Staters outtalade normer i cyberrymden

Gazmend Huskaj

Margarita Sallinen

CATS
CENTRUM FÖR ASYMMETRISKA HOT- OCH TERRORISMSTUDIER

Försvarshögskolan

Staters outtalade normer i cyberrymden

Förord

Frågor kring normer och policy kring offensiva cyberoperationer är mycket aktuella mot bakgrund av de allt mer uppmärksammade diskussionerna mellan t ex Ryssland och USA om hur att reagera och besvara avsiktliga cyberattacker mot kritisk infrastruktur. Det finns uttalade normer i folkrätten om vad man får göra, men det finns också outtalade normer som innebär att cyberspionage i sig inte är folkrättsligt förbjudet. Vad som inte medges i någon form är förstörande attacker mot kritisk infrastruktur, men som ändå förekommit av olika hackergrupper vilka utåt kan synas vara fristående men ändå oftast är tolererade av de stater där de har sin hemvist.

Denna i många stycken unika rapport belyser dessa normer samt beskriver hur olika länder agerat i enlighet med dessa, och som förhoppningsvis kan utgöra ett underlag för svenska nationella policydiskussioner inom cybersäkerhetsområdet.

Rapporten har tagits fram inom CATS - vid Institutionen för säkerhet, strategi och ledarskap (ISSL) och dess Centrum för totalförsvar och samhällets säkerhet CTSS - men med doktoranden Gazmend Huskaj vid Militärvetenskapliga institutionen, Försvarssystem som projektledare och med stöd av praktikanten vid Mastersprogrammet på den Statsvetenskapliga avdelningen.

Lars Nicander (PD)

Chef, Centrum för Asymmetriska Hot- och TerrorismStudier (CATS)

Sammanfattning

Den här rapporten presenterar vilka nationella outtalade normer som kan utläsas hos nio stater som bryter mot internationella överenskommelser i cyberrymden. Det finns olika sorters normer och många definitioner på vad det är, där uttalade normer ofta associeras till skrivna regler, medan outtalade normer associeras till underliggande värderingar som exempelvis styr diplomati. Diplomati är en praktik i hur stater ska interagera med varandra. Den Ryska Federationen använde sig exempelvis av diplomati 1998 under det första utskottet av FN:s generalförsamling då de lyfte frågan om hur informations- och telekommunikationsteknologier kan påverka internationell säkerhet. FN antog då en resolution och 2014/2015 presenterade de elva uttalade normer som ska gälla för ansvarsfullt statligt beteende i cyberrymden. Resultatet i denna rapport visar att alla nio stater har brutit mot FN:s uttalade normer men i olika grad/utsträckning. Resultatet visar därför på att de nationella outtalade normerna som kan utläsas hos de nio staterna under granskning i cyberrymden följer den geopolitiska och geoekonomiska situationen i den internationella miljön.

Nyckelord: Cybernormer; Offensiva Cyberoperationer; Geopolitik, Geoekonomi, Stater.

Projektledning
Dr. Lars Nicander, Anna Djup, Gazmend Huskaj

Projektledare
Gazmend Huskaj

Författare
Gazmend Huskaj

Margarita Sallinen

Innehållsförteckning

Förkortningar & definitioner

Cyberangrepp – direkt anfall, där med anfalla avses offensiva åtgärder (Reuter, 2003).

Cyberattack – handlingar som skapar märkbara förnekande effekter (dvs. degradering, störning, eller förstörelse) (JCOS, 2018, s. II-7).

Cyberdomän – den delen de tre sammanhängande lagren av cyberrymden: det fysiska nätverkslagret; det logiska nätverkslagret; och cyber-personalagret (JCOS, 2018, s. I-2).

Cyberkonflikt – konkurrenskraftig eller motsatt handling av oförenlighet: antagonistisk stat eller handling (som av olika idéer, intressen eller personer) vilka utspelar sig i och genom cyberrymden.

Cyberoperationer - en sekvens av planerade handlingar som utförs av en organiserad grupp människor med ett definierat syfte i och genom hårdvara och programvara som används för att skapa, bearbeta, lagra, hämta och sprida information i olika typer av sammankopplade nätverk som bygger ett stort, globalt nätverk, byggd och används av människor (Huskaj, Iftimie & Wilson, 2020).

Cyberrymd – Hårdvara och mjukvara som används för att skapa, bearbeta, lagra, hämta och sprida information i olika typer av sammankopplade nätverk som bygger ett stort, globalt nätverk, byggd och används av människor (Huskaj, 2019).

Daesh - Daesh (eller Da'ish), den arabiska akronymen som representerar jihadistgruppen i Syrien och Irak som har negativa nedsättande övertoner, vilket orsakar irritation för terrorist-gruppen (Irshaid, 2015).

Dataförstörelse - Användningen av skadlig programvara för att förstöra data på en dator eller för att göra en dator obrukbar (CFR, 2021b).

Distribuerad överbelastningsattack (DDoS) - Den avsiktliga förlamningen av ett datornätverk genom att överbelasta det med data som skickas samtidigt från många enskilda datorer (CFR, 2021b).

Doxing - Handlingen att söka och publicera privat eller identifiera information om en individ eller grupp på internet, vanligtvis med skadlig avsikt (CRF, 2021b).

FN – Förenta nationerna.

Finansiell vinning/stöld - Stöld av tillgångar, till exempel kryptovalutor eller kontanter, för ekonomisk vinst (CFR, 2021b).

Hack-n-leak – en informationsoperation bestående av en trestegsprocess: 1) att sprida ett falskt, partiskt eller överdrivet rykte för att diskreditera målet genom vanliga medier; 2) hacka direkt eller indirekt målet för att stjäla information om denne; 3) att läcka den hackade informationen.

IKT – informations- och telekommunikationsteknologi.

Informationskrigsföring – informationsoperation som genomförs under kris och krig för att främja eller uppnå särskilda politiska eller militära mål gentemot en eller flera motståndare (Grennert & Tham-Lindell).

Informationsoperationer - Informationsoperationer och krigföring, även känd som influensoperationer, inkluderar insamling av taktisk information om en motståndare samt spridning av propaganda i strävan efter en konkurrensfördel gentemot en motståndare (RAND, 2021).

Normer – outtalade (ibland även kallade sociala eller informella normer) – "Norms are the intersubjective beliefs about the social and natural world that define actors, their situations, and the possibilities of action. Norms are intersubjective in that they are beliefs rooted in and reproduced through social practice…Norms constitute actors and meaningful action by situating both in social roles" (Farrell, 2002, s. 49)

Normer – uttalade (kallas även formella normer) "formella normer är nedskrivna eller klart uttalade och kallas även regler" (Thornberg, 2013, s.30). Uttalade normer kännetecknas av att vara tydligt framförda överenskommelser, exempelvis strategier, manualer, policyinstrument etc. Trots att uttalade normer är nedskrivna så använder sig olika länder av dem på olika sätt och genomdriver dem på olika nivåer, beroende på landets kultur och det kulturella värdet man ser i att följa dem.

Offensiva cyberoperationer – en sekvens av handlingar som utförs av en organiserad grupp människor med ett definierat syfte genom användningen av offensiva metoder (Huskaj, Iftimie & Wilson, 2020).

Offensiva metoder – Buffer overflow; privilege escalation; rootkits; redirection and triggering; tunneling; collection/exfiltration; social engineering; web exploitation; persistent access; man-in-the-middle; (distributed) denial of service; obfuscation (Huskaj & Wilson, 2020).

Spionage - Handlingen att erhålla konfidentiell information utan informationsinnehavarens samtycke (CFR, 2021b).

Vandalism - Den obehöriga handlingen för att ändra utseendet på en webbplats eller ett socialt mediekonto (CFR, 2021b).

1 Introduktion

Introduktionen presenterar syfte, metod och upplägg för studien följt av bakgrunden till varför denna studie genomförs.

1.1 Syfte, metod och upplägg

Syftet med rapporten är att belysa frågan ***vilka nationella outtalade normer kan utläsas hos stater som bryter mot internationella överenskommelser i cyberrymden***. Rapporten baseras på en fallstudiestrategi, ett anpassat ramverk för metanormer och en rapportprocess som baseras på Yins (2018) forskningsprocess. Detaljerad information rörande rapportdesign återfinns i bilagan.

1.2 Bakgrund

Det finns olika sorters normer och många definitioner av vad det är (t.ex. Rossi & Berk, 1985; Schwartz, 1977; Cancian, 1975). Uttalade normer associeras till samhällets olika skrivna regler, som t.ex. lagar. Outtalade normer däremot är sociala företeelser kopplade till samhällets oskrivna regler och är intersubjektiva uppfattningar som delas av samhället, vilket i sin tur kan styra hur stater interagerar med varandra (Agius, 2019, ss. 80-82). Ett exempel är diplomati: en social praktik i hur stater ska interagera med varandra (Hurd, 2015). Att känna till skillnaden mellan en uttalad norm och en outtalad norm är viktigt att veta eftersom *outtalade* normer faller tillbaka på *underliggande värderingar*.

Stater använder diplomati, som styrs av outtalade normer, som ett verktyg och "åberopar lag för att stärka sina positioner i förhållande till andra stater genom att konstruera motiveringar som placerar deras politik och preferenser som överensstämmer med internationella lagar och normer" (Hurd, 2015, s. 31).

Ett exempel är hur den Ryska Federationen (hädanefter Ryssland) använde sig av diplomati när de 1998 i FN:s generalförsamlings första utskott lyfte frågan om hur informations- och telekommunikationsteknologier (IKT) kan påverka internationell säkerhet. Hotet som Ryssland såg kom från "informationsvapen och informationskrigföring, ett val av termer som antogs från mitten av 1990-talets aggressiva retorik som användes i USA:s militära doktrin" (Tikk & Kerttunen, 2017, s. 8). En rimlig slutsats är "att åtminstone ett delmål för Kreml var att motverka USA: s överlägsenhet i militär utveckling och utplacering av IKT som demonstrerades under första Gulfkriget och att begränsa ytterligare operativ utveckling inom detta område" (Tikk & Kerttunen, 2017, s. 8).

Varför är IKT viktigt? Jo, "få teknologier har varit lika kraftfulla som informations- och kommunikationsteknologier för att omforma ekonomier, samhällen och internationella relationer. Cyberrymden berör alla aspekter av våra liv." (FN, 2021). Idag kopplas några av de allra viktigaste samhällsfunktionerna i Sverige och andra länder världen över mot IKT. De positiva samhällsförändringarna syns både på individ- och samhällsnivå, i privat såväl som offentlig sektor (Säkerhetspolisen, 2020, ss. 6–7).

Nya teknologier och den snabba digitaliseringen är viktig för att Sverige ska kunna vara fortsatt konkurrenskraftig (RISE, 2019). Det snabba anammandet av nya teknologier och den snabba digitaliseringen kommer inte utan risk (FN, 2021; RISE, 2019). Risk är resultatet av hot och konsekvens, d.v.s. den sannolikhet hotet har att materialisera sig och om hotet materialiserar sig, konsekvenserna av det. Det finns flertalet fall där hoten har materialiserat sig genom offensiva cyberoperationer utförda av stater eller statsunderstödda aktörer. Några fall beskrivs nedan.

Stater investerar i och utvecklar förmågor och förband för offensiva cyberoperationer (Huskaj, 2019). Utöver stater, finns det även statsunderstödda aktörer samt kriminella organisationer som bedriver offensiva cyberoperationer. Det finns även mindre avancerade aktörer som utgör ett mindre hot, exempelvis olika lösa grupperingar och enskilda individer vilka använder redan existerande skript eller kod för att göra intrång i informationssystem. Fördelningen är dock inte så enkel.

För det första finns det en skillnad mellan demokratiska stater och autokratiska stater. Demokratiska stater har uttryckt att man följer internationell rätt och krigets lagar, samtidigt som myndigheter och förband som bedriver t.ex. offensiva cyberoperationer och cyberunderrättelseoperationer följer det demokratiska landets lagar och regler, men också befintliga överenskomna uttalade normer. Autokratiska stater som t.ex. Ryssland (Donner & Schwartz, 2014) och totalitära stater som t.ex. Kina (Babones, 2021) påstår sig följa internationell rätt och befintliga överenskomna uttalade normer, men deras beteende och handling säger annat. Nedan följer två exempel: Ryssland och Kina.

Ryssland angrep Estland 2007 efter att den dåvarande estniska regeringen beslöt att omlokalisera en sovjetisk staty i Tallinn i april 2007 (Ottis, 2008). Attackerna analyserades ur ett informationskrigsperspektiv som visade att de var politiskt motiverade. Dessutom visade vissa indikatorer att angriparna fick stöd från den ryska staten eftersom den ryska regeringen inte samarbetade med den estniska utredningen för att identifiera angriparna (Ottis, 2008). Ryssland har fortsatt att bedriva cyberangrepp mot länder i dess intressesfär, som t.ex. Ukraina och Georgien, men även mot länder som Sverige (Säkerhetspolisen, 2021; Collier & Leopold, 2018), Finland (SUPO, 2020), Norge (Reuters, 2021) och Danmark (Reuters, 2017).

Kina bedriver cyberangrepp internt för att kontrollera sin befolkning och externt för bl.a. dataförstörelse, förneka access, och spionagesyfte. De interna angreppen har riktats mot bl.a. tibetaner (men även utomlands) (CSIS, 2021), den muslimska uiguriska minoriteten (Crawley, 2019) och även mot Hong Kong-demonstranter (Mozur & Stevenson, 2019). Externt, bedriver man angrepp mot t.ex. ”journalister och verktyg som tillåter yttrandefrihet online” (DNI, 2021, s.8) men även mot Sverige (FRA, 2017, 2021; PwC & BAE Systems, 2017; Stubbs, Menn & Bing, 2019a, 2019b); Finland (SUPO, 2020), Norge (Stubbs, 2019) och Danmark (The Local, 2014).

Studiet av hoten från användningen av IKT har genomförts av FN:s fem grupper av statliga experter (Group of Governmental Experts, GGE). Den första gruppen samlades 2004 och: "It examined the impact of developments in information and communications technologies (ICTs) on national security and military affairs. The experts also considered whether their discussions should focus on information content or only on information infrastructure." (UNODA, 2019). Den första gruppen av statliga exporter lyckades inte att komma överens. Den tredje expertgruppen sammankallades 2014/2015 och det var först då som man kom överens om elva "norms, rules or principles of the responsible behaviour of States in the cyber-sphere as well as confidence building measures, international cooperation and capacity building, which could have wider application to all States" (UNODA, 2019, s. 2).

Normerna, reglerna eller principerna (uttalade normer) kan indelas i begränsande karaktär och "god praxis och positiva skyldigheter för internationell säkerhet" (CCDCOE, u.å.), men eftersom normerna, reglerna eller principerna är frivilliga och icke-bindande (FN, 2015), kan man anta att detta inte hindrar stater från att bedriva offensiva cyberoperationer. Denna rapport fokuserar endast på de fem uttalade normerna som anses vara av begränsande karaktär.

Men för att kunna förstå staters agerande i cyberrymden krävs det även en förståelse för de *outtalade* normerna som finns hos respektive stat. Outtalade normer är kopplade till samhällets så kallade oskrivna regler. Outtalade normer är intersubjektiva, vilket innebär att de baseras på subjektiva uppfattningar som delas av ett samhälle, eller en grupp inom ett samhälle. Outtalade normer kan exempelvis vara underliggande föreställningar, idéer och tankar om moral som formar människor (Åkesson, 2016, s. 3)

Konceptet om outtalade normer kommer från sociologin och är starkt kopplat till identitet och makt. När det handlar om outtalade normer och identitet drar man ofta parallellen till socialkonstruktivismen och dess teoretiska ståndpunkt att samhället konstrueras av dess människor, deras samspel och kommunikation med varandra (Agius, 2019, ss. 75-81). Ytterligare en viktig aspekt är att hur outtalade normer upplevs beror på plats och tid och att outtalade normer inte är statiska och förändras i tid och rum (Forum för levande historia, u.å.). Åkesson (2016, s. 14) beskriver outtalade normer som att "Normer har också att göra med hur vi förstår vår verklighet och vad vi tycker är sant och rätt, samt vilka föreställningar vi har om oss själva, andra och det omgivande samhället".

Därför leder det till frågan: ***Vilka nationella outtalade normer kan utläsas hos stater som bryter mot internationella överenskommelser i cyberrymden?***

Svaret på frågan fås genom att kartlägga staters uttalade normer (t.ex. cybersäkerhetsstrategier) i förhållande till deras faktiska beteende (offensiva cyberoperationer) i cyberrymden för att identifiera potentiella luckor mellan dem och befintliga överenskommelser. Genom att utgå från fem (5) av de normer, regler eller principer

(hädanefter normer), som anses vara av begränsande karaktär, granskas nio av FN:s medlemsstater och deras cyberoperationer de senaste 15 åren, mellan 2005 och 2020.

Klassificeringen bygger på Council on Foreign Relations (CFR) databas Cyber Operations Tracker (COT) som spårar cyberoperationer och deras syfte och mål. Syftena är uppdelade i åtta (8) kategorier: dataförstörelse, vandalism, DDoS, doxing, hack-n-leak, spionage (underrättelseinhämtning) och/eller finansiell vinning (CFR, 2021a). Författarna lade till kategorin ”hack-n-leak” för att specifikt bryta ut cyberoperationer med syfte att störa val.

Målen är indelade i fyra sektorer: civilsamhället, regeringar/myndigheter, militär och privatsektor. Författarna är medvetna om att stater, som t.ex. Kina, använder grupperingar för att under dagtid tjäna det kommunistiska partiet, och efter arbetstid bedriva ”ransomware”-angrepp för gruppens egen ekonomiska vinning dessa beaktas dock inte i rapporten. Vidare är författarna medvetna om att det genomförs cyberoperationer i industrispionage-syfte allierade-emellan (väst-mot-väst), detta beaktas dock ej i rapporten då det är utanför dess syfte.

Den här rapporten utvärderar slutligen med information utvunnet främst från COT vilka stater som bryter mot fem (5) av FN:s uttalade normer som anses vara av begränsande karaktär, och i vilken utsträckning. Därefter analyseras de enskilda staternas *outtalade* normer baserat på socialkonstruktivistisk teori och empirin ur COT, de outtalade normerna presenteras i form av fem teman/kategorier: ”Idéer om identitet med FN & självbild”; ” Uppfattning om Nationell Säkerhet”; ”Upplevda hotbilder”; ”Uppfattning om makt”; och ”Moral och lönsamhet.” Slutligen tolkas analysen i syfte att tolka vad det kan innebära för internationellt samarbete och samspel i cyberrymden.

COT har dock två begränsningar: a) informationen bygger på öppna källor, och b) personalen bakom COT är engelskspråkiga. Därmed bör det noteras att eftersom COT bygger på öppna källor är det naturligt att cyberoperationer som aldrig uppdagas inte heller finns med. Dessutom är det viktigt att ha i åtanke att informationen som COT inhämtar från är främst engelska källor, vilket innebär att det finns en inbyggd partiskhet i databasen. Emellertid, och som noterats ovan, har än dock vissa slutsatser kunnat dras trots den möjliga inbyggda partiskheten.

Rapporten är strukturerad enligt följande. Först beskrivs **2. Cyberrymden och offensiva cyberoperationer**, följt av resultatet **3. Staters beteende i Cyberrymden**. Därefter följer **4. Diskussion - Vad betyder detta?** och **5. Slutsatser**, **6. Avslutande reflektioner** och slutligen **7. Framtida studier**.

2 Cyberrymden och offensiva cyberoperationer

För att förstå operationsmiljön så måste man förstå cyberrymden. Cyberrymden definieras som "hårdvara och mjukvara som används för att skapa, bearbeta, lagra, hämta och sprida information i olika typer av sammankopplade nätverk som bygger ett stort, globalt nätverk, byggt och som används av människor" (Huskaj, 2019). Definitionen gör det som annars kan anses väldigt otydligt (cyber) till något greppbart och tydligt visar att cyberrymden existerar tack vare datorer och informationssystem som är uppkopplade i nätverk av nätverk, och som möjliggörs tack vare informations- och telekommunikationsteknologi.

Datorerna och de uppkopplade informationssystemen används av människor för att skapa, bearbeta, lagra, hämta och sprida information ur detsamma. Utöver människor kan även andra datorer, informationssystem, industriella styr- och kontrollsystem och IoT-enheter göra detsamma.

Operationer definieras som "en sekvens av planerade handlingar som utförs av en organiserad grupp människor med ett definierat syfte" (Huskaj & Wilson, 2020) i att uppnå ett mål. Målet kan vara strategiskt, operativt eller taktiskt.

Genom att beakta ovan, definieras offensiva cyberoperationer som:

> "en sekvens av planerade handlingar som utförs av en organiserad grupp människor med ett definierat syfte i och genom hårdvara och programvara som används för att skapa, bearbeta, lagra, hämta och sprida information i olika typer av sammankopplade nätverk som bygger ett stort, globalt nätverk, byggd och används av människor. Den offensiva aspekten inkluderar metoder för att påverka en motståndares målsystems konfidentialitet, integritet och / eller tillgänglighet"
>
> (Huskaj & Wilson, 2020).

Offensiva metoder är handlingar en operatör gör för att ge instruktioner till en dator som syftar till att påverka ett annat mål (dator, informationssystem, motsv.). Tabell 1 presenterar några offensiva metoder.

Tabell 1. Offensiva metoder med deras svenska och engelska benämning. Källa: Lotsson (2018; 2019a-d; 2020).

Offensiva metoder	Offensiva metoder (forts.)
Buffertöverfyllning (buffer overflow) [1]	Social manipulering (social engineering)
Behörighetsintrång (privilege escalation)	Man-i-mitten-attack (man-in-the-middle)
Spökprogram (rootkit)	Överbelastningsattack (denial of service)

[1] Se Förkortningar-kapitlet en lista på offensiva metoder.

Definitionerna är viktiga eftersom det minimerar risken för feltolkning för vad cyberrymden är; vad offensiva cyberoperationer är; offensiva metoder samt relaterade mål.

Vidare innebär dessa förklaringar möjligheter att jämföra offensiva metoder med typ av cyberoperation för att påvisa om en offensiv metod behövs för att en viss typ av cyberoperation ska lyckas. Tabell 2 nedan visar detta.

Tabell 2. Cyberoperationstyper och relaterade offensiva metoder.

Cyberoperationstyp	**Offensiv metod**[1]
Dataförstörelse	Offensiv metod (t.ex. social engineering) eller insider för att få fotfäste hos målets informations- och nätverkssystem.
DDoS	Offensiv metod (t.ex. social engineering, nyttjandet av sårbarhet) för att hacka datorer för att sedan nyttja dessa som ”zombier” i överbelastningsattacker.
Doxing	Offensiv metod (t.ex. social engineering, bruteforce) för att hacka sig in i målets email och/eller sociala-medier-konton.
Hack-n-leak[2]	Offensiv metod (t.ex. social engineering, bruteforce) för att hacka sig in i målets email och/eller sociala-medier-konton för att stödja en informationsoperation.
Finansiell stöld	Offensiv metod (t.ex. social engineering, bruteforce) för att ta sig in i målets informations- och nätverkssystem.
Sabotage	Offensiv metod (t.ex. social engineering, bruteforce, buffer overflow) för att ta sig in i målets informations- och nätverkssystem.
Spionage	Offensiv metod (t.ex. social engineering, bruteforce, buffer overflow) för att ta sig in i målets informations- och nätverkssystem.
Vandalism	Offensiv metod (t.ex. social engineering, bruteforce, buffer overflow) för att ta sig in i målets informations- och nätverkssystem.

[1] Se Förkortningar-kapitlet en lista på offensiva metoder.

[2] Enligt Vilmer (2019) är ”hack-n-leak” en informationsoperation.

Tabell 2 visar alltså att stater och relaterade aktörer har en vilja och intention att genom cyberrymden använda sig av offensiva handlingar och metoder med intentionen att medvetet sätta hårdvara, mjukvara, nätverk i ett tillstånd som de inte var avsedda för. Syftet med offensiva cyberoperationer kan vara att skaffa sig ekonomiska fördelar, förneka motståndare att skaffa sig vissa förmågor, men också i underrättelsesyfte.

Med andra ord kan syftet vara att använda sig av offensiva cyberoperationer som maktmedel i den internationella miljön. Att å ena sidan arbeta för uttalade normer, regler och lagar och att å andra sidan bedriva offensiva cyberoperationer är två exempel på uttalade och outtalade normer. Att det finns en uttalad norm nedskriven betyder inte automatiskt att det blir en outtalad norm att följa den uttalade normen, eftersom outtalade normer är sociala konstruktioner som uppkommer och ändras genom social förändring. Det innebär att

outtalade normer inom cybersäkerhet också är konstruerade och skapas av människan. Det är därför även möjligt att ändra nuvarande outtalade normer, genom till exempel att ifrågasätta och jobba mot att förändra dem.

3 Staters beteende i Cyberrymden

Alla stater under granskning bedriver offensiva cyberoperationer men syftet kan variera. En offensiv metod krävs för att t.ex. kunna genomföra en cyberunderrättelseoperation. Ett exempel på en offensiv metod är Spear-phishing. COT listar att det primära syftet med offensiva cyberoperationer (totalt 431 stycken) av de nio staterna under granskning är underrättelseinhämtning / spionage (totalt 337), följt av sabotage (totalt 17) och DDoS (totalt 17), Vandalism (totalt 15), Dataförstörelse (totalt 11), Finansiell stöld (totalt 7), Doxing (totalt 6) samt hack-n-leak (2). Totalt 21 offensiva cyberoperationer var inte kategoriserade av COT. Tabell 3 listar antalet cyberoperationer och deras syfte, medan tabell 4 visar vilka av FN:s gemensamma uttalade normer som har brutits genom nämnda cyberoperationer.

Tabell 3. Antal cyberoperationer som syfte per land i alfabetisk ordning.

Indikator	CN	FR	IL	IR	NK	NL	RU	UK	US
Hur många cyberoperationer totalt har staten genomfört mellan 2005–2020?	178	1	8	61	48	1	113	3	18
Har staten bedrivit Dataförstörelse?	1	-	1	4	1	-	2	-	2
Har staten bedrivit Vandalism?	-	-	-	1	-	-	9	-	5
Har staten bedrivit DDoS?	2	-	1	3	4	-	4	-	3
Har staten bedrivit Doxing?	-	-	-	-	2	-	4	-	-
Har staten bedrivit hack'n-leak inför val-rörelser (motsv.).	-	-	-	-	-	-	2[1]	-	-
Har staten bedrivit underrättelseinhämtning / spionage?	162	1	4	45	30	1	86	2	6
Har staten bedrivit operationer för finansiell vinning?	-	-	-	-	7	-	-	-	-
Har staten bedrivit sabotage?	1	-	2	3	-	-	8	1	2
(CO utan kategori)	12	-	-	5	4	-	-	-	-

[1] Rysslands hack-n-leak operation som påverkade det amerikanska valet 2016 klassas som ”compromise” av COT. Författarna har valt att explicit bryta ut för att påvisa påverkans-delen som cyberoperationer kan stödja. Den andra hack-n-leak operationen är den misslyckade påverkansoperationen mot det franska valet.

Tabell 4. Uttalade normer[1] (FN) som en stat har brutit genom sina cyberoperationer.

Norm	CN	FR	IL	IR	NK	NL	RU	UK	US
Stater bör inte medvetet tillåta att deras territorium används för internationellt felaktiga handlingar som använder IKT	x	x	x	x	x	x	x	x	x
Stater bör inte bedriva eller medvetet stödja IKT-verksamhet som avsiktligt skadar kritisk infrastruktur	x		x	x	x		x		x
Stater bör vidta åtgärder för att säkerställa försörjningskedjans säkerhet och bör försöka förhindra spridning av skadlig IKT och användning av skadliga dolda funktioner	x		x	x	x		x		x
[2] Stater bör inte bedriva eller medvetet stödja verksamhet för att skada informationssystemen för en annan stats beredskapsteam (CERT / CSIRTS) och bör inte använda sina egna team för skadlig internationell aktivitet									
Stater bör respektera FN: s resolutioner som är kopplade till mänskliga rättigheter på internet och till rätten till integritet i den digitala tidsåldern	x	x	x	x	x	x	x	x	x

[1] Normerna är hämtade från https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.

[2] Information som pekar på att stater medvetet har skadat informationssystemen för en annan stats beredskapsteam saknas.

Tabellen bör inte läsas i isolation utan förstås bäst tillsammans med svaren på frågeformuläret nedan samt sektionen diskussion och resultat. Frågeformuläret återfinns i Bilagan. Vidare bör det noteras att en cyberoperation kan ha flera mål och att siffrorna i tabellen inte matchar. Nedan följer sammanfattningar på alla stater under granskning och deras beteende i cyberrymden i alfabetisk ordning baserat på domännamn (t.ex. .cn, .fr, .il):

3.1 Kina (CN)

Kina ser cyberoperationer som en delmängd inom ramen för informationskrigsföring. I deras nationella cybersäkerhetsstrategi "China's Cyberspace National Security Strategy: Actively Defending Network Sovereignty!" (2016) nämns det att en av fyra strategiska uppgifter är att med kraft försvar den kinesiska cyberrymdens suveränintet genom att "adopt all measures including economy, administration, science and technology, law, diplomacy, and military, and unswervingly safeguard China's cyberspace sovereignty" (Red Dragon 1949, 2018). I samma strategi nämns det att "Without cybersecurity, there is no national security" (Red Dragon 1949, 2018). Det står även att alla aktörer som på något sätt försöker att påverka Kinas cyberrymdssuveränitet eller nationella säkerhet kommer att bestraffas. När och hur Kina bedriver cyberoperationer är upp till kommunistpartiet. Tabell 5 visar alla kinesiska cyberoperationer, typ och mål.

Tabell 5. Kinesiska cyberoperationer, typ och mål.

Mål	Fördelning	Dataförstörelse	DDoS	Doxing	Hack-n-Leak	Finansiell Stöld	Sabotage	Spionage	Vandalism	CO utan Typ	CO utan Typ/mål
Regeringar	87	-	-	-	-	-	-	84	-	3	-
Militär	21	-	1	4	1	-	-	21	-	-	-
Privatsektor	89	1	2	-	-	-	1	82	-	3	-
Civilsamhälle	39	-	1	3	4	-	-	36	-	2	-
Mål saknas	10	-	-	-	-	-	-	3	-	-	7
(CO utan kategori)		-	-	-	-	-	-	-	-	-	-

[1] Notera att en cyberoperation kan ha flera mål och att siffrorna i tabellen inte matchar, detta gäller alla tabeller.

Kina bedriver cyberoperationer när kommunistpartiet anser att dess intressen riskerar att påverkas. Den andra strategiska uppgiften går ut på att förhindra, stoppa och straffa:

> "Prevent, stop and punish any use of the Internet for treason, secession, sedition, subversion or incitement to subvert the people's democratic dictatorship; prevent, deter and punish the use of the Internet for theft, disclosure of state secrets and other acts that endanger national security; Prevent, stop and punish foreign forces in the use of the network for infiltration, destruction, subversion and separatist activities."
>
> (Red Dragon 1949, 2018).

Kinas ställning i världen ökar samtidigt som deras nationella intressen ökar. De nationella intressena är kopplade till investeringar och affärsverksamheter runtom i världen. Dessa växande intressen kräver en förmåga att ge säkerhet (Dahlgren, 2019, s. 5; RAND, 2016).

Den nationella cybersäkerhetsstrategin, i kombination med de nya lagarna (underrättelselagen, kontraspionagelagen och cybersäkerhetslagen) öppnar för Kina att bedriva cyberoperationer kontinuerligt över tiden. Den hårda tonen i den nationella cybersäkerhetsstrategin kopplat till kommunistpartiets styrning leder till att Kina använder sig av cyberangrepp som ett instrument för nationell politik.

Kina använder sig främst av cyberspionageoperationer för att driva sin politiska agenda framåt. I några få fall visar empirin att Kina har genomfört cyberoperationer för att förneka (överbelastningsattacker) dissidenters access till Internet och relaterade tjänster. I dagsläget saknas annan information än det som inhämtats från COT för hur Kina använder sig av cyberangrepp för den nationella politiken. RAND (2016) noterar dock att ”Kina kan ha en högre risktröskel än vad USA kan förvänta sig, särskilt när det gäller att försvara sådana ’kärnintressen’ som territorium och suveränitet.”

Det i kombination med Kinas [tvetydiga] ”no-first-use”-policy beträffande kärnvapen skulle eventuellt kunna överföras till storskaliga attacker på cyberområdet. Indikationer finns dock på att landet kommer att fortsätta bedriva cyberoperationer och angrepp mot mål som anses hota landets intressen (RAND, 2016). Kombinationen av det samt landets uttalade norm i cybersäkerhetsstrategin att använda sig av alla nödvändiga medel för att säkra sina nationella intressen innebär att Kina kan komma att bedriva en aggressiv cyberkonflikt när den måste. Däremot är det svårt att säga hur Kina kommer att bete sig *efter* en cyberkonflikt då staten har dementerat alla former av uttalanden om att landet bedriver offensiva cyberoperationer, främst i spionagesyfte mot västländer och relaterad privatsektor.

3.2 Frankrike (FR)

Frankrike har sedan 2008 ansett cyberrymden som en militär domän. Landet har i minst tio (10) dokument bidragit till utvecklingen av den militära cyberstrategin (Delerue et al., 2019). Det bör noteras att utöver den militära cyberstrategin så bedriver de olika underrättelsetjänsterna egna cyberoperationer, som inte täcks av den militära cyberstrategin (Delerue, et al., 2019). COT har registrerat endast en cyberoperation (SnowGlobe). Tabell 6 visar den franska cyberoperationen, typ och mål. Författarna har även valt att diskutera cyberoperationen ”SnowGlobe”, för att ge insikt i vilka tänkbara mål en statsaktör kan tänkas rikta sin cyberunderrättelseinhämtning mot. Tabell 7 visar utsatta länder.

Tabell 6. Frankrikes cyberoperationer typ och mål.

Mål	Fördelning	Dataförstörelse	DDoS	Doxing	Hack-n-Leak	Finansiell Stöld	Sabotage	Spionage	Vandalism	CO utan Typ	CO utan Typ/mål
Regeringar	1	-	-	-	-	-	-	1	-	-	-
Militär	-	-	-	-	-	-	-	-	-	-	-
Privatsektor	1	-	-	-	-	-	-	1	-	-	-
Civilsamhälle	-	-	-	-	-	-	-	-	-	-	-
Mål saknas	-	-	-	-	-	-	-	-	-	-	-
(CO utan kategori)	-	-	-	-	-	-	-	-	-	-	-

Cyberkonflikt i Frankrike har hörsammats och den franska försvarsministern lanserade landets militära cyberstrategi genom uttalandet “Cyber warfare has begun and France must be ready to fight it,” (Parly, 2019, som citerat av Delerue et al.). Lanseringen av den militära cyberstrategin och att publikt diskutera dess offensiva och defensiva delar syftar till att bekräfta Frankrikes status som en cybermakt (Delerue et al., 2019). När och hur Frankrike bedriver cyberoperationer visas av cyberoperationen Snowglobe. Snowglobe, daterat 2014, är enligt COT den enda noterade cyberoperationen, och bedöms vara associerad med Animal Farm. Animal Farm är “A threat actor, confirmed to be the French government, that targets governments, companies, media organizations, military contractors, and humanitarian organizations” (CFR, 2021d). Syftet med Snowglobe var underrättelseinhämtning riktat mot entiteter/organisationer enligt tabell 8.

Tabell 7. Länder utsatta för fransk underrättelseinhämtning.

Stater i alfabetisk ordning		
Algeriet	Malaysia	Storbritannien
Elfenbenskusten	Nederländerna	Syrien
Grekland	Norge	Turkiet
Iran	Ryssland	Tyskland
Kina	Spanien	USA

Follorou och Untersinger (2014) noterar att den kanadensiska signalunderrättelsetjänsten (CSE) identifierade ett okänt program/mjukvara (Snowglobe) avsedd för utrikes underrättelseinhämtning. Väl i målet, inhämtar mjukvaran epost från specifika och riktade konton (Follorou och Untersinger, 2014). Cyberunderrättelseoperationen Snowglobe riktade sig mot allierade och icke-allierade stater och deras organisationer (Follorou och Untersinger, 2014). Även om Snowglobe inte var ett cyberangrepp (det var en operation för utrikes underrättelseinhämtning), så visar operationen att Frankrike använder cyberoperationer som ett instrument för nationell säkerhetspolitik. Snowglobe riktade sig exempelvis mot Iran med fokus på nukleär forskning; europeiska supranationella organisationer som t.ex. European Financial Association; tidigare franska kolonier som t.ex. Algeriet och Elfenbenskusten; samt fransktalande organisationer som t.ex. media-organisationer (Follorou och Untersinger, 2014).

Tabell 8. Målen i Iran utsatta för fransk underrättelseinhämtning.

Entitet / Organisation	
Utrikesdepartementet	Irans universitet för vetenskap och teknologi
Irans atomenergiorganisation	Irans Datakommunikation
Iranska forskningsorganisationen för vetenskapsteknologi, Imam Hussein University	Universitetet Malek-E-Ashtar

Det är svårt att utifrån informationen på COT säga hur Frankrike bedriver cyberkonflikt när den måste: SnowGlobe är den enda cyberoperationen som loggats. Emellertid påvisar uttalandet "Cyberkrig har börjat och Frankrike måste vara redo att bekämpa det" (Parly, 2019, som citerat av Delerue et al.) vid lanseringen av den militära cyberstrategin att Frankrike har förmågor att bedriva offensiva cyberoperationer. Den första delen av den militära cyberstrategin definierar militäroffensiv cyberkrigföring som "alla militära åtgärder som genomförs i cyberrymden, till stöd eller inte för andra militära förmågor.

Cybervapen syftar, i enlighet med internationell rätt, att skapa effekter mot ett kontroversiellt datorsystem för att ändra tillgänglighet eller datakonfidentialitet" (Delerue, et al., 2019). Dessutom har man ökat och tilldelat betydande resurser för rekrytering av "cyber-kombattanter" från 3000 till 4000, och 1,6 miljarder Euro kommer att investeras för detta syfte (franska försvarsmaktsministeriet, 2018).

Hur har Frankrike betett sig efter Snowglobe? Enligt CFR:s byråchef Grigsby (2016) har Frankrike erkänt att de låg bakom SnowGlobe. Detta genom att den tidigare chefen för Frankrikes signalunderrättelsetjänst kopplad till utrikesunderrättelsetjänsten, DGSE Bernard Barbier, höll ett tal vid ett av Frankrikes bästa ingenjörsskolor och råkade försäga sig.

Sammanfattningsvis har Frankrike det som behövs för att kunna bedriva offensiva och defensiva cyberoperationer: en strategi, ett förhållningssätt mot internationell rätt, uttalat publikt i media att man investerar och rekryterar personal för att bedriva cyberoperationer, samt att man riktat budskapet både mot allierade och mot hotaktörer att de tänker bedriva cyberoperationer om de måste, samt att de tilldelat resurser och har en intention att bedriva offensiva cyberoperationer. Cyberoperationer i underrättelsesyfte bedrivs av de olika underrättelsetjänsterna.

3.3 Israel (IL)

Israel (IL) har tre (3) nationella strategier: resolution 3611 (2011), IDF-strategin (2015), och resolution 3270 från 2017 (UNIDIR, 2021b). Dessa visar också landets syn på cyberkonflikt. Resolution 3611:

> "The current National cyber-strategy of Israel stemmed from the National Cyber Initiative and was declared in the Government Resolution 3611 'Advancing the national capacity in cyberspace'. The Israeli strategy aims at cyber-power, including more comprehensive defence, advanced research and development, developing cyber-technology as an economic growth engine, and leveraging cybersecurity for enhanced international cooperation. The Israel National Cyber Bureau (INCB) was established to develop and implement the strategy."
>
> (Tabansky & Ben Israel, 2015, s. 49).

IDF-strategin finns i två versioner: 2015 och 2017. Eftersom båda är på hebreiska kommer 2015 att nämnas från UNIDIR (2021b). Enligt UNIDIR (2021b), listar IDF-strategin från 2015 fem punkter:

- Cyberdimensionen av nationell säkerhet måste stärkas, för att uppnå likhet med Israels befintliga underrättelse-, flyg- och sjöövelägsenhet;
- Skydds-, inhämtnings- och attackoperationer kommer att genomföras i cyberdomänen och Israel måste öka sin beredskap på detta område;
- En cyberorganisation från den israeliska försvarsmakten (IDF) ska inrättas för att utveckla landets cyberförmågor;
- IDF måste kunna fungera även under cyberattack;
- En kritisk del av cybersäkerhet är att utveckla cyberkrigsfunktioner för att stärka strategisk och taktisk avskräckning.

(UNIDIR, 2021b).

Israel bedriver cyberoperationer för att öka sitt inflytande i både Mellanöstern och i världen. Det indikerar på att Israel genomför cyberoperationer främst med syfte att inhämta underrättelser, men även för att sabotera, möjligen i samband med vedergällning. Israel, som i och med sitt unika geopolitiska läge ständigt känner sig under hot, använder cyberattacker som ett instrument för nationell politik eftersom de ser det som nödvändigt för att skydda deras stat och dess nationella intressen. Tabell 9 visar israeliska cyberoperationer.

Tabell 9. Israeliska cyberoperationer typ och mål.

Mål	Fördelning	Dataförstörelse	DDoS	Doxing	Hack-n-Leak	Finansiell Stöld	Sabotage	Spionage	Vandalism	CO utan Typ	CO utan Typ/mål
Regeringar	1	-	-	-	-	-	-	1	-	-	-
Militär	4	1	1	-	-	-	1	1	-	-	-
Privatsektor	5	1	-	-	-	-	1	3	-	-	-
Civilsamhälle	-	-	-	-	-	-	-	-	-	-	-
Mål saknas	-	-	-	-	-	-	-	-	-	-	-
(CO utan kategori)	-	-	-	-	-	-	-	-	-	-	-

Israel bedriver cyberkonflikt bland annat som vedergällning och som svar på incidenter då de själva blivit attackerade. Det ses då som en angelägenhet för nationell säkerhet och självförsvar. Ett exempel på detta är när Iran misstänkes för att ha försökt att hacka Israels vattenbolag (Ari Gross, 2020). Dessutom är det intressant att bedöma deras starka allians med USA och gemensamma cyberoperationer . Till exempel Stuxnet 2010 som riktades mot Iran vilken med största sannolikhet var en offensiv cyberoperation utförd tillsammans med USA.

Israel är starkt allierade med USA och Israel har stora motsättningar med Iran,. Detta syns även när man granskar empirin från COT då Iran är det land som främst är drabbat av israeliska cyberoperationer, liksom att Israel har bedrivit flest gemensamma cyberoperationer med USA. Resultatet är egentligen inte särskilt chockerande. Israel har ett nationellt intresse att bevara sin strategiska relation med USA. Det är alltså viktigt för bägge parter- Israel behöver USA som sin allierade med tanke på sitt unika geopolitiska läge, , samtidigt som USA har intressen i Mellanöstern och har ett nationellt intresse av att ha kvar Israel som allierad. Med tanke på Israels geopolitiska läge, kultur, statsskick och historia så är det mer sannolikt att de kommer att (fortsätta) fokusera på sitt närområde när det kommer till cyberoperationer och därför fortsätta hålla en god relation med i USA (Utrikespolitiska Institutet, 2021).

Israel har inte erkänt några cyberattacker hittills.

3.4 Iran (IR)

Iran (IR) har sedan Stuxnet utvecklat sina cyberförmågor, eller som den israeliske generalen Padan (2017) uttryckte det:

> "They are not the state of the art, they are not the strongest superpower in the cyber dimension, but they are getting better and better"
>
> (Padan, citerat av Rabinovitch, Cohen & Pleck, 2017).

Då en officiell cybersäkerhetsstrategi ej har identifierats, har Irans generalstab uttryckt att internationell rätt gäller i cyberrymden och bl.a. att ett förbud mot användning av våld och aggression kan gälla för användning av cyberrymden (UNIDIR, 2021a).

Iran är bland de mest aktiva staterna i cyberrymden och använder sig av offensiva cyberoperationer som ett instrument för nationell politik och som maktmedel i den internationella miljön. De använder sig av cyberoperationer för att öka sitt inflytande i Mellanöstern och många av attackerna riktar sig bland annat mot Israel. Iran bedriver även cyberspionage internationellt mot universitet (Cuthbertson, 2018), och angrepp mot kritisk infrastruktur (BBC, 2015a). De bedriver även många cyberoperationer mot Sverige, bland annat för spionage mot universitet och företag. Tabell 10 visar iranska cyberoperationer typ och mål.

Tabell 10. Iranska cyberoperationer typ och mål.

Mål	Fördelning	Dataförstörelse	DDoS	Doxing	Hack-n-Leak	Finansiell Stöld	Sabotage	Spionage	Vandalism	CO utan Typ	CO utan Typ/mål
Regeringar	32	-	-	-	-	-	2	26	-	-	-
Militär	5	-	-	-	-	-	-	5	-	-	-
Privatsektor	42	4	3	-	-	-	2	28	1	-	-
Civilsamhälle	13	-	-	-	-	-	-	13	-	-	-
Mål saknas	2	-	-	-	-	-	-	1	-	-	-
(CO utan kategori)		-	-	-	-	-	-	-	-	-	-

Iran ser cyberattacker som en del av ett kontinuum av konflikt. IRGC:s ställföreträdande befälhavare Hossein Salami sa:

> "We are in an atmosphere of a full-blown intelligence war with the US and the front of enemies of the Revolution and the Islamic system … This atmosphere is a combination of psychological warfare and cyber operation, military provocations, public diplomacy and intimidation tactics" (Salami, citerat av Lewis, 2019).

Iran förnekar att de är statssponsor när de misstänks ha bedrivit cyberattacker och förnekar ofta när de har blivit angripna, alternativt påstår att angreppen misslyckats. Iran förnekade redan 2010 när Stuxnet angrep deras uraninriktningscentrifuger (BBC, 2010). Detta beteende, att bekräfta men att tona ner, påvisas när Iran angrep komponenter i Israels vatteninfrastruktur men åstadkom ingen skada. Israel hämnades med angrepp på ”Shahid Rajaee”-hamnterminal, vars verksamhet stannade plötsligt och oförklarligt (Warrick & Nakashima, 2020). Iran bekräftade så småningom att de blivit utsatta för en cyberattack, men tonade ändå ner händelsen.

3.5 Nordkorea (NK)

Nordkorea (NK) saknar en officiell nationell cyberstrategi. Den primära drivkraften för en säkerhetsstrategi har varit att avskräcka utländsk inblandning genom att skaffa en kärnvapenförmåga; eliminera upplevda hot mot Kim-regimen, och upprätta en tro på att Nordkorea har rätt till respekt som en världsmakt (DHHS, 2021). Nordkorea har sedan 2009 utvecklat sina cyberförmågor, organisatoriskt, och med olika taktiker, tekniker och procedurer (Raska, 2020a), och uppvisar ett asymmetriskt uppträdande:

> “The use of cyber weapons of mass effectiveness alongside weapons of mass destruction provides Pyongyang with a unified asymmetric strategy designed to pressure the United States and the wider international community to recognize its legitimacy”
>
> (Raska, 2020b).

Nordkorea har strikta ekonomiska sanktioner mot sig på grund av sitt kärnvapenprogram. USA, tillsammans med likasinnade stater, har många gånger försökt att avskräcka Nordkoreas aktiviteter, både när det kommer till kärnvapenprogrammet men även när det gäller deras aktiviteter i cyberrymden. Nordkorea har sett på dessa aktiviteter som ett hot mot regimen och dess politiska och ekonomiska utveckling.

Mot den bakgrunden har Nordkoreas cyberoperationer sedan 2014 ökat och fokuserat på ekonomisk och politisk krigföring i syfte att kringgå de införda internationella sanktionerna (Raska, 2020a) för att kunna generera intäkter (DuBois, 2020). Cyberoperationerna syftar även till att säkra landets regimöverlevnad, bland annat genom politiskt spionage. Nordkoreas konventionella militära förmåga försvagas men de bedriver cyberoperationer för att fortsätta ses som relevanta av stormakter (Jun et al., 2015, s.12). Tabell 11 visar Nordkoreanska cyberoperationer, typ och mål.

Tabell 11. Nordkoreanska cyberoperationer typ och mål.

Mål	Fördelning	Dataförstörelse	DDoS	Doxing	Hack-n-Leak	Finansiell Stöld	Sabotage	Spionage	Vandalism	CO utan Typ	CO utan Typ/mål
Regeringar	18	-	2	1	-	1	-	11	-	2	-
Militär	2	-	1	-	-	-	-	1	-	-	-
Privatsektor	32	-	3	1	-	6	1	18	-	3	-
Civilsamhälle	3	-	-	1	-	-	-	2	-	-	-
Mål saknas	3	-	-	-	-	-	-	2	-	-	-
(CO utan kategori)	-	-	-	-	-	-	-	-	-	-	-

Nordkorea använder sig av statssponsrade aktörer, som t.ex. Hidden Kobra (Cybersecurity & Infrastructure Security Agency, 2017) och Lazarus. Lazarus misstänks bland annat ha legat bakom två stora incidenter: cyberattacken mot Sony Pictures 2014 och WannaCry (Corera, 2017).

Raska (2020b) noterar att Nordkoreas offensiva cyberoperationer visar på åtminstone tre distinkta egenskaper: a) deras enheter har visat stor mångfald vad gäller deras förmåga vilket gör attribuering svårt; b) Nordkorea har gradvis visat på beslutsamhet för cyber-eskalering riktad mot andra staters kritiska infrastruktur, såväl som privata företag och banker för olika politiska motiv, och c) den väsentliga "dialektiken" i NKs cyberrymd är fortfarande asymmetrisk.

NKs internetinfrastruktur av isolerad från övriga världen och går igenom två internetleverantörer: Kinas Unicorn och Rysslands TransTeleCom. Det innebär att nordkoreanska statssponsrade hotaktörer är spridda och kan befinna sig på andra håll i världen, bland annat Kina och Ryssland. Nordkorea är det enda landet som har bedrivit cyberoperationer för finansiell vinning.

Nordkorea förnekar att bedriva cyberoperationer eftersom de har en historia att förneka ansvar för deras operationer (Recorded Future, u.å.). I Sony Pictures-fallet uppvisade landet ett annat uppträdande när de erbjöd sig att samarbeta med USA gällande dataintrång, trots att Nordkorea hade utpekats som angripare. USA nekade erbjudandet (BBC, 2015b).

3.6 Nederländerna (NL)

Nederländerna (NL) har i sex (6) olika strategier beskrivit syftet med att investera i cyberförmågor, hur man ser på cybersäkerhet, samarbeten på internationell nivå, identifierat cyberhot som allt viktigare, och betonat att cyberhot är ett av de viktigaste hoten (UNIDIR, 2021c). Tabell 12 visar Nederländernas cyberoperationer, typ och mål

Tabell 12. Nederländernas cyberoperationer typ och mål.

Mål	Fördelning	Dataförstörelse	DDoS	Doxing	Hack-n-Leak	Finansiell Stöld	Sabotage	Spionage	Vandalism	CO utan Typ	CO utan Typ/mål
Regeringar	1	-	-	-	-	-	-	1	-	-	-
Militär	-	-	-	-	-	-	-	-	-	-	-
Privatsektor	-	-	-	-	-	-	-	-	-	-	-
Civilsamhälle	-	-	-	-	-	-	-	-	-	-	-
Mål saknas	-	-	-	-	-	-	-	-	-	-	-
(CO utan kategori)	-	-	-	-	-	-	-	-	-	-	-

Emellertid har Nederländerna (NL) bedrivit endast en cyberoperation mellan 2005 och 2020 med syftet spionage enligt COT. Cyberspionageoperationen var riktad mot den ryska statssponsrade-gruppen "Cozy Bear" som man bedömer låg bakom DNC-hacket under det amerikanska valet 2016 (Noack, 2018). Enligt Noack (2018) lyckades AIVD, den holländska underrättelse- och säkerhetstjänsten, ta sig in i den ryska gruppens nätverk, CCTV-kameror, och även bedöma lokaliseringen av gruppens lokaler till en universitetsbyggnad nära det röda torget. Den inhämtade informationen delgavs CIA och NSA.

Ytterligare information om hur NL använder cyberangrepp som ett instrument för nationell politik och cyberkonflikt saknas (till författarnas kännedom).

3.7 Ryssland (RU)

Ryssland har sex (6) strategier där ”doktrinen om informationssäkerhet” diskuterar fem områden för att säkerställa informationssäkerhet för nationellt försvar (UNIDIR, 2021d). I korthet är dessa 1) säkerställa strategisk avskräckning och förhindra militär konflikt; 2) uppgradera försvarsmaktens och relaterade entiteters informationssäkerhetssystem; 3) förutspå, identifiera och bedöma informationshot; 4) främja intressen för Rysslands allierade i informationssfären; 5) utjämna information och psykologisk handling, där utjämna har betydelsen ”att motverka en effekt genom att motverka den med något av samma kraft” (Oxford Lexico, 2021).

Ryssland ser cyberoperationer som en delmängd av informationskrigföring. I Ryssland pratas det inte om cyberkrigföring som en egen kategori, utan den ligger under paraplykonceptet informationskrigföring. Ryssland betraktar informationskrigföring som del av en helt egen krigsdomän, och cyber är en förlängning av den. Utöver cyberoperationer ingår även (bland annat) nätverksoperationer, elektronisk krigföring och påverkansoperationer i kategorin informationskrigföring (Connell & Vogler, 2016, s.1).

Ryssland använder informations- och cyberoperationer (informationskrigsföring) som ett instrument för nationell politik nationellt och internationellt för att underminera staters självförtroende när dessa går mot ryska intressen. Rysslands strategiska och nationella politiska vinning väger tyngre än att följa FN:s gemensamma normer. Rysk informationskrigföring täcker även, indirekt, staters allierade när dessa går mot ryska intressen: ”titta vad som händer när (eller om) ni går emot oss”.

Ytterligare exempel inkluderar för att kontrollera sin befolkning; stärka sitt inflytande på den internationella arenan och desinformation. Ryssland gör detta genom så kallade ”troll”; ”hackers” / ”crackers” (nationella och internationella), egna myndigheter (t.ex. FSB och SVR) och i kombination med konventionella militära maktmedel (hybridkrigföring). Tabell 13 visar ryska cyberoperationer typ och mål.

Tabell 13. Ryska cyberoperationer, typ och mål.

Mål	Fördelning	Dataförstörelse	DDoS	Doxing	Hack-n-Leak	Finansiell Stöld	Sabotage	Spionage	Vandalism	CO utan Typ	CO utan Typ/mål
Regeringar	66	1	3	1	2	-	3	84	1	2	-
Militär	16	-	1	-	-	-	-	21	1	1	-
Privatsektor	42	2	1	-	-	-	6	82	2	3	-
Civilsamhälle	24	-	-	4	-	-	2	36	-	-	-
Mål saknas	-	-	-	-	-	-	-	3	-	-	-
(CO utan kategori)	-	-	-	-	-	-	-	-	-	-	-

Bedömningen är att Ryssland ständigt vill bli betraktat som en stormakt i världsordningen tillsammans med USA och Kina. De bedriver främst cyberoperationer för att främja sina egna nationella intressen då de känner att deras regim är det minsta hotad. Flera exempel på Rysslands aggression i cyberrymden existerar, där några av dessa är: överbelastningsattackerna mot Estland 2007 då estniska webbplatser som Estlands regering, banker och medie- och nyhetsföretag angreps; inför och under Georgienkriget 2008 när Ryssland gick in för att ”avbryta folkrättsliga kränkningar i utbrytarrepublikerna Syd Ossetien och Abkhazien” (Fällman, 2010); inför och under den illegala annekteringen av Krimhalvön; och det så kallade ”DNC-hacket” (Democratic National Committee) när man bröt sig in i demokraternas email-server och använde WikiLeaks som publikationsplats (Nakashima & Harris, 2018).

Dessutom användes ”troll” och ”trollfabriker” för att föra sin agenda i cyberrymden framåt. Troll och trollfabriker använder exempelvis under valåret 2016 i USA, vilket var ett effektivt sätt för Ryssland för att underminera USA och deras cybersäkerhet i samband med valet (Jensen et al., 2019; Kurowska & Reshetnikov, 2018).

Ryssland sponsrar och tar hjälp av både nationella och internationella hackers och företag, vilket började under andra Tjetjenienkriget (år 2002). Då tog ryska studenter som också var hackers ner en populär webbsida som drevs av de tjetjenska rebellerna, och den ryska regeringen såg fördelen med att sponsra hackers för att driva sin agenda framåt. Fördelen med detta för Rysslands del är att de då, tack vare attribueringsproblematiken, skapa trovärdig förnekbarhet. För att kontrollera sin egen befolkning sponsrar Ryssland även internationella hackare och på så sätt utnyttjar Ryssland återigen de stora gränsöverskridande möjligheterna digitaliseringen har bidragit med till att föra sin politiska agenda framåt i cyberrymden (Soldatov & Borogan, 2018, s. 18).

I Ukraina-fallet används cyberoperationer i kombination med konventionella militära maktmedel (men ligger varje gång under tröskeln för krig). Detta och ovanstående exempel visar hur Ryssland bedriver cyberkonflikt när den måste.

Under och efter cyberkonflikt förnekar Ryssland alla anklagelser om att använda sig av cyberoperationer och nyttjar attribueringsproblematiken till sin fördel samtidigt som man skyller på västvärldens anti-ryska policy och paranoia när de blir anklagade för att vara hotaktör. Exempelvis påstod den ryska ambassaden i Washington att USA diskuterat så kallad "rysk inblandning" i presidentval i åratal, utan relevanta bevis (Bülow, 2020). Attribueringsproblematiken nyttjas också efter att cyberoperationer attribuerats till dem: det inte är statssponsrat utan kan vara patriotiska hackers som "hjälper fosterlandet", eller på så kallade "false-flag" -operations (Jensen et al., 2019, s. 226).

Förnekelse är också en genomgående linje i Ryssland, de förnekade till exempel NotPetya, som är starkt attribuerat till dem (BBC, 2018a). Rysslands förnekar inte endast aktiviteter när det kommer till cyberoperationer, det kan man även se under annekteringen av Krim då Putin förnekade att ha soldater i Ukraina. Likaså senast när Ryssland förnekade att de hade försökt att förgifta oppositionspolitikern Aleksej Navalnyj (Dagens Nyheter, 2020; Sjöström 2014).

Ryssland uttrycker även ofta att det är kränkande att bli utpekad som hotaktör när cyberattacker upptäckts och bekräftas att vara från ryskt territorium eftersom det i nästan alla fall saknas konkrets bevis. Till exempel, när Norges regering blev attackerade av rysk cyberoperation i oktober 2020 skyllde det norska parlamentet på Ryssland. Ryssland svarade då med påståenden som att "sådana uttalanden är oacceptabla" och att de kräver en förklaring (BBC, 2020; Посольство Российской Федерации в Норвегии, 2020)

Från Rysslands perspektiv ses det som att de automatiskt blir utpekade som hotaktör på grund av västerländsk paranoida och ingrodda anti-ryska policy, och att ge Ryssland skulden för cyberattacker är västerländsk desinformation (Holmqvist, 2021, s. 11), samtidigt som Ryssland uttrycker att det är kränkande att bli utpekad som hotaktör.

Ryssland pekades exempelvis ut som hotaktör av bl.a. Storbritannien i ett uttalande som anklagade Ryssland för att ligga bakom cyberattacker mot deras underrättelsetjänst. Ryssland svarade på detta med att de tycker att hotet från Ryssland är påhittat, och att Storbritannien har en policy som är ryssfientlig. Med andra ord uttrycker de det som att UK baserar sina påståenden på en tradition av västerländsk mobbing mot Ryssland (Imeson, 2019)

Sammanfattningsvis kan man säga att från ett västerländskt perspektiv att Ryssland bedöms kunna att starta en cyberoperation mer lättvindigt än troligen de flesta västerländska länder skulle tycka, bl.a. USA. Det ses i sin tur som aggressivt och offensivt, och som Connell & Vogler (2016) uttrycker det, bidrar till en provokation och därmed riskerar att bidra till eskalation i en redan kylig relation.

3.8 Storbritannien (UK)

Storbritanniens (UK) nya vision som en cybermakt är att vara en "responsible and democratic cyber power" (Steed, 2021). Fem policy-inriktningar ges för att uppnå detta: " influence, technological edge, a whole-of-nation cyber ecosystem, offensive cyber, and diplomacy" (Steed, 2021). Syftet med offensiva cyberoperationer är att detektera, störa och avskräcka UKs motståndare. Detta kommer att göras genom upprättandet av en "National Cyber Force" som är ett joint venture mellan GCHQ och försvarsdepartementet, men även personal från Secret Intelligence Service och Defense Science and Technology Laboratory (Steed, 2021).

Cybermakt definieras som:

> "The ability to protect and promote national interests in and through cyberspace: to realise the benefits that cyberspace offers to our citizens and economy, to work with partners towards a cyberspace that reflects our values, and to use cyber capabilities to influence events in the real world. Like wider S&T power, cyber power depends on the Government pursuing a whole-of-nation effort, bringing together industry and academia in partnership. It also involves engaging citizens, who have a central role to play in our national cyber security"
>
> (The UK Cabinet Office, 2021).

Storbritannien har en stark cyberförmåga och bedriver cyberoperationer internationellt i bl.a. spionage och sabotage-syfte. Att Storbritannien bedriver cyberoperationer i spionagesyfte är inget anmärkningsvärt då landet är med i Five-Eyes-underrättelsealliansen som består av ytterligare fyra engelsktalande länder: Kanada, Australian, Nya Zeeland och USA. Storbritannien har även tillsammans med USA inom ramen för terrorismbekämpning (BBC, 2018b) bedrivit cyberoperationer i sabotage-syfte mot Daesh. Tabell 14 visar brittiska cyberoperationer typ och mål.

Tabell 14. Brittiska cyberoperationer typ och mål.

Mål	Fördelning	Dataförstörelse	DDoS	Doxing	Hack-n-Leak	Finansiell Stöld	Sabotage	Spionage	Vandalism	CO utan Typ	CO utan Typ/mål
Regeringar	1	-	-	-	-	-	-	1	-	-	-
Militär	-	-	-	-	-	-	-	-	-	-	-
Privatsektor	2	-	-	-	-	-	-	2	-	-	-
Civilsamhälle	1	-	-	-	-	-	1 [1]	-	-	-	-
Mål saknas	-	-	-	-	-	-	-	-	-	-	-
(CO utan kategori)	-	-	-	-	-	-	-	-	-	-	-

[1] COT klassificerar cyberoperationen mot terrorgruppen DAESH som civilsamhället.

3.9 USA (US)

USA (US) har 15 strategier men den som fokuserar på genomförandet av cyberoperationer är "DoD Cyber Strategy 2018" (DoD, 2018). Här uttrycks det att amerikanska cyberförband kommer att operera jämsides med luft-, land-, sjö- och rymdförband, och att offensiva cyberoperationer kommer att genomföras över hela konfliktspektrat (DoD, 2018).

USA:s cyberstrategi pekar även ut vilka de anser vara de största rivalerna/motståndarna i cyberrymden: Ryssland, Kina, Iran och Nordkorea. Detta är förståeligt då många statsattribuerade grupper som riktar cyberoperationer mot USA opererar från Ryssland, bland annat FancyBear som tros ha kopplingar till den ryska underrättelsetjänsten; från Kina, exempelvis gruppen Zirconium, samt från Iran, exempelvis Phosphorous (Bülow, 2020).

USA använder offensiva cyberoperationer som ett instrument för nationell politik. USA:s offensiva cyberoperationer riktar sig mot mål internationellt som t.ex. Nordkorea (Gallagher, 2017) och Iran (Ali & Stewart, 2019). Det görs själv eller tillsammans med andra, som t.ex. Stuxnet med Israel, men även med andra organisationer. USA är, likt Storbritannien, till exempel med i underrättelsealliansen "Five Eyes". De samarbetade när de hackade ryska Google Yandex 2018 (Bing, Stubbs & Menn, 2019). USA använder även cyberoperationer en syftet att bekämpa terrorism. Tabell 15 visar amerikanska cyberoperationer typ och mål.

Tabell 15. Amerikanska cyberoperationer typ och mål.

Mål	Fördelning	Dataförstörelse	DDoS	Doxing	Hack-n-Leak	Finansiell Stöld	Sabotage	Spionage	Vandalism	CO utan Typ	CO utan Typ/mål
Regeringar	9	1	3	-	-	-	1	4	-	-	-
Militär	7	1	1	-	-	-	3	2	-	-	-
Privatsektor	6	1	-	-	-	-	1	4	-	-	-
Civilsamhälle	2	-	-	-	-	-	2	-	-	-	-
Mål saknas	-	-	-	-	-	-	-	-	-	-	-
(CO utan kategori)	-	-	-	-	-	-	-	-	-	-	-

USA bedriver cyberoperationer när deras intressen och nationella säkerhet hotas eller när deras avskräckning mot en hotaktör "misslyckas." USA genomförde offensiva cyberoperationer som vedergällning mot t.ex. Iran 2019, och mot exempelvis Ryssland för deras inbladning i "DNC-hacket". Hur USA beter sig efter en cyberkonflikt är starkt kopplat till den sittande presidenten. Personlighetsaspekter hos presidenterna beaktas inte i rapporten.

När Stuxnet slog till mot Iran 2010 och det mesta pekade mot USA erkände aldrig Obama-administrationen någon inbladning i det hela. Hittills har endast före detta president Donald Trump (2020) erkänt en cyberattack mot Ryssland år 2018 (Thiessen, 2020). Donald Trump erkände även att US Cyber Command bedrev en cyberoperation mot Iran 2019 för att sabotera/degradera Irans militära vapensystem (raket- och missiluppskjutningssystem) samt cyberattacker mot ryska trollfabriker år 2019 (som hade hänt 2016).

Trots att Donald Trump (USA) erkände cyberattacker mot Ryssland och ryska trollfabriker pekas USA inte ofta ut som huvudmisstänkt aktör (i alla fall inte i västerländsk media) - men man kan återigen som i alla andra fall dra en parallell till attriubueringsproblematiken - man kan inte med hundra procents säkerhet säga att de inte har gjort det och sedan kommit undan. Däremot så införs sanktioner mot länder som tros ha bedrivit cyberoperationer mot USA, exempelvis mot Kina (TT, 2018) och 2014 då Sony Hacket inträffade (som nämnd i sektionen om Nordkorea).

Cyberoperationen var å ena sidan inte riktad mot staten USA i sig men mot Sony Pictures som låg i USA, varför man valde ändå att koppla attacken till Nordkorea. Nordkorea förnekade som sagt sin inblandning men USA valde att ge straffpåföljder mot Nordkoreanska organisationer och aktörer som ett svar. Likaså försökte man offentligt hänga ut Nordkorea med taktiken "Name and shame" trots att man till hundra procent inte kunde veta vem det var som var angriparen. Strax efter Sony Hacket erbjöd sig Nordkorea att samarbeta vad gäller dataintrång, men USA nekade (BBC, 2015b).

4 Diskussion - Vad betyder detta?

Rapportens syfte var att svara på frågan: ***Vilka nationella outtalade normer kan utläsas hos stater som bryter mot internationella överenskommelser i cyberrymden?*** Rapporten identifierade outtalade normer hos de nio staterna under granskning vad rör idéer, föreställningar och moral som delades in i fem övergripande kategorier: 1. Idéer om ens identitet i världsordningen och därför självbild, 2. Uppfattning om nationell säkerhet 3. Upplevda hotbilder; 4. Uppfattning om makt; samt 5. Uppfattning och moral kring lönsamhet. Diskussionen är indelad i två delar: den första delen diskuterar empirin urvunnen ur COT och del två presenterar de möjliga tolkningar som kan göras om vilka outtalade normer som finns i cyberrymden baserat på den funna empirin och socialkonstruktivistisk teori.

4.1 Diskussion av empiri och resultat COT

Alla stater under granskning bedriver cyberunderrättelseoperationer; västerländska staters cyberoperationer förekommer i mindre omfattning i databasen än icke-västerländska och auktoritära stater; Frankrike och Nederländerna har endast bedrivit cyberunderrättelseoperationer; Storbritannien och USA har, utöver cyberunderrättelseoperationer, även bedrivit sabotage, medan det är endast USA som har bedrivit t.ex. dataförstörelse.

Vidare, icke-västerländska och auktoritära staterna varierar i operationstyp: när Kina har bedrivit en cyberoperation för sabotage, eller dataförstörelse, har Ryssland bedrivit nio (9) cyberoperationer för sabotage och två (2) för dataförstörelse. Ryssland har också en större palett då landet använder sig av Doxing (4), Hack-n-leak (2) och Vandalism (3), vilket t.ex. Kina inte gör. Att Ryssland använder sig av Doxing och Hack-n-leak är sannolikt ett tecken på statens perspektiv på cyberoperationer som en delmängd av informationsoperationer, inklusive påverkansoperationer.

Även Iran har bedrivit vandalism (1), och Nordkorea har bedrivit Doxing (3), men det är endast Nordkorea som har bedrivit cyberoperationer för finansiell vinning (7). Slutligen visar empirin från COT att trots antalet genomförda cyberoperationer så är en liten del av de som har genomförts för att sabotera eller förstöra. Tabell 16 visar genomförda typer av cyberoperationer, där Ryssland använder sig av cyberoperationer för att uppnå nästan alla nämnda effekter (6 av 7) (ej finansiell stöld), följt av Iran och Nordkorea (5 av 7); Kina, Israel och USA (4 av 7); UK (2 av 7); Frankrike och Nederländerna (1 av 7).

Tabell 16. Staters cyberoperationer typ.

Mål	Dataförstörelse	DDoS	Doxing	Hack-n-Leak	Finansiell Stöld	Sabotage	Spionage	Vandalism
Kina	x	x	-	-	-	x	x	-
Frankrike	-	-	-	-	-	-	x	-
Israel	x	x	-	-	-	x	x	-
Iran	x	x	-	-	-	x	x	x
Nordkorea	x	x	x	-	x	-	x	-
Nederländerna	-	-	-	-	-	-	x	-
Ryssland	x	x	x	x	-	x	x	x
Storbritannien	-	-	-	-	-	x	x	-
USA	x	x	-	-	-	x	x	-

Vidare, det finns också en skillnad i hur staterna bedriver sina cyberoperationer. De icke-västerländska och auktoritära staterna tillåter medvetet hotaktörer (proxies) bedriva offensiva cyberoperationer; staterna genomför medvetet offensiva cyberoperationer som till del stör och förstör kritisk infrastruktur, som t.ex. de ryska angreppen på Ukraina; staterna bedriver/genomför handlingar och aktiviteter för att påverka "supply chain security" t.ex. SolarWinds; de icke-västerländska och auktoritära staterna respekterar inte FN-resolutioner gällande mänskliga rättigheter på Internet och deras "privacy" i den digitala tidsåldern.

Vissa stater använder sig av organiserad brottslighet för att bedriva offensiva cyberoperationer. Gemensamt för de icke-västerländska och auktoritära staterna är att alla förnekar sin inblandning i cyberoperationer. Västerländska stater väljer dock att inte *kommentera* eventuella cyberoperationer, som t.ex. Nederländerna, medan auktoritära stater i stor utsträckning väljer att *förneka*.

Ytterligare en skillnad är att de västerländska staterna endast bedriver cyberoperationer internationellt, medan de icke-västerländska och auktoritära staterna bedriver cyberoperationer nationellt och internationellt. Vidare skulle man kunna säga att Ryssland och Kina, med sina helhetsperspektiv på informationskrigsföring där cyberoperationer och nätverksoperationer är en delmängd av dessa, de facto använder det koncept som USA tog fram under det första Irak-kriget "Desert Storm" 1991: "Information Warfare."

Slutligen, när staters cyberoperationer ställs mot det som klassificeras som cyberattack, det vill säga handlingar som skapar förnekande (degradera, störa, förstöra) effekter antingen i cyberrymden eller i den (cyber)fysiska domänen, har Kina, Israel, Iran, Ryssland och USA bedrivit cyberoperationer med alla tre nämnda effekter i åtanke. Nordkorea har bedrivit cyberoperationer med endast två nämnda effekter i åtanke. Storbritannien har bedrivit cyberoperationer med endast en effekt i åtanke, medan Frankrike och Nederländerna ej har bedrivit effekt-baserade cyberoperationer. Det bör också noteras att den inbyggda asymmetrin i cyberdomänen medger att ett land som Nordkorea kan utgöra ett hot mot USA. Tabell 17 visar staternas effektbaserade cyberoperationer.

Tabell 17. Staters effektbaserade cyberoperationer.

	Förstöra	**Degradera** **Störa**	**-**	**-**	**-**	**Degradera** **Störa** **Förstöra**	**-**	**-**
Stat	**Dataförstörelse**	**DDoS**	**Doxing**	**Hack-n-Leak**	**Finansiell Stöld**	**Sabotage**	**Spionage**	**Vandalism**
Kina	x	x	-	-	-	x	x	-
Frankrike	-	-	-	-	-	-	x	-
Israel	x	x	-	-	-	x	x	-
Iran	x	x	-	-	-	x	x	x
Nordkorea	x	x	x	-	x	-	x	-
Nederländerna	-	-	-	-	-	-	x	-
Ryssland	x	x	x	x	-	x	x	x
Storbritannien	-	-	-	-	-	x	x	-
USA	x	x	-	-	-	x	x	-

Vidare, alla nio stater bryter mot åtminstone två av FN:s uttalade normer, vilket syns i Tabell 4. Alla stater har till exempel brutit mot norm 1 och 5. Däremot måste den data läsas tillsammans med Tabell 3. En viktig aspekt är nämligen att de demokratiska staterna inte har brutit mot normerna i samma utsträckning som de auktoritära staterna har, då det är skillnad på att bryta norm 1 med en cyberoperation som Frankrike gjorde, och på att bryta norm 1 exempelvis 178 gånger, som Kina gjorde. Att Frankrike har brutit på norm 1 en gång är inte lika allvarligt som att Kina har brutit mot den normen 178 gånger.

4.2 Tolkningar av outtalade normer

Med resultatet av empirin från COT, tillsammans med kunskap om staternas historia, kultur, statsskick och relation till varandra, kan möjliga tolkningar göras om vilka outtalade normer som finns i cyberrymden och därmed kan forskningsfrågan besvaras.

Det är exempelvis märkbart att de demokratiska och auktoritära staterna har olika synsätt på världen, och därigenom även olika outtalade normer som styr deras beteende i den internationell miljön. Att förstå staternas synsätt på världen, staternas prioriteringar och agerande i cyberrymden har stor betydelse för att kunna tolka de outtalade normerna. Den här rapporten har identifierat fem övergripande kategorier med outtalade normer som kan tolkas av deras beteende av att använda sig av offensiva cyberoperationer som maktmedel i den internationella miljön, och de grundas i socialkonstruktivismen, nämligen idémässiga faktorer (staters möjliga uppfattningar, idéer, moral etc).

Dessa kategorier är: 1. Idéer om ens identitet i världsordningen och därför självbild, 2. Uppfattning om nationell säkerhet 3. Upplevda hotbilder; 4. Uppfattning om makt; samt 5. Uppfattning och moral kring lönsamhet. Trots att dessa fem kategorier med outtalade normer är tätt sammanlänkade och bör förstås i anslutning till varandra kommer de för klarhetens skull att diskuteras var för sig.

4.2.1 Idéer om identitet med FN & självbild

En möjlig tolkning av staternas skilda beteende när det kommer till att förhålla sig till FN:s gemensamma uttalade normer är den underliggande idén om identitet och självbild. Det finns det en stor skillnad på vilka stater som kan identifiera sig med FN och dess arbete med att främja fred. Det innebär att de västerländska och demokratiska staterna med stor sannolikhet känner en större press på sig att anpassa sig till FN:s uttalade normer, då de kan identifiera sig med den organisationen.

Auktoritära stater har inte som prioritet att identifieras med FN som organisation. De har exempelvis ett gemensamt intresse att ändra det internationella systemet för att kunna främja deras egna stater, vilket även blir tydligt inom cyberdomänen. Vidare, för de icke-västerländska och auktoritära staterna, finns det också andra organisationer som står dem kulturellt, historiskt och ideologiskt närmare. Till exempel Kina och Ryssland - båda är officiellt med i FN, men är två av de nio länderna som har bedrivit flest operationer och även brutit mot nästan alla cybernormer (4 av 5). De ser det med stor sannolikhet inte lika viktigt att följa FN:s normer som att rätta sig efter Shanghai Cooperation Organisation (SCO), där Ryssland och Kina kommit överens om att nationella intressen är prioritet.

Däremot ser man den senaste tiden ett maktskifte, och öst börjar få mer inflytande i FN (mer om detta längre ner). Detta syns även utifrån empirin från COT då FN:s syn på uttalade

normer traditionellt har utgått från en västerländsk tradition; men idag kan man se att USA drar sig från FN. Med detta så passar Ryssland och Kina på att ta över mer i FN, vilket leder till maktskiftet. Maktskiftet innebär också att auktoritära normer och värderingar tar mer plats i FN då fler ryska och kinesiska företrädare tar plats som chefer för befintliga och nya organisationselement och kan därmed tämligen självständigt bestämma tolkningar, aktiviteter, anställningar och befordran.

Detta är dock inte första gången det händer. Ett tidigare och tydligt exempel är debatten vad gäller Internationella Teleunionen – ett specialorgan inom FN- som handlade om västs perspektiv på att fokusera på global infrastruktur. Kina och Ryssland ville dock även täcka in innehåll och kunde då med stöd av arabiska länder ta över ITU som ett medel för att stärka auktoritära normer.

Det blir intressant att följa hur detta maktskifte kommer att utveckla sig och hur det kommer att påverka både de uttalade och outtalade normerna i cyberrymden vad gäller stater, deras självbild, och hur de identifierar sig med FN.

4.2.2 Uppfattning om nationell säkerhet

Stater har olika idéer om vad nationell säkerhet är och hur det förhåller sig till internationella relationer. Därför är det möjligt att tolka deras olika beteende och deras användning av offensiva cyberoperationer. För de flesta auktoritära stater går nationens säkerhet, och därför egenintresset, alltid först. Det går också hand i hand med hur man uppfattar användandet av offensiva cyberoperationer: ses det som en antagonistisk hämndaktion, eller legitimt försvar? De auktoritära staterna Kina, Iran, Nordkorea och Ryssland handlar på ett eller annat sätt efter egenintresse, och det är ingen skillnad när det gäller cyberrymden.

Att Ryssland bedriver offensiva cyberoperationer med syftet politiskt spionage kan bero vilket upplevt hot västvärlden utgör mot dem och därmed deras nationella säkerhet, lika mycket som väst ser Ryssland som ett hot. Om det är legitimt beror på perspektiv, från västs perspektiv ses det inte som legitimt, men tittar man på Rysslands historia och dess kultur ser de det med stor sannolikhet som legitimt, då de också vill stärka sitt inflytande i den pågående stormaktskonflikten. Det handlar om att vilja stärka och bevara sitt auktoritära styre (och då även hur de förhåller sig till andra stater - det handlar alltid om en rationell kalkyl när man ingår i en allians, där man väger in hur en annan stat kan främja ens egenintresse).

Kina och Ryssland har inte plötsligt skapat en bra relation för att de började tycka om varandra, utan för att de främjar varandras intressen, bland annat att peta ner USA från första platsen i stormaktstävlingen och kunna stärka sina auktoritära stater. Den outtalade normen för de auktoritära staterna blir så att försvara deras nationella säkerhet genom att ha en

aggressivare offensiv förmåga, vilket skapar spänningar när det kommer till att följa gemensamma uttalade normer.

När det kommer till de västerländska länderna USA, Frankrike, Nederländerna och Storbritannien, har de samma outtalade normer när det kommer till uppfattningen om nationell säkerhet är. Det finns mycket vilja till samarbete. Västländerna har samma värderingar och dels samma intressen – helt enkelt att samarbeta och främja fred. Det blir även intressant då man tittar på Israel, som är en demokrati med västerländska värderingar i Mellanöstern. För deras del handlar det också om att ha en stark relation för att upprätthålla sin nationella säkerhet, genom en bra relation med västvärlden och i synnerhet USA.

4.2.3 Upplevda hotbilder

Vad stater har för upplevd hotbild kan hjälpa att förstå varför gemensamma uttalade normer bryts i cyberrymden. Upplevda hotbilder går hand i hand med identitet och uppfattning om makt. Upplevda hotbilder styr om och varför stater väljer att använda sig av offensiva cyberoperationer. Ryssland t.ex. ser väst som ett hot, och därför bedriver de politiskt spionage. De "VET" att stater i västvärlden har en försvarsmakt som kanske försöker rusta upp för att möta hotet från dem, och då vill de veta exempelvis hur västvärldens militärförmåga ser ut. Likadant med Nordkorea: de ser USA och väst som ett hot mot deras regim och bedriver cyberoperationer i finansiellt syfte för att kunna fortsätta att finansiera sin slutna regim.

För auktoritära stater ses även kritik inifrån regimen som ett stort hot. Då demokratier tror på fri- och rättigheter och främjar dialog och oliktänkande, så är de auktoritära regimerna rädda för att det ska skapas grupper i deras samhälle med nya outtalade normer. De vill inte att yngre människor skapar grupper med nya normer som på något sätt hotar regimens outtalade normer som ofta bygger på strikt kontroll, oförändrade värderingar och regimstabilitet. Därför väger det möjligtvis tyngre för Iran att kunna bedriva cyberspionageoperationer för att samla underrättelser om exempelvis iranier i exil än att följa FN:s gemensamma normer.

Däremot så är den upplevda hotbilden i västvärlden ofta kopplat till asymmetriska hot som internationell terrorism och extremism (exempelvis högerextremism), vilket ses som ett legitimt mål att bedriva cyberoperationer mot, då det följer den outtalade normen att främja fred. Det är påtagligt när man undersöker vilka USA samt Storbritannien har riktat sina operationer mot och vilka sorts cyberoperationer de öppet erkänner, som t.ex. mot Daesh.

4.2.4 Uppfattning om makt

Vilka idéer stater har kring vad makt är kan hjälpa att förstå varför vissa stater bryter mot FN:s internationella uttalade normer medan andra stater inte gör det i lika stor utsträckning. Uppfattning om makt och vad det är går hand i hand med identitet och självbild. De auktoritära staterna uppfattar det som att ha makt när man är resursstark och självständig men även att man av andra stater uppfattas som skrämmande.

Auktoritära stater ser det som mäktigt att vara en stormakt i världen för man då har kontroll över resurser på ett annat sätt. Man måste förstå denna strävan i kontexten till deras historia, som ofta har brottats med instabilitet och ett ständigt tillstånd av krig (till exempel Nordkorea). Effekten blir att de fortfarande är i ett tillstånd av vaksamhet att vilja bevara sin egen stat. Det innebär att den outtalade normen kopplat till makt blir att ju mer resurser du har tillgång till, och ju mäktigare andra stater uppfattar dig, ju mäktigare är du.

På det sättet kan de uppnå två mål. Om dessa stater uppfattas som fruktade och skrämmande, signalerar det att man har makt och det ses som en avskräckning från att bli attackerad, och därför får de stanna i stormaktsspelet, och det signalerar till sin egen befolkning att det inte är en bra idé att gå mot regimen.

Uppfattning om makt handlar också om att kunna kontrollera sin egen befolkning, genom att låta dem tro att staten är fruktad, stark och skrämmande. Exempelvis Nordkorea, som är en sluten stat - de vill inte mot några som helst omständigheter öppna upp sitt samhälle mot omvärlden, de behöver upprätthålla sin propaganda om regimen för att säkerställa omvärlden och den egna befolkningens uppfattning om statens makt. Makt handlar om säkerheten av regimen, och för att säkerställa den får regimen inte öppnas upp, för då skulle det komma fram för den kontrollerade befolkningen hur omvärlden styrs, och att Kim Jong Un inte är lika mäktig som de blir manipulerade till att tro.

På det sättet väger Nordkorea och andra auktoritära staters egenintresse om regimöverlevnad tyngre än att följa FN:s gemensamma normer – de kan genom offensiva cyberoperationer få ett finger med i spelet på världskartan som en av de mest aktiva och fruktade hotaktörerna i cyberrymden och därmed bestryka sin uppfattning om att vara mäktiga. Det pekar på att en stat som bedriver offensiva cyberoperationer är uppdaterad i det digitaliserade samhället, att man har makt och kapacitet att skada en annan stats kritiska infrastruktur, oberoende hur många militära trupper de har.

Vidare, det är intressant att reflektera kring Iran och deras syn på makt och hur de vill bli uppfattade av omvärlden. Uppfattning om identitet och självuppfattning kan också kopplas till de auktoritära staternas syn på prestige och stolthet, exempelvis Iran, som ofta inte erkänner att de blivit attackerade av en cyberoperation utan bagatelliserar det istället.

De demokratiska länderna, i synnerhet länderna i Europa, ser däremot makt som att vilja främja fred, vara öppen för dialog och arbeta med orättvisa i världen och humanitära frågor.

De europeiska länderna har relativt sett starka ekonomier och resurser är inte ett lika stort problem som hos de auktoritära staterna. I västvärlden ses det även som att samarbete är makt och att ensam är inte stark. Det bidrar till att det finns stora olikheter i värdet i vad makt är mellan demokratiska och auktoritära stater.

De auktoritära staterna lägger mer prioritet på att framställa sig själva som mäktiga genom att visa sina "muskler", medan demokratier visar sin uppfattning om vad makt är genom att jobba mot alla människors fri- och rättigheter. Det synd exempelvis på att stater som är med i EU, i denna studie Frankrike och Nederländerna, i sina nationella cyberstrategier fokuserar mest på resiliens och utbildning – en stor skillnad mot Rysslands och Kinas som öppet skriver att de tar till vilka medel som än krävs för att skydda sin regim och dess regerande i cyberrymden.

4.2.5 Moral och lönsamhet

En fjärde outtalade norm som styr staters agerande handlar om det ses som moraliskt lönsamt att bedriva en cyberoperation och därmed bryta mot FN:s gemensamma uttalade normer. Detta går hand i hand med egenintresse och uppfattning om vad makt är. För länderna som bedriver offensiva cyberoperationer, vare sig det är Kina som bedriver industriellt spionage, Ryssland som bedriver politiskt spionage, USA som bekämpar terrorism, eller Nordkorea som ägnar sig åt finansiell vinning, så handlar det i grund och botten om lönsamhet med cyberoperationerna, och med detta sagt kan det dras paralleller till möjligheterna och problemen med att vara aktiv i cyberrymden.

Skillnaden mellan att bedriva konventionell krigföring är att man kan komma undan med cyberoperationer tack vare attribueringsproblematiken: det finns sällan straff utan endast en fördömanden. Det är även svårt, men inte omöjligt, att kunna ge en specifik stat skulden för en attack. Därför blir det svårt att avskräcka stater eftersom det sällan finns konsekvenser av cyberattacker, som t.ex. att bestraffa en stat för dess offensiva cyberoperationer.

För auktoritära stater ses en fördömelse inte som något som hotar deras regim, snarare tvärt om. Därför ses det som lönsamt att bedriva cyberoperationer mot andra stater om man får ut information ur till exempel en cyberspionageoperation som kan hjälpa att kartlägga det landets militära kapacitet. Det är dessutom ett modernt sätt att få uppmärksamhet i media och därigenom få en annan stat att frukta ens egen utan en riktig motåtgärd. Det går även hand i hand med att cyberoperationer i många fall är ett billigt sätt att kunna driva sin politiska agenda framåt.

En tankeväckande, men inte särskilt förvånande trend i cyberrymden är att flertalet auktoritära stater, där bland annat Ryssland, bedriver cyberoperationer med syftet spionage mot flertalet forskningscenter som tog fram vaccin under 2020 i samband med Covid 19-pandemin. En möjlig tolkning av detta handlar också om lönsamhet, att det ses som lönsamt

att vara i framkant i utvecklingen av vaccin, det går hand i hand med uppfattningen om makt och självbild och identitet.

Om en demokratisk stat däremot bryter mot en av FN:s gemensamma uttalade normer ses det förmodligen som pinsamt och omoraliskt, då det går mot tanken om att främja fred, stabilitet och internationellt samarbete. Det kan skada förtroende för den staten och därmed inte ses som lönsamt då många av västvärldens länder ser det som viktigt med samarbete och förtroende emellan varandra. Men när de demokratiska staterna bedrivit cyberoperationer mot terroristorganisationer så ses det som lönsamt då det är för ett gott ändamål som främjar fred.

Resultaten från rapporten måste sättas i kontext i dagens osäkra säkerhetspolitiska läge och blir därför inte särskilt förvånande med tanke på det dystra omvärldsläget. Med det sagt så kommer resultaten av rapporten, att alla nio stater på ett eller annat sätt och i olika utsträckningar bryter mot FN:s uttalade normer, med stor sannolikhet att fortsätta även i framtiden, så länge staterna känner att det är lönsamt att göra så. Resultaten pekar på att outtalade normer i respektive stat som rör idéer om identitet, nationella intressen, uppfattning om makt och lönsamhet och moral spelar stor roll i förståelsen om hur de använder sig av offensiva cyberoperationer som maktmedel i den internationella miljön.

Baserat på ovan, kan tesen att agerandet i cyberrymden följer geopolitik och geoekonomi – direktinvesteringar och framskjutna positioner – göras. Cyberdomänen, en ung domän, har inneburit nya möjligheter men även nya angreppssätt och till viss del gjort det svårt att applicera tänk efter resultaten av Första, Andra och det Kalla Kriget. Ett konkret exempel är cyberspionage. Spionage är ett accepterat fenomen i internationell rätt och har bedrivits så länge människan har existerat. Det finns dock en skillnad i konsekvenserna av spionage som görs av en mänsklig agent mot cyberspionage. En mänsklig agent tar en mängd risker och har inte tidigare kunnat ta med sig hur mycket hemligheter som helst, medan med cyberspionage så kan man stjäla en industris hela kunskap om stridsflygplan, nästa generations kommunikationsteknologi, eller statshemligheter. Konsekvenserna av cyberspionage kan ha sådana störande effekter att det kan påverka välståndet och konkurrenskraften i en stat.

5 Slutsatser

Syftet med rapporten var att besvara frågan ***Vilka nationella outtalade normer kan utläsas hos stater som bryter mot internationella överenskommelser i cyberrymden?*** Rapporten identifierade outtalade normer hos de nio staterna under granskning vad gäller idéer, föreställningar och moral som delades in i fem övergripande kategorier: 1. Idéer om ens identitet i världsordningen och därför självbild, 2. Uppfattning om nationell säkerhet 3. Upplevda hotbilder; 4. Uppfattning om makt; samt 5. Uppfattning och moral kring lönsamhet. Detta erhölls genom att först kartlägga staters uttalade normer (t.ex. cybersäkerhetsstrategier) i förhållande till deras faktiska beteende (offensiva cyberoperationer) i cyberrymden baserat på databasen Cyber Operations Tracker (COT). Med denna empiri kunde sedan se vilka av FN:s gemensamma normer som brutits och sedan kunde en tolkning av outtalade normer göras.

Resultatet visar att de fyra auktoritära staterna Kina, Iran, Nordkorea och Ryssland bedriver flest cyberoperationer och bryter mot flest av FN:s gemensamma uttalade normer. I de västerländska staternas nationella cyberstrategier nämns det ofta om att främja samarbete, utbildning och medvetenhet. Det är inte fallet för de auktoritära staterna, och inte minst för Nordkorea, som bygger hela sitt statsskick på att vara isolerade från omvärlden. De nationella cyberstrategierna hos de auktoritära staterna handlar istället om att vara defensiva genom en stark offensiv.

Detta innebär att stater anpassar sig efter en internationell uttalad norm, om staten kan identifiera sig själv med resten av gruppen. Detta kan man se då de demokratiska staterna Frankrike, Israel, Nederländerna, Storbritannien och USA har bedrivit betydligt färre cyberoperationer än de auktoritära, Kina, Iran, Nordkorea och Ryssland. De demokratiska staterna har därför inte heller brutit mot lika många av FN:s gemensamma uttalade normer. Det innebär att outtalade normer såsom staters självbild och idéer om ens egna identitet med FN, deras uppfattning om nationell säkerhet, deras upplevda hotbilder, deras uppfattning om makt och deras uppfattning om moral och lönsamhet påverkar hur de beter sig i cyberrymden. Staterna följer den geopolitiska och geoekonomiska utvecklingen samtidigt som IKT bidrar till en allvarligare situation då exempelvis industriellt spionage nu inte endast bedrivs av människor, utan genom cyberoperationer – som kan skada en stats konkurrenskraft.

6 Avslutande reflektioner

Det finns inga normer eller förbud som helt kan stoppa en annan stat, vare sig den är antagonistisk eller inte, från att bedriva offensiva cyberoperationer. Rapporten leder fram till insikten om behovet att på policynivå förstå och hantera utmaningarna i cyberrymden. Dels i stort hur den snabba digitaliseringen ska kopplas till cybersäkerheten. Dels mer specifikt exempelvis attributionsproblematiken, vilket i sin tur kopplas till de olika staternas världsuppfattningar och stormaktskonkurrensen. Detta varken mot civilsamhälle, regeringar/myndigheter, försvarsmakter eller den privata sektorn. Det är viktigt att acceptera.

Med detta sagt så leder rapporten fram till två viktiga insikter vad gäller både outtalade och uttalade normer. Dels är det viktigt att försöka förstå de outtalade normerna som finns i cyberrymden - nämligen de olika staternas världsuppfattningar och stormaktskonkurrensen. Outtalade normer kan nämligen styra hur stater förhåller sig till uttalade normer.

Dels är det viktigt att inse behovet att både förstå och hantera utmaningarna i cyberrymden på policynivå. Man bör förstå i stort hur den snabba digitaliseringen ska kopplas till cybersäkerheten, men även mer specifikt exempelvis vilken roll attributionsproblematiken har i cyberrymden.

Attribueringsproblematiken gör det också svårt, men inte omöjligt, att veta vem som är hotaktör och beroende på hur man väljer att kommunicera ut det till media. Det kan tolkas som en chansning när en hotaktör ska pekas ut men genom att hänvisa till t.ex. den egna underrättelsetjänsten så kan man minimera tolkningen om chansning. Vad man däremot kan göra är att jobba mot ett starkare cyber - "immunförsvar" där man jobbar mot att reducera risken för en cyberoperation till en acceptabel nivå och mot att göra det så svårt som möjligt för antagonistiska stater att attackera. Slutligen bör man inte utesluta användningen av offensiva cyberoperationer som en nogsamt övervägd respons till en annan stats agerande eller statsunderstödd aktörs agerande.

7 Framtida studier

Rapporten använder information från COT för att ge en översikt över hur offensiva cyberoperationer används i den internationella miljön. Databasen innehåller fler stater än de som täcks här. En framtida studie som granskar mindre stater och deras aktiviteter i cyberrymden, som t.ex. Vietnam, skulle kunna ge nya insikter och kan även jämföras med resultaten i denna rapport. En annan studie skulle kunna granska vilka stater som är de mest aktiva aktörerna i Afrika, samt syfte med deras cyberoperationer. En tredje studie kan vara att med utgångspunkt i COT göra en djupdykning på ett specifikt land, som t.ex. Kina, och identifiera topp-10 staterna som har utsatts för kinesiska cyberoperationer och relaterade syften.

Författarnas och projektledningens bidrag: Konceptualisering och projektidé, Gazmend Huskaj.; forsknings- och rapportstrategi, Gazmend Huskaj.; metod, Gazmend Huskaj.; tabeller och mjukvara, Margarita Sallinen och Gazmend Huskaj.; figurer, Gazmend Huskaj.; datainsamling och dataanalys, Margarita Sallinen och Gazmend Huskaj.; skrift-första utkast, Margarita Sallinen.; seminarium-review och kommentarer, Dr. Lars Nicander och Anna Djup.; skrift-andra utkast och redigering, Gazmend Huskaj.; seminarium-review och kommentarer, Dr. Lars Nicander och Anna Djup.; skrift-tredje utkast och redigering, Gazmend Huskaj.; skrift-tredje till sjätte utkast och redigering, Dr. Lars Nicander, Gazmend Huskaj, Margarita Sallinen och Anna Djup. Alla författare har läst och godkänt den publicerade versionen av manuskriptet.

Referenser

Ali, I. & Stewart, P. (2019, oktober 16). Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials. *Reuters*. https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive-idUSKBN1WV0EK.

Agius, C. (2019). Social Constructivism. In *Contemporary Security Studies* (5th Ed.). Oxford University Press

Ari Gross, J. (2020, maj 19). Cyberattack on port suggests Israeli tit-for-tat strategy, shows Iran vulnerable. *The Times of Israel*. https://www.timesofisrael.com/cyberattack-on-port-suggests-israeli-tit-for-tat-strategy-shows-iran-vulnerable/

Babones, S. (2021, april 10). China is governed by a totalitarian regime. Why is that so hard to say? *Foreign Policy*. https://foreignpolicy.com/2021/04/10/china-xi-jinping-totalitarian-authoritarian-debate/

BBC. (2010, november 24). Iran denies Stuxnet disrupted its nuclear programme. *BBC News*. https://www.bbc.com/news/technology-11821011

BBC. (2015a, december 21). Iranian Hackers 'Targeted' New York Dam. *BBC News*. https://www.bbc.com/news/technology-35151492

BBC. (2015b, januari 03). Sony cyber-attack: North Korea faces new US sanctions. *BBC News*. https://www.bbc.com/news/world-us-canada-30661973

BBC. (2018a, februari 15). UK and US blame Russia for 'malicious' NotPetya cyber-attack. *BBC News*. https://www.bbc.com/news/uk-politics-43062113

BBC. (2018b, april 12). UK Launched Cyber-attack on Islamic State. *BBC News*. https://www.bbc.com/news/technology-43738953

BBC. (2020, oktober 13). Norway blames Russia for cyberattack on parliament. BBC News. *BBC News*. https://www.bbc.com/news/world-europe-54518106

Bing, C., Stubbs, J. & Menn, J. (2019, juni 27). Exclusive: Western intelligence hacked 'Russia's Google' Yandex to spy on accounts – sources. *Reuters*. https://www.reuters.com/article/us-usa-cyber-yandex-exclusive-idUSKCN1TS2SX

Bülow, A. (2020, November 11). Microsoft: Ryska, kinesiska och iranska hackare riktar sig på Trumps och Bidens valkampanjer. *YLE*. https://svenska.yle.fi/artikel/2020/09/11/microsoft-ryska-kinesiska-och-iranska-hackare-riktar-in-sig-pa-trumps-och-bide

Cancian, F. M. (1975). *What are norms*. New York: Cambridge University Press.

CCDCOE. (u.å.) 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law. https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.

CFR. (2021a). *Cyber Operations Tracker*. https://www.cfr.org/cyber-operations/

CRF. (2021b). *Glossary*. https://www.cfr.org/cyber-operations/#Glossary

CFR. (2021c). *Our Methodology*. https://www.cfr.org/cyber-operations/#OurMethodology

CFR. (2021d). *Snowglobe*. https://microsites-live-backend.cfr.org/cyber-operations/snowglobe

Collier, K. & Leopold, J. (2018, augusti 10). Russian Hackers Targeted Swedish News Sites In 2016, State Department Cable Says. *Buzzfeed News*. https://www.buzzfeednews.com/article/kevincollier/2016-sweden-ddos-expressen-hack-russia-cables

Connell, M., & Vogler, S. (2016). *Russia´s approach to cyber warfare*. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

Corera, G. (2017, juni 16). NHS cyber-attack was 'launched from North Korea'. *BBC News*. https://www.bbc.com/news/technology-40297493

Crawley, K. (2019, November 10). Chinese Cyberwarfare Targets Uighur Population. *BlackBerry ThreatVector Blog*. https://blogs.blackberry.com/en/2019/10/chinese-cyberwarfare-targets-uighurs

CSIS. (2021). Significant Cyber Incidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cuthbertson, A. (2018, augusti 24). Iranian Hackers Attack UK Universities to Steal Secret Research. *Independent*. https://www.independent.co.uk/life-style/gadgets-and-tech/news/iran-hackers-uk-university-cyber-attack-security-cobalt-dickens-a8506406.html

Cybersecurity & Infrastructure Security Agency. (2017, juni 13). *Hidden Cobra – North Korea´s DDoS Botnet Infrastructure*. https://us-cert.cisa.gov/ncas/alerts/TA17-164A

Dahlgren, H. (2019). *Regeringens skrivelse 2019/20:18 Arbetet i frågor som rör Kina.* https://www.regeringen.se/4a72e0/contentassets/8a6d4e54b01d48ed9c196a252d09aff4/arbetet-i-fragor-som-ror-kina-skr-2019-20-18.pdf

DuBois, E. (2020, December 23). Building resilience to the North Korean cyber threat: Experts discuss. *The Brookings Institution.* https://www.brookings.edu/blog/order-from-chaos/2020/12/23/building-resilience-to-the-north-korean-cyber-threat-experts-discuss/

Delerue, F., Desforges, A. & Géry, A. (2019, april 23). A Close look at France's New Military Cyber Strategy. *War on the rocks*. https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/

DHHS. (2021). *North Korean Cyber Activity*. https://www.hhs.gov/sites/default/files/dprk-cyber-espionage.pdf

Dagens Nyheter. (2020, December 12). Ryssland förnekar FSB-skuld i förgiftning. *Dagens nyheter.* https://www.svd.se/ryssland-fornekar-fsb-skuld-i-forgiftning

DNI. (2021). *2021 Annual Threat Assessment of the U.S. Intelligence Community*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

DoD. (2018). *Summary - Department of Defense Cyber Strategy 2018*. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Donner, S. & Schwarz, R. (2014, februari 06). How Russia became an autocracy. https://www.bertelsmann-stiftung.de/en/topics/latest-news/2014/februar/how-russia-became-an-autocracy

Fällman, M. (2010). *Maktdemonstration Kaukasus*. https://www.diva-portal.org/smash/get/diva2:328566/FULLTEXT01.pdf.

Farrell, T. (2002). Constructivist Security Studies: Portrait of a Research Program. *International Studies Review, 4*(1), 49-72. https://doi.org/10.1111/1521-9488.t01-1-00252

FN. (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement

FN. (2021). *Developments in the field of information and telecommunications in the context of international security*. https://www.un.org/disarmament/ict-security/

Follorou, J., & Untersinger, M. (2014). Quand les Canadiens partent en chasse de « Babar ». *Le Monde*. https://www.lemonde.fr/international/article/2014/03/21/quand-les-canadiens-partent-en-chasse-de-babar_4387233_3210.html

Forum för Levande Historia. (u.å). *Samhällets normer och dess konsekvenser*. https://www.levandehistoria.se/vittnesmal-med-klassrumsovningar/tema-normer/1-samhallets-normer-och-dess-konsekvenser

FRA. (2017). *Årsrapport 2017*. https://fra.se/download/18.60b3f8fa16488d849a5104/1604415238634/FRA-arsrapport-2017-lowres.pdf

Franska försvarsmaktsministeriet. (2018). *Draft Military Planning Law - 2019/2025.* https://www.defense.gouv.fr/content/download/523961/9053454/file/MPL%202019-2025%20-%20Synopsis%20(EN).pdf

Gallagher, S. (2017). *As US launches DDoS attacks, N. Korea gets more bandwidth—from Russia.* https://arstechnica.com/information-technology/2017/10/as-us-launches-ddos-attacks-n-korea-gets-more-bandwidth-from-russia/

Grennert, J. & Tham-Lindell, M. (2002). *Cyberterrorism: Öppnar IT nya möjligheter för terrorism?* https://www.foi.se/rest-api/report/FOI-R--0626--SE.

Grigsby, A. (2016, September 15). Shouting at Americans: A peek into French signals intelligence. *Net Politics*. https://www.cfr.org/blog/shouting-americans-peek-french-signals-intelligence

Holmqvist, L. (2021). *Cyberhotet: attacker, spionage och krigföring*. https://www.forsvarsutbildarna.se/stockholm-sodermanland/wp-content/uploads/sites/26/2021/03/Slagfjadern_1-2021_web.pdf

Hurd, I. (2015). International law and the politics of diplomacy. In *O. Sending, V. Pouliot, & I. Neumann (Eds.), Diplomacy and the Making of World Politics* (Cambridge Studies in International Relations, pp. 31-54). Cambridge: Cambridge University Press. doi:10.1017/CBO9781316162903.002

Huskaj, G. (2019). *The Current State of Research in Offensive Cyberspace Operations*. In T. Cruz & P. Simoes (Eds.), 18th European Conference on Cyber Warfare and *Security* (pp. 660–667). Academic Conferences and Publishing International Ltd

Huskaj, G., & Wilson, R. L. (2020). *An Anticipatory Ethical Analysis of Offensive Cyberspace Operations.* In P. B. K. Payne & P. H. Wu (Eds.), ICCWS 2020 15th International Conference on Cyber Warfare and Security (pp. 512–520). Norfolk: Academic Conferences and Publishing International Limited

Huskaj, G., Iftimie, I. A., & Wilson, R. L. (2020). *Designing attack infrastructure for offensive cyberspace operations.* In European Conference on Information Warfare and Security, ECCWS (Vol. 2020-June, pp. 473–482). https://doi.org/10.34190/EWS.20.077

Imeson, M. (2019, oktober 14). Russia cyber aggression fuels tension with west. *Financial Times.* https://www.ft.com/content/0aa7a6e0-ca52-11e9-af46-b09e8bfe60c0

Irshaid, F. (2015, december 02). Isis, Isil, OS or Daesh? One group, many names. *BBC*. https://www.bbc.com/news/world-middle-east-27994277

JCOS. (2018). *Joint Publication 3-12 – Cyberspace Operations.* https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.

Jensen, B., Valeriano, B., & Maness, R. (2019). Fancy bears and digital trolls: cyber strategy with a Russian twist. *Journal of Strategic Studies, 42*(2), 212-234. https://doi.org/10.1080/01402390.2018.1559152

Jun, J., LaFoy, S., & Sohn, E. (2015). North Korea´s Cyber Operations Strategy and Responses. *CSIS Korea Chair*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf?fbclid=IwAR0pcdMoKJpPUTUC45EohJlJH0VabesCRHb8wfrCVuxKwypxOqK_pdPbQTQ

Kurowska, X., & Reshetnikov, A. (2018). *Russia´s trolling complex at home and abroad*. In Hacks, leaks and disruptions Russian Cyber Strategies. European Union Institute for Security Studies.

Lewis, J.A. (2019). Iran and Cyber Power. https://www.csis.org/analysis/iran-and-cyber-power.

Lotsson, A. (2018). Social manipulering. IT-ord. *Computer Sweden och IDG*. https://it-ord.idg.se/ord/social-manipulering/

Lotsson, A. (2019a). Buffertöverfyllning. IT-ord. *Computer Sweden och IDG*. https://it-ord.idg.se/ord/buffertoverfyllning/

Lotsson, A. (2019b). Behörighetsintrång. IT-ord. *Computer Sweden och IDG*. https://it-ord.idg.se/ord/behorighetsintrang/

Lotsson, A. (2019c). Spökprogram. IT-ord. *Computer Sweden och IDG*. https://it-ord.idg.se/ord/spokprogram/.

Lotsson, A. (2019d). Man-i-mitten-attack. IT-ord. *Computer Sweden och IDG*. https://it-ord.idg.se/ord/man-i-mitten-attack/

Lotsson, A. (2020). Överbelastningsattack. *Computer Sweden och IDG*. https://it-ord.idg.se/ord/overbelastningsattack/

Merriam-Webster (2021). *Conflict*. https://www.merriam-webster.com/dictionary/conflict.

Mozur, P. & Stevenson, A. (2019, juni 13). Chinese Cyberattack Hits Telegram, App Used by Hong Kong Protesters. *NY Times*. https://www.nytimes.com/2019/06/13/world/asia/hong-kong-telegram-protests.html

Nakashima, E., & Harris, S. (2018, juli 14). How the Russians hacked the DNC and passed its emails to WikiLeaks. *Washington Post*. https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html

Noack, R. (2018, januari 26). The Dutch were a secret U.S. ally in war against Russian hackers, local media reveal. *Washington Post*. https://www.washingtonpost.com/news/worldviews/wp/2018/01/26/dutch-media-reveal-country-to-be-secret-u-s-ally-in-war-against-russian-hackers/

Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Oxford Lexico. (2021). *Countervailing*. https://www.lexico.com/en/definition/countervailing

Посольство Российской Федерации в Норвегии. (2020, oktober 13). *Комментарий Посольства России в Норвегии*. https://norway.mid.ru/ru/embassy/press-centre/news/kommentariy_posolstva_rossii_v_norvegii_/

PwC & BAE Systems. (2017). *Operation Cloud Hopper*. https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

RAND. (2021). *Information Operations*. https://www.rand.org/topics/information-operations.html.

Rabinovitch, A., Cohen, T., & Pleck, D. (2017, oktober 31). Iran's hacking ability improving: Israeli general. *Reuters*. https://www.reuters.com/article/us-cyber-summit-padan/irans-hacking-ability-improving-israeli-general-idUSKBN1D02O0

Raska, M. (2020a). North Korea's Evolving Cyber Strategies: Continuity and Change. *SIRIUS – Zeitschrift für Strategische Analysen*, 4(2), 1-13. https://doi.org/10.1515/sirius-2020-3030

Raska, M. (2020b). North Korea's Evolving Cyber Warfare Strategy. *East Asia Forum*. https://www.eastasiaforum.org/2020/09/24/north-koreas-evolving-cyber-warfare-strategy/.

Recorded Future (u.å.). *North Korea Cyber Activity*. https://go.recordedfuture.com/hubfs/reports/north-korea-activity.pdf

Red Dragon 1949. (2018). *China's Cyberspace National Security Strategy: Actively Defending Network Sovereignty! // 中國的網絡空間國家安全戰略：積極捍衛網絡主權！* https://reddragon1949.com/tag/chinas-informatization-%E4%B8%AD%E5%9C%8B%E4%BF%A1%E6%81%AF%E5%8C%96/page/2/

Reuter, M. (2003). *Anfalla och attackera*. https://www.sprakinstitutet.fi/sv/publikationer/sprakspalter/reuters_rutor_1986_2013/2003/anfalla_och_attackera

Reuters. (2017). Russia hacked Danish defense for two years, minister tells newspaper. *Reuters*. https://www.reuters.com/article/us-denmark-security-russia-idUSKBN17P0NR

Reuters. (2021). Norway's parliament hit by new hack attack. *Reuters*. https://www.reuters.com/article/us-norway-cyber-idUSKBN2B21TX

RISE. (2019). *RISE inspel till regeringens forskningspolitik*. https://www.ri.se/sites/default/files/2019-11/RISE%20inspel%20till%20regeringens%20forskningspolitik-signed_0.pdf

Rossi, P. H., & Berk, R. A. (1985). Varieties of normative consensus. American Sociological Review, 50, 333-347.

Säkerhetspolisen. (2020). *Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden.* https://www.sakerhetspolisen.se/download/18.f2735ce171767402ba202/1591164566288/Rapport-Cybersakerhet-Hot-Metoder-Brister.pdf

Säkerhetspolisen. (2021). *Upprepade dataintrång del av en större påverkanskampanj*. https://www.sakerhetspolisen.se/ovrigt/pressrum/aktuellt/aktuellt/2021-04-13-upprepade-dataintrang-del-av-en-storre-paverkanskampanj.html

Schwartz, S. H. (1977). *Normative influences on altruism*. In L. Berkowitz (Ed.), Advances in experimental social psychology. 10, 221-279.

Sjöström, S. (2014, February 28). Ryssland förnekar trupper i Ukraina. *Sveriges Radio*. https://sverigesradio.se/artikel/5797161.

Soldatov, A., & Borogan, I. (2018). *Russia´s approach to cyber: the best defence is a good defence*. In Hacks, leaks and disruptions Russian Cyber Strategies. European Union Institute for Security Studies

Steed, D. (2021, maj 03). The United Kingdom's New Vision of Cyber Power. *War on the rocks.* https://warontherocks.com/2021/05/the-united-kingdoms-vision-of-cyber-power/

Stubbs, J. (2019). China hacked Norway's Visma to steal client secrets: investigators. *Reuters*. https://www.reuters.com/article/us-china-cyber-norway-visma-idUSKCN1PV141

Stubbs, J., Menn, J. & Bing, C. (2019a). Exclusive: China hacked eight major computer services firms in years-long attack. *Reuters*. https://www.reuters.com/article/us-china-cyber-cloudhopper-companies-exc-idUSKCN1TR1D4

Stubbs, J., Menn, J. & Bing, C. (2019b). Inside the West's failed fight against China's 'Cloud Hopper' hackers. *Reuters.* https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

SUPO. (2020). *SUPO 2020 Year Book*. https://vuosikirja.supo.fi/documents/62399122/66519032/Supo+Year+Book+2020.pdf/65663bab-fcf6-5d86-9e15-9a12ab37c3a5/Supo+Year+Book+2020.pdf?t=1616408481574.

Tabansky L., Ben Israel I. (2015) *The National Cyber-Strategy of Israel and the INCB.* In: Cybersecurity in Israel. SpringerBriefs in Cybersecurity. Springer, Cham. https://doi-org.ezp.sub.su.se/10.1007/978-3-319-18986-4_7

The Local. (2014, september 26). Danish defence secrets obtained by foreign spies. *The Local*. https://www.thelocal.dk/20140926/danish-defence-secrets-obtained-by-foreign-hackers/

The UK Cabinet Office. (2021). Global Britain in a Competitive Age: the Integrated Review of Security, *Defence, Development and Foreign Policy*. https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

Thiessen, M.A. (2020, juli 11). Opinion: Trump confirms, in an interview, a U.S. cyberattack on Russia. *Washington Post*. https://www.washingtonpost.com/opinions/2020/07/10/trump-confirms-an-interview-us-cyberattack-russia/

Thornberg, R. (2013). *Det sociala livet i skolan: socialpsykologi för lärare*. Liber

Tikk, E. & Kerttunen, M. (2017). *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*. https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf

TT. (2018, december 20). Sverige pekas ut som mål för kinas cyberattacker. *Svenska Dagbladet*. https://www.svd.se/usa-kineser-stams-for-hackerattacker

UNIDIR. (2021a). *Iran (Islamic Republic of).* https://unidir.org/cpp/en/states/iran

UNIDIR. (2021b). *Israel.* https://unidir.org/cpp/en/states/israel

UNIDIR. (2021c). *Netherlands*. https://unidir.org/cpp/en/states/netherlands

UNIDIR. (2021d). *Russian Federation*. https://unidir.org/cpp/en/states/russianfederation

UNODA. (2019). *Fact Sheet - Developments* In The Field of Information and Telecommunications in the Context of International Security. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf

Utrikespolitiska Institutet. (2021). *Landguiden – Israel utrikespolitik och försvar*. https://www.ui.se/landguiden/lander-och-omraden/asien/israel/israel-utrikespolitik-och-forsvar/

Vilmer, J-B. J. (2019). *What is a "Hack and Leak" Information Operation?* https://www.jargaldefacto.com/article/what-is-a-hack-and-leak-information-operation

Warrick, J. & Nakashima, E. (2020, maj 18). Officials: Israel linked to a disruptive cyberattack on Iranian port facility. *Washington Post*. https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

Åkesson, E. (2016). *Normer, normmedvetenhet och normkritik*. https://www.skolverket.se/download/18.653ebcff16519dc12ef362/1539586793376/Normer-normmedvetenhet-och-normkritik.pdf

Bilaga

1. Rapportdesign

Den här delen presenterar rapportdesignen. Den beskriver rapportstrategi, ett anpassat ramverk för metanormer, och slutligen rapportprocessen med relaterad projektplan och metod.

1.1. Rapportstrategi

Fallstudie som rapportstrategi är väl lämpad för att titta på enstaka fenomen och studera de djupt (Denscombe, 2014; Oates, 2005). Exempel på fenomen inkluderar policy, händelser, och processer (Denscombe, 2014). Att studera en stats utrikes- och säkerhetspolitik visar t.ex. statens fokus, potentiella upplevda hot, men också hur staten avser hantera det. Att studera en stats cybersäkerhetsstrategi kan visa hur mycket den staten värderar sin cyberrymd och de satsningar staten gör för att skydda sin cyberrymd mot hot. Att studera resultatet från de fem grupperna av statliga experter (GGE), men specifikt den från 2014/205 och de normer, regler eller principer för ansvarsfullt beteende inom cyberrymden, visar vad stater anser vara ansvarsfullt beteende.

1.2. Det anpassade ramverket för metanormer

Ramverket för metanormer (för hela ramverket se Rowe, 2018) har anpassats för att fokusera på offensiva cyberoperationer. Tabell 1 visar det anpassade ramverket med fokus på offensiva cyberoperationer.

Tabell 1. Ramverket för metanormer anpassat med fokus på offensiva cyberoperationer.

Metanormer för offensiva cyberoperationer
Vilken roll spelar cyberkonflikt i en nationell strategi?
Hur många cyberoperationer totalt har staten genomfört mellan 2005-2020?
Har staten bedrivit Dataförstörelse?
Har staten bedrivit Vandalism?
Har staten bedrivit DDoS?
Har staten bedrivit Doxing?
Har staten bedrivit hack'n-leak inför val-rörelser (motsv.)
Har staten bedrivit underrättelseinhämtning / spionage?
Har staten bedrivit operationer för finansiell vinning?
Har staten bedrivit Sabotage?
(CO utan kategori)

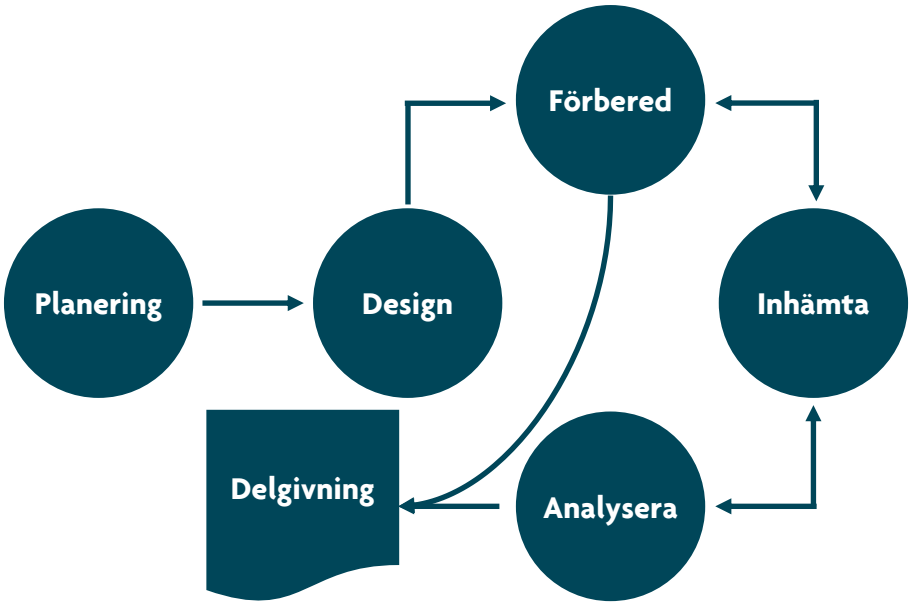
När använder en stat cyberattack som ett instrument för nationell politik?

Hur bedriver en stat cyberkonflikt när den måste?

Hur beter sig en stat efter cyberkonflikt(er)?

1.3. Rapportprocessen

Rapportprocessen baseras på Yins (2018) forskningsprocess, som visas i figur 1.



Figur 1. Yins (2018) forskningsprocess för att genomföra fallstudieforskning.

Planering för rapporten påbörjade den 11:e november 2020. Projektledaren/medförfattaren (GH) satte upp studien som ett projekt som sträckte sig från januari 2021 till juni 2021. Figur 2 visar projektet och associerade forskningsaktiviteter. Projektet sattes upp med en projektledning (LN, AD, GH), projektledare (GH), och forskningsassistent (MS). Därefter genomfördes riskhantering genom att sätta upp målet att ett första utkast på rapporten skulle presenteras den sista april (ca 80% av den totala tiden) i seminarieform. Därefter skulle kommentarer från seminariet beaktas och utgåva två (2) presenteras i slutet av maj i seminarieform. Kommentarerna från seminarium två (2) skulle därefter beaktas och en slutlig rapport presenteras i mitten av juni 2021.

Jan	Feb	Mar	Apr	Maj	Jun
18 – Kickoff			30 – 1:a utkast Seminarium	28 – 2:a utkast Seminarium	11 – Slutprodukt Seminarium
Inhämtning	Inhämtning och bearbetning	Analys/Syntes/ Produktion	Produktion	Produktion	Delgivning

Figur 2. Projektet för produktion av rapporten med associerade forskningsaktiviteter.

Problemet som ligger till grund för rapporten är att det finns normer, regler eller principer som har tagits fram för staters ansvarsfulla beteende i cyberrymden, alltså uttalade normer som man har kommit överens om. Emellertid bedrivs fortfarande offensiva cyberoperationer, och i vissa fall har antalet ökat. Det här är en indikator på att stater har outtalade normer och beter sig annorlunda än vad de säger formellt. Därför är det viktigt att studera fenomenet, vilket också leder till hur forskningsdesignen ska se ut, vilket har beskrivits i inledningen av detta kapitel.

Förberedelser innebar att ta fram en metod för att identifiera uttalade och outtalade normer. Metoden, i sig en komparativ sådan, gick ut på att identifiera överenskomna normer som stater har kommit överens om för ansvarsfullt beteende i cyberrymden, och normer för potentiell konflikt (metanormer). Metanormerna (Rowe, 2018) anpassades till ett ramverk för att endast titta på offensiva cyberoperationer. Ramverket har också satt de gränser för vad rapporten ska fokusera på och även fungerat som frågor som författarna har kunnat ställa för att lära sig mer on en stats beteende. De fem begränsande normerna är överenskomna normer som visar på staters ansvarsfulla beteende, och om inga av dessa bryts, då betyder det att staten efterlever de. Stater som bryter mot de överenskomna normerna kan innebära att de har outtalade normer. Detta ledde till formulering av frågan:

Vilka nationella outtalade normer kan utläsas hos stater som bryter mot internationella överenskommelser i cyberrymden?

Ytterligare förberedelser var att ta fram ett systematiskt arbetssätt. Det första steget var att identifiera en lämplig källa som räknar antalet cyberoperationer. Det andra steget var att upprätta ett lämpligt sätt att dokumentera och lagra den inhämtade informationen från källan. Council on Foreign Relations (COR) och deras Cyber Operations Tracker (COT) identifierades som lämplig källa som räknar antalet cyberoperationer vilka är publikt kända från stater eller hotaktörer vilka misstänks vara förknippade med stater (CFR, 2021a). COT har två begränsningar: attribuering och fullständighet av uppgifter.

Attribuering, att attribuera en cyberattack till en specifik stat, är en svår process och mycket omdebatterat. Databasen är inte fullständig på grund av den har en västerländsk vinkling, data kommer från uppgifter som är offentliga, och fullständig och tillförlitlig

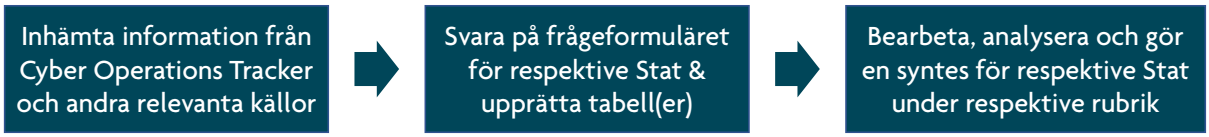
information om cyberincidenter och hotaktörer tar tid för informationen att dyka upp (CFR, 2021c).

Dokumentation, lagring och räkning av antal cyberoperationer gjordes med hjälp av R och Excel. COT har en funktion som gör det möjligt att ladda ner alla data för att göra egna beräkningar. Slutligen skulle staterna för vidare analys identifieras. Dessa identifierades i ett seminarium och valet föll på Kina, Frankrike, Israel, Irland, Nordkorea, Nederländerna, Ryssland, Storbritannien och USA. Staterna ordnades alfabetiskt baserat på deras domännamn: .cn för Kina; .fr för Frankrike; .il för Israel, osv.

Datainsamling genomfördes från COT, staters egna cybersäkerhetsstrategier (i de fall de kunde hittas) och andra källor. När information från andra källor har identifierats och använts presenteras denna i texten och referenslistan.

Analys av det insamlade datat genomfördes mot ramverket genom att i R och Excel räkna antalet cyberoperationer ett land har genomfört; dess syfte och mål.

Delgivning innebär att man i ett tidigt skede identifierar mottagargrupp (t.ex. praktiker, akademiker, övriga samhället) samt presentationssätt (t.ex. rapport, visuell presentation), samt kvalitetskrav på rapporten (Yin, 2018). Mottagargruppen är primärt praktiker, och akademiker och det övriga samhället. Praktiker verksamma i frågor rörande Sveriges säkerhet med fokus på cyberfrågor; akademiker och studenter verksamma i cyberfrågor. Det övriga samhället kan dra nytta av rapporten genom att t.ex. skriva en populärvetenskaplig artikel.



Figur 3. Metod för inhämtning av relevant information baserat på frågeformuläret.

Försvarshögskolan