



UiT Norges arktiske universitet

Det juridiske fakultet

Den folkerettslige stillingen til internasjonal spionasje, med et særlig fokus på cyberspionasje

Bendik Breivik Gran

Masteroppgave i rettsvitenskap, JUR-3902, desember 2022

Innholdsfortegnelse

1	Innledning.....	1
1.1	Oppgavens tema, bakgrunn og aktualitet	1
1.2	Folkerettslig metode og rettskildebildet	2
1.3	Avgrensninger og veien videre.....	6
2	Spionasje i det 21. århundre	8
2.1	Cyberspionasje.....	9
3	Folkerettens overordnede stilling til spionasje.....	11
3.1	Tillatelse foreligger ved mangel på forbud.....	11
3.2	Spionasje i lys av suverenitetsprinsippet	12
3.3	Spionasje i lys av prinsippet om ikke-intervensjon	15
3.3.1	Nicaragua v. United States of America.....	16
3.4	Spionasje som forebyggende selvforsvar	17
3.5	Eksisterer det sedvanerett som tillater spionasje?	19
3.6	Er spionasje i fredstid et internrettslig problem?.....	22
4	Den folkerettslige stillingen til spesifikke spionasjeformer	23
4.1	Spionasje utført med lovlig inntreden på territoriet.....	23
4.2	Spionasje utført uten lovlig inntreden på territoriet.....	24
4.3	Spionasje fra luft- og verdensrom	25
4.3.1	Spionasje i luftrommet utført av statlige flyfartøy	25
4.3.2	Spionasje i luftrommet utført av sivile flyfartøy	27
4.3.3	Spionasje fra verdensrommet	28
4.4	Cyberspionasje.....	29
4.4.1	Ekstraterritoriell cyberspionasje.....	29
4.4.2	Transnasjonal cyberspionasje.....	30
4.4.3	Økonomisk cyberspionasje	31
5	Diplomatisk spionasje	34

5.1	Persona non grata.....	35
5.2	Diplomatisk immunitet etter oppdragets opphør	36
5.3	Oppsummering av diplomatisk spionasje.....	37
6	Internasjonal humanitærrett.....	38
6.1	Cyberspionasje i lys av den internasjonale humanitærretten.....	41
7	Cyberspionasje tilknyttet ikke-statlige entiteter	42
7.1	Staters handleplikt innenfor sin egen jurisdiksjon.....	42
8	Avsluttende bemerkninger – er det et behov for en folkerettslig regulering av spionasje?	45
	Referanseliste	46

1 Innledning

1.1 Oppgavens tema, bakgrunn og aktualitet

Bruken av spionasje for å oppnå en fordel for sin egen stat, organisasjon eller annen gruppering strekker seg tilbake flere årtusener. Fra oldtidens historie illustreres betydningen av spionasje for krigføring godt av Sun Tzu: «So it is said that if you know others and know yourself, you will not be imperiled in a hundred battles».¹

Slik spionasje som sitatet sikter til er av en fysisk variant, og kan defineres som samling eller forsøk på samling av informasjon i territorium kontrollert av en motpart, gjennom handlinger utført på en bevisst hemmelig måte, eller under falske forutsetninger.²

Informasjonskrigen som blir beskrevet av Sun Tzu er enda mer aktuell den dag i dag. Spionasje har via teknologisk utvikling, gått over fra den tradisjonelle definisjonen til å også bli utøvd digitalt, såkalt cyberspionasje. Cyberspionasje «refers to any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information».³ Utviklingen har medført at stater har blitt mer sårbare for spionasje enn de var før den digitale revolusjonen.⁴

Det sentrale å poengtere ved definisjonene for både ordinær spionasje og cyberspionasje er at det er den fordekte siden av handlingene som *aktualiseres*. Handlingene tar sikte på å bli gjennomført i det skjulte, eller under falske forutsetninger. Det er også en viktig forskjell, spionasjedefinisjonen knytter seg til et fysisk område, mens en slik begrensning ikke gjelder for cyberspionasje.

Digital spionasje blir gjennomført i cyberspace.⁵ Cyberspace kan være vanskelig å definere, da det er uklart i hvor stor utstrekning de fysiske komponentene som danner rommet skal inkluderes. Denne oppgaven vil støtte seg på følgende definisjon: «The environment formed

¹ Tzu, Sun (1988) s. 82

² Henckaerts og Doswald-Beck (2005) (heretter ICRC) s. 390.

³ Schmitt (2017) (heretter Tallinn-manualen) regel 32 punkt 2.

⁴ Prop.80 L (2019-2020) Lov om Etterretningstjenesten, s. 15 (kapittel 3).

⁵ Cyberspace og IKT (Informasjons- og kommunikasjonsteknologi) vil brukes om hverandre.

by physical and non-physical components to store, modify, and exchange data using computer networks».⁶

Utgangspunktet i folkeretten er at ved fravær av et forbud, kan stater handle slik de måtte ønske.⁷ Det er noe uklart hvorvidt folkeretten som den eksisterer den dag i dag har noe forbud mot staters spionasje. Sitatet til Sun Tzu gir kanskje svaret på hvorfor rettstilstanden er uavklart. Å ha et innblikk i andre staters operasjoner og interesser kan være konfliktdempende, selv om du vet at du blir utsatt for det samme.⁸

Siktemålet med oppgaven er å analysere hvilken rettslig stilling internasjonal spionasje har *de lege lata*. Å fastslå om handlinger utgjør et folkerettsbrudd har stor betydning, da stater kun kan iverksette mottiltak dersom det blir utført rettsstridige handlinger mot staten.⁹

1.2 Folkerettslig metode og rettskildebildet

Temaet for oppgaven ligger innenfor folkeretten, hvor den juridiske metoden skiller seg fra den vi kjenner fra det nasjonale norske systemet. Det eksisterer ulikheter både i hva som kan benyttes som rettskilder, samt hvilken vekt ulike rettskilder kan tillegges.

Førende for hva som utgjør rettskilder, og hvilken vekt de skal tillegges, er statuttene til Den Internasjonale Domstol art. 38 (1) (a)-(c).¹⁰ Alle FNs medlemsstater er ved sitt medlemskap i FN også part til domstolen.¹¹ Statuttene hjemler traktater, folkerettslig sedvanerett og alminnelige rettsprinsipper som primære rettskilder. Rettspraksis og juridisk teori utgjør subsidiære kilder.¹² Med alminnelige rettsprinsipper siktes det til generelle normer man finner i de fleste nasjonale rettssystemer, slik som god tro og dommeres uavhengighet.¹³

⁶ Schmitt (2017) s. 564.

⁷ Punkt 2.2.

⁸ Buchan (2019) s. 30-31.

⁹ UNGA, ILC, Articles on State Responsibility A/56/10, november 2001, art. 49; Schmitt (2017) regel 20 avs. 1.

¹⁰ Statute of the International Court of Justice, 26. juni 1945 (in force 24. oktober 1945) (ICJ-statuttene).

¹¹ Charter of the United Nations, 26. juni 1945 (in force 24. oktober 1945), (FN-Pakten) art. 93 punkt 1; Statene må i tillegg ha godtatt jurisdiksjonen til domstolen.

¹² ICJ-statuttene art. 38 punkt 1 bokstav a-d.

¹³ Ruud og Ulfstein (2018) s. 82.

ICJ-statuttene har kun direkte bindende virkning for domstolen. Innholdet i artikkel 38 er imidlertid ansett for å gi uttrykk for rettskildefaktorerens relevans og vekt generelt for folkeretten, og er derfor sentral for oppgavens fremstilling.¹⁴

Traktater er avtaler som inngås mellom folkerettssubjekter.¹⁵ I motsetning til i det norske rettssystemet utgjør avtaler i folkeretten en rettskilde og ikke faktum.¹⁶ Oppgaven vil berøre en rekke slike avtaler, men av særskilt interesse er FN-pakten, som vil bli drøftet inngående senere.

Hvordan traktater skal tolkes er regulert gjennom Wien-konvensjonen om traktatretten art. 31-33.¹⁷ Konvensjonen reflekterer for det meste folkerettslig sedvanerett, og er dermed bindende også for land som ikke er part til avtalen.¹⁸ Mest sentralt står art. 31 første ledd, som slår fast at traktaters innhold skal tolkes i god tro gitt den naturlige språklige forståelsen av traktatens innhold, sett i kontekst av traktaten som en helhet.

Art. 33 tar for seg tilfeller hvor traktater er autentisert på mer enn ett språk. Oversatte traktater utgjør ikke autorative kilder, med visse unntak.¹⁹ De traktater oppgaven berører er gjennomgående autentisert på engelsk, men ikke norsk, og engelske versjoner vil derfor bli benyttet. Andre offisielle språkversjoner eksisterer for de fleste avtalene oppgaven berører, men av hensiktsmessighetsgrunner vil kun engelske utgaver bli brukt. Eventuelle språklige nyanseforskjeller mellom versjonene vil derfor ikke kunne hensyntas.²⁰

Folkerettslig sedvanerett er en primærkilde etter ICJ-statuttene. Vurderingsmomentene for om en sedvanerett eksisterer er om det foreligger «evidence of a general practice accepted as law».²¹ Kravet om «general practice» kan ses som et objektivt krav om statspraksis, hvor

¹⁴ Ruud og Ulfstein (2018) s. 71.

¹⁵ Oppgaven vil bruke begrepene «traktat», «konvensjon» og «avtale» om hverandre.

¹⁶ Helmersen (2014) s. 24 (e-bok).

¹⁷ Vienna Convention on the Law of Treaties, 23. mai 1969 (in force 27. januar 1980) (VCLT); Art. 32 berøres ikke i oppgavens videre innhold, og gås derfor ikke nærmere inn på.

¹⁸ Helmersen (2014) s. 25 (e-bok); Det kan være enkeltbestemmelser i traktaten som ikke har vært vurdert av ICJ, men innholdet i art. 31-33 reflekterer utvilsomt folkerettslig sedvanerett.

¹⁹ Se Wien-konvensjonen art. 33 punkt 2.

²⁰ VCLT art. 33.

²¹ ICJ-statuttene art. 38 punkt 1 bokstav b.

praksisen må ha vært «extensive and virtually uniform».²² Kravet om «accepted as law», eller *opinio juris*, blir subjektivt, og krever «evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it.»²³

Folkerettslig sedvanerett har stor betydning for oppgaven. Etablerte og anerkjente normer vil være viktige, men det vil også bli vurdert om det eksisterer handlemåter og tankesett som kan gi uttrykk for at det sedvaneretten endrer seg.

Rettslig teori er etter ICJ-statuttene en subsidiær rettskilde.²⁴ I motsetning til ved norske domstoler, hvor juridisk litteratur i stor grad siteres og argumenteres med, vises det veldig sjeldent til teori i ICJ sine flertallsavgjørelser.²⁵ Mangelen på direkte henvisninger er derimot noe misvisende, da dissenser og særvtum fra enkelte dommere ofte vil referere til teorien for sine standpunkter.²⁶

Tallinn-manualen er et sentralt verk for folkerettens stilling i cyberspace, og vil bli benyttet i stor grad for oppgavens fremstilling. Manualen er imidlertid et akademisk verk, og innholdet har derfor ikke noen formell rettslig vekt. Ekspertgruppen og øvrige bidragsytere er videre i stor grad tilknyttet NATO og vestlige land.²⁷ Det kan dermed ikke forutsettes at den reflekterer synet i for eksempel Kina og Russland på alle områder.

Grunnet mangelen på primære kilder som behandler den rettslige stillingen til internasjonal spionasje, vil subsidiære kilder spille en stor rolle. Hvilken vekt rettslig teori skal gis vil avhenge av argumentasjonens godhet og overbevisningsevne.²⁸

Den mest sentrale domstolen for oppgaven er Den Internasjonale Domstol.²⁹ Domstolen, som er et FN-organ, avsier utelukkende rådgivende uttalelser og avgjørelser tilknyttet tvister

²² Ruud & Ulfstein s. 77; North Sea Continental Shelf Cases, Judgment, I.C.J. Reports 1969 s. 3 (Nordsjø-saken) s. 43, premiss 74.

²³ Ruud og Ulfstein s. 77; Nordsjø-saken s. 44, premiss 77.

²⁴ ICJ-statuttene art. 38 punkt 1 bokstav d.

²⁵ Ruud og Ulfstein (2018) s. 84.

²⁶ Helmersen (2021) s. 45.

²⁷ Schmitt (2017) s. xii-xiix.

²⁸ Ruud og Ulfstein (2018) s. 84.

²⁹ The International Court of Justice (heretter ICJ).

mellom statsmakter.³⁰ Domstolen, forutsatt at den har jurisdiksjon, har kompetanse i alle saker relatert til traktatstolkning, folkerettslige spørsmål, eksistensen av og brudd på internasjonale forpliktelser, og erstatningsansvar ved påviste brudd.³¹

Det eksisterer per dags dato ingen internasjonale avgjørelser som stadfester spionasjehandlinger som et brudd på suverenitetsprinsippet.³² Mangelen på avgjørelser kan sannsynligvis forklares av blant annet staters generelle tilbakeholdenhet i å bringe tvister inn for domstolene.³³ Rettspraksis som berører beslektede rettsområder, slik som grensedragninger for suverenitets- og ikke-intervensjonsprinsippet vil derfor være av stor interesse for oppgaven.

Kompetansen til Sikkerhetsrådet følger av FN-pakten art. 24-26. Artikkelen 24 hjemler Sikkerhetsrådets viktigste ansvar, opprettholdelse av fred og sikkerhet i verden, med videre henvisninger til hvilke virkemidler Rådet kan benytte seg av. Artikkelen 25 fastsetter Sikkerhetsrådets adgang til å treffe bindende vedtak for FNs medlemsstater. Slike vedtak vil etter art. 103 ha forrang ved motstrid med en annen folkerettslig forpliktelse en medlemsstat måtte ha.³⁴ Resolusjoner fra Sikkerhetsrådet som berører tematikken for oppgaven vil dermed være av stor interesse.

Resolusjoner fra Generalforsamlingen og Sikkerhetsrådet har rettskildemessig vekt med bakgrunn i FN-Pakten. Generalforsamlingen består av representanter fra alle FNs medlemmer.³⁵ Generalforsamlingen kan i motsetning til Sikkerhetsrådet ikke treffe bindende vedtak, men de kan gi rådgivende uttalelser.³⁶ Sikkerhetsrådet behandler saker som

³⁰ ICJ-statuttene kapittel IV; ICJ-statuttene art. 34 punkt 1.

³¹ ICJ-statuttene art. 36 punkt 2 bokstav a-d.

³² Det Kongelige Utenriksdepartement, «Folkerettslige rammer for grenseoverskridende informasjonsinnhenting», (29. mai 2015), s. 3, <https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/2.pdf> (lest 15. november 2022).

³³ Ruud og Ulfstein (2018) s. 84.

³⁴ Art. 103 regulerer etter sitt innhold kun avtalebaserte forpliktelser, men er forstått til å også gjelde for sedvanerettslige forpliktelser, jf. Simma (2002) s. 1298-1299.

³⁵ FN-Pakten art. 9; Se motsatt art. 17, 19, 90 og 96.

³⁶ Helmersen (2014) s. 75 (e-bok).

omhandler internasjonal fred og sikkerhet, mens Generalforsamlingens virkeområde er bredere, og den kan etter art. 10 behandle alle saker innenfor FN-Paktens virkeområde.

Vedtakene er ikke bindende, men de er sentrale ved at de ofte reflekterer sedvaneretten for det aktuelle rettsområdet, eller at de bidrar til etableringen av slik rett.³⁷ Generalforsamlingens resolusjoner utgjør altså ingen primærkilde innenfor folkeretten, men kan bidra til å belyse hva som er den faktiske rettstilstanden.

1.3 Avgrensninger og veien videre

Oppgaven er positivt avgrenset til å behandle spionasje. Avgrensningen vil omfatte operasjoner som går over fra spionasje, til å utgjøre angrep på eller forsøk på innflytelse på en annen stats jurisdiksjon. Hvor en slik grense går vil bli behandlet.

Videre knytter oppgaven seg til det folkerettslige plan. Nasjonale regler og domsavgjørelser vil ikke vies oppmerksomhet direkte, men kan bli trukket frem for å belyse hvilken statspraksis og *opinio juris* som eksisterer.

Oppgaven knytter seg til de internasjonale relasjonene mellom statsmakter. Det vil derfor avgrenses mot individers rettigheter i møte med spionasje; menneskerettigheter kan potensielt sette begrensninger for staters spionasjehandling, men dette vil det ikke tas nærmere stilling til.

De folkerettslige følgene av eventuelle konklusjoner vil ikke bli vurdert i oppgaven. Det sentrale er utelukkende å redegjøre for hvilken folkerettslig stilling spionasje har i det internasjonale samfunnet. Hvilke mulige rettsmidler en stat som blir dømt for en rettsstridig bruk av spionasje overfor en annen statsmakt, kan bli møtt med, faller dermed utenfor oppgavens tema.

Oppgaven vil i kapittel 2 gi en sammenfatning av hvordan fysisk og digital spionasje gjennomføres i dag. Det vil trekkes frem ulike former for spionasje som det er aktuelt for oppgaven å se nærmere på.

³⁷ UNGA Res. 3232 (XXIX) 12. november 1974; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996 s. 226 (Atomvåpensaken) s. 254-255 premiss 70.

Det vil i kapittel 3 ses nærmere på folkerettens overordnede syn på spionasje i fredstid på et generelt plan. Kapittel 4 vil se nærmere på visse spionasjeformer mer spesifikt. Kapittel 5 og 6 vil ta for seg tematiske spionasjeformer, henholdsvis diplomati og internasjonal humanitærrett. Kapittel 7 vil se nærmere på spionasje som involverer ikke-statlige aktører. Kapittel 8 vil ta for seg avsluttende bemerkninger tilknyttet behovet for en mer konkret regulering.

2 Spionasje i det 21. århundre

Det er nærliggende for den videre fremstilling å først redegjøre for hvilket innhold og hvilke handlinger som faller innenfor spionasjebegrepet, for å slik skape en ramme for oppgavens fortsettelse. Overordnet knytter oppgaven seg til spionasje som gjennomføres av statsmakter, eller som kan knyttes til en stat.³⁸ For de tilfeller hvor handlingsutøveren ikke opererer på vegne av en stat vil det bli foretatt en separat drøftelse i kapittel 7.

Hensikten bak spionasje er å erververe informasjon. Det skjulte eller falske grunnlaget handlingene innehar er også sentralt, for eksempel vil ikke en væpnet aksjon som har som formål å samle informasjon om en stats kritiske infrastruktur være spionasje. Det kan formuleres som at to kumulative vilkår må være til stede; (i) siktemålet med handlingen er informasjonservervelse av beskyttet informasjon og (ii) handlingen utøves på hemmelig eller falskt grunnlag.

Informasjonen som blir ervervet må være omfattet av en viss form for beskyttelse. Om det ikke er snakk om hemmeligheter, men allment tilgjengelig informasjon, vil det ikke være snakk om en spionasjehandling. Illustrerende er den norske strafferettslovgivningen, som når det kommer til etterretningsvirksomhet kun er straffbart for virksomhet mot «statshemmeligheter».³⁹

Mulighetene til å bedrive spionasje har økt i tråd med verdens teknologiske utvikling. Fra å måtte fysisk befinne seg på en fremmed stats territorium for å innhente informasjon, kan den samme jobben nå gjøres fra verdensrommet, eller fra et kontor med aircondition på den andre siden av kloden. Kretsen som man spionerer på, og som gjensidig spionerer på en selv, har også utvidet seg i takt med denne utviklingen.

Selv om digitale fremskritt har gitt stater et større handlingsrom i forbindelse med hvordan de bedriver spionasje, spiller fysiske metoder fortsatt en sentral rolle. Som eksempel kan nevnes siktelsen mot den antatt russiske statsborgeren Mikhail Mikusjin, som oppholdt seg som

³⁸ For hvilke handlinger som kan tilskrives statsmakter se UNGA, ILC, Draft Articles on Responsibility of States for Internationally Wrongful Acts, A/56/83, 12. desember 2001, art. 4-9.

³⁹ Lov 20. mai 2005 nr. 28 om straff §§ 121 og 122.

gjesteforsker ved UiT.⁴⁰ Norge utfører også etterretning i andre stater, noe som ble synliggjort ved Frode Bergs domfellelse i Russland i 2019.

De fysiske og digitale sidene kan utgjøre forskjellige aspekter ved én og samme spionasjehandling. For eksempel vil det for et lukket datasystem kunne behøves fysisk tilstedeværelse for å oppnå tilgang, men hvor en slik oppnådd tilgang deretter kan medføre at den lagrede informasjonen kan sendes ut av systemet digitalt.

2.1 Cyberspionasje

Cyberoperasjon brukes ofte som en samlebetegnelse på en rekke ulike handlinger som blir utført i cyberspace. Skillet mellom cyberspionasje og øvrige cyberoperasjoner kan forklares ved de fysiske konsekvenser operasjonen har for det infiltrerte nettverket. Hvor noen cyberoperasjoner kan gå ut på å skade nettverket, søker cyberspionasje snarere å hente ut relevant informasjon uten å bli oppdaget.

Cyberspionasje kan gjennomføres i de tre ulike lagene av cyberspace.⁴¹ Det *fysiske*, som utgjør de fysiske komponentene til et nettverk; datamaskiner, kabler, servere og lignende. Det *logiske*; koblingene som gjør utvekslingen av informasjon mellom ulike nettverk og komponenter mulig. Det *sosiale*; individene og gruppene som er involvert i aktiviteter i cyberspace.

Området cyberspionasje blir utført fra er også relevant. Det typiske tilfellet en ser for seg er infiltrering av servere lokalisert i en annen stat, såkalt *ekstraterritoriell* spionasje. Spionasje kan også gjennomføres uten tilgang til slike servere, ved å plukke opp signaler som strekker seg inn på ens eget territorium, eller på vei til og fra satellitter i verdensrommet. Slik spionasje vil bli referert til som *transnasjonal* spionasje.

Det kan tenkes situasjoner som vil ha innslag av både skade og spionasje. En stat hacker seg inn i nettverket tilknyttet forsvarssystemene til en annen stat for å få hentet ut informasjon om systemene, og laster samtidig opp skadelig programvare for å skjule sine spor. Staten har hentet ut hemmelig informasjon, men har i prosessen også skadet sentrale

⁴⁰ Torkell J. Trædal m.fl., «PST har siktet gjesteforskeren i Tromsø for spionasje. Han nekter straffskyld.», Aftenposten, 28. oktober 2022, <https://www.aftenposten.no/norge/i/763Kpo/pst-har-siktet-gjesteforskeren-i-tromsoe-for-spionasje-han-nekter-straffskyld> (lest 31. oktober 2022).

⁴¹ Schmitt (2017) regel 1 punkt 3.

forsvarssystemer. Slik aktualiseres et spørsmål om operasjonen skal ses som en samlet handling, eller om skadeverket og spionasjen må vurderes separat.

Det er de reelle forholdene som her er avgjørende. Stater kan ikke gjemme seg bak termen cyberspionasje for å gjøre cyberoperasjoner av en mer inngripende art rettmessige.⁴²

Hensikten og følgene av en operasjon må i hvert enkelt tilfelle vurderes konkret for å avgjøre hvorvidt det har forekommet brudd på folkerettslige forpliktelser.

⁴² Schmitt (2017) regel 32 punkt 6 og 12.

3 Folkerettens overordnede stilling til spionasje

Det eksisterer tre forskjellige akademiske syn på den rettslige stillingen til spionasje i fredstid. Spionasje kan ses på som tillatt, forbudt eller ikke regulert. I praksis så er det kun relevant å ta stilling til hvorvidt en handling er forbudt eller ikke. Virkningen av at en handling klassifiseres som enten tillatt eller ikke regulert er identiske.

3.1 Tillatelse foreligger ved mangel på forbud

Retningsgivende for hva som er tillatt i folkeretten ved mangel på rettslig regulering er Lotus-prinsippet. Prinsippet er oppkalt etter en dom mellom Frankrike og Tyrkia, fra den tidligere Permanent Court of International Justice.⁴³ Prinsippet hjemler stater frihet til å utøve de handlinger de måtte ønske, så lenge handlingene ikke er dekket av et eksplisitt forbud.⁴⁴

Prinsippet anses i dag å utgjøre folkerettslig sedvanerett, da det blant annet er fulgt opp i en rådgivende uttalelse fra ICJ relatert til Kosovos uavhengighetserklæring av 17. februar 2008.⁴⁵ Domstolen konkluderte med at erklæringen ikke brøt med internasjonal rett, og at den derfor var gyldig.⁴⁶ Prinsippet blir aldri uttrykkelig referert til i flertallsvotumet, men det fremstår klart fra dommens innhold, samt fra dommer Simmas særvotum, at prinsippet var styrende for domstolens konklusjon.⁴⁷

Dommer Simma utgjorde en del av flertallet i Kosovo-uttalelsen, men retter i sitt særvotum kritikk mot domstolens anvendelse av Lotus-prinsippet. Han inntok standpunktet at kvaliteten til uttalelsen var svekket av et for snevert perspektiv, og for mekanisk fremgangsmåte.⁴⁸ Kritikken er av teoretisk interesse, men endrer ikke nevneverdig på vekten av flertallsvotumets syn på prinsippet.

Stater kan altså fritt gjennomføre handlinger som ikke strider mot gjeldende folkerett. Som nevnt tidligere i oppgaven eksisterer det ikke noen direkte regulering av spionasjes lovlig-

⁴³ The case of the S.S. "Lotus" 7. september 1927, PCIJ Reports Serie A nr. 10 (Lotus-saken).

⁴⁴ Lotus-saken s. 18 og 19.

⁴⁵ Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, I.C.J. Reports 2010 s. 403 (Kosovo-saken).

⁴⁶ Kosovo-saken s. 53 og 54 premiss 122 og 123.

⁴⁷ Kosovo-saken (Declaration of Judge Simma) s. 79 premiss 2.

⁴⁸ Kosovo-saken (Declaration of Judge Simma) s. 82 premiss 10.

eller ulovlighet. Det er derfor nærliggende å se på folkerettslige regler som er av mer overordnet karakter. Suverenitetsprinsippet står her sentralt.

Det har vokst frem en enighet om at internasjonal lov, samt suverenitet og dets avlede normer og prinsipper, også er gjeldende i cyberspace.⁴⁹

3.2 Spionasje i lys av suverenitetsprinsippet

Suverenitetsprinsippet utgjør kjernen i folkeretten, og gjelder som folkerettslig sedvanerett.⁵⁰

Den mest anerkjente definisjonen stammer fra Island of Palmas-saken fra 1928,

«[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State».⁵¹

I prinsippet ligger det at alle stater er suverene og uavhengige, det er staten selv som regulerer og styrer sine indre anliggender, ikke ytre makter.⁵² Handlinger fra andre statsmakter som forhindrer utøvelsen av disse privilegiene, vil være et inngrep i suverenitetsprinsippet, og dermed et brudd på folkeretten.

Prinsippet gjelder ikke absolutt. Staters suverenitet innebærer at de også kan avtale begrensninger i dens utstrekning. Tilknytningen til mellomstatlige organisasjoner som EU og FN er en overføring av deler av staters suverenitet.⁵³ Inngrep i prinsippet kan også skje gjennom fremveksten av folkerettslige sedvaner. Sedvaner kan sette føringer for staters opptreden uten noen eksplisitt aksept eller tiltredelse av praksisen.⁵⁴

⁴⁹ UNGA, «Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security», 24. juni 2013, UN Doc A/68/98 avs. 19-20. Fulgt opp av samme gruppe i 2015; 22. juli 2015, UN Doc A/70/174 avs. 28 (b).

⁵⁰ Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment, I.C.J. Reports 1986 (Nicaragua-saken) s. 123 premiss 263.

⁵¹ Island of Palmas (Neth. v. U.S.) (1928) 2 RIAA 829, s. 838.

⁵² Ruud og Ulfstein (2018) s. 21.

⁵³ Rose m.fl. (2020) s. 4; Forpliktelser som følger av tiltredelse til mer generelle avtaler vil også utgjøre en overføring av suverenitet, om ikke i like stor grad.

⁵⁴ UNGA, ILC, Draft conclusions on identification of customary international law: with commentaries, A/73/10, 2018, s. 140 konklusjon 10 punkt 3.

Den ene delen av prinsippet er likeverdighet. Ved likeverdighet mellom stater siktes det til deres likestilte plass i det internasjonale rettssystemet.⁵⁵ Stater vil naturligvis ha forskjellig reell makt og innflytelse, men de iboende rettighetene en stat innehar i kraft av å være suveren gjelder uavhengig av innbyggertall, økonomi og størrelsen på territoriet. Likeverdigheten til stater er kodifisert i FN-Pakten art. 2 (1).

Definisjonen fra Island of Palmas-saken gir uttrykk for den andre av suverenitetsprinsippet to deler, uavhengighet, også omtalt som territoriell suverenitet. Territoriell suverenitet er ofte sett på som den interne retten til selvbestemmelse, og den eksterne plikten til ikke-intervensjon.⁵⁶ Plikten til å ikke-intervenere i andre staters rett til selvbestemmelse vil drøftes under punkt 3.3.

For fysisk spionasje er det vanligvis relativt enkelt å slå fast om handlingene har vært utført innenfor et område som en stat har territoriell suverenitet over. Cyberspionasje skiller seg fra fysisk spionasje, ved at handlingen typisk utføres fra utenfor territoriet til den utsatte stat. Innholdet i den territoriale suvereniteten til stater står derfor sentralt for oppgaven.

Hvorvidt spionasje utgjør et brudd på suverenitetsprinsippet, er det i teorien og i statspraksis uenighet om. Uenigheten blir enda tydeligere når man begynner å dele opp spionasje i forskjellige undergrupper. Flere anerkjente forfattere innen internasjonal rett fra det forrige århundret uttalte seg om spionasjes folkerettslige stilling, med klart forskjellige synspunkter.

Professoren Quincy Wright mente at spionasje, eller hvilken som helst annen form for nasjonalt lovstridig penetrering av en stats territorium, utgjør et folkerettslig brudd på plikten til å respektere staters territoriale integritet og politiske uavhengighet.⁵⁷ Oppenheim anså derimot at det ikke var noe som hindret spionasje i fredstid, verken moralitet, politikk eller lovverk.⁵⁸ Demarest går ikke like langt som Oppenheim, han ser det som en uvennlig handling, men ikke et brudd på internasjonal rett.⁵⁹

⁵⁵ Rose m.fl. (2020) s. 2; Crawford (2019) s. 433.

⁵⁶ Shaw (2021) s. 194; Crawford (2019) s. 431.

⁵⁷ Wright (1962) s. 12.

⁵⁸ Oppenheim (1912) s. 511

⁵⁹ Demarest (1996) s. 347.

De nevnte akademikernes vurderinger ble gjort før fremveksten av internett og adgangen til å bedrive cyberspionasje. De relaterer seg dermed utelukkende til spionasje utført fysisk på en annen stats territorium.

Ekspertgruppen bak Tallinn-manualen uttaler på sin side at det ikke eksisterer noe generelt forbud mot spionasje, men at spionasjehandlinger likevel kan resultere i et brudd på internasjonal lov.⁶⁰ Det avgjørende er i deres øyne om et aspekt ved operasjonen bryter med anerkjent internasjonal rett.

Ekspertgruppen er derimot delt når det kommer til hvilke regler som kan komme til anvendelse, og hvilke typer handlinger som vil utgjøre brudd.⁶¹ Det er uenighet både relatert til betydningen av alvorlighetsgraden til cyberspionasjehandlinger og hvorvidt prinsippene om suverenitet og ikke-intervensjon er anvendelige ved spionasje.⁶²

Ett mindretall inntok standpunktet at cyberspionasje kan nå en alvorlighetsgrad som medfører et brudd på suverenitetsprinsippet, og viser spesifikt til ervervelsen av utskytningskoder til atomvåpen. Et annet mindretall mente omvendt at spionasjehandlinger utgjør et generelt unntak fra reglene om suverenitet og ikke-intervensjon.

Flertallet viste for det første punktet til at alvorlighetsgraden er ubetydelig, da mindretallets syn ikke reflektere gjeldende rett. For det andre punktet viste flertallet til at brudd på suverenitetsprinsippet kan forekomme ved å plante en USB-pinne i en datamaskin lokalisert på territoriet til en annen stat. Det bærende for flertallets syn var her ikke spionasjen i seg selv, men at handlingen foregikk på en annen stats territorium uten tillatelse.

Betydningen av staters territorielle integritet belyses godt av eksempelet i Tallinn-manualen. Flertallet av Tallinn-gruppen virker å støtte Wright sitt syn, om at spionasje er et brudd på staters territorielle integritet, hvis agenten blir sendt inn i en annen stat på falskt grunnlag.⁶³ Prinsippet om ikke-intervensjon er et annet grunnlag for at spionasje kan være en rettsstridig handling.

⁶⁰ Schmitt (2017) regel 32 punkt 6.

⁶¹ Schmitt (2017) regel 32 punkt 8 og 9.

⁶² Det er vanskelig å si noe håndfast om graden av uenighet, da manualen kun opererer med mindretall/flertall, ikke brøker.

⁶³ Se også Delupis (1984) s. 67.

3.3 Spionasje i lys av prinsippet om ikke-intervensjon

Prinsippet om ikke-intervensjon, eller forbudet mot intervensjon, er en folkerettslig sedvanerettsregel som gir suverene stater rett til å styre sine indre anliggender uten ekstern involvering.⁶⁴ Det kan utledes fra kodifiseringen av suverenitetsprinsippet i FN-Paktens art. 2 punkt 1.⁶⁵ Forbudets innhold er blant de mest uklare og omdiskuterte deler av folkeretten.⁶⁶

Tidligere ble forbudet mot intervensjon kun ansett å utgjøre et forbud mot maktbruk mellom stater, men innholdet er blitt betydelig utvidet gjennom blant annet Generalforsamlingens Friendly Relations Declaration av 1970, og Nicaragua-saken.⁶⁷ Forbudet mot bruk av makt kan i dag ses som en spesifikk anvendelse av prinsippet om ikke-intervensjon.⁶⁸ Maktanvendelsesforbudet fremgår av FN-Pakten art. 2 punkt 4.

Det vil i oppgaven ikke bli tatt nærmere stilling til hva som utgjør bruk av makt. Det fremstår som klart ut ifra dagens regel at spionasjehandlinger ikke vil kvalifisere til å utgjøre bruk av makt. Forbudet mot makt vil derfor i den videre fremstilling kun bli tatt stilling til for å belyse grensedragningene for prinsippet om ikke-intervensjon.

Generalforsamlingens deklarasjon slår fast at ulovlig intervensjon foreligger ved direkte eller indirekte innblanding, «for any reason whatever», i en stats interne eller eksterne anliggender.⁶⁹ Det samme gjelder ved forsøk på å underkaste seg muligheten til å styre en annen stats suverene rettighet, eller oppnå en hvilken som helst fordel, ved bruk av økonomiske, politiske eller andre tvangsmidler.⁷⁰

Deklarasjoner fra Generalforsamlingen er som nevnt tidligere ikke bindende. ICJ har derimot uttalt at innholdet i denne deklarasjonen gir uttrykk for det sedvanerettslige innholdet i forbudene mot intervensjon og bruk av makt.⁷¹ Domstolen viser i Nicaragua-saken til at

⁶⁴ Nicaragua-saken s. 96 premiss 202.

⁶⁵ Helmersen (2014) s. 123 (e-bok).

⁶⁶ Ruud & Ulfstein (2018) s. 198; Schmitt (2017) regel 66 avs. 6.

⁶⁷ Ruud og Ulfstein (2018) s. 198-199; UNGA Res 2625 (XXV) 24. oktober 1970.

⁶⁸ Jamnejad og Wood (2009) s. 348-349.

⁶⁹ UNGA Res 2625 (XXV) 24. oktober 1970, prinsipp c 1. avs.

⁷⁰ UNGA Res 2625 (XXV) 24. oktober 1970, prinsipp c 2. avs.

⁷¹ Nicaragua-saken s. 89-90 premiss 188.

deklarasjonen er en selvstendig rettskilde, den kodifiserer innholdet i de sedvanerettslige reglene, og er gjeldende også uavhengig av FN-Paktens bestemmelser.⁷²

3.3.1 Nicaragua v. United States of America

ICJ avsa i 1986 en dom som omhandler amerikansk støtte til militære og paramilitære aktiviteter i og mot Nicaragua. USA ble dømt for å ha brutt forbudene mot intervensjon og bruk av makt ved ulike handlinger. ICJ redegjorde i saken blant annet for innholdet i forbudet mot intervensjon og maktforbudet, i tillegg til grensdragninger mellom de to reglene.

Handlingene som ble utført av USA knyttet seg kort gjengitt til et forsøk på å presse frem en regimeendring i Nicaragua. USAs trening, bevæpning og utrustning av «contra forces» ble av domstolen ansett for å utgjøre et brudd på det sedvanerettslige forbudet mot bruk av makt.⁷³ De viser videre i samme premiss at forsyningen av midler til grupperingen ikke er et brudd på maktforbudet, men utvilsomt en ulovlig intervensjon.

Intervensjon er ikke automatisk et brudd på folkeretten, stater er ikke hindret fra å samhandle med andre nasjoner. ICJ fremhever dette ved å si at en intervensjon er rettsstridig når den bruker tvangsmetoder for å påvirke valg en stat har den suverene rett til å bestemme selv.⁷⁴ Tvangselementet må i tillegg være utslagsgivende for valget. Har staten som blir presset en egeninteresse i å handle slik de blir oppfordret til, og derfor gjør det av egen fri vilje, eller den enkelt kan motstå presset, vil ikke en ulovlig intervensjon foreligge.⁷⁵

Gruppen bak Tallinn-manualen anser at tvang foreligger hvor den aktuelle handlingen har potensialet til å tvinge den påvirkede staten til å handle, eller unnlate å handle når de ellers ville gjort det.⁷⁶

Eksistensen av et slikt tvangselement taler for at spionasje aldri vil rammes av forbudet. Ved spionasje utøves det ikke noen form for tvang, målet er jo tvert imot at det helst skal gjennomføres uten oppdagelse. Det er ikke isolert sett et forsøk på å fremprovosere en endring i staten som blir spionert på, kun å samle informasjon om interne forhold.

⁷² Nicaragua-saken s. 89-90 premiss 188.

⁷³ Nicaragua-saken s. 108-109 premiss 228.

⁷⁴ Nicaragua-saken s. 98 premiss 205.

⁷⁵ Jamnejad og Wood (2009) s. 348.

⁷⁶ Schmitt (2017) regel 66 punkt 21.

Informasjonen som erverves kan naturligvis brukes som ledd i en senere tvangshandling, men det er da den påfølgende handlingen som vil utgjøre ulovlig intervensjon, ikke spionasjen.

Handlingene som USA ble dømt for utgjorde et betydelig press på den sittende nicaraguanske regjeringen. Opprørsstyrkene må antas å ha fått en betydelig fordel i sin kamp, sammenlignet med om USA ikke hadde involvert seg i konflikten. Målet var i tillegg å erstatte den sittende regjeringen med et statsstyre som USA så seg mer tjent med. Å presse frem en regimeendring er et klart brudd på forbudet.⁷⁷

Domstolen tar et forbehold i avsnittet hvor de viser til elementet av tvang, ved at de kun definerer aspekter ved prinsippet så langt det er relevant for å komme til en avklaring i den konkrete tvisten.⁷⁸ Vurderes det opp mot Generalforsamlingens deklarasjon om innblanding «for any reason whatever», så er *kanskje* døren holdt åpen også for handlinger som ikke inneholder noen form for tvangselementer.

3.4 Spionasje som forebyggende selvforsvar

Noen akademikere støtter Wright og Delupis sitt syn om at en inntreden på falskt grunnlag av en stats agent er, eller kan være, et brudd på den territorielle integritet, men viser til at det fortsatt er tillatt som en form for forebyggende (preemptive) selvforsvar.⁷⁹ Den videre drøftelse i dette underkapitlet blir gjort med en forutsetning om at spionasje utgjør et brudd på en stats territorielle integritet.

Retten til bruk av selvforsvar er kodifisert i FN-Pakten art. 51. Av bestemmelsen følger det at Pakten ikke setter begrensninger for individuelt eller kollektivt selvforsvar i møte med et væpnet angrep. Det sentrale er at det etter ordlyden kreves et *igangsatt* væpnet angrep («occurs»). Individuelt eller kollektivt må i FN-Paktens sammenheng forstås som statsmakter, altså en individuell nasjon, eller en gruppering som for eksempel NATO.

⁷⁷ Jamnejad og Wood (2009) s. 368.

⁷⁸ Nicaragua-saken s. 98 premiss 205.

⁷⁹ Sulmasy og Yoo (2007) s. 637; Baker (2004) s. 1096; Begrepsbruken på området spriker veldig, og innholdet er det ikke enighet om. «Preventive», «preemptive», «peremptory» og «anticipatory» brukes om hverandre i litteraturen.

Artikkel 51 regulerer ikke uttømmende retten til selvforsvar, den er taus når det kommer til vurderingsmomenter for utøvelse av selvforsvar, og viser tilbake til en «inherent right».⁸⁰ Selve retten må være naturlig eller iboende i kraft av å være en suveren stat, og vil dermed være av sedvanerettslig karakter.⁸¹ En slik sedvanerett eksisterer, og innholdet i retten er ansett for å komme til uttrykk i form av kriteriene i Caroline-saken.⁸²

Caroline-saken knyttet seg til britisk ødeleggelse av det amerikanske skipet «The Caroline» i 1837. I etterkant av hendelsen oppsto det korrespondanse mellom Storbritannia og USA om lovligheten av handlingen, USAs utenriksminister viste til at det må foreligge «a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment of deliberation», og hvor handlingens nødvendighet er «limited by that necessity, and kept clearly within it».⁸³ Med andre ord foreligger det et nødvendighets- og proporsjonalitetskrav.⁸⁴

Spionasje som forebyggende selvforsvar er et høyst uregulert spørsmål på et allerede uavklart rettsområde. Spørsmålet er om sedvaneretten som eksisterer i form av Caroline-kriteriene står seg separat fra FN-Pakten, ved at det eksisterer en utvidelse hvor væpnet angrep ikke er et absolutt krav for selvforsvar. ICJ har vært unnvikende i å besvare hvorvidt en slik rett til forebyggende selvforsvar kan eksistere ved siden av art. 51.⁸⁵

Akademikere som mener at vilkårene for selvforsvar er oppfylte for spionasje i fredstid viser til trusselen som terrorisme og atomvåpen representerer for verdens stater.⁸⁶ Synspunktet har meritter, i og med at det kan være vanskelig å oppdage trusler mot fred og nasjonal sikkerhet uten et innsyn i hva andre stater bedriver. Det er heller ikke snakk om en bruk av makt mot staten en spionerer mot, slik sett er det mer proporsjonalt enn militære aksjoner.

På den annen side så passer ikke sedvaneretten inn med de begrensninger som selvforsvar er underlagt etter art. 51. Etter bestemmelsen plikter stater som utnytter seg av retten til

⁸⁰ Nicaragua-saken s. 84 premiss 176.

⁸¹ Nicaragua-saken s. 84 premiss 176.

⁸² Shaw (2021) s. 993; Crawford (2019) s. 724.

⁸³ Shaw (2021) s. 993.

⁸⁴ Nicaragua-saken s. 84 premiss 176.

⁸⁵ Shah (2007) s. 100.

⁸⁶ Sulmasy og Yoo (2007) s. 637; Baker (2004) s. 1096.

selvforsvar å rapportere de utførte handlingene til Sikkerhetsrådet. Stater melder ikke inn til Sikkerhetsrådet hvilke spionasjehandlinger de til enhver tid utfører, og på hvilke områder de blir utført. Hvorfor skal en sedvanerett som eksisterer ved siden av Pakten, og som har en lavere terskel, kunne tilsidesette oppsynet Sikkerhetsrådet har med selvforsvarshandlinger som følge av et væpnet angrep.⁸⁷

Det må også nevnes at de forfatterne det er vist til som støtte for eksistensen av forebyggende selvforsvar alle er amerikanere. Deres standpunkt kan tenkes å være formet med bakgrunn i at USA etter 11. september 2001 er en av de statene som til størst grad har benyttet seg av forebyggende selvforsvar, gjennom sin «war on terror».⁸⁸

Uavhengig av hvorvidt forebyggende selvforsvar eksisterer ved siden av art. 51, kan ikke den umiddelbare nødvendigheten som Caroline-kriteriene oppstiller ses å foreligge.

Nødvendigheten av en spionasjehandling kan ikke forsvares før informasjonen man erverver faktisk er på plass. Skulle det være ansett for rettmessig, vil det uansett bare legitimere bruken av spionasje mot atommakter og stater med aktive terrorregimer på sitt territorium.

3.5 Eksisterer det sedvanerett som tillater spionasje?

Om spionasje skulle vise seg å være forbudt med grunnlag i forbudet mot intervensjon eller brudd på en stats suverenitet, så kan det likevel være tillatt med en sedvanerettslig forankring. Som nevnt kan statspraksis og *opinio juris* skape sedvanerett i og utenfor avtaleregulerte områder.⁸⁹ For spionasje kan utviklingen av sedvanerett diskuteres inngående for en rekke ulike handlinger, men grunnet plasshensyn vil det heller foretas en mer overordnet drøftelse.

Det er vanskelig å forsvare et syn om forbud mot spionasje med bakgrunn i sedvanerett. Den utbredte og langvarige praksisen til spionasje både før og etter vedtakelsen av FN-Pakten harmoniserer ikke med de oppstilte kravene til sedvanerett.⁹⁰ Det samme gjør mangelen på internasjonal fordømmelse når spioner blir fanget på ens territorium. Hvorvidt det eksisterer tillatelse i form av sedvanerett er imidlertid mer uklart.

⁸⁷ Dinstein (2017) s. 225.

⁸⁸ Crawford (2019) s. 725; Dinstein (2017) s. 222.

⁸⁹ Punkt 1.2.2.

⁹⁰ Deeks (2015) s. 305.

Mindretallet i Tallinn-manualen som anså spionasje for å utgjøre et generelt unntak fra reglene om suverenitet og ikke-intervensjon mener det eksisterer tillatelse med en sedvanerettslig forankring.⁹¹

Nordsjø-saken stilte opp kravene til en «extensive and virtually uniform» statspraksis, og «evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it».⁹² Dommen setter en meget høy standard for statspraksis sitt omfang ved etableringen av sedvanerett. Innholdet kan derimot være preget av at tvisten knyttet seg til om sedvaneretter hadde etablert seg over kort tid.⁹³

Grunnet spionasjes lange og veletablerte bruk kan det argumenteres for at terskelen vil være lavere enn det som fremgår av Nordsjø-saken. ICJ virker å ha redusert kravet noe da de i Nicaragua-saken viste til at statspraksis ikke må være «[i]n absolutely rigorous conformity» med en påstått eksisterende sedvanerett.⁹⁴ En rekke andre momenter kan også være relevante ved en praksis sin betydning, for eksempel så vil ikke en innlandsstats praksis være særlig relevant for sedvaneretter tilknyttet havområder.⁹⁵

Det eksisterer statspraksis som tilsier at en sedvanerettslig tillatelse til å bedrive spionasje eksisterer. Russland hadde tidligere overenskomster med en rekke stater som opprinnelig var underlagt Sovjetunionen, om at de ikke skulle bedrive spionasje overfor hverandre.⁹⁶ Overenskomstene tyder på at det forelå en underforstått aksept om at spionasje ville vært lovlig å utføre med mindre en avtalebegrensning eksisterte.

Staters mangel på fordømmelse når de blir utsatt for spionasjehandlinger trekker i samme retning. Hvis spionasje var uønsket i det internasjonale samfunnet, er det spesielt at det ikke har vært noen større forsøk på å regulere dets bruk.

Omfanget er også relevant, noe som ble tydeliggjort etter Edward Snowden sine avsløringer tilknyttet det amerikanske National Security Agency. Avsløringene avdekket en praksis av

⁹¹ Punkt 3.2; Schmitt (2017) fotnote 388 til regel 32 punkt 9.

⁹² Nordsjø-saken s. 43-44 premiss 74 og 77.

⁹³ Nordsjø-saken s. 43 premiss 74.

⁹⁴ Nicaragua-saken s. 88 premiss 186.

⁹⁵ Shaw (2021) s. 67.

⁹⁶ Reisman (1995) s. 421.

meget omfattende cyberspionasje mot andre stater. Det vil være naivt å tro at ikke andre stater utfører lignende handlinger, om ikke nødvendigvis av så utbredt karakter som amerikanerne.⁹⁷

På den annen side ble synet til enkelte stater fremmet etter lekkasjen. Argentina, Bolivia, Brasil, Uruguay og Venezuela presenterte en felles verbal uttalelse til FNs generalsekretær, hvor de fordømte «[t]he acts of espionage (...) that violates our sovereignty».⁹⁸ Uttalelsene tyder i det minste på at det ikke er noen uniform global oppfatning om eksistensen av en sedvanerettslig tillatelse til å bedrive spionasje på andre stater.

Videre er den fordekte naturen til spionasje et argument mot eksistensen av noen sedvanerett.⁹⁹ Det er ikke tvilsomt at spionasje blir utøvd i et stort omfang, men måtene og utstrekningen det gjennomføres på er i stor grad skjult, nettopp på bakgrunn av at målet er at det skal gjennomføres uten at det blir oppdaget.

ILC har vist til at det er «[d]ifficult to see how practice can contribute to the formation of general customary international law unless and until it has been disclosed publicly».¹⁰⁰ Stater har, med unntak av enkeltepisoder, i stor grad unngått å diskutere spionasjes stilling i det internasjonale rettssamfunnet. Mangelen på fordømmelse kan brukes som argument for spionasjen lovlighet, men også det mangler offentlig åpenhet, og er derfor et relativt svakt argument for sedvanerettslig tillatelse.

Det fremstår som at de internasjonale aktørene blir mer og mer villige til å uttrykke sine standpunkter, men det eksisterer per dags dato ikke tilstrekkelig statspraksis eller håndfast *opinio juris* til å si at noen sedvanerettslig tillatelse har oppstått. Konklusjonen er derfor at

⁹⁷ Se slik den tidligere franske utenriksministeren Bernard Kouchner, «The magnitude of the eavesdropping is what shocked us (...) Let's be honest, we eavesdrop too. Everyone is listening to everyone else», Associated Press, «Germany's Merkel: A "serious breach" if U.S. tapped her cellphone», Los Angeles Times, 23. oktober 2013, <https://www.latimes.com/world/worldnow/la-fg-wn-germany-merkel-us-cellphone-20131023-story.html> (lest 29. november 2022).

⁹⁸ Note verbale dated 22 July 2013 from the Permanent Mission of the Bolivarian Republic of Venezuela to the United Nations addressed to the Secretary-General, UN Doc A/67/946, 29. juli 2013, s. 2.

⁹⁹ Buchan (2016) s. 81.

¹⁰⁰ UNGA, ILC, Second Report on the Identification of Customary International Law, A/CN.4/672, 22. mai 2014, avs. 47.

ved mangel på stadfestelse av et konkret folkerettsbrudd for en spesifikk spionasjehandling, så er spionasje tillatt grunnet mangel på regulering, jf. Lotus-prinsippet.

3.6 Er spionasje i fredstid et internrettslig problem?

Demarest er av den oppfatning at spionasje i fredstid alltid har blitt sett på som et problem for den nasjonale rett, selv om det har en klar internasjonal side.¹⁰¹ Et slikt syn kan forsvares i den utbredte statspraksisen som eksisterer, hvor en rekke stater har lovhjemler for å bedrive spionasje.¹⁰²

Stater kan være motvillige til å hevde at spionasje er et brudd på internasjonal rett, da de selv bedriver lignende handlinger.¹⁰³ Det vil være en politisk uheldig situasjon hvis man går ut og fordømmer en annen stat internasjonalt for en handling man senere blir tatt i å gjennomføre selv. Hvis det er tilfellet, vil situasjonen i praksis bli at spionasje er internasjonalt akseptert, men nasjonalt fordømt.

Stater kan innenfor sitt eget territorium beskytte seg mot spionasje ved å innføre strafferettslig lovgivning som et avskrekkende middel. Norge har slike lovhjemler i straffeloven §§ 121-124 og 126.¹⁰⁴ De fleste av verdens stater har lignende lovhjemler, for eksempel Tyskland, Kina og USA.¹⁰⁵

De nevnte momentene kan tale for at det internasjonale samfunnet ser seg fornøyd med en rett til nasjonal håndheving av spionasjehandling. Samtidig så er det vanskelig å gjøre et slikt syn gjeldende for grenseoverskridende cyberspionasje. Å utpeke ansvarlige individer er ikke nødvendigvis mulig, og den utsatte stat kan heller ikke håndheve sin lovgivning på en annen stats territorium.

¹⁰¹ Demarest (1996) s. 330.

¹⁰² Schmitt (2017) fotnote 385 til regel 32 punkt 5, med videre henvisninger.

¹⁰³ Bowman (1995) s. 328.

¹⁰⁴ Lov 20. mai 2005 nr. 28 om straff (straffeloven).

¹⁰⁵ Tyske Strafgesetzbuch (13. november 1998) § 96; kinesiske State Security Law of the People's Republic of China (22. februar 1993) art. 4; amerikanske U.S. Code: Title 18 (25. juni 1948) § 798.

4 Den folkerettslige stillingen til spesifikke spionasjeformer

4.1 Spionasje utført med lovlig inntreden på territoriet

Typisk så vil en stats spioner forsøke å infiltrere et annet lands hemmeligheter ved å arbeide i stillinger med tilgang til sensitiv informasjon, eller arbeide opp mot andre personer som sitter i slike stillinger. Slik spionasjevirksomhet er eksemplifisert tidligere i form av Frode Berg og Mikhail Mikusjin. Spioner som Berg og Mikusjin tar seg inn på staters territorium på lovlig vis, før de deretter utfører nasjonalt lovstridig etterretning.

De som ser slik spionasje som en folkerettsstridig handling returnerer til staters territorielle integritet som grunnlaget for sitt standpunkt.¹⁰⁶ Det har utvilsomt vært en utvikling i det internasjonale miljøet siden Oppenheim uttalte at det var ingenting som hindret spionasjevirksomhet. Innholdet i staters territorielle suverenitet har blitt betydelig utvidet gjennom domsavgjørelser og resolusjoner fra FNs Generalforsamling.¹⁰⁷

Spørsmålet er om utviklingen er kommet så langt at tilstedeværelsen til et individ eller en gruppering, som på hemmelige eller falske forutsetninger planlegger å begå et nasjonalt lovbrudd på en annen stats instruks, er folkerettsstridig.

Flertallet av Tallinn-manualen, som den mest autoritative akademiske teksten på cyberspace sitt område, mener at et suverenitetsbrudd blir begått ved fysisk spionasje.¹⁰⁸ Hvilken andel av ekspertene flertallet utgjorde fremkommer derimot ikke, og synet forsvares heller ikke utenom å vise til at det er en handling begått uten samtykke på fremmed territorium.

Å anse fysiske spionasjehandling for et territorielt suverenitetsbrudd kan tenkes å være konfliktdepende. Ved å se slike handlinger som et suverenitetsbrudd, vil stater potensielt være mer tilbakeholdne med sin bruk av spioner, av frykt for mottiltak og internasjonal kritikk.

¹⁰⁶ Punkt 3.2; Se også Buchan (2019) s. 53.

¹⁰⁷ Se slik Nicaragua-saken; UNGA Res 2625 (XXV) 24. oktober 1970; UNGA Res 36/103 (9. desember 1981).

¹⁰⁸ Schmitt (2017) regel 32 punkt 9.

På den annen side er det ikke en slik tilnærming stater virker å ha tatt. Det fremstår som at fysisk spionasje i det minste er tolerert. Grunnen er sannsynligvis at plasseringen av statlige spioner er noe som krever store mengder med tid, ressurser og flaks. Muligheten er der for at de kan erverve viktig informasjon, men ikke av et slikt omfang som de mer moderne cyberspionasjeformene er kapable til.

Videre er det opp til «[t]hose who assert the existence of a rule of law restricting state activity to show such a restrictive rule exists».¹⁰⁹ Selv om visse akademikere mener at et territorielt suverenitetsbrudd finner sted, så endrer ikke det på det faktum at det som er synlig av statlige holdninger til fysisk spionasje ikke reflekterer synet.

Med statspraksis som det tyngstveiende argument, er konklusjonen at fysisk spionasje i fredstid ikke medfører et folkerettsbrudd. Det må imidlertid nevnes at rettstilstanden er særdeles uavklart, noe som er reflektert i et meget delt akademisk syn.

Det ble tidligere konkludert med at det ikke foreligger en sedvanerettslig tillatelse, spionasje utført med lovlig inntreden på territoriet er derfor å anse som ikke-regulert av internasjonal rett, og er derfor tillatt som en følge av Lotus-prinsippet.

4.2 Spionasje utført uten lovlig inntreden på territoriet

Det kan stilles opp en annen type gruppe, som på samme vis som gruppen i det foregående punktet handler på statsinitiativ, men hvor den spionutsatte staten ikke har akseptert deres inntreden på sitt territorium. Det kan listes opp en uendelig rekke med grupper og enkeltpersoner som kunne utført slike handlinger, men mest praktisk og realistisk er militære styrker.

I Costa Rica mot Nicaragua tok ICJ for seg handlinger utført av Nicaragua i grenseområdene til Costa Rica.¹¹⁰ Tvisten knyttet seg til grensedragningen mellom territoriene til statene langs San Juan-elven. I anledning tvisten hadde militært personell fra Nicaragua oppholdt seg på områder som ICJ senere konkluderte med at tilhørte Costa Rica.

¹⁰⁹ Stone (1962) s. 33.

¹¹⁰ Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua), Judgment, I.C.J. Reports 2015, s. 665 (Costa Rica mot Nicaragua).

Styrkenes plassering ble av domstolen vurdert som et brudd på Costa Ricas rett til territoriell suverenitet.¹¹¹ Det var for domstolen tilstrekkelig at styrkene fysisk hadde vært på territoriet for å konstatere brudd, noe ytterligere krav om okkupasjon eller fiendtligheter rettet mot Costa Rica forelå ikke.¹¹²

Med bakgrunn i dommen kan det konkluderes med at militære grupperinger som igangsetter spionasjehandling på territoriet til staten det blir spionert på, bryter suverenitetsprinsippet. Det er uvesentlig hvorvidt spionasjen gjennomføres fysisk eller digitalt. Tilstedeværelsen blir bærende for suverenitetsbruddet, ikke handlingen eller resultatet som ønskes oppnådd.

Det kan stilles spørsmål ved om tilstedeværelsen til andre grupperinger enn militære vil utgjøre brudd på suverenitetsprinsippet. I Costa Rica mot Nicaragua knytter dommen seg utelukkende til plasseringen av militært personell. Sannsynligvis vil spørsmålet alltid måtte besvares bekreftende. Så lenge passeringen inn i statens territorium er gjennomført uten tillatelse, og gruppen eller individet jobber på instruks fra sendemakten, vil et brudd foreligge.

4.3 Spionasje fra luft- og verdensrom

4.3.1 Spionasje i luftrommet utført av statlige flyfartøy

At suverenitetsprinsippet strekker seg opp i luftrommet over staters territorier har vært allment akseptert siden første verdenskrig.¹¹³ Det har senere blitt bekreftet en rekke ganger, blant annet av ICJ, som har vist til at grenser er separasjoner av statssuvereniteter, på likt vis i den overliggende luftsøylen som på jordens overflate.¹¹⁴

Det er også avtalefestet gjennom ICAO-konvensjonen, som slår fast at stater har eksklusiv suverenitet i luftrommet over sitt territorium.¹¹⁵ Avtalen er ratifisert av 193 stater, inkludert alle FNs medlemsstater med unntak av Liechtenstein. Etter konvensjonen er fly brukt til militær-, toll- og politiformål ansett for å utgjøre statlige luftfartøy.¹¹⁶ Den slår videre fast at

¹¹¹ Costa Rica mot Nicaragua s. 703 avs. 93.

¹¹² Costa Rica mot Nicaragua s. 704-705 avs. 97 og 99.

¹¹³ Shaw (2021) s. 463; Ruud og Ulfstein (2018) s. 26.

¹¹⁴ Frontier Dispute, Judgment, 12. juli 2005, ICJ Reports 2005, s. 142 premiss 124.

¹¹⁵ Convention on International Civil Aviation, 7. desember 1944 (in force 4. april 1947) (ICAO-konvensjonen) art. 1.

¹¹⁶ ICAO-konvensjonen art. 3 b).

ingen statlige luftfartøy skal fly over territoriet til en medkontrahent, med mindre godkjennelse foreligger.¹¹⁷

Territoriell suverenitet over luftrommet kom på spissen etter USAs U2-flyvninger over Sovjetunionen under den kalde krigen. Det ble drevet fotografering av viktige sovjetiske mål fra en høyde USA anså Sovjetunionen for å mangle de militære egenskapene til å stoppe. Ett av flyene ble likevel skutt ned, og både flyet og piloten endte opp i sovjetisk besittelse. I kjølvannet av saken ble Sikkerhetsrådet samlet.

Sovjetunionen fremmet en resolusjon som fordømte handlingene, samt kategoriserte dem som brudd på suvereniteten til staten etter FN-Pakten art. 2 (1), og en «act of aggression» etter art. 39. Resolusjonen ble ikke vedtatt, men tilnærmet alle Sikkerhetsrådets representanter som uttalte seg, uttrykte et syn om at handlingene utgjorde et brudd på Sovjetunionens rett til territoriell suverenitet.¹¹⁸

Resolusjonen som til slutt ble vedtatt etter samlingen viser ikke spesifikt til U2-flyvningene, men en kan implisitt tolke suverenitetsbruddet ut fra vedtakelsestidspunktet og innholdet. Sikkerhetsrådet oppfordret dets medlemmer til å «[r]espect each other's sovereignty, territorial integrity and political independence, and to refrain from any action which might increase tensions».¹¹⁹

Gjennom Nicaragua-saken er nok problemstillingen endelig avklart. Domstolen viste til at «the principle of respect for territorial sovereignty is also directly infringed by the unauthorized overflight of a State's territory by aircraft belonging to or under the control of the government of another State».¹²⁰

Basert på den forutgående drøftelse stiller altså spionasje i det territoriale luftrom seg ganske identisk med tilstedeværelsen av militære styrker på territoriet til en annen stat. Plasseringen av statlige luftfartøy i en annen stats luftrom er et brudd på retten til territoriell suverenitet. Resultatet vil være det samme ved bruk av droner til spionasjehandling. Pilotløse luftfartøy

¹¹⁷ ICAO-konvensjonen art. 3 c).

¹¹⁸ UNSC, Security Council Official Records, 858th meeting, 24. mai 1960, avs. 9, 58, 78, 83 og 128; 859th meeting, 25. mai 1960, avs. 4 og 51.

¹¹⁹ UNSC Res 135 (27. mai 1960) UN Doc S/Res/135, punkt 2.

¹²⁰ Nicaragua-saken s. 118 premiss 251.

har etter ICAO-konvensjonen art. 8 ikke rett til å bevege seg inn i fremmed luftrom uten særlig autorisasjon. Droner vil på lik linje som bemannede luftfartøy bryte med den utsatte stats territorielle suverenitet.¹²¹

Drøftingen så langt, knytter seg utelukkende til statlige fly som tar seg inn i en annen stats territorium uten godkjenning. ICAO-konvensjonen og dens bestemmelser knytter seg derimot først og fremst til reguleringen av sivil luftfart.¹²²

4.3.2 Spionasje i luftrommet utført av sivile flyfartøy

Medkontrahentene til ICAO-konvensjonen er gjennom art. 30 og 36 gitt muligheten til å forby eller regulere bruk av fotografiske apparater og radioutstyr for sivile luftfartøy på sitt territorium. Stater kan også begrense eller forby adgangen til å fly over nærmere bestemte deler av sitt territorium etter art. 9. De nevnte begrensningene vil normalt følge av bilaterale eller multilaterale avtaler mellom ulike statsmakter. Det eksisterer et enormt antall slike avtaler, for eksempel så er Australia alene part i over 100.¹²³

Skulle et sivilt flyfartøy bedrive spionasje som er i strid med en slik bilateral avtale eller ICAO-konvensjonen, vil det normalt ikke foreligge noe folkerettsbrudd. Pliktsubjektet etter avtalene er de tiltrådte stater. Statene har imidlertid en positiv plikt til å ta «appropriate measures» for å forsikre seg om at sivile luftfartøy og operatører basert på sitt territorium, ikke bryter med vilkårene i ICAO-konvensjonen.¹²⁴

Staten hvor luftfartøyet eller operatøren er registrert, har altså en plikt til å drive oppsyn med disse. De har også en plikt til å ikke selv utnytte sivil luftfart for handlinger i strid med formålet til ICAO-konvensjonen.¹²⁵ Å bedrive spionasje ved hjelp av sivile luftfartøyer vil være klart i strid med formålet til avtalen. Å fastslå brudd på plikten til å drive oppsyn er også mulig, men det er nok praktisk langt vanskeligere.

¹²¹ Cornthwaite (2019) s. 514-515.

¹²² ICAO-konvensjonen art. 3 a).

¹²³ Australian Government, Australia's air services agreements & arrangements, <https://www.infrastructure.gov.au/infrastructure-transport-vehicles/aviation/international-aviation/air-services-agreements-arrangements> (lest 21. november 2022).

¹²⁴ ICAO-konvensjonen art. 3bis d).

¹²⁵ ICAO-konvensjonen art. 4.

En ytterligere problemstilling aktualiseres når man beveger seg utenfor det territorielle luftrommet til stater. Hva er rettstilstanden når spionasjen beveger seg fra å bli utført innenfor staters territorium til verdensrommet.

4.3.3 Spionasje fra verdensrommet

Spionsatellitter kan brukes til en rekke ulike formål. De kan brukes som en form for fysisk spionasje, ved å registrere endringer på og under bakkenivå, eller ta bilder av territoriet til andre stater. Skiftet fra kommunikasjon via kabler, til digitale og trådløse løsninger, har medført at de også kan benyttes til cyberspionasje, ved å plukke opp signaler som rekker ut til verdensrommet.¹²⁶

Traktaten om det ytre verdensrom setter begrensninger og føringer for bruken av verdensrommet.¹²⁷ Avtalen har 112 kontrahenter.¹²⁸ Etter art. 2 er det ytre verdensrom og dets himmellegemer fritatt fra suverenitetskrav av noen som helst form. Suverenitetsfriheten til verdensrommet er folkerettslig sedvanerett.¹²⁹ Det er noe mer uklart hvorvidt avtalens resterende innhold er det.

En allment akseptert definisjon for når en går over fra det territorielle luftrom til verdensrommet eksisterer derimot ikke.¹³⁰ Den uoffisielle høyden som går igjen er omtrent 160 kilometer, som er det laveste punktet satellitter fritt kan oppholde seg i bane rundt jorden.¹³¹ Bruken av spionsatellitter ble møtt med protest når USA begynte å sende slike opp på starten av 1960-tallet. Sovjetunionen uttalte ved sin representant i Generalforsamlingen i 1962 at de anså slik spionasje for å gripe inn i hemmeligheter som staten i kraft av sin

¹²⁶ Abbany, Zulfikar, «Modern spy satellites in an age of space wars», DW, 25. august 2020, <https://www.dw.com/en/modern-spy-satellites-in-an-age-of-space-wars/a-54691887> (lest 8. november 2022).

¹²⁷ Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 27. januar 1967 (in force 10. november 1967) (Traktaten om det ytre verdensrom).

¹²⁸ https://treaties.unoda.org/t/outer_space (lest 8. november 2022).

¹²⁹ Shaw (2021) s. 464-465.

¹³⁰ Crawford (2019) s. 332.

¹³¹ Crawford (2019) s. 333; Shaw (2021) s. 464.

suverenitet hadde en rett til å beskytte.¹³² Frankrike og Italia fremmet lignende syn for Sikkerhetsrådet etter U2-hendelsene.¹³³

Synet som ble fremmet den gang kan ikke lenger tas for gjeldende rett. Innholdet i Traktaten om det ytre verdensrom art. 2, samt statspraksis og *opinio juris* relatert til slike satelitters fysiske bruksområder, tilsier at de må anses for å være i tråd med internasjonal rett. Det samme er ikke nødvendigvis gjeldende for deres digitale bruksområder.

Internasjonal rett, herunder FN-Pakten, gjelder på lik linje i verdensrommet som den gjør på jorden.¹³⁴ Utføres det en folkerettsstridig cyberspionasjehandling fra en satellitt, vil ikke den ansvarlige stat være fratatt ansvar basert på at spionasjen gjennomføres fra verdensrommet.

4.4 Cyberspionasje

4.4.1 Ekstraterritoriell cyberspionasje

De som mener at ekstraterritoriell cyberspionasje er forbudt etter folkeretten, viser til at informasjonen som blir samlet inn befinner seg på IKT-instrumenter som utgjør en stats suverene cyberinfrastruktur. Synet er at infrastrukturen bør nyte den samme grad av beskyttelse som det fysiske territoriet har.¹³⁵

Det ble i punkt 4.2 konkludert med at fysisk spionasje i fredstid ikke utgjør et brudd på staters territorielle suverenitet. En forutsetning for at ekstraterritoriell spionasje medfører et brudd på retten etter dagens rettsstilstand, er at fysisk spionasje også gjør det. Selv om det blir oppnådd digital tilgang til fysisk infrastruktur i en fremmed stat, vil det i det aller minste ikke være noe mer alvorlig enn om den samme handlingen ble utført fra innenfor territoriet.

Synspunktet kan forsvares blant annet i at flertallet av Tallinn-manualens anså fysisk spionasje, men ikke ekstraterritoriell spionasje, for å utgjøre et folkerettsbrudd.¹³⁶ Norges

¹³² UNGA, Soviet Statement in the General Assembly, First Committee, 17th Session, 1298th Meeting, 3. desember 1962.

¹³³ UNSC, Security Council Official Records, 858th meeting, 24. mai 1960, avs. 15 og 128-130.

¹³⁴ UNGA Res 1721 (XVI) (20. desember 1961) Del A, punkt 1 (b).

¹³⁵ Buchan (2019) s. 54.

¹³⁶ Schmitt (2017) regel 32 punkt 8.

ekspert til statsuttalelser om internasjonal retts stilling ved bruk av informasjons- og kommunikasjonsteknologi har uttrykt et lignende syn.¹³⁷

Konklusjonen er dermed at ekstraterritoriell cyberspionasje ikke utgjør et brudd på en stats territorielle suverenitet. Rettstilstanden er i tillegg mindre usikker enn for slik fysisk spionasje som ble drøftet i punkt 4.1.

4.4.2 Transnasjonal cyberspionasje

Transnasjonal cyberspionasje skiller seg fra de øvrige formene av spionasje ved at en annen stats territorium eller infrastruktur ikke berøres. Spionasjeformen gjennomføres på territoriet til staten som bedriver spionasjen. Informasjonen blir ervervet enten ved å plukke opp signaler som strekker seg inn på ens eget territorium, eller ved informasjon som er lagret eller passerer gjennom statens IKT-systemer.

Grunnet mangelen på tilknytning til den utsatte stats territorium vil ikke slik transnasjonal cyberspionasje bryte med den territorielle integriteten til stater. Den territorielle suvereniteten til stater innebærer imidlertid også en rett for stater til å «perform inherently governmental functions» på sitt eget territorium.¹³⁸ Brudd på retten vil medføre at det foreligger et suverenitetsbrudd.¹³⁹

Noen uttømmende liste over hva som utgjør iboende statlige funksjoner eksisterer ikke, men eksempler er gjennomføringen av valg, skatteinnkreving og den effektive føringen av et demokrati.¹⁴⁰ Ulovlig innblanding kan forekomme hvor statshandlinger hindrer eller begrenser en annen stats adgang til å utføre slike statlige funksjoner.

¹³⁷ UNGA, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, A/76/136, 13. juli 2021, s. 66 fotnote 176.

¹³⁸ Island of Palmas-saken s. 838; Schmitt (2017) regel 4 punkt 10; Buchan (2019) s. 56.

¹³⁹ Brudd på retten til å gjennomføre statlige funksjoner kan anføres for alle spionasjeformer under kapittel 4, men det drøftes særskilt her, da det foreligger en høyere terskel enn for å konstatere brudd på en stats territorielle integritet.

¹⁴⁰ Schmitt (2017) regel 4 punkt 16.

Stater plikter ikke å offentliggjøre sine interne diskusjoner og politiske agendaer, ervervelsen av slik informasjon av en annen stat kan tenkes å gripe inn i en iboende rett til å utøve sine statlige prerogativer uten fremmed innsyn.¹⁴¹ På den annen side så fremstår det å være i utkanten av de funksjonene som er eksemplifisert.

Tallinn-manualen viser til at cyberoperasjoner kan utgjøre et brudd på retten til å utøve statlige funksjoner, men den viser kun konkret til at ulovlig innblanding kan forekomme ved endring eller destruksjon av data.¹⁴² En transnasjonal spionasjehandling vil utelukkende plukke opp eller kopiere informasjonen.

Videre har den Den europeiske menneskerettighetsdomstolen i *Weber og Saravia mot Tyskland* vurdert transnasjonal spionasjes rettslige stilling.¹⁴³ Avgjørelsen knytter seg til retten til privat- og familieliv etter Den europeiske menneskerettighetskonvensjonen art. 8.¹⁴⁴ Domstolen måtte ta stilling til hvorvidt Tyskland på sitt eget territorium kunne plukke opp signaler fra fremmede territorier. De konkluderte med at Tyskland ved sin transnasjonale spionasje ikke hadde brutt den territorielle suvereniteten til de fremmede statene.¹⁴⁵ Avgjørelsen har kun bindende virkning for partene til domstolen, men den gir likevel uttrykk for hva som utgjør gjeldende rett for et større antall stater.

Det er ikke tilstrekkelige holdepunkter for å konkludere med at transnasjonal cyberspionasje vil kunne medføre et brudd på en stats rett til å utføre iboende statlige funksjoner. Så lenge en stats handlinger ikke berører et annet territorium, så er ikke folkeretten et hinder for å plukke opp informasjon og signaler innenfor ens egne grenser.

4.4.3 Økonomisk cyberspionasje

Økonomisk cyberspionasje skiller seg fra det som så langt er diskutert, da det virker som at stater er mer villige til å arbeide mot en strengere regulering enn det de har vært for øvrige typer av spionasjehandling. Villigheten kan sannsynligvis forklares i at økonomisk cyberspionasje har mer håndfaste følger, nemlig økonomisk tap.

¹⁴¹ Peters (2017) s. 164-165.

¹⁴² Schmitt (2017) regel 4 punkt 16.

¹⁴³ *Weber og Saravia mot Tyskland* [J] 2006, no. 54934/00.

¹⁴⁴ Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. november 1950 (in force 3. september 1953).

¹⁴⁵ *Weber og Saravia mot Tyskland* [J] 2006, no. 54934/00, avs. 88.

Obama-regjeringen publiserte i 2011 «International Strategy for Cyberspace», hvor de viste til den enorme økonomiske belastningen industriell spionasje, herunder tyveriet av intellektuell eiendom og kommersiell informasjon kan ha.¹⁴⁶ De forpliktet seg deretter til å ta steg for å bygge et internasjonalt samfunn som anser slike handlinger for ulovlige, og som holder aktørene ansvarlige.

Bilateralt har det også vært en utvikling. Kina og USA kom i 2015 med en uttalelse etter Xi Jinpings besøk i USA, hvor statene gjensidig forpliktet seg politisk overfor hverandre til å avstå fra å gjennomføre IKT-tyverier.¹⁴⁷ Uttalelsen knyttet seg spesifikt til tyveri av konfidensiell forretningsinformasjon, åndsverk og forretningshemmeligheter, som blir innhentet av stater i den hensikt å gi en fordel til kommersielle sektorer eller selskaper. Kina og Storbritannia kom med en tilnærmet identisk uttalelse etter statsbesøket i England samme år.¹⁴⁸

Etter G20-toppmøtet i Antalya i 2015 presenterte gruppen et kommuniqué, hvor ett av punktene var en bekreftelse på at økonomisk cyberspionasje ikke skal støttes eller utføres.¹⁴⁹ De gjensidige politiske forpliktelsene relatert til IKT-tyveri, som kom etter Xi Jinpings to statsbesøk, virker å ha formet innholdet i G20-kommunikéen.

Ingen av de nevnte dokumentene har noen rettslig bindende kraft, og å bryte dem vil kun ha eventuelle politiske følger. Det slike dokumenter derimot kan gjøre er at de ved sin eksistens potensielt kan redusere bruken og omfanget av økonomisk cyberspionasje. Dersom statene etterlever synspunktene de har fremmet, kan det lede til ny folkerettslig sedvanerett grunnet statspraksis og *opinio juris* relatert til slike handlinger.

¹⁴⁶ International Strategy for Cyberspace, 29. mai 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (lest 26.10.2011) s. 18.

¹⁴⁷ Fact Sheet: President Xi Jinping's State Visit to the United States, 25. september 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> (lest 26.10.2022) Se punkt "Cybersecurity" avs. 2.

¹⁴⁸ UK-China Joint Statement 2015, 22. oktober 2015, <https://www.gov.uk/government/news/uk-china-joint-statement-2015> (lest 26.10.2022) avs. 18.

¹⁴⁹ G20 Leaders' Communiqué. Antalya Summit, 15-16. november 2015, <http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/> (lest 26.10.2022) punkt 26.

At de nevnte uttalelsene stammer fra verdens økonomiske supermakter er verdt å merke seg. Den faktiske innflytelsen de sterkere statene utøver kan bidra til å skape en global praksis langt raskere enn om synet ble fremmet av noen av verdens svakeste økonomier.¹⁵⁰

På den annen side er det ikke direkte oppsiktsvekkende at det er de største økonomiene som lengter mest etter en regulering. Som de rikeste nasjonene er de i de fleste tilfeller også de mest teknologisk avanserte, og industrihemmeligheter fra slike stater vil da naturligvis også være mer ettertraktede. Ønsket i uttalelsene kan derfor ikke uten videre forutsettes å ha en global forankring.

Videre skiller ikke Tallinn-manualen mellom ordinær cyberspionasje og økonomisk cyberspionasje.¹⁵¹ Det eksisterer heller ingen internasjonale avtaler som regulerer økonomisk cyberspionasje mellom kontrahentene. Som nevnt i punkt 3.5 er det grunnet den fordekte naturen til spionasje også vanskelig å bevise noen rettslig overbevisning.

At det eksisterer en endring er utvilsomt, men det foreligger ikke tilstrekkelige holdepunkter per i dag for å konkludere med at noen sedvanerett har krystallisert seg spesifikt for økonomisk cyberspionasje.

¹⁵⁰ Deeks (2015) s. 315

¹⁵¹ Schmitt (2017) regel 32.

5 Diplomatsk spionasje

Wien-konvensjonen om diplomatisk samkvem inneholder regler som regulerer plikter og rettigheter for permanente diplomatiske utsendinger.¹⁵² Konvensjonen anses å gi uttrykk for folkerettslig sedvanerett, da den er ratifisert av tilnærmet alle verdens stater, i tillegg til at den i stor grad var en kodifisering av eksisterende sedvanerett.¹⁵³

Konvensjonen hjemler innhenting av informasjon om vertsstaten som en av funksjonene til et diplomatisk oppdrag.¹⁵⁴ En slik informasjonssamling må ikke gjennomføres i strid med nasjonal lovgivning, men selv hvor ervervlsen er lovstridig, har diplomatiske utsendinger immunitet mot fengsling og straffeforfølgelse i vertsstaten.¹⁵⁵

Diplomatsk spionasje skjer i stor utstrekning. Den britiske professoren Anthony Glees uttalte til BBC i 2018 at «every embassy in the world has spies».¹⁵⁶ Det som skiller diplomatsk spionasje fra det som er redegjort for innledningsvis og under internasjonal humanitærrett er at den ikke i samme grad er gjennomført fordekt eller under falske forutsetninger.¹⁵⁷

Vertsstatene har en oversikt over fremmede diplomater som er på deres territorium, og det er lettere å drive kontroll med kjente spioner enn ukjente.¹⁵⁸

Ambassader arbeider for å representere deres hjemstater i utlandet. Ett av formålene med ambassader er å promotere vennlige relasjoner mellom stater.¹⁵⁹ De har en plikt, på tross av sin immunitet, til å respektere nasjonal lovgivning, og å ikke blande seg inn i vertsstatens interne anliggender.¹⁶⁰ Dersom disse pliktene brytes, innebærer det at sendestaten har brutt

¹⁵² Vienna Convention on Diplomatic Relations 18. april 1961 (in force 24. april 1964) (VCDR).

¹⁵³ Ruud og Ulfstein (2018) s. 49.

¹⁵⁴ VCDR art. 3 (1) bokstav d.

¹⁵⁵ VCDR art. 29 og 31 (1); Diplomater har også en tilnærmet komplett immunitet mot sivilrettslige søksmål, men sivilrettslige spørsmål vil av relevans ikke diskuteres nærmere.

¹⁵⁶ Glees, Anthony, «When is a diplomat really just a spy?», BBC News, 27. mars 2018, <https://www.bbc.com/news/newsbeat-43556816> (lest 6. oktober 2022).

¹⁵⁷ Unntaket her vil være utsendinger som forsøker å verve agenter i vertsstaten.

¹⁵⁸ Matos, Eugene og Zienkiewicz, Adrian, «International Law and Diplomatic Covert Intelligence» Diplomat Magazine, 21. februar 2022, <https://diplomatmagazine.eu/2022/02/21/international-law-and-diplomatic-covert-intelligence/#respond> (lest 6. oktober 2022). Se 3. avs.

¹⁵⁹ VCDR art. 3 (1) (e).

¹⁶⁰ VCDR art. 41 (1).

folkerettslige plikter gjennom sine representanter, gitt at representantene har handlet på statens instruks. Hvis bruddet er alvorlig nok, vil den ansvarlige utsendingen, eller potensielt alle oppdragets utsendinger, bli erklært som *persona non grata*.

5.1 *Persona non grata*

Selv om diplomatiske utsendinger er beskyttet mot nasjonal lovgivning, er ikke vernet absolutt. Den sendende stat kan velge å frafalle retten til immunitet.¹⁶¹ Vertsstaten for det diplomatiske oppdraget kan også på et hvilket som helst tidspunkt erklære agenter fra sendestaten som *persona non grata*.¹⁶² Følgen av en slik erklæring er i praksis at sendestaten plikter å hente hjem det uønskede individet innen en rimelig angitt tidsfrist.

Å utvise diplomater grunnet spionasje på vertsstaten skjer relativt ofte i verdenssammenheng. For eksempel ble en russisk diplomat i 2020 utvist fra Norge for å ha betalt for hemmelighetsstemplet informasjon fra en norsk statsborger.¹⁶³ Den aktuelle informasjonssamlingen var angivelig i strid med norsk lovgivning, og dermed utenfor den retten diplomater har etter VCDR art. 3 (1) bokstav d og art. 41 (1).

Det kan stilles spørsmål ved hensiktsmessigheten av å gi diplomatiske utsendinger immunitet for alle handlinger de begår under sitt oppdrag. Å begå spionasje mens man er beskyttet av diplomatisk immunitet er et misbruk av formålet og hensikten bak immunitetsreglene. Det er naturlig å anta at terskelen for å akseptere spionasje på vegne av sendestaten er lavere når sjansen for å bli møtt med represalier ikke foreligger.

Persona non grata erklæringer brukes primært som et politisk virkemiddel for å vise misnøye med sendestatens handlinger. Slike erklæringer er kun nyttige som et virkemiddel fra vertsstatens side overfor enkeltagenter hvis de uønskede handlingene blir oppdaget mens agenten fortsatt er en del av det diplomatiske oppdraget.

¹⁶¹ VCDR art. 32.

¹⁶² VCDR art. 9 (1).

¹⁶³ Johan Falnes, «Norge utviser russisk diplomat etter spionsiktelse», Aftenposten, 19. august 2020, <https://www.aftenposten.no/norge/i/e82MpK/norge-utviser-russisk-diplomat-etter-spionsiktelse>, (lest 3. oktober 2022).

5.2 Diplomatisk immunitet etter oppdragets opphør

Stater er som nevnt forhindret fra å straffeforfølge individer med status som diplomatiske utsendinger. Dersom det er påvist eller mistenkt et brudd på nasjonal lovgivning, og sendestaten ikke frafaller den diplomatiske immunitet, oppstår spørsmålet om stater kan straffeforfølge tidligere diplomatiske utsendinger for brudd på nasjonal lovgivning etter at deres diplomatiske oppdrag er avsluttet.

Diplomatisk immunitet er gjeldende for alle typer handlinger, men for «acts performed (...) in the exercise of his functions as a member of the mission, immunity shall continue to subsist».¹⁶⁴ Det er naturlig å tolke innholdet i VCDR art. 39 (2) som at ikke-offisielle handlinger vil kunne straffes etter utløpet av immuniteten. En slik forståelse medfører at også handlinger utført innen immuniteten var gjeldende etter VCDR art. 39 (1), vil kunne straffeforfølges etter immunitetens opphør.

Det er vanskeligere å trekke et skille for om noe utgjør en handling utført i tråd med ens funksjon som en statlig representant, og rent personlige handlinger. Her kan saken om den nevnte utvisningen av en russisk diplomat være illustrerende. Dersom den russiske stat har oppfordret til handlingene, er det klart at immuniteten gjelder også etter oppdragets opphør. Hvordan stiller det seg derimot om kjøpet av informasjon var økonomisk motivert for den enkelte tjenesteperson, med lovnader om kompensasjon fra en utenforstående tredjestat.

Det er også grupper med personer som nyter en avledet strafferettslig immunitet fra oppdragets offisielle utsendinger, eksempelvis familien til en diplomat.¹⁶⁵ Slike personer vil ikke ha offisielle plikter å utføre, og rettsstridige handlinger de har utført i løpet av oppholdet vil derfor aldri kunne nyte en slik evigvarende immunitet som offisielle utsendinger er tilsett.

En agent som utfører spionasje i tråd med sine offisielle plikter, vil aldri kunne straffes for handlingene dersom de ble utført mens det diplomatiske oppdraget foregikk. Mottakerstaten kan derimot straffe spionasje utført før oppdraget trådte i kraft, eller etter at det opphørte. De kan også straffe spionasje som ikke ble utført med bakgrunn i offisielle plikter.

Straffeadgangen forutsetter i alle tilfeller at immuniteten er frafalt av sendestaten i tråd med VCDR art. 32, eller har opphørt etter art. 39 (2).

¹⁶⁴ VCDR art. 39 (2).

¹⁶⁵ VCDR art. 37 (1) jf. art. 29-36.

5.3 Oppsummering av diplomatisk spionasje

Det sentrale å merke seg ved diplomatiske oppdrag er at det er den nasjonale lovgivningen hos mottakerstaten som står sentralt. Spionasje vil i de fleste stater bryte med den nasjonale lovgivningen, og folkerettsbruddet kommer som en følge av bruddet på nasjonale strafferettsregler. Hvorvidt vertsstaten kan møte spionasje med mottiltak utover en *persona non grata* erklæring, vil bero på om den konkrete spionasjen brøt med folkerettslige regler, som suverenitetsprinsippet eller forbudet mot intervensjon.

6 Internasjonal humanitærrett

Spionasje i krigstid er det eneste området innen oppgavens tematikk som har nedskrevne regler om spionasje. Rettssystemet som inneholder reglene er kjent som internasjonal humanitærrett, og er bygd opp av en lang rekke konvensjoner og sedvanerett.¹⁶⁶ International Committee of the Red Cross har i sin «Customary International Humanitarian Law» forsøkt å samle den gjeldende sedvaneretten.¹⁶⁷ Regelverket som eksisterer tar ikke for seg lovligheten av spionasje direkte, men knytter seg til forhold vedrørende spioner i krigstid.

For spionasje slår ICRC i regel 107 fast at en spion ikke har rett til status som krigsfange ved pågripelse, samt at de ikke kan dømmes uten retts sak. Avgjørende for om en kan klassifiseres som en spion er om informasjonssamlingen er gjort fordekt eller på falskt grunnlag, for eksempel ved bruk av motstanderens uniformer.¹⁶⁸ Spionasje i krigstid står i en særstilling rettslig sett, handlingen kan kun straffes hvis en blir fanget i gjerningsøyeblikket. Stillingen som spion faller bort, i motsetning til krigsforbrytere, som bærer med seg stempelet frem til de blir arrestert og soner sin straff.¹⁶⁹

Regel 107 gir uttrykk for hva som utgjør gjeldende folkerett når det kommer til hvem som kan klassifiseres som spioner og hvilke rettigheter de har. Det oppstår dermed et spørsmål om eksistensen av en slik spionregulering kun regulerer pliktene og rettighetene for den utsatte stat og spionen, eller om det også kan utledes en generell tillatelse eller forbud mot bruken av spioner i krigstid.

Blant konvensjonene som står sentralt for ICRC sin sedvanerettssamling er Tilleggsprotokoll 1 til Genève-konvensjonene og Haag-konvensjonen (IV) om landkrigens lover og sedvaner, og dens vedlegg.¹⁷⁰ Det følger av vedlegget til Haag-IV art. 24 at «Ruses of war and the

¹⁶⁶ Atomvåpensaken s. 34 avs. 75.

¹⁶⁷ Henckaerts og Doswald-Beck (2005).

¹⁶⁸ ICRC regel 107 s. 390.

¹⁶⁹ Demarest (1996) s. 332.

¹⁷⁰ Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8. juni 1977 (in force 7. desember 1979) (heretter Genève-konvensjon); Regulations concerning the Laws and Customs of War on Land, annexed to Convention (IV) respecting the Laws and Customs of War on Land, The Hague, 18. oktober 1907 (entry into force 26. januar 1910) (heretter Haag-IV).

employment of methods necessary for obtaining information about the enemy and the country are considered permissible». Genève-konvensjon inneholder ingen lignende formulering, den slår kun fast i hvilke tilfeller spionstempleet inntreer, den kan derfor ikke forstås som en fravikelse av formuleringen i Haag-IV art. 24.

En nærliggende forståelse å komme til av innholdet i de to avtalene er at alle handlinger som faller innenfor definisjonen til Haag-IV art. 24 er tillatte. Det settes ingen begrensninger på hvilke metoder en kan benytte seg av for å samle informasjon om ens fiende. På den annen side er det like aktuelt å konkludere med at bestemmelsene kun slår fast at de nevnte handlingene ikke er eksplisitt forbudte.

ICRC har kun videreført adgangen til benyttelse av såkalte krigslist (ruses of war) i regel 57. Krigslist er dermed lovlige så lenge de ikke er eksplisitt ulovlige etter den internasjonale humanitærretten. En lang rekke handlinger kan falle innenfor termen, men sentralt bak de alle er målet om å forvirre fienden.¹⁷¹ Blant de eksplisitt ulovlige finner vi «acts of perfidy», handlinger som utnytter fiendens forståelse om at man har en beskyttet status, for eksempel en urettmessig bruk av hvite flagg eller FN-uniformer.¹⁷² Det er naturlig å innfortolke de samme begrensningene i Haag-konvensjonen.¹⁷³

Spionasje faller ikke direkte inn under definisjonen av krigslist. ICRC uttaler seg heller ikke nærmere om adgangen til å bedrive spionasje. Det er derfor naturlig å se nærmere på om spionasje kan innfortolkes i innholdet som ble redegjort for i art. 24 i vedlegget til Haag-IV, og om avtalen utgjør gjeldende rett.

Nürnberg-domstolen uttalte seg i 1946 om den rettslige stillingen til traktaten. Selv om traktaten etter art. 2 kun gjelder mellom kontraherende parter, inntok domstolen det syn at traktatens innhold ved starten av 2. verdenskrig ga uttrykk for folkerettslig sedvanerett.¹⁷⁴ Sedvaneretter kan med tiden endres eller fravikes, men det kan ikke ses holdepunkter for å slå fast at Haag IV ikke lenger er en kodifikasjon av folkerettslig sedvanerett. Det neste som må avklares er dermed innholdet i art. 24.

¹⁷¹ ICRC regel 57 s. 204.

¹⁷² Se ICRC regel 58 og 60.

¹⁷³ VCLT art. 31 (3).

¹⁷⁴ Judgment of the Nuremberg International Military Tribunal 1946 (1947). 41 AJIL 172, s. 248-249.

Lovligheten av spionasje i krigstid kan begrunnes i at det ikke eksisterer generelle forpliktelser for stater til å respektere territoriet eller styresmaktene til en fiendtlig stat, i tillegg til at det ikke eksisterer spesifikke konvensjoner mot dets bruk.¹⁷⁵ Spionasjehandlinger ligner i tillegg ikke på handlinger som ulovlig bruk av det hvite flagg eller FN-uniformer, men mer på de lovlig nevnte krigslistene.

Eksistensen av sedvanerettslig regulering tilknyttet behandlingen av spioner dersom de skulle bli tatt i handlingen trekker i samme retning. Dersom verdens stater ønsket å forby spionasje kunne de ha gjort utøverne til krigsforbrytere, eller tatt inn et eksplisitt forbud. At behandlingen av spioner som blir tatt i spionasjehandlingen er regulert, taler for en implisitt aksept av deres rettmessige plass i krigssituasjoner.

Spionasje er særdeles vanskelig å oppdage, og kan ha katastrofale virkninger for den utsatte stat. Stater er til dels beskyttet ved at den reguleringen som foreligger skaper en avskrekkende effekt for potensielle spioner. Mangelen på krigsfangestatus betyr at en kan bli møtt med det mest alvorlige rettslige midlet, dødsstraff. Demarest argumenterer for lovligheten av spionasje med bakgrunn i et slikt syn.¹⁷⁶

På den annen side ble argumentet uttrykt i 1996, og det mister noe av sin verdi da antall land som har avskaffet dødsstraff har økt betraktelig. Siden 1996 har antall land som har avskaffet dødsstraff nesten doblet seg, og de utgjør over halvparten av verdens stater per dags dato.¹⁷⁷

Basert på den forutgående drøftelse utgjør ikke spionasje i krigstid et brudd på folkeretten. Det eksisterer kun en regulering av *når* noen kan klassifiseres som en spion, og hvilke rettigheter de har *dersom* de skulle bli fanget. Det eksisterer ingen folkerettslig regulering av spionasje i krigstid, og ved mangel på forbud så foreligger det som nevnt tidligere tillatelse.

¹⁷⁵ Wright (1962) s. 12.

¹⁷⁶ Demarest (1996) s. 338.

¹⁷⁷ Amnesty International, Death Penalty, <https://www.amnesty.org/en/what-we-do/death-penalty/> (lest 11.10.2022).

6.1 Cyberspionasje i lys av den internasjonale humanitærretten

Spionbestemmelsene i Haag-IV og AP1 er nøytrale når det kommer til formen spionasjen har.¹⁷⁸ Det som blir avgjørende for cyberspionasje i krigstid, i tillegg til at handlingene er fordekte eller utført på falskt grunnlag, er territoriet de utføres fra.

For at spionhjemlene skal komme til anvendelse må spionasjen ha blitt utført «in the zone of operations of a belligerent» etter Haag-IV, eller «territory controlled by an Adverse Party» etter Genève-konvensjonen.¹⁷⁹ Bestemmelsene gir uttrykk for folkerettslig sedvanerett, og er etter ordlyden gjeldende i områder det står strid om, eller som er kontrollert av motstanderen.¹⁸⁰

Cyberspionasje er derfor likestilt med fysisk spionasje i krigssituasjoner, og utgjør ikke et brudd på folkeretten. Det samme blir resultatet når spionasjen er utført utenfor de nevnte områdene, da prinsippet om suverenitet og ikke-intervensjon ikke kommer til anvendelse i krigstid.¹⁸¹

¹⁷⁸ Haag-IV art. 29 og 31; AP1 art. 46.

¹⁷⁹ Haag-IV art. 29; AP1 art. 46 punkt 2.

¹⁸⁰ Schmitt (2017) regel 89 punkt 2 og 7.

¹⁸¹ Schmitt (2017) regel 5 punkt 6.

7 Cyberspionasje tilknyttet ikke-statlige entiteter

Det som er drøftet så langt i oppgaven har utelukkende knyttet seg til tilfeller hvor stater har vært ansvarlige for spionasjehandlinger. Hensikten med å vurdere ikke-statlige entiteter separat er at deres handlinger ikke kan medføre brudd på suverenitetsprinsippet eller forbudene mot intervensjon og bruk av makt.¹⁸² Staten hvis territorium de oppholder seg på har imidlertid visse plikter.

7.1 Staters handleplikt innenfor sin egen jurisdiksjon

En forutsetning for å holde en stat ansvarlig for en internasjonal handling, er at en handling eller mangel på handling kan tilskrives staten, og at den utgjør et brudd på en folkerettslig forpliktelse.¹⁸³

Det påligger stater en sedvanerettslig aktsomhetsplikt (due diligence) når det kommer til handlinger som blir utført fra ens eget territorium.¹⁸⁴ Av ICJ er det formulert for stater som en «[o]bligation not to allow knowingly its territory to be used for acts contrary to the rights of other States».¹⁸⁵ Aktsomhetsplikten kan bli gjort gjeldende overfor en stat for handlinger som ikke bare er utført av staten selv, men også av private aktører.¹⁸⁶

Her blir aktsomhetsplikten kun drøftet opp mot cyberspionasje. De fysiske spionasjeformene vil medføre at man faktisk befinner seg på territoriet til staten som spionasjen blir utøvd mot, slike handlinger vil ikke falle innenfor den plikten som det ses nærmere på her.¹⁸⁷

Aktsomhetsplikt for en cyberspionasjehandling reiser videre spørsmål om statens kjennskap til handlingen, pliktens stilling i cyberspace, og alvorlighetsgraden som kreves for at staten skal være pålagt å agere.

¹⁸² Schmitt (2017) regel 33 punkt 2.

¹⁸³ UNGA, ILC, Draft Articles on Responsibility of States for Internationally Wrongful Acts, A/56/83, 12. desember 2001, art. 2 a) og b).

¹⁸⁴ Schmitt (2017) regel 6 punkt 1.

¹⁸⁵ The Corfu Channel-Case, Judgment, 9. April 1949, I.C.J. Reports 1949 s.4 (Corfu Channel-saken) s. 22.

¹⁸⁶ Crawford (2019) s. 527.

¹⁸⁷ Et unntak som kan tenkes er at private bedriver spionasje mot utenlandske ambassader, men vertsstaten har i slike tilfeller en særlig plikt til beskyttelse etter VCDR art. 22 (2).

Staten som cyberoperasjonen utøves fra, eller gjennom, må være klar over handlingens eksistens. Hvorvidt det blir oppdaget av staten selv, eller de blir informert av staten som cyberoperasjonen er rettet mot, er irrelevant. Så fort innsikt foreligger vil staten ha en plikt til å handle, forutsatt at de øvrige krav foreligger.

Ekspertgruppen til FN på cyberspace og nasjonal sikkerhet anbefalte i sine rapporter fra 2013 og 2015 at stater skulle forsikre seg om at deres territorier ikke ble benyttet til ulovlig IKT-bruk av ikke-statlige aktører.¹⁸⁸ Tallinn-gruppen ser det som klart at prinsippet gjelder, som en direkte følge av at suverenitetsprinsippet er anerkjent for å være gjeldende også i cyberspace.¹⁸⁹

Gruppens synspunkt kan forsvares ved folkerettens anvendelse også i cyberspace, men hvorvidt det faktisk utgjør gjeldende rett er ikke uten videre klart. Flere av de større statsaktørene når det kommer til cyberoperasjoner har ikke uttalt seg om aktsomhetspliktens stilling i cyberspace.¹⁹⁰ Det eksisterer heller ingen tilfeller hvor en stat har hevdet at en annen stat har brutt sin «cyber due diligence».¹⁹¹ Aktsomhetspliktens rettslige stilling i cyberspace må derfor anses som uavklart.

Gitt at plikten eksisterer, så vil den kun manifestere seg dersom handlingen medfører «serious adverse consequences» for den utsatte staten.¹⁹² Formuleringen stammer fra avgjørelser som knyttet seg til internasjonal miljørett.¹⁹³ Det nærmere innholdet og grensedragninger er uklart, men det må forstås som at det i det minste legger opp til en høy terskel.

Tallinn-manualen ser det videre som et krav at den aktuelle handlingen ville ha utgjort et folkerettsbrudd hvis den var utført av en stat, kontra et privat individ eller gruppering, som ikke arbeider på instruks fra en stat.¹⁹⁴ En ytterligere forutsetning for å konstatere et brudd

¹⁸⁸ UNGA, «Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security», 24. juni 2013, UN Doc A/68/98 avs. 23; 22. juli 2015, UN Doc A/70/174 avs. 28 (c).

¹⁸⁹ Schmitt (2017) regel 6 punkt 3.

¹⁹⁰ Jensen og Watts (2020-2021) s. 694-695 med videre henvisninger.

¹⁹¹ Jensen og Watts (2020-2021) s. 695.

¹⁹² Schmitt (2017) regel 6 punkt 21.

¹⁹³ Trail Smelter Case (U.S. v. Canada) (1938) 3 RIAA 1905, s. 1965; Schmitt (2017) regel 6 punkt 25.

¹⁹⁴ Schmitt (2017) regel 6 punkt 23.

på aktsomhetsplikten blir da at den aktuelle cyberoperasjonen ville utgjort et folkerettsbrudd om en stat var aktøren.

Basert på det foregående kan det oppstilles fire kumulative vilkår for at en stat har brutt sin aktsomhetsplikt ved å ikke stoppe en cyberspionasjehandling; (i) Aktsomhetsplikten gjelder i cyberspace, (ii) staten vet at handlingen utføres og hva den innebærer, (iii) handlingens gjennomførelse vil ha «serious adverse consequences» for den utsatte stat, og (iv) handlingen ville utgjort et folkerettsbrudd hvis den ble utført av en statsmakt.

Hvorvidt aktsomhetsplikten kan påberopes for cyberoperasjoner er som nevnt uavklart. Alvorlighetsgraden som kreves er høy, og ved fraværet av reelle fysiske konsekvenser er det vanskelig å se at terskelen er nådd. I tillegg er det uavklart om cyberspionasjehandling overhodet kan utgjøre et folkerettsbrudd. Vilkårene for aktsomhetsplikten vil derfor vanskelig kunne oppfylles for en cyberspionasjehandling.

Dersom det likevel skulle bli slått fast at aktsomhetsplikten er brutt for en stats manglende kontroll med cyberspionasje fra sitt territorium, vil den berørte stat kunne benytte seg av mottiltak. Tiltakene vil da kunne rette seg enten direkte mot den ikke-statlige aktøren, eller mot staten hvis territorium de opererer ut fra.¹⁹⁵

¹⁹⁵ Schmitt (2015-2016) s. 80.

8 Avsluttende bemerkninger – er det et behov for en folkerettslig regulering av spionasje?

Det fremstår som klart ut ifra det som er redegjort for av akademiske syn, staters opptreden og deres langvarige bruk, at fysisk spionasje ikke er særskilt regulert og heller ikke er ønsket regulert. Følgene av fysisk spionasje kan naturligvis være alvorlige, men det krever etter sin natur langt flere midler for å gjennomføre, samtidig som den potensielle informasjonservervelsen ofte er langt mindre enn ved cyberspionasje. Av den grunn er behovet for regulering ikke så påtrengende, og den statlige viljen til å forsøke å regulere dets bruk eksisterer nok ikke i tilstrekkelig grad per dags dato.

Samtidig vil trolig innholdet i det territorielle suverenitetsprinsippet fortsette å utvikle seg, slik at et forbud mot fysisk spionasje potensielt indirekte oppstår. En slik utvikling vil også kunne medføre innskrenkninger i adgangen til å bedrive ekstraterritoriell spionasje, selv uten spesifikke reguleringer av dette.

Det er imidlertid en mer konkret utvikling i det digitale rom, og omfanget av ekstraterritoriell spionasje ble for fullt tydeliggjort etter Snowden-avsløringene. Selv om det i oppgaven legges til grunn at bruken ikke medfører et brudd på internasjonal lov, er det slik den foreligger i dag stor sjanse for at man over de neste tiår vil se utviklinger.

For å oppnå en folkerettslig regulering vil antageligvis det første steget være tydeligere nasjonale posisjoner og inngåelse av bindende avtaler. Sannsynligvis vil slike avtaler innledningsvis måtte inngås mellom stater som har tilnærmet samme syn på ekstraterritoriell spionasje. Hvorvidt det er Vesten, Østen eller Sør-Amerika som leder an er uvesentlig, men det må skapes et fundament som kan lede til en mer uniform global regulering.

Som nevnt er det en rekke stater som ser et behov for en regulering av økonomisk cyberspionasje. Det er nærliggende å tro at hvis spionasje noensinne blir regulert, så vil det være regler og avtaler tilknyttet økonomisk cyberspionasje som danner grunnlaget.

Reguleringen på området vil dernest kunne anvendes som inspirasjon for å forme det videre arbeid med hensyn til andre spionasjeformer.

Referanseliste

Traktater og konvensjoner:

Haag-IV	Regulations concerning the Laws and Customs of War on Land, annexed to Convention (IV) respecting the Laws and Customs of War on Land, The Hague, 18. oktober 1907 (in force 26. januar 1910)
ICAO-konvensjonen	Convention on International Civil Aviation, 7. desember 1944 (in force 4. april 1947)
FN-Pakten	Charter of the United Nations, 26. juni 1945 (in force 24. oktober 1945)
ICJ-Statuttene	Statute of the International Court of Justice, 26. juni 1945 (in force 24. oktober 1945)
EMK	Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. november 1950 (in force 3. september 1953)
VCDR	Vienna Convention on Diplomatic Relations 18. april 1961 (in force 24. april 1964)
Outer Space Treaty	Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 27. januar 1967 (in force 10. november 1967)
VCDR	Vienna Convention on the Law of Treaties, 23. mai 1969 (in force 27. januar 1980)
Tilleggsprotokoll 1 til Genève-konvensjonene av 1949	Protocol Additional to the Geneva Conventions of 12 august 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8. juni 1977 (in force 7. desember 1979)

Internasjonal rettspraksis:

Island of Palmas-saken	Island of Palmas (Neth. v. U.S.) (1928) 2 RIAA 829
Lotus-saken	The case of the S.S. "Lotus" 7. september 1927, PCIJ Reports Serie A nr. 10
Trail Smelter-saken	Trail Smelter Case (U.S. v. Canada) (1938) 3 RIAA 1905
Nürnbergprosessen	Judgment of the Nuremberg International Military Tribunal 1946 (1947). 41 American Journal of International Law, 172
Corfu Channel-saken	The Corfu Channel-Case, Judgment, 9. April 1949, I.C.J. Reports 1949 s. 4
Nordsjø-saken	North Sea Continental Shelf Cases, Judgment, I.C.J. Reports 1969 s. 3
Nicaragua-saken	Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment, I.C.J. Reports 1986, s. 392
Atomvåpensaken	Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, s. 226
Weber og Saravia mot Tyskland	<i>Weber og Saravia mot Tyskland</i> [J], no. 54934/00, ECHR-XI
Kosovo-saken	Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, I.C.J. Reports 2010, s. 403
Costa Rica mot Nicaragua	Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua), Judgment,

Resolusjoner og dokumenter fra FNs Sikkerhetsråd og Generalforsamling:

- UNSC, Security Council Official Records, 858th meeting, 24. mai 1960
- UNSC, Security Council Official Records, 859th meeting, 25. mai 1960
- UNSC, Res 135 (27. mai 1960) UN Doc S/Res/135.
- UNGA Res 1721 (XVI) 20. desember 1961.
- UNGA, Soviet Statement in the General Assembly, First Committee, 17th Session, 1298th Meeting, 3. desember 1962.
- UNGA Res 2625 (XXV) 24. oktober 1970.
- UNGA Res. 3232 (XXIX) 12. november 1974.
- UNGA Res 36/103, 9. desember 1981.
- UNGA, ILC, Responsibility of States for Internationally Wrongful Acts, UN Doc A/56/83, 28. januar 2002.
- UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/9, 24. juni 2013.
- Note verbale dated 22 July 2013 from the Permanent Mission of the Bolivarian Republic of Venezuela to the United Nations addressed to the Secretary-General, UN Doc A/67/946, 29. juli 2013.
- UNGA, International Law Commission, Second Report on the Identification of Customary International Law, A/CN.4/672, 22. mai 2014.
- UNGA, 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, ILC, Draft conclusions on identification of customary international law: with commentaries, UN Doc A/73/10, 2018.
- UNGA, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace

in the Context of International Security established pursuant to General Assembly resolution 73/266, UN Doc A/76/136, 13. juli 2021.

Ikke bindende internasjonale dokumenter:

- Fact Sheet: President Xi Jinping's State Visit to the United States, 25. september 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> (lest 26.10.2022).
- UK-China Joint Statement 2015, 22. oktober 2015, <https://www.gov.uk/government/news/uk-china-joint-statement-2015> (lest 26.10.2022).
- G20 Leaders' Communiqué. Antalya Summit, 15-16. november 2015, <http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/> (lest 26.10.2022).

Nasjonal lovgivning, rettspraksis, forarbeider og dokumenter:

- Amerikanske U.S. Code: Title 18 (25. juni 1948), <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section798&num=0&edition=prelim> (lest 9. desember 2022).
- Tyske Strafgesetzbuch (13. November 1998), https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p0012 (lest 9. desember 2022).
- Kinesiske State Security Law of the People's Republic of China (22. februar 1993), http://www.npc.gov.cn/zgrdw/npc/lfzt/rlys/2014-08/31/content_1876769.htm (lest 9. desember 2022).
- Lov 20. mai 2005 nr. 28 om straff
- Det Kongelige Utenriksdepartement, «Folkerettslige rammer for grenseoverskridende informasjonsinnhenting», (29. mai 2015), <https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/2.pdf> (lest 15. november 2022).
- Prop.80 L (2019-2020) Lov om Etterretningstjenesten (etterretningstjenesteloven)
- Australian Government, Australia's air services agreements & arrangements, <https://www.infrastructure.gov.au/infrastructure-transport-vehicles/aviation/international-aviation/air-services-agreements-arrangements> (lest 21. november 2022).

Litteratur:

- Bowman, Michael E., «*Intelligence and international law*», *International Journal of Intelligence and Counterintelligence* 1995 8(3), s. 321-335.
- Buchan, Russell, «*The international legal regulation of state sponsored cyber espionage*» i Osula, Anna-Maria og Røigas, Henry, (Eds.) *International cyber norms: Legal, policy & industry perspectives*, NATO CCD COE Publications 2016, s. 65-86.
- Buchan, Russell, *Cyber espionage and international law*, Oxford: Hart Publishing 2019.
- Cornthwaite, Joshua L., «*Can we shoot down that drone: An examination of international law issues associated with the use of territorially intrusive aerial and maritime surveillance drones in peacetime*», *Cornell International Law Journal* 2019 52(3), s. 475-544.
- Crawford, James, *Brownlie's principles of public international law*, 9.utg., Oxford University Press 2019.
- Deeks, Ashley, «*An international legal framework for surveillance*», *Virginia Journal of International Law* 2015 55(2), s. 291-368.
- Delupis, Ingrid, «*Foreign warships and immunity for espionage*», *The American Journal of International Law* 1984 78(1), s. 53-75.
- Demarest, Geoffrey B., «*Espionage in international law*», *Denver Journal of International Law and Policy* 1996 24(2), s. 321-348.
- Dinstein, Yoram, *War aggression and self-defence*, 6. utg., Cambridge University Press 2017.
- Helmersen, Sondre Torp, *Folkerett: I et nøtteskall*, 1. utg., Gyldendal Norsk Forlag 2014.
- Helmersen, Sondre Torp, *The application of teachings by the International Court of Justice: Studies on international courts and tribunals*, Cambridge: Cambridge University Press 2021. DOI: <https://doi:10.1017/9781108933520>.
- Henckaerts, Jean-Marie og Doswald-Beck, Louise, *Customary international humanitarian law: Volume I: Rules*, 1. utg., Cambridge University Press 2015.
- Jamnejad, Maziar og Wood, Michael, «*The Principle of Non-intervention*», *Leiden Journal of International Law* 2009 22(2), s. 345-381.
- Jensen, Eric Talbot og Watts, Sean, «*Cyber due diligence*», *Oklahoma Law Review* 2021 73(4), s. 645-710.

- Matos, Eugene og Zienkiewicz, Adrian, «*International Law and Diplomatic Covert Intelligence*», *Diplomat Magazine*, 21. februar 2022, <https://diplomatmagazine.eu/2022/02/21/international-law-and-diplomatic-covert-intelligence/#respond> (lest 6. oktober 2022).
- Oppenheim, Lassa, *International law: A treatise*, 2. utg., Longmans, Green and Co. 1912.
- Reisman, Michael, W., «*Covert action*», *Yale Journal of International Law* 1995 20(2), s. 419-426.
- Rose, Cecily, mfl., *An introduction to public international law*, Cambridge University Press 2022.
- Ruud, Morten og Ulfstein, Geir, *Innføring i folkerett*, 5. utg., Universitetsforlaget 2018.
- Schmitt, Michael, «*In defense of due diligence in cyberspace*», *Yale Law Journal Forum* 2015-2016 125, s. 68-81.
- Schmitt, Michael, *Tallinn manual 2.0 on the international law applicable to cyber operations*, 2. utg., Cambridge University Press 2017.
- Shah, Niaz, A., «*Self-defence, anticipatory self-defence and pre-emption: international law's response to terrorism*», *Journal of Conflict & Security Law* 2007 12(1), s. 95-126.
- Shaw, Malcolm Nathan, *International law*, 9. utg., Cambridge University Press 2021.
- Simma, Bruno, *The Charter of the United Nations: A commentary: Second edition: Volume II*, Oxford University Press 2002.
- Stone, Julius, «*Legal problems of espionage in conditions of modern conflict*» i Stanger, Roland J., (Ed.) *Essays on espionage and international law*, Ohio State University Press 1962, s. 3-28.
- Sun, Tzu, oversatt av Cleary, Thomas, *The art of war*, Shambala Publications, Inc. 1988.
- Peters, Anne, «*Privacy, rechtsstaatlichkeit, and the legal limits on extraterritorial surveillance*», i Miller, Russell, (Ed.) *Privacy and power: A transatlantic dialogue in the shadow of the NSA-affair*, Cambridge University Press 2017, s. 145-179.
- Sulmasy, Glenn, og Yoo, John, «*Counterintuitive: Intelligence operations and international law*», *Michigan Journal of International Law* 2007 28(3), s. 625-638.

- Wright, Quincy, «*Espionage and the doctrine of non-intervention in internal affairs*» i Stanger, Roland J., (Ed.) *Essays on espionage and international law*, Ohio State University Press 1962, s. 3-28.

Nyhetsartikler:

- Associated Press, «Germany's Merkel: A "serious breach" if U.S. tapped her cellphone», Los Angeles Times, 23. oktober 2013, <https://www.latimes.com/world/worldnow/la-fg-wn-germany-merkel-us-cellphone-20131023-story.html> (lest 29. november 2022)
- Ukjent forfatter, «When is a diplomat really just a spy?», BBC News, 27. mars 2018, <https://www.bbc.com/news/newsbeat-43556816> (lest 6. oktober 2022).
- Abbany, Zulfikar, «Modern spy satellites in an age of space wars», DW, 25. august 2020, <https://www.dw.com/en/modern-spy-satellites-in-an-age-of-space-wars/a-54691887> (lest 8. november 2022).
- Johan Falnes, «Norge utviser russisk diplomat etter spionsiktelse», Aftenposten, 19. august 2020, <https://www.aftenposten.no/norge/i/e82MpK/norge-utviser-russisk-diplomat-etter-spionsiktelse>, (lest 3. oktober 2022).
- Torkell J. Trædal m.fl., «PST har siktet gjesteforskeren i Tromsø for spionasje. Han nekter straffskyld.», Aftenposten, 28. oktober 2022, <https://www.aftenposten.no/norge/i/763Kpo/pst-har-siktet-gjesteforskeren-i-tromsoe-for-spionasje-han-nekter-straffskyld> (lest 31. oktober 2022)

