Cyberoperationers attribution, tillvägagångssätt och sofistikation

HENRIK KARLZÉN

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se

FOI-R--4834--SE
ISSN 1650-1942

December 2019

Henrik Karlzén

Cyberoperationers attribution, tillvägagångssätt och sofistikation

Titel	Cyberoperationers attribution, tillvägagångsätt och sofistikation
Title	Cyber operations' attribution, modi operandi, and sophistication
Rapportnr/Report no	FOI-R--4834--SE
Månad/Month	December
Utgivningsår/Year	2019
Antal sidor/Pages	73
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	Informationssäkerhet
FoT-område	Operationer i cyberdomänen
Projektnr/Project no	E72787
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Bild/Cover: USA:s kongressbibliotek. Förlagan av Abraham Ortelius (1570).

Sammanfattning

Denna rapport beskriver hur cyberoperationer som rubricerats som statsstödda gått till och hur det genom attribution kan avgöras om de faktiskt var statsstödda. Dessutom beskrivs på vilka grunder cyberoperationer betraktas som sofistikerade. Eftersom det ofta sätts likhetstecken mellan statsstöd och sofistikation överlappar teknikerna för attribution till viss del med teknikerna för att ta reda på om en operation var sofistikerad. Tillsammans ger detta en grund för att identifiera vilka cyberoperationer som är av särskilt intresse för Försvarsmakten vad gäller försvar och aktiv förmåga.

Rapporten beskriver också trender för cyberoperationer, exempelvis vilka stater som ofta bedöms vara angripare och vilka som återkommer som offer. Vad gäller attributionen finns dock ofta många tillkortakommanden med långa och svaga beviskedjor där motbevis ibland till och med ignoreras. I rapporten föreslås därför att framtida forskning undersöker hur enkelt det är att bedöma attribution och huruvida angripare kan skydda sig mot attributionsteknikerna.

Operationernas tillvägagångssätt håller generellt en relativt låg sofistikationsgrad och vad som av olika tyckare framhålls som sofistikerat är sällan särskilt imponerande. Rapporten ger därför förslag på framtida forskning som utreder hur stater vill agera i cyberdomänen, bland annat med tanke på långsiktighet och målinriktning. Dessutom föreslås studier av inköp av cybervapen och vad det går att säga om de typer av cyberoperationer som inte alls upptäcks.

Nyckelord: operation, cyberoperation, cyberdomän, cybersäkerhet, informationssäkerhet, IT-säkerhet, attribution, tillvägagångssätt, sofistikation, angrepp, avancerad

Summary

This report describes how cyber operations classified as state supported take place and how it by attribution can be determined that they actually were state supported. It is also described on what basis cyber operations are considered sophisticated. Since an equal sign is often put between state support and sophistication, the techniques for attribution overlap to some part with the techniques used to find out if an operation was sophisticated. Together, this provides a basis for identifying which cyber operators that are of special interest to the Swedish Armed Forces in terms of defence and active capabilities.

The report also describes trends for cyber operations, such as which states often appear to be attackers and which recur as victims. However, the techniques for attribution have shortcomings in terms of long and weak chains of evidence where rebuttals are sometimes even ignored. The report therefore suggests that future research examines how easy it is to assess attribution and whether attackers can protect themselves from attribution techniques.

The operations' modi operandi generally holds a relatively low degree of sophistication and what is highlighted by various pundits as sophisticated is rarely impressive. The report thus provides suggestions for future research that more closely explores how states want to act in the cyber domain, including in terms of long-term goals and targeting. In addition, studies on cyber weapons procurement are proposed as well as on what can be said about the types of cyber operations that are not even discovered.

Keywords: operation, cyber operation, cyber domain, cyber security, information security, IT security, attribution, modus operandi, sophistication, attack, advanced

Innehållsförteckning

1 Inledning

Försvarsmakten har ett uttalat behov av att öka sin förmåga att utföra cyberoperationer.[1] Precis som inom andra domäner borde rimligtvis Försvarsmaktens förmåga främst vara fokuserad på operationer där stater är involverade och där tillvägagångssätten är mer sofistikerade. Denna rapport beskriver därför hur cyberoperationer som rubricerats som statsstödda gått till (*tillvägagångssätten*) och hur det genom *attribution* kan avgöras om de faktiskt var statsstödda. Dessutom beskrivs på vilka grunder cyberoperationer betraktas som *sofistikerade*. Eftersom det ofta sätts likhetstecken mellan statsstöd och sofistikation överlappar teknikerna för attribution till viss del med teknikerna för att ta reda på om en operation var sofistikerad.

Tillsammans ger rapportens tre huvuddelar (*attribution, tillvägagångssätt och sofistikation*) en grund för att identifiera vilka cyberoperationer som är av särskilt intresse för Försvarsmakten. Rapporten har tagits fram under det andra året av ett treårigt projekt inom ramen för Försvarsmaktens samlingsbeställning av forskning och teknikutveckling (FoT)[2]. Projektet utgår från sex forskningsfrågor (Karlzén och Lindahl, 2019)[3]:

1. Hur modelleras aktiv cyberförmåga?
2. Hur ska situationsuppfattning som möjliggör effektivt beslutsfattande kopplat till cyberoperationer uppnås?
3. Vad kan man förvänta sig för effekt av en typisk cyberoperation?
4. Vilka kompetenser, metoder, tekniker och verktyg krävs för att utföra cyberoperationer?
5. Hur kan tester, övningar och utbildningar nyttjas för att öka, utveckla, vidmakthålla och värdera önskade förmågor i cybermiljön?
6. Vad finns det för problematik kopplat till etik, juridik och folkrätt avseende operationer i cyberdomänen?

Rapporten fokuserar dock inte på alla dessa frågor. Baserat på studierna av *attribution*, *tillvägagångssätt och sofistikation* besvarar rapporten

[1] Detta behov har bland annat noterats av Försvarsutskottet i sitt betänkande 2014/15:FöU11 Försvarspolitisk inriktning – Sveriges försvar 2016–2020, skrivet 2015.

[2] Projektet heter Cyberoperationer. Cyberoperation definieras i denna rapport som *skeenden där antagonister med bestämt mål påverkar datorer negativt* (inspirerat av Karlzén m.fl., 2018).

[3] Forskningsfrågorna och specificerade varianter av desamma beskrivs vidare i en rapport om projektets forskningsplan (Karlzén och Lindahl, 2019).

framförallt forskningsfrågorna 1 (med avseende på hur *tillvägagångssätt* och *sofistikation* kan kategoriseras), 3 och 4. Studierna om *attribution* är vägledande i vilken evidens som finns för att operationer var statsstödda, vilket är av intresse för att avgöra operationers relevans för Försvarsmakten. Dessa studier kan också delvis besvara forskningsfråga 6 eftersom de möjliga reaktionerna på operationer beror på vem som utfört operationerna.

1.1 Läsanvisning och målgrupp

Rapporten är avsedd att läsas av den som är intresserad av cyberoperationer med statskoppling och särskilt operationernas tillvägagångssätt och hur sofistikerade tillvägagångssätten är samt hur väl det kan avgöras vem som ligger bakom operationen. Rapporten innehåller en hel del tekniska detaljer men för att förstå de vidare resonemangen krävs ingen djup teknisk förståelse.

I nästa avsnitt (1.2) beskrivs kortfattat några relevanta nedslag i vad FOI tidigare gjort på området. Därefter kommer ett metodkapitel (2) som beskriver vilka källor som valdes och hur den inhämtade litteraturen behandlades. I det följande kapitlet (3) ges några översiktliga observationer om de operationer som finns beskrivna och den databas som ligger till grund för data om operationerna och som finns beskrivna. Därpå följer kapitel om hur operationer attribueras till en viss angripare (4), vilka tillvägagångssätt som nyttjas av angriparna (5) samt hur det kan bedömas hur sofistikerad en operation var (6). Baserat på detta ges sedan några förslag på framtida forskning (7). Rapporten avslutas med referenser (8).

1.2 Tidigare FOI-arbete

Utöver forskning om allmän cybersäkerhet har FOI (och dess föregångare FOA) publicerat flera rapporter som närmare berör cyberoperationer. Dessa rapporter beskrivs kortfattat nedan indelade i attribution, tillvägagångssätt och sofistikation.

1.2.1 Attribution

Franke m.fl. (2012) beskrev hur texters författare kunde kännas igen baserat på sådant som ordval, vanliga felstavningar och social nätverksanalys för använda alias. Detta skulle kunna inspirera tekniker för attribution av cyberoperationer. Johansson m.fl. (2016) fortsatte på spåret författarigenkänning och tog bland annat upp att kombinationer av

olika särdrag kan användas tillsammans med metadata som publiceringstid för att avgöra vem som skrivit en text.

Flera rapporter berörde olika typer av samarbeten, internationella relationer och regleringar rörande cyberoperationer vilket relaterar till attribution. Karresand m.fl. (2006) studerade cyberkrig i relation till ett virtuellt rödakorsmärke. Eriksson och Fylkner (2000) studerade cyberrelaterad rustningskontroll. Fylkner m.fl. (2000a) undersökte olika organisationer och deras internationella engagemang inom cybersäkerhetsområdet. Exempelvis studerades statliga myndigheter, EU, Nato och internetorgan. Fylkner m.fl. (2000b) byggde vidare på detta och beskrev vilka delområden som lämpar sig för samarbete och hur samarbetena ska gå till.

1.2.2 Tillvägagångssätt

Grennert och Tham (2001) studerade icke-statliga aktörers (hacktivisters) utnyttjande av cyberoperationer under pågående konflikter med stater inblandade. Karresand m.fl. (2004) och Wedlin (2005) undersökte olika scenarier för cyberkrig. Karresand m.fl. (2009) studerade cyberförsvarsövningar.

Vidström (2012) beskrev en studie av industriella styrsystem som angreps i Stuxnet. Studien visade på svårigheter att förstå vad skadlig kod riktad mot industriella styrsystem gör, bland annat på grund av bristfällig dokumentation. Att förstå operationer enbart utifrån använd kod är med andra ord svårt.

Karresand (2001) och Karresand (2003) beskrev taxonomier för cybervapen, medan Lindahl m.fl. (2003) tog fram en prototyp för militära cybervapen. Holm (2018) beskrev bland annat verktyget Lore som utvecklas för att tillsammans med ramverket SVED och datorklustret CRATE möjliggöra automatisering av IT-säkerhetsövningar utan krav på specialistkompetens.

1.2.3 Sofistikation

Ånäs (2001) beskrev en kategorisering av cyberangripare, med kategorier som syfte, organisationsstorlek, kompetens och etisk begränsning. Lindahl och Westerdahl (2014) beskrev på ett liknande sätt typiska cyberangripares särtecken som att cybersoldater agerar i enlighet med en långsiktig politisk agenda och på ett välunderrättat, resursstarkt och organiserat sätt. Dessutom beskrevs cyberangrepps faser med underrättelseinhämtning, vapenutveckling och angrepp. Fylkner m.fl. (2003) beskrev svenska cybersäkerhetsexperters syn på cyberhotbilden

mot Sverige och vad som utgör kvalificerade antagonister och angrepp, vilket är snarlikt sofistikation. Fylkner m.fl. (2004) byggde vidare på detta och tog fram en modell för värdering av aktörers förmåga att genomföra kvalificerade cyberangrepp.

2 Metod

Rapportens metod kan delas in i tre delar:

1. Litteratur om specifika cyberoperationer. Denna litteratur identifierades i sin tur genom källhänvisningar i en databas över operationer. Hur databasen valdes beskrivs i avsnitt 2.1, medan avsnitt 2.2 beskriver hur databasens källor undersöktes och hur dessa källor ser ut.
2. Val av modell för cyberoperationers tillvägagångssätt, det vill säga vilken så kallad *cyber kill chain* (sv. cyberdödningskedja) som databaskällornas beskrivningar av tillvägagångssätt skulle kopplas till. Detta beskrivs i avsnitt 2.3. Litteraturen om modellerna utgörs av akademisk forskningslitteratur och dokument från cybersäkerhetsföretag.
3. Litteratur som mer allmänt behandlar cyberoperationer. Denna typ av litteratur är i huvudsak akademiska forskningsartiklar, men vissa dokument från cybersäkerhetsföretag och liknande organisationer inkluderades också (det vill säga så kallad grå litteratur). Detta beskrivs i avsnitt 2.4.

En generell anmärkning om källornas typ kan vara på sin plats. Akademiska forskningsartiklar håller en relativt hög kvalitetsnivå, men rör ganska sällan specifika genomförda operationer med någon större detaljnivå och särskilt inte sådana operationer som nyligen skett. Som komplement används därför nyhetsartiklar, rapporter från tankesmedjor och tekniska utredningar från cybersäkerhetsföretag. Dessa källor behandlar ofta ganska färska operationer. Dessutom har cybersäkerhetsföretag ofta bra inblick i operationer eftersom deras kunder blivit drabbade, även om det kan finnas begränsningar kring vad de kan beskriva utan att avslöja sina kunder. Vidare har media lättare än andra att få kontakt med konfidentiella källor inom myndigheter. Å andra sidan är nyhetsartiklar och liknande källor i lägre grad kvalitetsgranskade, varför deras tillförlitlighet kan vara låg.

2.1 Databaser med cyberoperationer

För att få en överblick över cyberoperationer och identifiera mer detaljerade källor gjordes en sökning på webben efter en lämplig databas som beskriver sådana operationer. Databasernas lämplighet baserades på en i huvudsak kvalitativ bedömning av de kriterier som beskrivs i avsnitt 2.1.1. Därefter beskriver avsnitt 2.1.2 olika databaser och ett val av databas görs med hjälp av kriterierna.

2.1.1 Kriterier för att välja databas

För att välja databas användes ett antal kriterier. Kriterierna baserades på en workshop som genomförts i projektet för att specificera vad som skulle krävas för att studera cyberoperationer i mer detalj. Här är syftet något annorlunda och kriterierna har därför anpassats något av denna rapports författare. Kriterierna för att välja databas var:

- **Fokus på operationer**
  Databasen bör vara fokuserad på operationer snarare än aktörer eller skadlig kod i allmänhet.
- **Innehåller hänvisningar till bra källor**
  Det blir enklare att hitta mer detaljerad information om operationerna. Hänvisningar ökar dessutom tillförlitligheten och kan kompensera för att databasförfattaren inte är en auktoritet.
- **Detaljrikedom**
  Detaljer om operationen kan exempelvis vara datum, tillvägagångssätt, angripare och offer.
- **Många operationer**
  Databasen bör vara så komplett som möjligt snarare än att fokusera på ett fåtal operationer.
- **Fokus på stater**
  Databasen bör vara fokuserad på operationer med statsstöd. Detta kriterium utvärderas på huruvida databasen själv bedömer om operationerna har statsstöd.
- **Tillförlitlighet baserad på författare och metodredovisning**
  Enskilda personer (hobbyister) räknas här som mindre tillförlitliga att driva databaser medan cybersäkerhetsföretag och tankesmedjor ses som mer tillförlitliga. Vad gäller metoden för sammanställning bör det framgå hur databasförfattarna gått tillväga för att ta fram databasen.

2.1.2 Databaser som valdes bland

I detta avsnitt gås kriterierna igenom ett efter ett och exkluderar databaser tills det bara finns en databas kvar som därmed väljs. Exkluderingen gjordes av rapportens författare med visst stöd av en annan forskare.

För varje databas anges ett Id som kan användas för att hitta länken till databasens webbplats. Dessa länkar anges i Tabell 1. Ju lägre Id desto tidigare exkluderades databasen (förutom för databasen med det högsta Id:et eftersom den databasen inte exkluderas).

Tabell 1: Länkar till databasernas webbplatser.

Id	Länk
1	github.com/sapphirex00/Threat-Hunting
2	aptmap.netlify.com/#
3	github.com/blackorbird/APT_REPORT
4	github.com/aptnotes/data
5	attack.mitre.org/groups/
6	apt.securelist.com/#!/threats/
7	virustotal.com/gui/
8	goo.gl/MYkxhT
9	csis.org/programs/technology-policy-program/significant-cyber-incidents
10	file.prio.no/journals/JPR/2014/51/3/Valeriano%20&%20Maness%202014%20replication%20&%20codebook.zip
11	cybercampaigns.net
12	github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections
13	github.com/fdiskyou/threat-INTel
14	securitywithoutborders.org/resources/targeted-surveillance-reports.html
15	cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/
16	hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/
17	github.com/vz-risk/VCDB
18	cfr.org/interactive/cyber-operations

2.1.2.1 Fokus på operationer

Det första kriteriet var att databasen skulle ha fokus på operationer.
Tabell 2 visar databaser som exkluderades på grund av detta kriterium.

Tabell 2: De databaser som valdes bort baserat på kriteriet *fokus på operationer*.

Id	Namn	Drivande	Operation	Kommentar
1	Threat-Hunting	Privatperson.	Nej, per aktör.	–
2	APTMAP	Privatpersoner.	Nej, per aktör.	–

Id	Namn	Drivande	Operation	Kommentar
3	APT_REPORT	Privatperson.	Nej, per aktör.	–
4	APTnotes data	Privatpersoner.	Nej, per rapport.	–
5	ATT&CK Groups	Cybersäkerhets-organisationen Mitre som sponsras av amerikanska staten.	Nej, per aktör.	–
6	Targeted Cyberattacks Logbook	Cybersäkerhets-företaget Kaspersky.	Nej, per aktör.	
7	Virustotal	Google.	Nej, per skadlig kod.	Operationsdetaljer syns inte i databasen. Dock syns den skadliga kodens nätverksanslutningar och systemförändringar beskrivs liksom vilka system den fungerar på och vilka av de vanligaste cybersäkerhetsprodukterna som kan upptäcka den.
8	APT Groups and Operations	Privatpersoner.	Nej, per aktör.	Även om aktörernas operationer och verktyg också nämns är källhänvisningarna per aktör snarare än per specifik operation.

2.1.2.2 Hänvisningar till bra källor

Det andra kriteriet var att databasen skulle ha hänvisningar till bra källor. Tabell 3 visar databaser som exkluderades på grund av detta kriterium.

Tabell 3: De databaser som valdes bort baserat på kriteriet *källhänvisningar*.

Id	Namn	Drivande	Källor	Kommentar
9	Significant Cyber Incidents	Amerikanska tankesmedjan CSIS.	Nej.	

Id	Namn	Drivande	Källor	Kommentar
10	Dyadic Cyber Incident and Dispute Data	Två forskare.	Bara vilket nyhetsmedium, utan specifik länk eller referens.	Bedömningen av om det var en stat som låg bakom operationen verifieras dock via rapporter från exempelvis cybersäkerhetsföretag.

2.1.2.3 Detaljrikedom

Det tredje kriteriet var att databasen skulle ha ordentligt med detaljer. Tabell 4 visar databaser som exkluderades på grund av detta kriterium.

Tabell 4: De databaser som valdes bort baserat på kriteriet *källhänvisningar*.

Id	Namn	Drivande	Detaljer	Kommentar
11	Cyber Campaigns	Privatperson.	Nej (länkar bara till källor).	–
12	APT & CyberCriminal Campaign Collection	Privatperson.	Enbart datum.	–
13	threat-INTel	Privatperson.	Enbart datum.	–
14	Reports on Targeted Surveillance of Civil Society	Kollektiv av hackare och säkerhetsexperter.	Enbart datum och offrets nationella tillhörighet.	–

2.1.2.4 Många operationer

Det fjärde kriteriet var att databasen skulle innehålla många operationer. Tabell 5 visar databaser som exkluderades på grund av detta kriterium.

Tabell 5: De databaser som valdes bort baserat på kriteriet *många operationer*.

Id	Namn	Drivande	Antal operationer	Kommentar
15	Relevante Cybervorfälle	En forskare.	Mycket få (exempelvis bara 4 operationer år 2017).	–

2.1.2.5 Statsfokus och allmän tillförlitlighet

Det femte kriteriet var att databasen skulle ha statsfokus och det sjätte kriteriet vara att databasen skulle vara tillförlitlig. Tabell 6 visar databaser som exkluderades på grund av dessa kriterier.

Tabell 6: De databaser som valdes bort baserat på kriterierna *statsfokus* och *tillförlitlighet*.

Id	Namn	Drivande	Statsfokus	Kommentar
16	Hackmageddon	Privatperson.	Nej, få av operationerna är statsstödda.	Bara en liten del av data rör *statsstödda* operationer vilket gör att databasen förmodligen är anpassad för andra ändamål. Att det är en privatperson som ligger bakom gör databasen mindre *tillförlitlig*. Källorna kan inte kompensera för detta eftersom det bara finns en källa per händelse och källorna är nästan alltid nyhetsmedier snarare än cybersäkerhetsföretags rapporter.
17	VERIS Community Database	Cybersäkerhetsföretaget Verizon.	Nej, få av operationerna verkar vara statsstödda.	Fokus är på hälsa och vård vilket förmodligen ger ett skevt urval. Den metod som använts för sammanställningen redovisas dessutom bara knapphändigt, vilket gör databasen mindre *tillförlitlig*.

2.1.2.6 Databasen som valdes

När alla kriterier använts återstod en databas, vilken inkluderas i Tabell 7.

Tabell 7: Databasen som valdes.

Id	Namn	Drivande	Kommentar
18	Cyber Operations Tracker	Amerikanska tankesmedjan Council on Foreign Relations (CFR).	Se nedan.

Den databas som passade bäst bedömdes vara Cyber Operations Tracker som drivs av CFR.[4] Denna databas är också den mest kompletta vad gäller statsstödda operationer enligt Romanosky och Boudreaux (2019). Det kan nämnas att många av de olika databaserna (delvis) baseras på varandra och det gäller även denna databas, som delvis baseras på databaserna med Id 6, 8 och 9.

Databasens författare medger att den har följande brister (CFR, 2019):

- Evidensen för att operationerna faktiskt utförs med statsstöd är ofta svag.
- Källorna är mestadels engelskspråkiga, vilket bland annat gör att engelskspråkiga länder som drabbas syns mer.
- Databasen baseras enbart på öppna källor och andra källor kan vara mer kompletta.[5]
- Eftersom mer information om operationer framkommer över tid, är databasen inte komplett och den kan i vissa delar vara knapphändig. Uppdateringar och ändringar av databasen görs varje kvartal.

Det är denna författares uppfattning att databasen förmodligen har dessa brister gemensamt med de andra nämnda databaserna.

Databasen beskrivs i mer detalj i kapitel 3.

[4] Databasen kommer i resterande rapporten att kallas för CFR-databasen (eller bara CFR).

[5] Det är rimligt att anta att vissa operationer är för svåra att upptäcka, åtminstone för de som öppet rapporter om operationer. Detta ger ett mörkertal och det verkar rimligt att det är just de svårupptäckta operationerna som har högst teknisk verkshöjd, som kan ge störst effekter och som har störst statligt stöd.

2.2 Läsning av CFR-källorna

För varje operation har CFR-databasen en till tre länkar till de källor (webbplatser) som legat till grund för databasens data om operationen och där mer information kan hittas. I medeltal har en operationer drygt två källor. Det kan vara på sin plats att göra några allmänna observationer om databasens källor (som helt och hållet är öppna):

- *Nyhetsartiklar* utgör drygt hälften av källorna. De mest återkommande medierna är i fallande ordning New York Times, Washington Post, Reuters, Wired, Wall Street Journal, BBC, Ars Technica, Bloomberg, The Guardian, Register och Scoop News. Tillsammans står de för över hälften av nyhetsartiklarna.
- *Cybersäkerhetsföretags rapporter* utgör drygt en tredjedel av källorna. De vanligaste källorna bland cybersäkerhetsföretagen är i fallande ordning Kaspersky, FireEye, Symantec och Palo Alto Networks. Tillsammans står dessa företag för ungefär hälften av cybersäkerhetsrapporterna.
- *Myndigheters rapporter* står för sju procent av källorna och majoriteten av myndighetsrapporterna är amerikanska.
- *Övriga källor* är bland annat dokument från tankesmedjor, forskningsorganisationer och frihetsfrämjande organisationer samt andra databaser. Dessutom tar CFR emot tips som sedan undersöks vidare.

För att få en hanterlig, men ändå relevant mängd källor att gå igenom, valdes enbart operationer från år 2017 ut.[6] Årtalet valdes av rapportens författare tillsammans med en annan forskare och baserades på att årtalet skulle vara någorlunda färskt, men också moget nog. Å andra sidan skulle 2018 års operationer inte upptäckts och slutanalyserats än i samma utsträckning.

Källorna lästes igenom av rapportens författare och en annan forskare och relevant information för attribution eller tillvägagångssätt noterades. Olika typer av utsagor om attribution delades in i kategorier som denna rapports författare såg som lämpliga, medan utsagor om tillvägagångssätt

[6] Databasen uppdateras varje kvartal och även tidigare kvartal (och år) kan då också ändras. Den bild denna rapport ger av 2017 års operationer speglar vad CFR-databasen innehöll 15 februari 2019. Detta motsvarar 45 operationer och 25 november 2019 innehöll databasen samma operationer för 2019 även om det inte kontrollerats att alla detaljer är desamma.

delades in i olika steg enligt Lockheed Martins modell Cyber Kill Chain (LMCKC), vilken beskrivs närmare i nästa avsnitt.

2.3 Val av cyber kill chain

Cyberoperationers tillvägagångssätt kan modelleras på olika sätt, bland annat med så kallade cyber kill chains (sv. cyberdödarkedjor). Det finns flera sådana kedjemodeller, men den mest vedertagna är Lockheed Martins Cyber Kill Chain (LMCKC). Av detta skäl valdes LMCKC som består av de sju stegen *rekognoscering*, *vapentillverkning*, *leverans* (av vapnet), *utnyttjande* (av sårbarhet), *installation*, *ledning* (eng. command and control) och *agerande* (för att uppnå målet). Valet gjordes av denna rapports författare tillsammans med en annan forskare.

Det kan vara på sin plats att även beskriva kritik mot, och alternativ till, LMCKC eftersom det kan visa på dess begränsningar. Framförallt rör det sig om hur många steg som behövs och vad som ska ligga i respektive steg. I de två följande avsnitten beskrivs modeller som jämfört med LMCKC har färre steg (avsnitt 2.3.1) och fler eller alternativa steg (avsnitt 2.3.2).

2.3.1 Färre steg

Vissa steg i LMCKC sker ofta snabbare än andra steg. De två sista stegen (*ledning* och *agerande*) utgör till exempel ofta den största och långsammaste delen (Zeng och Germanos, 2019). Cho m.fl. (2018) föreslog en variant där stegen *utnyttjande* och *installation* lades ihop eftersom dessa steg sker så snabbt. Amerikanska försvarsdepartementet lade också ihop dessa steg plus *leverans* i sitt få-tillgång-steg (eng. gain access) (United States Department of Defense, 2018).

2.3.2 Fler steg eller alternativa steg

Jämfört med LMCKC lägger flera modeller till (uttryckliga) steg för hur angripare tar sig vidare i systemet. Det kan göra att stegen i LMCKC upprepas, exempelvis så att det inledande steget för *rekognosering* sker igen när angriparen kommit in i systemet (som i Hewlett Packard Enterprise, 2014; Malone, 2016), eller rentav kontinuerligt (som i United States Department of Defense, 2018). Upprepningar av stegen *utnyttjande*, *vapentillverkning* och *installation* görs också i en modell av Malone (2016). Förutom upprepningar finns ibland steg för privilegieeskalering (eng. privilege escalation) (Malone, 2016; United States Department of Defense, 2018; Mitre, 2019d) och vidare rörelser i nätverket (eng. lateral movement) (Zeng och Germanos, 2019; Hewlett

Packard Enterprise, 2014; Malone, 2016; Mitre, 2019d; United States Department of Defense, 2018).

Ett annat vanligt tillägg är ett steg för ihärdighet (eng. persistence) (Zeng och Germanos, 2019; Hewlett Packard Enterprise, 2014; United States Department of Defense, 2018; Mitre, 2019a) vilket i LMCKC ingår i *installation*.

LMCKC:s sista steg *agerande* delas ibland upp i flera steg (Hewlett Packard Enterprise, 2014; Malone, 2016) såsom inhämtning och exfiltrering (att föra ut data) (United States Department of Defense, 2018; Mitre, 2019a).

2.4 Forskningsartiklar och grå litteratur

Relevanta forskningsartiklar om attribution, cyber kill chain och sofistikation identifierades genom sökningar med den akademiska sökmotorn Google Scholar[7] och i databasen Scopus[8]. Särskild vikt lades vid högciterade artiklar. Söksträngarna utgjordes i huvudsak av de engelska termerna *attribution*, *cyber kill chain* och *sophistication* samt synonymer till desamma, i olika kombinationer med ord som *cyber*, *attack*, *threat*, *weapon* och *military*.

När särskilt intressanta forskningsartiklar identifierades gjordes nya sökningar efter andra dokument som citerar de intressanta artiklarna och därmed bygger vidare på dem. Förutom att andra citerar artiklarna bygger artiklarna själva på andras arbete, det vill säga artiklarnas referenser. Artiklars intressanta referenser undersöktes också. Litteratursökningen avslutades när nya artiklar inte längre tillförde någon ny relevant kunskap.

Förutom sökningarna med Google Scholar och i Scopus, gjordes också sökningar med vanliga Google för att hitta relevanta dokument skrivna av cybersäkerhetsföretag och liknande organisationer. Sådana dokument som liknar forskningsartiklar, men inte är på akademisk nivå, benämns ofta grå litteratur.[9]

Både när det gäller Google Scholar och vanliga Google anpassades resultaten efter denna rapports författares sökhistorik (och kanske övriga

[7] Scholar.google.se

[8] Scopus.com

[9] I grå litteratur ingår också utkast till forskningsartiklar.

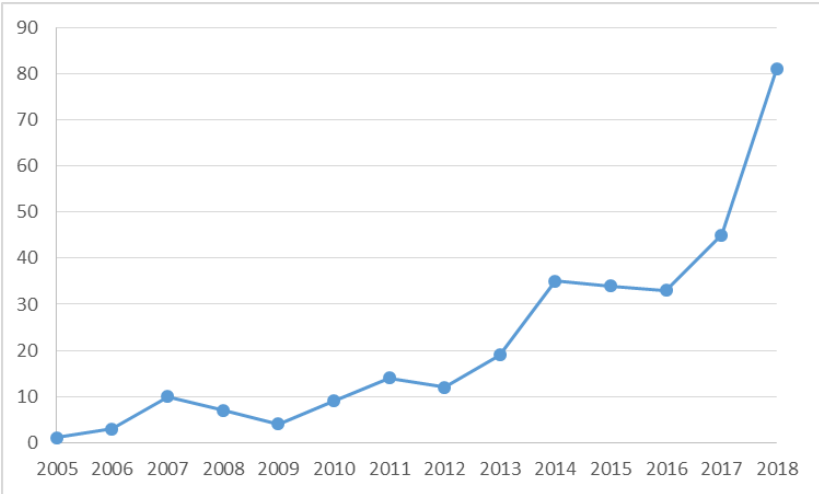
FOI:s sökhistorik). Det kan ha gett en vinkling i vilka dokument som hittades. Å andra sidan motsvarar detta författarens bedömning av vilka av hittade dokument som är intressanta.

De olika dokumenten lästes igenom och relevanta utsagor extraherades. Utsagorna kategoriserades enligt vad denna rapports författare såg som en rimlig indelning och på ett sätt som gav ett komplement till utsagorna från CFR-källorna. Kategoriseringen anpassades efter hand när materialet växte fram och med tanke på vilka liknande indelningar som gjorts i litteraturen.

Det är dock troligt att andra författare (bedömare) hade gett upphov till (delvis) andra kategoriseringar. I huvudsak är dock kategoriseringarna till för att redovisa forskningsområdet på ett pedagogiskt sätt snarare än att ge någon form av kvalitativ bedömning av litteraturen. Även med en annan indelning skulle resultatet som helhet alltså bli likartat.

3 Cyberoperationsdatabasen

CFR-databasen beskriver 307 statsstödda cyberoperationer genom åren (2005–2018).[10] Hur antalet operationer varierat över åren visas i Figur 1.



Figur 1: Varje års antal operationer som redovisas i CFR-databasen.

I databasen definieras operationer bara informellt som *avgränsade händelser i vilka hotaktörer negativt påverkar (komprometterar) datornätverk*. I Tabell 8 anges vilka variabler (kolumner) databasen har och för varje variabel anges också i de flesta fall vilka av de följande avsnitten som tar upp mer om den. Variablerna som rör databasens källor har redan behandlats i avsnitt 2.2. För några variabler ges ingen vidare beskrivning i rapporten (markerade med – i kolumn två i tabellen).

[10] Senare år inkluderas inte här eftersom 2019 inte löpt ut än och det dessutom finns viss eftersläpning med rapporteringen.

Tabell 8: CFR-databasens variabler och var i rapporten det går att läsa mer om dem.

Variabel	Avsnitt att läsa mer
Titel	3.3
Datum	3
Hackergrupp operationen kopplats till (eng. affiliation)	(–)
Beskrivning i löptext	(–)
Offrets svar (plus källa för svaret)	3.4
Sponsor (angripare)	3.2
Typ av operation	3.3
Typ av offer	3.1
Offer	3.1
Källa 1	2.2
Källa 2	2.2
Källa 3	2.2

Ett (fritt översatt) exempel på vilken information som ges om en operation i databasen visas i Figur 2. Notera att vissa kolumner inte innehöll någon data för denna operation varför de kolumnerna inte syns här.

Titel	Datum	Beskrivning
Komprommetering av Nordkoreanska kärnvapenprogrammet.	2017-03-04	En hotaktör, som tros vara USA, riktade in sig på datornätverk och elektroniska komponenter associerade med Nordkoreanska kärnvapenprogrammet för att sabotera och försena dess utveckling.

Sponsor	Typ av operation	Typ av offer	Offer	Källa 1
USA	Sabotage	Militär	Nordkorea	nytimes.com/…

Figur 2: Exempel på en operation i CFR-databasen. För att ta mindre plats i sidled har operationen inte beskrivits på en enda rad och källa 1 har kortats ner.

3.1 Offer

Hälften av operationerna har bara ett offer. Den andra hälften är ganska jämnt fördelat över 2–15 offer, plus ett fåtal operationer med upp till 27 offer. Som offer förekommer både länder, enskilda statliga departement eller myndigheter, företag och andra organisationer. I databasen delas offren in i fyra kategorier. Den vanligaste kategorin är civila myndigheter (offer 159 gånger), följt av privat sektor (151), civilsamhälle (54) och militär (49).

Det klart vanligaste offret i absoluta tal är USA (i 24 % av operationerna). Många andra länder (22) har varit offer 10–36 gånger. De vanligaste offren per capita är i fallande ordning Kiribati (offer 8,6 gånger per en miljon invånare[11]), Barbados (3,5), Montenegro (3,2), Brunei (2,3), Israel (2,1), Surinam (1,7), Luxemburg (1,7), Qatar (1,4), Hongkong[12] (1,4), Schweiz (1,3). Per capita är Sverige det 24:e vanligaste offret (0,7) och USA det 61:a (0,2).

3.2 Angripare (sponsorer)

Kina är det land som sägs ligga bakom klart flest operationer över tid (111 operationer, varav 20 under 2018) och har varit verksamt under en längre tid. Ryssland har dock snabbt vuxit fram de senaste åren och är för 2018 den största sponsorn (26 operationer). De andra vanligaste sponsorerna är Iran (29 operationer totalt, varav 5 under 2018) och Nordkorea (25 totalt, varav 9 under 2018), USA (10 totalt, 0 under 2018) och Israel (6 totalt, 0 totalt). Sverige syns inte som sponsor för någon operation.

De vanligaste sponsorerna per capita är i fallande ordning Nordkorea (sponsor 1,0 gånger per miljon invånare), Israel (0,7), Ryssland (0,5), Iran (0,4), Panama (0,2) och Förenade Arabemiraten (0,2).

Generellt ligger bara ett land i taget bakom operationerna men det finns ett fåtal undantag där samarbete verkar ha skett mellan USA och Israel (2 gånger), USA och Storbritannien (1 gång), USA och Taiwan[13] (1 gång) samt Kina och Ryssland (1 gång).

[11] Enligt 2018 års siffror i Förenade Nationerna (2019).

[12] Hongkong står med bland länder här men utgör en särskild administrativ region inom Kina (Utrikespolitiska institutet, 2019).

[13] Taiwan står med bland länder här och fungerar i praktiken ”som en självständig stat även om det bara erkänns av ett fåtal andra länder” (Utrikespolitiska institutet, 2019).

3.3 Effekter, evidens och omfång

De allra flesta operationer utgör underrättelseinhämtning (som påverkar informationens konfidentialitet; 250 operationer) med ett betydligt lägre antal operationer som på andra sätt förstör för offret: tillgänglighetsangrepp (DoS) 16 operationer, sabotage 16, datadestruktion 7, doxing[14] 6, defacement[15] 3.

Titlarna som ges för operationerna indikerar att databasen i en liten del av fallen försöker beskriva evidensen för att operationen har skett, exempelvis *anklagas* (4 fall) eller *sägs ha* (1). Titlarna beskriver också ibland vilken framgång angriparen hade med ord som *försökte* (7 fall), *riktade* (43) *angrep* (3) och *kompromitterade* (94). Titlarna beskriver också i vissa fall omfånget, det vill säga om det exempelvis rörde sig om en *incident* (5 fall), *intrång* (2), *operation* (7) eller *kampanj* (3).

3.4 Offrets svar

Databasen beskriver i vissa fall om offret eller offren svarat på angreppet. Sådana svar är oftast i form av *fördömanden* (efter 41 operationer) men det är inte heller ovanligt med *åtal* (efter 15 operationer). Även *sanktioner* (efter 5 operationer) förekommer. I ett (1) fall beskrivs att offret *förnekade* att det blivit angripet och i ett (1) annat fall att offret istället *bekräftade*. Inga svar med samma mynt syns uttryckligen och det gör inte heller väpnade svar i andra domäner än cyber.

[14] Vid doxing samlar angriparen in känsliga dokument och publicerar offentligt för att till exempel förödmjuka offret.

[15] Vid defacement hackar angriparen en hemsida och byter ut den mot angriparens eget budskap.

4 Attribution

Det är rimligt att anta att de allra flesta vill vara anonyma när de utför cyberoperationer. Det är också rimligt att anta att det vore nyttigt för offer och andra att trots det avslöja angriparen. I detta kapitel undersöks därför attribution[16] – det vill säga fastställandet av vem som utfört en operation.

Att attribuera cyberoperationer är i dagsläget svårt, långsamt och saknar skalbarhet (Keromytis, 2016) även om Bartholomew och Guerrero-Saade (2016) hävdar att svårigheterna ofta uppförstoras av media i försök att rapportera balanserat. Å andra sidan bör det beaktas att det även för icke-skadlig kod (i legitim mjukvara) kan vara svårt att veta vem som tillverkat de olika delarna. Att attribuera kräver i många fall veckor eller månader av analysarbete (ODNI, 2018).

Det finns flera anledningar till att vilja attribuera cyberangrepp. Först och främst vill offret (eller någon annan) förmodligen förändra sin relation med den som angripit, exempelvis genom sanktioner (Davis m.fl., 2017) eller genom att slå tillbaka (Nicholson m.fl., 2015). Förmodligen är detta viktigare om angriparen är någon som inte förväntades agera på ett sådant sätt (exempelvis om avtal har ingåtts om fred i cyberrymden (Porter, 2017)), eller när relationen redan är svag. Att attribuera angrepp kan göra att angriparen av liknande skäl avskräcks till att fortsätta pågående angrepp eller påbörjandet av nya angrepp (Nicholson m.fl., 2015; Davis m.fl., 2017; Floyd, 2018).

En annan anledning att attribuera är att avgöra vems ansvar det är att hantera angreppets följder eller vem som skulle se till att det inte skedde. Det kan till exempel spela roll för försäkringsbolags skyldighet att betala de försäkrade (offren) huruvida ett cyberangrepp utfördes av en stat eller ej. Det pågår en rättstvist i miljardklassen mellan ett försäkringsbolag och ett av offren för NotPetya, där offret hävdar att försäkringsbolaget nekat utbetalning och hänvisat till statsinblandning som orsak, medan offret anser att försäkringsbolaget har bevisbördan för statsinblandningen (Illinois, 2018). Ett annat exempel är att tillverkare och försäljare av cybervapen kanske bara får beväpna vissa organisationer och kan ha ett ansvar att vapnen inte sprids, något som är svårt att kontrollera (Ahmed och Perlroth, 2019).

[16] På svenska används ibland begreppet ”hänförbarhet” eller ”att hänföra”, se exempelvis Zouave (2019) och SOU 2011:76 (2011). Dessutom används ibland ”utpekande” eller ”att utpeka”, men det fungerar bara när ens åsikt offentliggörs. I denna rapport används istället ”attribution” och ”att attribuera” vilket ligger närmare de begrepp som används i den huvudsakligt engelskspråkiga litteraturen.

En tredje anledning till att attribuera cyberangrepp är att få bättre förståelse för hoten och därmed ett bättre försvar (Davis m.fl., 2017) (Nicholson m.fl., 2015). Ytterligare en anledning till att attribuera, som framförallt gäller cybersäkerhetsföretag, är marknadsföringsskäl (Davis m.fl., 2017).

I nästa avsnitt presenteras olika indikatorer för attribution (4.1) vilket utgör huvuddelen av kapitlet. Därefter kommer ett avsnitt (4.2) om indikatorernas användning som tar upp huruvida offentligt utpekande är nyttigt, vilken nivå av bevisföring som krävs samt vilka svagheter som finns med indikatorerna och hur de ska vägas samman.

4.1 Indikatorer för attribution

I detta avsnitt beskrivs hur forskningslitteraturen och källorna till CFR:s cyberoperationsdatabas (för operationer som utfördes 2017) attribuerar cyberoperationer. Detta innebär att analysen grundar sig i teori (forskningslitteratur) och kontrollerar hur väl teorin fungerar i praktiken (CFR-källorna). De olika sätten (fortsättningsvis benämnda indikatorer) från forskningslitteraturen matchas mot indikatorerna från databasens källor, när så är möjligt. Indikatorerna från forskningslitteraturen är beskrivna på en ganska generell nivå, medan indikatorerna från databaskällorna är mer exemplifierande. Attribution handlar ofta om att ta reda på om en operation var statsstödd och sofistikation ses ofta som ett tecken på att en operation var statsstödd. Av dessa skäl finns visst överlapp mellan indikatorerna för attribution och indikatorerna på sofistikation (vilka beskrivs i avsnitt 6.1).

I de följande avsnitten beskrivs hur indikatorerna delats in i kategorier (4.1.1), vilka generella tillkortakommanden och typiska mätproblem som finns för indikatorerna (4.1.2) och till sist själva indikatorerna och mer specifika problem (4.1.3).

4.1.1 Indikatorkategorier

Indikatorerna delas in i kategorier som valdes efter vad denna rapports författare tyckte verkade lämpliga. Lämpligheten baserades i huvudsak på att kategorierna skulle dela in data i hanterbara delmängder och samtidigt skilja sig åt någorlunda väl. Följande kategorier valdes:

- **Matchande mål**
  Olika operationer kan exempelvis ha mål med liknande effekt och mål som verkar stämma med vad en viss nation vill har utfört.

- **Språk som använts**
  Vilket (naturligt) språk en operation utförs på kan visa sig på sådant som artefakter i kod och i metadata.
- **Angriparens arbetstid**
  Beroende på tidsstämplar i kod och nätverkstrafik avslöjas troliga arbetstider och tidszoner.
- **Domäner och IP-adresser**
  Operationerna kan spåras till IP-adresser och ledas från olika domäner.
- **Resurser**
  En del operationer tar större resurser i anspråk såsom mer bandbredd, mer metodik och bättre möjligheter till testning på förhand.
- **Taktiker, tekniker och procedurer (TTP)**
  Hur skadlig kod ser ut, vilka sårbarheter som utnyttjas och hur angriparen döljer sitt agerande är exempel på sådant som rör operationens TTP.
- **Uttalanden och motaktioner**
  Vissa operationer leder till uttalanden om skuld och motaktioner vilket kan visa vem som låg bakom operationen.

I forskningslitteraturen har flera andra kategoriseringar föreslagits, exempelvis:

- Wheeler m.fl. (2003) ger en taxonomi med attributionskategorier, men tar i stort sett bara upp indikatorer som kommer till på grund av nätverkskommunikation, vilket är smalare än denna rapports omfång. Dessutom är taxonomin tänkt att användas för att göra om system så att de blir mer anpassade för att lättare attribuera angrepp, snarare än vilka indikatorer som kan användas i dagsläget.
- Cook m.fl. (2016) delar bland annat in indikatorerna efter huruvida de rör nätverkskommunikation, forensisk analys av datorn, analys av den skadliga koden eller icke-tekniska metoder (underrättelselett). Med andra ord är indelningen mer till för mätmetoder för indikatorerna snarare än indikatorerna själva.
- Rid och Buchanan (2015) redovisar en ostrukturerad metod som tar upp frågor vars svar kan sägas utgöra indikatorer. Indikatorerna är exempelvis vad målet var och hur riktad operationen var, vilket språk som användes, vilken tid den skadliga koden kompilerades, vilken teknisk infrastruktur som användes, hur svårt det var, vilka resurser som krävdes och hur angriparen verkar ha varit organiserad. Dessa indikatorer passar väl in i de kategorier av indikatorer som används i denna rapport. Artikeln tog dock som helhet upp över hundra indikatorer, indelade i över trettio kategorier. I denna FOI-rapport

valdes istället en mer strukturerad och mer hanterlig mängd kategorier, som samtidigt täcker in samtliga indikatorer från artikeln.

Det kan också nämnas att amerikanska underrättelsetjänst (ODNI, 2018) använder kategorierna återkommande tillvägagångssätt, infrastruktur, skadlig kod, motivation och indikatorer från externa källor. En viktig del enligt samma källa är att leta efter misstag angriparna gjort.

4.1.2 Generella problem med indikatorerna

Att hitta en korrekt och fullständig uppsättning indikatorer är en utmaning och indikatorerna måste dessutom vara möjliga att använda i praktiken (mätbara). Generella tillkortakommanden för indikatorerna och typiska mätproblem beskrivs därför nedan. I avsnitt 4.1.3 beskrivs sedan för varje indikatorkategori vilka problem litteraturen eller denna rapports författare sett.

För det första räcker det förmodligen inte med en enskild indikator. Att exempelvis koppla operationen till en viss tidszon är otillräckligt om tidszonen omfattar flera länder. Att bedöma hur riktad en operation var baserat på vad den slog mot är ofullständigt om operationen egentligen kan ha varit avsedd att slå mot fler eller färre (eller andra) mål. Att en operation inte krävde stora resurser kan på liknande sätt bara ge insikt i angriparens minsta mängd resurser.

För det andra kan det vara svårt att mäta en del av indikatorerna. Exempelvis kanske det inte är möjligt att analysera systemförändringar eller den skadliga koden, på grund av att systemet inte sparade loggar, eller att koden var för svår att förstå. En annan möjlighet är att ens möjligheter till mätningar utanför cyberdomänen (vilket föreslås i Wheeler m.fl., 2003; Cook m.fl., 2016) är begränsade, exempelvis för att tillstånd till husrannsakan inte fås (Romanosky och Boudreaux, 2019) eller att det är oklart till vilken grad det går att lita på relevanta uttalanden som sker.

För det tredje kan angriparna bli varse om vilka indikatorer som används och därför ändra sitt beteende för att göra indikatorerna svårmätta eller rentav irrelevanta. Angripare lägger ner mycket kraft på att förhindra attribution (Boot, 2019). De kan exempelvis göra koden svårare att inspektera eller köra. I det kända fallet Stuxnet har det uppskattats att mer än hälften av vapnets utvecklingskostnader gick till att dölja angreppet (Langner, 2013). Stuxnet kan dock vara ett specialfall. Det har föreslagits att det var USA som låg bakom Stuxnet och att USA agerar mer dolt än andra stater (Romanosky och Boudreaux, 2019). I vissa fall kan motverkandet av attribution vara huvudsyftet och då att en stat angriper för att få det att se ut som att en andra stat är angripen av en tredje

(snarare än den första) (Wheeler m.fl., 2003). Att angriparen luras att den är någon annan kan exempelvis ta sig uttryck i att angriparen ställer om sin dators klocka för att arbetstiden ska se ut att stämma med en annan tidszon.

Det bör dock noteras att angriparen i vissa fall faktiskt inte vill vara anonym, varför attributionen kan vara mer rättfram. Exempelvis kan en angripare vilja göra anspråk på (eng. claim) ett angrepp (Davis m.fl., 2017). Anledningen till det kan i sin tur vara att vilja visa sin förmåga (Floyd, 2018). Det har exempelvis spekulerats att den som låg bakom Stuxnet-operationen efter ett tag närmast ville bli upptäckt för att bli först med dylik cyberoperation lite som i rymdkapplöpningen (Langner, 2013). Kearns (2019) kom fram till att för terroristattentat är sannolikheten för anspråkstagande högre när:

- Målet är militärt – kanske för att militära mål ses som mer acceptabla, vilket gör sannolikheten för badwill lägre.
- Angreppet är mer spektakulärt eller ovanligt – inklusive vid fler dödade, förutom när antalet döda var extremt, vilket spekulerades kunde göra angriparen försiktigare.
- När många andra grupper annars kan göra sig ett namn genom att ta anspråk.

Det bör dock noteras att terrorattentat inte nödvändigtvis har så mycket gemensamt med (statliga) cyberoperationer och att vissa personer och grupper kan vilja ta åt sig äran för en operation trots att de faktiskt inte utförde den, vilket kan förvirra attributionsförsöken.

4.1.3 Indikatorerna

I Tabell 10 beskrivs indikatorerna för attribution som identifierats i forskningslitteraturen och i CFR-källorna. Indikatorerna är indelade i kategorierna som beskrevs i avsnitt 4.1.1. I slutet av varje kategori finns identifierade problem med kategorierna.

För att kortare kunna referera till forskningslitteraturen ges först varje referens ett kortnamn (bokstäver), vilket återges i Tabell 9.

Tabell 9: Referenser (källor) och vilken bokstav som används för att referera till dem.

Bokstav	Referens
a	Healey, citerad av Jolley (2017)
b	Ottis, 2009
c	Lin, 2016
d	Rid och Buchanan, 2015

Bokstav	Referens
e	Rosenbaum, 2012
f	Bartholomew och Guerrero-Saade, 2016
g	Fagerland och Grange, 2014
h	Cook m.fl., 2016
i	Mateski m.fl., 2012
j	Boot, 2019
k	Langner, 2013
l	Nicholson m.fl., 2015
m	Caliskan m.fl., 2018

Tabell 10: Indikatorer för attribution indelade i kategorier samt problem med indikatorerna.

Indikatorer för attribution	
Matchande mål	
Forskningen	**CFR-källorna**
Matchande doktrin, policy och politiskt klimat.[a]	Offret var ”ryskfientligt” (ThreatConnect, 2017a).
	Offret var en industri som Iran visat intresse för (O'Leary m.fl., 2017).
	Offrets politiska motståndare stöddes av Ryssland (Seibt, 2017).
	I linje med nationella intressen (O'Leary m.fl., 2017).
	Normala mål för Kina (PWC, 2017).
	Offer som tidigare angripits av en viss hackergrupp (Great, 2017a).
	Iran har ofta gett sig på denna typ av mål (kritisk infrastruktur) (Newman, 2017).
Vilken typ av effekt som uppnås.[b,d]	

Sammanfaller med traditionella militära operationer.[a, b, d]	
Riktat eller oriktat samt mängd sidoskada.[a, b, d, e]	
Problem med ovan indikatorer	
Att komma fram till vem som har matchande doktrin, policy eller politiskt klimat är förmodligen svårt. Ofta finns många som har liknande mål. Politiken är komplicerad och förmodligen vill stater göra allt för att få fördelar även om de är mer försiktiga mot sina allierade. Att gå på vilken effekt som uppnås är av likartade skäl troligen svårt. Vissa aktörer kanske bara vill uppnå vissa typer av effekter, men när det gäller stater som aktörer har de förmodligen en bred front.	
Det är nog svårt att se samband med annat eftersom så mycket händer hela tiden och allt fler aktörer har möjlighet att agera på fler platser med olika former av exempelvis traditionella kinetiska operationer. Att CFR inte har specifika exempel på dessa typer av korskopplingar talar ju också för att det är svårt att hitta kopplingarna.	
Det är ofta svårt att veta hur riktad en operation var tänkt att vara och eftersom offer sällan delar data med varandra är det dessutom svårt att veta hur riktat en operation slog.	
Språk som använts	
Forskningen	**CFR-källorna**
Verktyg innehållande text på nationellt (naturligt) språk.[a, d]	Kod som innehåller artefakter skrivna på Farsi (O'Leary m.fl., 2017).
	Användning av kinesiska tecken (Secureworks, 2017).
Språkkunskaper.[f]	Engelskan som användes var antingen infantil, skriven av någon med ett annat modersmål eller skriven med brittisk dialekt (Great, 2017a).
Systemspråk.[d]	Dokument skrivna med saudisk tangentbordsinställning (Reaqta, 2017).
	Metadata pekar på ukrainsk text, men texten är på ryska (Atch och Neray, 2017).
Problem med ovan indikatorer	

Angripare kan medvetet försöka luras genom att lägga in text på olika språk[f, j] eller genom att ställa om sina systems språkinställningar (Pahi och Skopik, 2019; Burgess, 2017).	
Det finns många dialekter av språk, vilket kan förvirra analytiker (även om det också kan göra en språkanalys exaktare).	
Angriparens arbetstid	
Forskningen	**CFR-källorna**
Arbetstider ger trolig tidszon.[d, f, g]	Minskad angreppsaktivitet på nationella helgdagar (Secureworks, 2017).
	Sammanföll med (den ovanliga) iranska arbetsveckan (O'Leary m.fl., 2017).
Tidpunkter för kompilering.[d]	Kompilering oftast på kinesisk arbetstid (PWC, 2017).
När angreppet skedde.[d]	
Problem med ovan indikatorer	
Tidsstämplar kan förfalskas.[g, j]	
Angriparna kan arbeta vid ovanliga arbetstider. En vanlig (vuxen) anställd kanske mest arbetar vid vanlig arbetstid medan tonårshackare kanske hellre är verksamma kvällstid. I sådana fall behöver analytikern veta åldern på den som ligger bakom operationen för att kunna göra en korrekt bedömning. Tidszoner omfattar dessutom ofta många länder vilket gör det svårt att exempelvis skilja på arbete utfört i Moskva (Ryssland) och Riyadh (Saudiarabien).	
Det är förmodligen ofta svårt att veta vid vilken tid en operation skedde, vilket kan förklara varför exempel på angreppstid saknas i CFR.	
Domäner och IP-adresser[17]	
Forskningen	**CFR-källorna**
Domän.[h]	Spoofad domän (ThreatConnect, 2017b).

[17] Att gå baklänges i angreppsvägen tillbaka till angriparen kallas ofta bakåtspårning (eng. traceback) (Cook m.fl., 2016; Wheeler m.fl., 2003).

	Använde länkar via legitima webbplatser för att lura nätfiskefilter (ThreatConnect, 2017a).
	Iranska DNS-servrar (O'Leary m.fl., 2017).
IP-address.[a, i, j]	IP-adresser tillhörande Sydsudan och Kongo-Kinshasa (Great, 2017a).
	Iranska IP-adresser (Newman, 2017).
	Vissa ledningsdomäner (C2) har IP-adresser närliggande de som använts i en tidigare operation (PWC, 2017).
	Ledningsinfrastruktur (C2) använde samma IP-adresser som en tidigare operation (Symantec, 2017a).
	IP-adress spårad till Teheran (Reaqta, 2017).
	Använde normalt proxy, men anslöt ibland (troligtvis av misstag) direkt och då från ett visst kinesiskt närverk (Hegel, 2018).
	Anslöt normalt via satellit, men när länken gick ner anslöts istället via ett etiopiskt nätverk (Marczak m.fl., 2017).
Problem med ovan indikatorer	
Domäner kan enkelt registreras i någon annans namn.	
IP-adresser kan ofta förfalskas eller döljas genom en proxy (Nicholson m.fl., 2015; Pahi och Skopik, 2019). Det är förmodligen också svårt att veta om angriparens riktiga IP-adress används eller om angriparen vill få det att verka som att plötsligt agerande utan proxy till följd av ett misstag (som avslöjar angriparens IP-adress) när det i själva verket är en vilseledande manöver.	
Resurser	
Forskningen	**CFR-källorna**

Resurer i allmänhet.[d]	Förmåga (Atch och Neray, 2017).
Metodik.[b]	
Styrning.[d]	
Organisering i delar.[d]	Flera lag som samarbetade (Hegel, 2018).
	Flera lag (PWC, 2017).
Bättre underrättelser.[d, k]	
Testmöjligheter, exempelvis med kopior av stora system.[k]	
Bandbredd.[h]	
Antal steg.[d, i, l]	
Antal misstag.[d]	
Problem med ovan indikatorer	
Vilka resurser som krävs varierar mycket mellan operationer och ofta kan en typ av resurs ersätta en annan.	
Det är nog svårt att veta vad som är misstag och vad som istället är vilseledning.	

Taktiker, tekniker och procedurer (TTP)	
Forskningen	**CFR-källorna**
Tekniker och infrastrukturer som används i visst land.[j]	Samma taktik (Seibt, 2017; Marczak m.fl., 2017).
Hur mjukvaran införskaffats.[h]	Verktyg baserade på öppen källkod (Lancaster, 2017).
	Iranska verktyg (O'Leary m.fl., 2017).
	Verktyget hade köpts in och vilka som fått demonstration av det avslöjades av publika loggfiler (Marczak m.fl., 2017).
Tidsstämpelformatering.[j]	
Användarnamn och namnval.[d, f]	Namn återkommer i kod och dylikt (Symantec, 2017a; O'Leary m.fl., 2017).
Programmeringsspråk.[j]	
Kompilator.[j]	

Programmerarstil.[j, l, m]	
Kodblock.[j]	Verktyg ofta använt av Iran (Newman, 2017).
Likheter av binärkod konverterad till bilder.[j]	
Heltalstyper som används.[j]	
Sårbarhet som utnyttjas.[d]	
	Liknande kod (Symantec, 2017a).
	Tidigare versioner av verktygen väldigt lika de som använts i andra operationer (Symantec, 2017a).
Anti-attribution-metoder.[d, j]	Liknande kodobfuskering (Symantec, 2017a).
Preferens för en viss typ av krypteringsmekanism.[j]	Samma krypteringsmekanism som tidigare operationer (Hegel, 2018).
Samma lösenord som använts för att dölja kod som i andra operationer.[j]	
Funktionsanrop och funktionslängd.[j]	
Flertrådsmodell.[j]	
Biometri, exempelvis tangentbordsanvändning.[c]	
Antal gånger angriparen återvänder till systemet.[l]	
Sättet att föra ut (exfiltrera) data.[j]	
Teknisk sofistikation.[a]	
Problem med ovan indikatorer	
Det är lätt att få tag på cybervapen, vilket gör det svårt att koppla vapen till aktör. Exempelvis använder operationer piratkopierad mjukvara, öppet tillgängliga verktyg[f] och en angripares kod kan ibland återanvändas av andra angripare[f, j], vilket är lätt eftersom modulärt programmeringssätt är praxis[k].	

Förmodligen är det ganska enkelt att dölja det mesta av ens programmeringsstil och om många programmerare hjälps åt vattnas den personliga stilen ur. Detta kan visserligen resultera i att exempelvis en organisatorisk eller nationell stil då bli tydligare. Dessutom används exempelvis virtuella maskiner med intetsägande[f] användarnamn eller namn som är påhittade för att vara vilseledande[j].
Det är svårt att analysera koden eftersom tillgång till källkoden[j] och dokumentation oftast saknas. Dessutom är det inte lämpligt att låta koden köra hur som helst och se vad som händer. Angriparna kan exempelvis se till att koden upptäcker att den försöker köras i en sandlåda (eng. sandbox) eller debugger och därmed inte tillåter körning.[j] Koden kan dessutom delvis vara krypterad när den inte körs.[j] En sak som gör det svårare är också att de analyser analytiker och forskare gör kan sätta spår i ledningssystemloggarna (C2-loggarna), vilket kan förvirra andra analytiker och forskare.[g]
Det är svårt att jämföra mer direkt aktivt mänskligt agerande i systemen, såsom tangentbordsanvändningsstil, på grund av avsaknad av data. Det kan vara en förklaring till varför CFR inte nämner exempel på sådant. Angripare kan också uppmärksamma upptäcktsförsök och då avsluta operationen. Exempelvis kan honeypots (avsiktligt sårbara datorer som ska upptäcka angripare när de angrips[h]) vara alltför lätta att ta sig in i[l].
Det är svårt att bedöma sofistikation (se också kapitel 6). Dessutom räcker nog bara slutsatsen om att en operation var sofistikerad för att kunna tala om att en stat legat bakom operationen, men inte vilken stat.

Uttalanden och motaktioner

Forskningen	**CFR-källorna**
Offentliga uttalanden.[a]	Utrikesminister ansåg att en statsaktör låg bakom operationen (Goeij, 2017).
	Italienska myndighetspersoner trodde Ryssland låg bakom operationen (Kirchgaessner, 2017).
	En amerikansk politiker (och en tankesmedja) hävdade att angriparnas IP-adresser spårats till Ryssland (Huetteman, 2017).
	Cybersäkerhetsföretag och amerikanska myndighetspersoner sade att hackergruppen arbetade åt ryska militära underrättelsetjänsten (Homewood, 2017).

Anspråk på att ligga bakom operationen (eng. claim).[d, i]	En tidigare panamansk säkerhetsanalytiker erkände inblandning (Reyes m.fl., 2017).
Rättsväsendet gör inga insatser eller når ingen framgång.[a, b, d]	
Problem med ovan indikatorer	
Personer och organisationer som uttalar sig har sina skäl till det och kan ha en dold agenda, vinkla eller ljuga. Det är svårt att veta vilka det går att lita på.	
Det är nog svårt veta om rättsväsendet faktiskt kört fast eller låstas som att det inte kommer någon vart. Dessutom ligger förmodligen cybersäkerhetsföretagens analyser före rättsväsendets agerande, varför företagen inte kan dra några slutsatser om det.	

4.2 Indikatorernas användning

De följande avsnitten tar upp nyttan med offentligt utpekande (4.2.1), nivån av bevisföring som krävs (4.2.2) samt svagheter med indikatorerna och deras sammanvägning (4.2.3).

4.2.1 Att (inte) peka ut offentligt

I vissa fall finns det intresse av att ta reda på vem som utförde ett angrepp utan att öppet tala om ens slutsats. Anledningen till att inte offentligt peka ut någon kan exempelvis vara att inte varsko angriparen (Bartholomew och Guerrero-Saade, 2016; Rid och Buchanan, 2015) eller att låta angriparen leva i ovisshet om huruvida det kommer ett straff eller motangrepp (Lin, 2016). Det kan också vara poänglöst att öppet attribuera ett angrepp till en stat på grund av att det i alla fall inte finns några möjliga svar eller sanktioner att tillgå (Bartholomew och Guerrero-Saade, 2016). I linje med det verkar stater oftare peka ut stater som angripare än vad företag gör (Mueller m.fl., 2019). Ännu värre än att inte ha något att sätta emot, är att anklagandet av en stat kan leda till negativa konsekvenser för den som anklagar. Exempelvis hävdade en chef för angreppsanalys vid Kaspersky att han fick inbrott i sitt hem med budskapet att ta en paus i analysen av en viss skadlig kod (Romanosky och Boudreaux, 2019). Det är också möjligt att man drabbas av repressalier om man har fel (Romanosky och Boudreaux, 2019). I sådana fall kan det vara bättre att vara en anonym källa till en tidning (Davis m.fl., 2017).

Ytterligare en anledning till att inte öppet attribuera är att undvika att röja någons operation (Rid och Buchanan, 2015). Exempelvis kanske man

bara drabbats som offer i form av sidoskador av ett angrepp som riktade sig mot ens fiender (Romanosky och Boudreaux, 2019).

En annan möjlighet är att inte bita den hand som föder en eller ens allierad. Exempelvis finns det tecken på att cybersäkerhetsföretagen ogärna pekar ut de stater som stöttar dem. USA-baserade cybersäkerhetsföretag pekar normalt inte ut amerikanska staten (Romanosky och Boudreaux, 2019; Yadron, 2015). Å andra sidan pekar ryska Kaspersky normalt inte ut stater, men gjorde ändå det i ett fall med rysk statlig inblandning (Bartholomew och Guerrero-Saade, 2016; Yadron, 2015). Dock gjordes denna attribution av den amerikanska fristående grenen av företaget (Yadron, 2015) som skapades efter att Kaspersky inte längre fick sälja till amerikanska myndigheter (Volz, 2017). Kopplingarna mellan stater och cybersäkerhetsföretag är ofta ganska starka, exempelvis för företag som CrowdStrike och Palo Alto Networks vars grundare eller höga chefer tidigare varit verksamma inom myndigheter (Romanosky och Boudreaux, 2019) och FireEye som finansierats av CIA (Yadron, 2015). Japanska cybersäkerhetsföretaget TrendMicro säger sig inte attribuera angrepp till stater (Malik, 2017).

Slutligen kan öppen attribution oavsiktligt avslöja ens källor och metoder för attribution och underrättelseinhämtning (Rid och Buchanan, 2015; Bartholomew och Guerrero-Saade, 2016). Ofta är det statliga myndigheter som inte vill avslöja detaljer, men även företag som exempelvis Google och Facebook vill inte avslöja sina källor och metoder, vilket framgår av deras varningar till användare som kan ha drabbats av statsangrepp (Grosse, 2012; Stamos, 2015).

4.2.2 Vilken nivå av bevisföring som krävs

En viktig aspekt av attribution är hur starka bevisen måste vara, det vill säga hur mycket ovisshet som kan accepteras (Davis m.fl., 2017; Shakarian m.fl., 2015; Farral, 2017). Kina har till exempel kritiserat USA för att använda alltför svaga bevis (Kinas utrikesdepartement 2015a; 2015b). Det krävs olika starka bevis beroende på ändamålet med attributionen. Att få en angripare fälld i domstol kräver mycket starka bevis (Berghel, 2017), medan bevisen troligtvis inte behöver vara lika starka för att avgöra om ett motangrepp får genomföras (Tsagourias, 2012). Sämre bevis kan också vara nyttiga för att leda fram till starkare bevis där de sämre bevisen kan ses som ledtrådar och de starkare som de som faktiskt kan användas som grund för att agera mot andra (Clark och Landau, 2010). Shamsi m.fl. (2016) bedömde styrkan för attributionen för några omskrivna cyberangrepp och kom fram till att styrkan oftast är låg (identifiering av vapnet) eller medelhög (identifiering av landet), med ett undantag där styrkan var hög (identifiering av personen).

Det är rimligt att anta att den som inte själv kan få fram bevis som når upp till rådande gräns för utpekning, inte vill acceptera den rådande gränsen. Antingen ses då den rådande gränsen som för hög (för att själv kunna peka ut någon) eller som för låg (eftersom den ger andra möjlighet att peka ut någon utan att man själv har den möjligheten). Exempelvis Schmitt och Vihul (2017) spekulerar kring detta.

4.2.3 Att väga samman indikatorerna

Förutom problem som rör enskilda indikatorer för attribution är en anledning till svårigheterna med attribution hur indikatorerna läggs samman och värderas. Beviskedjorna är ofta väldigt svaga och bygger ofta på andra svaga bevis från andra operationer. Vilken typ av bevis som används skiljer sig åt från gång till gång och motbevis ignoreras som regel. Detta påminner om hur samma typ av våldsdåd ibland ses som terrorism och i andra fall som ett utslag av gärningspersonens mentala ohälsa (Noor m.fl., 2018). Ibland, som i PWC (2017) ses till och med bevis som går åt andra hållet som tecken på vilseledning. Fokker och Beek (2019) utgör ett undantag med försök till hypotesfalsifiering. Inom amerikansk underrättelsetjänst rekommenderas också att olika hypoteser jämförs (ODNI, 2018).

Det vore lämpligt med en bedömning av ovissheten för attributionen (Rid och Buchanan, 2015), men sådan rapporteras sällan, med Hegel (2018) som ett av få undantag. En vedertagen ovisshetsskala saknas dock (Davis m.fl., 2017). Amerikansk underrättelsetjänst använder en ovisshetsskala med tre steg från låg till mellan och till sist högt förtroende för slutsatserna (ODNI, 2018). Samma källa redovisar också ett exempel med en ovisshetsskala i två steg för några operationer under 2017.

Det finns också ett behov av en rigorös metodik som inkluderar oberoende granskning av bevisföringen (Davis m.fl., 2017). Viss granskning fås i sällsynta fall genom att de olika cybersäkerhetsföretagen inte håller med varandra (Lancaster, 2017 visar på ett sådant fall), kanske för att vinna marknadsandelar (Davis m.fl., 2017). Amerikansk underrättelsetjänst ser användning av externa källor och samarbete som viktiga delar av metoden för attribution (ODNI, 2018).

Ett intressant försök rapporterades i Homewood (2017) där försök gjordes för att få kontakt med gruppen som pekats ut som ansvarig. Kontakten ledde dock inte till någon kommentar från gruppen.

5 Tillvägagångssätt

I detta kapitel beskrivs vanliga tillvägagångssätt. Till skillnad från kapitlet om attribution är det i huvudsak en beskrivande genomgång utan analys. En analys av vilka tillvägagångssätt som är mer lämpliga än andra och vilka skydd som är tillämpliga, faller utanför ramarna för denna rapport. Nästa kapitel spinner dock vidare på tillvägagångssätten och analyserar hur sofistikerade de är.

Tillvägagångssätten är indelade i Lockheed Martins Cyber Kill Chain (LMCKC). LMCKC består av sju steg:

1. Rekognoscering.
2. Vapentillverkning.
3. Leverans (av vapnet).
4. Utnyttjande (av sårbarhet).
5. Installation.
6. Ledning (eng. command and control).
7. Agerande (för att uppnå målet).

För varje steg i LMCKC finns i Tabell 12 en (fritt översatt och nedkortad) definition av steget från Lockheed Martin själva. Dessutom finns typexempel (ett urval) som mestadels kommer från Lockheed Martin (2006)[18], men också från andra källor (främst olika publikationer från Mitre[19]). Dessutom ges, indelat i stegen, exempel på hur operationerna i CFR skedde enligt CFR-källorna.

Det kan noteras att CFR-källorna sällan ger en tillräckligt komplett beskrivning av en operation för att det för den enskilda operationen ska kunna gå att förstå vad som sker i varje steg. I denna rapport görs dock ingen uppdelning per operation utan det räcker med att någon källa för någon operation beskrivit något belysande som skett i ett visst steg. Litteraturen med typiska exempel återfinns som referenser i Tabell 11. Där finns också en bokstav per referens för att kortare kunna referera i de kommande avsnitten.

[18] Eftersom källan utgör presentationsbilder (slides) har viss tolkning behövt göras.

[19] Mitre tillhandahåller dessutom exempel på hur olika aktörer använt olika tillvägagångssätt. Se exempelvis Procedure Examples för riktat nätfiske på https://attack.mitre.org/techniques/T1192/

Tabell 11: Referenser (källor) och vilken bokstav som används för att referera till dem.

Bokstav	Referens
a	Lockheed Martin, 2006
b	Hutchins m.fl., 2011
c	Hewlett Packard Enterprise, 2014
d	Mitre, 2019b
e	Mitre, 2019c
f	Cho m.fl., 2018
g	Mitre, 2019d

Tabell 12: Tillvägagångssätt indelade i stegen från LMCKC.

Tillvägagångssätt enligt LMCKC	
Rekognoscering (eng. reconnaissance) Definition[b]: *Forskning, identifiering och val av mål (exempelvis information om specifik teknologi).*	
Typiska exempel	**CFR**
Samla in mejladresser.[a]	Hitta information som rör enskilda individer.
Identifiera anställda på sociala medier.[a]	
Samla in pressmeddelanden och konferensdeltagarlistor.[a]	
Identifiera kritisk personal.[d]	
Samla in organisationsspecifik information.[d]	
Hitta internetanslutna datorer.[a, d]	
Hitta sårbarheter i teknik, personal och organisation.[d]	Hitta sårbarheter och inloggningsuppgifter.
	Lära sig om verktyg (exempelvis produktdemonstrationer).
Vapentillverkning (eng. weaponization) Definition[b]: *Ihopkopplande av kod som utnyttjar en sårbarhet med möjlighet att ansluta hem.*	

Typiska exempel	**CFR**
Skaffa ett verktyg för vapentillverkning.[a, d]	Skaffa vapen genom köp eller egentillverkning, alternativt nyttjande av öppen källkod eller en variant av ett välkänt vapen.
Testa verktyg.[d]	
Välja bakdörr.[a]	
Välja ledningsinfrastruktur.[a, d]	Skapa C2-domän.
Välja lockbetesdokument.[a]	Skapa grund för att luras, exempelvis ta fram bluffmejl, bluffhemsida och bluffcertifikat.
Välja uppdrags-ID.[a]	
Leverans (eng. delivery) Definition[b]: *Överföring av vapnet till målet.*	
Typiska exempel	**CFR**
Mejl.[a, b, c, e, g]	Mejl med länk eller bilaga.
	Sms med länk.
Sociala medier.[a]	
USB-sticka.[a, b, c, g]	Flyttbara media.
Komprometterad webbplats (så kallad vattenhålsangrepp efter eng. watering hole attack).[a, b, c, e, g]	Komprometterad webbplats.
Angrepp mot webbservrar (ex. SQL-injection eller att utnyttja applikationer som vänder sig till användare).[a, f]	
Komprometterad leveranskedja.[e, g]	Kapad mjukvaruuppdatering.
Utnyttjande (eng. exploitation) Definition[b]: *Utnyttjande av sårbarhet vilket leder till att angriparens kod körs.*	
Typiska exempel	**CFR**
(Utnyttjande av) framtagen eller inskaffad ny sårbarhet (zero-day).[a]	Utnyttjande av ny sårbarhet (zero-day).

(Utnyttjande av) sårbarhet som möjliggör buffer overflow.[e]	
	Utnyttjande av möjlighet att köra makron.
	Utnyttjande av sårbarhet i nätverksprotokoll för delning av skrivare och filer (SMB).
Knäckning av lösenord.[a, e, f, g]	Knäckning av lösenord.
	Extrahera lagrade inloggningsuppgifter från minnet.
	Stöld av inloggningsuppgifter.
Öppnande av bifogad fil.[a]	Lura användaren att öppna bifogad fil.
Klickande på länk.[a]	Lura användaren att klicka på länk.
	Lura användaren att uppge inloggningsuppgifter.
	Lura användaren att uppdatera eller installera skadlig kod som ser ut som legitim.
Installation (eng. installation) Definition[b]: *Installation som leder till att angriparen kan fortleva i systemet.*	
Typiska exempel	**CFR**
Installera verktyg på webbserver.[a]	
Installera bakdörr på klienten.[a]	Installera bakdörr på klienten.
Injicera kod i en körande process.[e, g]	Integrera i andra processer.
Ändra en systemtjänst.[g]	
Lägga till systemtjänster.[a, e, g]	
Schemalägga en aktivitet.[e, g]	
Lägga till autostartsnycklar i registret.[a, g]	Lägga till som autostart.
Modifiera bootloadern.[g]	Modifiera bootloadern.
Manipulera användarkonto.[g]	Manipulera användarkonto.
Lägga till användarkonto.[g]	

Ändra standardprogram för olika filändelser och kortkommandon.[g]	
Manipulera kodens installationsdatum.[a, g]	Förstöra bevis.
Ha vilseledande filändelser.[e, g]	Ha namn likt godartade filer.
	Dölja med steganografi.
Dölja med kryptering.[g]	Dölja med kryptering.
Dölja med dolda filer och mappar.[g]	
Förstora filstorleken för att undgå matchning baserat på filens hash.[e]	
	Hålla låg profil.
	Uppdatera sin kod.
Inaktivera säkerhetsfunktioner.[e, g]	Stänga av säkerhetsmekanismer, ex inaktivera brandvägg.
Öppna nätverksport.[g]	Öppna nätverksport.

Ledning (eng. command and control, C2)

Definition[b]: *Etablerandet av kommunikationskanal som typiskt ger angriparen manuell kontroll av systemet.*

Typiska exempel	**CFR**
Via webben, DNS eller mejl.[a]	Legitimt webbhotell.
	Övertagen webbplats.
	Ledningscentral placerad i mållandet för att undvika internationell kommunikationskontroll.
Krypterad kommunikation.[g]	Krypterad kommunikation.
Via flyttbara media.[g]	
Via proxy.[g]	Via proxy.
	(Ingen).

Agerande (eng. actions on objectives)

Definition[b]: *Agera för att uppnå slutmålen (datainsamling eller påverkan på datas riktighet eller tillgänglighet) alternativt för att sprida sig vidare.*

Typiska exempel	CFR
Privilegieeskalering.[a, e, g]	Samla in inloggningsuppgifter.
Intern rekognoscering.[a, g]	Kartlägga nätverket.
Röra sig i nätet.[g]	Röra sig i nätet.
Samla in lagrad data och nya indata.[g]	Samla in data, både lagrad och ny, via exempelvis mikrofon.
Förstöra eller utpressa genom kryptering.[g]	Förstöra eller utpressa genom kryptering.
Förstöra data.[g]	
Ändra data.[g]	Ändra information.
	Plantera desinformation.
Utnyttja beräkningsresurser.[g]	
Hindra tillgång med otillgänglighetsangrepp (DoS).[e, g]	Hindra tillgång med otillgänglighetsangrepp (DoS).

6 Sofistikation

Mer sofistikerade operationer kräver andra – förmodligen svårare – motåtgärder än mindre sofistikerade operationer (Guitton och Korzak, 2013). Att skydda sig mot mindre sofistikerade operationer är förmodligen ganska rättframt och sådana operationer är därför av mindre intresse för forskning på cyberoperationsområdet. Det är därför av vikt att avgöra vilka operationer som är (mer) sofistikerade. Det finns dock ingen vedertagen definition av vilka operationer som är sofistikerade (Guitton och Korzak, 2013) och en begränsad mängd forskning har genomförts för att försöka skapa en definition (DePaula och Goel, 2016). Ingen kvantitativ analys av sofistikation för cyberoperationer har genomförts (DePaula och Goel, 2016). Slutsatser om sofistikation dras ofta på svaga grunder (Buchanan, 2017) och media är okritiska till påståenden om sofistikation (Buchanan, 2017).

Det är betydligt lättare att hitta expertbedömningar av vad som är sofistikerat än definitioner och skalor för vad experterna ser som sofistikerat. Källorna är inte överens om vilka operationer som är sofistikerade (se exempelvis Higbee, 2013) och kritik har riktats mot det slarviga och slentrianmässiga sätt sofistikation används på (Winkler, 2015; Guitton och Korzak, 2013). Helt klart finns det ingen mening med att betrakta något som sofistikerat om allt annat också är det eftersom begreppet då blir intetsägande (Buchanan, 2017). Det finns flera olika anledningar till att hävda att en operation var sofistikerad trots att den inte egentligen var det. Företag som drabbats av angrepp vill inte erkänna sina brister och överdriver istället den förmåga angriparen uppvisat. Vidare får cybersäkerhetsföretagen mer fokus när de kallar angreppen sofistikerade (Buchanan, 2017). Det har lett till att en del kritiska röster börjat använda begreppet avancerad persistent marknadsföring, vilket påminner om begreppet avancerade persistenta hot eller APT:er (eng. advanced persistent threats) som ibland likställts med sofistikerade angripare (DePaula och Goel, 2016; NIST, 2011).

I återstoden av kapitlet beskrivs indikatorer på operationers sofistikation (6.1) och sofistikationsgrad (6.2).

6.1 Indikatorer på operationers sofistikation

I litteraturen finns olika mer eller mindre tydliga uttalanden om vad som räknas som sofistikation. Dessa uttalanden (indikatorerna) har delats in i kategorier. Kategorierna är snarlika de egenskaper kvalificerade

(sofistikerade) aktörer bedömts ha enligt experter i tidigare forskning (Fylkner, 2003) och utgörs av:

- **Mer riktat**
  En del operationer är mer avgränsade mot specifika mål snarare än att vilja slå brett (och urskillningslöst).
- **Svårare mål och syften**
  En del operationer har svårare mål. Här ingår också hur stor effekt som uppnås och under hur lång tid.
- **Mer resurser**
  En del operationer kräver större resurser som mer personal, mer kunskap, bättre rutiner och mer tillgång.
- **Mer unika och bättre verktyg**
  En del operationer utnyttjar nyare sårbarheter, kräver mer testning och mer komplexa verktyg.
- **Mer svårupptäckt**
  En del operationer är mindre synliga och använder olika tekniker för att dölja sig, förfalska, kryptera och tar olika grepp för att hindra att operationen kopplas samman med en aktören tidigare utfört.

Dessutom överlappar indikatorerna delvis med de indikatorer för attribution som beskrevs i avsnitt 4.1. Detta beror på att attributionen ofta handlar om att ta reda på om en operation var statsstödd och det via om den var sofistikerad.

I de följande avsnitten beskrivs generella motargument mot kategorierna (6.1.1) och själva indikatorerna tillsammans med mer specifika motargument (6.1.2).

6.1.1 Generella motargument mot indikatorerna

För varje föreslagen indikatorkategori ges motargument (validitetsproblem) mot indikatorerna. Motargumenten kan vara av olika typer:

- **Indikatorerna kanske bara är tillämpliga ibland**
  Exempelvis behövs inte alltid sofistikerade vapen även om den bakomliggande angriparen kan ha tillgång till sådana. Och att ha möjlighet att angripa mer riktat eller mot svårare mål innebär inte automatiskt att aktören agerar så. På motsvarande sätt kanske vad som ibland är sofistikerat annars är det motsatta. Exempelvis är en angripare som inte viker ner sig för utmaningen att ta sig förbi många skydd i vissa fall mer sofistikerad, samtidigt som envisheten i själva verket vara ett tecken på dumhet om angriparen helt enkelt inte inser att målet är omöjligt att forcera.

- **Indikatorerna kanske är otillräckliga**
  Sofistikerade angripare kan ha mer att förlora och kanske därför inte kan ta så stora risker (exempelvis vad gäller upptäckt). Men minskad risk leder kanske även till minskade möjligheter.

Det bör också noteras att det förutom motargumenten också kan vara svårt att mäta indikatorerna:

- **Det är ibland svårt att uppfatta indikatorerna**
  Exempelvis kan det vara svårt att utifrån en operations effekter veta hur riktad operationen var avsedd att vara.
- **Det är ibland svårt att göra de värderingar som krävs**
  Ett exempel på detta rör bedömning av cybervapens tekniska verkshöjd. Det vore rimligt att göra bedömningarna baserat på hur mycket använda sårbarheter är värda men det är svårt eftersom empiriska data om sårbarheter är svåra att få tag i (Stevens, 2012), sårbarhetsmarknaden relativt oreglerad (Miller, 2007) och belöningar för att hitta buggar inte nödvändigtvis mer rättvisande (Finifter m.fl., 2013).

6.1.2 Indikatorerna

I Tabell 14 beskrivs indikatorerna för attribution som identifierats i forskningslitteraturen och i CFR-databasens källor. Indikatorerna är indelade i kategorier och i slutet av varje kategori finns identifierade motargument mot kategorierna. Vad CFR-databasens källor kallar sofistikerat framgår dock bara i undantagsfall (och det finns inte för alla kategorier av indikatorer). Istället saknar källornas uttalanden om sofistikation normalt tydlig koppling till en viss aspekt (indikator) hos operationen och är mer allmänna uttalanden och slutsatser av en längre beskrivning. Mer om detta framkommer också i slutet av avsnittet om sofistikationsgrad (6.2).

Den litteratur som användes för att identifiera indikatorerna återfinns som referenser i Tabell 13. Där finns också en bokstav per referens för att kortare kunna referera i de kommande avsnitten.

Tabell 13: Referenser (källor) och vilken bokstav som används för att referera till dem.

Bokstav	Referens
a	Casey, 2007
b	DePaula och Goel, 2016
c	Chen m.fl., 2014
d	Mateski m.fl., 2012

e	Duggan m.fl., 2007
f	Mirkovic och Reiher, 2004
g	Piper, 2013
h	Aitel, 2016
i	Willett, 2019
j	Buchanan, 2017
k	Kjaerland, 2006
l	Guitton och Korzak, 2013
m	Seebruck, 2015
n	Betz och Stevens, 2012
o	NIST, 2011
p	Holm och Sommestad, 2017
q	Miller, 2007
r	Huang m.fl., 2015
s	Nye, 2010 citerad i Haaster, 2016

Tabell 14: Indikatorer på sofistikation indelade i kategorier samt motargument mot indikatorerna.

Indikatorer på sofistikation
Mer riktat
Forskningen
Mer riktat i allmänhet.[a, b, c, g, h, i, j]
Förstå risken för sidoskador och utveckla insatsreglerna (eng. rules of engagement) enligt det.[i]
Politiskt styrt.[l]
Motargument
Det kan vara sofistikerat att slå brett (mot många) snarare än att vara riktad.

Det behöver inte vara mer sofistikerat att bry sig om sidoskador även om man skulle kunna göra det. Å andra sidan kan hotaktörer bakom mer sofistikerade operationer förmodligen utöva mer inflytande på vilka sidoskador som anses acceptabla.
Förmodligen är politiken väldigt komplex och man vill typiskt slå mot alla, även om man är mer försiktigt mot sina allierade.
Svårare mål och syften
Forskningen
Svårare mål och syften i allmänhet.[a, b, d, f, m]
Har industriella informations- och styrsystem som mål.[n]
Saboterar.[l]
Uppnår sitt mål.[b]
Uppnår större effekt.[d, f]
Utför svårare operationer.[j]
Är mer ihärdig (eng. persistence).[b, c, e, f, h, o]
Är mer hängiven.[a, e, o]
Motargument
Det är oklart hur väl sofistikation verkligen kan bedömas utifrån motiv.[m] Visserligen kan aktörer med sofistikerad förmåga inhämta underrättelser i andra operationer utanför cyberdomänen men det betyder inte nödvändigtvis att de aktörerna istället fokuserar på sabotage i cyberdomänen. Att inhämta information kan vara enklare att göra via cyberdomänen medan sabotage kan vara enklare att genomföra utanför cyberdomänen.
En del mål kan vara så svårangripna att de närmast är lönlösa att angripa, vilket mer sofistikerade angripare nog har vetskap om, till skillnad från mindre sofistikerade angripare. Med andra ord kanske mindre sofistikerade angripare i vissa fall ger sig på svårare mål i större utsträckning än vad mer sofistikerade angripare gör.
Att angriparen ger sig på mindre svåra mål innebär inte att angriparen inte hade kunnat ge sig på svårare mål.[j]

Ihärdighet och hängivenhet behövs inte om man nått sitt mål. Med andra ord kan det i vissa fall vara ett tecken på att man inte lyckats och alltså är mindre sofistikerad.	
Mer resurser	
Forskningen	**CFR-källorna**
Mer resurer i allmänhet.[b, f, i, k, o]	Mer kontroll (Great, 2017c).
Mer personal.[e]	Strikt organisering (Great, 2017c).
Mer cyberkunskap.[d, e]	
Mer kunskap om fysiska system.[e]	
Mer expertis.[i, j, o]	
Gör färre misstag (relativt sett).[j]	
Lär sig från sina misstag.[p]	
Bättre kultur.[i]	
Bättre nätverksinfrastruktur.[h, k]	
Har stulna digitala signaturer.[b]	Angrepp mot leveranskedjan (Cherepanov, 2017).
Kan hantera stora mängder data.[i]	
Är snabbare.[b, j]	
Bättre procedurer.[j]	
Bättre strategier.[i]	
Mer precisa underrättelser[l] och mer precis analys.[k]	Mer kunskap om målet (Symantec, 2017b).
Mer inflytande över datorer och nätverk.[s]	
Bättre lägesuppfattning.[i]	
Mer förutseende.[j]	
Mer åtkomst.[a, b, d, e]	

Mer tid som kan avsättas.[d]	
Motargument	
Mycket av resurserna bygger på underrättelser och underrättelseanalys vilket visserligen kan visa på sofistikation men inte nödvändigtvis cybersofistikation.	
Många resurser kan köpas och pengar behöver inte vara ett tecken på sofistikation.	

Mer unika och bättre verktyg	
Forskningen	**CFR-källorna**
Mer unika och bättre verktyg i allmänhet.[d, j]	Bättre verktyg (Perlroth och Shane, 2017).
	Mer modulära verktyg (Howell O'Neill, 2017).
	Inhämtar information via fler kanaler på målsystemet (C4I och Naor, 2017).
	Utnyttjar sårbarheter som gör det möjligt att köra osignerad kod (Great, 2017b).
Utnyttjar svårare och nyare sårbarheter (eng. zero-days).[b, c, d, f, l, q, r]	Zero-days (Symantec, 2017b; Great, 2017b).
Mer anpassad kod och procedurer.[h, j, k, p]	Skräddarsydd kod (PWC, 2017).
Mer testning.[h]	
Mer komplex kod.[b]	Anpassar verktyg under användning (Newman, 2017).
Svårförståeligare operationer.[j]	
Flera tekniker.[b, f, g, k, o]	
Motargument	
Verktyg, inklusive vapen som ger sig på sårbarheter som inte är allmänt kända (zero-days), kan köpas och pengar behöver inte vara ett tecken på sofistikation.[b] även om hur pengarna spenderas (motivationen) kan ses som det (jämför indikatorkategorin *svårare mål och syften*).	

En mer sofistikerad angripare är nog mer mogen och det innebär användning av mer standardiserade verktyg snarare än att de måste anpassas. Mer standardiserade verktyg kan också enklare automatiseras.[h] Å andra sidan måste detta vägas mot att ökad standardisering leder till enklare upptäckt.

Mer svårupptäckt	
Forskningen	**CFR-källorna**
Smygteknik (eng. stealth).[a, b, c, d, e, g]	Injicerar verktyget i dll-filer (Atch och Neray, 2017).
Mindre synlig.[a]	Använder legitima gratissajter för lagring eftersom sådana inte kräver registrering (Atch och Neray, 2017).
	Använder lagringstjänsten Dropbox för att föra ut data eftersom den sällan blockeras eller övervakas (Atch och Neray, 2017).
Använder dolda kanaler.[a]	
Krypterar kommunikation och utförsel av data.[a]	
Krypterar sina aktiviteter.[b]	Använder krypterade dll-filer (Atch och Neray, 2017).
Använder tekniker som döljer sina vapen.[a]	Kör plugins i minnet (Great, 2017b; Newman, 2017).
Förfalskar sin identitet med spoofing.[b, f]	
Mer genomförandesäkerhet (eng. operations security), exempelvis återanvänder inte vapen.[h]	
Motargument	
Bara för att man kan vara osynlig betyder inte det att man nödvändigtvis vill vara det.[a] (Se också avsnitt 4.1.)	
Det är bara upptäckta operationer som kan analyseras varför alla operationer som upptäckts kanske ska ses som mindre sofistikerade.	

6.2 Sofistikationsgrad

En fråga är hur många indikatorer på sofistikation som måste uppfyllas för att ett angrepp eller en angripare ska räknas som sofistikerad och hur väl indikatorerna måste uppfyllas. Det vore lämpligt att ha en skala med steg för olika nivåer av (indikationsuppfyllnad av) sofistikation. I linje med detta beskrev Willett (2019) några indikatorer på sofistikation och nämnde att nästa steg i den forskningen var att ta fram nivåer. Litteraturen beskriver också några olika försök till att ta fram nivåer:

- Kjaerland (2006) beskrev tre nivåer för angripare som: använder andras verktyg (lägsta nivån), ändrar eller tillverkar enkla verktyg (mellersta nivån), tar fram komplexa verktyg (högsta nivån).
- Duggan m.fl. (2007) använde dels nivåerna låg, mellan och hög, dels antal dagar eller månader respektive antal personer.
- DePaula och Goel (2016) bedömde sofistikationsgraden efter hur många av deras kriterier på sofistikation som uppfylldes.
- Aitel (2016) rangordnade informellt olika nivåer för sina indikatorer på sofistikation, exempelvis genom att beskriva huruvida cybervapnet tetades manuellt eller automatiskt.
- Amerikanska Defense Science Board (2013) tog fram en sexgradig skala för angripare där nivå ett är den enklaste och nivå sex den mest avancerade. Nivå ett inkluderar angripare som använder verktyg utvecklade av andra, nivå två innebär egenutvecklade verktyg men som utnyttjar kända sårbarheter, nivå tre hittar egna sårbarheter, nivå fyra visar på mer organisering, nivå fem påverkar produkter för att göra dem osäkrare och till slut nivå sex som kan kombinera cyberförmågor med andra militära och underrättelsemässiga förmågor.

En annan fråga är vilken sofistikationsgrad utförda operationer typiskt har. Enligt DePaula och Goel (2016) har sofistikationsgraden för uppmärksammade angrepp generellt inte ökat med åren och de flesta sådana angrepp har låg nivå av sofistikation. Över 90 % av alla angrepp utnyttjar mindre än 10 % av kända sårbarheter (Allodi, 2015) och det tar flera år innan en utnyttjad sårbarhet byts ut mot en annan (Allodi m.fl., 2017). Tid till upptäckt för vanliga angrepp är typiskt månader medan angreppen sällan tar mer än minuter (Tableau, 2019). Å andra sidan blir vad som räknas som sofistikerat snart relativt ordinärt på ganska kort tid (DePaula och Goel, 2016). En möjlig slutsats är att sofistikation ofta används synonymt med *nytt* snarare än med ord som *svårt* och *komplicerat*.

Baserat på kapitel 5 kan slutsatsen dras att de flesta cyberoperationer består av relativt enkla (osofistikerade) tillvägagångssätt. Det finns gott om standardmässiga angreppsverktyg, användare är ganska lättlurade, sårbarheter finns och förblir länge, och de flesta har inte vetskap om vad som sker i deras system eller i omvärlden. När något i tillvägagångssättet faktiskt är sofistikerat är det ofta sådant som sker utanför cyberdomänen, som exempelvis klassisk underrättelseinhämtning eller att övertyga en insider. Dessutom är det snarare än svårighetsgrad oftare omständlighet som är barriären för angripare. Det bör dock noteras att CFR-databasen i stor utsträckning är baserad på cybersäkerhetsföretagens rapporter och att de företagen förmodligen i huvudsak är intresserade av operationer som rör många (potentiella kunder). Så om de mer sofistikerade operationerna är mer riktade innebär det att dessa inte beskrivs i samma utsträckning. Å andra sidan beskriver CFR-källorna ofta slentrianmässigt och otydligt operationer som sofistikerade. Bara i ett fåtal fall nämns istället att en operation var relativt *osofistikerad* (Minerva och ClearSky, 2015; FireEye, 2017; Reaqta, 2017). Dessutom är modellen (LMCKC), som tillvägagångssätten delats in efter, kvalitativ snarare än kvantitativ och säger därför inte så mycket om sofistikationsgraden.

7 Diskussion och framtida forskning

Rapporten baseras i stor utsträckning på data från en cyberoperationsdatabas som drivs av den amerikanska tankesmedjan CFR. Även om det bedömdes att CFR-databasen var den mest lämpade för studierna, finns det andra liknande databaser det skulle gå att jämföra resultaten med. Till exempel skulle göra det möjligt att avgöra hur mycket subjektivitet som finns i databasen (och de bedömningar som gjorts av den i denna rapport). Det skulle också vara möjligt att granska hur korrekta databaserna egentligen är genom att jämföra datakällor mot varandra och göra egna tester av hur operationer faktiskt kan ha gått till. Dessutom har åtminstone CFR-databasen en struktur som kräver information som den sällan inkluderar. Det vore intressant att studera huruvida databasen kunde kompletteras med den informationen eller om de detaljerna faktiskt är för svåra att få tag på data om. Det kan också undersökas hur databasens struktur skulle kunna förbättras genom att göras mer finmaskig eller genom att ha mer kontroll av vilka alternativ som är möjliga att ange för varje del av strukturen.

I de följande avsnitten dras slutsatser och förslag ges på framtida forskning. Det finns ett avsnitt för vart och ett av de tre forskningsinriktningarna rapporten haft.

7.1 Attribution

Att avgöra vem som ligger bakom en cyberoperation (det vill säga att attribuera den) är av intresse bland annat för att agera mot angriparen och på rätt sätt. Till exempel är det förmodligen inte en militär fråga att en enskild individ slår mot ett svenskt företag, men om en stat gör det kan även Försvarsmakten tänkas bli inblandad. Samtidigt är attribution svårt. Cybersäkerhetsaktörers offentliga uttalanden framstår ofta som politiskt färgade och attribution görs sällan med rigorösa metoder som inkluderar oberoende granskning av bevisföringen och ger en bedömning av ovissheten av attributionen.

Det pågår omfattande forskning för att förbättra möjligheterna till attribution. Amerikanska forskningsmyndigheten Darpas program för förbättrad attribution (eng. Enhanced Attribution) löper 1 nov 2016–1 maj 2021 och syftar till att förbättra attributionsmöjligheterna samt statens möjligheter att öppet avslöja sina slutsatser utan att skada sina källor och metoder (Crone, 2019; Darpa, 2016a). Målet är en minskning av mödan

och tiden det tar att attribuera från månader till timmar och till och med sekunder (Darpa, 2016b).

En åtgärd för att förbättra attributionsmöjligheterna som föreslagits är att göra det svårare att vara anonym på internet (Nicholson m.fl., 2015). Exempelvis skulle internetprotokollen kunna göras mer resistenta mot spoofing och svårattribuerad trafik skulle kunna filtreras bort av routrarna. En särskild avanonymiserad del av internet undersöktes av Darpa 2002, men projektet lades ner på grund av stark kritik (Wheeler m.fl., 2003). Det skulle onekligen vara svårt och dyrt att göra om internet till en helt icke-anonym plats (Cook m.fl., 2016) och påverkan på människors personliga integritet i olika sammanhang vore avsevärd (Clark och Landau, 2010).

Det finns också många försök till ökat samarbete för bättre attribution. Det finns många olika aktörer som utför, eller skulle kunna utföra, attribution. Men i dagsläget delar aktörer normalt inte data och slutledningar med varandra (Davis m.fl., 2017, Bartholomew och Guerrero-Saade, 2016). Cybersäkerhetsföretagen har stora antal kunder och är verksamma i många länder, vilket ger goda insikter i vad som sker i olika nät (Romanosky och Boudreaux, 2019), samtidigt som de har fokus på teknisk förmåga snarare än analysförmåga (Bartholomew och Guerrero-Saade, 2016). Olika företag klassificerar dessutom angrepp på olika grunder (Bartholomew och Guerrero-Saade, 2016). Underrättelsetjänster har goda källor inom cyber och dessutom inom övriga domäner (Malik, 2017; Symantec, 2018), men kan i mindre mån prata öppet om attribution. För att förbättra möjligheterna till attribution vore ökat samarbete mellan olika aktörer därför nyttigt. Av detta skäl har ett konsortium av privata aktörer föreslagits (Davis m.fl., 2017) och likaså en neutral global sammanslutning (Mueller m.fl., 2019), ett cyber-IAEA (likt det internationella atomenergiorganet) (Neutze, 2016) och en internationell cyberattributionsdomstol (Chernenko m.fl., 2018).

Några av de frågor som behöver besvaras för att uppnå bättre attribution är:

- Hur enkelt är det i praktiken att utifrån en viss kod bedöma sådant som programmerarens arbetstid, naturliga språk och programmeringsstil?
- Hur enkelt är det att skriva kod som skyddar sig mot olika typer av granskning med avseende på attribution?
- Vilka typer av operationer attribueras eller tas i anspråk (eng. claims) i större utsträckning än andra typer?
- Vilka aktörer har syften som liknar de stater har vad gäller cyberoperationer?

7.2 Tillvägagångssätt

Operationers tillvägagångssätt kan delas in på olika sätt. I denna rapport delades tillvägagångssätten in i steg enligt Lockheed Martins Cyber Kill Chain (LMCKC). Några generella slutsatser per steg följer nedan:

- **Rekognoscering**
  Den rekognoscering som framgår är generellt ganska enkel. Det är möjligt att det typiskt inte krävs så svår rekognoscering för att kunna genomföra cyberoperationer, men det är också svårt att utifrån data om vad som skett i ens system kunna dra slutsatser om vilken rekognoscering som skett inför eller i början av operationen. Rekognoscering som sker löpande för att angriparen ska tas sig vidare i näten är dock enklare att bilda sig en uppfattning om.
- **Leverans**
  Operationerna baseras ofta på att vanliga användare luras att agera på ett för angriparen fördelaktigt sätt. Framförallt används nätfiske men även sådant som att ligga och vänta på att användare ska surfa in på en webbplats man tagit över.
- **Utnyttjande**
  Till stor del används återanvänds verktyg och välkända sårbarheter utnyttjas såsom att lura användare att öppna bifogade filer. Samtidigt är förmodligen operationer som utförs med nyare (okända) sårbarheter förmodligen också svårare att upptäcka varför de inte syns så mycket i tillgängliga data.
- **Installation**
  Operationerna fortlever genom många olika metoder och till stor del går det ut på att hålla sig dold.
- **Ledning**
  Operationerna leds typiskt tämligen enkelt via legitima webbhotell och tidigare övertagna webbplatser, med en proxy mellan sig och ledningscentralen för att minska sannolikheten för att bli spårad.
- **Agerande**
  Mycket agerande går ut på att gå vidare i nät och därmed att börja om med det första steget (rekognoscering). Slutmålet är oftast att inhämta data, även om det också förekommer andra mål som att exempelvis ändra eller förstöra data.

Som helhet ger indelningen i steg en översikt över operationers tillvägagångssätt. Samtidigt är det rimligt att det är i operationernas detaljer de svårare delarna finns. Det är också möjligt att operationer snarare är mödosamma att utföra än svåra.

Några relevanta framtida forskningsfrågor är:

- Hur väl kan standardmässiga skydd stoppa generella typer av operationer?
- Är skydd verksamma mot enskilda steg av operationerna eller är skydden mer generella varför sättet att dela in operationer med LMCKC är mer lämpat för att förstå angrepp snarare än försvar?
- Hur förhåller sig LMCKC med andra sätt att modellera operationer, såsom attackträd?

7.3 Sofistikation

Cyberoperationer kallas ofta sofistikerade utan att det anges vad det är som gör dem sofistikerade. Många aktörer som uttalar sig har dessutom något att vinna på att operationerna ses som sofistikerade. Operationer som bygger på tämligen vanliga angreppssätt som nätfiske och utnyttjande av välkända sårbarheter bör knappast ses som sofistikerade. Men bland de kända statsstödda cyberoperationerna använder en stor del sådana enklare typer av tillvägagångssätt. Med andra ord verkar inte statsstödet i sig nödvändigtvis resultera i mer sofistikerade operationer. Det är också oklart hur stater vill agera i cyberdomänen. Kanske har de inget större intresse av att utföra svåra, riktade och långsiktiga operationer. Några frågor som därför behöver besvaras är:

- Hur kan det avgöras hur riktad en operation var tänkt att vara?
- Hur riktade operationer vill stater utföra och i vilken utsträckning bryr de sig om sidoskador i cyberdomänen?
- Hur enkelt är det att begränsa ett cybervapens verkan till ett fåtal system?
- I vilken mån används mekanismer (som självförstöring eller målsökning) som hindrar att redan använda vapen används för ytterligare ändamål?
- Hur långsiktigt agerar stater i cyberdomänen?
- Utförs statsstödda cyberoperationer bäst av paramilitära organisationer, militära förband, militära specialförband eller underrättelsetjänster? Har alla varianterna med utförare sina användningsområden?
- I vilken utsträckning kan färdiga cybervapen köpas in?
    - Kan man få vapnen anpassade?
    - Var går skiljelinjen mellan vapen och försvarssystem?
    - Vem har inflytande över tillverkarna?

- Vad kan man säga om operationer som inte upptäckts, det vill säga mörkertalet som förmodligen är de mest sofistikerade cyberoperationerna?

8 Referenser

Ablon, L., Libicki, M. 2014. Markets for Cybercrime Tools and Stolen Data, Hackers' Bazaar. *RAND*.

Ahmed, B. A., Perlroth, N. 2019. Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families. *New York Times*. Hämtad från https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html

Aitel, D. 2016. Useful Fundamental Metrics for Cyber Power. *CyberSecPolitics*. Hämtad från https://cybersecpolitics.blogspot.com/2016/06/useful-fundamental-metrics-for-cyber.html

Allodi, L. 2015. The Heavy Tails of Vulnerability Exploitation. *7th International Symposium on Engineering Secure Software and Systems*.

Allodi, L., Massacci, F., Williams, J. 2017. The Work-Averse Cyber Attacker Model: Theory and Evidence From Two Million Attack Signatures.

Atch, D., Neray, P. 2017. Operation BugDrop: CyberX Discovers Large-Scale Cyber-Reconnaissance Operation Targeting Ukrainian Organizations. *CyberX Labs*. Hämtad från https://cyberx-labs.com/en/blog/operation-bugdrop-cyberx-discovers-large-scale-cyber-reconnaissance-operation/

Bartholomew, B., Guerrero-Saade, J. A. 2016. Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks. *Virus Bulletin*, vol. oktober. Hämtad från https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Bartholomew-GuerreroSaade.pdf

Berghel, H. 2017. On the Problem of (Cyber) Attribution. *Computer*, vol. 50:3.

Betz, D., Stevens, T. 2012. Cyberspace and the State. Toward a Strategy for Information.

Boebert, E. 2010. *A Survey on Challenges in Attribution. Proceedings of a Workshop on Deterring Cyberattacks*. National Academies Press.

Boot, C. 2019. *Applying Supervised Learning on Malware Authorship Attribution*. Radboud University Nijmegen.

Buchanan, B. 2017. The Legend of Sophistication in Cyber Operations. *The Cyber Security Project. Harvard Kennedy School. Belfer Center.*, 30.

Hämtad från https://www.belfercenter.org/sites/default/files/files/publication/Legend Sophistication - web.pdf

Burgess, M. 2017. WikiLeaks drops' Grasshopper' documents, part four of its CIA Vault 7 files. *Wired*. Hämtad från https://www.wired.co.uk/article/cia-files-wikileaks-vault-7

Caliskan, A., Yamaguchi, F., Dauber, E., Harang, R., Rieck, K., Greenstadt, R., Narayanan, A. 2018. When Coding Style Survives Compilation: De-anonymizing Programmers from Executable Binaries. In *Network and Distributed Systems Security (NDSS) Symposium*.

C4I, IDF., Naor, I. 2017. Breaking The Weakest Link Of The Strongest Chain. Securelist, *Kaspersky*. Hämtad från https://securelist.com/breaking-the-weakest-link-of-the-strongest-chain/77562/

Casey, T. 2007. Threat Agent Library. *Intel*, vol. september.

CFR. 2019. Cyber Operations Tracker. *Coouncil on Foreign Relations*. Hämtad från https://www.cfr.org/interactive/cyber-operations

Chen, P., Desmet, L., Huygens, C. 2014. A Study on Advanced Persistent. *International Conference on Communications and Multimedia Security*.

Cherepanov, A. 2017. TeleBots are back: Supply‑chain attacks against Ukraine. *Eset*. Hämtad från https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/

Chernenko, E., Demidov, O., Lukyanov, F. 2018. Increasing international cooperation and cybersecurity and adapting cyber norms. *Council on Foreign Relations*. Hämtad från www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

Cho, S., Han, I., Jeong, H., Kim, J., Koo, S., Oh, H., Park, M. 2018. Cyber kill chain based threat taxonomy and its application on cyber common operational picture. *2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2018*.

Clark, D. D., Landau, S. 2010. The Problem isn't Attribution; It's Multi-Stage Attacks. *ACM ReArch*.

Cook, A., Nicholson, A., Janicke, H., Maglaras, L., Smith, R. 2016. Attribution of Cyber Attacks on Industrial Control Systems. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 3:7, 151158.

Crone, I. 2019. Enhanced Attribution. *DARPA*. Hämtad från https://www.darpa.mil/program/enhanced-attribution

Darpa. 2016a. Broad Agency Announcement Enhanced Attribution. DARPA-BAA-16-34.

Darpa. 2016b. DARPA ‐ BAA ‐ 16 ‐ 34.

Davis, J., Boudreaux, B., Welburn, J., Aguirre, J., Ogletree, C., McGovern, G., Chase, M. 2017. *Stateless Attribution: Toward International Accountability in Cyberspace*. *RAND*.

Defense Science Board. 2013. TASK FORCE REPORT: Resilient Military Systems and the Advanced Cyber Threat. *Department of Defense, USA*.

DePaula, N., Goel, S. 2016. A Sophistication Index for Evaluating Security Breaches. *Symposium on Information Assurance*, vol. 11.

Duggan, D. P., Thomas, S. R., Veitch, C. K. K., Woodard, L. 2007. Categorizing Threat: Building and Using a Generic Threat Matrix. *SANDIA Report*, vol. september.

Eriksson, A. E., Fylkner, M. 2000. IT-relaterade hot i nätverkssamhället-förslag till en svensk proaktiv agenda. *Försvarets forskningsanstalt.* FOA-R—00-01459-170-SE.

Fagerland, S., Grange, W. 2014. The Inception Framework: Cloud-hosted APT. *Blue Coat Systems*. Hämtad från papers3://publication/uuid/9895E08F-CDA5-45C3-BDB0-F768F3652BDF

Farral, T. 2017. The attribution problem with information security attacks. *Network Security*, vol. 5.

Finifter, M., Akhawe, D., Wagner, D. 2013. An Empirical Study of Vulnerability Rewards Programs. *Proceedings of the 22nd USENIX Security Symposium*. Hämtad från https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf

FireEye. 2017. Threat Research, APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat. Hämtad från https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

Floyd, G. S. 2018. Attribution and Operational Art : Implications for Competing in Time. *Strategic Studies Quarterly*, vol. 12:2.

Fokker, J., Beek, C. 2019. Ryuk Ransomware Attack: Rush to Attribution Misses the Point. *McAfee Blogs*. Hämtad från https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-to-attribution-misses-the-point/

Franke, U., Johansson, F., Jändel, M. 2012. Tekniker för analys av data från webben Tekniker för analys av data från webben. *Totalförsvarets forskningsinstitut.* FOI-R--3532--SE.

Fylkner, M., Grennert, J., Mittermaier, E. 2000a. Internationellt samarbete kring IT-hot; Aktörer och initiativ - några exempel. *Försvarets forskningsanstalt.* FOA-R—00-01517-170-SE.

Fylkner, M., Grennert, J., Mittermaier, E. 2000b. Internationellt samarbete kring IT-hot: Om vad? Mellan vilka? Hur?. *Försvarets forskningsanstalt.* FOA-R—00-01518-170-SE.

Fylkner, M., Carlsen, H., Lewerentz, B. 2003. Det kvalificerade IT-hotet - vad säger experterna? En empirisk studie om samtida hot och sårbarheter i nätverkssamhället. *Totalförsvarets forskningsinstitut.* FOI-R--1105--SE.

Fylkner, M., Carlsen, H., Lewerentz, B., Eriksson, A.E. 2004. Aktörer, antagonister och angrepp - En studie om det kvalificerade IT-hotet. *Totalförsvarets forskningsinstitut.* FOI-R--1182--SE.

Förenade Nationerna, Department of Economic and Social Affairs, Population Division (2019). World Population Prospects 2019, Online Edition. Rev. 1.

Goeij, H. de. 2017. Czech Government Suspects Foreign Power in Hacking of Its Email. *The New York Times*. Hämtad från https://www.nytimes.com/2017/01/31/world/europe/czech-government-suspects-foreign-power-in-hacking-of-its-email.html?_r=1%0A

Great. 2017a. Introducing WhiteBear. *Securelist, Kaspersky*. Hämtad från https://securelist.com/introducing-whitebear/81638/%0A

Great. 2017b. Unraveling the Lamberts Toolkit, An Overview of a Color-coded Multi-Stage Arsenal. *Kaspersky*. Hämtad från https://securelist.com/unraveling-the-lamberts-toolkit/77990/

Great. 2017c. Lazarus Under The Hood. *Kaspersky*. Hämtad från https://securelist.com/lazarus-under-the-hood/77908/

Grennert, J., Tham, M. 2001. Att påverka konflikter med IT-vapen: Icke-statliga aktörers möjligheter till inverkan på konfliktförlopp. *Totalförsvarets forskningsinstitut.* FOI-R--0263--SE.

Grosse, E. 2012. Security warnings for suspected state-sponsored attacks. *Google Security Blog*.

Guitton, C., Korzak, E. 2013. The Sophistication Criterion for Attribution: Identifying the Perpetrators of Cyber-Attacks. *RUSI Journal*, vol. 158:4.

Haaster, J. van. 2016. Assessing cyber power. *International Conference on Cyber Conflict*.

Hegel, T. 2018. Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers. *401Trg*. Hämtad från https://401trg.pw/burning-umbrella/

Hewlett Packard Enterprise. 2014. HP Attack Life Cycle use case methodology.

Higbee, A. 2013. Defining a Sophisticated Attack. *Cofense*. Hämtad från https://cofense.com/defining-a-sophisticated-attack/

Holm, H., Sommestad, T. 2017. So long, and thanks for only using readily available scripts. *Information and Computer Security*, vol. 25:1.

Holm, H. 2018. Arbete utfört inom ÖvExCND under 2018. *Totalförsvarets forskningsinstitut.* FOI Memo 6541.

Homewood, B. 2017. IAAF says medical records compromised by Fancy Bear hacking group. *Reuters*. Hämtad från http://www.reuters.com/article/us-sport-doping-iaaf-idUSKBN1750ZM%0A

Howell O'Neill, P. 2017. Previously unknown cyber-espionage group has successfully hacked in South America since 2015. *Cyberscoop*. Hämtad från https://www.cyberscoop.com/previously-unknown-cyber-espionage-group-successfully-hacked-south-america-since-2015/

Huang, Z., Shen, C. C., Doshiy, S., Thomasy, N., Duong, H. 2015. Difficulty-level metric for cyber security training. *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision*.

Huetteman, E. 2017. Marco Rubio Says His Campaign Was a Target of Russian Cyberattacks. *The New York Times*. Hämtad från https://www.nytimes.com/2017/03/30/us/politics/marco-rubio-russian-cyberattacks.html%0A

Hutchins, E., Cloppert, M., Amin, R. 2011. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *6th International Conference on Information Warfare and Security, ICIW 2011*.

Illinois. 2018. 2018 WL 4941760 (Ill.Cir.Ct.) (Trial Pleading) Circuit Court of Illinois. MONDELEZ INTERNATIONAL, INC., Plaintiff, v. ZURICH AMERICAN INSURANCE COMPANY, Defendant.

Johansson, F., Kaati, L., Isbister, T. I. M., Litsegård, P. 2016. Avanonymisering i sociala medier. *Totalförsvarets forskningsinstitut.* FOI-R--4293--SE.

Jolley, J. D. 2017. *Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law*. University of Glasgow.

Karlzén, H., Granlund, H., Wedlin, M. 2018. Operationer i cyberdomänen, En inventering av svensk forskning, *Totalförsvarets forskningsinstitut*. FOI-R--4594--SE.

Karlzén, H. Lindahl, D. 2019. Operationer i cyberdomänen, En inledande forskningsplan. *Totalförsvarets forskningsinstitut.* FOI-R--4686--SE.

Karresand, M. 2001. TEBIT Teknisk Beskrivningsmodell för IT-vapen. *Totalförsvarets forskningsinstitut.* FOI-R--0305--SE.

Karresand, M. 2003. A Proposed Taxonomy of Software Weapons. *Totalförsvarets forskningsinstitut.* FOI-R--0840--SE.

Karresand, M., Persson, M., Lindahl, D. 2004. Scenarion och trender inom framtida informationskrigföring ur ett tekniskt perspektiv. *Totalförsvarets forskningsinstitut.* FOI-R--1283--SE.

Karresand, M., Persson, M. 2006. Strid i IT-domänen. *Totalförsvarets forskningsinstitut.* FOI-R--2192--SE.

Karresand, M., Hunstad, A. 2009. Försvar av IT-system. *Totalförsvarets forskningsinstitut.* FOI-R--2921--SE.

Kearns, E.M. 2019. When to Take Credit for Terrorism? A Cross-National Examination of Claims and Attributions. *Terrorism and Political Violence*.

Keromytis, A. 2016. Enhanced Attribution. *DARPA*. Hämtad från https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/enhanced-attribution/

Kinas utrikesdepartement. 2015a, 5 juni. Foreign Ministry Spokesperson Hong Lei's Regular Press Conference. *Ministry of Foreign Affairs, the People's Republic of China*.

Kinas utrikesdepartement. 2015b, 10 juli. Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference. *Ministry of Foreign Affairs, the People's Republic of China*.

Kirchgaessner, S. 2017. Russia suspected over hacking attack on Italian foreign ministry. *The Guardian*. Hämtad från https://www.theguardian.com/world/2017/feb/10/russia-suspected-over-hacking-attack-on-italian-foreign-ministry

Kjaerland, M. 2006. A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers and Security*, vol. 25:7.

Lancaster, T. 2017. Muddying the Water : Targeted Attacks in the Middle East. *Palo Alto Networks*. Hämtad från https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/%0A

Langner, R. 2013. To Kill a Centrifuge. *The Langner Group*.

Lin, H. 2016. Attribution of Malicious Cyber Incidents. *A HOOVER INSTITUTION ESSAY. Aegis Paper Series*, vol. 1607. Hämtad från https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf

Lindahl, D., Persson, M., Vidström, A., Wedlin, M. 2003. Triops, prototyp för IT-vapen. *Totalförsvarets forskningsinstitut.* FOI-R--0843--SE.

Lindahl, D., Westerdahl, L. 2014. RPAS och cybersäkerhet. *Totalförsvarets forskningsinstitut.* FOI-R--4046--SE.

Lockheed Martin. 2006. Gaining the advantage?, vol. 60:1.

Malik, W. 2017. What are the benefits of attribution? *TrendMicro*.

Malone, S.T. 2016. Using an expanded cyber kill chain model to increase attack resiliency. *Black Hat*.

Marczak, B. 2017. Champing at the Cyberbit. *The Citizen Lab*. Hämtad från https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/%0A

Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., Frye, J. 2012. Cyber Threat Metrics. *SANDIA Report. SAND2012-2427*, vol. mars.

Miller, C. 2007. The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales. *Independent Security Evaluators*. Hämtad från http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.139.5718

Minerva och ClearSky. 2015. CopyKittens Attack Group. *Minerva Labs och ClearSky Cyber Security.* Hämtad från https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf

Mirkovic, J., Reiher, P. 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. *Computer Communication Review*, vol. 34:2.

Mitre. 2019a. Pre-att&ck. Hämtad från https://attack.mitre.org/resources/pre-introduction/

Mitre. 2019b. PRE-ATT&CK Tactics. Hämtad från https://attack.mitre.org/tactics/pre/

Mitre. 2019c. Common Attack Pattern Enumeration and Classification. CAPEC VIEW: Mechanisms of Attack. Hämtad från https://capec.mitre.org/data/definitions/1000.html

Mitre. 2019d. ATT&CK Matrix for Enterprise. Hämtad från https://attack.mitre.org/

Mueller, M., Grindal, K., Kuerbis, B., Badiei, F. 2019. Cyber Attribution. *The Cyber Defense Review*, vol. 4:1.

Neutze, J. 2016. The role of cybernorms in preventing digital warfare. *Microsoft EU Policy Blog*. Hämtad från https://blogs.microsoft.com/eupolicy/2016/07/08/the-role-of-cybernorms-in-preventing-digital-warfare/

Newman, L. 2017. Iranian Hackers Have Been Infiltrating Critical Infrastructure Companies. *Wired*. Hämtad från https://www.wired.com/story/apt-34-iranian-hackers-critical-infrastructure-companies/%0A

Nicholson, A., Janicke, H., Watson, T., Smith, R. 2015. Rolling the Dice - Deceptive authentication for attack attribution. *Proceedings of the 10th International Conference on Cyber Warfare and Security, ICCWS 2015*.

NIST. 2011. NIST Special Publication 800-39, Managing Information Security Risk Organization, Mission, and Information System View. *Nist Special Publication*, vol. mars. Hämtad från http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

Noor, M., Kteily, N., Siem, B., Mazziotta, A. 2018. "Terrorist" of "Mentally Ill": Motivated biases rooted in partisanship shape attributions about violent actors. *Social Psychological and Personality Science*.

Nye, J.S. 2010. Cyber Power. *Cambridge: Harvard Kennedy School Belfer Center for Science and International Affairs.*

ODNI, Office of the director of national intelligence. 2018. A Guide to Cyber Attribution.

O'Leary, J., Kimble, J., Vanderlee, K., Fraser, N. 2017. Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors

and has Ties to Destructive Malware. *FireEye*. Hämtad från https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html%0A

Ottis, R. 2009. Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability. *European Conference on Information Warfare and Security*.

Pahi, T., Skopik, F. 2019. Cyber Attribution 2.0 : Capture the False Flag. *European Conference on Cyber Warfare and Security*.

Perlroth, N., Shane, S. 2017. How Israel Caught Russian Hackers Scouring the World for U.S. Secrets. *New York Times*. Hämtad från https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html?_r=0

Piper, S. 2013. *Definitive Guide to Next-Generation Threat Protection*.

Pitropakis, N., Panaousis, E., Giannakoulias, A., Kalpakis, G., Rodriguez, R. D., Sarigiannidis, P. 2018. An enhanced cyber attack attribution framework. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11033 LNCS*.

Porter, C. 2017. Private Sector Cyber Intelligence Could Be Key to Workable Cyber Arms Control Treaties. *Lawfare*. Hämtad från https://www.lawfareblog.com/private-sector-cyber-intelligence-could-be-key-workable-cyber-arms-control-treaties

PWC. 2017. Operation Cloud Hopper. *PwC*. Hämtad från www.pwc.co.uk/cyber%0Ahttps://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

Reaqta. 2017. A dive into MuddyWater APT targeting. *Reaqta*. Hämtad från https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/%0A

Reyes, G., Adams, D., Cooper, J., Camacaro, D. 2017. EXCLUSIVE: Panama’s expresident wiretapped Americans, according to court documents. *Univision*. Hämtad från https://www.univision.com/univision-news/latin-america/exclusive-panamas-ex-president-wiretapped-americans-according-to-court-documents%0A

Rid, T., Buchanan, B. 2015. Attributing Cyber Attacks. *Journal of Strategic Studies*, vol.38:1–2.

Romanosky, S., Boudreaux, B. 2019. Private Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government. *National Security Research Division. RAND*, vol. februari.

Rosenbaum, B. R. 2012. Richard Clarke on Who Was Behind the Stuxnet Attack. *Smithsonian Magazine*.

Schmitt, M., Vihul, L. 2017. International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms. *Just Security*. Hämtad från https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/

Secureworks. 2017. BRONZE BUTLER Targets Japanese Enterprises. *Secureworks*. Hämtad från https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses%0A

Seebruck, R. 2015. A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation*, vol. 14.

Seibt, S. 2017. Cyber experts "99% sure" Russian hackers are targeting Macron. *France 24*. Hämtad från http://www.france24.com/en/20170426-france-macron-cyber-security-russia-presidential-campaign%0A

Shakarian, P., Simari, G. I., Moores, G., Parsons, S. 2015. Cyber attribution: An argumentation-based approach. *Advances in Information Security*, vol. 56.

Shamsi, J. A., Zeadally, S., Sheikh, F., Flowers, A. 2016. Attribution in cyberspace: techniques and legal implications. *Security and Communication Networks*, vol. 9:15.

SOU 2011:76. 2011. Våld och tvång under internationella militära insatser. Betänkande av Fredsinsatsutredningen. *Statens Offentliga Utredningar*.

Stamos, A. 2015. Notifications for targeted attacks. *Facebook.Com*. Hämtad från https://www.facebook.com/notes/facebook-security/notifications-for-targeted-attacks/10153092994615766?_fb_noscript=1

Stevens, T. 2017. Cyberweapons: Power and the governance of the invisible. *International Politics*.

Symantec. 2017a. WannaCry: Ransomware attacks show strong links to Lazarus group. *Symantec*. Hämtad från https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

Symantec. 2017b. Longhorn: Tools used by cyberespionage group linked to Vault 7. Hämtad från https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7

Symantec. 2018. The Cyber Security Whodunnit: Challenges in Attribution of Targeted Attacks. Hämtad från https://www.symantec.com/blogs/expert-perspectives/cyber-security-whodunnit-challenges-attribution-targeted-attacks

Tableau. 2019. VERIS Community Database (VCDB). Hämtad från https://public.tableau.com/profile/jay.jacobs#!/vizhome/vcdb/Overview

ThreatConnect. 2017a. Fancy Bear Pens the Worst Blog Posts Ever. *ThreatConnect*. Hämtad från threatconnect.com/blog/fancy-bear-leverages-blogspot

ThreatConnect. 2017b. Parlez-vous Fancy? *ThreatConnect*. Hämtad från threatconnect.com/blog/activity-targeting-french-election

Toon, J. 2019. $ 17 Million Contract Will Help Establish Science of Cyber Attribution. *GATech*. Hämtad från https://rh.gatech.edu/news/584327/17-million-contract-will-help-establish-science-cyber-attribution

Tsagourias, N. 2012. Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, vol. 17:2.

Tsyrklevich, V. 2015. Hacking Team: a zero-day market case study Vitaliy Toropov. Hämtad från https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/

United States Department of Defense. 2018. Cybersecurity Test and Evaluation Guidebook Version 2.0.

Utrikespolitiska institutet. Landguiden. Hongkong. 2019. Hämtad från https://www.ui.se/landguiden/lander-och-omraden/asien/hongkong/

Wedlin, M., 2005. CNA-scenarier ur ett tekniskt perspektiv. *Totalförsvarets forskningsinstitut.* FOI-R--1620--SE.

Wheeler, D. A., Larsen, G. N., Leader, T. 2003. Techniques for cyber attack attribution. *Institute for Defense Analyses*, vol. oktober. Hämtad från https://apps.dtic.mil/dtic/tr/fulltext/u2/a468859.pdf%0Ahttp://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA468859

Vidström, A. 2012. Möjligheter och problem vid analys av fientlig kod riktad mot Siemens S7-serie. *Totalförsvarets forskningsinstitut.* FOI-R--3567--SE.

Willett, M. 2019. Assessing cyber power. *Survival, vol. 61:*1.

Winkler, I. 2015. The ‘sophisticated attack’ myth. *Computerworld*.

Volz, D. 2017. Trump Signs into Law U.S. Government Ban on Kaspersky Lab Software. *Reuters*. Hämtad från https://uk.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUKKBN1E62V4

Yadron, D. 2015. When Cybersecurity Meets Geopolitics. *Wall Street Journal*. Hämtad från https://blogs.wsj.com/digits/2015/03/23/when-cybersecurity-meets-geopolitics/

Zeng, W., Germanos, V. 2019. Modelling Hybrid Cyber Kill Chain. *CEUR Workshop Proceedings*. Hämtad från http://ceur-ws.org/Vol-2424/paper10.pdf

Zouave, E. 2019. Aktiva operationer på cyberdomänen Aktiva operationer på cyberdomänen. *Totalförsvarets forskningsinstitut.* FOI-R--4776--SE.

Ånäs, P. 2001. Aktören vid IT-relaterade attacker - vem, varför och hur?. *Totalförsvarets forskningsinstitut.* FOI-R--0271--SE.