Lunds universitet
Statsvetenskapliga institutionen

STVA22
HT22
Handledare: Daniel Møller Ølgaard

SolarWinds hack och det nya kriget

Hur cyberangrepp såsom SolarWinds hack
har påverkat modern krigföring

André Fhager & Joy Vikström

Abstract

I den här teorigenererande studien utforskas hur cyberangrepp såsom SolarWinds hack har påverkat möjligheterna att föra krig mot andra stater. Vi ämnar göra detta genom att undersöka aspekter som exempelvis vad man kan uppnå med cyberkrigföring, hur staters förståelse av krig ser ut idag, implikationer av anonymitet i cyberrymden samt hur militära maktstrukturer förändras. Uppsatsen tar formen av en fallstudie där cyberattacken mot SolarWinds undersöks i syfte att agera som vägledning för applicerande av teori samt som praktisk anknytningspunkt. Analysen tar avstamp i de specifika aspekterna av SolarWinds hack för att leda till mer generella perspektiv på cyberattacker och krigföring. Utifrån vår diskussion identifierar vi fyra teman som är väsentliga för besvarandet av frågeställningen; ökade möjligheter inom krigföring, ovisshet och misstänksamhet, cyberkrigföring som komplement kontra alternativ samt förändring av militära maktstrukturer.

Nyckelord: cyberkrigföring, SolarWinds hack, cyberattacker, cyberangrepp, krig
Antal ord: 10215

Innehållsförteckning:

1. Inledning

"Den största och mest sofistikerade attacken som världen har sett", så beskriver Microsofts ordförande Brad Smith cyberangreppet mot SolarWinds 2020 (Reuters, 2021). Inträdet av cyberattacker av denna utsträckning har väckt uppmärksamhet runt om i världen, och även väckt frågan om hur dessa kan komma att påverka krigföring som helhet. Med anledning av detta har vi valt att utforska SolarWinds hack med förhoppningen att ta reda på och belysa hur cyberangrepp påverkar möjligheterna att föra krig mot andra stater.

1.1 Syfte och frågeställning

Syftet med uppsatsen är att utforska om och hur cyberattacker såsom *SolarWinds hack* har påverkat möjligheterna till att föra krig mot andra stater. Vi ämnar göra detta genom att undersöka bland annat vad man kan uppnå med cyberkrigföring, hur staters förståelse av krig ser ut idag, implikationer av anonymitet i cyberrymden samt hur militära maktstrukturer förändras. Vidare är vårt syfte att generera och utveckla teoribildning kring hur cyberkrigföring påverkar krig idag genom att studera *SolarWinds hack* och på så sätt se hur de nämnda koncepten yttrar sig i praktiken.

Vi formulerar frågeställningen:

- *Hur har cyberangrepp såsom SolarWinds hack påverkat möjligheterna till att föra krig mot andra stater?*

Cyberangrepp är fortfarande ett relativt nytt fenomen, och dess påverkan på krigföring är således ett högst relevant ämne att utforska. Dessutom är angreppet mot SolarWinds i och med att det inträffat så nyligen som 2020 relativt outforskat. Vi motiverar således vår frågeställning inomvetenskapligt utifrån att vi avser föra tidigare forskning framåt på ett ämne som inte haft lika många år i centrum som många andra statsvetenskapliga områden, samt genom att vi applicerar tidigare forskning på ett fall som inte blivit studerat i hög omfattning. Vidare avser vi utveckla och förtydliga förståelsen av krig idag.

Frågeställningen har också en utomvetenskaplig relevans genom att forskning på området cyberkrigföring och hur det påverkar krig idag kan ge vägledning och vara av vikt för beslutsfattare inom säkerhetspolitik. Således kan en utredning av en frågeställning likt denna agera som en påminnelse om den betydande roll som cyberkrigföring har och fallet med SolarWinds agerar som en redogörelse för riskerna med att negligera åtgärder av

cybersäkerhetskaraktär. SolarWinds hack var ett mycket uppmärksammat cyberangrepp som påverkade många aktörer i samhället, såväl företag som offentlig sektor, och på så vis kan även vårt val av fall motiveras utifrån utomvetenskaplig relevans.

1.2 Operationalisering och avgränsning

Det finns flera olika typer av cyberattacker, däribland DoD-attacker (överbelastningsattacker), informationsattacker och desinformation, spionage, doxing, förstörande av väsentlig infrastruktur, etc. Inom ramen för den här uppsatsen tillämpar vi en bred förståelse och definition av begreppet, vilket inkluderar alla dessa varianter. Detta innebär alltså att fallet SolarWinds hack inkluderas inom termen cyberattack även om detta inte är självklart utifrån en snävare definition som enbart innefattar störningar, skada och förstörelse av infrastruktur. Genomgående i texten använder vi oss av termerna "cyberattack" och "cyberangrepp" synonymt.

Vi avgränsar omfånget av uppsatsen till cyberangrepp som utförts inom krig och konflikt av aktörer med politiska motiv, med andra ord berör vi inte attacker utförda av kriminella som endast är ute efter personlig vinning, till exempel genom utpressning för lösensummor. Frågeställningen besvaras utifrån en helhetsbild av hur cyberangrepp har påverkat krigföring, men det bör understrykas att vi främst fokuserar vår anknytning till cyberangreppet som skedde mot SolarWinds corporation år 2020.

Krig är ett annat begrepp som bör förtydligas. Krig definieras som "storskaligt organiserat våld mellan politiskt organiserade grupper" (Andersson, 2014, s. 150). Ett ofta förekommande, men inte obestritt, kriterium är att det skall ha skett minst 1000 krigsrelaterade dödsoffer inom tolv månader – till skillnad från väpnad konflikt för vilket kriteriet är 25 stridsrelaterade dödsoffer mellan två parter under ett kalenderår (ibid). Cyberangrepp inkluderas inte nödvändigtvis i den här traditionella förståelsen av krig, men ändå talas det om "cyberkrig" och "cyberkrigföring". Vad är ett krig idag och vad innefattar det? Eftersom vår frågeställning kräver ett utforskande av förståelsen av krig, lämnar vi definierandet av vad som räknas som krig till analys- och diskussionsavsnitten.

Emellertid kan det göras en distinktion mellan cyberattacker och cyberkrigföring. Cyberattacker syftar på isolerade händelser medan cyberkrigföring är en kampanj som utgörs av samordnade, avsiktliga och statligt finansierade cyberattacker med syfte att negativt påverka en eller flera staters ekonomiska och operationella infrastruktur (Datta, 2022, s. 115-116).

1.3 Metod, Teori och Material

Vi använder oss av en kvalitativ metod då vi gör en fallstudie på *SolarWinds hack.* I och med att cyberattacker är ett väldigt brett ämne kan vi genom att utgå från ett specifikt fall behålla ett stadigt fokus och en klar empirisk anknytning, och således minimera risken för att uppsatsen blir spretig och ofokuserad. Med avseende på den tidsbegränsning och det omfång som uppsatsen innefattar, hjälper metodvalet av en fallstudie oss även att i största mån kunna gå på djupet inom vårt valda fall (Lindvall, 2007, s. 270-271) istället för att enbart ytligt kunna beskriva de verkningar som cyberattacker har på krigföring.

Vårt val att genomföra en fallstudie beror också på att vi är inspirerade av "grounded theory" (se mer nedan) i vilken den empiriska förankringen är central, och genom att studera ett fall på djupet hoppas vi kunna uppnå det. Vid ett användande av grounded theory börjar man i regel genom att studera ett ingångsfall som man anser vara intressant (Esaiasson et. al., 2017, s. 127), och vi menar att SolarWinds hack är passande för det ändamålet.

Vi motiverar valet av fall genom att SolarWinds hack var ett mycket omfattande cyberangrepp som drabbade tusentals företag och statliga organisationer globalt. Microsofts ordförande Brad Smith beskrev till och med fallet som "den största och mest sofistikerade attacken som världen har sett" (Reuters, 2021). Således kan det ses som ett paradigmatiskt fall i och med att attacken hade ett större omfång än tidigare fall av cyberangrepp. Vidare utfördes SolarWinds hack år 2020, vilket är i vår relativa nutid. Detta talar för motiveringen av vårt val både utifrån att en analys av fallet är högst relevant även idag och utifrån att det är relativt outforskat då det inte hunnits göra många studier på fallet.

Eftersom vi inte sedan tidigare har en oerhört bred kunskap inom ämnet cyberattacker och eftersom det inte är vår avsikt att studera fallet utifrån några teoretiska glasögon, har vi valt att utföra vår studie med inspiration av grounded theory. Till skillnad från hypotetisk-deduktiv metod formulerar vi inte en hypotes på förhand som vi sedan prövar. Istället låter vi, i enlighet med grounded theory, fallet leda oss till intressanta aspekter av cyberattacker som vi har valt att analysera mer på djupet med hjälp av relevant litteratur och forskning, detta för att utveckla teori som är förankrad i empiri och inte "luftiga skrivbordskonstruktioner" (Esaiasson et. al., 2017, s. 127-128). Vår frågeställning avser att ta reda på hur möjligheterna till krigföring har påverkats av cyberattackers inträde på den internationella arenan, i vår analys av SolarWinds Hack har detta utforskats och sedan sammanställs som övergripande teman av förändringen i diskussionen. Ett användande av grounded theory innebär alltså att vi använder oss av en induktiv metod (ibid, s. 127).

För att fullända applikationen av grounded theory skulle dessa teman inom senare forskning kunnas testas på fler likartade och olikartade fall (Esaiasson et. al., 2017, s. 127) för att sedan

kunna användas för att utmana nuvarande teoribildning och traditionella perspektiv på krigföring. Detta är något som skulle vara intressant att vidare utforska, men inom ramen för uppsatsens omfång och tidsrymd har vi valt att avgränsa vår frågeställning till att främst utforska hur möjligheterna till krigföring påverkas empiriskt. En aspekt av grounded theory är att den aldrig blir färdig. Vanligtvis går man tillväga på så sätt att man har ett ingångsfall, i vårt fall SolarWinds hack, och formulerar en första version av grundläggande begrepp och övriga slutsatser. Senare kan man pröva och utveckla sina slutsatser på fler fall för att se till att teorin är fast rotad i empirin (ibid, s. 127). Den här uppsatsen utgör alltså studien av ingångsfallet, och på så sätt avser vi göra ett kumulativt bidrag till forskningen (ibid, s. 20-21) samtidigt som vi även uppmanar till fortsatt forskning.

Vi använder oss genomgående av tidigare forskning och litteratur i analysen för att öka vetenskapligheten och undvika att dra arbiträra slutsatser och/eller tolkningar, vilket är viktigt då vår studie genom sitt kumulativa bidrag har en teoriutvecklande ansats. Däremot bör det understrykas att det material som har valts ut som teoretisk grund motiveras utifrån att det under analysen visat sig vara relevant för vårt fall och alltså inte är givet på förhand, i enlighet med vårt metodval. Materialet består därmed av flera olika forskares teorier som kan förklara flera olika aspekter av fallet Solarwinds hack och dess implikationer på cyberkrigföring.

1.4 Bakgrund

SolarWinds är ett välkänt amerikanskt företag som specialiserar sig i mjukvaru-utveckling, vilket de förser till bland annat stora företag och statliga amerikanska organisationer som till exempel departement. År 2020 blev företaget utsatt för vad som kallas för en “supply chain- attack”. Likt vanliga varor följer även mjukvaruprodukter, såsom de som SolarWinds distribuerar, en produktionskedja innan de överlämnas till konsumenterna. En supply chain-attack ämnar att hitta en svag punkt i termer av cybersäkerhet inom denna produktionskedja och hitta en väg in i systemet. Därifrån kan man arbeta med att införa så kallad illvillig kod, dvs. kod som är ämnad att främja hackarnas mål och inte företagets egna, med aspirationen att denna kod kommer att spridas till de konsumenter som tar emot varan (Alkhadra et al., 2021). På så sätt kan man vid en lyckad operation infiltrera ett större antal organisationer än vad man skulle kunna med enskilda attacker mot specifika mål. I fallet med SolarWinds var den svaga länken SolarWinds Orion Platform där illvillig kod blev infört i en mjukvaruuppdatering som sedan blev hämtad hos ungefär 18 000 konsumenter (Bhunia & Sterle, 2021)

En stor mängd av företag och organisationer blev påverkade av cyberattacken och en lista på de 18 000 konsumenter som hämtade den illvilliga koden skulle vara excessivt. Bland de mest nämnvärda företagen finner vi däremot framträdande IT-företag som Microsoft, Intel, och Nvidia och cybersäkerhets-företag som FireEye (Bhunia & Sterle, 2021). Dessutom blev ett flertal departement från den amerikanska staten påverkade av supply chain- attacken. Däribland hittar vi

finansdepartementet, utrikesdepartementet, handelsdepartementet och justitiedepartementet. Mest nämnvärda är däremot det amerikanska försvarsdepartementet och det amerikanska energidepartementet som rapporterat att Pentagon respektive “the National Nuclear Security Administration” har blivit påverkat, samt “the Department of Homeland Security” (Alkhadra et al., 2021).

Detta leder onekligen till stora kostnader för de påverkade. Gärningsaktören bakom cyberattacken fick i och med den illvilliga kodens framgång ta del av konfidentiell information vilken de sedan bland annat kan stjäla, förstöra eller sträva efter att förfalska (Bhunia & Sterle, 2021). Dessutom tillkommer det även stora ekonomiska kostnader då resurser behövs läggas på att upptäcka och hantera viruset, vilket både innebär en kostnad direkt i och med att resurserna inte är gratis men också indirekt då både resurserna och tiden som läggs ned hade kunnat användas på att maximera produktivitet. Dessutom finns det även en kostnad i tillit och gott rykte hos organisationerna då det faktum att de blev angripna kan ses som ett tecken på dålig säkerhet (Alkhadra et al., 2021).

Vem som har utfört attacken är fortfarande inte helt klarlagt. Ett flertal individer och organisationer som är verksamma inom cyberaktiviteter tillsammans med statliga ombud har däremot pekat ut den Ryska Federationens Yttre Underrättelsetjänst (SVR) som ansvariga eftersom attacken påminner om andra försök som har gjorts för att komma åt USAs mjukvarusystem, som exempelvis när en grupp vid namn Cozy Bear försökte få tillgång till vita huset och utrikesdepartementets e-mail system 2014 (Alkhadra et al., 2021). Hackergruppen Cozy Bear är även den grupp som anklagats av bland annat FireEye - ett amerikanskt företag som specialiserar sig inom cybersäkerhet, och som också var de som först upptäckte attacken mot Solarwinds - för att ha utfört supply chain- attacken (Tidy, 2020).

Som svar på den ryska statens misstänkta inverkan i cyberattacken mot SolarWinds införde USA sanktioner mot Ryssland med syftet att avskräcka från fortsatt agerande inom destabiliserande cyberattacker. Sanktionerna hade enligt Joe Biden kunnat vara mer aggressiva, men valet att avvika från mer drastiska åtgärder motiveras med att vägen till en lösning bör vara en diplomatisk process för att undvika oönskad eskalering (BBC, 2021).

2. Analys

2.1 Vad man kan uppnå med cyberattacker

En väsentlig del av att förstå hur cyberangrepp såsom SolarWinds hack har påverkat möjligheterna till att föra krig mot andra stater är att förstå vad man kan uppnå med cyberkrigföring. Genom attacken mot SolarWinds kunde gärningsaktören få tillgång till känslig information från alltifrån det amerikanska försvaret och politiska organ till multinationella

företag inkl. ledande cybersäkerhetsföretag. Informationen som rör det amerikanska försvaret kan ge fördelar i ett potentiellt framtida traditionellt krig samt i cyberkrig. Vidare kan ett inhämtande av informationen som rör cybersäkerhetsföretag såsom FireEye användas för att förbättra sina cyberattacker då man kan få ytterligare kunskap om motståndarens strategier, försvar och svagheter. Vidare kan informationen som berör företag användas för att utveckla det egna landets industri och innovation, och på så sätt få fördelar i konkurrensen på den internationella marknaden, dvs. en form av industrispionage.

Det kan dras en parallell till *privat information* som en del av förhandlingsmodellen av krig ("the bargaining model of war") och att en informationsasymmetri av faktorer som kan påverka utfallet av krig (exempelvis militär förmåga och strategi, nya vapensystem, allierade, etc.) mellan de inblandade staterna innebär olika uppskattningar av sannolikheten att krig kommer bryta ut. Om skillnaden är avsevärd kan den mer informerade aktören ställa större krav och acceptera färre eftergifter än vad den andra lär acceptera, vilket ökar risken för krig. Den som vet mest har störst makt inom förhandlingar (Levy & Thompson, 2010, s. 65-66), att jämföra med Francis Bacons tes "kunskap är makt". På så sätt kan espionage-operationen ses som ett försök att försöka minska informationsasymmetrin kring motståndarens strategier och skapa sig en fördel i en eventuell händelse att ett krig i traditionell bemärkelse riskerar att bryta ut.

SolarWinds var en mycket storskalig attack i bemärkelsen att den dels drabbade väldigt många företag, myndigheter och organisationer då SolarWinds hade omkring 30 000 kunder varav ca 18 000 fick den skadliga uppdateringen – men också för att attacken riktade sig mot aktörer i flera delar av världen; de drabbade befann sig i Nordamerika, Europa, Asien och Mellanöstern (Tidy, 2020). Att på annat sätt än genom cyberkrigföring genomföra en attack som drabbar 1) så många aktörer och 2) aktörer på så spridda geografiska platser hade varit mycket svårt – praktiskt, tidsmässigt och ur ekonomisk synvinkel. Det är mer eller mindre omöjligt att försöka få tag på samma mängd av och nivå av känslighet på information som man fick vid SolarWinds hack utan möjligheten till cyberangrepp. Att genomföra en supply chain-attack på ett mjukvaruföretag kan jämföras med att ha insiders i 18 000 organisationer. Det bör lyftas att cyberkrigföring många gånger är billigare än annan typ av krigföring sett till vad man kan åstadkomma. För det första är det billigare att utveckla cybervapen än utvecklandet av andra typer av vapen som kan skapa jämnstor skada (Jonsson, 2019, s. 109). Vidare kan cyberangrepp vara mindre kostsamt både ekonomiskt, då man kan substituera arbete med kapital (Bracken, 2017, s. 148) vilket inte minst är fördelaktigt i de länder vars relativa fördel är kapital, men även i termer av förlorade liv då man slipper använda sig av trupper med soldater.

Attacken mot SolarWinds innebar att även organisationer i länder som inte är förhållandevis geografiskt nära Ryssland drabbades. Enligt traditionella teorier om internationell rivalitet är geografisk distans en avgörande aspekt för om stater kommer vara involverade i en konflikt eller krig med varandra eller inte, då det helt enkelt inte är realistiskt och/eller kostnadseffektivt att

transportera beväpnade styrkor oerhört långa sträckor och till exempel över ett hav. Vidare lär inte motstridiga intressen, dvs. incitament till att ingå i en konflikt, uppstå om länderna ligger geografiskt långt ifrån varandra då de sannolikt inte kommer ha mycket kontakt med varandra, enligt teorin (Levy & Thompson, 2010, s. 56). Cyberkrigföring förändrar förutsättningarna för vad som är praktiskt möjligt och om krig inte längre enbart innefattar beväpnade styrkor – vilket utforskas i nästa rubrik – försvinner problemet med att förflytta beväpnade soldater; hackarna kan sitta varsomhelst och genomföra attacken. På så sätt kan förutsättningarna för vilka stater som kan föra krig mot varandra förändras. Det är möjligt att den andra delen av teorin, dvs. att geografisk distans spelar roll för uppkomsten av motstridiga intressen, håller. Samtidigt stämmer det inte nödvändigtvis att stater som är geografiskt långt ifrån varandra inte har kontakt med varandra i den globaliserade världen. Vidare, om det gäller till exempel en konflikt om vilken stat som har mest makt eller är största ekonomin behöver rivalerna inte vara geografiskt nära, ett exempel är Kina och USA som har Stilla Havet emellan sig.

Attacken mot SolarWinds innebar inte enbart att hackarna fick tillgång till känslig information genom en espionage-operation, den resulterade också i ekonomisk skada. SolarWinds uppger att de spenderade mellan 18-19 miljoner dollar på att utreda och åtgärda attacken enbart de första tre månaderna efter attacken upptäcktes (Satter, 2021). Cybersäkerhetsvärderingsföretaget BitSight samarbetade med Kovrr, vilka specialiserar sig på att finansiellt kvantifiera cyberrisk, för att ta fram en gemensam analys av den finansiella påverkan av SolarWinds hack och de uppskattar att de försäkrade förlusterna är ca 90 miljoner dollar (Shah, 2021). Vidare rapporterade Roll Call att amerikanska företag och myndigheter skulle behöva spendera upp till 100 miljarder dollar på att hantera och åtgärda skadan från attacken (Alkhadra et al., 2021; Ratnam, 2021). Attacken medförde också effekter på aktiehandeln för de drabbade företagen, exempelvis sjönk SolarWinds egen aktie med 23% en vecka efter attacken (Novet, 2020) och en månad senare rapporterades det om att den sjunkit 40% (Levisohn, 2021). Detta drabbar alltså inte bara företagen internt, men också alla som äger aktier i de berörda företagen. Det kan också tilläggas att röjda affärshemligheter och industrispionage-aspekten kan få ekonomiska konsekvenser.

Det är svårt att estimera de totala kostnaderna som följde SolarWinds hack då de inte kan reduceras till en enskild faktor och då man dessutom behöver ta hänsyn till konfidentiell och/eller känslig data med koppling till exempelvis de amerikanska försvarsmyndigheter som drabbats, vilket skulle medföra en risk för USAs nationella säkerhet. Alkhadra et al. lyfter att man därmed inte bör estimera kostnaderna endast i de pengar som spenderats, men snarare utifrån att förstå och uppskatta de direkta kostnader som krävs för att upptäcka och hantera viruset, indirekta kostnader som följer av att organisationen förlorar tillit och gott rykte samt gömda kostnader som följer av att tid som skulle kunna läggas på att maximera organisationens produktivitet istället behövs läggas på hantering av cyberangreppet (Alkhadra et al., 2021). Dessa kostnader måste estimeras i relation till att SolarWinds, som tidigare nämnt, hade 30 000 kunder varav 18 000 laddade ner den skadliga uppdateringen. Trots svårigheterna att estimera

exakta kostnader för SolarWinds hack kan man konstatera att attacken resulterade i stora kostnader för företag och finansbransch samt för myndigheter, departement och organisationer inom offentlig sektor – vilket kan påverka staters ekonomi i stort. Ett ofta förekommande mål för cyberattacker är att försvaga motståndarens ekonomi, och detta är betydelsefullt i den ryska förståelsen av krig (Jonsson, 2019, s. 2-8, 108), vilket kommer återkopplas till och analyseras djupare under nästa rubrik *"Förståelsen av krig"* då även förekomsten av ekonomiskt krig lyfts.

En annan aspekt av attacken mot SolarWinds är att den skapade oro samt påverkade tilliten till inte bara SolarWinds, men också de företag, myndigheter och organisationer som drabbades. Som nämnt innebar attacken bland annat indirekta kostnader som följer av att organisationer förlorar tillit och gott rykte. Att tillit rubbas kan inte enbart reduceras till ekonomisk skada, det utgör också en skada i sig själv. Ett syfte med att genomföra cyberattacker är att man kan skapa oro bland folket samt rubba tillit och stabilitet (Jonsson, 2019, s. 108, 152-153). Att cybersäkerhetsföretag såsom FireEye samt amerikanska försvaret och departement drabbades är särskilt värt att lyfta i sammanhanget. Attacken kan skapa oro bland både tjänstemän och medborgare för både de ekonomiska konsekvenserna som följde samt för vilken känslig information hackarna fått tillgång till och faktumet att detta är möjligt. Vidare kan det dras en parallell till informationskrigföring, som är en central del av Rysslands krigsstrategi (ibid, s. 2-8). Människor som är oroliga och har minskad tillit till samhället kan argumenteras lättare falla offer för desinformation.

En annan aspekt av att bedriva cyberkrigföring är att stater inte behöver officiellt deklarera krig (Jonsson, 2019, s. 108), vilket kan innebära att man i högre utsträckning kan operera under radarn och att det är lättare att undgå ansvar. Det kan dras en parallell till att det ofta är svårt att fastställa och bevisa vilken aktör som genomfört/beställt och är ansvarig för ett cyberangrepp. Attacken mot SolarWinds tros ha utförts av gruppen Cozy Bear på uppdrag av den ryska federationens yttre underrättelsetjänst (SVR) i syftet av en espionage-operation, men detta har emellertid inte kunnat bevisas. Även om det kan vara svårare att fastställa vilken aktör som är ansvarig för ett cyberangrepp och gärningsaktören därmed kan undgå konsekvenser i form av bestraffning, pekade USAs presidentiella administration ändå officiellt ut Ryssland som skyldig för SolarWinds hack och införde sanktioner mot Ryssland. Emellertid finns det möjlighet för Ryssland att säga att anklagelserna är västs propaganda då det inte går att bevisa att det var dem som genomförde cyberangreppet – vilket kan utgöra ytterligare ett led i informationskriget som benämns i kommande avsnitt.

2.2 Förståelsen av krig

En annan väsentlig del av att förstå hur cyberangrepp såsom SolarWinds hack har påverkat möjligheterna till att föra krig mot andra stater är att utforska staters förståelse av krig och vilken roll cyberkrigföring spelar i denna. Möjligheten att genomföra cyberangrepp har förändrat

förståelsen av krig för en del stater, däribland för Ryssland som tros ligga bakom attacken mot SolarWinds.

Den ryska uppfattningen representerad av den politiska eliten och centrala militärteoretiker är att konceptet krig förändrats fundamentalt då icke-militära medel såsom cyberattacker är så effektiva och kraftfulla att de bör förstås som våldsamma – de beräknas vara fyra gånger så viktiga som militära medel och utgör en egen form av krigföring. Den ryska uppfattningen är att icke-militära medel, däribland informationskrigföring, kan skapa förödande konsekvenser i lika hög grad som massförstörelsevapen som exempelvis kärnvapen (Jonsson, 2019, s. 4-7). Exempelvis menar Sergei Komov, en av Rysslands mest framträdande teoretiker inom informationskrigföring, tillsammans med representanter från ryska försvarsdepartementet och GRU att cybervapen kan skapa katastrofala skador på avgörande industriella, ekonomiska, energi- och kommunikationsanläggningar. Vidare kan man med cybervapen skapa ekonomisk kris eller kollaps, förstöra regerings- och militär verksamhet samt skapa panik och uppgivenhet i befolkningen (ibid, s. 108-109). Krig kan alltså inte längre enbart ses som beväpnade styrkor, vilket reflekteras i den allmänna uppfattningen bland forskare i Ryssland samt i ryska säkerhetsdoktriner och nyckeltjänstemän. Resultatet är att gränsdragningen mellan krig och fred har suddats ut, vilket man är medveten om. Vidare ser Ryssland västs – i bemärkelsen USA med dess europeiska allierade – spridande av pro-demokratiska budskap och främjande av mänskliga rättigheter som medveten krigföring gentemot dem eftersom att denna typ av informationskrigföring möjliggör så kallade “färgrevolutioner” som skett i till exempel Ukraina och Georgien, vilket Ryssland uppfattar som det största hotet mot dem från väst då man anser att syftet är att destabilisera samhället och hjärntvätta folket till att vända sig emot de styrande. Likaledes uppfattar man även västs ekonomiska sanktioner som ekonomisk krigföring i syfte att provocera fram ett regimskifte. Den ryska uppfattningen är att Ryssland befinner sig i ett krig med väst, ett krig som förs med med icke-militära medel i form av ett cyber-/informationskrig samt ekonomiskt krig men likväl ett krig (ibid, s. 5-7, 105-110, 120-125).

Utifrån detta kan attacken mot SolarWinds förstås som en del av ett större cyberkrig mellan Ryssland och väst. Möjligtvis kan angreppet också ses som en del av ett ekonomiskt krig. Även om attacken på SolarWinds drabbade organisationer världen över, var merparten av de drabbade i väst, framförallt i USA. Det är sannolikt att den huvudsakliga måltavlan var det amerikanska försvaret, men också andra amerikanska myndigheter och cybersäkerhetsföretag (Tidy, 2021; Willett, 2021, s. 11). Detta kan förstås inom ramen för att USA är tongivande i spridandet av liberala, pro-demokratiska budskap och även har bedrivit *social engineering* i öststater som exempelvis Ukraina, vilket Ryssland alltså uppfattar som medveten informationskrigföring (Jonsson, 2019, s. 2-5, 114-123; Mearsheimer, 2014, s. 77-80).

Om SolarWinds hack bör förstås också som en del av ett ekonomiskt krig bör det lyftas att sanktionerna som USA införde kan uppfattas av Ryssland som ett offensivt svar. Från västs håll

upplevs ett införande av sanktioner som en åtgärd som är “short of war”, dvs. ligger på en lägre nivå än krig (Jonsson, 2019, s. 2), vilket yttrar sig exempelvis genom USAs president Bidens uttalande i samband med tillkännagivandet av sanktionerna om att man vill de-eskalera situationen (Morrison, 2021). Enligt den ryska uppfattningen är sanktioner däremot inte en de-eskalering utan snarare en del av krigföring (Jonsson, 2019, s. 2). Ryssland och väst har alltså två ganska olika förståelser av hur krigföring bedrivs samt vad som är krig och inte, vilket även bör tas i beaktning när man analyserar händelsen.

Flertalet beslutsfattare har beskrivit attacken mot SolarWinds som “an act of war” (Wheeler, 2021; Willett, 2021, s. 8-9). Samtidigt finns det cybersäkerhetsexperter som menar att SolarWinds hack inte var en krigshandling men enbart en espionage-operation och att man bör vara försiktig med att göra sådana uttalanden. Författarna argumenterar att SolarWinds hack inte bör ses som krigföring eller ens en attack då operationen inte störde, förstörde eller skadade människor, system eller infrastruktur (ibid). Huruvida det sistnämnda påståendet stämmer kan ifrågasättas, som tidigare nämnt resulterade SolarWinds hack till ekonomiska förluster för företag, offentlig sektor inkl. amerikanska försvaret, och till viss del även finansbransch. Angreppet kan även argumenteras påverka tillit till säkerhet och skapa oro bland såväl medborgare som tjänstemän. Å andra sidan kanske hackarna inte räknade med att bli upptäckta och att de nämnda konsekvenserna inte var menade eller syftet med operationen. Det leder snarare an till den filosofiska frågan om det är uppsåt eller konsekvenser som avgör vad som är en attack eller krigshandling och inte. Vägvalet i den här frågan har också avgörande följder för huruvida man väljer att betrakta Solarwinds hack som en del av ett ekonomiskt krig eller inte.

Jonsson lyfter att det gjorts för lite västerländsk forskning på den ryska förståelsen av krig och att man snarare tenderar att fokusera på hur krig förändras generellt med antagandet att det är och förstås likadant för alla stater. Vidare menar han att en viktig insikt är att olika samhällen med olika kulturer och värderingar kan uppfatta samma fenomen, i det här fallet krig, olika. Kultur är en väsentlig kontext och förståelsen av krig kan inte isoleras från kultur – vilket är särskilt relevant för den ryska förståelsen av krig i vilken den ryska kulturen spelar stor roll (Jonsson, 2019, s. 7-8). Med andra ord, om vi förutsätter att attacken mot SolarWinds gjordes av en hackergrupp med stöd av den ryska regeringen och underrättelsetjänsten, kan vi inte tolka den enbart utifrån ett västerländskt perspektiv med en västerländsk förståelse av krig. Vi måste försöka förstå attacken inom ramen för den ryska kulturen och synen på krigföring. Ett avfärdande av konsekvenserna av SolarWinds hack – påverkan på ekonomi och tillit, som utgör en central del av rysk icke-militär krigföring – kan argumenteras vara naivt och en snävt västerländsk tolkning av krigföring. Samtidigt saknar vi kunskap om gärningsaktörens uppsåt, dvs. vilka konsekvenser som var menade och inte, och vi bör ta den kunskapsbristen i beaktning.

2.3 Staters fokus på cyberkapacitet

Fallet med SolarWinds- attacken är en tydlig påminnelse om omfattningen av fenomenet att cyberkapacitet, och inte minst cybersäkerhet, är ett område som ofta får sekundär roll i staters beslutsfattande. Attacken lyckades penetrera flera amerikanska institutioner med hög konfidentiell status och utvinna information från dessa. Om cybersäkerhet hade setts som den högsta prioriteten på den amerikanska statens agenda skulle detta troligtvis aldrig kunnat ske. På samma sätt ser vi hur denna effekt även återfinns hos företag då tusentals verksamheter blev infiltrerade av den illvilliga koden. Detta gäller onekligen även det företag som är den huvudsakliga aktören inom denna cyberattack, nämligen SolarWinds. I en artikel som skrivits av ett antal medlemmar i redaktionen för *IEEE Security and Privacy* i syfte att lägga fram olika perspektiv på incidenten skriver Bruce Schneier att SolarWinds i en stor utsträckning har vänt ryggen mot cybersäkerhetsfrågor eftersom de inte bedömdes vara lönsamt. Han skriver att företagets ägare, private equity-bolaget Thoma Bravo, är välkända för storskaligt kostnadsreducerande och att SolarWinds advisor för cybersäkerhet slutade på företaget med anledning att till och med grundläggande säkerhetsåtgärder ständigt avvisades (Benzel et al. 2021). Detta visar vidare på de stora incitament som finns för att utföra attacker såsom den mot SolarWinds då det mindre utvecklade försvaret inom cyberrymden är väldigt sårbart och förhållandevis enkelt att penetrera, samtidigt som man kan utvinna oerhört värdefull information och infiltrera de institutioner som påverkats av attackerna.

I och med attacken mot SolarWinds, i kombination med ett större nätverk av cyberangrepp mot bland annat Estland, Georgien, Ukraina och USA, ser vi att det finns ett land som är ett undantag för påståendet att cyber-åtgärder inte är en huvudprioritet för stater - nämligen Ryssland. Som tidigare redovisats för är den ryska uppfattningen att det pågår ett större informationskrig mellan deras egna stat och västvärlden, ett krig som till huvudsaklig del utspelar sig inom cyberrymden. De menar att det finns ett hot från västvärlden som består i informationskampanjer mot länder i Rysslands närområde och att de genom detta sprider deras agenda vilken tvärt går emot den ryska statens ideal (Jonsson, 2019, s. 108-109, 120-123). Således är Ryssland utifrån sitt perspektiv tvungna att utvidga sin kapacitet inom ramen för åtgärder inom cyberrymden och använda dessa ökade tillgångar för att motarbeta väst och delta i ett sorts informationskrig. Denna utveckling av rysk cyberkapacitet är något vi har sett klart och tydligt då staten har utfört kontinuerliga angrepp mot bland annat Estland (mest nämnvärt överbelastningsattackerna 2007) och Ukraina, men inte minst i och med attacken mot SolarWinds 2020. Angreppet mot SolarWinds visar på en utförlig operation med stora vinningar i relation till Rysslands uppfattade krig mot väst. Hackergruppen fick tillgång till känsliga dokument från allt från Homeland Security till National Nuclear Security Administration vilket gör attacken ett oerhört lyckat fall av så kallat cyberspionage mot en stat som sedan lång tid tillbaka setts som huvudsaklig ideologisk och global politisk statsfiende till Ryssland, nämligen USA (Azim, Khan & Rashid, 2021, s. 658).

Samtidigt som vi ser Ryssland utföra angrepp som dessa och ständigt uppvisa sin stora utveckling inom cybersfären så präglas resten av den internationella arenan av en avsaknad av motsvariga kapaciteter från andra länder. Med USA som exempel kan vi se att det genom åren har förekommit en undvikelse från att utveckla motsvarande kapaciteter inom cyberrymden och istället har fokus lagts på traditionell militär kapacitet. Detta har lett till att cyberrymden är ett slagfält där Ryssland återkommande vinner och utan hinder kan utföra handlingar såsom det utförliga spionaget genom supply chain-attacken mot SolarWinds (Azim, Khan & Rashid, 2021, s. 658).

Detta får en stor relevans när man ser det utifrån kontexten av att det finns en uppfattning av att det pågår en "Russian Power decline" där Ryssland som tidigare stormakt i Sovjetunionens glansdagar i allt större utsträckning förlorar sitt fäste på den internationella arenan. Michael Kofman och Andrea Kendall- Taylor beskriver i sin text "The Myth of Russian Decline - Why Moscow Will Be a Persistent Power" att det utifrån bland annat uttalanden från den amerikanska statsledningen med president Joe Biden i spetsen verkar som att det finns en uppfattning om att Ryssland är ett minskande hot på världsarenan med en stagnant ekonomi och en minskande population. Istället läggs det huvudsakliga fokuset inom amerikansk utrikespolitik på att motsätta sig den snabbt utvecklande stormakten Kina (Kendall-Taylor & Kofman, 2021. s.142-145). Kofman och Kendall-Taylor argumenterar i sin text för att detta är en felaktig uppskattning i och med det faktum att faktorer som exempelvis ekonomiska tillgångar inte nödvändigtvis genomgår en snabb utveckling inte är relevanta svagheter då Ryssland redan har stark ekonomi och militära kapaciteter som fortfarande kräver uppmärksamhet från amerikanskt håll. I kontexten för vårt fokus på cyberrymden ser vi att det mycket möjligt finns skäl att påstå att det finns mer kritik mot försummelsen av Ryssland som en stormakt inom världspolitiken än vad Kofman och Kendall-Taylor har framfört - nämligen att Ryssland är en av de stater som är mest prevalent inom cyber-arenan. Även om Ryssland inte till synes utvecklas i de områden som traditionellt sett har utgjort hot mot andra stater så finns det alltså skäl att ha i beaktning att cyberattackers ökade prevalens inom krig och konflikt kan utgöra en ny arena där Ryssland utvecklas i betydligt högre takt än andra stater. Om Ryssland således ska se som en revisionistisk stat som strävar efter att återta sin plats som stormakt ser vi att de tydligt har hittat en del av världspolitiken där de har ett markant försprång i jämförelse med andra stater. Landets cybermilitära kapaciteter är väldigt utvidgade och utvecklas även i snabb takt, om detta skulle fortsätta, samtidigt som andra stater fortsätter negligera det brådskande behovet att utveckla den egna cyberrymden, så finns det en möjlighet för Ryssland att gripa för att bli en sorts hegemon inom den cybermilitära arenan (Azim, Khan & Rashid, 2021, s. 649-650). Vi ser således att espionage som SolarWinds tillsammans med andra cyberattacker kan ha stora konsekvenser inom krig mellan stater och till och med ensamt förändra militära maktstrukturer och hotbilder på den internationella arenan.

2.4 Ytterligare implikationer

2.4.1 Operation under radarn

En annan stor aspekt av supply chain- attacken mot SolarWinds är att det finns en huvudsaklig avsaknad av motåtgärder mot de misstänkta gärningsaktörerna. En stor del av detta kan troligtvis attribueras till det faktum att det, som tidigare diskuterat, fortfarande råder en stor osäkerhet i exakt vem som orsakat attacken, vilket leder till att utförandet av en sorts hämnd-åtgärd blir väldigt komplicerat. Den ledande teorin om vem som ligger bakom angreppet är att det är en hackergrupp som fått finansiellt stöd från den ryska federationens underrättelsetjänst (SVR) och utfört attacken på deras beställning. Detta skulle innebära att det är ett angrepp som utförts mellanstatligt mellan två stormakter. Om detta skulle ha varit ett angrepp av ett traditionellt militärt slag, där det är tydligt att Ryssland har attackerat USA, skulle konsekvenserna kunna bli förödande. Ända sedan kalla kriget har de båda stormakterna lyckats bibehålla fred, till stor del med hjälp av en skräck för kärnvapen och ömsesidig garanterad förstörelse (MAD). Detta fungerar eftersom båda sidor är medvetna om att aggression mot den andra parten har risken att eskalera genom en upprustningsspiral till ett storskaligt våld med kärnvapen som skulle jämna ut nationerna med marken (Hall, 2014. s. 64). I fallet av SolarWinds ser vi att någon sådan eskalering inte ägt rum, utan den största repressalien som Ryssland har fått i koppling till attacken är ekonomiska sanktioner från USA. Ryssland har ständigt nekat att de skulle ha någon inblandning i attacken, och den osäkerhet som således fortfarande råder kring vem som faktiskt har utfört angreppet är troligtvis en stor förklaring till att inga större motangrepp har utförts. Det faktum att hackare kan utföra storskaliga operationer och samtidigt till stor del befinna sig under radarn gör att eventuella motangrepp som utförs av stater på basis av misstankar skulle kunna vara mycket riskfyllda, då motangreppen i sig skulle kunna leda till totalt onödig eskalering om misstankarna är fel. Att det kan vara svårt att identifiera vart cyberangrepp härstammat från och den svårighet som därmed uppstår i att bestraffa attackerna kan vara något som öppnar dörren till offensiva åtgärder som annars inte skulle kunna inträffa och således förändra paradigmet för krigföring. Cyberangrepp som det mot SolarWinds kan alltså ses som ett sätt att undvika eskalering eller förödande motangrepp och således vara ett säkrare sätt att bedriva krigföring mot stater som besitter hög militär kapacitet (Bracken, 2017, s. 152).

2.4.2 Diskrepans mellan utveckling av cyberattacker och cyberförsvar

En annan förklaring bakom att cyberattacker i större utsträckning blir effektiva som medel inom krigföring, är att cyberattacker normalt sett utvecklas i en högre takt än försvarsåtgärderna (Gupta & Venkatraman, 2017. s. 83-85). Detta beror till stor del på att det på många sätt är cyberattackerna som leder utvecklingen inom fältet, eftersom cybersäkerheten endast behövs när det finns någonting att skydda sig mot. När en ny form av cyberattacker utvecklas och upptäcks behöver staterna utveckla ett skydd mot dessa, vilket är en lång och tidskrävande process. Detta ger både den nykomna cyberattacken tid att verka, och även tid för att utveckla nya former av cyberattacker som det ännu inte finns försvar mot (ibid, s. 84-85). Med detta i åtanke är det inte

svårt att se varför cyberattacker oftast utvecklas snabbare än cybersäkerheten, och för att hitta ett talande exempel för detta behöver vi inte kolla längre än fallet med SolarWinds. Det faktum att hackergruppen som utförde angreppet mot SolarWinds lyckades befinna sig innanför systemen hos specialister inom cybersäkerhet såsom FireEye och det amerikanska försvarsdepartementet i flera månader samt få tillgång till deras och många andra organisationers konfidentiella dokument talar starkt för ansatsen om att cyberattacker utvecklas snabbare än försvaret mot dem. Om fallet skulle vara det motsatta skulle troligtvis koden inte kunna komma in i systemet överhuvudtaget, och skulle definitivt inte gå obemärkt förbi i den utsträckta tidsperiod som den gjorde.

Denna diskrepans i hur snabbt utvecklingen inom fälten av cyberattacker respektive cybersäkerhet förs framåt leder till att det finns ett ökat incitament för stater att lägga ett stort fokus vid cyberattacker inom krigföring. Som tidigare diskuterat kan exempelvis innehavandet av massförstörelsevapen göra det effektivt sett omöjligt för andra stater att utföra offensiva angrepp inom traditionell krigföring utan att bli bemötta av motangrepp av en extrem grad, vilket gör detta till ett sorts ultimat försvar i enlighet med teorin om kärnvapenfred. Något liknande återfinns emellertid inte inom sfären av cybersäkerhet. Cyberattackerna utvecklas snabbare än cyberförsvaret vilket gör att man inte fullständigt kan försäkra sina system från att bli angripna, och som tidigare diskuterat är cyberattacker med samma förödande kraft som kärnvapen inte applicerbart som ett hot om “mutual destruction” som avskräcker angripare eftersom det inte är lika tydligt vart cyberattacken härstammar från och således vart massförstörelsevapnet skall riktas.

2.4.3 Wakeup Call och upprustning

Gupta och Venkatraman menar att en möjlig konsekvens av storskaliga cyberattacker är att det agerar som en “wakeup call” för nationerna som blir utsatta att de behöver lägga större satsningar på sin cyberkapacitet (Gupta & Venkatraman, 2017. s. 83-84). Detta är onekligen fallet med cyberattacken mot SolarWinds då den har ökat uppmärksamheten kring hoten om cyberattacker samt den ökade prevalensen av dessa inom krigföring. Dan Lorenc, som är grundare och VD för företaget Chainguard, som specialiserar sig inom säkerhet mot supply chain-attacker, sa “After the SolarWinds incident, it almost was a night and day shift in awareness and momentum” (Hay Newman, 2021). Det finns en mängd andra exempel på Rysslands användning av både supply chain-attacker och cyberattacker i allmänhet, inte minst i landets geografiska närområde som Ukraina och Baltikum. Det faktum att SolarWinds-attacken var riktad mot USA och stora teknologi-företag gjorde däremot att detta resonerade starkare just i dessa sfärer och har lett till en ökad uppmärksamhet hos dem. “It definitely was a turning point” sa Eric Brewer, vice ordförande för Google (Hay Newman, 2021). Detta går starkt i linje med Gupta och Venkatramans tes om att det ofta krävs en storskalig cyberattack för att adekvata satsningar ska läggas på cybersäkerhetsfrågor, Vi ser därmed att attacker som SolarWinds hack

har potential att bidra till upprustning inom cyberkapacitet, vilket vidare kan öka vikten av cyberrymden inom framtida krigföring.

2.4.4 Hackergrupper och organisationers inflytande

Det finns inget konstaterande om vem som utförde attacken mot SolarWinds 2020 och ingen har öppet tagit på sig skulden. Som tidigare nämnt är den ledande teorin att attacken har utförts av Cozy Bear, en cyberkriminell grupp som är väl bekanta med den typ av "supply chain-attack" som angreppet mot SolarWinds är klassificerat som, på beställning av SVR. Det faktum att en stat kan anlita en grupp som Cozy Bear och uppnå så mycket som man gjorde med SolarWinds-attacken, som att samla konfidentiell information från myndigheter, få tillgång till databaser av gigantiska företag på världsarenan och skapa stor ekonomisk förlust hos alla påverkade, är också något som visar på en annan konsekvens av cyberattackernas inträde i krig och konflikt – nämligen att grupper av hackers kan få en stor påverkan i konflikter. Stater blir allt mer beroende utav sin tillgång till cyberrymden och klassificerad information arkiveras ständigt inom den. Attacker som SolarWinds visar på hur stater kan använda sig av samarbeten med hackergrupper som Cozy Bear för att åstadkomma oerhört utförliga espionage. Men hackergruppers inflytande sträcker sig längre än så. Som tidigare nämnt finns det idag möjlighet till cyberattacker som kan orsaka extrema mängder skada och i och med att cyberattacker ständigt utvecklas så kan man bara fantisera kring hur förödande de under kommande tid kan bli, med hot mot exempelvis kärnkraftsreaktorer. Att denna militära makt landar hos hackergrupper gör både att stater får ökade möjligheter att föra krig mot andra stater genom att anlita grupper av detta slag, särskilt om staten själv inte har välutvecklade resurser i cyberrymden, men det gör också att vi kan se ett möjligt skifte där stater inte längre är de enda aktörerna med möjlighet att föra krig mot andra stater. Vår frågeställning om hur staters möjligheter att föra krig med varandra har påverkats av cyberattackers inträde kanske således inte bara blir besvarad med tanke på att hackergrupper kan anlitas för staternas vinning, utan den blir möjligtvis även ifrågasatt kring huruvida stater fortfarande bör ses som de enda aktörerna på den internationella arenan som krig är centrerat kring.

3. Diskussion

3.1 Ökade Möjligheter inom Krigföring

Attacken mot SolarWinds gav hackarna tillträde till ca 18 000 organisationers databaser. Hur mycket av denna information som faktiskt var eftersträvad är fortfarande inte klarlagt, men en sak står definitivt säkert – en espionageoperation av denna utsträckning skulle aldrig vara möjlig om det inte vore för inträdet av cyberrymden och de möjligheter till krigföring som den för med sig. Tanken på att ha 18 000 olika insiders i allt från företag till amerikanska försvarsdepartement som skulle dela med sig av relevanta konfidentiella dokument är något som nästan är

skrattretande att överväga. Supply chain- attacken mot SolarWinds visade däremot på att det är möjligt att uppnå samma nivå av espionage med hjälp av cyberangrepp.

I analysen såg vi att SolarWinds visar på att cyberkrigföring öppnar möjligheter som traditionell krigföring inte kan likna sig med – inte bara i termer av hur många organisationer som påverkades, utan även i hur geografiskt spridda dessa organisationer är. Att kunna angripa organisationer som sprider sig över hela Nordamerika, Europa, och Asien samtidigt är något som är praktiskt omöjligt utanför ramen av cyberattacker. Utöver detta var inte attacken endast effektiv som en form av espionage, utan var också effektiv i termer av en ekonomisk krigföring då det uppstod stora kostnader för såväl företag och stater (även om man inte kan vara säker på om dessa konsekvenser var menade). Inte nog med det så finns det även skäl att tro att en attack som denna har lett till minskad tillit till de organisationer som blivit drabbade. Inte minst gäller detta institutioner som amerikanska försvarsdepartement och cybersäkerhetsföretag som FireEye som är menade att motarbeta det som de själva blev utsatta för.

Angreppet mot SolarWinds är en tydlig indikation på att cyberattackernas intåg i krigföring har påverkat fältet oerhört. När man dessutom inkluderar att cyberattacker av mer aggressiv natur har potential att förstöra infrastruktur, begränsa kommunikationsmöjligheter och sprida desinformation så finns det tydliga tecken på att traditionell krigföring är för evigt förändrad.

3.2 Ovisshet och Misstänksamhet

Vid noga studerande av fallet med cyberangreppet mot SolarWinds 2020 har vi funnit att en sak som präglar cyberkrigföring, på ett helt annat sätt än med traditionell krigföring, är ovisshet. Till att börja med såg vi att det finns en ovisshet om vem som har utfört handlingen. Ingen har tagit på sig skulden för att ha angripit SolarWinds Corporation och det finns inget spår som kunnat avgöra vem som ligger bakom supply chain- attacken. Vi har sett att flera individer och organisationer som är verksamma inom fältet för cyberaktiviteter samt politiska ledare pekar fingret mot den ryska statens underrättelsetjänst (SVR) som de menar ha anlitat gruppen Cozy Bear för att utföra attacken. Vi analyserade den osäkerhet som ändå kvarstod inom cyberattacken utifrån att det ger stater en möjlighet att operera “under radarn” inom krigföring. Misstänksamheten mot SVR och Cozy Bear har mycket att göra med de mål som attacken tros ha, vilka skulle vara förenliga med eventuella intressen för den ryska staten.

Däremot har det även uppenbarat sig att det består en stor osäkerhet även i termer av vilka mål som gärningsaktören bakom angreppet förväntas ha. Angreppet mot SolarWinds var väldigt omfattande och ca 18 000 organisationer laddade ned den illvilliga koden. I och med att angreppet var en supply chain- attack där gärningsaktören har hackat sig in hos en distributör istället för direkt på specifika organisationer blir det väldigt svårt att veta vilka organisationer som faktiskt var måltavlorna för operationen. Vi har sett att det mest troliga scenariot uppfattas

vara att det är ett espionage på uppdrag av SVR då angreppet gav tillgång till konfidentiell amerikansk militär- och försvarsinformation, men det finns även ett flertal andra möjligheter som exempelvis att angreppet bör förstås som en ekonomisk krigföring där målet är att försvaga den västliga ekonomin genom de kostnader som angreppet utgjorde eller att angreppet har utförts i syfte att utvinna information om R&D från stora teknologi-företag som Microsoft och Intel.

Denna ovisshet introducerar något som efter vår studie framstår som en av de större påverkningarna som inträdet av cyberattacker har haft inom krig och konflikt. Att kunna operera under radarn och skapa ovisshet kring både vem som har utfört handlingen och vad uppsåtet har varit är något som är vanligt förekommande inom cyberattacker, vilket inte kan sägas om traditionell krigföring. När trupper i uniform intar ett land är det knappast något tvivel om vilket land som har orsakat attacken, och en bomb som släpps i en stad har knappast någon större ovisshet kring sig i termer av uppsåt. Givetvis finns det attacker av traditionellt slag som fortfarande omges av ett visst mysterium kring dessa frågor, som exempelvis attacken mot Nordstream år 2022 (Adler, 2022), men dessa attacker är få och sällan förekommande. Cyberattacker har däremot gjort ovisshet kring exempelvis aktör och uppsåt till något som kan komma att bli en vanlig företeelse inom krigföring.

Konsekvenser och fördelar med att operera under radarn och skapa ovisshet är något som därför har blivit ett genomgående tema i analysen. I fallet med SolarWinds såg vi hur ovissheten har hämmat både möjligheterna för hämndåtgärder från de utsatta och applikation av lagar inom internationell rätt - vilket visar på svårigheten att hålla gärningsaktörer till svars för deras handlingar. Vi skulle däremot även vilja diskutera denna problematik i en större kontext. I och med cyberattackers framväxt som en allt större del av modern krigföring kommer även ovissheten ta en större plats på den internationella arenan. Ovisshet kring attacker för onekligen även med sig en misstänksamhet mot vilka man tror har orsakat attacken. Detta är något som både offensiva stater och individuella grupper skulle kunna ta nytta av genom att utföra angrepp i syfte att skapa misstänksamhet mellan två andra stater (exempelvis om dessa är i en pågående dispyt om målet för angreppet). Således kan cyberattacker få utvidgade taktiska implikationer då man kan öka misstänksamhet mellan stater som ses som opponenter på den internationella arenan, som en utökad aspekt av informationskrig. I en värld där cyberattacker blir mer och mer vanligt förekommande skulle ovisshet och misstänksamhet kunna prägla inte bara cyberrymden utan den internationella arenan som helhet och utöka belägget för realismens ansats om “allas krig mot alla” där tillit och samarbete försvåras och den egna statens säkerhet värnas.

3.3 Komplement kontra alternativ

I vår analys av hur cyberangrepp såsom SolarWinds hack påverkat möjligheterna till att föra krig mot andra stater, uppstår frågan om huruvida cyberkrigföring bör ses som ett komplement eller ett alternativ till traditionell krigföring.

Inom ramen för cyberkrigföring som komplement kan cyberangrepp som SolarWinds användas för att få information som ger avgörande fördelar i ett eventuellt framtida eller pågående traditionellt krig. Det kan också återkopplas till teorin om *privat information*, och att man genom en sådan här espionage-operation kan få tydligare uppfattning om förutsättningarna och sannolikheten för att ett traditionellt krig skall bryta ut. Cyberkrigföring kan även förstås som ett komplement till traditionell krigföring genom att man i ett traditionellt krig med hjälp av cyberattacker exempelvis kan slå ut väsentlig infrastruktur, förstöra regerings- och militär verksamhet eller sänka moralen genom påverkanskampanjer, i syfte att få en fördel i det traditionella kriget. Genom att försvåra för militär och civilbefolkning kan man påverka motståndskraften och uthålligheten hos staten man för krig mot. Cyberkrigföring som komplement i traditionellt krig kan också möjliggöra för mindre trupper att besegra större styrkor. Ett exempel, som också är en av de första nyckelhändelserna som visade på betydelsen av information-teknisk krigföring och utspelade sig under Gulfkriget (1990-1991), är när amerikanska trupper lyckades, med mycket få förluster, besegra de betydligt större irakiska trupperna på grund av högre utveckling inom cybersfären då amerikanska styrkor bl. a. inriktade sig på irakisk kommunikation- och informationsinfrastruktur (Jonsson, s. 12, 105-106).

Emellertid visar analysen att cyberkrigföring också kan utgöra en krigföring i sig, dvs. ett alternativ till traditionell krigföring. Icke-militära medel såsom cyberangrepp kan skapa minst lika stor, om inte större, skada i jämförelse med traditionella militära medel. Vidare är cyberkrigföring väldigt effektivt utifrån att man kan skapa förödande skador samtidigt som det är mindre kostsamt än traditionell krigföring. Huruvida stater ser cyberkrigföring som ett alternativ till traditionell krigföring skiljer sig emellertid stater emellan. Den ryska förståelsen av krig har breddats, krig kan inte enbart ses som beväpnade styrkor längre och uppfattningen är att man är i krig med väst på cyberarenan. Samtidigt inkluderar den västerländska förståelsen av krig sällan icke-militära medel. Resultatet blir att de två sidorna verkar samt uppfattar motståndarens handlingar utifrån ramverket för sin egen förståelse av krig.

Utifrån cyberkrigföringens effektivitet och möjligheter är det inte osannolikt att tänka sig att större fokus kommer att läggas på cyberkrigföring som alternativ till traditionell krigföring. SolarWinds hack har beskrivits som ett “wake-up call” och med avseende på analysen om cybersäkerhet är det inte otänkbart att även väst kommer lägga mer resurser på cybersfären och att den västerländska förståelsen av krig kommer att breddas.

Att cyberkrigföring kan ses som ett alternativ till beväpnade styrkor innebär inte att den senare kommer försvinna helt, men snarare att det utgör ett alternativ i bemärkelsen att krig kan föras på olika arenor; den fysiska arenan eller på cyberarenan. Det är viktigt att ha i åtanke att konsekvenserna gör sig märkta i den fysiska arenan oavsett form av krigföring. Krigföring på cyberarenan kan tänkas leda till mindre blodspillan och förluster av liv än traditionell krigföring

med beväpnade styrkor. Samtidigt kan cyberattacker leda till förödande skador på samhället till den grad att det sker en samhällskollaps – annars hade inte exempelvis Ryssland lagt så stor vikt vid den här typen av krigföring, vilket har framkommit i analysen. Attacken mot SolarWinds var allvarlig, men den ödelade inte samhället. En mer intensiv och aggressiv våg av attacker – mot essentiell infrastruktur eller genom mer subtil informationskrigföring och påverkanskampanjer, varav det senare nästan kan vara farligast – är något helt annat.

Vidare finns det risk att cyberattacker drabbar civila till en större grad än attacker gjorda av beväpnade styrkor. I traditionella krig är de huvudsakliga målen motståndarens militär och enligt krigsetik skall civila hållas utanför till så stor grad som möjligt – detta frångås visserligen inte sällan, inte minst i Rysslands krig i Ukraina då även civila har varit måltavlor för den ryska militären. Emellertid finns risk för att fler krigsbrott begås genom att civila blir måltavla när krigföring sker på cyberarenan. Själva poängen med cyberkrigföring och det som gör det just så kraftfullt är att man kan ödelägga ett samhälle, och det gör man bäst genom att omöjliggöra ett vardagsliv för civilbefolkningen. I ett cyberkrig kanske civilbefolkningen inte blir beskjutna eller bombade, men de kan få utstå svält och köld, vilket kan leda till döden. Cyberkrigföring som alternativ till traditionellt krig kan argumenteras leda till mindre blodutgjutelse, men det leder inte nödvändigtvis till mindre lidande för civilbefolkning.

I stor skala kan cyberattacker skapa katastrofal skada på ett samhälle, men för nuvarande påminner de flesta attacker om SolarWinds på så sätt att det rör sig om relativt enstaka attacker som dyker upp då och då och stör människor i deras vardagsliv – samhället kan försvagas något tillfälligt men efter ett tag går livet vidare. När krig förs genom cyberkrigföring suddas gränsdragningen mellan krig och fred som vi känner till det ut, och detta är någonting som är framträdande just när det sker attacker som SolarWinds, dvs. cyberattacker i mindre skala till skillnad från det dystopiska scenariot när cyberattacker används mer offensivt som nyligen diskuterats. Att gärningsaktören är okänd eller obekräftad, dvs. det att man inte vet vem som bär skulden men att det ändå finns en aning, tillför ytterligare ett element till att gränsdragningen mellan krig och fred suddas ut. När cyberkrigföring utgör det alternativa kriget behöver stater inte deklarera krig på samma sätt som i traditionell krigföring, vilket kan skapa mer ovisshet bland befolkning och beslutsfattare, vilket tidigare diskuterats.

Som framkommit i analysen innebär svårigheten att bekräfta vem som bär skulden för en cyberattack att man kan begå fler attacker och undgå ansvar, till skillnad från traditionell krigföring. En fråga som uppstår med anledning av att förståelsen av krig breddas till att inkludera cyberkrigföring är huruvida det blir krig, i bred förståelse, oftare? Eller är det snarare så att krig i traditionell, snäv definition blir mindre vanligt förekommande? Det här är något som kan vara intressant att studera i framtiden.

3.4 Förändring av Maktstrukturer

En annan aspekt av cyberattacker som med utgångspunkt i SolarWinds visat sig bli ett genomgående tema är att inträdet av cyberattacker inom krig och konflikt har potential att få stor påverkan på skiften inom de militära maktstrukturerna på den internationella arenan. Cyberrymdens ökade inflytande på krigföring har onekligen lett till många utmaningar för stater vars strategi har genomsyrats av en utveckling av huvudsakligen traditionella militära medel och således även ett förkastande av utveckling av cyberkapacitet. På samma sätt ser vi däremot att förändringen av krigföring även kan ses som en möjlighet för de aktörer som har valt att lägga ett stort fokus på utveckling av just cybermilitära medel.

I och med Rysslands misstänkta medverkan i angreppen mot SolarWinds ledde vår analys kring incidenten oss till ett studerande av Rysslands kapacitet inom cyberkrigföring. Detta visade sig vara ett praktexemplar på en stat som har tagit nytta av det förväntade skiftet inom krigföring genom att utveckla starka cybermilitära tillgångar. Vid studerandet av detta ansåg vi att det finns anledning att tänka sig att uppfattningen av Ryssland som en krympande militärmakt med en stagnant ekonomi och en minskande befolkning är missvisande och att det istället finns skäl att tro att Ryssland istället skulle kunna få en markant högre militär maktposition där det till och med finns tecken på en utveckling av staten som en cyberhegemon. Ett sådant skifte i militärmakt skulle onekligen inte bara påverka Ryssland utan alla som har gjort stora satsningar på cyberkapacitet (eller som har en brist på satsningar av sådan karaktär). Således kan vi se hur cyberkrigföringens ökade prevalens på den internationella arenan kan bidra till ett skifte i maktrelationer mellan stater och kan således även ge nya indikationer på hur eventuella framtida konflikter kan förväntas spela ut.

I vår analys framgick däremot även att stater inte är de enda aktörer vars makt inom krig och konflikt förändras. I samband med utredandet av hackergruppen Cozy Bear framgick även att grupper med cybermilitär kapacitet både har fått och kan förväntas få mer inflytande på den internationella arenan. Analysen kring SolarWinds visade ett möjligt exempel på hur stater kan använda sig av mindre grupper för att åstadkomma sina mål inom krigföring och på så sätt utöka sin makt. Däremot ser vi även att grupperna i sig själva kan få mer makt. På grund av cyberattackernas effektivitet i både kostnad och i vad de kan åstadkomma så kan självständiga organisationer med politiska mål få ökade möjligheter att uppnå dessa på ett sätt som inte traditionell krigföring kan erbjuda. Hacktivistgrupper har vid flera tillfällen visat sig kunnat ha en stor påverkan på konflikter genom att exempelvis motarbeta begränsningar av internetåtkomst utförda av stater för att minska informationsflöden till dess medborgare. Terrorgrupper är en annan typ av organisation som skulle kunna uppnå mycket med hjälp av cyberattacker. Det är inte ovanligt att sådana grupper har ambitioner att attackera och föra krig mot hela nationer, vilket inte är möjligt att realistiskt sett uppnå med de begränsade traditionella militära medel som de ofta innehar. Med intåget av cyberkrigföring finns det däremot möjlighet för dessa grupper att expandera utsträckningen av deras krigföring och således uppnå mer makt och inflytande.

4. Slutsatser

I besvarandet av frågeställningen "*Hur har cyberangrepp såsom SolarWinds hack påverkat möjligheterna till att föra krig mot andra stater?"* har vi identifierat fyra huvudsakliga teman; a) ökade möjligheter inom krigföring, b) ovisshet och misstänksamhet, c) cyberkrigföring som komplement kontra alternativ samt d) förändring av militära maktstrukturer.

Vår fallstudie av SolarWinds hack visade tydligt att cyberattacker har utökat de möjligheter som finns tillgängliga inom krigföring. Den utförliga attacken gjorde det möjligt att både bedriva espionage mot och skapa stora ekonomiska kostnader för en oerhört stor mängd företag och politiska organ trots det faktum att dessa befinner sig på geografiskt spridda platser. Cyberkrigföring har med andra ord möjliggjort att man kan attackera 1) en högre mängd aktörer och 2) aktörer oavsett geografisk distans. Det här kan utmana traditionella teorier om vilka stater som kan tänkas gå i krig med varandra då det finns färre hinder än i traditionell krigföring i kombination med en alltmer globaliserad värld. En annan möjlighet med cyberangrepp är att man kan påverka tillit och stabilitet i ett samhälle, och på så sätt även minska motståndarens förmåga att slå tillbaka.

Vi har även sett att cyberrymden präglas av en osäkerhet, vilket har stora implikationer på krigföring genom att det möjliggör operationer "under radarn". Detta innebär att gärningsaktörer ofta inte kan konstateras ligga bakom attacker som de utfört, och således inte heller kan ställas till svars för dessa. Denna anonymitet leder till att cyberangrepp i stor utsträckning kan utföras utan någon större rädsla för hämndåtgärder, vilket även har möjlighet att kringgå koncept som är allmänt vedertagna inom traditionell krigföring såsom kärnvapenfred. Vidare leder osäkerheten kring att man inte kan veta vem som utfört en attack till att det bildas en ökad misstänksamhet på den internationella arenan. Detta är också något som kan utnyttjas inom informationskrigföring genom att man kan skylla cyberangrepp på andra stater, vilket således är en utökad taktisk implikation av cyberattacker på krigföring. Vidare, om den ansvariga staten pekas ut som gärningsaktör finns möjligheten att framhålla att anklagelsen mot dem snarare är en del av ett informationskrig.

Vi har sett att cyberkrigföring kan ses både som ett komplement och som ett alternativ till traditionell krigföring. Som komplement kan det skapa avsevärda fördelar för gärningsaktören i det traditionella kriget, exempelvis genom espionage eller attacker mot infrastruktur. Emellertid kan cyberkrigföring också utgöra ett alternativ till traditionell krigföring, vilket inte innebär att beväpnade styrkor kommer att försvinna helt – snarare att ett resultat av möjligheten till att genomföra cyberattacker är att det har skapats olika arenor för krig; cyberarenan och den fysiska arenan. Konsekvenserna av cyberkrigföring märks dock fortfarande huvudsakligen på den fysiska arenan. När medlen är icke-militära påverkar det också framförallt de som är utanför den

militära sfären, dvs. civila riskerar att bli mål i högre utsträckning än i traditionellt krig. Cyberkrigföring och de ökade möjligheter som det innebär har resulterat i att krig som koncept har breddats, men stater kan även ha olika förståelser av krig.

Att stater har olika förståelser av krig har också lett till att de har lagt olika stor vikt vid utvecklandet av cyberkapacitet. Vid ett skifte inom krigföring mot ett ökat fokus på cyberrymden skulle detta ha implikationer för hur militära maktstrukturer på den internationella arenan förändras. Detta eftersom stater med välutvecklad cyberkapacitet skulle få ett försprång inom detta skifte i jämförelse med de som inte har haft samma utveckling. Utöver detta finns det även möjlighet för oberoende grupper och organisationer med hög cyberkapacitet att få ett större inflytande över krigföring. Detta eftersom det inte längre är nödvändigt att besitta en armé eller andra tillgångar inom traditionell krigföring för att kunna ha en betydande påverkan på utkomsten av krig och konflikter.

Sammanlagt har vi utifrån vår studie klarlagt att cyberattacker såsom den mot SolarWinds Corporation 2020 har påverkat krigföring mot stater i en stor utsträckning och på flera olika sätt. Dessutom finns det, i och med att världens förlitande på cyberrymden i kontemporär tid snabbt har ökat och fortsätter att öka, skäl att tro att denna påverkan inte kommer att saktas ned i någon nämnvärd utsträckning. Därför finns det ständigt utrymme för fortsatt forskning inom ämnet, och framtida cyberattacker kan komma att påverka krigföring på sätt som vi idag inte hade kunnat tänka oss. Således är det i och med slutförandet av vår studie tid för oss att bevittna skiftet till - *det nya kriget.*

Referenser

Adler, Katya (2022). A journey to the site of the Nord Stream explosions. *BBC.* 18 november. Länk: https://www.bbc.com/news/world-63636181 (hämtad: 2022-12-24)

Alkhadra, Rahaf; Abuzaid, Joud; AlShammari, Mariam & Mohammad, Nazeeruddin (2021). SolarWinds Hack: In-Depth Analysis and Countermeasures. *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT),* s. 1-7. Länk: https://ieeexplore-ieee-org.ludwig.lub.lu.se/document/9579611 (hämtad: 2022-12-16)

Andersson, Jan Joel (2014). *Krig och konflikter.* i: Gustavsson, Jakob & Tallberg, Jonas (red.) (2014). *Internationella relationer.* 3:e uppl. Lund: Studentlitteratur.

BBC (2021). *US imposes sanctions on Russia over cyber-attacks*. 16 april. Länk: https://www.bbc.com/news/technology-56755484 (hämtad: 2022-12-21)

Benzel, Terry; Bret Michael, James; Landwehr, Carl; Mannan, Mohammad; Massacci, Fabio; Mirkovic, Jelena; Peisert, Sean; Prakash, Atul; Schneier, Bruce & Okhravi, Hamed (2021). Perspectives on the SolarWinds Incident. *IEEE Security & Privacy*, vol. 19(2), s. 7-13. Länk: https://ieeexplore-ieee-org.ludwig.lub.lu.se/stamp/stamp.jsp?tp=&arnumber=9382367 (hämtad: 2022-12-12)

Bhunia, Suman & Sterle, Lindsey (2021). On SolarWinds Orion Platform Security Breach. *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, s. 636-641. Länk: https://ieeexplore-ieee-org.ludwig.lub.lu.se/document/9604375 (hämtad: 2022-12-16)

Bracken, Paul (2018). Cyberwar and its strategic context. *Georgetown Journal of International Affairs*, vol. 18(3), s. 147-157.

Datta, Prattim (2022). Hannibal at the gates: Cyberwarfare and the SolarWinds Sunburst hack. *Journal of Information Technology Teaching Cases*, vol. 12(2), s. 115–120.

Esaiasson, Peter; Gilljam, Mikael; Oscarsson, Henrik; Towns, Ann E. & Wängnerud, Lena (2017). *Metodpraktikan: konsten att studera samhälle, individ och marknad.* 5:e uppl. Stockholm: Wolters Kluwer.

Gupta, Karun & Venkatraman, B. (2017). Cybersecurity - Its Effects on National Security and International Relations. *Indian Journal of Law & Public Policy*, Vol. 3(2), s. 75-88. Länk: https://heinonline-org.ludwig.lub.lu.se/HOL/Page?lname=Venkatraman&public=false&collection=journals&handle=hein.journals/ijlpp3&men_hide=false&men_tab=toc&kind=&page=75 (hämtad: 2022-12-12)

Hall, Martin (2014). *Realism.* i: Gustavsson, Jakob & Tallberg, Jonas (red.) (2014). *Internationella relationer.* 3:e uppl. Lund: Studentlitteratur.

Hay Newman, Lily (2021). A Year After the SolarWinds Hack, Supply Chain Threats Still Loom. *Wired.* 8 december. Länk: https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/ (hämtad: 2022-12-04)

Jonsson, Oscar (2019). *The Russian understanding of war: blurring the lines between war and peace.* Washington, DC: Georgetown University Press.

Kendall-Taylor, Andrea & Kofman, Michael (2021).The Myth of Russian Decline: Why Moscow Will Be a Persistent Power. *Foreign Affairs*, vol. 100(6), s. 142-152. Länk: https://heinonline-org.ludwig.lub.lu.se/HOL/P?h=hein.journals/fora100&i=1276 (hämtad: 2022-12-27)

Levisohn, Ben (2021). The SolarWinds Hack Was Huge. Here's Why JPMorgan Is Defending the Stock. *Barrison's.* 14 januari. Länk:

https://www.barrons.com/articles/the-solarwinds-hack-was-huge-jpmorgan-is-defending-the-stock-51610645288 (hämtad: 2022-12-29)

Levy, Jack S. & Thompson, William R. (2010). *Causes of war.* Chichester: Wiley-Blackwell.

Lindvall, Johannes (2007). Fallstudiestrategier. *Statsvetenskaplig tidskrift*, vol. 109(3), s. 270-278.

Morrison, Sara (2021). Biden makes good on his promise to punish Russia for the massive SolarWinds hack. *Vox.* 15 april. Länk: https://www.vox.com/recode/22385555/biden-solarwinds-hack-russia-sanctions (hämtad: 2022-12-28)

Novet, Jordan (2020). SolarWinds hack has shaved 23% from software company's stock this week. *CNBC.* 16 december. Länk: https://www.cnbc.com/2020/12/16/solarwinds-hack-triggers-23percent-stock-haircut-this-week-so-far

Azim, Syed Wasif; Khan, Anum Yar & Rashid, Asma; & (2021). Cyber hegemony and information warfare: A case of Russia. *Liberal Arts and Social Sciences International Journal*, vol. 5(1), s. 648–666. Länk: https://doaj.org/article/dd952c544ae04884954c9007e0501128 (hämtad: 2023-01-02)
tml (2022-12-16)

Ratnam, Glopal (2021). Cleaning up SolarWinds hack may cost as much as $100 billion. *Roll Call.* 11 januari. Länk: https://rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/ (hämtad: 2022-12-18)

Reuters (2021), *SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president.* 15 februari. Länk:

https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R (hämtad: 2022-12-14)

Satter, Raphael (2021). SolarWinds says dealing with hack fallout cost at least $18 million. *Reuters.* 13 april. Länk: https://www.reuters.com/technology/solarwinds-says-dealing-with-hack-fallout-cost-least-18-million-2021-04-13/ (hämtad: 2022-12-18)

Shah, Samit (2021). *The Financial Impact of SolarWinds Breach.* BitSight. 12 januari. Länk: https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided (2022-12-28)

Tidy, Joe (2020). SolarWinds: Why the Sunburst hack is so serious. *BBC.* 16 december. Länk: https://www.bbc.com/news/technology-55321643 (hämtad: 2022-12-12)

Wheeler, Tarah (2021). The danger in calling the SolarWinds breach “an act of war”. *Brookings Institution.* 4 mars. Länk: https://www.brookings.edu/techstream/the-danger-in-calling-the-solarwinds-breach-an-act-of-war/ (hämtad: 2022-12-19)

Willett, Marcus (2021). Lessons of the SolarWinds hack. *Survival*, vol. 63(2), s. 7-26. Länk: https://www.tandfonline.com/doi/full/10.1080/00396338.2021.1906001 (hämtad: 2022-12-19)