JURIDISKA FAKULTETEN

vid Lunds universitet

Johanna Jakobsson

Cyberoperationer – i gråzon av folkrättslig reglering?

En kritisk analys av suveränitetsprincipens tillämplighet på cyberoperationer

LAGF03 Rättsvetenskaplig uppsats

Kandidatuppsats på juristprogrammet

15 högskolepoäng

Handledare: Aurelija Lukoseviciene

Termin: HT23

Innehåll

Summary

The development of cyberspace and the measures that can be taken within its area presents significant challenges for the regulation of public international law. Currently there is no framework specifically regulating cyberspace, old rules are instead applied to new modern methods. It is established that the prohibition of the use of force in Article 2(4) of the UN Charter and the principle of non-intervention are applicable to cyber operations. However, it remains unclear how rules apply to low-intensity cyber operations that fall below the thresholds of the prohibition of the use of force in Article 2(4) of the UN Charter and the principle of non-intervention.

In the Tallinn Manual 2.0, the principle of sovereignty was classified as a primary rule, leading to a debate about the actual existence of the principle as an international customary rule in the cyber area. The classification means that low-intensity cyber operations can be considered as prohibited acts under international law. To determine the existence of an international customary rule, general practice and opinio juris in the field must be considered. The paper presents two perspectives on the applicability of the principle of sovereignty in relations to cyber operations, where it is seen either as a binding rule or as a guiding principle. If the principle of sovereignty is considered a binding rule, there is regulation for low-intensity cyber operations, meaning, states can be held accountable and other states can take countermeasures. If the rule is not considered a binding rule, the grey area persists, allowing states to take actions against other states without facing accountability.

The general practice and opinio juris currently available are not sufficient to establish the principle of sovereignty as an internationally binding customary rule. Therefore, it can be concluded that the legal situation is unclear. While there is a clear classification in doctrine, it is not considered binding. Because the international customary law in this area is unclear, it is crucial for states to come together to regulate the gray zone of public international law through a treaty.

Sammanfattning

Utvecklingen av cyberrymden och de åtgärder som kan vidtas inom dess område innebär stora utmaningar för den folkrättsliga regleringen. Det finns ännu inget regelverk som reglerar cyberrymden; i stället appliceras gamla regler på nya moderna metoder. Det är konstaterat att våldsförbudet i artikel 2(4) FN-stadgan samt principen om non-interventionen är tillämpliga på cyberoperationer. Det är dock oklart vad som gäller för lågintensiva cyberoperationer, de som faller under trösklarna för våldsförbudet i artikel 2(4) FN-stadgan och principen om non-intervention.

I Tallinn Manualen 2.0 klassificerades suveränitetsprincipen som en primär regel, vilket ledde till en debatt om principens verkliga existens som en internationell sedvanerättslig regel på cyberområdet. Med denna klassificering kan lågintensiva cyberoperationer betraktas som otillåtna handlingar inom folkrätten. För att avgöra om en internationell sedvanerättslig regel existerar måste man granska allmän praxis samt opinio juris på området. Uppsatsen presenterar två olika perspektiv på suveränitetsprincipens tillämplighet på cyberområdet där den antingen ses som en bindande regel eller som en vägledande princip. Om suveränitetsprincipen utgör en bindande regel innebär det att det finns en reglering för lågintensiva cyberoperationer och stater kan därmed hållas ansvariga samt att andra stater kan vidta motåtgärder. Om regeln däremot inte anses utgöra en bindande regel blir gråzonen mer definitiv, vilket innebär att stater kan dra nytta av detta för att vidta åtgärder mot andra stater men undgå statsansvar.

Den allmänna praxis och opinio juris som finns kan inte anses vara tillräcklig för att fastställa suveränitetsprincipen som en internationell sedvanerättslig bindande regel. Det kan därmed konstateras att rättsläget är oklart. Det finns en tydlig klassificering i doktrin, men den anses inte vara bindande. Den folkrättsliga regleringen kan därför inte anses vara tillräcklig för att omfatta de lågintensiva cyberoperationerna. Eftersom den internationella sedvanerätten på området är oklar kan det anses vara av stor vikt att stater gemensamt går samman för att genom traktat reglera de lågintensiva cyberoperationer som hamnar i en gråzon inom folkrätten.

Förkortningar

CCDCOE	Cooperative Cyber Defence Center of Excellence
DRK	Demokratiska Republiken Kongo
FN	Förenta nationerna
FN-stadgan	Förenta nationernas stadga
ICJ	Internationella domstolen (International Court of Justice)
ICJ-stadgan	Stadgan för den internationella domstolen
NATO	North Atlantic Treaty Organisation
USA	United States of America (Amerikas förenta stater)

1 Inledning

1.1 Bakgrund

I april 2022 rapporterades det i media att Microsoft hade kartlagt 237 cyberattacker mot Ukraina utförda av ryska statliga aktörer precis innan kriget inleddes. Målet med var att förstöra, störa eller infiltrera.[1] I ett pressmeddelande från Europeiska unionens råd beskrivs Rysslands användning av cyberoperationer mot Ukraina. En cyberattack inträffade en timme före Rysslands oberättigade invasion av Ukraina den 24 februari 2022 och underlättade det militära angreppet. Cyberattacken fick betydande konsekvenser och orsakade breda kommunikationsavbrott och störningar för flera offentliga myndigheter, företag och användare i Ukraina.[2]

Lågintensiva cyberoperationer som utförs före destruktiva eller våldsamma attacker ger en sannolik bild av framtida statliga cyberoperationer. Utöver att vara högst genomförbara och ofta kostnadseffektiva är lågintensiva cyberoperationer en möjlighet till anonymitet. Detta förhindrar identifiering av attackerade mål samt minskar risken för allvarliga motåtgärder. Lågintensiva cyberoperationer ger därmed stater lockande möjligheter att försvaga motståndare samtidigt som de undviker de sannolika strategiska och juridiska konsekvenserna för massivt förstörande cyberoperationer.[3]

Inom folkrätten är det generellt accepterat att cyberoperationer kan betraktas som handlingar som utlöser våldsförbudet artikel 2(4) FN-stadgan, under förutsättning att en sådan handling uppnår tröskeln för våldsförbudet.[4] Principen om non-intervention anses också vara tillämplig inom folkrätten när det gäller vid cyberoperationer.[5] För att en handling ska kvalificeras och uppnå tröskeln för våldsförbudet i 2(4) FN-stadgan eller principen om non-intervention krävs emellertid en viss grad av intensitet, som är relativt hög, samt att det ofta ställs krav på en fysisk skada. Cyberoperationer har generellt en tendens att utgöra en minimal nivå av våldsanvändning och når därmed inte den intensiteten som krävs för att uppnå dessa trösklar. Detta innebär att lågintensiva cyberoperationer, som inte kvalificeras inom våldsförbudet i artikel 2(4) FN-

[1] Sjöholm, *Svenska Dagbladet*.
[2] Europeiska unionens råd, Pressmeddelande.
[3] Watts, s. 2.
[4] Schmitt, Tallinn Manual 2.0, s. 328.
[5] Schmitt, Tallinn Manual 2.0, s. 312.

stadgan eller en handling mot principen om non-intervention, hamnar i en gråzon inom folkrätten.[6]

Problemet i uppsatsen kan illustreras med följande exempel: Landet X utsätts för tre typer av cyberoperationer av land Y. Den första cyberoperationen resulterar i fysisk skada och dödsfall i landet X, vilket strider mot våldsförbudet i artikel 2(4) FN-stadgan och ger upphov till statsansvar för land Y.[7] Den andra cyberoperationen innebär att land Y fjärrändrar elektroniska röster i landet X:s val och därigenom manipulera valprocessen. Denna cyberoperation kan vara förbjuden enligt principen om non-intervention och medföra statsansvar för land Y.[8] Den tredje cyberoperationen resulterade i reparation och ersättning av fysiska komponenter, såsom tusentals hårddiskar för land X. Denna cyberoperation faller utanför både våldsförbudet i artikel 2(4) FN-stadgan och principen om non-intervention.[9] Här är rättsläget oklart, och denna typ av cyberoperationer väcker ett antal frågor. Kan cyberoperationerna regleras av suveränitetsprincipen? Är suveränitetsprincipen en internationell sedvanerättsligt bindande regel på cyberområdet? Det är dessa frågor som denna uppsats kommer fokusera på att besvara.

1.2 Syfte och frågeställning

Syftet med uppsatsen är att redogöra för den folkrättsliga regleringen av lågintensiva cyberoperationer[10] och om den kan anses vara tillräcklig med utgångspunkt i suveränitetsprincipen.

Mot bakgrund av uppsatsen syfte ska följande frågeställningar besvaras:

- Hur tillämpas suveränitetsprincipen i allmänhet respektive på cyberområdet?
- Är suveränitetsprincipen en internationell sedvanerättsligt bindande regel som kan appliceras på cyberområdet?

Utifrån frågeställningarna ska en diskussion om dagens folkrättsliga reglering är tillräcklig för att omfatta lågintensiva cyberoperationer göras.

[6] Schmitt, Grey Zones in the International Law of Cyberspace, s. 4–5.
[7] Delerue, s. 288–290.
[8] Schmitt, Tallinn Manual 2.0, s. 313 p. 2.
[9] Schmitt, Tallinn Manual 2.0, s. 21.
[10] Se definition i avsnitt 1.6.

1.3 Avgränsningar

Uppsatsens omfattning är begränsad till att undersöka hur folkrätt appliceras på cyberoperationer i fredstid. På grund av uppsatsens begränsade omfång kommer den inte att redogöra för trösklarna för våldsförbudet i artikel 2(4) FN-stadgan eller principen om non-intervention. Detta eftersom uppsatsen är ämnad att behandla lågintensiva cyberoperationer som hamnar i gråzonerna under tröskeln för våldsförbudet i artikel 2(4) FN-stadgan och non-interventionen, eftersom dessa tendera att hamna i skymundan. På grund av uppsatsens avgränsning kommer den inte belysa problematiken med hänförbarhet för statsansvar utan detta förutsätts i uppsatsen för en vidare diskussion. Uppsatsen kommer endast behandla cyberoperationen som utförs mellan stater och avgränsas därmed från privata aktörer. Suveränitetsprincipen är en utbredd regel inom folkrätten och har ett stort omfång. I uppsatsen kommer redogörelsen för suveränitetsprincipen i allmänhet att göras översiktligt med en mer ingående redogörelse för tillämpningen på cyberdområdet.

1.4 Metod

Uppsatsen skrivs utifrån ett internationellt och allmänt kritiskt perspektiv för att belysa problematiken med regleringen av lågintensiva cyberoperationer inom dagens folkrättsliga reglering. Den rättsliga utgångspunkten kommer vara suveränitetsprincipen. Uppsatsen tillämpar en rättsdogmatisk metod, vilket innebär att utreda gällande rätt och applicera den på ett aktuellt problem. Utgångspunkten i metoden är tillämpning av allmänt accepterade rättskällor.[11] Oklarheten om huruvida suveränitetsprincipen anses vara en bindande regel i relation till lågintensiva cyberoperationer motiverar tillämpningen av den rättsdogmatiska metoden.

Uppsatsen kommer utgå från den internationella rättskällehierarkin med fokus på internationell sedvanerätt. För att fastställa huruvida suveränitetsprincipen utgör en internationell sedvanerättslig bindande regel kommer främst sekundära källor, internationella rättsfall samt doktrin användas. Genom tillämpningen av den rättsdogmatiska metoden kommer olika element i rättskälleläran analyseras för att skildra hur rättsregeln, suveränitetsprincipen, tillämpas och tolkas i cyberområdet. För att bedöma om något utgör internationell sedvanerätt kommer både allmän praxis och opinio juris att beaktas. Uppsatsen kommer presentera allmän praxis, opinio juris

[11] Kleineman i Nääx & Zamboni, s. 21.

samt en redogörelse för diskussion i doktrin för att avgöra huruvida suveränitetsprincipen anses utgöra internationell sedvanerätt på cyberområdet.

1.5 Material, forskningsläge och källkritik

Uppsatsen utgår från folkrättsliga källor, vilka skiljer sig från den nationella rättens rättskällor. Enligt artikel 38(1) i ICJ-stadgan består rättskällorna inom folkrätten av internationella konventioner, internationell sedvanerätt, allmänna principer, praxis från internationella domstolar samt doktrin.[12] Det finns ingen rättskällehierarki, vilket innebär att traktaträtt och internationell sedvanerätt har samma status som bindande regler.[13] Internationella rättsfall från ICJ och doktrin betraktas som sekundära källor enligt artikel 38(1)(d) ICJ-stadgan. Existensen av domstolspraxis från en ICJ kan dock utgöra övertygande bevis och beslutens prejudikatvärde kan påverka staters allmänna praxis. Därmed kan beslut från internationella domstolar bidra till utvecklingen av internationell sedvanerätt inom folkrätten.[14] Folkrätten består till stor del av traktaträtt, vilket utgörs av skriftliga avtal som binder de deltagande staterna till vissa åtaganden och förpliktelser.[15] Utöver traktaträtten finns internationell sedvanerätt som kan förklaras som en generell praxis accepterad av stater som rätt.[16] Internationell sedvanerätt kommer förklaras mer ingående i avsnitt 3.

Eftersom regleringen av cyberoperationer inom folkrätten är begränsad, kommer sekundära källor användas i större utsträckning. Uppsatsen utgår därmed främst från sekundära källor, såsom doktrin och internationella rättsfall, för att redogöra för internationell sedvanerätt. Den doktrin som tillämpas i uppsatsen är den mest framstående inom cyberjuridik, vilket i kombination med en frånvaro av internationella konventioner på området styrker valet av källor. Doktrin på området används för att förstå tillämpningen av primärkällor, i detta faller suveränitetsprincipen. All litteratur som används är på engelska, vilket kan påverka ordens betydelse vid översättning till svenska.

Delar av uppsatsen bygger på ”The Tallinn Manual on the International Law Applicable to Cyber Warfare"[17] och ”The Tallinn Manual 2.0 on the International Law Applicable to Cyber

[12] Shaw, s. 52.
[13] Rose, s. 17.
[14] Doswald-Beck & Henckaerts, s. xl.
[15] Shaw, s. 69.
[16] Se ICJ-stadgan, Artikel 38(1)(b).
[17] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare.

Operations” [18], som är de mest detaljerade och utvecklade dokumenten inom området för cyberjuridik. Manualerna har publicerats under ledning av NATO:s Cooperative Cyber Defence Centre of Excellence (CCDCOE). Tallinn Manual är ett försök att kodifiera sedvanerätt inom det cyberjuridiska området men utgör inte ett juridiskt bindande dokument. Vid läsning av Tallinn Manualerna bör läsaren vara medveten om att manualen är författad av en grupp internationella rättsexperter utan ett formellt deltagande från stater. Många av författarna till övriga källor som har används i uppsatsen har varit delaktiga i framtagandet av Tallinn Manualerna.

Det finns ett behov att vidare forska på cyberrymden, särskilt inom området för cyberoperationer. Förutom Tallinn Manualerna, som nämnts ovan, pågår det för närvarande en process för en ny uppdatering av manualen, Tallinn Manual 3.0.[19] Som framgår av uppsatsen pågår det en diskussion i doktrin huruvida suveränitetsprincipen ska anses utgöra en bindande regel på cyberområdet. Även denna fråga kräver ytterligare forskning.

1.6 Terminologi

I dagens moderna samhälle har vi blivit mer beroende av datorer, datorsystem och nätverk, där avgörande tjänster förlitar sig på internet.[20] Begreppet cyberrymden har varken en vetenskaplig eller juridisk definition. I doktrin fastställs dock olika definitioner som tillämpas.[21] Baserat på uppsatsens omfång och syfte kommer cyberrymden definieras som den virtuella verklighet som utgörs av datanätverk.[22]

Även cyberoperationer har ingen entydig definition. I uppsatsen kommer cyberoperation definieras som användningen av cyberrymdens förmågor där det primära syftet är att uppnå mål i eller genom cyberrymden.[23] Vid benämningen av de cyberoperationer som hamnar i gråzonen, som alltså inte når trösklarna för våldsförbudet i artikel 2(4) FN-stadgan eller principen om non-intervention, används begreppet lågintensiva cyberoperationer.

[18] Schmitt, Tallinn Manual 2.0.
[19] Se *CCDCOE to Host the Tallinn Manual 3.0 Process*.
[20] Roscini, s.1.
[21] Delerue, s. 29–30.
[22] Oxford English Dictionary ”cyberspace”.
[23] Joint Chiefs of Staff. s. II-1.

1.7 Disposition

Uppsatsens huvuddel inleds i avsnitt 2 med en beskrivning av under vilka förutsättningar internationell sedvanerätt uppstår. Efterföljande avsnitt 3 återger suveränitetsprincipen, dess allmänna tolkning och tillämpning, samt, med utgångspunkt i doktrin, mer ingående förutsättningarna för suveränitetsprincipen på cyberområdet och vad som föreskrivs för att det ska anses att en stats suveränitet är kränkt.

Vidare i avsnitt 4 presenteras diskussionen i doktrin, suveränitetsprincipen som en internationellt sedvanerättslig bindande regel eller som en vägledande princip. Redogörelsen för detta görs för att fastställa huruvida suveränitetsprincipen utgör en bindande regel som kan kränkas och därmed aktualisera vissa åtgärder som andra stater kan vidta. Att utvärdera detta anses vara en viktig del för att kunna besvara frågeställningen om huruvida folkrätten är tillräckligt reglerad för att omfatta lågintensiva cyberoperationer.

Till sist, i avsnitt 5, besvaras frågeställningarna som presenterats i inledningen. Det görs en analys av huruvida suveränitetsprincipen är en bindande regel i relation till cyberoperationer samt en slutsats om dagens folkrätt är tillräckligt reglerad för att omfatta lågintensiva cyberoperationer.

2 Internationell sedvanerätt

2.1 Introduktion

Frånvaron av en internationell lagstiftare har gjort den internationella sedvanerätten en särskilt viktig källa inom folkrätten, där många välkända principer härstammar från gemensam tillämpning och mellanstatlig praxis.[24] Internationell sedvanerätt utgörs av processen när oskriven lag skapas, ändras och upphävs.[25] Den uppstår när två förutsättningar är uppfyllda. (1) staters allmän praxis och (2) opinio juris, uppfattning av stater att den allmänna praxisen är lagligt bindande. Allmän praxis är ett objektivt kriterium medan opinio juris är subjektivt.[26] Existensen av en internationell sedvanerätt kan i praktiken vara svårt att bevisa.[27]

2.2 Allmän praxis

För att ett specifikt mönster av statligt beteende ska bli juridiskt bindande måste det utgöra allmän praxis. I de flesta fall krävs en konsekvent upprepning av ett visst beteende, vilket innebär att stater under en betydande tidsperiod har agerat på ett visst, identiskt, sätt när de ställs inför liknande omständigheter och fakta.[28] Mängden allmän praxis som krävs för att skildra internationell sedvanerätt beror på den förväntade frekvensen av praxisen beroende på omständigheterna.[29] När allmän praxis varierar kan det anses indikera att det inte existerar en allmän praxis som stödjer internationell sedvanerätt. Men viss inkonsekvent praxis behöver inte underminera internationell sedvanerätt, särskilt när den inkonsekventa praxisen anse utgöra ett brott mot regeln.[30] Allmän praxis måste vara konsekvent, varaktig och allmän. Konsekventelementet kräver att beteendet är rimligt enhetligt. I Nicaragua-fallet uttalade domstolen att det inte kan förväntas att stater har agerat "fullständig konsekvent".[31] När det gäller varaktighet utvecklas allmän praxis vanligtvis långsamt och gradvis över tid, ofta genom års upprepade beteende.[32]

[24] Henriksen, s. 23.
[25] Rose, s, 19.
[26] Henriksen, s. 23.
[27] Rose, s. 19.
[28] Henriksen, s. 23.
[29] Rose, s. 21.
[30] Ibid.
[31] Henriksen, s. 24.
[32] Ibid.

Det tredje elementet av praxis är allmänhetens omfattning, hur utbrett deltagandet i praxis är. Även om enhällighet inte krävs, bör praxis inkludera majoriteten av staterna.[33]

Allmän praxis kan yttra sig i både staters verbala och fysiska handlingar. De fysiska och verbala handlingarna måste även offentliggöras och vara officiella för att skapa internationell sedvanerätt.[34] Exempel på staters fysiska handlingar är användningen av specifika vapen och hur staterna beter sig när de använder dem.[35] Även utförandet av militära operationer till exempel beslagtagande av ett utländskt fartyg är exempel på fysiska handlingar.[36] Exempel på staters verbala handlingar kan vara diplomatiska uttalanden, pressmeddelanden, officiella manualer och internationella organisationers anförande.[37]

2.3 Opinio juris

För att allmän praxis ska anses vara juridisk bindande sedvanerätt krävs det att den accepteras som lag, kravet på opinio juris. Det subjektiva elementet förutsätter därmed ett bevis på att allmän praxis accepteras som lag.[38] Att fastställa opinio juris är kontroversiellt och det finns teoretiska svårigheter i kravet på att en stat måste handla på ett visst sätt på grund av en uppfattning att det krävs lagligen.[39] Denna svårighet uppstår då stater ofta inte förklarar varför den handlar eller underlåter att handla på ett visst sätt.[40]

Uttryck för opinio juris kan återfinnas i nationella strategidokument, riktlinjer, rapporter, manualer av internationella organisationer samt uttalanden från politiker.[41] Den särskilda form i vilken praxis och denna rättsliga övertygelse behöver uttryckas kan variera beroende på om den aktuella regeln innehåller ett förbud, en skyldighet eller en rättighet att agera på ett visst sätt.[42] Eftersom uppsatsen behandlar uppkomsten av en förbudsnorm kan opinio juris yttra sig i form av uttalanden om att sådant beteende är förbjudet och fördömanden av fall där det förbjudna

[33] North Sea Continental Shelf Cases, para. 74.
[34] Doswald-Beck & Henckaerts, s. xxxviii—xl.
[35] Ibid.
[36] Henriksen, s. 24.
[37] Ibid.
[38] Artikel 38(1)(b) ICJ-stadgan.
[39] Henriksen, s. 23.
[40] Ibid.
[41] Väljataga, s. 4.
[42] Doswald-Beck & Henckaerts, s. xlvi.

beteendet faktiskt ägde rum, eventuellt kombinerat med rättfärdigande eller ursäkter från den kritiserade staten, men också fysisk praxis av att avstå från det förbjudna beteendet.[43]

[43] Doswald-Beck & Henckaerts, s. xlv.

3 Suveränitetsprincipen

3.1 Allmänt om suveränitetsprincipen och dess tillämpning

Suveränitetsprincipen utgör den mest fundamentala principen inom folkrätten.[44] Samtidigt finns det skiljaktigheter huruvida principen existerar som en bindande verkställbar regel[45] eller om den i stället verkar som en grundläggande princip som underbygger andra bindande regler.[46]

Artikel 2(1) och artikel 2(7) FN-stadgan återger två funktioner av statssuveränitet. Artikel 2(1) FN-stadgan betonar principen om samtliga medlemmars suveräna likställdhet, externa suveräniteten. Stater är juridiskt jämställda; varje stat är skyldig att respektera andra staters personliga och territoriella integritet, politiska oberoende samt lojalt uppfylla sina internationella åtaganden.[47] Artikel 2(7) FN-stadgan betonar förbudet för FN att ingripa i frågor väsentliga för vederbörande stats egen behörighet, intern suveränitet.[48] Intern suveränitet erkänner stater som enhet som utövar kontroll över ett definierat territorium och människor inom territoriet.[49]

En kränkning av suveränitetsprincipen förekommer om en stat fysisk inträder i en annan stats territorium eller nationellt luftrum utan samtycke eller annat undantag inom folkrätten.[50]

3.2 Suveränitetsprincipens tillämpning på cyberområdet

3.2.1 Intern och extern suveränitet

Tallinn Manual 2.0, regel 3, beskriver att stater har extern suveränitet över sina cyberaktiviteter i internationella relationer. De är fria att vidta cyberoperationer utanför sitt territorium, under förutsättning att det inte strider mot folkrätten. Det ger staterna självständighet i sina externa

[44] Se Bardo Fassbender `artikel 2(1)´ i Simma m.fl.
[45] Schmitt & Vihul, Lex lata vel non?, s. 213–218.
[46] Corn & Taylor, s. 208.
[47] Military and Paramilitary Activities in and against Nicaragua, para. 202.
[48] Se FN-stadgan artikel 2(7).
[49] Crawford, s. 448.
[50] Schmitt, Tallinn Manual 2.0, s. 19, p. 6.

relationer och möjliggör deltagande i internationella överenskommelser och beslut som rör cybertraktat.[51]

I Tallinn Manual 2.0, regel 2, återges att stater har intern suveränitet över sin cyberinfrastruktur och cyberaktiviteter inom sitt territorium. Det innebär att stater har rätt att vidta åtgärder inom dessa områden i enlighet med internationell lag, med möjlighet att reglera dem nationellt och skydda dem enligt folkrättsliga regler.[52]

3.2.2 Kränkning av suveränitetsprincipen

Tallinn Manual 2.0, regel 4, fastställer att en stat inte får bedriva cyberoperationer som kränker en annan stats suveränitet. Det framgår att den rättsliga karaktären av cyberoperationer är oklar inom folkrätten, och det finns inget traktat som reglerar frågan.[53] Trots detta bedömde Tallinn Manualens expertgrupp lagligheten utifrån två olika grunder. Den första grunden beskrivs utifrån graden av kränkning av statens territoriella integritet. Grunden baseras på antagandet att en stat kontrollerar åtkomsten till sitt suveräna territorium. Den andra grunden utgår från huruvida det har förekommit ingrepp eller tillgrepp av inneboende statliga funktioner. Grunden baseras på antagandet att en stats suveräna rätt att inom sitt territorium har en uteslutande rätt att utöva inneboende statliga funktioner.[54]

3.2.2.1 Graden av kränkning av statens territoriella integritet

Den första grunden delades upp i tre distinkta nivåer för vad som utgör en kränkning av en stats suveränitet. Den första nivån utgörs av fysisk skada, exempelvis användningen av skadlig programvara som orsakar fel i kylkomponenter i utrustning, som leder till överhettning och smältning av komponenter. Den andra nivån består av förlust av funktionalitet, exempelvis om en cyberoperation stör eller inaktiverar kritiska system, vilket resulterar i att den inte fungerar normalt. Den tredje nivån utgörs av kränkning av territoriell integritet under tröskeln för förlust av funktionalitet alltså cyberoperationer som inte orsakar en fullständig förlust av funktionalitet men ändå kränker en annan stats territoriella integritet. Till exempel vid cyberoperationer som ändrar eller raderar data som lagrats i cyberinfrastruktur utan att orsaka fysiska eller funktionella konsekvenser. Expertgruppen noterade att dessa operationer också kan utgöra intervention

[51] Schmitt, Tallinn Manual 2.0, s. 16, p. 2.
[52] Ibid. s. 13, p. 1.
[53] Ibid. s. 20, p. 10.
[54] Ibid. s. 20 p. 10.

eller bryta mot våldsförbudet i artikel 2(4) FN-stadgan, beroende på cyberoperationens svårighetsgrad och konsekvenser.[55]

3.2.2.2 Ingrepp eller tillgrepp av en annan stats inneboende statliga funktion

Den andra grunden för kränkning av suveränitet, är att kränkningen uppstår när en stats cyberoperation innebär ett ingrepp eller tillgrepp av en annan stats inneboende statliga funktioner. Expertgruppen kunde inte enhetligt definiera ”inneboende statlig funktion” men de var överens om att en cyberoperation som ingriper i data eller tjänster som är nödvändiga för utförandet av inneboende statliga funktioner är förbjuden som en kränkning av suveränitet. Det framställs att officiell kommunikation mellan en stats ledning utgör inneboende statlig funktion medan information som publiceras och kommuniceras på en statlig webbplats inte utgör en inneboende statlig funktion, även om den är statlig.[56]

[55] Schmitt, Tallinn Manual 2.0, s. 20 p. 11.
[56] Ibid. s. 20 p. 15–17.

4 Diskussion i doktrin; Suveränitetsprincipen som en bindande regel eller vägledande princip

4.1 Generellt

Beroende på om suveränitetsprincipen anses vara en internationell sedvanerättsligt bindande regel eller inte påverkar hur stater lagligen kan använda cyberoperationer. Om en stat bryter mot suveränitetsprincipen som en sedvanerättsligt bindande regel bör detta leda till statsansvar för den staten enligt folkrätten och en rätt för den andra staten att vidta åtgärder. Om suveränitetsprincipen i stället inte ses som en bindande regel utan en grundläggande princip, skulle den främst fungera som en vägledning för staters interaktioner. Därmed kan stater hävda att de är fria att tillämpa lågintensiva cyberoperationer som metod, vilket skulle strida mot suveränitetsprincipen men som inte uppfyller tröskeln för non-intervention eller våldsförbudet i artikel 2(4) FN-stadgan.[57] Sedan publiceringen av Tallinn Manual 2.0 har diskussionen om suveränitetsprincipen som regel varit mycket omdebatterad i cyberrelaterad doktrin.[58]

En viktig aspekt för uppsatsen är skillnaden mellan en generell princip och en primär regel. Både principer och primära regler är källor inom internationell rätt.[59] Primära regler förelägger skyldigheter eller förbud för stater, vilket innebär att en primär regel kan brytas. Det är dock oklart huruvida en grundläggande princip kan brytas på samma sätt.[60]

4.2 Suveränitetsprincipen som en bindande regel

4.2.1 Allmän praxis

Schmitt och Vihul, förespråkare för suveränitetsprincipen som en bindande regel, baserar sin ståndpunkt på allmän praxis och hänvisar till händelser i luftrum, havsområde och landområde. Exempel inom luftrum, som tydligt illustrerar suveränitetsprincipen som en bindande rättslig

[57] Ericson, s. 209.
[58] Se till exempel, Corn & Taylor; Schmitt och Vihul, Respect for Sovereignty in Cyberspace. mm.
[59] Se ICJ-stadgan, Artikel 38(1).
[60] Se Schmitt & Vihul, Respect for Sovereignty in Cyberspace. (not 12) s. 1641.

regel är två händelser från 1960 vilka involverande amerikanska spaningsflygplan och Sovjetunionen.[61] I det första fallet sköts ett U-2 flygplan ned i sovjetiskt luftrum, och USA protesterade inte, medan de i det andra fallet fördömde Sovjets nedskjutning av ett RB-47 flygplan som flög över internationellt luftrum. Skillnaden mellan reaktionerna förklaras av platserna där flygplanen befann sig vid tidpunkten för nedskjutningarna. U-2 var i sovjetiskt luftrum, vilket betraktades som en kränkning av Sovjets suveränitet, medan RB-47 flög över internationellt luftrum enligt USA:s uppfattning och ansågs därför inte utgöra en kränkning av Sovjetunionens territoriella suveränitet.[62]

En händelse inom havsområdet som författarna skildrar som ett ytterligare fall som ger uttryck för att suveränitetsprincipen utgör en internationellt sedvanerättsligt bindande regel. En incident inträffade 2016 i den persiska viken där iranska styrkor tillfångatog tio amerikanska flottsoldater och beslagtog två båtar som hade inträtt på iranskt territoriellt hav. Efter förhandling med den amerikanska regeringen frisläpptes flottsoldaterna och båtarna. USA framförde inga protester mot Irans handlingar i stället tackade den amerikanska utrikesministern för snabb respons och frigivning. Denna händelse understryker att USA förstod att de hade inkräktat på iransk suveränitet och därmed inte protesterat mot de iranska handlingarna.[63]

Författarna använder sig av ytterligare ett välkänt exempel som redogör för suveränitetsprincipen om en internationellt sedvanerättsligt bindande regel på landområdet, fallet Adolf Eichmann. Eichmann var en av de ledande aktörerna bakom förintelsen och flydde efter andra världskriget till Argentina. På 1960-talet grep den israeliska underrättelsetjänsten honom på argentinskt territorium och ställde honom inför rätta i Israel. Argentina tog upp ärendet till FN:s säkerhetsråd och anklagade Israel för att ha kränkt Argentinas suveränitet genom att utöva exekutiv jurisdiktion på argentinskt territorium. Säkerhetsrådet antog därefter en resolution där man noterade att Israel hade olagligen kränkt Argentinas stats suveränitet och att Israel därmed skulle ersätta Argentina enligt folkrättslig reglering. [64]

[61] Schmitt & Vihul, Respect for soverignty in cyberspace. s. 1656–1657.
[62] Lissitzyn, s. 135 ff.
[63] Schmitt & Vihul, Respect for soverignty in cyberspace. s. 1658.
[64] Ibid. s. 1659.

4.2.2 Opinio juris

För att återge opinio juris på området använder Schmitt och Vihul sig av ett flertal uttalanden och ståndpunkter som länder har uttryckt. Författarna hänvisar till ett dokument som släpptes av USA:s försvarsdepartement på slutet av 1990-talet, där de förklarade sin ståndpunkt gällande cyberoperationer i relation till suveränitetsprincipen. De återgav att ett obehörigt elektroniskt intrång i ett annat lands datorsystem mycket väl kan komma att betraktas som en kränkning av statens suveränitet. Det ansågs även kunna betraktas som likvärdigt med ett fysiskt intrång på ett lands territorium.[65] Frågan vid den tiden var inte om cyberoperationer kunde kränka en annan stats suveränitet, utan vid vilken punkt de gjorde det. Att cyberoperationer kunde kränka en annan stats suveränitet togs som en normativ givenhet.[66]

Författarna hänvisar vidare till ett tal från år 2012 ,om den folkrättsliga regleringen i cyberrymden, där den tidigare juridiska rådgivaren för USA:s utrikesdepartement, Harold Koh, framställde att USA anser att suveränitetsprincipen är etablerad inom folkrätten och tillämplig i cyberrymden. Koh betonade vikten av att stater som genomför cyberoperationer i andra stater måste respektera dessa staters suveränitet.[67] Kohs ståndpunkt bekräftades av hans efterträdare, Brian Egan, som tillade att tröskeln för när en cyberoperation kränker en annan stats suveränitet måste fastställas genom statlig allmän praxis och opinio juris.[68] Både Koh och Egan behandlade suveränitetsprincipen som skild från våldsförbudet i artikel 2(4) FN-stadgan och principen om non-intervention, vilket antyder att suveränitetsprincipen betraktas som en fristående bindande regel.[69]

USA har på senare tid anslutit sig till en annan uppfattning och förklarar sin ståndpunkt att suveränitetsprincipen snarare utgör en vägledande princip än en bindande regel.[70] Denna ståndpunkt kommer diskuteras vidare i avsnitt 5.4.

[65] U.S. Department of Defence of General Counsel, An Assessment of International Legal Issues in Information Operations. s. 485.
[66] Schmitt & Vihul, Respect for soverignty in cyberspace. s. 1640.
[67] Ibid. s. 1663–1664.
[68] Ibid. s. 1664.
[69] Ibid. s. 1663–1664.
[70] Väljataga, s. 7.

Schmitt och Vilhul redogör för hur Sovjet Premiärminister Khrushchev, år 1959, konfirmerar att Sovjet accepterar suveränitetsprincipen som en förbudsregel samt att han använder den fristående från sådana handlingar som klassas inom principen om non-intervention.[71]

Ryssland och Kina försvarar starkt suveränitetsprincipens bindande karaktär i cyberrymden.[72] I juni 2016 undertecknade de ett gemensamt uttalande om samarbete inom utvecklingen av informationsutrymmet, där betonar deras åtagande att "gemensamt verka för respekt för och motstå intrång på varje lands suveränitet i informationsutrymmet".[73] Kina, känt som en av världens största statliga sponsorer av cyberattacker, har gjort suveränitet till hörnstenen i sin internationella cybersäkerhetspolitik. Kinas nationella cybersäkerhetsstrategi fastslår tydligt att ingen kränkning av suveränitet i cyberrymden kommer att tolereras.[74]

4.2.3 Internationella rättsfall

Som beskrivet ovan är internationella rättsfall en sekundär källa inom folkrätten men som kan utgöra ett bevis för att en internationell sedvanerätt existerar.[75] För att redogöra för huruvida suveränitetsprincipen anses utgöra en internationell sedvanerättslig bindande regel på cyberområdet presenteras följande internationella rättsfall.

I Lotus-målet återger ICJ att den grundläggande restriktionen för stater som uppstår inom folkrätten är att en annan stat inte får utöva makt i någon form på en annan stats territorium.[76] Författarna argumenterar utifrån fallet och drar slutsatsen att om en stat, utan samtycke, utför handlingar på en annan stats territorium innebär det ett brott mot statens förpliktelser enligt suveränitetsprincipen. De anser att domstolen behandlar suveränitetsprincipen som en regel som sätter bindande begränsningar för staters handlingar på andra staters territorium.[77]

Ett annat uppmärksammat fall som berör suveränitetsprincipen är Corfu Channel. Fallet handlar om en tvist mellan Storbritannien och Albanien som uppstod då ett brittiskt krigsfartyg passerade Korfu kanalen då det träffades av albanska havsminor. Efter incidenten körde den brittiska kungliga flottan ännu en gång in i Korfukanalen för att genomföra minröjningsoperationer.[78]

[71] Schmitt & Vihul, Respect for soverignty in cyberspace. s. 1661.
[72] Väljataga, s. 7.
[73] Ibid.
[74] Ibid.
[75] Doswald-Beck & Henckaerts, s. xl.
[76] The Case of the S.S. Lotus, para. 45.
[77] Schmitt & Vihul, Respect for soverignty in cyberspace. s. 1651.
[78] Se Corfu Channel.

Domstolen ansåg Albanien ansvarig för den skada som skett på det brittiska krigsfartyget. Däremot menade domstolen att genom att den brittiska kungliga flottans inträde in i Korfukanalen för minrengöringen, utan Albaniens samtycke, utgjorde ett brott mot suveränitetsprincipen.[79]

I Nicaragua-fallet lyftes frågan om suveränitetsprincipen ytterligare. Fallet handlade om Nicaraguas påstående om att USA hade brutit mot sina förpliktelser enligt internationell sedvanerätt och kränkt Nicaraguas suveränitet genom beväpnade attacker mot Nicaragua från luft, land och hav.[80] När domstolen redogjorde för påståendet beskrev de sambandet mellan suveränitetsprincipen, våldsförbudet i artikel 2(4) FN-stadgan och principen om non-intervention där de tydligt differentierade dem och påpekade att en handling kan bryta mot mer än en av reglerna. Enligt domstolens uppfattning har suveränitetsprincipen ett oberoende värde. Domstolen kom fram till att USA hade brutit mot samtliga regler, våldsförbudet i artikel 2(4) FN-stadgan, principen om non-interventionen samt suveränitetsprincipen.[81] Enligt författarna behandlar domstolen suveränitetsprincipen som en fristående primär regel med samma normativa kraft som de andra.[82]

4.3 Suveränitetsprincipen som en vägledande princip

Corn och Taylor, två högt uppställda juridiska rådgivare inom det amerikanska försvarsdepartementet[83], argumenterar för att cyberoperationer som inte faller inom våldsförbudet i artikel 2(4) FN-stadgan eller principen om non-intervention inte är förbjudna. I stället argumenterar de för att suveränitetsprincipen ska ses som en princip inom folkrätten som kan användas som ett vägledande verktyg.[84] Författarna baserar detta på att det inte finns tillräckligt mycket allmän praxis eller opinio juris som konfirmera att principen är en bindande regel.[85]

För att understryka sina argument emot suveränitetsprincipen som en internationell sedvanerättsligt bindande regel diskuterar de hur folkrätten har utvecklats i rymden, luftrum och hav, där det konstateras att de olika områdenas tillämpning av suveränitetsprincipen skiljer sig betydligt.[86] När det gäller yttre rymden så anses objekt som befinner sig i yttre rymden bortom någon nations nationella territoriella anspråk och är alltså tillgängligt för exploatering av alla

[79] Corfu Channel s. 36; Schmitt and Vihul, Respect for soverignty in cyberspace. s. 1651.

[81] Military and Paramilitary Activities in and against Nicaragua, s. 128, para 251.
[82] Schmitt & Vihul, Respect for soverignty in cyberspace. s. 1653–1654.
[83] Se Corn & Taylor, (not 1) s. 207.
[84] Corn & Taylor, s. 205–212.
[85] Ibid. s. 208.
[86] Ibid. s. 210.

stater. Förekommande har fastställts i traktat och är nu även accepterat som internationell sedvanerätt.[87] Detta skiljer sig från vad som är reglerat när det gäller inträdde i annan stats luftrum utan samtycke, där detta ses som en allvarlig överträdelse av folkrätten.[88] När det gäller inträde på annan stats territoriella vatten så är detta beroende på fakta och omständigheterna i det enskilda fallet om det anses vara tillåtet eller inte, men att det i flera fall kan ske utan en stats samtycke. Som huvudregel gäller att territorialhavet är okränkbart men det har genom internationell sedvanerätt utvecklats undantag såsom rätt till oskadlig genomfart och transitpassage.[89] Baserat på det återgivna exempel drar författarna slutsatsen om utvecklingen av starkt olika regleringar på dessa områden understryker att suveränitetsprincipen inte utgör en universell regel som därmed kan tillämpas i cyberrymden.[90]

Corn och Taylor använder sig även av två rättsfall för att styrka sina argument. Författarna hänvisar också till Cofu Channel-fallet, som berörts i avsnitt 4.2.3, men menar i stället att fallet inte stödjer suveränitetsprincipens existens som en fristående internationellt sedvanerättsligt bindande regel. De menar i stället att fallet nådde en högre tröskel än den som påstås vara suveränitetsprincipen.[91]

Fallet Democratic Repulic of the Congo v. Uganda bekräftar, enligt Corn och Taylor, att suveränitetsprincipen inte utgör en fristående internationell sedvanerättsligt bindande regel.[92] I fallet anklagade Demokratiska republiken Kongo, DRK, Uganda för överträdelse av våldsförbudet i 2(4) FN-stadgan, principen om non-intervention samt DRKs suveränitet då de hade engagerat sig i militära aktiviteter, ockuperat dess territorium samt stöttat rebellgrupper.[93] ICJ fann att Uganda hade överträtt DRKs suveränitet och territoriella integritet. Domstolen beskriver att Ugandas handlingar utgjorde ett ingrepp i DRKs inre angelägenheter.[94] Corn och Taylor hävdar att domstolens användning av begreppet ”territoriell integritet” har hämtats från artikel 2(4) FN-stadgan, våldsförbudet, och att handlingarna därmed anses indikera på en överträdelse av en högre tröskel än suveränitetsprincipen. Författarna återger även att domstolen endast konstaterade att Uganda hade överträtt våldsförbudet i artikel 2(4) FN-stadgan och principen om

[87] Corn & Taylor, s. 210.
[88] Ibid.
[89] Ibid.
[90] Ibid.
[91] Ibid.
[92] Armed Activities on the Territory of the Congo, s. 168.
[93] Armed Activities on the Territory of the Congo, para. 24.
[94] Armed Activities on the Territory of the Congo, para. 165.

non-intervention utan att nämna en överträdelse av suveränitetsprincipen.[95] Corn och Taylor drog därmed slutsatsen att domstolen inte fastställde att en överträdelse av suveränitetsprincipen är oberoende av våldsförbudet i artikel 2(4) FN-stadgan eller principen om non-intervention. Författarna anser sålunda att suveränitetsprincipen inte utgör en fristående internationell sedvanerättslig bindande regel.[96]

[95] Armed Activities on the Territory of the Congo, para. 345; Corn & Taylor, s. 210.

[96] Corn & Taylor s. 210.

5 Analys och slutsats

5.1 Analys

5.1.1 Hur tillämpas suveränitetsprincipen i allmänhet respektive på cyberområdet?

Suveränitetsprincipen består av intern och extern suveränitet som förelägger stater rättigheter och skyldigheter i relation till staten i sig men också i relation till andra stater. Suveränitetsprincipen i allmänhet utgörs av den externa suveräniteten som betonar staters likställdhet, där varje stat är skyldig att respektera andra staters personliga och territoriella integritet. Den interna suveräniteten erkänner stater som enhet som utövar kontroll över ett definierat territorium och människorna inom territoriet.

Tillämpning av suveränitetsprincipen på cyberområdet omfattar också intern och extern suveränitet. Den externa suveräniteten applicerad på cyberområdet återger en möjlighet att vidta cyberoperationer utanför sitt territorium under förutsättning att det inte strider mot folkrättsliga regleringar. Den interna suveräniteten applicerad på cyberområdet betonar varje stats rättighet att reglera cyberinfrastruktur och cyberaktiviteter inom statens territorium i enlighet med folkrättsliga regleringar.

En kränkning av en stats suveränitet föreligger i allmänhet om en annan stat inträder i en annan stats territorium eller nationella luftrum. Applicerat på cyberområdet framför doktrin att en kränkning av suveränitetsprincipen föreligger förutsatt att det finns en viss grad av kräkning av statens territoriella integritet samt att det förekommit ett ingrepp eller tillgrepp i en annan stats inneboende statliga funktion.

Det finns inga primära källor inom folkrätten som bekräftar denna utgångspunkt på cyberområdet. Tallinn Manualen ses vara ett försök att kodifiera internationell sedvanerätt för att kartlägga ett regelverk på cyberområdet. För att ett regelverk på cyberområdet ska anses vara bindande krävs tillräcklig allmän praxis och opinio juris eller att stater tillsammans genom traktat skapar ett regelverk för att få en enhetlig och tillförlitlig tillämpning av suveränitetsprincipen på cyberområdet.

5.1.2 Är suveränitetsprincipen en internationell sedvanerättsligt bindande regel som kan appliceras på cyberområdet?

Corn och Taylor påstår att det inte finns tillräckligt med allmän praxis och opinio juris som styrker att cyberoperationer under trösklarna för principen om non-intervention och våldsförbudet i 2(4) FN-stadgan utgör en kränkning mot internationell sedvanerätt. När det gäller allmän praxis är denna som sagt sparsam när det gäller cyberoperationer men med ett antal analogier som Schmitt och Vihul använder sig av kan en diskussion föras. Den allmänna praxisen som redogjorts för i avsnitt 4.2.1., framställd av Schmitt och Vihul genomsyras av en uppfattning att suveränitetsprincipen utgör en fristående bindande regel med en operativ effekt. Det gemensamma i de fall som diskuterats ovan är att suveränitetsprincipen behandlas som en regel som kan överträdas och som skiljer sig från de andra reglerna som härstammar från samma princip, våldsförbudet i artikel 2(4) FN-stadgan och principen om non-intervention.

Att USA har anslutit sig till ståndpunkten att suveränitetsprincipen utgör en vägledande princip snarare än en bindande regel kan anses vara en indikation på att suveränitetsprincipen inte är en bindande regel. Om flera länder ansluter sig till denna uppfattning kan den internationella sedvanerätten utvecklas till att gråzonen blir definitiv och att det därmed krävas en internationell konvention för att reglera lågintensiva cyberoperationer.

Corn och Taylor hävdar vidare att utvecklingen av starkt olika regleringar av suveränitetsprincipen på luft, havs, land och rymdområdet understryker att suveränitetsprincipen inte utgör en universell regel som kan tillämpas i cyberrymden. Att en överträdelse av en annan stats luftrum och landområde anses utgöra kränkning av suveränitetsprincipen är en konsekvent uppfattning inom folkrätten. När det gäller yttre rymden har stater genom ingående av traktat beslutat att yttre rymden inte är föremål för nationellt anspråk på suveränitet. Detta indikerar att om det inte funnits någon regel, som nu accepteras i sedvanerätten, skulle territoriell suveränitet ses som standard och att den sträcker sig bortom luftrummet ovanför en stats suveräna territorium och i yttre rymden. Regleringen av yttrerymden bör ses som en lex specialis medan suveränitetsprincipen anses utgöra en lex generalis. Att en stat utan samtycke kan inträda i en annan stats territorialhav beror på utveckling av internationell sedvanerätt i form av undantag. Huvudregeln och principen om en stat okränkbara territorialhav kvarstår med undantag för undantagen. Det kan därmed inte antas att detta påstående undanröjer suveränitetsprincipen utan samma resonemang som för yttre rymden kan göras.

Corn och Taylor hävdar att eftersom vissa av de aktuella internationella rättsfallen också utgjorde en kränkning av våldsförbudet i artikel 2(4) FN-stadgan och en kränkning av principen om non-intervention, utgjorde de överträdelser av suveränitet och territoriell integritet "i vidare bemärkelse". Det kan dock ifrågasättas varför domstolen iså fall skulle hänvisa explicit till en överträdelse av suveränitet, särskilt från de andra två förbuden, när domstolens funktion är att bedöma om den aktuella handlingen utgjorde specifika internationellt otillåtna handlingar. I domen Corfu Channel drog domstolen slutsatsen att minröjningsoperationen i Albaniens territorialvatten och utgrävningen av kanalerna samt Nicaraguas etablerande av en militär närvaro på costaricanskt territorium bara utgjorde överträdelser av suveränitet, inte en kränkning av principen om non-intervention eller våldsförbudet i artikel 2(4) FN-stadgan. Om det var tillräckligt för domstolen att fatta ett beslut i dessa fall på grund av överträdelser av suveränitet, kan en slutsats att suveränitetsprincipen fungerar som en primär regel inom folkrätten dras.

Det anses vara oklart huruvida suveränitetsprincipen utgör en internationell sedvanerättslig bindande regel. Appliceringen av analogier som allmän praxis kan anses vara en brist i att avgöra internationell sedvanerätt. Men eftersom cyberoperationer är svårt att hänföra till stater bör det anses vara tillräckligt för att föra en diskussion. Skiftet i USA:s uttryck för opinio juris i frågan indikerar att en annan riktning av internationell sedvanerätt håller på att utvecklas. Utifrån analysen dras slutsatsen att det är oklart huruvida den allmänna praxisen och opinio juris faktiskt uttrycker suveränitetsprincipen som bindande regel på cyberdområdet.

Förutsatt att suveränitetsprincipen utgör en internationell sedvanerättsligt bindande regel så dras slutsatsen att dagens reglering är tillräcklig för att omfatta de lågintensiva cyberoperationer som används i dagens samhälle. Om det däremot skulle ge uttryck åt att suveränitetsprincipen inte utgör en sådan bindande regel så skulle det vara nödvändigt att få till en förändring och utveckling av folkrätten på cyberområdet. Om suveränitetsprincipen utgör en internationell sedvanerättsligt bindande regel innebär det att stater kan hållas ansvariga för lågintensiva cyberoperationer och att stater därmed inte kan utnyttja den gråzon som finns under trösklarna för våldsförbudet i 2(4) FN-stadgan och principen om non-interventionen. Om suveränitetsprincipen anses som en internationell sedvanerättsligt bindande regel hade Rysslands cyberoperationer mot Ukraina innan invasionen kunnat anses utgöra en kränkning av suveränitetsprincipen och därmed hade statsansvar kunnat utkrävs samt rätt för Ukraina att vidta vissa motåtgärder mot Ryssland redan innan den fullskaliga invasionen.

5.2 Slutsats

De förutsättningar som återges för att suveränitetsprincipen kan vara en bindande regel inom cyberområdet skildras i doktrin vilket innebär att det inte är ett bevis på internationell sedvanerätt utan endast ett försök av kodifiering av internationell sedvanerätt. En frånvaro av allmän praxis av cyberoperationer medför att slutsatsen om suveränitetsprincipen är en bindande regel på cyberområdet måste dras baserat på analogier från andra folkrättsliga områden. Det kan anses att genom denna applicering av analogier kan slutsatsen dras att suveränitetsprincipen anses utgöra en fristående bindande regel. I kombination med opinio juris på området kan det bekräftas att ett stort antal av de starkaste cyberstaterna har en uppfattning att suveränitetsprincipen är en bindande regel på cyberområdet. Det kan dock ifrågasättas om det idag är internationell sedvanerätt eller om den internationella sedvanerätten skapas i och med USAs ändrade ståndpunkt.

Utifrån den allmänna praxis och opinio juris som presenteras kan det anses att den folkrättsliga regleringen av lågintensiva cyberoperationer på cyberområdet är oklar. Det anses att en bristfällig reglering av lågintensiva cyberoperationer utgör en fördel för de stater som har en stark cyberinfrastruktur, då de både kan skydda sig och utföra cyberoperationer utan att bli påkomna och därmed komma undan ansvar och motåtgärder. De länder som kommer bli negativt påverkade av en bristfällig reglering är länder med svag cyberinfrastruktur. Eftersom den internationella sedvanerätten på området är oklar kan det anses att det är av stor vikt att stater gemensamt går samman för att genom traktat reglera de lågintensiva cyberoperationer som hamnar i en gråzon inom folkrätten.

Källförteckning

Litteratur:

Bruno Simma. (red.). *The Charter of the United Nations – A Commentary, vol I*. 3 uppl, Oxford: Oxford University Press, 2012.

Corn, Gary P.; Taylor, Robert, Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: *Sovereignty in the Age of Cyber* The American Journal of International Law Unbound, Vol. 111. Cambridge: Cambridge University Press, 2017. E-bok.

Crawford, James, *Brownlie's Priniciples of Public International Law.* 8 uppl. Oxford: Oxford University Press, 2012.

Doswald-Beck, Louise; Henckaerts, Jean-Marie. *International Committee of the Red Cross – Customary International Humanitarian Law:* Volume I: Rules. Cambridge: Cambridge University Press, 2005. E-bok.

Delerue, François. *Cyber operations and international law*. Cambridge: Cambridge University Press, 2020.

Ericson, Marika. *On the Vitrual Borderline: Cyber Operations and their Impact on the Paradigms for Peace and War*. Uppsala: Uppsala Universitet, 2020.

Henriksen, A. *International Law.* 4 uppl. Oxford University Press, 2023.

Nääx,Maria; Zamboni, Mauro (red.). *Juridisk metodlära*. 2 uppl. Studentlitteratur, 2018.

Roscini, Marco. *Cyber Operations and the Use of Force in International Law.* Oxford: Oxford University Press, 2014. E-bok.

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

Schmitt, Micheal N. (red.). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press, 2013. E-bok.

Schmitt, Micheal 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 uppl. Cambridge: Cambridge University Press, 2017.

Schmitt, Michael N.; Vihul, Liis, Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Sovereignty in Cyberspace: *Lex Lata Vel Non?.* The American Journal of International Law Unbound, Vol. 111. Cambridge: Cambridge University Press, 2017. E-bok.

Shawn, Malcom N. *International Law*. 8 uppl. Cambridge: Cambridge University Press, 2017. E-bok.

Artiklar:

Lissitzyn, Oliver. J. 'Some Legal Implications of the U-2 and RB-47 Incidents.' The American Journal of International Law, Vol. 56, No. 1, 1963.

Schmitt, Michael. N. 'Grey Zones in the International Law of Cyberspace.' The Yale Journal of International Law, 2017.

Schmitt, Michael N.; Vihul, Liis. 'Respect for Sovereignty in Cyberspace.' Texas Law Review Vol. 95, 2017.

U.S. Department of Defence Office of General Counsel, 'An Assessment of International Legal Issues in Information Operations.' 2 uppl. 1999.

Watts, S. (2014). 'Low-intensity Cyber Operations and the Principle of Non-intervention.' . Creighton University School of Law.

Rättsfall:

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Merits (2005) ICJ Reports 168.

Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), Merits (1949) ICJ Reports 4.

North Sea Continental Shelf Cases (Federal Republic of Germany/Netherlands), Merits (1969) ICJ Reports 3.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits (1986) ICJ Reports 14.

The Case of the S.S. Lotus (France v. Turkey), Judgment (1927) P.C.I.J. (ser A) No. 10.

Övrigt:

Europeiska unionens råd, Pressmeddelande. *Ryska cyberoperationer mot Ukraina: uttalande av EU:s utrikesrepresentant på EU:s vägnar.* (22-05-10).

https://www.consilium.europa.eu/sv/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/ (hämtad 2023-12-19)

Joint Chiefs of Staff. 'Joint publication 3-12 Cyberspace Operations', 2018.

Oxford English Dictionary "cyberspace". OED Online. Oxford University Press. https://www.oed.com/dictionary/cyberspace_n?tab=meaning_and_use#12786295 (hämtad 2023-11-27)

Sjöholm, Gustav. 'Microsoft: 237 cyberattacker mot Ukraina'. Svenska Dagbladet, 2022-04-28. https://www.svd.se/a/Xq1j9g/237-cyberattacker-mot-ukraina, (hämtad 2023-12-19)

The NATO Cooperative Cyber Defence Centre of Excellence. CCDCOE to Host the Tallinn Manual 3.0 Process. https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/ (hämtad 23-12-27)

Väljataga, Ann. Tracing *opinio juris* in National Cyber Security Strategy Documents (NATO CCDCOE, 2018) tillgänligt på https://ccdcoe.org/uploads/2019/01/Tracing-opinio-juris-in-NCSS-2.docx.pdf , (hämtad 23-12-21)