



Författare: Wilma Ivarsson	Årskull: 231
Lärosäte: Försvarshögskolan	
Handledare: Eric Skoog	
Antal ord: 11996	
<p>Konsten att avskräcka på det digitala slagfältet En deskriptiv studie om Finlands cyberavskräckningsstrategi innan och efter Nato</p> <p><u>Abstract</u></p> <p><i>”Deterrence is concerned with influencing the choices that another party will make, and doing it by influencing his expectations of how we will behave”</i></p> <p style="text-align: right;"><i>- Thomas C. Schelling (1960)</i></p> <p>This quote captures the essence of deterrence. While modern warfare has become more complex and now includes elements beyond conventional methods, it has in the past decade reshaped the traditional understanding of who or what should be deterred. Previous research has shown that states uses deterrence as a method to counter and respond to cyberattacks. Although cyber deterrence is perceived as a complex and controversial concept, it has the potential to contribute to improved stability in cyberspace.</p> <p>Since joining Nato in 2023, Finland is expected to adapt to and integrate NATO’s strategic concept at the national level. This results in changing security environment and a shift in strategic direction. This study therefore aims to examine how Finland uses cyber deterrence in its cyber strategy before and after joining Nato, in order to increase the understanding of how small states use cyber deterrence in a changing security environment. The study's research question is: <i>How does Finland use cyber deterrence in its cyber strategy before and after NATO membership?</i></p> <p>To answer the research question, this study will use a theory-consuming descriptive approach, and the empirical material will be analysed through qualitative text analysis. The theoretical framework consists of cyber deterrence by denial and punishment, which are two of the most prominent strategies of cyber deterrence in previous research.</p> <p>The results of this study show that Finland’s cyber strategy prior to NATO membership has primarily relied on cyber deterrence through denial, with elements of cyber deterrence by</p>	

punishment. After Finland's NATO accession, the analysis shows that the country continues to predominantly use cyber deterrence through denial, but with a clearer presence of cyber deterrence through punishment than before.

This shows that the cyber deterrence capabilities of small states do not necessarily have to be merely defensive and preventive due to their often inferior position relative to great powers, but can also include more active elements for deterrence purposes. Given the current global security situation, continued research in this area is important to strengthen global cybersecurity.

Nyckelord: Cyberavskräkning, Finland, Förnekande, Besträffning, Cyberstrategi, Cybersäkerhet

Självständigt arbete, Påbyggnadskurs Krigsvetenskap (15 HP)

Innehållsförteckning

1. Inledning	4
2. Problemformulering	5
3. Tidigare forskning	6
4. Syfte och frågeställning	11
4.1 Avgränsningar	11
5. Teori	11
5.1 Cyberavskräckningsteori	11
5.2 Cyberavskräckning genom bestraffning	12
5.3 Cyberavskräckning genom förnekande	13
5.4 Teorikritik	14
6. Metod	15
6.1 Forskningsdesign	15
6.2. Operationalisering	16
6.2.1. Operationalisering av cyberavskräckning genom bestraffning	16
6.2.1. Operationalisering av cyberavskräckning genom förnekande	18
7. Material	21
7.1 Källkritik	21
7.2 Forskningsetik	22
8. Analys	22
8.1 Före Nato-inträdet	23
8.1.1. Cyberavskräckning genom bestraffning	23
8.1.2. Cyberavskräckning genom förnekande	25
8.2. Efter Nato-inträdet	27
8.2.1. Cyberavskräckning genom bestraffning	27
8.2.2. Cyberavskräckning genom förnekande	30
9. Slutsatser	32
10. Diskussion	34
10.1. Relevans för yrkesutövningen	36
10.2. Vidare forskning	37
11. Källförteckning	37

1. Inledning

” Deterrence is concerned with influencing the choices that another party will make, and doing it by influencing his expectations of how we will behave”

- Thomas C. Schelling
(1960)

Detta citat fångar kärnan i avskräckning och visar att det inte enbart handlar om att påverka en motståndares val, utan även om att forma dess förväntningar på hur en avskräckande stat kommer att agera. Modern krigföring har i sin tur blivit alltmer komplex och omfattar inslag bortom konventionella metoder, vilket har förändrat den traditionella synen på vem eller vad som bör avskräckas.

Historiskt förknippas avskräckning med kärnvapenkappupprustningen mellan USA och Sovjetunionen och kalla kriget, där strategin utvecklades som ett sätt att skydda sig utan att använda direkt militärt våld (Nye 2017, s.45). Avskräckning innebär att få någon att avstå från att göra något genom att övertyga dem om att kostnaderna kommer att överstiga den förväntade nyttan (Nye 2017, s. 45). De mest grundläggande antagandena för att avskräckning ska uppfattas som trovärdig är att användaren besitter kapacitet, kommunikationsförmåga och engagemang (Angstrom & Widen 2014, s. 47–48). I takt med att slagfältet har förskjutits från den traditionella till den digitala arenan uppstår frågan om hur stater tillämpar avskräckning på ett trovärdigt och effektivt sätt även i cyberdomänen.

Cyberhoten i Europa ökar och Finlands cybersäkerhetsår 2025 präglades av en negativ utveckling där hotbilden förblev förhöjd och antalet incidenter kvarstod på en hög nivå (Traficom 2025). Ryssland utgör det främsta hotet inom cyberhändelser enligt finska säkerhets- och underrättelsetjänsten, där cyberoperationer mot Finland genomförda av rysk underrättelsetjänst har ökat (SUPO 2025). Finlands chef för skyddspolisens kontraspionageavdelning, Teemu Liikkanen, har uttalat sig om att när kriget i Ukraina avtar eller slutar kommer Ryssland att kunna omdirigera cyberkapacitet som för närvarande är knuten till Ukraina även mot Finland (Traficom 2025). Det går därför inte att utesluta att

cyberhoten kommer att intensifieras ytterligare, vilket ställer högre krav på landets cybersäkerhet. Tidigare forskning har visat att stater nyttjar avskräckning som metod för att motverka och bemöta cyberangrepp, såväl småstater som stormakter. Trots att cyberavskräckning uppfattas som ett komplext och omtvistat koncept har det potential att bidra till förbättrad stabilitet i cyberrymden (Lawson 2017, s. 436).

2. Problemformulering

Hybridhot och hybridkrigföring blir alltmer framträdande och används återkommande inom nyhetsmedier som ett samlingsnamn för såsom sabotage, cyberhot och propaganda. Cyber är ett brett begrepp och inkluderar en mängd olika digitala, trådlösa och datorrelaterade aktiviteter (Nye 2017, s. 46). Inom hybridkrigföring kan en motståndare använda såväl cyberattacker som mer omfattande cyberoperationer i syfte att uppnå specifika mål. Ryssland har framgångsrikt använt cyberoperationer i tidigare konflikter och utgör ett av de största hoten mot närliggande länder (Lanoszka 2016, s. 187). Cyberoperationer har potential att destabilisera samhällen och försvaga en motståndare, vilket gör dem till ett kraftfullt vapen i modern krigföring (Aras & Süvari 2015, s. 437–438).

Traditionell avskräckningsteori vilar framför allt på två inriktningar: ett trovärdigt hot om *bestraffning* och *förnekande* av vinster från en handling (Nye 2017, s. 54). Avskräckning genom bestraffning innebär att skapa eller förstärka en motståndares rädsla för konsekvenserna av en handling (Nye 2017, s. 55). Konceptet var framträdande under kärnvapenkapprustningen mellan USA och Sovjetunionen, där hot om omfattande vedergällning användes för att avskräcka motparten från att initiera ett angrepp (Nye 2017, s.55). Avskräckning genom förnekande innebär i kontrast till bestraffning att göra ett mål så svårt att attackera att det inte är värt för motståndaren att göra det (Lawson 2017, s.432).

Avskräckningsteori har kommit att användas inom olika domäner. Robert Pape (2014) föreslår att inkludera både bestraffning och förnekande inom luftmaktsteorin där logiken kring avskräckning finns kvar men är anpassad utifrån luftdomänen (Angstrom & Widen 2014, s. 153). Även inom sjöoperationer utgör förnekande av sjökontroll en grundläggande strategi inom sjömaktsteori (Angstrom & Widen 2014, s. 135). Nato erkände 2016 cyberrymden som den femte domänen, efter mark, luft, sjö och rymd, vilket innebär att den betraktas som ett operationsområde (Nato 2024). Det finns ännu ingen entydig cyberavskräckningsteori, men flera forskare, däribland Joseph Nye (2017) och N.J. Ryan (2018), har bidragit till

utvecklingen av konceptet. Cyberkrigföring finns på samtliga krigföringsnivåer, taktiskt, operativt och strategiskt, men skiljer sig däremot från de övriga domänerna, vilket gör att det uppstår meningsskiljaktigheter inom forskningen om cyberavskräckning är uppnåbart. Det finns tre tydliga argument inom forskningen som förklarar varför cyberavskräckning kan vara svårt att uppnå:

1. Utmaningen med att identifiera och tillskriva en motståndare (Lawson 2017, s. 433)
2. Avsaknaden av traditionell suveränitet innebär att en aktör kan påverka mål globalt utan existerande fysiska gränser (Borghard & Lonergan 2023, s. 536).
3. Ständig uppkoppling och kontakt inom domänen (Borghard & Lonergan 2023, s. 536).

Trots oenigheten kring cyberavskräckningens effektivitet i cyberdomänen och avsaknaden av en enhetlig cyberavskräckningsteori visar forskningen att stater ändå nyttjar avskräckning i sina cyberstrategier, med varierande omfattning och tillvägagångssätt. Framträdande exempel är studier som genomförts på stormakter som USA, där användningen av cyberavskräckning har identifierats (Borghard & Lonergan 2023, s. 534). Småstater är mindre framträdande inom forskningen, men Li (2024) är en av forskarna som studerat småstaters användning av cyberavskräckning genom förnekande och bestraffning inom ramen för en flerfallstudie av Estland och Singapore.

Finland är ett av länderna som inom tidigare forskning ingår i kategorin småstater (Sulg & Crandall 2020, s. 112; Rickli 2008, s. 320). Förutom att Finland utgör ett särskilt intressant fall med anledning av sitt geografiska läge i relation till Ryssland och nationella investeringar i cybersäkerhet, har landet också varit försvarsalliansfritt under större delen av cyberkrigföringens framväxt. Sedan Nato-inträdet 2023 förväntas Finland anpassa och integrera Natos strategiska koncept på nationell nivå (Nato 2022 a). Vilket resulterar i en förändrad säkerhetsmiljö och strategisk inriktning för landet. Denna studie ämnar därav att undersöka hur Finland använder cyberavskräckning i sin cyberstrategi innan och efter Nato-inträdet.

3. Tidigare forskning

Följande avsnitt syftar till att redogöra för forskningsläget kring cyber som en del av hybridkrigföring samt den komplexitet som präglar cyberavskräckning. Inledningsvis beskrivs Rysslands användning av hybridkrigföring och genomförande av cyberoperationer inom tidigare konflikter för att belysa en av de primära hotaktörerna mot Finland. Därefter redogörs

det för den historiska relevansen för avskräckningsteorin och de olika synsätten på tillämpningen av konceptet inom cyberdomänen. Slutligen sammanfattas tidigare forskning för att identifiera den forskningsfråga som studien avser att besvara.

Rysslands hybridkrigföring

I artikeln *Russian hybrid warfare and extended deterrence in eastern Europe* beskriver Lanoszka (2016) logiken bakom Rysslands användning av hybridkrigföring och varför tidigare sovjetrepubliker och angränsande länder, som de baltiska staterna, är särskilt sårbara. Trots att den är skriven innan Rysslands invasion av Ukraina 2022 lyfter den relevanta infallsvinklar kring hybridkrigföring. Lanoszka inleder med att definiera hybridkrigföring enligt Murray Williamson & Peter R. Mansoor (2012). ”Hybridkrigföring är en konflikt som involverar en kombination av konventionella militära styrkor och irreguljära (guerilla, insurgeneter och terrorister), vilket kan inkludera både statliga och icke-statliga aktörer, som syftar till att uppnå ett gemensamt politiskt mål” (Lanoszka 2016, s. 178). Som en del av irreguljär krigföring nämner Lanoszka kriminell oordning där krigförande agenter använder sig av hit-and-run-attacker, cyberattacker, sabotage eller kidnappning (Lanoszka 2016, s.179). Vidare i artikeln skriver Lanoszka att angränsade länder samt tidigare sovjetrepubliker är sårbara för hybridkrigföring om Ryssland har ett intresse av att expandera eller återupprätta sin regionala hegemoni (Lanoszka 2016, s. 187). Han ser detta som fullt möjligt och lyfter frågan: hur kan USA och Nato bidra med skydd och avskräckning mot Ryssland för att förhindra att de använder hybrida tillvägagångssätt mot dessa länder (Lanoszka 2016, s. 176). De baltiska länderna har länge ingått i Natos gemensamma skydd under artikel 5, men är fortfarande sårbara om västliga allierade saknar viljan att försvara dem (Lanoszka 2016, s. 192). Samtidigt försöker rysk hybridkrigföring undergräva detta genom att utnyttja situationer som gör det direkt svårare att koppla Ryssland till aggressiva handlingar (Lanoszka 2016, s. 192).

Vidare undersöker Aras & Süvari (2025) i sin artikel *Unveiling Russia's secret weapon: cyber-electronic operations in hybrid warfare*, hur Ryssland har genomfört cyberelektroniska operationer inom hybridkrigföring genom en analys av interventionerna i Georgien 2008, Ukraina 2014 och Syrien 2015. Författarna förklarar att cyberattacker som är riktade mot motståndarens sårbara punkter inom informationskrigföring är en central del av hybridkrigföringskonceptet (Aras & Süvari 2025, s. 435). Dessa operationer och attacker riktar sig mot fysiska och virtuella strukturer, programvara, hårdvara och infrastruktursystem i cybermiljön (Aras & Süvari 2025, s. 435). Målet är att komma över känslig information som

tillhör motståndaren, manipulera information och förhindra användare från att få tillgång till information på online plattformar (Aras & Süvari 2025, s. 437). Antalet svagt skyddade nätverk är omfattande, vilket gör att det inte är svårt för högteknologiska aktörer att upptäcka och skada dem (Aras & Süvari 2025, s. 437–438). Dessutom är risken för angriparen låg, vilket resulterat i att cyberattacker används allt oftare på det hybrida slagfältet och att aktörer konstant försöker förbättra sina cyberförmågor ytterligare (Aras & Süvari 2025, s. 438). Undersökningen visade att Ryssland har genomfört cyberelektroniska attacker koordinerade med andra komponenter av hybridkrigföring i de tidigare konflikterna, Georgien, Ukraina och Syrien, vilket har resulterat i framgångsrika operationer (Aras & Süvari 2025, s. 446–447). Sedan Georgienkriget har Ryssland investerat kraftigt i att förbättra sina cyberelektroniska förmågor, vilket har lett till att de har blivit en global cybermakt (Aras och Süvari 2025, s. 447). Fortsatt beskriver Aras och Süvari (2025, s. 447) att cyberoperationer har potential att destabilisera samhällen och försvaga en motståndare, vilket gör dem till ett kraftfullt vapen i modern krigföring. Det är därför av betydelse att vidta förberedande åtgärder som internationellt samarbete och kollektivt försvar för att motverka cyberattacker och cyberoperationer (Aras & Süvari 2025, s. 447).

Cyberavskräckning

Lawson (2017) beskriver i sin artikel *Deterrence in Cyberspace: a Silver bullet or a sacred cow?* de utmaningar som är förknippade med begreppet cyberavskräckning. Författaren nämner cyberavskräckning genom bestraffning och förnekande som de mer framträdande strategierna med anledning av deras historiska betydelse utanför cyberdomänen (Lawson 2016, s.432). Lawson hävdar att både cyberavskräckning genom förnekande och bestraffning har sina utmaningar, men att begreppen trots allt är validerade och avgörande för att leverera strategisk stabilitet (Lawson 2017, s. 432). Författaren presenterar två nyckelfaktorer för att cyberavskräckning genom bestraffning ska uppfattas som trovärdig: förmågan att bestraffa och viljan att använda den förmågan, eller åtminstone övertyga motståndaren om att den sannolikt kommer att användas (Lawson 2017, s. 432). För cyberavskräckning genom förnekande handlar det i stället om att göra ett mål så svårt att attackera att det inte är värt för motståndaren att göra det. Lawson (2017, s. 433) betonar att den största problematiken med cyberavskräckning och konflikter i cyberrymden generellt är utmaningarna med att identifiera och tillskriva en angripare. Utan förståelse för detta är det svårt att utveckla en fungerande cyberavskräckningsstrategi (Lawson 2017, s. 433). Författaren konstaterar att cyberavskräckning är ett komplext och omtvistat koncept, men har potential att bidra till

förbättrad stabilitet i cyberrymden (Lawson 2017, s. 436). För att det ska fungera menar han att den bestraffande och förnekande cyberavskräckningsstrategin behöver kombineras för att förhindra attacker, men anpassas efter de olika hotaktörerna i cyberrymden för att få full effekt (Lawson 2017, s. 436).

Enligt Borghard och Lonergan (2023, s.534) är det många forskare och yrkesutövare som inte är övertygade om att cyberavskräckning är uppnåbart. I artikeln *deterrence by denial in cyberspace* diskuterar författarna implementeringen av cyberavskräckning genom bestraffning och förnekande likt Lawson (2017), men förespråkar den sistnämnda som den mer framgångsrika för cyberrymden (Borghard & Lonergan 2023, s. 534). Under 2010-talet formades två huvudsakliga synsätt på cyberavskräckning: de starka avskräckningspessimisterna och de försiktiga avskräckningsoptimisterna (Borghard & Lonergan 2023, s.536). Avskräckningspessimister, såsom Richard Harknett (2017) och Michael Fischerkeller (2017), hävdar att cyberrymden har särskilda egenskaper, saknar traditionell suveränitet och utgör en miljö präglad av ständig kontakt (Borghard & Lonergan 2023, s. 536). Detta skulle därför innebära att skyddet av cyberrymden och främjandet av nationella intressen inte kan baseras på avskräckning som den centrala strategin (Borghard & Lonergan 2023, s. 536). Omvänt försökte de försiktigt optimistiska, som Jacquelyn Schneider (2023) och Joseph Nye (2017), förfina och nyansera den tidigare litteraturen om cyberavskräckning samt bevara konceptet där det var möjligt. Borghard och Lonergan (2023, s.537) vill bygga vidare på de ”försiktiga avskräckningsoptimisterna” och menar att traditionell avskräckning genom bestraffning, som har sin utgångspunkt i kärnvapenavskräckning, är utmanande att applicera i cyberrymden. Författarna argumenterar för att avskräckning genom förnekande är mer lämplig och hur en sådan implementering skulle användas i den amerikanska cyberstrategin, där bestraffande avskräckning är mer integrerad (Borghard & Lonergan 2023, s. 534).

Lawson (2017) samt Borghard och Lonergan (2023) utgår ifrån amerikanska cyberstrategier och policydokument i sina studier. Detta speglar forskningen inom cyberavskräckning då en majoritet av studierna har baserats på stormakter. Li (2024) skriver i sin artikel *Asymmetry in the digital age: Cyber deterrence strategies for small states* om utmaningarna för mindre stater att använda cyberavskräckning och avskräcka cyberattacker samt cyberhot som kan hota den nationella säkerheten. Författaren menar att småstater har begränsade nationella resurser och cyberkapaciteter, vilket begränsar deras förmåga att effektivt avskräcka stormakter (Li 2024, s.71). Till skillnad från konventionella militära operationer ligger

cyberattacker ofta under gränsen för väpnad konflikt, vilket gör det möjligt för en motståndare att orsaka skada utan att framkalla omfattande vedergällningar (Li 2024, s.71). Flertalet studier har undersökt hur cyberavskräckning används mellan stormakter som USA, Ryssland och Kina, men inte hur småstater kan avskräcka stormakter i cyberrymden (Li 2024, s.71). Författaren konstaterar att Estland använder sig av både bestraffande avskräckning genom bland annat offentlig attribuering och förnekande avskräckning genom samarbete mellan myndigheter och organisationer i hela samhället (Li 2024, s. 80–81). Samtidigt använder småstater cyberavskräckning om än med medel som skiljer sig från de som används av stormakter (Li 2024, s. 81). Författaren identifierar att det finns två faktorer som formar en småstats inställning till cyberavskräckning; första faktorn är begränsade resurser och geopolitiska sårbarheter som minskar effekten av cyberavskräckning genom bestraffning (Li 2024, s. 85). Andra faktorn är om småstater har asymmetriska fördelar som gör avskräckning genom förnekelse till en mer kostnadseffektiv och genomförbar strategi (Li 2024, s. 85).

Sammanfattning:

Lanoszka (2016) och Aras & Süvari (2025) redogör tillsammans för Rysslands användning av hybridkrigföring och landets benägenhet att använda cyberattacker som aggressiv handling mot närliggande länder. Om stater som riskerar att drabbas inte kan skydda och försvara sig mot cyberangrepp, kan konsekvenserna bli omfattande. Därför betonar både Lanoszka (2016, s. 191) och Aras & Süvari (2025, s. 447) samordnat försvar och internationella samarbeten. Samtidigt påpekar Lanoszka (2016, s. 176) att det finns en rädsla hos de baltiska länderna för att ett Nato-medlemskap inte garanterar skydd mot cyberhot och cyberoperationer. Då Finland befinner sig i ett liknande säkerhetsläge efter sitt Nato-inträde är detta en relevant aspekt att lyfta inom tidigare forskning.

De mest framträdande strategierna för cyberavskräckning inom tidigare forskning är förnekande och bestraffning (Lawson 2016, s.432; Borghard & Lonergan 2023, s. 534). Samtidigt råder det en oenighet kring cyberavskräcknings faktiska potential att användas i praktiken, vilket diskuteras av både Lawson (2016, s. 433) och Borghard & Lonergan (2023, s. 534). Detta är ett centralt problemområde inom forskningen, men trots oenigheter visar författarna Li (2024, s. 80–81) och Lawson (2016, s.534) att såväl småstater som stormakter nyttjar cyberavskräckning i sina cyberstrategier med olika medel och metoder.

Tidigare forskning har i begränsad utsträckning analyserat hur småstater använder cyberavskräckning i sina nationella cyberstrategier, särskilt i kontexten av en förändrad

säkerhetsmiljö. Finland utgör ett särskilt intressant fall i detta sammanhang då landet, tillsammans med Sverige, beslutade sig för att ansöka om medlemskap i Nato i en tid då cyber har fått ökad strategisk betydelse för nationell säkerhet. Landets geografiska läge mot Ryssland i kombination med stora nationella satsningar inom cybersäkerhet skapar förutsättningar för cyberavskräckning, som förväntas användas i dess cyberstrategi. Finlands Nato-inträde 2023 innebar en tydlig omställning i landets säkerhetsmiljö, vilket möjliggör en studie kring hur cyberavskräckning används innan och efter att landet blev medlem.

4. Syfte och frågeställning

Denna studie syftar till att bidra till den övergripande forskningen om cyberavskräckning genom en analys av Finlands cyberstrategi innan och efter Nato-inträdet. Mer specifikt syftar studien till att redogöra för hur cyberavskräckning används i den finska cyberstrategin. Detta för att öka förståelsen för hur småstaters användning av cyberavskräckning påverkas i en förändrad säkerhetsmiljö.

Följande frågeställning kommer besvaras:

Hur använder Finland cyberavskräckning i sin cyberstrategi innan och efter Nato-inträdet?

4.1 Avgränsningar

Studien avgränsas till Finlands cyberstrategi innan och efter Nato-inträdet, vilket gäller tidsperioden innan respektive efter 2023. För att undvika ett alltför omfattande empiriskt material publicerat innan 2023 begränsas studien till 2013–2023, då detta var en tidsperiod då cyberhoten intensifierades och Finland inledde mer utbredda satsningar inom cybersäkerhet. Tidsperioden efter 2023 begränsas inte utan anses motsvara empiriskt tidsperioden innan Nato-inträdet.

5. Teori

5.1 Cyberavskräckningsteori

Det teoretiska ramverket kommer att utgå från cyberavskräckning genom *bestraffning* och *förnekande*, vilka utgör grunden för cyberavskräckning inom tidigare forskning. Båda har sin utgångspunkt i traditionell avskräckningsteori men har senare även använts inom

utvecklingen av cyberavskräckningsteori (Lawson 2016, s.432). Eftersom det saknas en entydig strategi för hur stater mest effektivt avskräcker hot och angrepp i cyberdomänen, baseras det teoretiska ramverket på bidrag från flera framträdande författare inom cyberavskräckning. Samtliga författare inkluderar cyberavskräckning genom bestraffning och förnekande i sina respektive teoretiska ansatser, vilket gör dem till vedertagna teoretiska begrepp att nyttja inom studien.

5.2 Cyberavskräckning genom bestraffning

Avskräckning genom bestraffning antyder för en angripare att det kommer att bli betydande vedergällningar i form av *offensiva åtgärder* i händelse av en attack (Iasiello 2014, s. 55). Inom cyberrymden kan det ta formen av digitala vedergällningar mot en aktör som genomfört en cyberattack eller en förebyggande cyberattack mot en förväntad motståndare (Iasiello 2014, s.55). Utanför cyberrymden kan offensiva åtgärder innebära kinetiska attacker mot fysiska mål eller genom diplomatiska medel, som ekonomiska sanktioner (Iasiello 2024, s. 55). Det ska finnas en vilja och förmåga hos den avskräckande staten att utföra offensiva åtgärder, vilket måste upprätthållas under en lång tidsperiod för att inte förlora avskräckningens trovärdighet (Tor 2017, s. 107–108). Ett av de mer kontroversiella sätten att bemöta ett cyberangrepp är att ”hacka tillbaka”; dock finns ett antal risker förknippade med detta som eskalerande attacker och felaktig tillskrivning av aktör (Ryan 2018, s. 333).

Hotet om eller användningen av bestraffande åtgärder måste stå i *proportion* till den inledande attacken (Iasiello 2014, s.59). En stat måste inte bara slå tillbaka mot angriparen utan också göra det på ett sådant sätt att dess poäng framgår, utan att för den delen väcka starka internationella reaktioner (Iasiello 2014, s. 59). Detta kan vara svårt att uppnå i cyberrymden av flertalet anledningar men all typ av kinetisk eller icke kinetisk respons, förväntade konsekvenser och bedömning av eventuella förluster, samt de potentiella politiska konsekvenserna bör beaktas i beslutsprocessen (Iasiello 2014, s. 60).

För att cyberavskräckning genom bestraffning ska uppfattas som trovärdig finns ett grundläggande behov av att attribuera en motståndare, vilket det finns utmaningar med i cyberrymden (Nye 2017, s. 55). Att inte kunna tillskriva en motståndare till en attack eller ett hot, försämrar både trovärdigheten och sänder en otydlig avskräckningssignal då såväl initierade attacker som repressalier inte kan riktas mot en oidentifierad aktör (Tor 2017, s. 100). För att kunna tillskriva en cyberincident till en aktör krävs stor teknisk expertis, stöd av organisatorisk samordning och en politisk vilja att hålla en angripare ansvarig (Ryan 2018, s.

333). Om den avskräckande staten har ett starkt samarbetsavtal mellan nationella brottsbekämpande myndigheter är det enkelt att se varför hot om bestraffning kan vara fördelaktigt (Ryan 2018, s.333). Då en aktör isåfall behöver vara högkvalificerad och mycket teknisk kompetent för att undgå upptäckt (Ryan 2018, s. 333)

Kommunikation är en av de mest fundamentala faktorerna för att såväl bestraffande som förnekande avskräckning ska uppfattas som trovärdigt av en motståndare (Iasiello 2014, s. 56). För avskräckning genom bestraffning handlar det om att vara tydlig med vad som händer om man går över gränsen och även vara beredd att agera i linje med det som har uttalats (Iasiello 2014, s. 56). Inom cyberdomänen blir detta desto viktigare eftersom domänen är genomsyrad av tvetydighet (Iasiello 2014, s. 56).

Signalering är fundamentalt för att avskräckningen ska uppfattas som trovärdig och handlar om att ha såväl förmågan som viljan att demonstrera sina intentioner med attacker eller motåtgärder (Iasiello 2014, s.57). Utan möjlighet att signalera blir cyberavskräckning genom bestraffning ineffektiv och riskerar att missförstås eller misstolkas, vilket ökar risken för eskalering och konflikt (Iasiello 2014, s. 57). Signalering kan ske öppet, i hemlighet eller genom diplomatiska, ekonomiska eller militära tillvägagångssätt som militärövningar (Iasiello 2024, s. 57).

5.3 Cyberavskräckning genom förnekande

Avskräckning genom förnekande innebär att en stat försöker övertyga en potentiell angripare om att ett angrepp inte kommer att lyckas och att de därmed förnekas de fördelar de hoppas uppnå (Iasiello 2014, s. 55). Detta har under en längre tid varit en gynnsam strategi inom cyberavskräckning, särskilt med tanke på att avskräckning genom bestraffning anses vara mer utmanande (Ryan 2018, s. 334). En liknelse som kan förklara fenomenet är att se staten som en fästning som byggs med högre och tjockare murar samt djupare vallgravar för att skydda de mest värdefulla kronjuvelerna och hålla människor säkra (Ryan 2018, s. 334). Detta ska göra att motståndaren uppfattar fästningen som för välförsvard för att initiera en attack (Ryan 2018, s. 334). Fördelen med denna strategi är att den är mindre konflikt driven och baseras på *defensiva åtgärder*, vilket både inkluderar att förhindra motståndaren från att agera och en lösning vid ett angrepp (Ryan 2018, s. 334). I cyberrymden antar avskräckning genom förnekande en mer defensiv roll genom att avskräcka eller störa attacker via robusta system eller, proaktiva och kostsamma förberedelser (Iasiello 2014, s. 56). Det kräver ett stort, fokuserat åtagande från en regering för att säkra de system och nätverk under dess kontroll, i

kombination med fullt samarbete från ägarna av infrastrukturen (Iasiello 2014, s.56). Defensiva åtgärder stärks också genom att försöka lura en angripare (Ryan 2018, s.334). Om en aktör aktivt undviker nyligen försvarade nätverk för att den psykologiskt tror att de är för skyddade eller ogenomträngliga, kan den potentiellt avskräckas genom förnekelse (Ryan 2018, s. 334).

Som nämnts spelar *kommunikation* även en viktig roll för avskräckning genom förnekande eftersom effektiv kommunikation mellan stater inger trovärdighet (Iasiello 2024, s.56). För förnekande avskräckning handlar detta om att förmedla en stats förmåga till cybersäkerhet och informationssäkerhet (Iasiello 2024, s. 57). Detta uppnås genom att göra ett mål tillräckligt svårt och kostsamt för en motståndare att angripa, vilket sker genom att utveckla en mer robust och säker cyberinfrastruktur med hjälp av kontinuerlig teknisk innovation och moderna skyddsmetoder (Tor 2017, s.108). Det förväntade resultatet är att en angripare avstår från att genomföra ett angrepp eftersom det skulle kräva för omfattande resurser (Tor 2017, s. 108).

En förutsättning för trovärdig cyberavskräckning genom förnekande är att motståndaren uppfattar en *överlägsenhet i cyberrymden* (Tor 2017, s. 108). Detta gäller särskilt inom underrättelseverksamhet och offensiva förmågor, i syfte att kunna övertyga en motståndare om att det inte är realistiskt att vinna på grund av ett avgörande kvalitativt övertag (Tor 2017, s.108)

5.4 Teorikritik

Med anledning av att det inte finns en entydig cyberavskräckningsteori samt att större delen av tidigare forskning diskuterar cyberavskräckning genom bestraffning och förnekande, ansågs det teoretiska ramverket vara lämpligt för studien. Författare som N.J. Ryan (2018, s.332) har förutom cyberavskräckning genom bestraffning och förnekande sammanfattat andra sätt för att uppnå cyberavskräckningsförmåga: association, entanglement, samt normer och tabun. Dessa nämner även författaren Joseph Nye (2017, s. 58–62), vilket gör dem tillräckligt etablerade för att användas i studien. Däremot ansågs enbart avskräckning genom association och entanglement vara potentiella val, med anledning av att normer och tabun kan vara outtalade i strategierna och därav svåra att identifiera genom den valda forskningsdesignen. Tidigare forskning har övervägande diskuterat cyberavskräckning genom bestraffning och förnekande, med anledning av dess historiska betydelse inom andra domäner, vilket gör att den har en stark teoretisk förankring inom området. Därför behandlas inte

samtliga identifierade strategier för cyberavskräckning inom studien, vilket möjliggör en mer fördjupad analys av de två utvalda strategierna. Då teorin består av en sammanfattning av olika författare blir betydelsen av begreppsvaliditet högre, vilket upprätthålls genom att i operationaliseringen tydliggöra vilket empiriskt material som begreppen och tillhörande indikatorer utgår ifrån.

6. Metod

6.1 Forskningsdesign

Forskningsdesignen för studien baseras på både syfte och frågeställning, vilket gör en beskrivande enfallsstudie med teorikonsumerande ansats lämplig. Detta för att kunna kartlägga och identifiera hur avskräckning används i Finlands cyberstrategi, med fokus på att öka förståelsen för småstaters utformning av cyberstrategier, snarare än att pröva teorin eller förklara ett kausalt samband (Esaiasson, Gilljam, Oscarsson, Sundell, Towns & Wängnerud 2024, s. 28–29). Även om studien utgår ifrån en analys av innan och efter Finland blev medlem i Nato, syftar den inte till att påvisa att Nato-medlemskapet utgör en enskild kausal mekanism bakom utfallet. Utan enbart att redogöra för hur något ser ut innan och efter en tydlig brytpunkt. Teorin kommer att nyttjas som ett analysverktyg för att kategorisera den insamlade informationen där Finlands cyberstrategi kommer att vara i centrum, vilket innebär att den mest optimala teorin väljs ut utifrån val av fall (Esaiasson m.fl. 2024, s. 38). Den utvalda forskningsdesignen begränsar studiens generaliserbarhet eftersom den baseras på ett mindre urval av fall, men kan bidra till att belysa olika aspekter av ämnet cyberavskräckning och ge en bättre förståelse för fenomenet, vilket även kan vara till stöd för andra forskare inom forskningsområdet (Esaiasson m.fl. 2024, s. 29–31). Studien har en enfallsdesign med flera analysenheter då det är Finlands cyberstrategi under två tidsperioder som ska analyseras och omfattar olika strategidokument, publikationer och uttalanden (Johannessen, Tufte & Christoffersen 2020, s. 196).

För att analysera den insamlade empirin nyttjas kvalitativ textanalys, vilket möjliggör en strukturerad genomgång av materialet med stöd av teorin (Esaiasson 2024, s.309). Denna metod lämpar sig för studien då den syftar till att bringa reda i texter och genom systematisk läsning beröra aspekter som inte öppet uttrycks utan kan döljas i texterna (Esaiasson 2024, s. 309–310). Cyberavskräckning är inte alltid enkel att identifiera i praktiken, vilket gör kvalitativ analys användbar för att upptäcka subtila och dolda framställningar av konceptet.

För att uppnå god begreppsvaliditet är operationaliseringen av cyberavskräckning central, eftersom den avgör i vilken utsträckning som analysen faktiskt fångar det fenomen som ämnas undersökas (Esaiasson m.fl. 2024, s. 126). Det teoretiska ramverket som nyttjas kommer att bestå av tydliga definitioner av avskräckning genom bestraffning och förnekande, för att uppnå en bredare beskrivning av begreppen och därav uppnå högre begreppsvaliditet. Resultatets validitet är även den av betydelse där reliabiliteten behöver beaktas. För att minimera risken för godtyckliga tolkningar kommer analysen att underbyggas med citat och referat från det empiriska källmaterialet (Esaiasson 2024, s. 130–131). Detta bidrar sin tur till att stärka resultatets validitet genom att beskrivningarna hålls nära det empiriska källmaterialet.

6.2. Operationalisering

Cyberavskräckning genom bestraffning och förnekande operationaliseras till begrepp baserat på det teoretiska ramverket. Inom respektive begrepp kommer indikatorer på vad som eftersöks i det empiriska materialet inom analysen att definieras.

6.2.1. Operationalisering av cyberavskräckning genom bestraffning

Utifrån beskrivningarna operationaliseras avskräckning genom bestraffning till *offensiva åtgärder, proportionalitet, attribuering, kommunikation och signalering*. Eftersom proportion är kopplad till uttalade hot och användningen av offensiva åtgärder, används de tillsammans inom analysen. Kommunikation och signalering kan uppfattas som överlappande, men det framgår en tydlig distinktion i att kommunikation rör vad som sägs eller uttrycks, medan signalering gäller beteende och handlingar.

Offensiva åtgärder och proportionalitet

Avskräckning genom bestraffning antyder för en angripare att det kommer att bli betydande vedergällningar i form av *offensiva åtgärder* i händelse av en attack (Iasiello 2014, s. 55). Inom cyberrymden kan det ta formen av digitala vedergällningar mot en aktör som genomfört en cyberattack eller en förebyggande cyberattack mot en förväntad motståndare (Iasiello 2014, s.55). Utanför cyberrymden kan offensiva åtgärder innebära kinetiska attacker mot fysiska mål eller genom diplomatiska medel, som ekonomiska sanktioner (Iasiello 2024, s. 55).

Hotet om eller användningen av bestraffande åtgärder måste stå i *proportion* till den inledande attacken (Iasiello 2014, s.59). En stat måste inte bara slå tillbaka mot angriparen utan också göra det på ett sådant sätt att dess poäng framgår, utan att för den delen väcka starka internationella reaktioner (Iasiello 2014, s. 59).

Hur beskriver Finland användningen av offensiva åtgärder som svar på cyberincidenter?

Hur står offensiva åtgärder i proportion till en cyberincident?

Attribuering:

För att avskräckning genom bestraffning ska uppfattas som trovärdig finns ett stort grundläggande behov av att *attribuera* en motståndare, vilket det finns utmaningar med i cyberrymden (Nye 2017, s. 55). Att inte kunna tillskriva en motståndare försvårar både hotets trovärdighet och sänder en otydlig avskräckningssignal, då såväl initierade attacker som repressalier inte kan riktas mot en oidentifierad aktör (Tor 2017, s. 100). För att kunna tillskriva en cyberincident till en aktör krävs stor teknisk expertis, stöd av organisatorisk samordning och en politisk vilja att hålla en angripare ansvarig (Ryan 2018, s. 333).

Hur arbetar Finland med att identifiera motståndare i cyberdomänen?

Vad utgör det primära hotet i Finlands cyberstrategier?

Kommunikation

För avskräckning genom bestraffning handlar kommunikation om att vara tydlig med vad som händer om man går över gränsen och även vara beredd att agera i linje med det som har uttalats (Iasiello 2014, s. 56). Annars riskerar stater att förlora sin internationella trovärdighet om de misslyckas med att förmedla detta (Iasiello 2014, s. 56). Inom cyberdomänen blir detta desto viktigare eftersom domänen är genomsyrad av tvetydighet (Iasiello 2014, s. 56).

Hur har Finland kommunicerat gränssättning gentemot en motståndare inom cyberdomänen?

Signalering

Signalering är fundamentalt för att avskräckningen ska uppfattas som trovärdig och handlar om att ha såväl förmågan som viljan att demonstrera sina intentioner med attacker eller motåtgärder (Iasiello 2014, s.57). Utan möjlighet att signalera blir cyberavskräckning genom bestraffning ineffektiv och riskerar att missförstås eller misstolkas, vilket ökar risken för eskalering och konflikt (Iasiello 2014, s. 57). Signalering kan ske öppet, i hemlighet eller

genom diplomatiska, ekonomiska eller militära tillvägagångssätt som militärövningar (Iasiello 2024, s. 57).

Hur har Finland signalerat vilja och förmåga att använda bestraffning som svar på cyberincidenter?

6.2.1. Operationalisering av cyberavskräckning genom förnekande

Utifrån beskrivningarna operationaliseras avskräckning genom förnekande genom begreppen *defensiva åtgärder*, *kommunikation* och *överlägsenhet*. Kommunikation används både för bestraffande och förnekande, men skiljs åt inom analysen.

Defensiva åtgärder

Förnekande cyberavskräckning är mindre konflikt driven och baseras på *defensiva åtgärder*, vilket både inkluderar att förhindra motståndaren från att agera och en lösning vid ett angrepp (Ryan 2018, s. 334). I cyberrymden antar avskräckning genom förnekande en mer defensiv roll genom att avskräcka eller störa attacker via robusta system eller, proaktiva och kostsamma förberedelser (Iasiello 2014, s. 56).

Hur beskriver Finland sin användning och utveckling av defensiva åtgärder som svar på cyberincidenter?

Kommunikation

Effektiv *kommunikation* mellan stater inger trovärdighet (Iasiello 2024, s.56). För förnekande avskräckning handlar detta om att förmedla en stats förmåga till cyber- och informationssäkerhet (Iasiello 2024, s. 57). Det förväntade resultatet är att en angripare avstår från att genomföra ett angrepp eftersom det skulle kräva för omfattande resurser (Tor 2017, s. 108).

Hur beskriver Finland sin förmåga till cyber- och informationssäkerhet?

Överlägsenhet

En betydelsefull förutsättning för trovärdig cyberavskräckning genom förnekande är att motståndaren uppfattar en *överlägsenhet i cyberrymden* (Tor 2017, s. 108). Detta gäller särskilt inom underrättelseverksamhet och offensiva förmågor, i syfte att kunna övertyga en motståndare om att det inte är realistiskt att vinna på grund av ett avgörande kvalitativt övertag (Tor 2017, s.108)

Hur beskrivs Finlands cyberförmågor i relation till andra stater?

Tabell 1: Översikt operationalisering

Teori	Begrepp	Indikatorer	Frågeställning
Avskräckning genom bestraffning	Offensiva åtgärder och proportionalitet	<ul style="list-style-type: none"> • Offensiva/aktiva åtgärder mot cyberincidenter. • Digitala vedergällningar. • Kinetiska attacker mot fysiska mål som svar på cyberattacker. • Diplomatiska medel, ekonomiska sanktioner som svar på cyberattacker. • Proportionalitet vid offensiva åtgärder i cyberdomänen. • Nationella cyberlagar. 	<p>Hur beskriver Finland användningen av offensiva åtgärder som svar på cyberincidenter?</p> <p>Hur står offensiva åtgärder i proportion till en cyberincident?</p>
	Attribuering	<ul style="list-style-type: none"> • Hotbild, hotaktörer, proxyaktörer. • Offentliga uttalande om stater kopplade till cyberangrepp. • Teknisk expertis och politisk vilja att hålla en angripare ansvarig. • Attribuering/tillskrivning/identifiering av en motståndare. • Underrättelse och informationsinhämtning 	<p>Hur arbetar Finland med att identifiera motståndare i cyberdomänen?</p> <p>Vad utgör det primära hotet i Finlands cyberstrategier?</p>
	Kommunikation	<ul style="list-style-type: none"> • Nationellt och internationellt agerande mot cyberincidenter. 	<p>Hur har Finland kommunicerat gränssättning gentemot en</p>

		<ul style="list-style-type: none"> • Uttalade konsekvenser vid gränsöverskridande cyberincidenter. • Viljan att hålla en aktör ansvarig. 	motståndare inom cyberdomänen?
	Signalering	<ul style="list-style-type: none"> • Deltagande i militär/försvarsövningar • Ekonomiska satsningar och budget relaterat till cyberförsvar och cybersäkerhet • Diplomatiska handlingar 	Hur har Finland signalerat vilja och förmåga att använda bestraffning som svar på cyberincidenter?
Avskräckning genom förnekande	Defensiva åtgärder	<ul style="list-style-type: none"> • Proaktiva, defensiva cybersäkerhetsåtgärder • Nationellt och internationellt samarbete inom cybersäkerhet • Informationsdelning • Robusta digitala system • Utbildning och kompetensutveckling inom cybersäkerhet • Samordning mellan myndigheter 	Hur beskriver Finland sin användning och utveckling av defensiva åtgärder som svar på cyberincidenter?
	Kommunikation	<ul style="list-style-type: none"> • Skydd av vital digital infrastruktur • Återhämtning av digitala system efter cyberangrepp (resiliens) • Cybermotståndskraft i samhället • Övergripande cybersäkerhet i samhället • Krisberedskap 	Hur beskriver Finland sin förmåga till cyber- och informationssäkerhet?

	Överlägsenhet	<ul style="list-style-type: none"> • Digitalisering i samhället • Samarbete inom olika sektorer i samhället • Teknisk utbildningsnivå och kompetens • Internationella samarbeten (EU/NATO/FN m.fl.) 	Hur beskrivs Finlands cyberförmågor i relation till andra stater?
--	----------------------	---	---

7. Material

Samtligt empiriskt material kommer att bestå av offentliga finska källor som behandlar de översiktliga nationella cyberstrategierna och inte enskilda företag eller organisationers interna strategier. Valet av enbart offentliga källor motiveras av författarens begränsade tillgång till sekretessbelagda källor samt med hänsyn till spridning av känslig information. Empiriurvalet utgår från finländska källor för att säkerställa att det nationella perspektivet framgår. Detta begränsar inte möjligheten till en djupgående analys, utan snarare ger det en övergripande bild utifrån källor som finns tillgängliga för allmänheten. Eftersom företag och organisationer skall utgå ifrån den nationella handlingsplanen anses inte enskilda strategier vara centrala för analysen. Organisationer som är verksamma inom den nationella cybersäkerheten kommer däremot att inkluderas, men inte deras interna strategiska handlingsplaner.

Cyberstrategi betraktas inom studien som en samlad strategisk inriktning för Finlands arbete inom cybersäkerhet och cyberförsvar. Den sammanställda empirin består av offentliga cybersäkerhetsstrategier mellan 2013 och 2030, myndighetsrapporter från finländska underrättelse- och säkerhetspolisen (SUPO) samt uttalanden från relevanta myndigheter och organisationer som finska Försvarsmakten och Nato.

Vid insamling av empiriskt material har författaren utgått ifrån huvudkällan inom arbetet, Finlands regering, och vidare sökt inom relaterade arkiv och hänvisade myndighetssidor.

7.1 Källkritik

Det empiriska materialet som används inom studien är primärkällor publicerade av Finlands regering och tillhörande myndigheter, vilket gör att risken för förfalskning och manipulation av texternas innehåll är låg (Esaiasson m.fl. 2024, s. 138). Därav bedöms källornas äkthet vara hög och även deras trovärdighet eftersom primärkällor oftast klassas som mer trovärdiga än sekundärkällor (Esaiasson m.fl. 2024, s. 140). Samtidigt är cybersäkerhetsstrategier politiskt styrda, vilket innebär att de kan vara medvetet eller omedvetet vinklade för att framhäva sina styrkor och undvika förekomsten av brister och svagheter i dokumenten (Esaiasson m.fl. 2024, s. 142-143). Liknande gäller Finlands försvarsmakt och SUPO, där publiceringen av översiktsrapporter inte vill inge ett svagt intryck. Därför finns det risk att skribenterna tenderar att överdriva eller utelämna information, vilket innebär att det bör beaktas att de eventuellt inte är neutrala i sina beskrivningar. Det finns även förväntningar på de gällande dokumenten och strategierna som publiceras av regeringen och statliga myndigheter. Vilket både är fördelaktigt kopplat till kvalitet men innebär också att de kan vara svåra att revidera och anpassa i takt med omvärldsläget och därigenom påverka hur samtida källan framstår (Esaiasson 2024, s. 141). Däremot avser det mindre revideringar utan större påverkan, då omfattande revideringar i stället leder till fullständigt uppdaterade versioner av årsrapporter, cybersäkerhetsstrategier och lagtexter.

7.2 Forskningsetik

Författaren har tagit hänsyn till eventuella etiska implikationer utifrån val av källor och har eftersträvat objektivitet genom hela arbetsprocessen. Då studien behandlar aktuella nationella säkerhetsfrågor är författaren medveten om att resultatet både kan bidra till ökad förståelse inom cybersäkerhet och ge insikter om sårbarheter. Samtidigt har studien enbart baserats på offentligt empiriskt material, vilket går i linje med tidigare forskares källmaterial inom cybersäkerhet och bedöms därför inte utgöra ett etiskt problem. Teorin berör inom vissa aspekter våldsanvändning, vilket beaktas inom beskrivningen av den för att det inte ska uppfattas som att studien främjar sådana handlingar.

8. Analys

Analysen kommer att struktureras genom att inledningsvis presentera svaren på analysfrågorna kopplade till cyberstrategin innan Nato-inträdet och därefter presentera analysen av cyberstrategin efter Nato-inträdet. En sammanfattning kommer att presenteras efter respektive analysdel för att kunna återknyta till studiens forskningsfråga i slutsatsen.

8.1 Före Nato-inträdet

8.1.1. Cyberavskräckning genom bestraffning

Hur beskriver Finland användningen av offensiva åtgärder som svar på cyberincidenter?

Hur står möjliga offensiva åtgärder i proportion till en cyberincident?

I Finlands cybersäkerhetsstrategi (2013, s. 8) står det att landets militära cyberkapacitet omfattar underrättelsetjänster samt cyberattack- och försvarskapaciteter. För Finlands cybersäkerhetsstrategi (2019, s. 5) nämns motåtgärder inom cyberdomänen vilka kan bestå av brottsbekämpande åtgärder, diplomatiska åtgärder eller aktiva cybermotåtgärder.

Finlands utrikesministerium (2020, s. 1) beskriver den lagstiftning som Finland tillämpar inom cyberdomänen och internationell rätt och framhåller att denna överensstämmer med FN-stadgan. Detta innebär att en cyberattack kan omfattas av rätten till självförsvar och användandet av våld om den uppfyller kriterierna: att den är tillräckligt allvarlig samt leder till omfattande konsekvenser inom statens territorium eller i områden inom dess jurisdiktion, som liknar dem vid fysisk våldsanvändning (Finlands utrikesministerium 2020, s. 6). Detta innebär också att våldsanvändningen inte får vara oproportionerlig eller överdriven (Finlands utrikesministerium 2020, s. 7).

Hur arbetar Finland med att identifiera motståndare i cyberdomänen?

Vad utgör det primära hotet i Finlands cyberstrategier?

Finlands cybersäkerhetscentrum ska upprätthålla förmågan att sammanställa situationsmedvetenhet dygnet runt och samarbete mellan myndigheter och näringsliv (Finlands regering 2019, s. 7). Detta ska främja Finlands förmåga att identifiera och varna för hot mot informationssäkerheten och förbättra möjligheten för såväl näringslivet som offentliga förvaltningen att förbereda sig för hot mot informationssäkerheten (Finlands regering 2019, s. 7). Målet är att förbättra situationsmedvetenheten hos olika aktörer i samhället genom att förse dem med realtidsinformation om sårbarheter, störningar och deras effekter (Finlands regering 2013, s. 7). Situationsbilden inkluderar även hotbedömningar inom cyberrymden (Finlands regering 2013, s.7).

I Finlands nationella säkerhetsöversikt (2021, s.34) konstateras det att statligt sponsrat cyberspionage är det mest kritiska cyberhotet mot den nationella säkerheten. Samtidigt som

Finland är ett mål för ständiga försök till cyberspionage (Finlands regering 2021, s.34). Auktoritära stater använder cyberspionage för att samla in underrättelser till stöd för sin egen nationella politik och för att påverka de beslutsfattare som är måltavlor för sådana operationer (SUPO 2021, s. 2). De kan även försöka utöva en avskräckande effekt genom att demonstrera sin förmåga att verka i en cybermiljö (SUPO 2021, s. 2). Även i Finlands cybersäkerhetsstrategi (2019, s. 4) framgår cyberbrottslighet, cyberspionage och statligt främmande underrättelsearbete som primära föränderliga hot.

Hur har Finland kommunicerat gränssättning gentemot en motståndare inom cyberdomänen?

I Finlands cybersäkerhetsstrategi (2013, s.8) beskrivs det att målet för Finland är att upptäcka och identifiera eventuella störningar i vitala funktioner som framkommer och reagera på dem på ett sätt som minimerar deras akuta effekter. Senare i Finlands cybersäkerhetsstrategi (2019, s.5) framgår det att cybermiljön ska skyddas genom att höja tröskeln för olika typer av cyberattacker genom att exempelvis förbättra observations- och attributionsförmågan för cyberattacker samt förmågan att reagera. Motåtgärder kan bestå av brottsbekämpande åtgärder, diplomatiska åtgärder eller aktiva cybermotåtgärder (Finlands regering 2019, s. 5).

Hur har Finland signalerat vilja och förmåga att använda bestraffning som svar på cyberincidenter?

Resursfördelning är ett sätt att signalera och bygga förmåga, vilket inkluderar ekonomiska satsningar. Där är ett exempel Finlands upprättande av cybersäkerhetscentret hos dåvarande Finska trafik- och kommunikationsverket 2013 (Finlands regering 2013, s. 7).

De tillgängliga budgetöversikterna mellan 2019 och 2023 (Finlands finansdepartement 2026) specificerar inte några ekonomiska satsningar på cybersäkerhet utan inkluderar detta i landets försvarsbudget för respektive år.

Även om Finland inte blev medlem i Nato förrän 2023, slöt de ett politiskt ramavtal 2017 om samarbete inom cyberförsvar (Nato 2017). Avtalet skulle göra det möjligt för Nato och Finland att bättre skydda och förbättra motståndskraften hos sina nätverk genom förbättrad situationsmedvetenhet och informationsutbyte mellan länderna (Nato 2017). Finland har även bjudits in att delta i gemensamma cyberförsvarsövningar som Locked Shields 2021/2022 samt Cyber Coalition 2021/2022 (Nato 2022 b). Under övningen Locked Shields 2022 utsågs Finland som ”vinnare” av övningen (Nato 2022 b). Detta genom att visa på landets förmåga

att försvara sig och respondera inom cyberdomänen, inom ramen för en övning som Nato beskriver som: ”Den största och mest komplexa verklighetssimulerade internationella cyberförsvarsövningen i världen” (Nato 2022 b).

8.1.2. Cybervskräkning genom förnekande

Hur beskriver Finland sin användning och utveckling av defensiva åtgärder som svar på cyberincidenter?

I Finlands cybersäkerhetsstrategi (2013, s. 8) framgår det att Försvarsmakten kommer att skydda sina system på ett sådant sätt att de kan utföra sina uppgifter oberoende av hoten i cybervärlden. Detta inkluderar garantier för cyberförmågor, underrättelser och proaktiva åtgärder i cyberrymden som en del av de militära styrkorna (Finlands regering 2013, s.8). Vidare beskrivs det i försvarsrapporten (2021, s. 34) att cyberdomänen kommer att skyddas genom att höja tröskeln för cyberattacker.

Riktlinjerna inom Finlands cybersäkerhetsstrategi (2013, s. 7) redogör för olika nationella sektors beredskap för att säkra vitala funktioner under såväl normala som störda förhållanden ska förbättras genom att regelbundna övningar organiseras. Målet med övningarna är att öka deltagarnas möjlighet att avslöja sårbarheter i sina egna handlingar och system och utveckla sina förmågor (Finlands regering 2013, s. 7).

EU:s riktlinjer för utveckling av ett starkt cyberförsvar beaktas vid utvecklingen av cyberförmågorna. Inom ramen för EU bidrar Finland till kampen mot cyberbrottslighet genom internationellt samarbete mellan rätts- och brottsbekämpande myndigheter och genom att bidra till utvecklingen av internationell rätt och internationella avtal (Finlands regering 2013, s. 8).

Hur beskriver Finland sin förmåga till cyber- och informationssäkerhet?

I Finlands cybersäkerhetsstrategi (2013, s. 1–2) framgår det att landet som ett litet, kompetent och samarbetsriktat land har utmärkta chanser att bli ledande inom cybersäkerhet. Landet hade redan tidigt i cyberutvecklingen målet att vara en internationell föregångare inom cybersäkerhet. Senast 2016 skulle landet vara en global föregångare mot cyberhot och i hanteringen av störningar orsakade av dessa hot (Finlands regering 2013, s. 3). Genomgående i deras cyberstrategi är modellen för övergripande säkerhet (comprehensive security), som motsvarar Sveriges totalförsvar och utgör grunden för det finländska samhällets motståndskraft (Finlands regering 2013 s.1). Detta innebär att den heltäckande säkerheten för

samhällets vitala funktioner tillgodoses genom samarbete mellan myndigheter, näringslivet, organisationer och medborgare under alla omständigheter och på alla samhällsnivåer (Finlands regering 2024, s. 49).

”Nationell cybermotståndskraft kommer att anpassas för att säkerställa den beredskap och förutsäggelseförmåga som krävs för att uppnå målen för övergripande säkerhet och för att underlätta dess operativa förmåga under cyberstörningar samt återhämtning efter störningar” (Finlands regering 2013, s. 4). Finland framhäver beredskap, förutsägelse av hot, redundans och återhämtning efter en attack, vilket är vad cyberresiliens bygger på, då det inte enbart handlar om att skydda sig mot cyberattacker utan också om att kunna stå emot, anpassa sig och snabbt återhämta sig (Finländska regeringen 2024, s. 49). Inom Finlands cybersäkerhetsstrategi (2019, s.9) finns en tydlig ansvarsdelning mellan myndigheter, organisationer och institutioner för att upprätthålla cybersäkerheten. Det betonas att det krävs en hög utbildningsnivå inom nationellt kritiska cyberkompetensnivåer som kommer säkerställas genom stöd av både nationella och internationella övningar och utbildningar (Finlands regering 2019, s. 9).

Hur beskrivs Finlands cyberförmågor i relation till andra stater?

Finland har arbetat enligt sin modell för övergripande säkerhet (comprehensive security) under flera år innan Nato-medlemskapet. Modellen innebär att den heltäckande säkerheten för samhällets vitala funktioner tillgodoses genom samarbete mellan myndigheter, näringslivet, organisationer och medborgare under alla omständigheter och på alla samhällsnivåer (Finlands regering 2024, s. 49). Finland har bland annat ett cybersäkerhetscentre vid finska trafik- och kommunikationsverket (Traficom) som är Finlands nationella myndighet för att skydda digitala kommunikationsnät och tjänster (Traficom 2026).

Finland har länge haft ett aktivt samarbete med Europeiska unionen, vilket betonas i landets cybersäkerhetsstrategi (Finlands regering 2013, s. 9). Där framgår det att EU samt många internationella organisationer, såsom FN och Nato, är viktiga mötesplatser för landets cybersäkerhet. Även i Finlands cybersäkerhetsstrategi (2019, s. 5) står det att samarbetet inom EU utgör ryggraden för Finlands nationella cybersäkerhetspolitik och dess utveckling. Där Finland deltar aktivt i utvecklingen av EU:s gemensamma utrikes- och säkerhetspolitik för cybersäkerhet (Finlands regering 2019, s. 5). Genom EU-medlemskapet får Finland även tillgång till ekonomiska och politiska verktyg kopplat till sanktioner och rättsliga påföljder för en identifierad angripare.

Sammanfattning:

Finland inkluderar offensiva förmågor inom sin militära cyberkapacitet, men de beskrivs på en övergripande nivå. Exempelvis vad diplomatiska samt aktiva cybermotåtgärder innebär specificeras inte ytterligare. Landet betonar situationsmedvetenhet och förvarning samt hotbedömning, vilket är en förutsättning för att tillskriva en motståndare. Däremot framgår inte den konkreta arbetsprocessen för informationsinhämtningen. Det primära hotet utgörs av cyberspionage kompletterat av cyberbrottslighet och främmande underrättelsearbete. Finland beskriver hotbilden i generella termer och specificerar varken statliga aktörer eller proxyaktörer. Det framgår att störningar av vitala funktioner kommer att leda till reaktioner samt att de vill höja tröskeln för angrepp genom bland annat situationsmedvetenhet och förmågan att reagera. Detta kopplas inte till någon tydlig gränssättning och förblir otydligt. Finlands ekonomiska satsningar på cybersäkerhet, deltagande i nationella gemensamma försvarsövningar och avtal med Nato stärker dess trovärdiga förmåga att inte enbart förebygga cyberattacker utan också potentiellt bemöta dem med bestraffande åtgärder. Finland beskriver användningen av defensiva åtgärder som underrättelseförmågor och proaktiva åtgärder för att bemöta hot i cyberdomänen. Samtidigt betonar landet att detta ska höja tröskeln för cyberattacker. Regelbundna övningar och internationellt samarbete är en viktig del för att stärka och vidareutveckla de defensiva cyberförmågorna. Finland uttrycker en tydlig vilja till att vara ledande inom cyber- och informationssäkerhet där samarbetet mellan olika samhällsaktörer är en central del inom den övergripande säkerheten. De betonar beredskap, förutsägelseförmåga samt cyberresiliens och ett robust digitaliserat samhälle. Finland beskriver sina förmågor som starkt utvecklade i ett internationellt sammanhang, där landet har en samhällsintegrerad cybersäkerhetsstruktur som bidrar till ett kollektivt cyberförsvar. Samarbetet med EU har bidragit till ett politiskt och ekonomiskt fördel kopplat till sanktioner och ekonomiska påföljder, vilket bidrar till landets övergripande avskräckningsförmåga.

8.2. Efter Nato-inträdet

8.2.1. Cyberavskräckning genom bestraffning

Hur beskriver Finland användningen av offensiva åtgärder som svar på cyberincidenter?

Hur står möjliga offensiva åtgärder i proportion till en cyberincident?

I Finlands cybersäkerhetsstrategi (2024, s. 36) har de fyra tydliga strategiska mål för att snabbt kunna agera mot cyberhot och även säkerställa den nationella suveräniteten. En del av

dessa är att hantera cyberhot genom diplomati, underrättelsetjänst, informationshantering och strategisk kommunikation, militär kapacitet samt ekonomiska och finansiella metoder (Finlands regering 2024, s. 40). De betonar även att Finland ska bemöta de geopolitiska utmaningarna som cybermiljön innebär genom aktiv cyberdiplomati, cyberförsvar och cybersäkerhetsåtgärder, både självständigt och som en del av multilaterala aktiviteter (Finlands regering 2024, s. 37).

Aktörer i såväl privat som offentlig sektor ska ha tydligare roller och befogenheter samt förmågan att reagera på cyberincidenter (Finlands regering 2024, s.37).

Cyberförsvarsdoktrinen ska ge nationella operativa principer för att reagera på statsstödda hot och hot mot den nationella säkerheten (Finlands regering 2024, s.37). Det betonas att svaren på ett cyberhot måste vara heltäckande, långsiktiga och i rätt tid (Finlands regering 2024, s. 37).

Som tidigare konstaterades ska våldsanvändningen inte vara oproportionerlig eller överdriven (Finlands utrikesministerium 2020, s. 7). Lagstiftningen är fortsatt gällande för Finland 2026 med vissa revideringar utifrån medlemskapet i Nato, men inte gällande proportionalitet kopplad till våldsanvändning i cyberrymden.

Hur arbetar Finland med att identifiera motståndare i cyberdomänen?

Vad utgör det primära hotet i Finlands cyberstrategier?

Finland beskriver i sin cybersäkerhetsstrategi (2024) hur de ska gå tillväga för att tillskriva aktörer i cyberrymden. De beskriver att attribuering sker genom att samla in och analysera fakta, genomföra teknisk, politisk och juridisk bedömning, fatta beslut och slutligen kommunicera sådana beslut till olika organisationer och myndigheter (Finlands regering 2024, s. 39). Processen inkluderar inhämtad information från underrättelse-, cybersäkerhets-, utrednings- och andra offentliga myndigheter inom ramen för deras ordinarie uppgifter (Finlands regering 2024, s.39). Detta innebär att underrättelse- och säkerhetsmyndigheter ska ha utökade befogenheter att dela information (Finlands regering 2024, s.39).

Finlands cybersäkerhetsstrategi (2024) noterar att sedan cybersäkerhetsstrategin (2019) har säkerhetsläget drastiskt förändrats av bland annat covid-19-pandemin och Rysslands invasion av Ukraina 2022 och inte minst Finlands Nato-medlemskap (Finlands regering 2024, s.13). Hoten har blivit alltmer mångsidiga och hotet från statligt cyberspionage är inte längre begränsat till att enbart forma utrikes- och säkerhetspolitik utan även andra delar av samhället

(Finlands regering 2024, s. 20). Cyberhoten är alltmer kopplade till organiserad cyberbrottslighet och statsstödda aktörer. Stater anlitar i större utsträckning kriminella grupper (Proxyaktörer) som mellanhänder för att genomföra attacker, vilket gör det svårare för försvararen att identifiera hotet och ger dem mer flexibilitet i sina operationer (Finlands regering 2024, s. 15). Samtidigt har Finlands underrättelse- och säkerhetsavdelning (SUPO) direkt uttalat att både Ryssland och Kina utgör ett hot mot landets cybersäkerhet, där Ryssland kan omdirigera cyberresurser från Ukraina mot Finland i en nära framtid (SUPO 2025).

Hur har Finland kommunicerat gränssättning gentemot en motståndare inom cyberdomänen?

I Finlands cybersäkerhetsstrategi (2024, s. 40) beskrivs det att målet för Finland är att reagera på cyberhot orsakade av tredjepart, länder som inte ingår i samma allianser eller samarbeten, genom både förebyggande, reaktiva och långsiktiga åtgärder. Detta genom diplomati, underrättelsetjänst, informationshantering och strategisk kommunikation, militär kapacitet samt ekonomiska och finansiella metoder (Finlands regering 2024, s. 40). En stat kan hållas ansvarig för varje cyberoperation som bryter mot internationella förpliktelser om dess egna organ (eller proxyer) kan identifieras som förövare (Finlands regering 2024, s. 40). I Finlands cybersäkerhetsstrategi (2024) betonar Finlands premiärminister Petteri Orpo att landet eftersträvar att vara en stark cybersäkerhetspartner i Europeiska unionen och Nato, där de kommande cybersäkerhetsdoktrinerna kommer att tillhandahålla nationella operativa principer för att hantera statsstödda hot och hot mot nationell säkerhet (Finlands regering 2024, s. 8).

Hur har Finland signalerat vilja och förmåga att använda bestraffning som svar på cyberincidenter?

I den reviderade finska cybersäkerhetsstrategin (2024) förtydligas koordinering på strategisk nivå, men det konstaterades trots allt att det fanns utmaningar med att implementera den på grund av frånvaron av en inkluderande budget eller tilldelade resurser inom cybersäkerhet (National Audit Office of Finland 2025).

Finland deltog 2025 i cyberövningen Cyberflag (25–2) tillsammans med bland annat svenska Försvarsmakten. Övningen organiserades av US Cyber Command och inkluderade cyberspecialister från cirka 20 länder runt om i världen (Finlands försvarsmakt 2025). Finland deltog också i Natos övning Cyber Coalition 2024 där totalt 27 Nato-medlemsländer deltog, med motiveringen: ”Att dela information om cyberhot i realtid mellan allierade hjälper till att identifiera de ansvariga hotaktörerna och vid behov reagera på dem – gemensamt om det behövs” (Finlands Försvarsmakt 2024).

Samuel Bergström, chef för Finlands nationella cybersäkerhetscentrets avdelning för incidenthantering, kommenterade kring övningen: ” När civila och militära myndigheter tränar tillsammans kan eventuella utmaningar som kan uppstå identifieras och bemötas gemensamt och snabbt ” (Finlands Försvarsmakt 2024). Syftet med denna typ av övningar är att träna på att möta hot i en simulerad cybermiljö och dela erfarenheter länder emellan (Finlands Försvarsmakt 2024). Gemensamma försvarsövningar är ett sätt för Finland att utåt visa att de upprätthåller sina cyberkapaciteter och utvecklar dem genom samarbeten med andra nationer (Finlands Försvarsmakt 2024).

8.2.2. Cyberavskräckning genom förnekande

Hur beskriver Finland användning och utveckling av defensiva åtgärder som svar på cyberincidenter?

Ett Natomedlemskap stärker Finlands säkerhet och försvar, men medför också nya utmaningar och skyldigheter (Finlands regering 2024, s.14). Natomedlemskapets avskräckande effekt kan leda till att fokus för fientliga operationer i allt högre grad förskjuts från traditionella hot till cyberdomänen där förövarna mer troligt kan förneka inblandning (Finlands regering 2024, s. 14).

I Finlands cybersäkerhetsstrategi (2024, s. 27) framgår det att landet har en proaktiv inställning i arbetet mot cyberhot. Detta är en del av Finlands förebyggande arbete och inkluderar även att befolkningen ska tro på att samhället kan fungera under alla omständigheter (Finlands regering 2024, s.27).

Cyberövningar utgör en grund för stark cybermotståndskraft i samhället som helhet. Övningsmiljöer och verksamhetsmodeller för cybersäkerhet måste kontinuerligt utvecklas för att svara mot en föränderlig verksamhetsmiljö (Finlands regering 2024 s.30). Den finska infrastrukturen utvecklas som en del av alliansens infrastruktur, vilket stärker samarbetet inom alliansen och cyberförsvaret (Finlands regering 2024, s.34). Majoritet av de sju grundläggande kraven för motståndskraft som Nato har definierat ställer även krav på utveckling av den nationella cybersäkerheten (Finlands regering 2024. 34).

Hur beskriver Finland sin förmåga till cyber- och informationssäkerhet?

I Finlands cybersäkerhetsstrategi (2024) betonas landets roll inom Natos kollektiva försvar, men fortsatt cybersäkerhet som en viktig delkomponent i deras modell för övergripande säkerhet (comprehensive security) från cybersäkerhetsstrategierna 2013 och 2019. Cyber- och

informationssystem är en grund för samhällets cybermotståndskraft och därför måste de ägna uppmärksamhet åt att upphandla, utveckla och underhålla sådana system inom både offentlig och privat sektor (Finlands regering 2024, s. 28). Ömsesidigt förtroende mellan olika aktörer i samhället och förtroende för offentliga institutioner och deras tjänster bidrar till att bygga upp en stark nationell motståndskraft (Finlands regering 2024, s.28). Finland anser att för ett framgångsrikt nationellt cybersäkerhetsarbete krävs förtroende, beredskap, gemensam situationsmedvetenhet och snabba insatser (Finlands regering 2024, s. 28–29).

Hur beskrivs Finlands cyberförmågor i relation till andra stater?

Cyberstrategin efter Nato-inträdet bibehåller centrala inslag från tidigare strategi, som modellen för övergripande säkerhet och det aktiva medlemskapet i EU. Cybersäkerhet är en viktig del av den finska modellen för övergripande säkerhet och samhället är nästan helt digitaliserat (Finlands regering 2024, s. 8).

Finlands premiärminister uttrycker sig enligt följande: *Hundratals specialister och intressenter från den offentliga och privata sektorn, forskarsamhället och civilsamhällesorganisationer har deltagit i utformningen av [cybersäkerhets] strategin. Detta är ett utmärkt exempel på det finska samhällets engagemang och den finska modellen för heltäckande säkerhet* (Finlands regering 2024, s. 9).

I Finlands cybersäkerhetsstrategi (2024, s. 17) står det att en ständigt växande andel av den dagliga mänskliga aktiviteten och användningen av offentliga tjänster sker i en digital miljö. Offentlig förvaltning och tjänster i Finland hamnar därför ofta på första plats i internationella digitaliseringsrankningar (Finlands regering 2024, s.17).

Komplementet är den gemensamma försvarsförmågan tillsammans med Nato. I Finlands cybersäkerhetsstrategi (2024, s. 34) framgår det att Finland är en konstruktiv, pålitlig och kapabel NATO-allierad som upprätthåller en stark nationell försvarsförmåga som en del av NATO:s gemensamma avskräckning och försvar och som aktivt deltar i utvecklingen av NATO:s cyberförsvar. Enligt Finlands cybersäkerhetsstrategi (2024, s. 34) är det viktigt att samordna EU:s och Natos nationella syn på cybersäkerhet och cyberförsvar för att stärka såväl den internationella som Finlands nationella cybersäkerhet. Samarbete med såväl EU som Nato medger fördelar för underrättelse och informationsspridning och gemensam försvarsplanering (Finlands regering 2024, s.34).

Sammanfattning:

Finland beskriver offensiva åtgärder som svar på cyberattacker genom en bredare beskrivning som inkluderar att kunna agera mot cyberhot och säkerställa den nationella suveräniteten. Detta kan bemötas genom såväl diplomati som militär respons eller ekonomiska och finansiella metoder. Cyberförsvarsdoktrinen ska reglera de operativa principerna som gäller för statsstödda hot. Samtidigt ska responsen fortsatt vara proportionerlig och värderad utifrån angreppets omfattning. Finland arbetar med att identifiera motståndare genom en strukturerad attribueringsprocess som sträcker sig från insamling av information till juridisk bedömning och samverkan mellan olika myndigheter och organisationer. De lyfter att hoten blir alltmer mångsidiga där cyberspionage utgör ett av de primära hoten tillsammans med organiserad cyberbrottslighet och statsstödda aktörer. Ryssland och Kina lyfts fram som centrala hotaktörer, där även proxyaktörer blir mer framträdande. En stat kan hållas ansvarig för varje cyberoperation som bryter mot internationella förpliktelser om dess egna organ, eller proxyaktörer, kan identifieras som förövare. Detta är ett sätt att kommunicera vad gränsen går för ett hot eller angrepp, eftersom det signalerar att så länge en aktör kan identifieras kommer det få följder. De potentiella följderna specificeras inte utan beskrivs som ett brett spektrum av åtgärder. Finland signalerar förmågan att använda bestraffning som svar på cyberattacker genom fortsatt aktivt deltagande i internationella cyberövningar med Nato och andra allierade. Samtidigt framgår det att avsaknaden av en budget och tilldelade resurser inom deras reviderade cybersäkerhetsstrategi skapar utmaningar för dess trovärdighet. Finland beskriver att de har en proaktiv inställning i arbetet mot cyberhot som inkluderar förebyggande arbete och att befolkningen ska ha inställningen att samhället fungerar även vid omfattande cyberincidenter. Detta utgör en del av både det tekniska och det psykologiska svaret på cyberincidenter. Samtidigt ställer Nato-medlemskapet krav på utveckling av cybersäkerheten och den finländska infrastrukturen ska utvecklas som en del av alliansen. Finland förmedlar att deras cybersäkerhet fortsatt är en viktig delkomponent i deras modell för övergripande säkerhet och att det finns en stark nationell motståndskraft. Samtidigt bidrar Nato-medlemskapet till utveckling av dessa förmågor. Finland betonar landets integrering inom det internationella samfundet genom medlemskapet i EU och Nato. De antyder att landet är en pålitligt och kapabel Nato-allierad som upprätthåller en stark nationell försvarsförmåga som en del av den gemensamma avskräckningen och cyberförsvaret. Samtidigt betonas landets nationella förmåga och engagemang för heltäckande cybersäkerhet i samhället.

9. Slutsatser

För att återknyta till forskningsfrågan: *Hur använder Finland cyberavskräckning i sin cyberstrategi innan och efter Nato-inträdet?*

Analysen visar att Finland i sin cyberstrategi innan Nato-inträdet framför allt använder cyberavskräckning genom förnekande, med inslag av bestraffande cyberavskräckning.

Finland arbetar med att kunna stå emot, anpassa sig och snabbt återhämta sig från cyberangrepp. Tydligt är deras modell för övergripande säkerhet där cybersäkerhet redan före Nato-inträdet har haft en viktig roll och inkluderat flera samhällsviktiga aktörer.

Tröskeeffekten används som ett sätt att förhindra angrepp och inkluderar såväl förebyggande som proaktiva åtgärder. Finland beskriver sina cyberförmågor som starkt utvecklade i ett internationellt sammanhang, där landet har en samhällsintegrerad cybersäkerhetsstruktur som bidrar till ett kollektivt cyberförsvar. Samarbetet med EU har bidragit till möjliga politiska och ekonomiska påföljder för en identifierad angripare, vilket bidrar till landets övergripande avskräckningsförmåga. Sammantaget höjer detta tröskeln för ett angrepp, vilket ska förneka angriparen den förväntade nyttan.

Avskräckning genom bestraffning används mer indirekt i cyberstrategin. Detta sker genom en delvis utvecklad attribueringsmetod, uttalade och proportionerliga motåtgärder samt signalering av förmåga genom försvarsövningar. Det anges däremot ingen tydlig gräns för en motståndare i cyberdomänen, begränsade angivna ekonomiska satsningar och resursallokeringar för deras cybersäkerhet, samt enbart en generell beskrivning av aktiva och diplomatiska åtgärder. Sammantaget framgår avskräckning genom bestraffning främst genom att signalera förmågan till det snarare än en tydlig vilja. Som tidigare har konstaterats krävs både en tydlig förmåga och en tydlig vilja för att hotet om bestraffning ska uppfattas som trovärdigt, vilket gör att Finlands användning blir mer indirekt.

Analysen av Finlands cyberstrategi efter Nato-inträdet visar att landet fortsatt övervägande använder avskräckning genom förnekande. Cyberstrategin har däremot ett tydligare bestraffande inslag än före Nato-inträdet.

Finland har blivit tydligare med hur de praktiskt går tillväga för att tillskriva en motståndare i cyberrymden med utökade befogenheter inom underrättelse- och säkerhetsmyndigheter för att analysera den insamlade informationen. Finland har även uttalat sig om att Ryssland och Kina utgör en del av den primära hotbilden, vilket de tidigare hade varit restriktiva med och i stället beskrivit utifrån generella termer. De har även tydligare definierat vilka handlingar som utlöser motåtgärder, genom att beskriva att varje cyberoperation som bryter mot

internationella förpliktelser av dess egna organ, eller proxyaktörer, och kan identifieras som förövare kommer att hållas ansvarig. Samtidigt har signalering genom deltagande i cyberförsvarsövningar fortsatt och Finland har förutom aktivt deltagande i Nato-ledda övningar även visat prov på hög kompetens och vilja till utveckling av cyberförmågor. Även om avskräckning genom bestraffning framkommer tydligare i cyberstrategin, finns det fortsatt en avsaknad av uttalade offensiva åtgärder och en vilja att använda dem.

Finlands förnekande cyberavskräckning är fortsatt ett tydligt inslag och i stort sett oförändrad sedan före NATO-inträdet. Finland har fortsatt att integrera cyberförsvar i modellen för övergripande säkerhet och betonar samarbetet mellan olika aktörer i samhället och förtroende för offentliga institutioner. Efter nato-inträdet finns det en förhöjd risk att fientliga operationer förskjuts till cyberdomänen eftersom en aktör enklare kan förneka inblandning, vilket ställer högre krav på förebyggande och defensiva åtgärder. Samtidigt fortsätter Finland att trycka på sin proaktiva inställning till cyberhot och betonar en systematisk utveckling och upprätthållande av cyberförsvaret. En av de tydligaste fördelarna efter Nato-inträdet är utökad underrättelse- och informationsspridning och gemensam försvarsplanering.

10. Diskussion

Finland har i sin cyberstrategi innan Nato-inträdet främst använt sig av cyberavskräckning genom förnekande, med inslag av bestraffande cyberavskräckning. Efter Nato-inträdet visar analysresultatet att landet fortsatt övervägande använder cyberavskräckning genom förnekande, men har ett tydligare inslag av cyberavskräckning genom bestraffning än tidigare. Detta har besvarat studiens huvudfrågeställning: *Hur använder Finlands cyberavskräckning i sin cyberstrategi innan och efter Nato-inträdet?*

Finland har visat att de använder en kombination av olika strategier inom cyberavskräckning för att uppnå trovärdighet och effektivitet, vilket tidigare forskning genom Lawson (2017) och Borghard och Lonergan (2023) förespråkar. Däremot visade resultatet att landet både innan och efter Nato-inträdet framför allt använder sig av förnekande cyberavskräckning, vilket tyder på en mer defensiv och förebyggande inställning trots ett medlemskap i Nato. Det finns inslag av cyberavskräckning genom bestraffning i båda strategierna i form av attribuering, signalering och till viss del kommunicerade tröskelöverskridande gränser. Samtidigt framstår viljan att använda offensiva åtgärder som otydlig, trots att förmågan kan antydas. Användningen utesluts däremot inte vid en cyberattack eller ett cyberhot som hotar den

nationella suveräniteten. Att Finland som en småstat innan Nato-inträdet framför allt använde cyberavskräckning genom att förneka en motståndare är inte oväntat med tanke på deras dåvarande säkerhetsläge. Samtidigt är deras förmåga till cyberavskräckning genom bestraffning redan innan medlemskapet mer oväntad med tanke på att det oftast är förknippat med stormakter. Det ska däremot understrykas att det finns flera komponenter som saknas för att Finland såväl innan som efter Nato-inträdet ska uppnå full trovärdig och effektiv cyberavskräckning genom bestraffning. Landets kapacitet att i framtiden potentiellt ha både förmåga och vilja efter en längre integrering i Natos strategiska koncept ska inte undervärderas. Samtidigt utgör deras användning av förnekande cyberavskräckning en viktig del av den nuvarande cyberstrategin och bör fortsatt vidareutvecklas.

Resultatet kan kopplas tillbaka till syftet med studien, som var att bidra till den övergripande forskningen om cyberavskräckning och mer specifikt redogöra för hur cyberavskräckning används i den finska cyberstrategin innan och efter Nato. Detta för att öka förståelsen för hur småstaters användning av cyberavskräckning påverkas i en förändrad säkerhetsmiljö. Studien har bidragit med ökad förståelse för hur en småstat som Finland har byggt upp en grund för användning av både cyberavskräckning genom förnekande och bestraffning redan innan Nato-medlemskapet. För att därefter utveckla detta inom ramen för en försvarsallians. Finlands cyberavskräckning har gått från att användas enbart som ett verktyg för att säkra den nationella territoriella säkerheten till att även bidra till den kollektiva avskräckningen hos alliansen. Detta visar hur småstaters cyberavskräckningsförmåga inte enbart behöver vara defensiv och förebyggande med anledning av deras ofta underlägsna position gentemot stormakter, utan även kan omfatta aktiva inslag i avskräckningssyfte. Utöver det övergripande syftet har studien bidragit till diskussionen kring cyberavskräckningsteori genom att belysa hur traditionell avskräckningsteori har anpassats till cyberdomänen och dess unika egenskaper.

Valet av teori har påverkat vad som har undersökts inom cyberavskräckning. Som nämnts under teoriasnittet finns det andra sätt för stater att använda cyberavskräckning än enbart genom förnekande och bestraffning. Detta gör att det finns delar som inte behandlas, men samtidigt har möjliggjort en djupare analys inom det valda området. Vilket har skapat förutsättningar för att bygga vidare på studien genom att undersöka cyberavskräckning genom exempelvis association, normer och tabun samt entanglement.

Då det empiriska materialet baseras på offentliga dokument och uttalanden går det inte att utesluta att mer omfattande svar på analysfrågorna hade funnits i sekretessbelagda dokument, som Finlands försvarsdoktrin. Detsamma gäller uttalande från politiker eller andra myndighetspersoner som inte påträffades vid sökning efter empiriskt material. Samtidigt har det funnits en transparens i studien om att det empiriska materialet baseras på offentliga dokument och uttalanden, med anledning av saknad åtkomst och av att inte diskutera känslig information. Trots begränsningen har samtliga analysfrågor kunnat besvaras i olika utsträckning och återknytas till huvudfrågeställningen.

Författaren har kontinuerligt reflekterat över forskningsdesignen kopplad till studien. Valet av en deskriptiv ansats har varit lämpligt för att besvara forskningsfrågan, samt att en kvalitativ textanalys har möjliggjort en djupgående genomgång av det empiriska materialet.

Textanalysen har varit omfattande kopplad till det empiriska materialet där cyberavskräckning inte framgår uttryckligen. En mer generaliserbar ansats, som teoriprövande, hade även kunnat vara lämplig inom studien men hade inneburit en annan forskningsfråga samt ett annat syfte för studien.

Avslutningsvis har Finland inom denna studie visat att trots att cyberavskräckning är komplex finns det flera tillvägagångssätt som tillsammans stärker landets motståndskraft inom cyberdomänen, både som icke-Natoallierad och inom ramen för Natos kollektiva försvar.

10.1. Relevans för yrkesutövningen

Cyberdomänen används dagligen av personal i hela den svenska Försvarsmakten där cybersäkerhet alltid ska beaktas vid all användning. Sverige har, likt Finland, också blivit medlem i Nato under en tidsperiod där digitalisering och exploatering i cyberrymden har blivit högaktuella. Som officer är det en nödvändighet att inte bara ha förståelse för vad ett cyberangrepp eller cyberhot kan innebära för konsekvenser för samhället, utan även för hur det förväntas förebyggas och alternativt bemötas på en strategisk nivå. Medlemskapet i Nato innebär också att alliansens strategiska koncept ska implementeras i de nationella strategierna, vilket även gäller för cyberdomänen. Att ha kunskap om vad förändringar som dessa kan innebära för utformningen av landets cyberstrategi kan ha betydelse för hur man agerar i händelse av ett potentiellt cyberangrepp eller cyberhot. Som officer är det av värde att inte enbart ha förståelse för hur den egna staten använder cyberavskräckning, utan även för hur

stater med liknande säkerhetspolitisk inriktning går till väga. Det kan bidra till utvecklingen av Sveriges cyberavskräckning där Försvarsmakten tillsammans med andra myndigheter och organisationer behöver samarbeta.

10.2. Vidare forskning

Studien kan byggas vidare genom att byta fall från Finland till Sverige för att se potentiella likheter och skillnader i användningen av cyberavskräckning. Då studien enbart är deskriptiv skulle detta utöka kunskapen om hur förändringar i en säkerhetsmiljö påverkar användningen av cyberavskräckning, även för andra småstater. Sverige kan antingen användas inom en enfallsstudie, i likhet med Finland, eller ingå i en jämförande fallstudie där resultatet från denna studie används för att jämföra med Sverige.

Ett annat alternativ är att nyttja teoridelarna som inte tillämpades inom ramen för denna studie för att undersöka hur Finland använder andra strategier inom cyberavskräckning. Förslagsvis att även undersöka hur de använder avskräckning genom association, normer och tabun samt entanglement. Detta skulle kunna nyansera studien ytterligare eftersom cyberavskräckningsteorin inte avgränsas till enbart förnekande och bestraffning.

Slutligen hade studien kunnat genomföras med en förklarande ansats, där Nato-medlemskapet utgör en förklaringsfaktor för att cyberavskräckning skulle se likadan eller annorlunda ut efter ett Nato-medlemskap. En sådan undersökning skulle kunna omfatta en processpåring för att kunna identifiera mekanismen mellan orsak och förväntad effekt.

11. Källförteckning

Aras, H. & Süvari, K. (2025). Unveiling Russia's secret weapon: cyber-electronic operations in hybrid warfare. *Defence studies* 25(3): s.435-450. https://anna-lindh.primo.exlibrisgroup.com/permalink/46LIBRIS_ALB_INST/bohm8h/cdi_proquest_journals_3257977485

Borghard, E.D. & Lonergan, S.W. (2023). Deterrence by denial in cyberspace. *Journal of strategic studies* 46(3): s. 534-569. https://anna-lindh.primo.exlibrisgroup.com/permalink/46LIBRIS_ALB_INST/bohm8h/cdi_crossref_citationtrail_10_1080_01402390_2021_1944856

Essaiasson, P., Gilljam, M., Oscarsson, H., Sundell, A., Towns, A. & Wägnerud, L. (2024). *Metodpraktikan: Konsten att studera människor, organisationer och samhällen*. 6:e uppl. Stockholm: Norstedt Juridik AB.

Fischerkeller, M. Incorporating offensive cyber operations into conventional deterrence strategies. *Routledge London* 59(1): s.103-134. https://anna-lindh.primo.exlibrisgroup.com/permalink/46LIBRIS_ALB_INST/bohm8h/cdi_informaworld_taylorfrancis_310_1080_00396338_2017_1282679

Finlands finansdepartement. (2026). *Budget reviews*. <https://vm.fi/en/the-budget>

Finlands Försvarsmakt. (2024). *Countering cyber threats calls for international cooperation and training*. <https://puolustusvoimat.fi/en/-/countering-cyber-threats-calls-for-international-cooperation-and-training> (Hämtad 2026-04-29)

Finlands Försvarsmakt. (2025). *Finlands och Sveriges cybersäkerhetsförmågor testades i USA:s Cyber Flag-övning*. <https://puolustusvoimat.fi/sv/-/finlands-och-sveriges-cybersakerhetsformagor-testades-i-usa-s-cyber-flag-ovning> (Hämtad 2026-04-29)

Finlands regering. (2013). *Finland's cyber security strategy*. https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/FI_NCSS_2013_en.pdf

Finlands regering. (2019). *Finland's cyber security strategy*. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Finlands regering. (2021). *Government's Defence Report*. <https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/a09bd153-e661-45f6-8be7-5f3724253e14/content>

Finlands regering. (2024). *Finlands cyber security strategy*. <https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/e5575ec3-1ce2-4f0a-aaff-50154789cb6d/content>

Finlands utrikesministerium. (2020). *International law and cyberspace: Finland's national position*. https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727

Harknett, R. & Nye, J.S. Is deterrence possible in cyberspace? *International security* 42(2): s. 196-199. https://anna-lindh.primo.exlibrisgroup.com/permalink/46LIBRIS_ALB_INST/bohm8h/cdi_projectmuse_journals_676860_S1531480417200060

Iasiello, E. (2014). Is cyber deterrence an illusory course of action?. *Journal of strategic security* 7(1): s. 54-67. <https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1337&context=jss>

Johannessen, A., Tufte, P.A. & Christoffersen, L. (2020). *Introduktion till samhällsvetenskaplig metod*. 2:e uppl. Stockholm: Liber AB.

Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. *International Affairs* 92(1): s. 175-195. <https://www.jstor.org/stable/24757841>

Lawson, E. (2017). Deterrence in cyberspace: a Silver Bullet or a Sacred Cow? *Philosophy & technology* 31(3): 431–436. <https://doi-org.proxy.annalindhbiblioteket.se/10.1007/s13347-017-0267-1>

Li, T.Y. (2024). Assymetry in the Digital Age: Cyver Deterrence Strategies for Small States. *Journal of Strategic Security* 17(4). <https://www.jstor.org/stable/48807804>

Lonergan, E.D. & Schneider, J. The power of beliefs in US cyber strategy: The evolving role of deterrence, norms and escalation. *Journal of cybersecurity* 9(1): s. 1-10. https://anna-lindh.primo.exlibrisgroup.com/permalink/46LIBRIS_ALB_INST/bohm8h/cdi_proquest_journals_3168762998

National Audit Office of Finland. (2025). *Conclusions and recommendations 8/2025: State of cybersecurity management in the central government*. <https://vtv.fi/wp-content/uploads/2025/10/NAOF-recommendations-8-2025-State-of-cybersecurity-management-in-the-central-government.pdf>

Nato a. (2022). *Strategic concept*. <https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf> (Hämtad 2026-03-30).

Nato b. (2022). NATO allies and partners participate in large-scale cyber defence exercise. <https://www.nato.int/en/news-and-events/articles/news/2022/04/25/nato-allies-and-partners-participate-in-large-scale-cyber-defence-exercise> (Hämtad 2026-04-29)

- Nato (2024). *Cyber defence*. <https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence> (Hämtad 2026-03-26).
- Nye, J.S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security* 41(3): s. 44-71. <https://www.jstor.org/stable/26777790>
- Pape, R. (2014). *Bombing to win: Air Power and coercion in war*. Cornell University Press.
- Rickli, J-M. (2008). European Small States' Military Policies After The Cold War: From Territorial To Niche Strategies. *Cambridge review of international affairs*. 21(3): s. 307-325. <https://www-tandfonline-com.proxy.annalindhbiblioteket.se/doi/pdf/10.1080/09557570802253435?needAccess=true>
- Ryan, N.J. (2018). Five kinds of cyber deterrence. *Philosophy & technology* 31(3): s. 331-338. <https://link-springer-com.proxy.annalindhbiblioteket.se/content/pdf/10.1007/s13347-016-0251-1.pdf>
- Schelling, T.C. (1960). *The strategy of conflict*. Cambridge, MA: Harvard University Press.
- Sulg, M. & Crandall, M. (2020). Geopolitics: The Seen and Unseen in Small State Foreign Policy. *Journal of regional security*. 15(1): s. 109-130. <https://scindeks-clanci.ceon.rs/data/pdf/2217-995X/2020/2217-995X2001109S.pdf>
- SUPO. (2021). *National security overview*. <https://supo.fi/documents/38197657/39761266/National+Security+Overview+2021.pdf/a772aa98-30bc-1bcc-62c0-9d77dda2733b/National+Security+Overview+2021.pdf?t=1649405324653>
- (Hämtad 2026-03-30)
- SUPO (2025). *Finland must prepare for growth in Russian influencing*. <https://supo.fi/en/-/finland-must-prepare-for-growth-in-russian-influencing> (Hämtad 2026-03-26)
- Traficom (2026). *Finlands cybersäkerhetsår 2025 – hotnivån förblev förhöjd och antalet allvarliga incidenter på en hög nivå*. <https://www.traficom.fi/sv/nyheter/finlands-cybersakerhetsar-2025-hotnivan-forblev-forhojd-och-antalet-allvarliga-incidenter-pa-en-hog-niva> (Hämtad 2026-03-26)
- Tor, U. (2017). Cumulative deterrence as a new Paradigm for cyber deterrence. *Journal of strategic security* 40 (1-2): s. 92-117. <https://www-tandfonline->

com.proxy.annalindbiblioteket.se/doi/pdf/10.1080/01402390.2015.1115975?needAccess=true

Widén, J. & Angstrom, J. (2014). *Contemporary Military Theory : The Dynamics of War*.
Routledge.

Williamsson, M. & Mansoor, P.R. (2012). *Hybrid warfare: Fighting Complex Opponents from the ancient world to the present*. Cambridge University Press.