delar. Även den interna validiteten är stärkt genom att intervjuguidens utformning var anpassad efter studiens syfte, frågeställningar, tidigare forskning och teoretiska utgångspunkter. Således ställdes frågor till respondenterna som var relaterade till det ämne som studien hade för avsikt att undersöka.

6. Resultat

I avsnittet för resultat presenteras studiens empiriska material i form av transkriberade intervjuer med åtta respondenter. Empirin redovisas utifrån de teman som intervjuguiden var indelad i, vilken i sin tur var utformad efter studiens syfte, frågeställningar, tidigare forskning och valda teorier. Resultatets teman består således av: "Respondenternas bakgrund", "Dataintrång som brottstyp", "Effekter och hantering av olovliga slagningar" och "Det svenska Natomedlemskapet".

6.1 Redogörelse av empiriskt material

6.1.1 Respondenternas bakgrund

Respondenterna i studien har varierad arbetserfarenhet och arbetar inom olika brottsbekämpande myndighetsområden, således erbjöd intervjuerna olika perspektiv

utifrån olika verksamheter. Dessutom är intervjupersonerna verksamma i olika delar av landet, vilket bidrog till geografisk spridning med perspektiv från olika regioner. En kortare beskrivning av de intervjuade presenteras i bilaga 5.

I samband med första temat fick intervjupersonerna frågan om vad de ansåg vara det främsta målet för sin verksamhet, samt vilken betydelse rättssäkerheten ansågs ha inom myndigheten. Inledningsvis konstateras att Intervjuperson A, C, D, F, G och H, som alla arbetar inom Polismyndigheten, beskrev myndighetens främsta roll som brottsbekämpning. Vidare framförde Intervjuperson B, som arbetar hos tingsrätten, att rättsskipning är det främsta målet för domstolsverksamheten. Intervjuperson E, som arbetar inom Kronofogden, lyfte myndighetens uppgift att upprätthålla samhällets betalningsmoral.

Samtliga intervjupersoner konstaterade att rättssäkerheten är en viktig del av den myndighet de är verksamma inom. Intervjuperson B poängterade betydelsen av att alla ska behandlas lika, oavsett bakgrund och tillgångar, i rättskipningen. Även Intervjuperson F poängterade att det är viktigt att alla behandlas lika, dessutom framförde både Intervjuperson F och G vikten av tydliga krav för myndigheternas verksamhet eftersom Polismyndigheten har möjligheter att inskränka andra människors friheter. Vidare framförde Intervjuperson C, D och H att Polismyndigheten befinner sig inom en förtroendebransch där myndigheten har som uppgift att beivra och förebygga brott för att skapa trygghet för medborgarna. Vikten av att genomföra åtgärder med stöd i lagtext var en aspekt som både Intervjuperson A och E lyfte i relation till upprätthållandet av rättssäkerhet.

6.1.2 Dataintrång som brottstyp

När respondenterna blev tillfrågade om dess uppfattning kring varför de tror att myndighetspersonal inom myndigheter åtalas för dataintrång så varierade svaren mellan respondenterna. Intervjuperson A och D, som arbetar inom polisen, framförde att de inte var förvånade över att domsluten såg ut som de gjorde eftersom olovliga registerslagningar oftast är relaterade till myndighetens system samt att det således blir lättare med bevisning. Vidare framförde Intervjuperson E, som är verksam inom Kronofogden, att

myndighetspersonal som döms för dataintrång är ett tecken på rättssäkerhet eftersom myndigheten är skyldig att anmäla sådana brott. Intervjuperson G betonade en förvåning över att många döms för dataintrång eftersom verksamma inom Polismyndigheten ständigt påminns om att slagningar endast får göras om de är tjänsterelaterade.

I samband med frågan om vad respondenterna ansåg att förekomsten av olovliga registerslagningar inom myndigheter skulle kunna bero på, svarade Intervjuperson A, D, G och H, som arbetar inom polisen, samt Intervjuperson B och E, som arbetar i tingsrätten respektive Kronofogden, att de tror att sökningarna främst görs på grund av nyfikenhet. Okunskap eller vana var ytterligare en möjlig anledning varför myndighetsanställda genomför otillåtna registerslagningar. Intervjuperson E tillade att en annan möjlig anledning skulle kunna vara påfrestning utifrån. Intervjuperson B och C poängterade att det finns de som blir övertygade av någon som är involverad inom organiserad brottslighet. Dessutom framförde Intervjuperson B att som en konsekvens av det försämrade säkerhetsläget kan de anställda uppleva att det finns ett ökat behov att slå i registerna:

> [...] jag tror ju mycket är ren okunskap. Sen så är det ren nyfikenhet. [...] med inträdet i Nato och ett försämrat säkerhetsläge, så är det ju ett ökat behov för människor att slå i de här registrena, och många upplever att de har ett stort behov. [...] Sen kan det bli så att det är organiserad brottslighet som vill bereda sig tillgång till det här, och då försöker att övertyga någon anställd som har tillgång i offentlig verksamhet, att dela med sig av uppgifter. (Intervjuperson B)

Vidare kan framhävas att Intervjuperson C som arbetar inom polisen istället betonade rekryteringsprocessen:

> Dels så tror jag att det är tillgängligheten, systemen är väldigt väldigt lättillgängliga [...]. Sen så i vissa fall så ser vi också att [...] asså att det är fel med rekryteringen redan från början,
> [...] och sen även då personer som har en dold agenda, vi har ju sett det här med infiltration inom myndigheter har ju blivit, det har ju blivit vanligare sista åren och man ser ju att det finns personer som har kopplingar till olika kriminella individer [...] som tar en anställning inom Polismyndigheten, Kriminalvården, tingsrätten just med av den anledningen. (Intervjuperson C)

Utöver nyfikenhet poängterades även tillgängligheten och myndighetens IT-system som en ytterligare anledning till varför brottet förekommer enligt Intervjuperson B, C, F, G, och H. Här poängterades framförallt polisens tjänstemobiler som en lättillgänglig källa till att genomföra slagningar enligt Intervjuperson C, F, G och H. Vidare framhävdes en befintlig otydlighet enligt respondenterna kring vad som får göras respektive inte:

> [...] du är alltid polis liksom, det är inte så att du stänger av och på någon switch-knapp när du går hem utan du är alltid polis, ser man då en skum bil som du kanske känner igen från ditt arbetspass och så gör man en slagning, [...] du slog på en granne istället och då helt plötsligt så har du gjort ett dataintrång fast uppsåtet var kanske egentligen att du skulle bara se så att det var rätt bil så att du ringer dina kollegor som jobbar för att förhindra att den här kanske rattfylleristen fortsätter att köra bil. Det är där dilemman har varit och det är där diskussioner har varit inom Polismyndigheten sista åren, vart går den här gränsen liksom. (Intervjuperson C)

> [...] är du ledig och ser en bil som du misstänker är rattfylla, då kan du slå på den för att sen rapportera det här vidare till dina kollegor som jobbar och så där, [...] nja men det är ju lite oklart om vi får göra så[...]. Ja så lite oklart är det ju och vi får inte så mycket direktiv från jobbet om det heller (Intervjuperson D)

> [...] som myndigheten är inte helt på det klara heller vad som är en olovlig dataslagning. (Intervjuperson G)

> Sen är det väl en del som kanske tycker att, ja om man säger i gränslandet med vad som är tjänsterelaterat och inte, att det kanske fortfarande är lite osäkert vad som gäller där. (Intervjuperson H)

6.1.3 Effekter och hantering av olovliga slagningar

Vad gäller uppfattade konsekvenser av olovliga slagningar inom myndigheter svarade samtliga intervjupersoner att de tror att förtroendet för myndighetens verksamhet kan drabbas negativt, vilket i sin tur drabbar organisationers legitimitet. Intervjuperson A som arbetar inom polisen och Intervjuperson B som arbetar på tingsrätt, poängterade att medborgare ska kunna lita på att myndigheterna ägnar sig åt sin verksamhet och inget

utöver befogenhet. I relation till myndighetens befogenhet framförde Intervjuperson F, som arbetar hos polisen, att samhället sätter begränsningar i form av lagar med syfte att följas. Personen tillade dessutom att domsluten påverkar vad samhället anser om myndigheten:

> Jag tycker ändå att när man läser vad folk tycker om Polismyndigheten i Sverige så brukar samhället ha positiva tankar om polisen i jämförelse med andra länder, och det vill vi såklart behålla och höja. Men sådana domar är ju skadliga för myndigheten och vad folk tycker om myndigheten, alltså vad medborgarna tycker. (Intervjuperson F)

Vidare betonade Intervjuperson H, som också arbetar som polis, att ett minskat förtroende för myndigheten kan få konsekvenser för dennes verksamhet i allmänhetens ovilja att medverka i utredningar och hjälpa polisen. Intervjuperson C, som även denne är verksam inom polisen, lyfte ytterligare risken med att medborgarna upplever att de inte kan lita på myndigheten och istället tar saken i egna händer:

> [...] det påverkar ju förtroendet väldigt negativt och i slutändan kan ju det, det kan ju resultera i folk kan känna att man inte kan vända sig till Polismyndigheten för det går ju inte att lita på dom, jag tar saken i egna händer istället och löser det här, för tar polisen saken i egna händer då kan jag också ta saken i egna händer, och då handlar det om en situation där, [...] hela statens grund faller ju på nåt sätt. (Intervjuperson C)

Intervjuperson E, som är anställd inom Kronofogden, framförde att det finns konsekvenser som påverkar både på individ- och samhällsnivå. På individnivå påverkas den person som sökningen är gjord på i förhållande till integritetsfrågor. På samhällsnivå, i relation till förtroendeeffekten, lyfte Intervjuperson E ett exempel med andra rättskulturer där det finns en negativ association kring myndigheter, där människor väljer att inte kontakta myndigheten vid behov och att sådan kultur inte bör utvecklas i Sverige:

> [...] men det beror på att man har dåliga erfarenheter från hemlandet, det här med rättskultur, legal culture, det avgör om man kommer att kontakta myndigheter, för man hade inte förtroende för myndigheter i hemlandet och då tar man inte kontakt med myndigheterna i Sverige heller, och dit vill vi inte komma. (Intervjuperson E)

I samband med frågan om hur olovliga registerslagningar skulle kunna förebyggas framhävde Intervjuperson A, B, C, D, F, G och H vikten av utbildning och informationsspridning bland personalen. Intervjuperson A, C, F och G, som alla arbetar inom polisen, poängterade även kontinuerlig fortbildning och påminnelser under anställningen. Intervjuperson C framhävde dessutom att lagstiftningens formulering kring dataintrång bör tydliggöras. Detta med anledning av den nya teknik som tillkommit under senare år och således inte passar in i förhållande till den tidpunkt då lagtexten skrevs.

6.1.4 Det svenska Natomedlemskapet

Huruvida Sveriges inträde i Nato har diskuterats inom myndigheten skiljer sig mellan respondenterna. Intervjuperson A inom polisen och Intervjuperson B inom tingsrätten, framhävde att det diskuterats lite, samtidigt som polisanställda Intervjuperson C berättade att det diskuterats en del i samband med arbetsuppgifter som kan tillkomma. Intervjuperson F, som också är polisanställd, tillade att det främst diskuterats kollegor sinsemellan, samt eventuellt högre upp i ledningen. Intervjuperson D och G som även dessa arbetar inom polisen, samt Intervjuperson E inom Kronofogden, menade att inträdet inte har diskuterats alls, i alla fall inte vad som berört intervjupersonernas verksamheter.

Intervjuperson A, C, F, G och H som alla är anställda inom polisen, samt Intervjuperson B och E som arbetar inom tingsrätten respektive Kronofogden, framförde att innebörden av cybersäkerhet är viktig för respektive verksamhet. Däremot lyfte Intervjuperson A, B, C, D och F att cybersäkerheten inte direkt är en del av den egna verksamheten.

Vad gäller frågan om Sveriges inträde i Nato och dess betydelse för det svenska totalförsvaret kan inledningsvis nämnas att samtliga intervjuade aktörer inte var medvetna om vad medlemskapet kunde innebära i praktiken. Samarbete mellan olika länder var däremot något som polisanställda i form av Intervjuperson A, C, D och F framförde som potentiella möjligheter i och med Nato-inträdet. Kunskapsutbyte och utbildning mellan olika länder var ytterligare en aspekt som skulle kunna förekomma enligt Intervjuperson C, D, G och H, vilka alla är verksamma inom polisen.

Intervjuperson C poängterade framförallt upprustning och mer resurser inom militär verksamhet som en möjlig följd av Natomedlemskapet. Respondenten framhävde dessutom att medlemskapet kan sätta nya krav på Sverige i relation till att landet tidigare haft en tendens att tro gott om andra:

> Sverige är ju ett land där man [...] lite raljerande så men vi tror ju väldigt väldigt gott om alla och det lyser också igenom hur vi hanterar vissa frågor inom landets försvarspolitik och säkerhetspolitik och, så jag tror att, ja vi, det behövs nog göras en hel del. (Intervjuperson C)

Vidare betonades även ett ökat samarbete enligt Intervjuperson C, framförallt med de nordiska länderna, vilket var något som Intervjuperson F också poängterade. Intervjuperson A, F och H lyfte även det rådande samarbetet med Europol och Interpol. Intervjuperson E framhöll att Kronofogden inte är den första myndigheten som Nato i huvudsak träffar, där andra myndigheter, som polisen exempelvis, kan märka av inträdet på ett annat sätt.

I samband med frågan om huruvida aktörerna tror att förekomsten av olovliga registerslagningar inom myndigheter kan påverkas av inträdet i Nato var respondenternas svar skiljaktiga. Intervjuperson A uppfattade inte att brottstypen eller den typen av information kommer att behöva lämnas ut i större utsträckning än tidigare med anledning av dess privata karaktär. Intervjuperson F framförde att Sveriges befintliga regelverk är tillräckligt tydliga, vilket innebar att personen inte uppfattade någon ändring som nödvändig för tillfället. Noggrannare rekrytering var någonting som Intervjuperson C lyfte i förhållande till risk för infiltration, där försiktighetsåtgärder mot infiltration även var något som påpekades enligt Intervjuperson E. Intervjuperson G, som är polisanställd, framhöll att förändringar kan komma att vara möjliga, men att det främst är spionerи och liknande brottstyper som skulle påverkas av Nato. Att det blir tydligare riktlinjer kring vad som får göras respektive inte, var något som polisanställda Intervjuperson D och H har förhoppning om ska utvecklas.

En reflektion som skiljer sig från övriga respondenter kommer från Intervjuperson B, som arbetar inom tingsrätten, som diskuterade hur brottstypen kan komma att betraktas annorlunda i förhållande till hur Sveriges säkerhetssituation ändras:

> [...] i den mån att det ändrar vår säkerhetssituation och vår säkerhetsbild. Att vi får kanske nya allierade, nya fiender så hotbilden ändras och så ändras ju den typen av personer som kanske skulle vilja angripa systemet och tillförskansa sig uppgifter, medan även motivationer hos många inom offentlig verksamhet kan ta intryck av det här. Till exempel att inför ett ökat säkerhetshot, inför att vi är medlemmar i Nato och så, så kan det viljas göras slagningar som inte är okej. (Intervjuperson B)

En annan viktig aspekt som Intervjuperson B framhävde var att det finns risk att dataintrång kommer att bli en brottstyp som blir lättare att lagföra personer som sysslar med säkerhetshotande verksamhet för:

> Vi har ju fått väldigt många lagar på den nationella säkerhets- och anti-terrorlagen [...]. Många av de här lagarna är under vår nuvarande process och rättegångsform är förenade med väldigt stora bevissvårigheter. Medan dataintrång är ju ett långt lättare brott att bevisa. Så jag tror ju att det kommer bli i någon mån någon slags bekväm go to för att lagföra individer som sysslar med säkerhetshotande verksamhet. (Intervjuperson B)

I intervjuernas avslutande skede fick respondenterna frågan om de trodde att straffbestämmelsen för olovlig registerslagning, det vill säga dataintrång, kan komma att påverkas i framtiden med anledning av Nato. Intervjuperson A, som är polisanställd, hade inte uppfattningen att bestämmelsen kan ändras för tillfället och poängterade även att personen snarare ser Nato som ett militärt samarbete i jämförelse med samarbetet i EU. Intervjuperson G, som också arbetar inom polisen, instämde i uppfattningen att lagändring inte kan komma att ske för tillfället, däremot poängterades att lagförslag klubbas igenom utan närmare eftertanke och att det således finns en möjlighet till lagändring i framtiden:

> Det är jättesvårt men spontant säger jag nej, det tror jag inte. Men som allt annat som händer i samhället nu, det är lagförslag som klubbas igenom utan någon närmare eftertanke så kanske det finns en möjlighet. (Intervjuperson G)

Intervjuperson F, som också är polisanställd, framförde vidare att EU-lagarna anses tillräckligt tydliga, varav personen hade svårt att se att det kan bli en ändring på grund av Nato för tillfället. Intervjuperson B och C, som arbetar inom tingsrätten respektive polisen, menade att det troligtvis är andra brottstyper där straffskalan kommer att ändras, som exempelvis spionage eller nationella säkerhetsbrott.

7. Analys

I följande avsnitt redovisas studiens resultat i relation till arbetets tidigare forskning, samt de analytiska verktygen i form legitimitetsteori och nyinstitutionell teori som gemensamt syftar till att besvara studiens valda forskningsfrågor. Utifrån ett kvalitativt analysförfarande i form av en tematisk analys- och kodningsprocess i relation till studiens syfte och frågeställningar, identifierades tre framträdande teman vilka presenteras som "Myndighetens anseende", "Reglernas tolkning" och "Natodiskursen".

7.1 Myndighetens anseende

En trend som gick att urskilja från resultatet var hur respondenterna såg på förekomsten av olovliga registerslagningar inom en myndighet kopplat till dennes anseende. När respondenterna fick frågan om vilken betydelse rättssäkerheten har för respektive myndighetsverksamhet, ansåg samtliga att denna var av angelägen vikt. Som anledning lyfte Intervjuperson C, D och H, med bakgrund i Polismyndigheten, att detta berodde på myndighetens egenskap som förtroendebransch. Att förtroende är betydande för Polismyndighetens verksamhet förklarades sedermera av Intervjuperson F och G genom att lyfta hur de har viss rättighet att inskränka andra människors friheter i sin yrkesutövning.

Dessa påståenden från studiens respondenter blir fortsatt intressanta att sätta i relation till Sunshines och Tylers (2003, s.518) studie med fokus på poliser. Studien visade normativt stöd förankrat i sociala värdeuppfattningar från allmänheten som avgörande för polisens

verksamhetsutövning (ibid., s.534-535). En sådan social värdeuppfattning, som därav antas kritisk, menas vidare vara beroende av den tillit och förtroende som finns för polisen. Sålunda antas respondenternas ovan redogjorda utsagor och beskrivning av Polismyndigheten som förtroendebransch, gå i linje med Sunshines och Tylers (ibid.) slutsatser.

Vidare uppgav samtliga intervjupersoner, i samband med att intervjun behandlade effekter av förekomsten av olovliga slagningar inom myndigheten, en oro för att förtroendet för myndighetens verksamhet skulle drabbas negativt av ett sådant uppträdande. En konsekvens av skadat förtroende belyses av respondenterna i hur människor då riskerar att ta saken i egna händer på grund av en ovilja att vända sig till polisen. Intervjuperson E lyfte hur negativa erfarenheter av andra länder visats då denna mött människor från andra kulturer som är ovilliga att samarbeta. Genom detta lyfts ytterligare negativa konsekvenser i hur respondenten menar att detta leder till ett försvårande för sin yrkesutövning, vilket belyser hur den rådande rättskulturen kan få innebörd för myndighetsverksamheter. Samtliga respondenter lyfte vidare hur förtroendefrågan sålunda antas få negativ påverkan för legitimiteten hos respektive myndighet.

Ett sådant resonemang kring legtimititetsbrist och dess konsekvenser kan återigen hänföras till Tyler och hans normativa legitimitetsprinciper. I denna teori om legitimitet lyfts hur regelefterlevnad och acceptans för rättsliga myndigheter är det som anses mest centralt för deras verksamheter (Tyler & Mentovich 2023, s.10). Detta är möjligt att utläsa ur föreliggande studies intervjuer, bland annat genom hur Intervjuperson C lyfte att då människor frångår myndigheterna och tar saker i egna händer, riskerar hela statens grund att fallera.

Genom att se till det normativa legitimitetsbegreppet som för studien anammats, så beskrivs här bedömningen av en auktoritets handlingar som önskvärda, korrekta eller lämpliga, utgöra grund i det rådande socialt konstruerade systemet av värderingar och sociala normer (Tyler 2022, s.761). Mot denna grund kan antaganden om att förekomsten av olovliga

slagningar drabbar legitimiteten göras mot förklaringen att allmänheten delar ett värderingssystem där myndigheternas avvikande från befogenheter ses som icke önskvärda (Weber 1983, s.147-148). Sålunda påverkar brister i legitimitet anseendet av myndigheten hos betraktaren (Weber 1983, s.147-148; Tyler 2022., s.762).

Ett slutligt perspektiv som är av intresse, sett till respondenternas behandling av förtroende och legitimitet, tillhandahåller undersökningens tidigare forskning. Tidigare har i en svensk kontext Polismyndighetens användning av ansiktsigenkänning sett till frågor om legitimitet undersökts (Eneman et al. 2022, s.219-220, 230). När detta verktyg missbrukats har detta fått stor uppståndelse på grund av hur en sådan felaktig användning går emot frågor som berör integritet (ibid., s.222, 230). Här framhävs att balansgången mellan integritet och brottsbekämpning är av stor vikt inom polisens arbete för att detta ska uppfattas som legitimt, och sålunda antas en svensk rättskultur påvisas där brott mot integritetsfrågor anses särskilt viktiga (ibid.).

Vidare är detta intressant att applicera på förekomsten av olovliga registerslagningar som studien undersökt. Respondenterna uppgav i intervjuerna att de har tillgång till ett flertal register innehållande privat, och ibland känslig, information. Sålunda görs en fråga om integritet sig gällande även här. Sett till den rättskultur som påvisades av Eneman et al. (2022, s.222, 230) kan den upplevda legitimiteten därför antas inneha ytterligare känslighet för förekomsten av olovliga slagningar, i samband med hur detta uppträdande möjligen utgör risker gentemot personlig integritet. Skulle så vara fallet kan det finnas skäl att anta ett hot mot rättssäkerheten som, för att återgå till vart denna diskussion började, ansågs av samtliga intervjupersoner vara en vital del i myndighetsutövningen.

7.2 Reglernas tolkning

Ett ytterligare tema som identifierades i studiens resultat var huruvida lagstiftning samt interna riktlinjer uppfattades som tydliga respektive inte. I samband med vad förekomsten av olovliga registerslagningar kunde bero på förekom exempelvis nyfikenhet, okunskap och tillgänglighet som möjliga motiv. Alla intervjuade aktörer konstaterade att rättssäkerhet är

en viktig del av verksamheten, vilket således innebär att handlingar görs med stöd i lagtext, vilket även framfördes av Intervjuperson A och E. Kunskapen om vad som är korrekt tolkning av lagstiftningen är således en viktig del av myndighetsutövningen.

Tolkning av riktlinjer kan vidare relateras till nyinstitutionell teori och begreppet *institutionaliserad myt*, som beskriver den klyfta mellan det som organisationsmedlemmarna faktiskt utövar i relation till den rationella skepnad som organisationen vill uppnå genom att anpassa sig efter miljön (Meyer & Rowan 1977, s.340-341). Här kan isomorfism i form av en tvingande karaktär tillämpas genom att mindre organisationer tvingas förhålla sig till en större organisation för att överleva inom fältet (DiMaggio & Powell 1983, s.150). I detta sammanhang kan statsmakten som producerar straffbelagd lagstiftning tolkas som den större organisationen i förhållande till de mindre organisationerna som utgörs av myndigheter. Om myndigheterna inte följer dessa lagar, och dess medlemmar begår brott i form av dataintrång, påverkar detta organisationens anseende, vilket i sin tur har inverkan på huruvida organisationen överlever inom organisationsfältet. Att myndigheterna anmäler sina egna anställda för dataintrång kan således tolkas som ett viktigt steg i förtroendebyggande och ett sätt att upprätthålla myten om en rationell organisation.

Olovliga slagningar som genomförs av ren nyfikenhet kan vidare relateras till den modell som Venables (2021, s.1, 9) presenterar, varav *human layer* är en av tre komponenter i att skapa förståelse för cyberrymdens uppbyggnad. Venables (ibid., s.9) framför att den kunskap som människan innehar om cyberrymden och dess karaktär påverkar hur människan agerar. Således kan utbildning bland personal tolkas som en del i utvecklingen av ett starkare cyberförsvar, vilket är något som de intervjuade respondenterna tar upp i relation till tydligare riktlinjer om vad som är tillåtet. Utvecklingen av regelverk kring informationssäkerhet, likt det som Ording, Gao och Chen (2022, s.418) hänvisar till som ISP-utveckling, är ytterligare en aspekt som kan relateras till regelverkets diffusa tydning. Här rekommenderas exempelvis att organisationer tydligt definierar regelverk för att informationssäkerhet ska kunna tillgodose det skydd som är nödvändigt för organisationen.

Bättre definition av regler kan således vara en möjlig åtgärd för myndighetsaktörer i att få djupare förståelse för innebörden av informationshantering (ibid., s.430).

Vidare är utbildning ett tillvägagångssätt som de intervjuade respondenterna framhävde i relation till att förebygga otillåtna slagningar. Detta kan i sin tur relateras till normativ isomorfism, vilket beskrivs utifrån tendensen att fler organisationer anställer personal med samma utbildning och akademisk bakgrund (DiMaggio & Powell 1983, s.152). I detta sammanhang kan däremot konstateras att bristen på kunskap kring vad som är lagligt respektive inte är gällande. Om personalen inom respektive myndighet får utbildning och fortbildning skulle detta kunna bidra till att organisationer får en gemensam uppfattning om hur brottstypen utspelar sig i praktiken, vilket således bidrar till att organisationernas kunskapsnivåer och professionalisering likriktas och agerar utifrån samma förutsättningar. Följaktligen ökar organisationers möjlighet att uppfattas som rationella och överlever således inom fältet (DiMaggio & Powell 1983, s.149; Eriksson-Zetterquist, Kalling & Styhre 2015, s.298).

Utbildning och informationsspridning kan vidare relateras till delar av studiens tidigare forskning som framhäver samarbete i form av kunskapsspridning om cybersäkerhet, vilket inkluderar en förståelse kring konsekvenserna då privat information nås ut till obehöriga aktörer. Exempelvis framhäver Tasevski (2015, s.8) kunskapsspridning i form av informationskampanjer och projekt för att sprida upplysning och inrättandet av en generell cybersäkerhetskultur. Napetvaridze och Chochica (2019, s.176) samt Pravdiuk (2022, s.21) exemplifierar mer samarbete och kunskapsutbyte mellan dels olika professioner, dels mellan utbildningsprogram, för att utveckla en gemensam förståelse för hur information hanteras på ett cybersäkert sätt.

Vidare kan de intervjuade aktörernas uppfattningar om riktlinjernas tolkning analyseras i relation till huruvida lagstiftningen uppfattas som legitim. Intervjuperson C, D, G och H menade att de har uppfattningen att en del slagningar hamnar i gråzonen. Bland annat lyfts exempel i form av att det är skillnad om personen har onda avsikter bakom slagningen

respektive inte. Intervjuperson C menade exempelvis att lagstiftningen bör uppdateras för att lagtexten är förlegad eftersom samma förutsättningar med tjänstemobil inte fanns då lagtexten skrevs. Detta kan således tolkas som att praxis inte uppfattas som legitim (Tyler & Mentovich 2023, s.10), i de sammanhang personer döms för dataintrång utan onda avsikter och endast vill genomföra sitt brottsbeivrande arbete som polis.

Avslutningsvis kan dock konstateras att två respondenter framhävde att det redan finns tillräckliga direktiv på vad som är tillåtet och inte. Intervjuperson A och G betonade att de som är verksamma inom myndigheten ständigt påminns om att slagningar måste vara tjänsterelaterade. Däremot poängteras i detta sammanhang att innebörden av begreppet *tjänsterelaterat* kan tolkas varierande, vilket således medför problematik i yrkesutövningen i vad som uppfattas som tillåtet respektive inte.

7.3 Natodiskursen

Inledningsvis kan konstateras att Sveriges inträde i Nato inte har berört de intervjuade aktörernas verksamhet i större utsträckning. I vad aktörerna tror att Nato kan medföra för möjligheter framfördes samarbete som ett alternativ, varav Intervjuperson A, F och H poängterade att det redan finns ett existerande samarbete med Europol och Interpol, samtidigt som Intervjuperson C och F framhävde att samarbetet med de nordiska länderna kan öka (jfr. Bennesved, Ingemarsdotter & McWilliams 2023, s.4). Ett förbättrat samarbete kan exempelvis kopplas till det Ilie et al. (2011, s.440) och Jacuch (2021, s.110) framhäver i form av att samordnade åtgärder mellan aktörer bidrar till ett effektivare cyberförsvar. Vidare kan vikten av samarbetet relateras till bättre förutsättningar för kompetensutveckling som Gao och Chen (2022, s.699-700) samt Pleta, Karasov och Jakštas (2018, s.568, 576) menar att Nato kan medföra i cybersäkerhetsfrågor.

Generellt uppfattade samtliga respondenter att lagstiftningen, samt betraktandet av dataintrång, inte kommer att påverkas av att Sverige gått med i Nato. Intervjuperson B, som arbetar som rådman, hänvisade däremot till hur tillämpningen av lagstiftningen kan förväntas komma att präglas av nya tendenser i och med det svenska Natomedlemskapet.

Detta motiverades vidare i hur dataintrång är lätt att bevisa och att detta lagrum sålunda kommer åberopas vid lagföring av säkerhetshotande verksamheter. Mot detta kan lagen antas komma att tillämpas i större utsträckning i och med inträdet i Nato. Påståendet om dessa nya tillämpningsmöjligheter företräddes sedermera av att Intervjuperson B uttalat att en konsekvens av Natomedlemskapet kan förväntas i hur nya fiender kommer leda till en förändrad hotbild. Dessa två påståenden kan vidare förstås som en indikation på att behovet av lagföring för säkerhetshotande verksamhet kommer att öka.

Detta är sedermera intressant utifrån det som påträffades i studiens litteraturöversikt, där statens hantering i bemötandet av cyberbrottslighet och hur detta uppfattas av befolkningen är betydande. Det lyfts hur denna uppfattning kan ha koppling till förtroendet och den upplevda legitimiteten hos staten genom att det blir en uppvisning av dennes avskräckningsförmåga (Devanny, Goldoni & Medeiros 2022, s.34), vilket sedermera kan antas grundas i att statens agerande stämmer överens med medborgarnas uppfattningar om sociala värden (Tyler 2006, s.7, 165-166; Sunshine & Tyler 2003, s.524-535). Utifrån denna uppfattning kan lagstiftningen om dataintrång antas inneha förmåga som avskräckningsverktyg, i hur dennes lätthet för bevisning i större utsträckning möjliggör lagföring, vilket i sin tur utgör statens bemötande av cyberbrottslighet.

Avskräckning av brottslighet har vidare lyfts som en viktig komponent inom staters försvar (jfr. Bennesved, Ingemarsdotter & McWilliams 2023, s.2-3; jfr. Prop 2022/23:74, s.24), och utifrån den avskräckande aspekten som kan utläsas ur Intervjuperson B:s uttalande förklaras sålunda lagrummet för dataintrång få en avsevärd betydelse i hanteringen av den ökade hotbild som tros komma med Natomedlemskapet. Här kan däremot bedömas vidare relevant att beakta den möjliga risk med ökad statlig sanktionering som Lobato och Kenkel (2015, s.23-24, 38-39) lyfter i hur sådan tendens, på grund av cybersäkerhetens sträckning över både den offentliga och privata sektorn, kan få konsekvenser i en begränsning av grundläggande fri- och rättigheter. Därigenom ställs potentiella möjligheter och risker med ökad lagföring för dataintrång i motsättning till varandra och antas således indikera på en viss komplexitet i den tänkbara utvecklingen i och med inträdet i Nato.

Sju av respondenterna framhävde att cybersäkerhet är en viktig del av myndighetsverksamheten i helhet, däremot var arbetet i att stärka försvaret inget som direkt berörde aktörernas verksamhet enligt Intervjuperson A, B, C, D och F. Trots att de således inte såg en direkt påverkan på deras arbete, erkände de behovet av riktlinjer och åtgärder för att hantera eventuella hot mot säkerheten. Vidare lyfte Intervjuperson B hur Natomedlemskapet kan komma att påverka Sveriges säkerhetssituation genom den ändrade hotbild som uppstår i samband med nya allierade, respektive fiender. Följaktligen lyfts hur den typen av personer som kan antas gynnas av att angripa Sveriges system för att utvinna information kommer att ändras. Däribland uttryckte Intervjuperson B hur intryck av detta även kan visas i motivationen hos många inom offentlig verksamhet och en vilja att göra slagningar som inte är okej kan på så sätt öka. Här kan Intervjuperson B och C:s utsagor tilläggas om befintlig risk för infiltrering då rekrytering av fel personer kan leda till att människor med en dold agenda kan få anställning inom myndigheterna.

Detta resonemang är vidare intressant att sätta i förhållande till Venables (2021, s.9) begrepp *human layer*. Begreppet betonar mänskliga funktioner i dennes mottaglighet för påverkan, och betonar människans roll och betydelse i cyberrymden (ibid.). Denna påverkan kan sålunda antas bli synlig i de resonemang som Intervjuperson B, respektive C fört fram, och på så sätt blir dessa styrkta av Venables (ibid.) argument.

Avslutningsvis kan en kritisk reflektion i förhållande till analysavsnittet lyftas gällande vald teoretisk ansats i relation till den empiri som berörde Nato. Respondenterna konstaterade att medlemskapet inte märkts av i större utsträckning, vilket kan vara en konsekvens av att medlemskapet gick igenom våren år 2024, vilket var samma år som denna studie författades. Med anledning av studiens deduktiva angreppssätt (Bryman 2018, s.47-49) konstateras att den tidigare forskningen har störst relevans inom detta tema eftersom det är svårt att analysera legitimitet och institutionella förändringar när medlemskapet inte blivit tillräckligt påtagbart än.

8. Avslutande diskussion

Detta avsnitt inleds med en diskussion för att sedan presentera studiens slutsatser och förslag på framtida forskning. Slutsatserna relateras till undersökningens syfte och frågeställningar.

8.1. Diskussion

Syftet med arbetet var att undersöka svensk cybersäkerhet och den rättsliga kapaciteten inom området med hänsyn till ett svenskt medlemskap i Nato och dess potentiella påverkan på nationellt cyberförsvar. Särskild uppmärksamhet riktades mot svensk lagstiftning kring dataintrång, med fokus på olovliga registerslagningar som främst utförs via anställning inom myndighet. Sålunda föreslogs ett inifrån-ut-perspektiv där fokus lades på tänkbara försvarsåtgärder gentemot inhemska aktörer. För att uppfylla syftet utformades två frågeställningar vilka genom studien ämnades besvaras.

För att uppnå syftet valdes ett kvalitativt angreppssätt i form av semistrukturerade intervjuer. Syftet med intervjuerna var att utforska uppfattningar hos verksamma inom brottsbekämpande myndigheter i Sverige, där relevans bedömdes i ett övervägande fokus på Polismyndigheten. På så sätt möjliggjordes erhållandet av för studien intressanta och nyanserade infallsvinklar vilka sedermera utgjorde underlag för analys. Sålunda möjliggjordes en djupare förståelse för uppfattningar kopplade till dataintrång och det svenska Natomedlemskapet, medan inkluderingen av ytterligare två myndigheter, utöver Polismyndigheten, bidrog med kompletterande perspektiv, intressanta för arbetet. Däremot valdes en teoretisk ansats bestående av delar som ofta förankras med kvantitativ forskning i och med anammandet av Tylers (2022) legitimitetsbegrepp. Detta val har tidigare motiverats utifrån intresset i bidraget till kompletterande infallsvinklar (se rubrik “4.1 Legitimitetsteori” och “5.1 Studiens utformning”), men vidare kan en kritisk diskussion kring ett sådant metodologiskt förfarande vara väsentlig.

Här kan en diskussion föras gällande kunskapsteoretiska frågor i relation till studiens tillvägagångssätt i förhållande till val av teoretisk ansats. Bryman (2018, s.51-52, 54-56) lyfter två huvudsakliga perspektiv kopplade till epistemologiska frågor, ett naturvetenskapligt perspektiv relaterat till positivism, samt ett interpretativistiskt perspektiv som betonar tolkning. Webers (1983, s.3-5) arbete främhäver i huvudsak ett förståelseinriktat perspektiv med betoning på meningsskapande och tolkning i relation till människors kunskap och handlingar. Fokus på förståelse och tolkning, framför positivistisk vetenskap, är vidare något som Meyers och Rowans (1977, s.343) samt DiMaggios och Powells (1983, s.150, 158) studier kan tolkas fokusera på genom studiet av hur organisationer påverkas av och bemöter sociala normer och institutionella förändringar.

Däremot skiljer sig Tylers (2022) legitimitet från tolkningsperspektivet eftersom denna åskådning av legitimitet baseras på ett kvantitativt angreppssätt, med fokus på det som är mätbart. Således konstateras att delar av Tylers arbete kan härledas från ett positivistiskt synsätt där legitimitet tolkas som en mätbar fråga (Bryman 2018, s.51, 61). I och med det kvalitativa angreppssätt som valts för studien har Tylers (2022) legitimitetsbegrepp därför använts för en annan tolkning där betydelsen av legitimitet sätts i relation till människors förståelse och tolkning (jfr. Dalen 2015, s.18-19), vilket sedermera innebär att riktningen för studien blir något avvikande från ursprunget till Tylers (2022) användning av legitimitetsbegreppet. Detta synliggörs genom hur studiens resultat motsvarar ett inifrån-perspektiv tillhandahållet av professionellt förankrade åsikter kring legitimitet, istället för vad som varit Tylers tidigare huvudfokus, ett perspektiv utifrån, som kommer från allmänhetens personliga legitimitetsuppfattningar (jfr. Tyler 2022, s.762).

Vidare kan känsligheten i studiens natur lyftas. Detta då fokus delvis har varit att undersöka inställningar för brottsligt beteende inom myndigheter. I och med denna känsliga karaktär skulle ett kvantitativt tillvägagångssätt vara passande i och med att det inte skulle medföra samma personliga kontakt som för den forskningsdesign som förelåg undersökningen. Däremot går det kvalitativa tillvägagångssättet mer i linje med studiens syfte i och med dennes karaktärisering av att skapa förståelse, framför att mäta förekomst eller omfång

(Bryman 2018, s.454-455). Det anses däremot nödvändigt att förtydliga att studien inte behandlat något särskilt rättsfall, samt att studiens respondenter inte har någon koppling till de domar som framgår i bilaga 1. Målet med studien har inte varit att rikta in sig på dömda myndighetsutövare då detta skulle innebära en ökad känslighet.

8.2 Slutsatser

Den första frågeställningen som förelåg arbetet var "Hur uppfattar aktörer inom svensk brottsbekämpande myndighetsverksamhet olovliga registerslagningar i relation till legitimitet och rättssäkerhet?". Här tyder analysen på att respondenterna inom sin myndighetsverksamhet såg olovliga registerslagningar som en allvarlig fråga som både påverkar legitimitet och rättssäkerhet. Rättssäkerheten lyftes som en betydande komponent inom myndigheterna och deras verksamheter, och förekomsten av olovliga registerslagningar ansågs kunna drabba denna negativt. Bristande rättssäkerhet framhölls sedermera få negativa konsekvenser för det allmänna förtroendet till myndigheterna, vilket vidare betonades som avgörande för deras verksamhet. Ett bristande förtroende ansågs fortsättningsvis hänga ihop med brister i legitimitet, och lyftes kunna leda till att allmänhetens samarbete med myndigheter riskerar att minska, vilket i sin tur blir en försvårande omständighet för myndigheternas arbete. Sålunda pekar analysen på att en upplevd legitimitet är beroende av hur allmänheten bedömer myndighetens agerande, samt blir avgörande för myndighetsverksamheten i stort.

Den andra frågeställningen som undersökningen ämnade besvara var "Vilka förväntade rättsliga effekter tror brottsbekämpande myndighetspersonal att Sveriges Natomedlemskap kan ha på cybersäkerheten och förekomsten av olovliga registerslagningar inom myndigheter?". Enligt den del av analysen som behandlar denna undersökningsfråga förväntade sig inte respondenterna att Sveriges medlemskap i Nato kommer att påverka förekomsten av olovliga registerslagningar i större utsträckning. Däremot betonades vikten av samarbete för att stärka det svenska försvaret och därtill cybersäkerheten. Det påpekades vidare att hotbilden kan förändras med Natomedlemskapet i hur detta kan tänkas öka risken för slagningar med icke gynnsamma motiv, därtill även risken för ökad infiltration inom

myndigheter. Det betonades också att behovet av riktlinjer och åtgärder för att hantera säkerhetshot förblir relevant, oavsett Natomedlemskapet.

Denna studie har framhävt förekomsten av olovliga registerslagningar inom myndigheter (se bilaga 1), och sammantaget har analysen bidragit med en djupare insikt i hur aktörer inom svensk brottsbekämpande myndighetsverksamhet betraktar brottstypen olovliga registerslagningar i relation till legitimitet och rättssäkerhet, samt förväntade rättsliga effekter av Natomedlemskapet kopplat till dessa aktiviteter. Det understryks hur behovet av tydliga riktlinjer, utbildning och samarbete för att upprätthålla laglighet och förtroende inom myndighetsverksamheten blir väsentligt även i ett förändrat säkerhetspolitiskt sammanhang, och slutsatserna kan därför antas intressanta ur ett rättssociologiskt perspektiv på regelefterlevnad i en säkerhetsrelaterad kontext (jfr. Baier, Svensson & Nafstad 2018, s.74-76).

8.3 Framtida forskning

Mot bakgrunden att cyberhot är ett ytterst utspritt fenomen finns det en stor mängd aspekter som kan bli relevanta att undersöka i framtiden. I denna studie har flertalet infallsvinklar som väckt intresse påträffats, men som vidare inte varit möjliga att inkludera på grund av studiens begränsade omfång. Bland annat framkom det ur intervjuerna hur andra lagstiftningar än dataintrång primärt förväntades påverkas av det svenska Natomedlemskapet. Denna iakttagelse skulle sålunda förespråka att studie av svensk rättslig kapacitet i upprätthållande av cybersäkerhet i relation till Natomedlemskapet, framöver blir relevant att undersöka utifrån andra eller flera lagrum.

Fortsättningsvis var rättskultur ett begrepp som togs upp av en av studiens respondenter men som, på grund av studiens omfång, inte behandlades i större utsträckning. Att diskutera och analysera rättskultur som begrepp i relation till betraktandet av myndighetsverksamhet är därför något som bedöms intressant att studera närmare, vilket förslagsvis kan utvecklas i framtida forskning.

Ett ytterligare begrepp som åskådliggjorts i arbetet är *procedural justice,* men då studien valde att utgå från legitimitetsbegreppet specifikt så gavs teorin inte något större fokus. Det skulle därför fortsatt kunna vara av intresse att tillämpa *procedural justice* och dess helhetliga innebörd i en svensk kontext, inom vilken vid tiden för utförd undersökning, det påvisats föreligga en påfallande kunskapslucka gällande myndighetsverksamhet och dennes relation till nationell cybersäkerhet (se rubrik "3.4 Slutsatser av tidigare forskning").

Referenslista

Baier, M., Nafstad, I. & Svensson, M. (2018). *Om rättssociologi*. Lund: Studentlitteratur.

Bennesved, P., Ingemarsdotter, J. & McWilliams, A. (2023). *Hur påverkar ett Natomedlemskap civilt försvar? Perspektiv från Norge och Danmark.* FOI Totalförsvarets forskningsinstitut. https://www.foi.se/rest-api/report/FOI%20Memo%208233 [2024-03-24]

Boréus, K. & Kohl, S. (2018). Innehållsanalys. I Bergström, G. & Boréus, K. (red.) 4 uppl. *Textens mening och makt: metodbok i samhällsvetenskaplig text- och diskursanalys.* Lund: Studentlitteratur.

Brottsförebyggande rådet. (2022). Klassificering av brott. 2022_Kla Klassificering av brott v 10.2.pdf [2024-03-24]

Bryman, A. (2018). *Samhällsvetenskapliga metoder*. 3 uppl. Malmö Liber.

Carrapico, H. & Farrand, B. (2017). Dialogue, partnership and empowerment for network and informations security: the changing role of the private sector from objects of regulation to regulation shapers, *Crime law and Social change,* 67(3), s.245-263. doi: 10.1007/s10611-016-9652-4.

Dalen, M. (2015). *Intervju som metod*. 2 uppl. Malmö: Gleerups.

Denscombe, M. (2018). *Forskningshandboken: för småskaliga forskningsprojekt inom samhällsvetenskaperna.* 4 uppl. Lund: Studentlitteratur AB.

Devanny, J. Goldoni, L. R. F., & Medeiros, B. P. (2022). Strategy in an Uncertain Domain: Threat and Response in Cyberspace, *Journal of Strategic Security,* 15(2), s.33-47. doi: 10.5038/1944-0472.15.2.1954.

DiMaggio, P.J. & Powell, W.W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields, *American Sociological Review*, 48(2), s.147-160. doi: 10.2307/2095101

Efthymiopoulos, M.P. (2019). A cyber-security framework for development, defense and innovation at NATO, *Journal of Innovation and Entrepreneurship*, 8(1), s.1-26, doi: 10.1186/s13731-019-0105-z.

Eneman, M., Ljungberg, J., Raviola, E. & Rolandsson, B. (2022). The sensitive nature of facial recognition: Tensions between the Swedish police and regulatory authorities, *Information Polity*, 27(2), s.219–232. doi:10.3233/IP-211538.

Engdahl, O. & Larsson, B. (2011). *Sociologiska perspektiv - grundläggande begrepp och teorier*. 2 uppl. Studentlitteratur: Lund.

Eriksson-Zetterquist, U. (2009). *Institutionell teori: idéer, moden, förändring*. Liber AB: Stockholm.

Eriksson-Zetterquist, U., Kalling, T. & Styhre, A. (2015). *Organisation och organisering.* 4 uppl. Liber AB: Stockholm.

Europaparlamentet och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF. (EUT L 218 14.08.2013, s.8–14). [2024-03-18] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32013L0040

Försvarshögskolan. (2023). Förutsättningar för krisberedskap och totalförsvar i Sverige. https://fhs.diva-portal.org/smash/get/diva2:1805339/FULLTEXT03.pdf [2024-03-23]

Gao, X. & Chen, X. (2022). Role enactment and the contestation of global cybersecurity governance, *Defence Studies,* 22(4) s.689-708. doi: 10.1080/14702436.2022.2110485.

Givens, A.D., Busch, N.E., & Bersin, A.D. (2018). Going global: The international dimensions of U.S homeland security policy, *Journal of Strategic Security,*11(3), s.1-34. doi: 10.5038/1944-0472.11.3.1689.

Hart, C. (2018). *Doing a literature review: releasing the research imagination*. 2 uppl. Los Angeles: SAGE.

Hugyik, A. (2020). Best practices in the application of the concept of resilience: building hybrid warfare and cybersecurity capabilities in the hungarian defense forces, *Connections*, 19(4), s.25–38. doi:10.11610/Connections.19.4.02.

Hydén, H. (2002). *Rättssociologi som rättsvetenskap*. Lund: Studentlitteratur AB.

Iancu, E-A.,Tuşa, E., Iancu, N., Simion, E. & Moise, A-C. (2023). Preventing computer crimes by knowing the legal regulations that ensure the protection of computer systems, *Juridical Tribune,* 13(3), s.365-383. doi: 10.24818/TBJ/2023/13/3.03.

Ilie, M., Mutulescu, A-S., Artene, D.A., Bratu, S. & Fainsi, F. (2011). International Cyber Security through Co-Operation, *Economics, Management & Financial Markets*, 6(2), s.438–448. https://ludwig.lub.lu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=bth&AN=64433435&site=eds-live&scope=site [2024-03-26]

Integritetsmyndigheten. (2023). *Brottsbekämpande verksamheter och personuppgiftsbehandling.* https://www.imy.se/bdl [2024-05-27]

Jacuch, A. (2021). Comparative analysis of cybersecurity strategies. European union strategy and policies. Polish and selected countries strategies, *Online journal modelling the new europe*, (37), s.102-120. doi: 10.24193/OJMNE.2021.37.06

Kelly, N. & Montasari, R. (2023). Police and Cybercrime: Evaluating Law Enforcement's Cyber Capacity and Capability. I Montasari, R. (red). *Applications for Artificial Intelligence and Digital Forensics in National Security.* Cham: Springer International Publishing. doi: 10.1007/978-3-031-40118-3.

Komalasari, R. and Mustafa, C. (2023). A Healthy Game-Theoretic Evaluation of NATO and Indonesia's Policies in the Context of International Law, *Jurnal Pertahanan: Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism & Integrity*, 9(2), s.333–349. doi: 10.33172/jp.v9i2.16794

Kronofogden. (u.å). *Uppdrag och värdegrund.* https://kronofogden.se/om-kronofogden/uppdrag-och-vardegrund [2024-05-24]

Levi, M., Sacks, A. & Tyler, T. (2009). Conceptualizing legitimacy, measuring legitimating beliefs, *American Behavioral Scientist,* 53, s.354-375. doi: 10.1177/0002764209338797.

Lindskog, E., Huuva, L., Lehtinen, S. & Shannon, D. (2022). *Polisanmälda dataintrång: Karaktär, utmaningar, utvecklingsområden.* Brottsförebyggande rådet. https://bra.se/download/18.57223f611841889cd023b5/1666871966529/2022_Polisanmalda_dataintrang.pdf [2024-03-24]

Lindstedt, I. (2019). *Forskningens hantverk*. 2 uppl. Lund: Studentlitteratur.

Lindstrom, G. & Luiijf, E. (2012). Political aims & policy methods. I Klimburg, A. (red). *National Cyber Security Framework Manual.* NATO CCD COE Publication: Tallinn.

Lobato, L. C. & Kenkel, K. M. (2015). Discourses of cyberspace securitization in Brazil and in the United States, *Revista Brasileira de Política Internacional,* 58(2), s.23-43. doi: 10.1590/0034-7329201500202.

Lonardo, L. (2021). EU Law Against Hybrid Threats: A First Assessment, *European Papers*, 6(2), s.1075–1096. doi: 10.15166/2499-8249/514

Lundin, L-E. & Magnusson, G. (2022). På allvar. Svensk säkerhetspolitik i ofärdstider. Slutrapport från SES-projektet. *Kungl Krigsvetenskapsakademien.*

Meares, T. L., Tyler, T. R. , & Gardener, J. (2015). LAWFUL OR FAIR? HOW COPS AND LAYPEOPLE PERCEIVE GOOD POLICING, *The Journal of Criminal Law and Criminology,* 105 (2), s.297-343. http://www.jstor.org/stable/26402450 [2024-04-18]

Meyer, J.W & Rowan, B. (1977). Institutionalized Organizations: Formal structure as Myth and Ceremony, *American Journal of Sociology*, 83(2), s.340-363. http://www.jstor.org/stable/2778293 [2024-04-09]

Meyer, J. (2021). Institutional Theory and World Society (2009). I Jepperson, R.L. & Meyer, J.W. (red.) *Institutional Theory: The Cultural Construction of Organizations, States, and Identities*. Cambridge: Cambridge University Press. doi: 10.1017/9781139939744.011.

Montasari, R. (2023). Countering Cyberterrorism. The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity. *Cham: Springer International Publishing.* doi: 10.1007/978-3-031-21920-7.

Montasari, R. (2024). Cyberspace, Cyberterrorism and International Security in the Fourth Industrial Revolution. *Cham: Springer Nature.* doi: 10.1007/978-3-031-50454-9

Myndigheten för samhällsskydd och beredskap (2024). *Vad är NATO?* https://www.msb.se/sv/vart-att-veta-om-nato/vad-ar-nato/ [Hämtad 21-03-24]

Månson, P. (2007). Max Weber. I Andersen, Heine & Kaspersen, Lars Bo (red.) *Klassisk och modern samhällsteori*. 3 uppl. Lund: Studentlitteratur

Napetvaridze, V. & Chochia, A. (2019). Cybersecurity in the making-policy and law: A case study of Georgia, *International and Comparative law review,* 19(2), s.155-180. doi: 10.2478/iclr-2019-0019.

National cyber security centre. (2016). *Glossary*. https://www.ncsc.gov.uk/section/advice-guidance/glossary [2024-03-24]

Nato (2023). *Cyber defence.* https://www.nato.int/cps/en/natohq/topics_78170.htm [2024-03-22]

Ording, L.G, Gao, S. & Chen, W. (2022). The influence of inputs in the information security policy development: an institutional perspective, *Transforming Government: People, Process and Policy*, 16(4), s.418–435. doi: 10.1108/TG-03-2022-0030.

Pleta, T., Karasov, S. & Jakštas, T. (2018). The means to secure critical energy infrastructure in the context of hybrid warfare: The case of Ukraine, *Journal of security and sustainability issues,* 7(3), s.567-577. doi: 10.9770/jssi.2018.7.3(16).

Polisen. (2023). *Uppdrag och mål*. https://polisen.se/om-polisen/uppdrag-och-mal/ [2024-05-24]

Pravdiuk, A. (2022). The state and current issues of legal regulation of cyber security in Ukraine, *European political and law discourse,* 9(3): s.19-28. doi: 10.46340/eppd.2022.9.3.3.

Regeringskansliet (2023). *Myndigheter.* https://www.regeringen.se/lattlast-information-om-regeringen-och-regeringskansliet/myndigheter/ [2024-05-02]

Regeringskansliet (2024a). *Detta är NATO.* https://www.regeringen.se/regeringens-politik/sverige-i-nato/detta-ar-nato/ [2024-03-21]

Regeringskansliet (2024b). *Sveriges roll i Nato.* https://www.regeringen.se/regeringens-politik/sverige-i-nato/sveriges-roll-i-nato/ [2024-03-21]

Rådets rambeslut 2005/222/RIF av den 24 februari 2005 om angrepp mot informationssystem (EUT L 69 16.03.2005, s.67–71). https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32005F0222 [2024-03-18]

Semenenko, O., Dobrovolsky, U., Sliusarenko, M., Levchenko, I. & Mytchenko, S. (2023). Legal aspects of the cybertechnology development and the cyberweapon use in the state defence sphere: Global and Ukrainian experience, *Social and legal studios,* 6(4): s.192-199. doi: 10.32518/sals4.2023.192.

Shopina, I., Dmytro, K., Khrystynchenko, N., Zhukov, S. & Shpenov, D. (2020). Cybersecurity: legal and organizational support in leading countries, NATO and EU standards, J*ournal of security and sustainability issues,* 9(3): s.977-992. doi: 10.9770/jssi.2020.9.3(22).

Stoddart, K. (2022). *Cyberwarfare. Threats to Critical Infrastructure.* Cham: Springer International Publishing. doi: 10.1007/978-3-030-97299-8.

Stoltenberg, J. (2019). *The Secretary General's Annual Report.* Nato. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf [2024-03-22]

Sunshine, J., & Tyler, T. R. (2003). The role of procedural justice and legitimacy in shaping public support for policing, *Law & Society Review,* 37(3), 513–548. doi: 10.1111/1540-5893.3703002

Svensson, P. (2023). En helt egen tröskel för tillåtlighet - mostridiga domar när poliser åtalas för dataintrång, *Norstedts juridik*, 17 oktober. https://www.nj.se/nyheter/en-helt-egen-troskel-for-tillatlighet-motstridiga-domar-nar-poliser-atalas-for-dataintrang [2024-04-26]

Sveriges Domstolar. (2022). *Domare - ett ansvarsfullt och utvecklande arbete.* https://www.domstol.se/jobba-hos-oss/sa-blir-du-domare/om-domaryrket/ [2024-05-24]

Sörensen, K. (2023). *Kort om avskräckning*. FOI Totalförsvarets forskningsinstitut. https://www.foi.se/rest-api/report/FOI%20Memo%208204 [2024-05-23]

Tasevski, P. (2015). Macedonian Path Towards Cybersecurity, *Information & Security*, 32(2), s.1–11. doi: 10.11610/isij.3204.

Träskman, P. & Wennberg, S. (2019). *Brottsbalken. En kommentar. Del 1. Studentutgåva.* Stockholm: Norstedts Juridik.

Tyler, T.R. (1988). What is Procedural Justice?: Criteria used by Citizens to Assess the Fairness of Legal Procedures. *Law & Society Review,* 22(1), s.103-136. doi: 10.2307/3053563.

Tyler, T. R. (2003). Procedural justice, legitimacy, and the effective rule of law. I M. H. Tonry (red.). *Crime and justice: A review of research.* Chicago; London: University of Chicago Press.

Tyler, T. R. (2006). *Why People Obey the Law*. Princeton University Press. doi: 10.2307/j.ctv1j66769.

Tyler, T. R. (2022). Understanding the Psychology of Social Order, *American Journal of Comparative Law,* 69 (4), s.784-776. doi:10.1093/ajcl/avac001

Tyler, T. R. & Mentovich, A. (2023). Mechanisms Of Legal Effect: Procedural Justice Theory. *Temple University Beasley School of Law.* https://phlr.org/sites/default/files/downloads/resource/CPHLR-TheoryMethods2023_ProceduralJustice.pdf [2024-04-15]

Urinboyev, R., Wickenberg, P. & Leo, U. (2016). Child Rights, Classroom and School Management: A Systematic Literature Review, *International Journal of Children's Rights*, 24(3): s.522–547. doi:10.1163/15718182-02403002.

Venables, A. (2021). Modelling Cyberspace to Determine Cybersecurity Training Requirements, *Frontiers in Education,* 6, doi: 10.3389/feduc.2021.768037.

Vetenskapsrådet. (2017). *God forskningssed*. Stockholm: Vetenskapsrådet.

Warner, C. (2023). Law Enforcement and Digital Policing of the Dark Web: An Assasment to the Technical, Ethical and Legal Issues. I Montasari, R. (red). *Applications for Artificial Intelligence and Digital Forensics in National Security.* Cham: Springer International Publishing. DOI: 10.1007/978-3-031-40118-3.

Weber, M. (1983). *Ekonomi och samhälle: förståendesociologins grunder. 1 Sociologiska begrepp och definitioner. Ekonomi, samhällsordning och grupper.* Lund: Argos.

Willers, J-O. (2021). Seeding the cloud: Consultancy services in the nascent field of cyber capacity building, *Public administration.* doi: 10.1111/padm.12773.

Åklagarmyndigheten. (u.å). *Rättssäkerhet*.
https://www.aklagare.se/ordlista/r/rattssakerhet/ [2024-05-11]

Författningar (SFS)

SFS 1962:700. *Brottsbalk*.

SFS 1973:289. *Datalagen*.

SFS 1998:204. *Personuppgiftslagen*.

SFS 2014:302. *Lag om ändring i brottsbalken.*

Offentliga tryck

Propositioner

Prop. 2003/04:164. *Sveriges antagande av rambeslut om angrepp mot informationssystem.*

Prop. 2006/07:66. *Angrepp mot informationssystem.*

Prop. 2013/14:92. *Skärpt straff för dataintrång.*

Prop. 2022/23:74. *Sveriges medlemskap i Nato.*

Direktiv

Dir. 2011:98. *Tillträde till Europarådets konvention om it-relaterad brottslighet med tilläggsprotokoll*.

Bilagor

Bilaga 1. Dataintrångsdomslut

Tingsrätt	Domar med brottsrubricering dataintrång	Friad från dataintrång, olovlig registerslagning inom myndighet (Mål.nr)	Dömd för dataintrång, olovlig registerslagning inom myndighet (Mål.nr)	Både friad från, och dömd för dataintrång, olovlig registerslagning inom myndighet (Mål.nr)
Attunda tingsrätt	12	1. B 3317-21 2. B 3657-21	1. B 344-23 2. B 11863-22	-
Blekinge tingsrätt	4	-	-	-
Göteborgs tingsrätt	9	-	1. B 6286-23	1. B 7681-23
Halmstads tingsrätt	6	-	-	-
Hälsinglands tingsrätt	1	-	-	-
Jönköpings tingsrätt	5	-	1. B 2598-21	-
Kalmar tingsrätt	9	-	1. B 1249-20 2. B 1769-19	-
Kristianstads tingsrätt	4	-	1. B 322-20	1. B 1926-19
Linköpings tingsrätt	9	1. B 4178-20	1. B 884-23 2. B 1126-21 3. B 3042-21	1. B 1665-20 2. B 1882-20
Luleå tingsrätt	10	-	1. B 277-19	-
Lunds tingsrätt	22	-	1. B 6140-18 2. B 6980-21	1. B 6328-21
Lycksele tingsrätt	5	-	1. B 322-21	-
Malmö tingsrätt	7	1. B 6020-19 2. B 12739-21	1. B 2149-22 2. B 5212-19 3. B 11163-18	-
Nacka tingsrätt	2	-	1. B 588-21	-

Norrköpings tingsrätt	4	-	-	-
Nyköpings tingsrätt	3	-	-	-
Skaraborgs tingsrätt	5	-	1. B 2472-21	-
Södertälje tingsrätt	2	-	1. B 1631-22	-
Södertörns tingsrätt	8	-	1. B 18304-23 2. B 18891-22 3. B 3389-22 4. B 16809-20 5. B 17865-21	-
Stockholms tingsrätt	12	-	1. B 348-20 2. B 411-20 3. B 3700-21 4. B 6579-21	1. B 2390-19 2. B 15404-19
Umeå tingsrätt	8	-	-	-
Varbergs tingsrätt	3	-	1. B 1495-19 2. B 2819-21	1. B 570-20
Vänersborg tingsrätt	8	1. B 1165-20	1. B 999-22 2. B 3681-21	-
Värmlands tingsrätt	1	-	1. B 295-19	-
Västmanlands tingsrätt	15	-	1. B 3365-22 2. B 5470-19	-
Ystad tingsrätt	5	-	-	-
Ångermanlands tingsrätt	4	-	1. B 2604-22	-
Östersunds tingsrätt	11	-	1. B 714-21	-
Totalt:	194	6	38	8

Bilaga 2. Deskriptiv analys

Författare	År	Språk	Geografisk avgränsning	Nyckelord
Carrapico, H. & Farrand, B.	2017	Eng	EU	Network governance, network information security, regulation, regulatory capitalism
Devanny, J. Goldoni, L. R. F., & Medeiros, B. P.	2022	Eng	Estland, Georgien, Ukraina, USA	Saknas
Efthymiop oulos, M.P.	2019	Eng	Nato	Business resilience, collective defense, cyber-security, entrepreneurship, innovation, management, military, NATO, network-centric operations. Strategy
Eneman, M., Ljungberg, J., Raviola, E. & Rolandsso n, B.	2022	Eng	Sverige	Surveillance, facial recognition, privacy, affordance, legitimacy, police authority, regulatory authorities, institutional dialogue, qualitative document analysis
Gao, X. & Chen, X.	2022	Eng	EU, USA	Cyberspace, European Union, interpolarity
Givens, A.D., Busch, N.E., & Bersin, A.D.	2018	Eng	USA	Saknas
Hugyik, A.	2020	Eng	Ungern	Cyber defense, EU, Hungary, hybrid warfare, intelligence, military, NATO, resilience, security policy
Iancu, E-A.,Tuşa, E., Iancu, N., Simion, E. & Moise, A-C.	2023	Eng	Rumänien, EU	Criminal offence, cyber security, cyber space, education, law
Ilie, M., Mutulescu, A-S., Artene, D.A., Bratu,	2011	Eng	EU	Co-operation, cyber crime, cyber warfare, law enforcement, peace, security

S. & Fainsi, F.				
Jacuch, A.	2021	Eng	EU, Polen	Cybersecurity, cyberspace, EU cyber security and policies, national cyber security strategy
Komalasari, R. & Mustafa, C.	2023	Eng	Indonesien, Nato	Cyber terrorism, game theory, conflict resolution, military science
Lobato, L. C. & Kenkel, K. M.	2015	Eng	Brasilien, USA	Copenhagen school; cyberspace; international security; securitization
Lonardo, L.	2021	Eng	EU, Nato	Eu law, external relations, security and defence, hybrid threats, disinformation, competence, law, law of Europe, KJ-KKZ
Napetvaridze, V. & Chochia, A.	2019	Eng	Georgien	Cybersecurity, georgia, international telecommunication union, ranking
Ording, L.G, Gao, S. & Chen, W.	2022	Eng	Sverige	Information security policy development, information security, inputs, institutional theory, social-organisationl perspective
Pleta, T., Karasov, S. & Jakštas, T.	2018	Eng	Ukraina	Critical infrastructure protection, cybersecurity, cybersecurity legislation, hybrid warfare, Ukraine
Pravdiuk, A.	2022	Eng	Ukraina	Cyber defense, cyber protection, cybersecurity, cyberspace, information law, information security, information society
Semenenko, O., Dobrovolsky, U., Sliusarenko, M., Levchenko, I. & Mytchenko, S.	2023	Eng	Ukraina, Tyskland, Frankrike, Storbritannien och Indonesien	Computer attacks, digital development, information wars, national security, virtual space
Shopina, I., Dmytro, K., Khrystynchenko, N.,	2020	Eng	Nato, EU, Ukraina, Frankrike, USA och Storbritannien	Cyber defense, cybersecurity, cyberspace

Zhukov, S. & Shpenov, D.				
Tasevski, P.	2015	Eng	Makedonien	Macedonia, cyber, establishment, MKD-CIRT, strategy, security
Venables, A.	2021	Eng	Nato	Cyber operations; cyber situational awareness: cybersecurity; cybersecurity training; cyberspace; threat modelling
Willers, J-O.	2021	Eng	Framgår ej	Saknas

Bilaga 3. Intervjuguide

Inledande information

Inledningsvis tänkte vi informera om studiens syfte och vad intervjun har för roll i studien. Vi ämnar att studera hur dataintrångsbrottet olovlig registerslagning uppfattas enligt olika aktörer inom domstolsväsendet och andra rättstillämpande myndigheter. Vi vill undersöka hur dessa aktörer uppfattar gällande lagstiftning om olovlig registerslagning, dennes förhållande till frågor rörande rättssäkerhet och legitimitet och Sveriges roll som medlemsstat i Nato.

Vi som författar denna uppsats är två studenter som läser kandidatprogrammet inom kriminologi med inriktning rättssociologi vid Lunds universitet. Den färdiga uppsatsen kommer att publiceras på LUP Student Papers, som tillhör universitetet, där du som deltagare får möjlighet att läsa uppsatsen i samband med uppsatsens publikation.

Innan vi sätter igång med intervjun tänkte vi gå igenom lite information gällande forskningsetiska principer. Denna intervju kommer att spelas in i form av en ljudfil vid ett godkänt samtycke från dig. Ljudfilen kommer sedan att transkriberas och därefter kommer ljudfilen att raderas. Ditt namn, eventuella kontaktuppgifter eller information som kan kopplas till dig kommer att kodas om eller tas bort, således kommer arbetet avidentifieras.

Om det förekommer en fråga som du känner dig obekväm med eller inte vill svara på så behöver du inte svara på frågan.

- Godkänner du fortfarande din medverkan?
- Samtycker du till att vi spelar in ljudet under intervjun?
- Har du någon fråga innan vi sätter igång?
- Då kommer jag att sätta igång ljudinspelningen och så sätter vi igång med intervjun.

Tema 1: Bakgrund

- Hur länge har du arbetat inom den myndighet som du är verksam inom/på idag?

- Hur skulle du beskriva din yrkesroll?
    - Yrkestitel? Arbetsuppgifter?
- Förekommer registerslagningar i ditt arbete?
    - Skulle du kunna beskriva hur du använder registerslagningar i din yrkesutövning?
- Berätta vad du anser vara det främsta målet för din myndighet?
    - Berätta vilken betydelse du anser att rättssäkerheten har inom din verksamhet?

Tema 2: Dataintrång som brottstyp och dess förekomst

- Hur skulle du beskriva dataintrångsbrott så som du uppfattar brottstypen?
- Hur ställer du dig till tendensen att många som åtalas för dataintrång är myndighetsanställda som genomför en olovlig slagning på sin arbetsplats?
- Vilka uppfattningar och erfarenheter har du av olovliga registerslagningar inom den myndighet/verksamhet där du är verksam? (Du behöver inte berätta om du själv genomfört en olovlig registerslagning.)
- Finns det en intern medvetenhet om att olovliga registerslagningar sker inom myndigheten?
- Vad tror du förekomsten av otillåtna slagningar inom myndigheter kan bero på?

Tema 3: Effekter och hantering av olovliga registerslagningar

- Vilka konsekvenser tror du att otillåtna slagningar inom myndigheter kan medföra?
    - För samhällets syn på, och tillförlit för Sveriges myndigheter?
    - Vad tror du att detta skulle kunna få för konsekvenser för legitimiteten hos rättsväsendet?
- Hur tror du att olovliga slagningar inom myndigheter kan förebyggas?

Tema 4: Det svenska Natomedlemskapet

- Har Sveriges inträde i Nato diskuterats inom myndigheten?
- Hur skulle du beskriva myndighetens roll inom Sveriges totalförsvar?

- Är myndighetens roll som bidragande till civilförsvaret inom digitala miljöer någonting som diskuteras inom myndigheten?
- Hur ser du på cybersäkerhetens innebörd för det svenska totalförsvaret?
- Vilken innebörd tror du att Sveriges medlemskap i Nato kommer att få för det svenska totalförsvaret?
    - Sett till den myndighet du är verksam inom: Vad tror du medlemskapet kommer kunna bidra med för möjligheter för Sveriges totalförsvar?
    - Sett till den myndighet du är verksam inom: Tror du att nya krav kommer att ställas på Sverige kring frågor som berör säkerhets- och riskhantering?
- Tror du att konsekvenserna av förekomsten av olovliga registerslagningar inom myndigheter kan påverkas av att Sverige blivit medlem i Nato?
    - Tror du att olovliga registerslagningar kommer att betraktas annorlunda i relation till exempelvis säkerhetsfrågor?
- Tror du att straffbestämmelsen om olovlig registerslagning kan påverkas i framtiden av det svenska Nato-medlemskapet?
    - Tror du straffbestämmelsen kommer att vara densamma, förmildras eller skärpas i framtiden?
- Finns det något mer du vill berätta om som vi inte har frågat om?

Tema 5: Övrigt

- Får vi återkomma med uppföljande frågor?
- Vet du någon/har du någon kontakt som du tror skulle vara intresserad av att ställa upp i en intervju?
- Tack för ditt deltagande!

Bilaga 4. Information- och samtyckesblankett

Information till medverkan i undersökning gällande uppfattning kring olovlig registerslagning

Vi är två studenter vid namn Clara Antlöv och Julia Johansson Forssén som för tillfället läser den sjätte terminen på kandidatprogrammet i kriminologi vid Lunds universitet. Under denna vårtermin skriver vi vårt examensarbete inom kandidatkursen RÄSK02, som är kandidatkursen inom rättssociologi vid Rättssociologiska institutionen. Vi hör av oss till dig för att höra ifall du skulle vara intresserad av att vara med i vår undersökning. Din medverkan kommer endast att genomföras vid muntligt och skriftligt samtycke.

Examensarbetet undersöker dataintrångsbrott, med fokus på olovliga registerslagningar inom myndigheter. Vi vill undersöka hur brottstypen uppfattas av olika aktörer och vad den kan ha för relation till Sveriges inträde i Nato. Syftet med studien är att undersöka hur aktörer uppfattar den gällande lag- och straffbestämmelsen samt om de tror att bestämmelsen kan påverkas i framtiden i relation till Sveriges inträde i Nato och vad brottstypen kan ha för konsekvenser för upprätthållandet av myndigheters legitimitet.

Den valda metoden för vår datainsamling är kvalitativ intervju. Intervjun beräknas ta 45-60 minuter och kan ske på distans. Med samtycke kommer intervjun att spelas in och transkriberas. I examensarbetet kommer intervjuerna att avidentifieras. Uppgifterna kommer endast att användas till examensarbetets ändamål. Medverkan är helt frivillig och det är möjligt att dra tillbaka din medverkan när du vill, utan att ange skäl. När undersökningen är sammanställd kommer arbetet att presenteras som ett examensarbete vid Lunds universitet och sedan digitalt publiceras på LUP Student Papers, vilket är en publiceringstjänst som tillhör universitetet.

Om du väljer att avbryta din medverkan kommer vi att sluta behandla personuppgifter som vi tidigare samlat in i enlighet med samtycke. Om du har någon fundering går det bra att kontakta oss på:

Clara Antlöv *Julia Johansson Forssén*

Svarsblankett

- Jag har tagit del av informationen
- Jag samtycker till min medverkan i studien
- Jag är medveten om att mitt deltagande är frivilligt och att jag kan säga upp min medverkan när som helst utan att ange skäl
- Jag samtycker till att intervjun spelas in i form av en ljudfil som kommer att raderas efter att intervjun har transkriberats

Datum:_____

Underskrift:_____

Namnförtydligande:_____

Bilaga 5. Beskrivning av de intervjuade

Intervjuperson	**Myndighet**	**Yrkesroll**	**Tjänsterelaterade erfarenheter av registerslagningar**
Intervjuperson A	Polismyndigheten	PKC-operatör. Arbetat med det i 1-5 år.	Gör slagningar i samband med tjänst vid samtal som leder till polisanmälan.
Intervjuperson B	Tingsrätten	Rådman vid tingsrätten. Arbetat med rättsprocesser i 10-15 år.	Behandlat flera ärenden som involverar brottstypen, dels som förundersökningsledare och dels som domare.
Intervjuperson C	Polismyndigheten	Förundersökningsledare inom polisen. Arbetat som polis i 5-10 år.	Registerslagningar är vidare något som inkluderas mycket i intervjupersonens tjänst och arbetsuppgifter.
Intervjuperson D	Polismyndigheten	Ingripande polis. Jobbat som polis i 5-10 år.	Använder sig av registerslagningar i tjänsten, bland annat i samband med ingripande och misstänkta fordon.
Intervjuperson E	Kronofogde-myndigheten	Analytiker bland annat. Arbetat inom Kronofogden i 15-20 år.	Förekommer tillgång till olika typer av register, allt från indrivningsdatabas till skuldsaneringsdatabas exempelvis, som inkluderas som en del i yrkesutövningen.
Intervjuperson F	Polismyndigheten	Ingripande polis, arbetat med det i 1-5 år.	Förekommer registerslagningar inom tjänsten vid patrullering, exempelvis för att söka upp bilar och föraren.
Intervjuperson G	Polismyndigheten	Polis, arbetat i yttre tjänst, förundersökningsledare, gruppchef och utbildare. Arbetat i 15-20 år.	Förekommer slagningar på personer som involveras i ärenden, både i yttre tjänst men inom ledningscentralen.
Intervjuperson H	Polismyndigheten	Polis i yttre tjänst. Arbetar med ingripande verksamhet. Jobbat som polis i 1-5 år.	Använder sig av en stor mängd slagningar i samband med kontroller av personer och fordon.