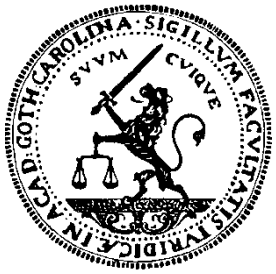

JURIDISKA FAKULTETEN

VID LUNDS UNIVERSITET

Sofie Bokwall

Viktlös folkrätt i cyberrymden?

En kritisk analys av non-interventionsprincipen och ansvarsluckan vid cyberangrepp

LAGF03 Rättsvetenskaplig uppsats

Kandidatuppsats på juristprogrammet

15 högskolepoäng

Handledare: Aurelija Lukoseviciene

Termin: VT26

Innehåll

Summary

In the context of a deteriorating security landscape, cyberattacks have become increasingly frequent in international relations. Because these operations rarely meet the threshold for the use of force under Article 2(4) of the UN Charter, the principle of non-intervention serves as the applicable legal framework. The purpose of this thesis is to describe and critically analyze the applicability of the non-intervention principle to cyberattacks targeting infrastructure. In particular, it examines the prerequisites for establishing state responsibility when such operations are conducted by non-state actors. The study uses a legal dogmatic method combined with a critical perspective, drawing primarily on the jurisprudence of the International Court of Justice, the International Law Commission's Articles on State Responsibility, and the expert doctrine Tallinn Manual 2.0.

The thesis demonstrates that the current framework of international law has significant shortcomings in providing adequate protection to targeted states. The application of the law is impeded by the difficulty of adapting traditional legal criteria to cyberspace. First, the element of coercion poses a major obstacle. While cyberattacks often paralyze vital societal functions, they fall outside the strict legal definition of coercion because they generally lack explicit dictatorial demands. Second, the strict requirement of effective control required for attribution creates an accountability gap when states use private hacker groups. Finally, the thesis concludes that the principle of due diligence fails as an alternative basis for responsibility due to evidentiary challenges regarding state knowledge and territorial control.

The conclusion is that the current legal paradigm, in practice, shields the attacking state rather than protecting the victim state. As long as leading cyber nations maintain strategic silence in their state practice to preserve their offensive freedom of action, the development of legal norms will be impeded. Consequently, the unique nature of cyberspace creates a legal imbalance that the traditional system of international law is ill-equipped to manage.

Sammanfattning

Med hänsyn till det försämrade säkerhetspolitiska läget har cyberangrepp blivit ett allt vanligare inslag i internationella relationer. Eftersom dessa åtgärder sällan uppnår tröskeln för väpnat våld enligt FN-stadgans artikel 2(4) aktualiseras i stället den internationella sedvanerättsliga principen om non-intervention. Syftet med denna uppsats är att redogöra för och kritiskt analysera non-interventionsprincipens tillämplighet på cyberangrepp mot infrastruktur. Särskilt behandlas förutsättningarna för att utkräva statsansvar när operationer utförs av icke-statliga aktörer. Undersökningen genomförs med en rättsdogmatisk metod i kombination med ett kritiskt perspektiv, med huvudsaklig utgångspunkt i Internationella domstolens praxis, International Law Commissions artiklar om statsansvar samt expertdoktrinen Tallinn Manual 2.0.

Uppsatsen visar att den gällande folkrättsliga ramen har betydande brister avseende att erbjuda drabbade stater ett ändamålsenligt skydd. Tillämpningen försvåras av att traditionella rekvisit är svårförenliga med cyberrymden. För det första utgör tvångsrekvisitet ett hinder. Cyberangrepp lamslår ofta samhällsviktiga funktioner men faller utanför den strikta definitionen av tvång, eftersom det saknar uttryckliga diktatoriska krav. För det andra medför det stränga kravet på effektiv kontroll för hänförbarhet en omfattande ansvarslucka när stater utnyttjar privata hackergrupper. Slutligen konstateras att principen om tillbörlig aktsamhet brister som alternativ ansvarsgrund till följd av bevisproblem rörande staters kunskapskrav och territoriella kontroll.

Slutsatsen är att det rådande rättsläget i praktiken skyddar den angripande staten snarare än den drabbade. Så länge tongivande cybernationer i sin statspraxis upprätthåller en strategisk tystnad för att bevara sin egen handlingsfrihet hämmas normutvecklingen. Cyberrymdens unika karaktär skapar alltså en rättslig obalans som det traditionella folkrättsliga systemet har svårt att hantera.

Förkortningar

ARSIWA	Draft Articles on Responsibility of States for Internationally Wrongful Acts
Corfu Channel-målet	*The Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)*
FN	Förenta nationerna
GGE	Group of Governmental Experts (FN)
ICJ	International Court of Justice
ICTY	International Criminal Tribunal for the former Yugoslavia
ILC	International Law Commission
Kongo-målet	*Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*
Nicaragua-målet	*Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*
PCIJ	Permanent Court of International Justice
Tadic-målet	*Prosecutor v. Dusko Tadic*
Tallinn Manual	Tallinn Manual 2.0 on the International Law Applicable to Cyber operations

1 Inledning

1.1 Bakgrund

Nästan varje vecka får jag en push-notis från en nyhetstjänst om att en matbutik, ett universitet, en streamingtjänst eller Sveriges elnät har blivit utsatta för ett cyberangrepp. Lösenord som läckts, information från användarnas profiler som finns att köpa på den svarta marknaden och betalsystem som ligger nere.

Det moderna samhället bygger på en överenskommelse om att den digitala infrastrukturen ska fungera. Vi är idag beroende av uppkopplade system för att allt från elförsörjning och sjukhus ska fungera, till att handla mat och betala våra räkningar. Baksidan av detta är en stor sårbarhet. Cyberrymden har blivit en arena för internationella konflikter, där främmande makter kontinuerligt angriper svenska intressen. Det mesta av detta sker i det dolda, under radarn för allmänheten.[1]

Ett konkret exempel är den omfattande attacken sommaren 2021 då Coop tvingades stänga nästan 800 butiker över hela Sverige efter att deras mjukvaruleverantör hackats.[2] Även Lunds universitet blev utsatta för ett cyberangrepp när universitetets systemleverantör angreps. Då blev personuppgifter om anställda läckta och kunde köpas på internet.[3] Samtidigt rapporterar svenska myndigheter löpande om hur kritisk infrastruktur, som det svenska elnätet, utsätts för avancerade intrångsförsök.[4] Frågans aktualitet är alltså direkt kopplad till dagens geopolitiska spänningar. Den regelbaserade världsordningen är under press, vilket illustreras av såväl kriget i Ukraina som

[1] Myndigheten för civilt försvar, *Cyberangreppens utveckling 2023–2025: Årsrapport cyberincidentrapportering 2025*, mars 2026, s. 3 och 61.

[2] Jenny Toresson, ´It-attacken mot Coop – detta har hänt´, SVT, 5 juli 2021, https://www.svt.se/nyheter/inrikes/it-attacken-mot-coop-detta-har-hant (besökt 2026-04-15).

[3] ´Angående cyberangreppet mot vår systemleverantör Miljödata´, Lunds universitet, 15 september 2025, https://www.medarbetarwebben.lu.se/artikel/angaende-cyberangreppet-mot-var-systemleverantor-miljodata (besökt 2026-04-15).

[4] Svenska Kraftnät, ´Samlad information om dataintrånget´, 30 oktober 2025, https://www.svk.se/sakerhet-och-beredskap/cybersakerhet/samlad-information-om-datain-tranget/ (besökt 2026-04-15).

anfallen mot Iran av Israel och USA, samt en alltmer gränsöverskridande maktutövning av auktoritära stater.[5]

Eftersom de flesta cyberangrepp, även de som får stora konsekvenser, sällan når upp till gränsen för militärt våld, hamnar fokus inte på våldsförbudet i Förenta nationernas (FN) stadga, utan i stället på det internationella sedvanerättsliga förbudet mot otillåten inblandning i andra staters inre angelägenheter (non-interventionsprincipen).[6] Principen innebär att ingen stat har rätt att blanda sig i en annan stats inre eller yttre angelägenheter.[7] Den förbjuder alla former av direkt fysisk intervention på en stats territorium, men även vissa typer av indirekt intervention.[8]

När den här typen av cyberoperationer inträffar väcks frågan om ansvarsskyldighet. Den traditionella folkrätten har historiskt fokuserat på fysiskt våld och terrorhandlingar. Men hur tillämpar man en äldre lagstiftning på moderna problem? Och vem ska stå till svars?

1.2 Syfte och frågeställning

Syftet med uppsatsen är att redogöra för och kritiskt analysera hur non-interventionsprincipen tillämpas på moderna cyberangrepp och vad detta innebär för staters ansvar. Det är tekniskt och juridiskt utmanande att överhuvudtaget kunna binda en attack till en främmande stat. Det är även svårt att dra gränsen för när ett angrepp övergår till att bli en tvångsåtgärd riktad mot en stats suveränitet. Diskussionen befinner sig alltså i en gråzon.

Mot bakgrund av syftet ska följande frågeställningar besvaras:

- Hur kan non-interventionsprincipen appliceras på moderna cyberangrepp?

[5] Sveriges Radio, `Attackerna mot Iran – detta har hänt`, 2 mars 2026, https://www.sverigesradio.se/artikel/attackerna-mot-iran-detta-har-hant (besökt 2026-05-19).

[6] UN General Assembly, Resolution 2625 (XXV), Declaration on Principles of International Law concerning Friendly Relations, UN Doc A/RES/2625(XXV) (24 oktober 1970).

[7] Jfr FN-stadgan art. 2(7).

[8] Nicaragua Judgment, 1986, s. 14, para 205.

- Vilken betydelse har det att utföraren är en privat aktör i förhållande till staters ansvar?

1.3 Avgränsning

Uppsatsen är begränsad till att undersöka gällande internationell sedvanerätt med fokus på cyberangrepp riktade mot infrastruktur. Givet folkrättens omfattning och cyberrymdens problematik kommer uppsatsen materiellt avgränsas till att analysera dessa angrepp i ljuset av non-interventionsprincipen.

Våldsförbudet i artikel 2.4 FN-stadgan kommer således inte att behandlas. Motiveringen till detta är att tröskeln för vad som utgör våldsanvändning inom folkrätten är högt ställd och cyberangrepp mot civil infrastruktur faller regelmässigt under denna gräns. Non-interventionsprincipen utgör därmed en mer relevant ram då den fångar upp de angrepp som befinner sig i en mer svårnavigerad gråzon strax under våldsförbudet.

Slutligen avgränsas uppsatsen till att primärt undersöka cyberangrepp som utförs av icke-statliga aktörer. Det motiveras av den praktiska verkligheten i cyberrymden, där stater sällan öppet tillkännager sin inblandning i cyberangrepp.

1.4 Metod & material

För att uppnå syftet och besvara frågeställningarna tillämpas en rättsdogmatisk metod som, i denna uppsats, syftar till att identifiera, tolka och problematisera gällande rätt.[9] Metoden tar sin utgångspunkt i de vedertagna internationella rättskällorna såsom de kommer till uttryck i artikel 38(1) i Internationella domstolens (ICJ) stadga. Eftersom det inte råder någon formell hierarki mellan folkrättens primära rättskällor tillämpas traktat och internationell sedvanerätt jämsides. Doktrin tillämpas därefter, i enlighet med art 38(1)(d), som ett hjälpmedel för att tolka gällande rätt.[10]

[9] Kleineman i Nääv & Zamboni, *Juridisk Metodlära*, s. 25.
[10] Rose, *An Introduction to Public International Law,* s. 17.

Med hänsyn till att cyberrätt utgör ett relativt nytt och oreglerat rättsområde, där konventionell praxis saknas eller är tvetydig, kommer uppsatsen att i betydande utsträckning ta sin utgångspunkt i internationell doktrin. Särskild tyngdpunkt läggs vid *Tallinn Manual 2.0 on the International Law Applicable to Cyber operations* (Tallinn Manual), vilket utgör den mest auktoritativa tolkningen av hur befintlig folkrätt appliceras i cyberrymden. Tallinn Manual ställer upp 154 regler om cyberrymden och är framtagen av en oberoende internationell expertgrupp som sammankallades av NATO Cooperative Cyber Defence Centre of Excellence. De arbetar nu med att utveckla en tredje och mer uppdaterad version med större fokus på statspraxis.[11] Manualen är auktoritativ som doktrin men måste betraktas som subsidiär till traktat och sedvanerätt. Den får inte ses som en färdig kodifiering eftersom den bygger på experternas logiska deduktioner snarare än på en analys av hur stater faktiskt agerar i cyberrymden.[12]

För att fastställa förutsättningarna för staters ansvar för privata aktörers handlande tillämpas International Law Commissions (ILC) artiklar om statsansvar (ARSIWA), vilka i stor utsträckning anses ge uttryck för gällande sedvanerätt.[13]

Då den moderna folkrättsliga debatten rörande cyberoperationer nästan uteslutande förs på engelska, är merparten av uppsatsens källmaterial författade på engelska. För att undvika syftningsfel och betydelseglidningar har stor noggrannhet iakttagits vid översättningen av engelska begrepp till svenska. I de fall en direkt svensk översättning saknas behålls originalbegreppen kursiverade inom parentes. Alla citat är översatta med försiktighet. Utöver den traditionella rättsdogmatiska metoden anläggs även ett rättskritiskt perspektiv i uppsatsens analyserande delar. Syftet med perspektivet är att utvärdera

[11] CCDCOE, `CCDCOE to host the Tallinn Manual 3.0 process`, 2020, https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/ (besökt 2026-05-14).

[12] Efrony & Shany, `A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice´, s. 654–655; Art 38(1)(d) ICJ-stadga.

[13] International Law Commission, Draft Articles of States for Internationally Wrongful Acts, with commentaries, Yearbook of the International Law Commission, 2001, vil. II, Part Two, s. 48, para. 5.

huruvida gällande rätt är ändamålsenlig för att hantera dagens hotbild och konsekvenser rörande cyberattacker.

1.5 Forskningsläge

Den folkrättsliga regleringen av cyberrymden utgör ett förhållandevis ungt forskningsområde. Eftersom det saknas specifika internationella traktat som reglerar cyberangrepp, har doktrin och expertgrupper kommit att spela en stor roll för rättsbildningen. Navet i den akademiska debatten utgörs av expertdoktrin Tallinn Manual. Forskningen kan i stor utsträckning delas in i två läger: de som menar att de traditionella folkrättsliga principerna är direkt applicerbara på cyberrymden genom analogier och de som framhåller att cyberrymdens unika karaktär skapar regulatoriska luckor där gällande rätt är otillräcklig. Ett centralt bidrag till den kritiska debatten utgörs av Dan Efrony och Yuval Shany som i sin studie ifrågasätter huruvida Tallinn Manual faktiskt återspeglar gällande rätt. De för fram tesen att manualen riskerar att bli en ”regelbok på hyllan” då stater i sin faktiska praxis ofta väljer att ignorera dess slutsatser eller avstå från att karakterisera cyberangrepp som folkrättsbrott. Det är alltså stor skillnad mellan experternas tolkning och staternas faktiska agerande.[14]

Givet uppsatsens avgränsning mot non-interventionsprincipen och icke-statliga aktörer aktualiseras särskilt forskning kring tolkningen av tvångsrekvisitet samt beviskraven för statligt ansvar. Forskare som Harriet Moynihan illustrerar exempelvis ett mer modernt synsätt inom doktrin som ifrågasätter det traditionella uppsåtskravet och argumenterar för att storskaliga effekter av cyberangrepp i sig självt bör kunna konstituera ett otillåtet tvång. Samtidigt pågår en intensiv debatt om huruvida principen om tillbörlig aktsamhet faktiskt har uppnått status som internationell sedvanerätt i cyberkontext.[15]

[14] Efrony & Shany, ´A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice, American Journal of International Law, s. 584–585.

[15] Moynihan, Harriet, `The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention`, s. 28 & 36.

1.6 Disposition

Framställningen är uppdelad i tre kapitel. Det inledande kapitel 1 syftar till att sätta ramarna för uppsatsen genom att presentera bakgrund, syfte och frågeställningar. Därefter redogörs för den rättsdogmatiska metoden, materialet samt det aktuella forskningsläget kring folkrättens tillämpning i cyberrymden.

I kapitel 2 presenteras gällande rätt. Kapitlet utgör uppsatsens deskriptiva grund och behandlar först suveränitetsprincipen som ligger till grund för non-interventionsprincipen. Vidare redogörs för non-interventionsprincipens rekvisit samt de folkrättsliga reglerna för statsansvar och hänförbarhet enligt ARSIWA.

Kapitel 3 utgör uppsatsens analytiska del och här tillämpas den gällande rätten på moderna cyberangrepp. Först problematiseras tvångskravets tillämplighet i en digital kontext och staternas strategiska tystnad. Sedan analyseras den ansvarslucka som uppstår när stater utnyttjar icke-statliga aktörer för att utföra angreppen, varvid beviskraven för effektiv kontroll ställs mot principen om tillbörlig aktsamhet. Slutligen sammanfattas uppsatsens rön i avslutande slutsatser. Här besvaras de inledande frågeställningarna, konsekvenserna av det nuvarande rättsläget lyfts fram och frågan om behovet av ett nytt kompletterande folkrättsligt regelverk adresseras.

2 Non-interventionsprincipen

2.1 Suveränitet

Suveränitetsprincipen är en av folkrättens bärande principer och bygger på staters formella oberoende och jämlikhet. Denna tanke kodifieras i FN-stadgans artikel 2(1), som fastslår att organisationen vilar på alla dess medlemmars suveräna likställdhet. Vilket innebär att varje stat är skyldig att respektera andra staters territoriella integritet och politiska oberoende.

Den klassiska definitionen av suveränitetsprincipen framgår av Island of Palmas-skiljedomen från 1928 som lyder:

> Suveränitet i relation mellan staterna innebär oberoende. Oberoende avseende ett visst territorium innebär rätten att där, med uteslutande av varje annan stat, utöva statliga funktioner.[16]

Domaren i målet fastslog alltså att suveränitet är synonymt med oberoende och att detta oberoende i sin tur innebär en exklusiv rätt för staten att inom ett avgränsat territorium utöva statliga funktioner.

2.1.1 Suveränitet i cyberrymden

I Tallinn Manual har experter på folkrätt och cyberrymden träffats för att bland annat diskutera hur man tillämpar suveränitetsprincipen på cyberaktivitet. Vissa menar att cyberrymden är en sorts ”global domän” som ingen kan ha suveränitet över. Expertgruppen bakom Tallinn Manual håller däremot inte med och slår i sin ”Rule 1” fast att eftersom cyberaktiviteter utförs och får konsekvenser inom staters territorium, av personer som agerar inom detta territorium som staterna har exklusiv suveränitet över, råder suveränitet även i cyberrymden. [17]

Detta konkretiseras i ”Rule 2”, som tydliggör att en stat utövar suverän kontroll över den cyberinfrastruktur och de personer som befinner sig på dess

[16] Island of Palmas Case, s. 838, (egen översättning).
[17] Schmitt, `The Tallinn Manual 2.0`, s. 12–13.

territorium. Expertgruppen bakom manualen framhåller att cyberrymden, trots sin gränsöverskridande natur, i grunden vilar på fysiska komponenter såsom servrar och kablar. Det är den territoriella förankring av infrastrukturen som utgör den folkrättsliga grunden för att hävda statssuveränitet i den digitala miljön.[18]

Det är skillnad på intern och extern suveränitet. Intern suveränitet i cyberrymden innebär att en stat har rätt att fritt vidta åtgärder för att reglera cyberaktivitet inom staten, av såväl privat som offentlig karaktär, så länge det inte strider mot internationell rätt. Staten har alltså jurisdiktion att lagstifta om, verkställa och döma i frågor som rör dess digitala sfär.[19]

Den externa suveräniteten handlar i stället om statens oberoende i dess internationella relationer. Denna princip ger stater frihet att agera i cyberrymden utanför sitt eget territorium och en frihet att utforma sin egen utrikespolitik och ingå internationella avtal.[20] Suveränitetsprincipen är alltså nära sammankopplad med, och utgör grunden för non-interventionsprincipen.

2.1.2 Suveränitet - en bindande norm eller övergripande princip?

Trots en generell konsensus om att suveränitet gäller i cyberrymden, pågår en debatt kring huruvida suveränitetsprincipen utgör en fristående primärregel vars överträdelse i sig utgör ett folkrättsbrott, eller om den endast är en övergripande princip. Denna gränsdragning är avgörande för bedömningen vilket jag återkommer till i avsnitt 3.1.1.

Å ena sidan argumenterar vissa för att suveränitet i sig inte utgör en självständig regel. Enligt detta synsätt fungerar suveräniteten snarare som ett fundament som bär upp andra bindande normer, såsom våldsförbudet och non-interventionsprincipen som behandlas i avsnitt 2.2. Som stöd för detta anförs bland annat den internationella acceptansen för fredstida spionage. Förespråkarna menar att stater historiskt sett har bedrivit spionage på främmande

[18] Schmitt, `The Tallinn Manual 2.0`, s. 12–13.
[19] Ibid, s. 13.
[20] Ibid, s. 16.

territorium utan att detta i sig har ansetts utgöra folkrättsbrott, förutsatt att agerandet inte kränkt ett specifikt förbud. Utifrån den logiken skulle inte heller cyberintrång per automatik utgöra folkrättsbrott enbart i egenskap av att det inkräktar på en annan stats cyberinfrastruktur.[21]

Å andra sidan kritiseras detta synsätt av andra folkrättsexperter, däribland Michael N. Schmitt och Liis Vihul, vilka i likhet med gruppen bakom Tallinn Manual argumenterar för att territoriell suveränitet utgör en stark primärregel. Enligt detta är förpliktelsen att respektera andra staters territoriella okränkbarhet direkt bindande. Schmitt och Vihul påtalar att förekomsten av folkrättsliga undantag, såsom rätten till oskadlig genomfart i sjörätten, inte motbevisar existensen av en suveränitetsregel. Tvärtom bekräftar sådana undantag att huvudregeln är att det territoriella oberoendet är okränkbart. Även staters tysta acceptans av spionage förstås enligt detta synsätt bäst som ett potentiellt sedvanerättsligt undantag, snarare än ett bevis för att suveräniteten i allmänhet skulle sakna bindande verkan.[22]

Den senare uppfattningen finner även stöd i ICJ:s praxis. I både *The Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)* (Corfu Channel-målet) och *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (Nicaragua-målet) har domstolen uttryckligen behandlat kränkningar av den territoriella suveräniteten som självständiga folkrättsbrott, separat bedömda från frågor rörande exempelvis våldsförbudet.[23]

2.2 Brott mot non-interventionsprincipen

Non-interventionsprincipen utgör en fundamental hörnsten i folkrätten. Dess status som internationell sedvanerätt bekräftas i rättspraxis och bland folkrättsexperter som även understryker principens nära koppling till suveränitetsprincipen. Trots att olaglig intervention inte uttryckligen finns som ett självständigt förbud i FN-stadgan, betraktas den som en nödvändig

[21] Schmitt & Vihul, `Respect for soverignity in cyberspace`, s. 1641–1643.
[22] Ibid, s. 1645.
[23] Corfu Channel Judgment, 1949, s. 35; Nicaragua Judgment, 1986, para 202.

konsekvens av staters suveräna jämlikhet enligt FN-stadgans art. 2(1). Principens status som internationell sedvanerätt fastställdes av ICJ i Nicaragua-målet. Domstolen slog där fast att det krävs två kumulativa rekvisit för att en handling ska anses strida mot non-interventionsprincipen; dels måste inblandningen rikta sig mot en annan stats *domainé réservé*, dels måste den innefatta ett inslag av tvång. Principen förbjuder alltså stater från att direkt eller indirekt ingripa i en annan stats inre eller yttre angelägenheter genom åtgärder som innefattar ett inslag av tvång.[24]

För att undersöka om non-interventionsprincipen i praktiken kan appliceras på cyberangrepp, kommer respektive rekvisit som fastställdes i Nicaragua-målet att undersökas nedan.

2.2.1 Domaine réservé

Det första kumulativa rekvisitet för att ett brott mot non-interventionsprincipen ska ha skett är att interventionen skett inom en stats *domaine réservé*.

En stats *domaine réservé* avser de rättsliga områden och samhällsfunktioner där staten, i kraft av sin suveränitet, har exklusiv rätt att fatta beslut helt fritt från yttre inblandning. De handlar om de områden som inte är reglerade av internationella förpliktelser. Det är alltså inom en stats *domaine réservé* som andra stater inte får intervenera, där har staten helt exklusiv behörighet.[25] Exempel på sådana områden är valet av ekonomiska, politiska och sociala system och hur en stat förbinder sig internationellt.[26]

I en digital kontext innebär det att ett cyberangrepp måste inkräkta på just någon av dessa funktioner vilka inte är helt lätta att fastställa. Enligt experterna är en stats *domaine réservé* helt beroende på hur staten agerar och vad som är *opinio juris*. Omfattning kan även ändras över tid. Detta beror på vilka nya traktat och internationella förbindelser staten ingår. I takt med att stater

[24] Nicaragua Judgment 1986, para 202; Schmitt, `Tallinn Manual 2.0`, s. 312.

[25] Ziegler, Katja S., ´Domaine Réservé´, para 1, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1398#:~:text=1%20The%20notion%20of%20domaine,see%20also%20Jurisdiction%20of%20States (besökt 2026-04-29).

[26] Nicaragua Judgment, 1986, s. 14, para 205.

ingår dessa krymper alltså området där de har helt exklusiv beslutanderätt. Om en stat har åtagit sig förpliktelser rörande exempelvis digital handel eller mänskliga rättigheter på nätet, lyfts dessa frågor ur behörigheten. En yttre inblandning i dessa processer ska då i stället prövas mot de specifika avtalen snarare än non-interventionsprincipen.[27]

Enligt expertgruppens kommentarer till ”Rule 66” förbjuder regeln statliga cyberoperationer som innefattar tvång och som syftar till att begränsa en annan stats exklusiva befogenheter inom dessa områden. En viktig slutsats de drar av detta är att det skyddade området enligt non-interventionsprincipen i stor utsträckning sammanfaller med de rättigheter som tillkommer stater enligt suveränitetsprincipen. I en cyberkontext innebär detta att en stats *domaine réservé* inte bara omfattar de fysiska institutionerna, utan även de digitala processer och den infrastruktur som krävs för att staten ska kunna utöva sin suveränitet. En cyberoperation som medelst tvång stör exempelvis ett valsystem eller en centralbanks digitala funktioner träffar således direkt kärnan av statens exklusiva nationella kompetens.[28]

2.2.2 Tvångskravet

Det andra kumulativa rekvisitet för att en handling ska utgöra en folkrättsstridig intervention är att inblandningen sker med tvång. Som ICJ uttryckte det i Nicaragua-målet är tvånget själva kärnan som definierar en förbjuden intervention. Tvång föreligger när en stat genom påtryckningar avser att tvinga fram ett agerande, eller en underlåtenhet att agera, från en annan stat inom ramen för dess *domaine réservé*. Handlingen måste ha en karaktär som berövar den andra staten dess fria vilja att besluta inom sin exklusiva kompetens.[29]

Tröskeln för tvång kan uppnås på flera olika sätt och kräver inte nödvändigtvis ett uttalat syfte att störta en utländsk regering, som var fallet i Nicaragua-målet.[30] Detta klargjordes av ICJ i målet *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo c. Uganda 2005)* (Kongo-

[27] Ziegler, Katja S., ´Domaine Réservé´, para 2.
[28] Schmitt, `The Tallinn Manual 2.0`, s. 314.
[29] Nicaragua Judgment, 1986, s. 14, para 205.
[30] Ibid.

målet). Domstolen framhöll att åtgärder som innebär att en stat utövar kontroll över eller lamslår centrala funktioner inom en stats territorium, även om de motiveras av egna säkerhetsbehov, kan utgöra tvingande och därmed ett otillåtet ingrepp i statens inre angelägenheter.[31]

Även om militärt våld är den mest uppenbara formen av tvång är det alltså tydligt att likaså andra former är förbjudna. Staters agerande i modern tid erbjuder åtskilliga exempel på sådana icke-militära tvångsmetoder, såsom allvarliga ekonomiska och finansiella påtryckningar i syfte att framtvinga politiska beslut. Samtidigt måste tvång särskiljas från politisk påverkan. Att en stat utnyttjar ovänliga diplomatiska eller politiska positioner gentemot en annan stat utgör i sig självt inte ett folkrättsstridigt tvång.[32]

Utgångspunkten är alltså att rent ekonomiska åtgärder generellt sett inte utgör en folkrättsstridig intervention. Stater har rätt att fritt välja sina handelspartners, en princip som i cyberrymden innebär att en stat exempelvis har rätt att neka en annan stat tillgång till servrar och e-handel inom det egna territoriet. Däremot framhålls en avgörande skillnad vid tillämpningen på cyberrymden. Till skillnad från klassiska ekonomiska sanktioner, som ofta utgörs av passivitet genom att en stat avstår handel, utgör cyberåtgärder aktiva tekniska åtgärder. Även om syftet primärt är ekonomiskt, kan sådana aktiva cyberoperationer kvalificeras som en otillåten intervention förutsatt att den uppnår tvångskriteriet. Expertgruppen bakom Tallinn Manual understryker dock att uppsåt utgör en nödvändig beståndsdel, vilket innebär att det utöver den tvingande effekten måste finnas ett uttryckligt syfte att tvinga målstaten att agera i en angelägenhet som ligger inom dess suveränitet. Om exempelvis en cyberkriminell grupp utför ett cyberangrepp med ett renodlat ekonomiskt uppsåt, brister agerandet i kravet på ett uppsåt att *de jure* styra målstatens inre angelägenheter.[33]

[31] Congo Judgment, 2005, s. 227, para 163–164.
[32] Marcelo Kohen, ´The Principle of Non-Intervention 25 Years after the Nicaragua Judgment´, s. 161.
[33] Schmitt, `The Tallinn Manual 2.0`, s. 324.

I doktrin görs en distinktion mellan legitim påverkan och folkrättsstridigt tvång. Denna gränsdragning har sin grund i den klassiska definitionen av intervention som formulerades av L.F.L Oppenheim:

> (…) inblandningen måste innefatta våldsanvändning, vara diktatorisk eller på annat sätt tvingande, och i praktiken beröva den stat som inblandningen riktas mot, kontrollen över den aktuella angelägenheten. Enbart inblandning utgör inte en intervention.[34]

En olaglig cyberintervention förutsätter alltså en inblandning av diktatorisk eller annan tvingande karaktär. Det räcker således inte att en stat försöker övertala eller påverka en annan stats beslut. Inblandningen måste vara så pass tvingande att den i praktiken berövar staten dess fria vilja och kontroll över situationen. Detta bekräftas i Nicaragua-målet.[35]

Som även framgår av ICJ:s resonemang i Kongo-målet ligger fokus på handlingens tvingande verkan snarare än på angriparens slutgiltiga politiska mål.[36] Att använda digitala medel för att lamslå en stats kritiska infrastruktur i syfte att framtvinga politiska eftergifter är ett tydligt exempel på en sådan diktatorisk inblandning som berövar staten kontrollen över dess egna angelägenheter.[37]

Ett centralt problem vid bedömningen av tvångsrekvisitet i cyberrymden är att digitala attacker sällan åtföljs av uttryckliga krav eller ultimatum. I en analys från *Chatham House* belyser Harriet Moynihan utmaningen. Eftersom stater sällan uttrycker sina avsikter vid cyberoperationer riskerar gränsen mellan otillåtet tvång och accepterad digital påverkan att suddas ut. Frågan blir därför hur det överhuvudtaget går att bevisa att en stat har utsatts för ett diktatoriskt tvång, när angreppet uteslutande sker genom kod och ofta utan explicita hot.[38]

---

[34] Sir Robert Jennings & Sir Arthur Watts (red.), `Oppenheim´s International Law`, s 432 (egen översättning).

[35] Nicaragua Judgment, 1986, s. 14, para. 205.

[36] Congo Judgment, 2005, s. 227, para 163–165.

[37] Schmitt, `The Tallinn Manual 2.0`, s. 312 ff & 315.

[38] Moynihan, Harriet, `The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention, s. 28 & 36.

För att förebygga detta bevisproblem kan man föra argument för att cyberoperationens skala och allvarlighetsgrad i kombination med måltavlans karaktär, kan fungera som omständigheter som visar på att tvång föreligger. Enligt detta synsätt kan själva effekten av en omfattande cyberattack ersätta kravet på ett uttalat tvång. Om en cyberoperation exempelvis lamslår en stats nationella infrastruktur, såsom fallet var vid NotPetya-attacken mot Ukraina[39], kan attackens massiva påverkan i sig utgöra ett sådant intensivt tryck att det berövar målstaten dess fria handlingsutrymme. Attackens omfattning blir därmed själva bäraren av den diktatoriska karaktären, vilket möjliggör att även cyberangrepp utan ett uttalat tvång kan klassificeras som folkrättsstridiga interventioner, förutsatt att de träffar statens *domaine réservé*.[40]

2.2.3 Hänförbarhet

För att en stat ska kunna hållas internationellt ansvarig för en operation som bryter mot non-interventionsprincipen krävs det att handlingen kan tillskrivas staten. Reglerna för detta återfinns i ARSIWA.[41]

Huvudregeln i ARSIWA art. 4 föreskriver att en stats statsorgan agerar på en stats vägnar och att dess handlingar därför ska tillskrivas den staten. I en cyberkontext bekräftas denna princip av expertgruppen bakom Tallinn Manual, som i sin ”Rule 15” slår fast att cyberoperationer utförda av exempelvis en stats militär direkt kan hänföras till staten. I dessa fall är ansvarsbedömningen inte särskilt komplicerad. Utmaningen, och det som gör cyberrymden snårig, uppstår när operationer genomförs av privata aktörer eller oberoende hackergrupper.[42]

Enligt ARSIWA art. 8 kan en sådan icke-statlig aktörs handlingar hänföras till en stat endast om personen eller gruppen agerar på instruktion av, under ledning av eller under kontroll av den staten. Motsvarande regel för

[39] SVT Nyheter, `Massiv nätattack mot banker och storföretag, 27 juni 2017, https://www.svt.se/nyheter/utrikes/massiv-natattack-mot-banker-och-storforetag (besökt 2026-05-11).

[40] Moynihan, Harriet, `The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention`, s. 36.

[41] UN General Assembly, Responsibility of States for Internationally Wrongful Acts, 28 januari 2002, A/RES/56/83.

[42] Schmitt, `The Tallinn Manual 2.0`, s. 87.

cyberrymden finns i Tallinn Manual där expertgruppen konstaterar att ARSIWA art. 8 kan tillämpas på cyberoperationer utförda av privata aktörer så länge staten har den kontroll som krävs.[43] Att i praktiken kunna bevisa att sådan kontroll föreligger är inte helt okomplicerat. Det är en hög tröskel att nå upp till för att en stat ska anses ansvariga för en privat aktörs handlingar. Huvudregeln är nämligen att en stat inte bär det ansvaret, förutom i specifika fall när aktören och staten har en konkret sammankoppling.[44]

För att kunna tillämpa ARSIWA art. 8 och hålla en stat ansvarig för en cyberoperation utförd av en icke-statlig aktör, måste graden av statlig inblandning alltså fastställas. Internationell praxis uppvisar dock en konflikt gällande vilket beviskrav som ska tillämpas för att ”på instruktion av, under ledning av eller under kontroll av” ska anses föreligga. Den traditionella och mest auktoritativa måttstocken formulerades av ICJ i Nicaragua-målet. Domstolen slog fast att det krävs effektiv kontroll över de specifika operationerna under vilka angreppen begicks för att agerandet ska kunna tillskrivas staten.[45] ILC:s kommentarer till ARSIWA art. 8 stöder denna tolkning och betonar att det inte räcker med allmänt stöd eller finansiering. Staten måste ha dirigerat eller kontrollerat den specifika operationen. [46]

Som en reaktion på den höga tröskeln formulerade Appellationskammaren vid International Criminal Tribunal for the former Yugoslavia (ICTY) i *Prosecutor v. Dusko Tadic* (Tadic-målet) ett alternativ till effektiv kontrolltestet, nämligen övergripande kontroll. Domstolen menade att det för hänförbarhet till en stat av en organiserad väpnad grupps handlingar inte var nödvändigt att kräva effektiv kontroll över varje enskild operation. I stället räckte

[43] Schmitt, `The Tallinn Manual 2.0`, s. 95.

[44] International Law Commission, Draft Articles of States for Internationally Wrongful Acts, with commentaries, Yearbook of the International Law Commission, 2001, vol. II, Part Two.

[45] Nicaragua Judgment, 1986, para 115.

[46] International Law Commission, Draft Articles of States for Internationally Wrongful Acts, with commentaries, Yearbook of the International Law Commission, 2001, vol. II, Part Two, s. 47, para. 3.

det med att staten utövade en generell kontroll över gruppen, vilket inkluderade deltagande i planering och övervakning.[47]

Det ska dock noteras att ILC i sina kommentarer till ARSIWA gör klart att Tadic-målets lägre beviskrav inte rubbar Nicaragua-målets position som gällande rätt för just tillskrivande av statsansvar. Tadic-målet behandlar enskilda individers straffansvar medan Nicaragua-målet rör staters ansvar.[48] Även expertgruppen bakom Tallinn Manual landade i att det är just ICJ:s stränga krav på effektiv kontroll som gäller även i cyberrymden.[49]

Vid en applicering på cyberrymden medför dock effektiv kontroll-testet en betydande utmaning bevisrättsligt. Gruppen bakom Tallinn Manual tydliggör i sina kommentarer att det inte räcker att en stat förser digitala sårbarheter åt en hackergrupp eller ens ger gruppen specifik skadlig kod. För att en cyberoperation ska kunna hänföras till staten måste det kunna bevisas att staten har instruerat eller utövat detaljerad kontroll. Eftersom stater ofta utnyttjar privata aktörer just för att uppnå trovärdig förnekbarhet (*plausible deniability*) är detta ett beviskrav som den angripna staten i praktiken sällan kan uppfylla.[50]

Detta stränga beviskrav skapar en omfattande ansvarslucka. Cyberoperationer med stora effekter kan regelmässigt falla under tröskeln för hänförbarhet. Det innebär att målstaten står utan traditionella folkrättsliga motåtgärder gentemot den stat som i bakgrunden stöttar angriparna. Konsekvensen blir att den internationella sedvanerätten riskerar att framstå som otillräcklig för att hantera den digitala hotbilden. Detta väcker i sin tur en befogad fråga om huruvida folkrätten är i direkt behov av en normutveckling, exempelvis genom en sänkt bevisbörda vid just sådana här cyberkonflikter, för att effektivt kunna värna staters suveränitet.

[47] Prosecutor v. Dusko Tadic, ICTY,1999, para. 117 och 145.

[48] International Law Commission, Draft Articles of States for Internationally Wrongful Acts, with commentaries, Yearbook of the International Law Commission, 2001, vil. II, Part Two, s. 48, para. 5.

[49] Schmitt, The Tallinn Manual, s. 95.

[50] Ibid.

2.3 Passivitet & principen om tillbörlig aktsamhet

Som konstaterat ovan uppställer det traditionella folkrättsliga regelverket höga trösklar för att ett cyberangrepp utförd av en privat aktör ska kunna hänföras till en stat. I de fall en träffad stat kan spåra en attack till servrar belägna i andra staters territorium, men saknar bevis för att den staten har kontrollerat eller instruerat hackarna, uppstår en ansvarslucka. Det är här principen om tillbörlig aktsamhet aktualiseras. Här prövas alltså inte huruvida staten är ansvarig för själva cyberangreppet, utan snarare om staten är ansvarig för sin underlåtenhet att förhindra att dess territorium används för att skada en annan stat. Principen om tillbörlig aktsamhet inom folkrätten härrör från statens territoriella suveränitet. I Corfu Channel-målet fastslog ICJ att varje stat har en skyldighet att inte medvetet låta sitt territorium användas för handlingar som strider mot andra staters rättigheter och suveränitet.[51]

I en cyberkontext har gruppen bakom Tallinn Manual kodifierat denna princip i ”Rule 6”. Enligt denna regel är en stat skyldig att utöva tillbörlig aktsamhet för att säkerställa att cyberinfrastruktur belägen på dess territorium inte används för att utföra cyberoperationer som allvarligt skadar andra stater. Principen är en handlingsplikt snarare än en resultatplikt. Staten måste alltså vidta rimliga åtgärder, men garanterar inte att utnyttjande av cyberinfrastrukturen inte kommer att ske.[52]

I Corfu Channel-målet ställer ICJ upp ett krav på att staten faktiskt måste ha känt till, eller i varje fall borde ha känt till aktiviteten, för att anses ha brustit i sin aktsamhet.[53] Det är däremot betydligt enklare att exempelvis bevisa att en stat kände till att minor placerades ut i deras territorialvatten än att en stat känner till vad som sker på servrar som finns inom deras territorium. Det finns alltså två problem med tillämpningen av tillbörlig aktsamhet på cyberangrepp: dels att principen blir verkningslös på grund av ett för högt beviskrav,

[51] Corfu Channel Judgment, 1949, s. 22.
[52] Schmitt, `The Tallinn Manual 2.0`, s. 30.
[53] Corfu Channel Judgment, 1949, s. 22.

dels att om man sänker kravet kan det bli ett orimligt högt ställt krav som riskerar att kränka den personliga integriteten.

Frågan om huruvida tillbörlig aktsamhet applicerad på cyberrymden utgör bindande sedvanerätt (*lex lata*) eller enbart en rekommenderad handlingsnorm (*lex ferenda*) är omdebatterad.[54] Å ena sidan gör expertgruppen bakom Tallinn Manual gällande att principen är fullt bindande även i den digitala sfären. I sin formulering av ”Rule 6” används ordet ”*must*”, vilket speglar deras bedömning att tillbörlig aktsamhet utgör *lex lata*, med direkt koppling till suveränitetsprincipen.[55] Å andra sidan visar praxis en annan hållning. I FN:s Group of Governmental Experts (GGE) rapport från 2015, som utgör en politisk överenskommelse mellan ledande cybernationer, används i stället ordet ”*should*” gällande staters ansvar att inte låta sitt territorium användas för cyberoperationer. GGE-rapporten klassificerar uttryckligen dessa riktlinjer som frivilliga och icke-bindande normer. Detta indikerar starkt att staterna betraktar tillbörlig aktsamhet i cyberrymden som ett önskvärt beteende snarare än en plikt.[56]

För att nyansera den bilden argumenterar andra folkrättsexperter för att debatten har blivit för låst vid just den här uppdelningen. De menar att fokus i stället bör ligga på substansen och att stater, oavsett bristen på konsensus kring en specifik cyberregel, redan är bundna av ett lapptäcke av befintliga folkrättsliga skyldigheter som gäller per automatik. Detta aktsamhetskrav beskrivs som en flexibel uppförandeplikt som helt beror på statens faktiska kapacitet och resurser i den enskilda situationen. Folkrätten kräver alltså inte det omöjliga, vilket även stämmer överens med gruppen bakom Tallinn Manual som avvisar att gällande rätt skulle kräva en generell och kontinuerlig övervakning av staters nätverk.[57]

[54] Coco & de Souza Dias, `Cyber Due Diligence: A Patchwork of Protective Obligations in International Law`, s. 772–773.

[55] Schmitt, `The Tallinn Manual 2.0`, s. 31.

[56] UN General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 juli 2015, para 13(c) och 13(e).

[57] Coco & de Souza Dias, `Cyber Due Diligence: A Patchwork of Protective Obligations in International Law`, s. 772 ff.

Vid fastställandet av gällande rätt i enlighet med källhierarkin i art. 38(1) ICJ-stadgan väger GGE-rapporten tyngre eftersom den utgör en stark indikator på staternas gemensamma rättsövertygelse. Då Tallinn Manual i strikt folkrättslig mening utgör doktrin, och därmed endast ett subsidiärt hjälpmedel enligt art. 38(1)(d), kan inte den på egen hand etablera bindande sedvanerätt.[58]

[58] UN General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 juli 2015, para 13(c) och 13(e).

3 Analys och slutsats

3.1 Hur kan non-interventionsprincipen tillämpas på cyberangrepp i praktiken?

En grundläggande förutsättning för att överhuvudtaget kunna applicera non-interventionsprincipen på cyberangrepp är fastställandet av suveränitetsprincipens folkrättsliga status. Utifrån den utredda doktrin och internationella praxisen framstår det som nödvändigt att betrakta suveräniteten i cyberrymden som en självständig primärregel och inte endast som en övergripande princip, en skillnad som är av fundamental betydelse. Om man i stället skulle följa den linje som flera tongivande stater förespråkar, att suveränitet i cyberrymden saknar bindande verkan som egen regel, existerar nämligen inget generellt förbud mot digitala intrång. I ett sådant scenario utgör non-interventionsprincipen i praktiken det enda folkrättsliga skyddsnätet under tröskeln för väpnat våld enligt våldsförbudet. Denna insikt gör att det är helt avgörande att granska hur väl principens rekvisit faktiskt fungerar i cyberrymden.

När principernas teoretiska karaktär överförs till den praktiska tillämpningen uppstår flera hinder. Särskilt problematiskt är tolkningen av tvångsrekvisitet. I en traditionell kontext är tvång förknippat med diktatoriska ultimatum som fråntar staten dess fria vilja. Cyberoperationer utformas däremot specifikt för att störa och förvirra en annan stat. Eftersom cyberangrepp sällan inbegriper uttryckliga politiska krav, faller de flesta under tröskeln för vad folkrätten strikt definierar som tvång. Det uppstår då en obalans mellan en handlings faktiska skadeverkan och dess rättsliga klassificering. Detta blir särskilt påtagligt när rätten appliceras på storskaliga angrepp. Om en främmande aktör exempelvis lamslår en stor del av den svenska matförsörjningen i utpressningssyfte, är effekterna ur ett samhällsperspektiv katastrofala. Ändå riskerar agerandet att undslippa klassificeringen som en otillåten intervention, enbart på grund av att det diktatoriska uppsåtet att styra statens inre angelägenheter saknas. Om rättsordningen inte kan skydda statens mest vitala funktioner mot lamslagning, måste non-interventionsprincipens praktiska relevans starkt ifrågasättas.

I ljuset av denna otillräcklighet krävs ett ifrågasättande av den doktrin gruppen bakom Tallinn Manual förespråkar. Gruppen vidhåller det traditionella kravet på ett uttryckligt tvingande uppsåt. Som framhållits i utredningen utgör dock manualen endast doktrin och kan inte på egen hand etablera bindande sedvanerätt. Ett alternativ till det traditionella kravet är att i stället låta angreppets skala och allvarlighetsgrad utgöra indikatorer på att tvång föreligger. Det framstår mer ändamålsenligt att låta effekten av attacken vara bärare av den diktatoriska karaktären. En övergång till ett effektbaserat synsätt är dock inte en okomplicerad lösning, eftersom en sådan sänkning av tröskeln gör det svårt att skilja mellan en otillåten intervention och accepterat cyberspionage.

Dagens statspraxis präglas dock av en strategisk tystnad, vilket hämmar framväxten av ny sedvanerätt och lämnar ansvarsluckan öppen. Denna passivitet bottnar sällan i en genuin rättslig osäkerhet, utan snarare i en säkerhetspolitisk strategi. Stormakter med stora välutvecklade cyberförmågor, såsom USA, Ryssland och Kina, har ett starkt egenintresse av att upprätthålla en tvetydighet. Genom att avstå från att tydligt definiera vad som utgör en otillåten intervention i cyberrymden, undviker de att skapa ny sedvana och att binda sina egna händer gällande framtida cyberangrepp. Denna ovilja från världssamfundets starkaste aktörer att forma bindande normer gör att bland annat Tallinn Manual-gruppens slutsatser isoleras från den faktiska statspraxisen.

3.2 Vilken betydelse har det att utföraren är en privat aktör i förhållande till staters ansvar?

Den andra centrala utmaningen med att tillämpa non-interventionsprincipen på modern cyberkrigföring rör själva aktören. Dess anonyma natur gör det i praktiken mycket fördelaktigt för stater att anlita eller tolerera privata hackergrupper. Det är troligtvis inte en slumpmässig utveckling, utan ett medvetet utnyttjande av den traditionella folkrättens utformning och de högt ställda beviskraven för statsansvar.

Grundproblemet ligger i hänförbarheten. Enligt ARSIWA art. 8 och ICJ:s praxis i Nicaragua-målet krävs effektiv kontroll över den specifika operationen för att en icke-statlig aktörs handlingar ska kunna tillskrivas en stat. I

en digital miljö blir detta krav på detaljstyrning nästintill oöverstigligt för den angripna staten att bevisa. Tadic-målets lägre krav på övergripande kontroll framstår verkligen som mer ändamålsenliga i en cyberkontext. Det lägre kravet ska däremot ställas mot risken att ett sådant sänkt beviskrav riskerar att urholka statssuveräniteten eftersom stater då kan hållas ansvariga för privata aktörers agerande utifrån diffusa kopplingar. Ett krav som kan bli för högt att ställa på stater och som riskerar att bli oproportionerligt.

När beviskraven för hänförbarhet brister vänds blicken i stället mot principen om tillbörlig aktsamhet som en potentiell subsidiär ansvarsgrund. Om en stat inte kan fällas för själva angreppet, aktualiseras frågan om staten kan ställas till svars för sin passivitet, alltså underlåtenheten att förhindra att dess cyberinfrastruktur används för att skada en annan stat. Här uppstår dock en direkt krock med non-interventionsprincipens rekvisit. Även om det objektivt kan fastställas att en stat har brustit i sin aktsamhetsplikt, är en sådan passivitet inte av diktatorisk natur. En underlåtenhet att agera kan vara folkrättsligt klandervärt, men den saknar det element av aktivt tvång som utgör förutsättningen för en otillåten intervention. Den angripna staten går således miste om principens skydd även via denna alternativa ansvarsväg.

Vidare kompliceras principen om tillbörlig aktsamhet av det kunskapskrav som formulerades i Corfu Channel-målet. För att en stat ska anses ha brustit i sin aktsamhet krävs att den faktiskt kände till, eller i vart fall borde ha känt till, aktiviteten. Ett strikt tillämpande i cyberrymden skulle innebära att stater förväntas ha en hög grad av kontroll över den datatrafik som passerar deras servrar. Ett argument emot detta är att en sådan massövervakning står i direkt konflikt med rätten till personlig integritet. Detta tåls dock att problematiseras. Idag finns det regleringar, både nationella och internationella, där stater redan ålagt sig själva och privata aktörer skyldigheter att övervaka, lagra och säkerhetspröva digital infrastruktur. Att stater därmed skulle sakna teknisk eller juridisk kapacitet att upprätthålla en viss grad av kontroll över sitt territorium klingar därför delvis falskt. Svårigheten ligger snarare i folkrättens trubbighet: hur ska en gräns dras mellan den legitima proportionerliga

övervakningen som krävs för att upprätthålla tillbörlig aktsamhet och den oproportionerliga massövervakningen som kränker den personliga integriteten?

Detta kompliceras ytterligare av att en aktör kan befinna sig fysiskt inom en stats territorium, men välja att slussa och dölja sin aktivitet genom servrar belägna i en helt annan stat. Att kräva att en stat ska kunna upptäcka och avvärja avancerade operationer som endast ”studsar” mot dess servrar, men som styrs utifrån, kan bli ett för högt ställt krav.

3.3 Slutsats

Denna uppsats visar att non-interventionsprincipen, i sin nuvarande utformning, brister i att erbjuda ett ändamålsenligt skydd mot cyberangrepp riktade mot stater. Principen är därmed närmast omöjlig att applicera på moderna cyberangrepp. Problematiken grundar sig inte i en isolerad regel, utan i den kumulativa effekten av hur sedvanerätten tillämpar traditionella rekvisit på moderna hot. Dels saknar cyberangrepp oftast det uttryckliga tvång som principen förutsätter, dels gör kravet på effektiv kontroll det nästintill omöjligt att fälla en stat när angreppet utförs av icke-statliga aktörer.

Konsekvensen av detta är att stater idag kan utnyttja fristående hackergrupper för fientliga operationer. Den traditionella folkrätten har i detta avseende blivit en formell sköld för den stat som orkestrerar angreppet, i stället för ett skydd för den stat som drabbas. För att folkrätten på detta område inte ska reduceras till bara en teoretisk konstruktion krävs en utveckling där cyberangreppets skala och effekter tillåts utgöra bärare av tvångskravet. Initiativ som Tallinn Manual har visserligen stakat ut en väg framåt, men folkrätten skapas i slutändan av stater, inte av experter. Så länge staterna, drivna av strategiska intressen, förhåller sig passiva och inte genom konsekvent statspraxis och *opinio juris* anammar dessa tolkningar, förblir expertinitiativen verkningslösa och cyberrymden fortsätter att utgöra en frizon för angrepp.

Källförteckning

Litteratur

Coco, Antonio & de Souza Dias, Talita, `Cyber Due Diligence: A Patchwork of Protective Obligations in International Law´, *The European Journal of International Law*, vol. 32, nr. 3, 2021, s. 771–805.

Efrony, Dan & Shany, Yuval, ´A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice, *American Journal of International Law*, vol. 112, nr 4, 2018, s. 583–657.

Jennings, Robert & Watts, Arthur (red.), *Oppenheim´s International Law*, Volume 1: Peace, 9:e uppl., Longman, London, 1992.

Kleineman, Jan (2025), `Rättsdogmatisk metod`, i: Nääv, Maria & Zamboni, Mauro (red.), *Juridisk Metodlära*, 3:e uppl., Studentlitteratur, Lund, 2025.

Kohen, Marcelo, `The Principle of Non-intervention 25 Years after the Nicaragua Judgment`, *Leiden Journal of International Law*, vol 25, nr. 1, 2012, s. 157–164.

Moynihan, Harriet, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, Chatham House, 2019.

Rose, Cecily (red.), *An Introduction to Public International Law*, Cambridge University Press, Cambridge, 2021.

Sandgren, Claes, *Rättsvetenskap för uppsatsförfattare*, 6:e uppl., Norstedts Juridik, Stockholm, 2025.

Schmitt, Michael N. (red.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence,* 2:a uppl., Cambridge University Press, Cambridge, 2017.

Schmitt, Michael N. & Vihul, Liis, `Sovereignty in Cyberspace: Lex Lata Vel Non?, *The Amercan Journal of International Law Unbound,* vol. 111, 2017, s. 213–218.

Internationella dokument

Förenta Nationernas stadga (antagen 26 juni 1945, ikraftträdande 24 oktober 1945)

International Law Commission, `Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries`, *Yearbook of the International Law Commission*, vol. II, part two, UN Doc. A/56/10, 2001.

Stadga för Internationella domstolen (antagen 26 juni 1945)

UNGA, `Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security`, UN Doc A/70/174, 22 juli 2015.

UNGA, Res 2625 (XXV), `Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations`, UN Doc A/RES/2625(XXV), 24 oktober 1970.

Rättsfall

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), dom den 19 december 2005, *ICJ Reports*. [Cit. Congo Judgment, 2005.]

Corfu Channel (United Kingdom v. Albania), dom den 9 april 1949, *ICJ Reports*. [Cit. Corfu Channel Judgment, 1949.]

Island of Palmas case (Netherlands, USA), 4 april 1928, Reports of International Arbitral Awards (RIAA), vol. II. [Cit. Island of Palmas case]

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), dom den 27 juni 1986, *ICJ Reports*. [Cit. Nicaragua Judgment, 1986.]

Prosecutor v. Tadic, ICTY (Appeals Chamber), Case No. IT-94-1, dom den 15 juli 1999. [Cit. Prosecutor v. Dusko Tadic, ICTY, 1999.]

Övrigt

CCDCOE, `CCDCOE to host the Tallinn Manual 3.0 process`, *CCDCOE*, 2020, https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/ (besökt 2026-05-14)

Lunds universitet, `Angående cyberangreppet mot vår systemleverantör Miljödata`, *Medarbetarwebben*, 15 september 2025, https://www.medarbetarwebben.lu.se/artikel/angaende-cyberangreppet-mot-var-systemleverantor-miljodata (besökt 2026-04-15)

Myndigheten för civilt försvar, *Cyberangreppens utveckling 2023–2025: Årsrapport cyberincidentrapportering 2025*, nr. MCF0108, Karlstad, mars 2026.

Svenska kraftnät, `Samlad information om dataintrånget`, *Svenska Kraftnät*, 30 oktober 2025, https://www.svk.se/sakerhet-och-beredskap/cybersakerhet/samlad-information-om-dataintranget/ (besökt 2026-04-15)

SVT Nyheter, `Massiv nätattack mot banker och storföretag`, *SVT Nyheter*, 27 juni 2017, https://www.svt.se/nyheter/utrikes/massiv-natattack-mot-banker-och-storforetag (besökt 2026-05-11)

Sveriges Radio, `Attackerna mot Iran – detta har hänt`, Sveriges Radio, 2 mars 2026, https://www.sverigesradio.se/artikel/attackerna-mot-iran-detta-har-hant (besökt 2026-05-19)

Toresson, Jenny, `IT-attacken mot Coop – detta har hänt`, *SVT Nyheter*, 5 juli 2021, https://www.svt.se/nyheter/inrikes/it-attacken-mot-coop-detta-har-hant (besökt 2026-04-15)

Ziegler, Katja S., ´Domaine Réservé´, *Max Planck Encyclopedia of Public International Law*, Oxford University press, uppdaterad april 2013. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1398#:~:text=1%20The%20notion%20of%20do-maine,see%20also%20Jurisdiction%20of%20States (besökt 2026-04-29)