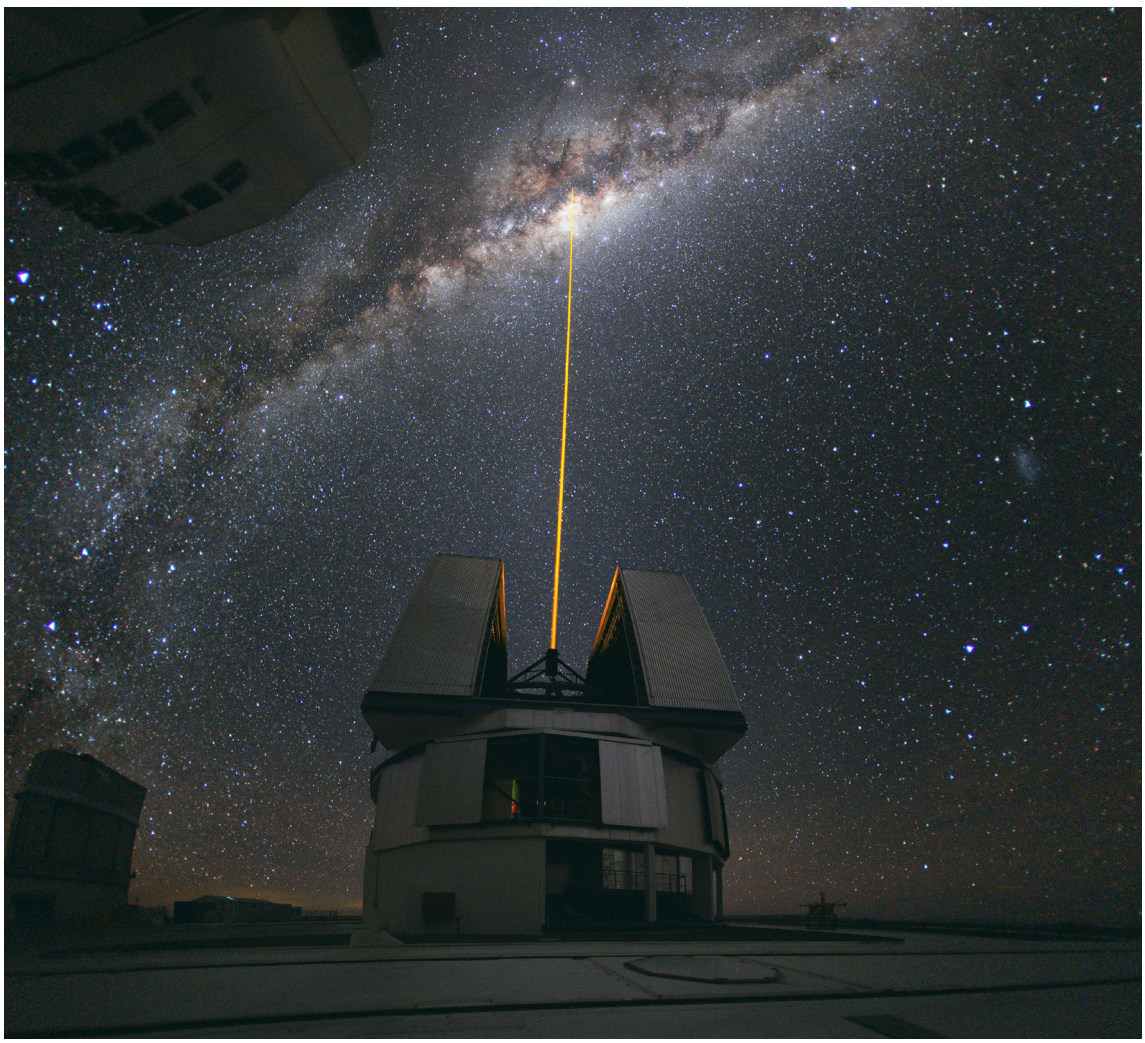
FOI

Cyberoperationer

En slutrapport

HENRIK KARLZÉN



FOI-R--5072--SE
ISSN 1650-1942 December 2020

Henrik Karlzén

Cyberoperationer

En slutrapport

Titel	Cyberoperationer – En slutrapport
Title	Cyber operations – A final report
Rapportnr/Report no	FOI-R--5072--SE
Månad/Month	December
Utgivningsår/Year	2020
Antal sidor/Pages	44
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	Informationssäkerhet
FoT-område	Operationer i cyberdomänen
Projektnr/Project no	E72887
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Bild/Cover: ESO/Y. Beletsky

Sammanfattning

Cyberoperationer utgörs av militärt agerande som syftar till att påverka cyberdomänen och därmed nå en bestämd målsättning. Agerandet kan vara både defensivt och offensivt. Rapporten utgör en slutrapport för det projekt om cyberoperationer som utförts vid FOI åren 2017–2020 åt Försvarsmakten. Fokus ligger därför på Försvarsmaktens behov av ökad förmåga att utföra cyberoperationer.

Rapporten sammanfattar projektbakgrunden och det arbete som utförts i projektet, inklusive rapporter, memon, forskningsartiklar och webbinarier. Sex forskningsfrågor besvaras och framtida forskningsmöjligheter föreslås. Nedan ges en sammanfattning av rapportens slutsatser.

Forskningen om modellering på området är ganska begränsad. Ofta fokuserar modellerna på tekniskt arbete och är förenklade så att operationer sker i steg utan cykler, med inslag av manuell styrning under tiden samt med generella syften.

Att uppnå situationsförståelse på området är svårt på grund av att tekniska delar måste sammanföras med organisatorisk ledning. Det är också svårt att attribuera genomförda operationer eftersom aktörer inte är öppna med vad de gör. Utpekanden av angripare efter angrepp verkar göras på svag grund.

Cyberoperationer verkar i huvudsak handla om underrättelseinhämtning. Cybersabotage är ovanligare vilket kan bero på att sabotage är enklare att utföra utanför cyberdomänen. I öppna källor framgår att en stor del av cyberoperationernas offer hör hemma i USA, vilket kan bero på att det där finns attraktiva mål eller att källorna fokuserar på USA.

Cyberoperationer beskrivna i öppna källor verkar inte ha krävt så mycket sofistikation för att utföra. Men det kan finnas ett mörkertal av sofistikerade operationer som inte upptäcks. Källorna tyder i alla fall på att det främst är resursstarka och mogna organisationer som utför operationer.

Cyberoperationer kan på teknisk nivå övas i cyberanläggningar. Avsaknaden av data om riktiga cyberoperationer ger dock begränsningar i realismen. Det är dessutom en utmaning att kombinera tekniska övningar med diskussionsövningar på ledningsnivå.

Folkrättsligt saknas klara regler för vad som är tillåtet i cyberdomänen även om sammanslutningar som EU och Nato börjat ta fram egna regler och tolkningar. En svårighet är att militära och civila cybersystem ofta är sammanflätade varför det i cyberdomänen saknas klara distinktioner mellan vad som är militärt och vad som är civilt.

Nyckelord: cyberdomän, cyberoperation, cybersäkerhet, cyberförmåga, cyberförsvar

Summary

Cyber operations consist of military actions aiming to affect the cyber domain and thereby reaching a specific goal. The actions can be both defensive and offensive. The report constitutes a final report for the project on cyber operations carried out at FOI in the years 2017–2020 for the Swedish Armed Forces. The focus is therefore on the Swedish Armed Forces' need for increased capability to conduct cyber operations.

The report summarises the project background and the work carried out in the project, including reports, memos, research papers, and webinars. Six research questions are answered and future research opportunities are suggested. Below is a summary of the report’s conclusions.

Research on modelling in this area is limited. The models often focus on technical work, and are simplified so that the operations occur in steps without cycles, with elements of manual control, and for general purposes.

Achieving situation awareness in the area is difficult because technical parts must be combined with organisational management. It is also difficult to attribute performed operations since actors are not open about what they do. Designations of attackers after attacks seem to be made on weak basis.

Cyber operations seem mainly to be about intelligence gathering. Cyber sabotage is less common which may be due to sabotage being easier to perform outside the cyber domain. Open sources reveal that a large part of the cyber operations victims belong to the U.S.A., which may reveal their targets attractiveness, or the focus of the sources used.

Cyber operations described in open sources do not seem to have required much sophistication, but there may be undetected operations that are sophisticated. In any case, the sources indicate that cyber operations are mainly performed by resourceful and mature organisations.

Cyber operation exercises can be staged at the technical level in cyber ranges. However, the lack of data on real cyber operations limits the realism. Furthermore, it is a challenge to combine technical exercises with discussion based tabletop exercises at the command and control level.

Under international law, there are no clear rules for what is allowed in the cyber domain, even though associations such as the EU and NATO have begun to develop their own rules and interpretations. Military and civilian cyber systems are often intertwined, resulting in unclear distinctions between the two.

Keywords: cyber domain, cyber operation, cyber security, cyber capability, cyber defence

Innehållsförteckning

1 Inledning 8
1.1 Läsanvisning 9
2 Bakgrund 10
2.1 Omvärlden och svensk försvarsinriktning 10
2.2 Relaterad FOI-forskning 11
2.3 Inventering av svensk forskning 15
2.4 Inventering av internationell forskning 16
2.5 Inledande forskningsplan 17
3 Projektresultaten 19
3.1 Folkrättslig utveckling 20
3.2 Modellering och simulering av effekter 21
3.3 Offensiv modell 21
3.4 Attribution, tillvägagångssätt och sofistikation 22
3.5 Övningen SAFE Cyber 2019 25
3.6 Cyberoperationer som genomfördes 2019 26
3.7 Standardisering för modellering och simulering 26
3.8 Svenska definitioner 26
3.9 Simulering av effekter 27
3.10 Informationselement i incidentrapporter 27
3.11 Cyberoperationer som genomfördes 2020 27
3.12 Webbinarier 28
3.13 Samarbeten 28
3.14 Kommande resultat 29
4 Slutsatser 30
4.1 Hur modelleras aktiv cyberförmåga? 30
4.2 Hur ska situationsförståelse som möjliggör effektivt beslutsfattande kopplat till cyberoperationer uppnås? 31
4.3 Vad kan man förvänta sig för effekt av en typisk cyberoperation? 32
4.4 Vilka kompetenser, metoder, tekniker och verktyg krävs för att utföra cyberoperationer? 34

4.5 Hur kan tester, övningar och utbildningar nyttjas för att öka, utveckla, vidmakthålla och värdera önskade förmågor i cybermiljön? 35

4.6 Vad finns det för problematik kopplat till etik, juridik och folkrätt avseende operationer i cyberdomänen? 36

5 Referenser 38

5.1 Publicerat i projektet 38

5.2 Övriga referenser 39

1 Inledning

Försvarsmakten har ett uttalat behov av att öka sin förmåga att utföra operationer i cyberdomänen, så kallade cyberoperationer (Försvarsutskottet, 2015). Enligt Försvarsmaktens *Doktrin för Gemensamma operationer* är cyberdomänen en del av informationsmiljön som består av bland annat IT-system, datornätverk och tillhörande information (Försvarsmakten, 2020). Det är därför rimligt att se cyberoperationer som en variant av informationsoperationer, vilka definieras i samma källa. En tolkning är därför att en cyberoperation utgörs av militärt agerande som syftar till att påverka cyberdomänen och därmed nå en bestämd målsättning. Agerandet kan vara både defensivt och offensivt (Försvarets radioanstalt och Försvarsmakten, 2016). Inom cybersäkerhetsområdet är fokus ofta på att en angripare försöker ta sig in i ett system medan försvararna försöker motstå angreppet. Sådana angrepp och försvar kan ingå i en cyberoperation. Men en cyberoperation kan också inkludera tekniska, organisatoriska och underrättelsemässiga förberedelser för angrepp eller försvar samt bestå av kedjor av händelser med flera angrepp och flera försvarsinsatser. Dessutom kan cyberoperationer också bestå av agerande som sker utanför cyberdomänen. På liknande sätt kan cyberoperationer ha effekter utanför cyberdomänen, utöver de effekter som sker i cyberdomänen. Det bör observeras att begreppsanvändningen på området är ung snarare än väletablerad. Ett snarlikt begrepp är dator- och nätverksoperation (eng. Computer Network Operation, CNO) (Försvarets radioanstalt och Försvarsmakten, 2016).

Denna rapport utgör en slutrapport för det projekt om cyberoperationer som genomförts vid FOI åren 2017–2020 inom ramen för Försvarsmaktens samlingsbeställning av forskning och teknikutveckling (FoT). Rapporten sammanfattar projektbakgrunden, det arbete som utförts, de slutsatser som kan dras och vilka framtida forskningsmöjligheter som finns.

Projektet har utgått från sex forskningsfrågor:

1. Hur modelleras aktiv cyberförmåga?
2. Hur ska situationsförståelse 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?

De fem första forskningsfrågorna utgår från den ursprungliga beställningen. Den sista forskningsfrågan har sitt ursprung i en utvidgning som gjordes under projektets genomförande. Detta beskrivs i memot *Utveckling av forskningsområde Operationer i cyberdomänen* (Wedlin m.fl., 2017). Memot ger också en skiss för projektet och förklarar bakgrund och syfte. Dessutom beskrivs grundläggande definitioner och några preliminära resultat.

Under projektet visade det sig snabbt att forskningsområdet cyberoperationer är brett och tvärvetenskapligt (Karlzén och Lindahl, 2019). Exempelvis samsas tekniska aspekter med verksamhetsprocesser och samhällseffekter. FOI:s projektgrupp har på liknande sätt haft en bred kompetens. Den breda kompetensen möter forskningsområdets bredd samtidigt som det kan vara en utmaning för projektmedlemmarna att förstå varandras synvinklar.

Något som begränsat studierna av ämnet är svårigheten att få tag i tillförlitliga data om genomförda cyberoperationer. De som utför operationerna vill typiskt hålla dem hemliga medan den som drabbas av dem inte gärna vill avslöja detaljer om vilka sårbarheter som användes eller vilka effekter operationerna gav (eller ens erkänna att operationerna drabbade dem). De data om (påstått) genomförda cyberoperationer som använts i projektet har i huvudsak bestått av databasen Cyber Operations Tracker[1] vilket är den mest kompletta vad gäller statsstödda operationer. Databasen bygger på källor som till stor del utgörs av nyhetsartiklar och cybersäkerhetsföretags rapporter. Även dessa källor har legat till grund för projektresultaten. Utöver dessa data har projektresultaten tagits fram utifrån analyser av akademiska forskningsartiklar och studier i samband med cyberförsvarsövningar.

1.1 Läsanvisning

Kapitel 2 ger en kortfattad bakgrund om hur omvärlden förändrats det senaste dryga decenniet samt en inblick i den nya svenska försvarsinriktning som gett upphov till projektet Dessutom beskrivs relaterad forskning som genomförts utanför projektet.

Kapitel 2.3 sammanfattar de rapporter, memon, akademiska forskningsartiklar och annat som projektet producerat.

Kapitel 4 presenterar projektets slutsatser. Detta görs genom att de olika projektresultaten beskrivs indelat efter var och en av projektets sex forskningsfrågor. I samband med detta ges också förslag på nya forskningsfrågor som framtida forskning inom andra projekt kan besvara.

[1] https://www.cfr.org/cyber-operations

2 Bakgrund

I nästa avsnitt (2.1) beskrivs kortfattat hur omvärldsutvecklingen och svensk försvarsinriktning lett fram till detta projekt om cyberoperationer. Avsnittet därefter (2.2) beskriver FOI-forskning som är relaterad till forskningsområdet, men som utförts utanför projektet. Detta kompletteras i två följande avsnitt med forskning som utförts i Sverige (2.3) respektive internationellt (2.4). Till viss del syns FOI-forskningen även i dessa beskrivningar. Kapitlet avslutas med ett avsnitt (2.5) som beskriver en inledande forskningsplan för projektet.

2.1 Omvärlden och svensk försvarsinriktning

Begrepp med *cyber*[2] som prefix har populariserats av USA och enligt Försvarsberedningen (2013) använder majoriteten av världens länder begreppet *cybersäkerhet* i bemärkelsen att motstå IT-angrepp eller att hantera IT-incidenter.

USA:s militär har lagt mycket resurser på cyberdomänen de senaste femton åren. Exempelvis lanserades en ny cyberkrigsdoktrin 2008 (Harrington, 2008a) och samma år infördes nya utbildningar och karriärspår för cybersoldater (Harrington, 2008b samt Boleng m.fl., 2008). År 2010 tog ett cyberkommando form (U.S. Cyber Command, 2020) och samma år upptäcktes det välkända cybervapnet Stuxnet (Langner, 2013) vars användning ofta tillskrivs USA och Israel med iransk urananrikningsindustri som mål (Nakashima och Warrick, 2012).

En omfattande cyberoperation skedde 2007 mot Nato-medlemmen Estland (Fiorenza, 2007), vilken snabbade på etablerandet av ett Nato-ackrediterat cyberförsvarscentrum i Tallinn 2008, där Sverige nu är så kallad bidragande deltagare (eng. Contributing Participant; CCDCOE, 2020). Strax efter operationen tog dessutom internationell forskning om cyberoperationer fart, mätt i antal publicerade forskningsartiklar (Karlzén och Lindahl, 2019).

Begrepp med *cyber* är ovanligare i exempelvis Ryssland och Kina (Giles och Hagestad, 2013). Även om terminologin skiljer sig från västvärlden finns även där mycket aktivitet inom området, till exempel ryska statens arbete med att öka kontrollen över den trafik som kommer in eller lämnar landet, hur trafiken

[2] Prefixet *cyber* kommer av grekiskans ord för att styra (Arquilla och Ronfeldt, 1993) vilket i Försvarsmaktssammanhang kan sägas ingå i begreppet ledning. *Cyber* infördes i (bland annat) datavetenskapen 1948 när Wiener (1948) använde *cybernetics* för att beskriva samverkan mellan människa och maskin i form av kontroll och kommunikation.

dirigeras och oberoendet av (övriga) internet (Vendil Pallin, 2019a och 2019b; Kukkola m.fl., 2019).[3]

Även i Sverige har fokus på cyberförsvar ökat. Under rubriken cyberförsvar fick Försvarsmakten år 2015 instruktionen att bli bättre på att ”*förebygga, upptäcka, förhindra och aktivt hantera konsekvenserna av antagonistiska it-angrepp från kvalificerade statliga eller statsstödda aktörer…[inklusive att] genomföra aktiva operationer i cybermiljön”* (Försvarsdepartementet, 2015). Försvarsmakten har ökat sina satsningar på forskning i cyberdomänen (Försvarsmakten, 2018).

2.2 Relaterad FOI-forskning

I det här avsnittet beskrivs relaterad FOI-forskning som identifierats och som har koppling till forskningsområdet. De beskrivningar som getts i bakgrundavsnitten i projektets tidigare rapporter återanvänds till viss del.

2.2.1 Modeller för cybervapen

Karresand (2001; 2003) beskrev taxonomier för cybervapen. Lindahl m.fl. (2003) tog fram en prototyp för militära cybervapen och nämnde att vapnen borde utformas på ett modulärt sätt där de lätt kan förändras till skillnad från ett statiskt vapen som lätt blir föråldrat. Lindahl och Westerdahl (2014) beskrev cyberangrepps faser med underrättelseinhämtning, vapenutveckling och angrepp. På senare år har FOI utvecklat verktyget Lore och ramverket SVED för att möjliggöra automatisering av angrepp i övningar. Se även Holm (2018).

2.2.2 Situationsförståelse i cyberdomänen

Lundholm m.fl. (2011) beskrev tidig begreppslig förvirring om vad som kunde avses med lägesbild (dvs. situationsförståelse[4]) på informationsarenan och huruvida gemensam lägesbild avsåg att alla personer har samma lägesbild eller att en lägesbild sammanställts från varje arenas lägesbild.

Franke och Brynielsson (2014) genomförde den första systematiska genomgången av forskningslitteraturen om situationsförståelse i cyberdomänen. Det visade sig att mycket av forskningen varit inriktad på industriella styrsystem och på algoritmer för intrångsdetektion, medan en mindre andel forskning fokuserat på vilseledning, förståelse av angripares beteende och utvärdering av

[3] Sverige har det mindre långtgående målet att *”elektronisk kommunikation i Sverige ska vara tillgänglig oberoende av funktioner utanför landets gränser.”* (Regeringen, 2017)

[4] Ett annat likvärdigt begrepp är *lägesuppfattning*. På engelska blir det *situation awareness* eller *situational awareness*.

cyberstridsskador (effekter). Dessutom noterades det att mer empiri behövdes på området, vilket exempelvis kan byggas upp genom studier av övningar.

Schubert m.fl. (2016) studerade vilseledning, där falsk aktivitet uppvisas för att ge motståndaren felaktig situationsförståelse. Två exempel på detta inom cyberdomänen är honungsfällor (falska system som ser ut som riktiga system vilket lockar angripare som därmed upptäcks; eng. honeypots) och nätfiske (bedrägliga meddelanden). Snarlikt är också moving target defence (där systemet skyddas genom ständiga förändringar som gör att angriparen inte hinner identifiera var sårbarheter finns).

Vad gäller situationsförståelse och övningar föreslog Brynielsson m.fl. (2016) en metod för att sätta upp experiment för situationsförståelse inom ramen för cyberförsvarsövningar, exempelvis där de som övar ska identifiera vilka andra övande som angriper. Lif m.fl. (2017) tog i samband med övningar fram en metod för att mäta situationsförståelsen hos logganalytiker genom att till exempel studera vilka händelser analytikern trodde var angrepp och i så fall i vilken fas angreppet var i och vilka system som var drabbade. Severin (2018) undersökte förvarningar om ökad fientlig aktivitet (inte specifikt i cyberdomänen) och svårigheten i att avgöra när en reaktion krävs, när själva kriget inletts samt vilken uppdelning av olika roller och ansvar som är lämplig.

2.2.3 Cyberhotbilden

Mittermaier och Westrin (1999) studerade infrastrukturens sårbarhet rörande informationskrigföring och vad en angripare behöver veta om infrastruktursystemen för att kunna påverka dem. Grennert och Tham Lindell (2002) beskrev hotbilden mot Sverige vad gäller cyberterrorism. Fylkner m.fl. (2003) beskrev svenska cybersäkerhetsexperters syn på cyberhotbilden mot Sverige.

Intresserade läsare kan också läsa mer om cyberoperationer och svensk hotbild i den populärvetenskapliga texten *Internet som militär arena – en utmaning i totalförsvaret* av Wedlin och Westring (2017). På senare år har FOI dessutom beskrivit cyberhotbilden vad gäller cyberkriminalitet, där cyberdomänen utnyttjas för terrorism, bedrägeri, barnpornografi med mera. (se Wedlin m.fl., 2019).

2.2.4 Cyberaktörer

Ånäs (2001) beskrev en kategorisering av cyberangripare, med kategorier som syfte, organisationsstorlek, kompetens och etisk begränsning. Fylkner m.fl. (2004) tog fram en modell för värdering av aktörers förmåga att genomföra kvalificerade cyberangrepp. Heickerö (2006) beskrev olika aktörers drivkraft och resurser samt metoder, effekter och skydd. Senare beskrev Heickerö (2010) olika ryska cyberaktörer. Lindahl och Westerdahl (2014) studerade cyberangripares

särtecken och fann att cybersoldater agerar i enlighet med en långsiktig politisk agenda och på ett välunderrättat, resursstarkt och organiserat sätt.

2.2.5 Analys av cybervapen

Vidström beskrev analys av ett upptäckt virus (2002) och analyserade skadlig kod som användes för att angripa industriella informations- och styrsystem i cyberoperationen Stuxnet (2012).

2.2.6 Cyberförsvarsövningar

Flera cyberförsvarsövningar har genomförts som en del av FOI:s forskning.

År 2000 invigdes FOI:s IT-försvarslaboratorium och året därpå utvecklades ett laboratorienät som var likt de som fortfarande används idag. År 2008 tog FOI över en avlagd superdator och byggde upp en övning med hjälp av den. Övningen genomfördes i distribuerad form i samarbete med estniska Sivak (nu Nato-ackrediterade cyberförsvarcentret CCDCOE) med två lag av studenter vid Linköpings universitet och två lag från Tallinns universitet. Övningsdeltagarna övade på att försvara sig mot angrepp. År 2010 skedde en ny övning i samarbete med esterna. I samband med övningen började FOI även anamma delar av Natos begreppsterminologi.

Sedan 2010 har FOI utfört ungefär en övning årligen och av varierande storlek, med olika uppdragsgivare och med deltagare från olika organisationer. Cyberanläggningen som används som teknisk infrastruktur för övningarna går numera under namnet CRATE och den byggs kontinuerligt ut.[5]

Intresserade läsare kan läsa mer om cyberförsvarsövningar i den akademiska forskningsartikeln *Cyber security exercises and competitions as a platform for cyber security experiments* av Sommestad och Hallberg (2012). Utanför projektet men under dess gång har det bland annat skrivits om vilka rekommendationer om utförandet av övningar som finns i svenska och europeiska policydokument (Zouave och Colde, 2020).

2.2.7 Cyberkrigföring och cyberstrategi

Grennert och Tham (2001) studerade icke-statliga aktörers (hacktivisters) utnyttjande av cyberoperationer under pågående konflikter med stater inblandade. Kindvall och Nordstrand (2003) studerade informationskrigföring och dess roll jämte sådant som telekrig och ledningskrigföring. Karresand m.fl. (2004) samt Wedlin (2005) undersökte olika scenarier för cyberkrig. Kindvall

[5] För att läsa mer om CRATE se Westerdahl (2020) eller foi.se/crate. FOI har också utfört forskning med hjälp av en ledningskrigssimulator med syfte att visualisera hur ledningsförmåga påverkas av ledningskrigföring (i form av både cyberkrig och telekrig) (se Hammervik m.fl., 2009 samt avsnitt 3.2).

(2005) undersökte det amerikanska konceptet effektbaserade operationer där fokus ligger på strategisk nivå, underrättelser och samverkan i större utsträckning än i andra typer av operationer. Heickerö (2006) studerade teorier och metoder för informationskrigföring.

Heickerö (2008) beskrev kinesisk syn på informationskrigföring och skillnader mot amerikansk syn. På senare år beskrev Englund (2019) Kinas industriella cyberspionage, dess motiv och mål samt organisationerna bakom spionaget.

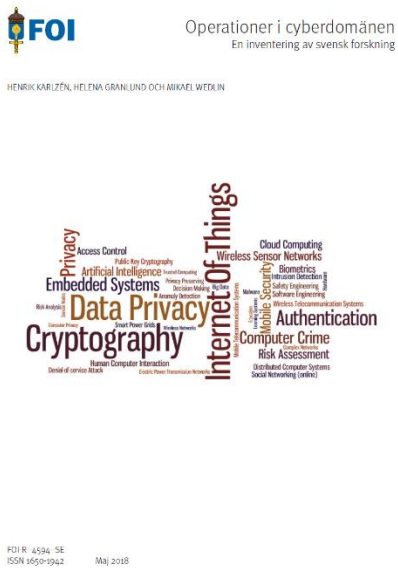
Heickerö (2010) undersökte ryska informationsoperationer, rysk syn på cyberhot och faktiska cyberhot som realiserats. Hagström Frisell och Zetterlund (2013) förutspådde vilken försvarspolitisk inriktning USA, Storbritannien och Frankrike skulle ta med inom bland annat cyberdomänen. Franke (2015) beskrev rysk doktrin om informationskrigföring, cyberkrigföring och informationssäkerhet. Vendil Pallin (2017) studerade Rysslands långsiktiga informationssäkerhetsstrategi som bland annat syftar till att öka kontrollen över den ryska delen av internet. Dessa studier har fortsatt: se Vendil Pallin (2019a och 2019b) som också nämns i avsnitt 2.1.

2.2.8 Internationellt cybersamarbete

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, samt hur samarbetena ska gå till. Karresand och Persson (2006) studerade virtuella rödakorsmärken i relation till cyberkrig.

2.3 Inventering av svensk forskning

För att skapa en första vy av forskningsområdet gjordes en inventering av svenska akademiska forskningsartiklar i rapporten *Operationer i cyberdomänen. En inventering av svensk forskning.* (Karlzén m.fl., 2018)[6]. Först gjordes ett försök till att avgränsa forskningsområdet, men med slutsatsen att det var svårt att dra områdets gränser. Eftersom forskningsområdet var nytt och saknade tydliga gränser utfördes inventeringen brett och omfattade hela cybersäkerhetsområdet (vilket omfattar både informationssäkerhet och IT-säkerhet).



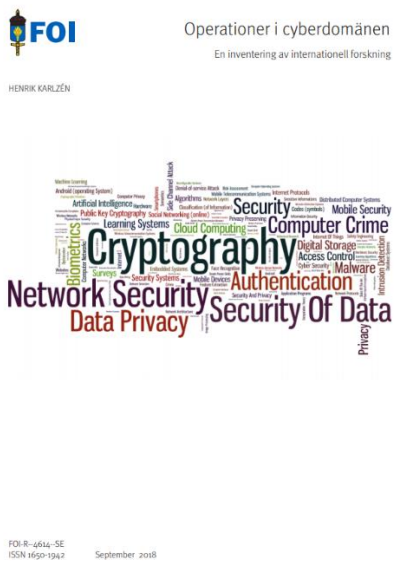
Genom sökning i forskningsdatabasen Scopus följt av manuell filtrering erhölls knappt 1000 forskningsartiklar. Utifrån dessa artiklar noterades i vilka tidskrifter och i samband med vilka konferenser artiklarna publicerats och hur många andra artiklar som citerade artiklarna. Vidare noterades vilka svenska universitet och andra svenska organisationer som låg bakom artiklarna och vilka dessa organisationer författade artiklarna tillsammans med inom Sverige och internationellt. På så sätt sammanställdes vilken kompetens som finns var.

Dessutom sammanställdes utifrån artiklarna vilka delområden varje svensk organisation forskar om. Det gick också att se vissa delområden (såsom forensik, lägesuppfattning, virtualisering och nätfiske) som särskilt få organisationer forskade om. Vidare sågs att vissa delområden (såsom sakernas internet, AI, lägesuppfattning och nätfiske) vuxit i de senaste årens forskning jämfört med hur det sett ut tidigare i liknande äldre inventeringar. Det noterades också att FOI forskade om vissa delområden (lägesuppfattning, regelefterlevnad, träning och militära aspekter) som få andra forskar om samt tvärtom att FOI inte forskade om vissa annars vanliga delområden (såsom personlig integritet, kryptografi och sakernas internet). Som komplettering till att skapa en bild av forskningen utifrån forskningsartiklar, undersöktes också vad organisationernas webbsidor säger att organisationerna forskar om. En slutsats var att vad organisationerna säger sig forska om och faktiskt publicerar forskning om skiljde sig åt en del.

[6] Rapporten sammanfattades kortfattat i memot Karlzén och Wedlin (2018).

Slutligen drogs slutsatsen att det vore bra att göra denna typ av inventeringar med jämna mellanrum för att följa upp utvecklingen över tid.

2.4 Inventering av internationell forskning



På liknande sätt som inventeringen av svenska forskningsartiklar i föregående gjordes, utfördes en inventering av internationell cybersäkerhetsforskning i rapporten *Operationer i cyberdomänen. En inventering av internationell forskning* (Karlzén, 2018). Eftersom det publiceras så mycket mer internationellt än enbart i Sverige infördes vissa nya begränsningar för att få en hanterbar mängd forskningsartiklar att analysera. Tre olika urval gjordes; de mest citerade artiklarna, de högst rankade tidskrifterna och konferenserna, samt översiktsartiklar som sammanställer en rad andra forskningsartiklar inom ett område. Totalt gav detta urval drygt 3500 artiklar.

En slutsats som drogs var att bara hälften av de tidskrifter och konferenser som artiklarna publicerades i hade särskilt cybersäkerhetsfokus. En annan slutsats var att forskningen var spridd över många länder. Kopplat till detta gjordes också en analys av vilka länder som ligger bakom flest och färst artiklar jämfört med hur mycket pengar de lägger på forskning.

Det fanns flera mindre kända universitet och organisationer bland de som var flitigast att publicera sin forskning. Samtidigt fanns det flera mer kända universitet som inte var så synliga som det skulle kunna förväntas med tanke på deras goda rykte.

De tio delar av forskningsområdet där det publiceras flest forskningsartiklar var i fallande ordning (med störst delområde först): kryptografi, cyberfysiska system, personlig integritet, molnet, åtkomstkontroll, administrativ säkerhet, biometri, intrångsdetektering, skadlig kod och mjukvara samt artificiell intelligens. Delområdena uppvisar stort ämnesmässigt överlapp med de delområden som är vanligast i enbart svensk forskning, med undantag av några specifika domäner (elektronisk röstning, fordon, hälsa, industri och militär) som verkar prägla svensk forskning. I en stor övergripande internationell inventering syns dock av naturliga skäl inte alla mindre delområden på aggregerad nivå.

Delområdena jämfördes också med vad några större forskningsfinansiärers forskningsutlysningar fokuserade på. Det noterades att samtliga undersökta finansiärer hade utlysningar om cyberfysiska system men ingen om varken biometri eller intrångsdetektering. Vidare hade bara en finansiär med personlig integritet trots att det är ett av de mest frekvent förekommande delområdena bland artiklarna.

2.5 Inledande forskningsplan

För att komma fram till en väg framåt i projektet togs en inledande forskningsplan fram i rapporten *Operationer i cyberdomänen. En inledande forskningsplan* (Karlzén och Lindahl, 2019). Forskningsplanen utgick från en smalare inventering än vad som tidigare gjorts och fokuserades på cyberoperationer i militärt perspektiv. Detta perspektiv gav drygt 600 akademiska forskningsartiklar och visade att det är ett tvärvetenskapligt forskningsområde (vilket också speglas av de kompetenser detta projekts medarbetare har).

Det noterades att nästan hälften av artiklarna hade skrivits vid universitet och försvarsorganisationer i USA. Här fanns en mindre geografisk spridning än för cybersäkerhetsområdet som helhet. Det noterades också att antalet artiklar som skrivits per år till viss del kunde kopplas till hur USA byggt upp sin cyberförmåga och till antalet cyberoperationer som genomförts i praktiken.

Per forskningsfråga analyserades de mest citerade artiklarna tillsammans med de nyaste. Nedan ges ett utdrag av vad analysen kom fram till, indelat per forskningsfråga.

Vad gäller forskningsfråga 1 (om modellering) beskrevs att vilken modell som är lämpligast beror på vilka detaljer som behövs. Exempelvis beror det på vilket behov som finns av att agera dolt. Det beror också på vilket syfte som ska uppnås.

För forskningsfråga 2 (om situationsförståelse) beskrevs att det vore lämpligt att försvarare håller sig uppdaterade om angreppsmetoder och då inte minst genom informationsdelning med andra försvarare.

För forskningsfråga 3 (om effekter) beskrevs att cyberoperationer bör ha politiska eller militära mål samt att ingen cyberoperation någonsin (fram till år 2012) skadat vare sig byggnader eller människor. Det noterades därför att framtida forskning om cyberoperationers effekter bör utreda vilka politiska och militära mål cyberoperationer kan ha samt om cyberoperationer kan skada byggnader och människor.

För forskningsfråga 4 (om kompetenser och tekniker) undersöktes om cyberangrepp är svårare att genomföra än vad som ofta sägs. Det noterades därför att framtida forskning bör utreda hur svårt det är att utföra offensiva cyberoperationer.

För forskningsfråga 5 (om övning och utbildning) beskrevs allmänt om övning. Det beskrevs också vad som krävs för att en genomförd operation ska kunna studeras genom att återskapas. En slutsats var att det behöver finnas tillräckliga beskrivningar om operationen, gå att få tag på de programvaror som användes, samt vara en operation som skett tillräckligt nyligen och som varit tillräckligt komplex för att ge några insikter.

För forskningsfråga 6 (om etik och folkrätt) beskrevs att skapandet av folkrätt utifrån erfarenheter från angränsande områden inte nödvändigtvis är en framkomlig väg. Det beskrevs också att folkrätten behöver reglera vilka mål militär verksamhet får agera mot och att det i cyberdomänen inte alltid finns klara distinktioner mellan vad som är militärt och vad som är civilt. Exempelvis är militär verksamhet ofta byggd på civil infrastruktur. Det noterades att cybervapentillverkare kan komma att räknas som militärer om de gör uppdateringar av vapnen strax före vapnen används. Det noterades också att det är oklart i vilken utsträckning det är tillåtet att skicka cybervapen via civila nät. Det föreslogs att framtida forskning undersöker hur sidoskador (utanför det avsedda målet; snarlikt vådabekämpning) kan undvikas på neutrala eller civila.

En annan aspekt som lyftes fram kring forskningsfråga 6 var att det nog finns ett samband mellan styrkan i cyberangrepps effekter och deras legalitet. Vissa röster har, på grund av att de upplever effekterna som mycket allvarliga, förordat minimering av cybervapen genom icke-spridningsavtal och etiska stigman likt de för kemiska, biologiska, radiologiska och nukleära vapen.

3 Projektresultaten

I de följande avsnitten sammanfattas de resultat projektet producerat (exklusive denna slutrapport och de resultat som beskrivits tidigare i rapporten). Det rör sig om rapporter och memon utgivna av FOI, akademiska forskningsartiklar samt rapporter framtagna i samarbete med andra organisationer. Bland resultaten beskrivs också genomförda online-seminarier (webbinarier) och projektets olika samarbeten med andra organisationer. Resultaten beskrivs kronologiskt med start i det först producerade. Några av resultaten har inte hunnit publiceras än men beskrivs ändå sist i kapitlet.

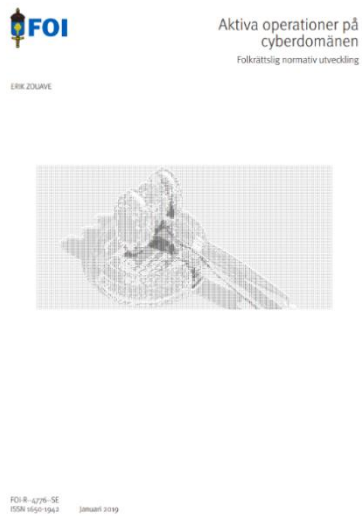
Vilka forskningsfrågor de olika resultaten ämnat besvara syns i Tabell 1. Det bör noteras att även om två projektresultat behandlat samma forskningsfråga kan ett av projektresultaten ha behandlat forskningsfrågan i (betydligt) större (eller mindre) utsträckning än det andra projektresultatet. Någon särskiljande kvantitativ bedömning har inte gjorts.

Tabell 1: Vilka forskningsfrågor (FF 1-6) projektresultaten (beskrivna i 3.1-3.18) avhandlat (markerat med ●). Forskningsfrågorna återfinns i rapportens inledning men kan sammanfattas med FF 1 = modellering, FF 2 = situationsförståelse, FF 3 = effekter, FF 4 = kompetens och tekniker, FF 5 = övning och utbildning, FF 6 = etik och folkrätt.

Projektresultat	FF 1	FF 2	FF 3	FF 4	FF 5	FF 6
3.1						●
3.2			●		●	
3.3	●					●
3.4	●	●	●	●		●
3.5		●			●	
3.6			●	●		
3.7	●				●	
3.8	●					
3.9					●	
3.10		●			●	
3.11			●	●		●
3.12			●	●		●
3.13			●	●	●	●
3.14	●				●	

3.1 Folkrättslig utveckling

I rapporten *Aktiva operationer på cyberdomänen. Folkrättslig normativ utveckling* (Zouave, 2019)[7] beskrivs utvecklingen av folkrättsliga normer för cyberoperationer internationellt. Framförallt beskrivs försöken att tillämpa och utveckla folkrätten inom mellanstatliga och överstatliga organisationer som EU, FN och Nato. Rapporten tar också upp olika begrepp inom cyberoperationer enligt svensk lagstiftning.



I de olika dokumenten inom folkrätten visades det på kopplingar mellan cyberoperation och områden såsom yttre rymd, autonoma vapensystem, artificiell intelligens, allmänna val, civil–militär samverkan och mänskliga rättigheter.

Rapporten visar att det finns utbredd konsensus att folkrätten gäller i cyberdomänen. De internationella organisationerna och deras medlemsstater poängterar betydelsen av FN-stadgan, krigets lagar och mänskliga rättigheter. Trots detta saknas konsensus om hur folkrätten ska tillämpas. Sammanslutningar av likasinnade stater såsom EU och Nato har kommit längre i att precisera tillämpningar än exempelvis expertgrupperna inom FN. Detta tydliggörs av att Nato fastställt att cyberangrepp, likt kinetiska angrepp, kan föranleda kollektivt självförsvar och därmed även kan betraktas som en form av aggression och väpnat angrepp.

En framträdande publikation om folkrätten för cyberoperationer är Tallinnmanualen som beskriver staters rättigheter och skyldigheter rörande cyberoperationer i krig och fred. Det bör dock påpekas att Tallinnmanualen enbart är rådgivande. En slutsats är dessutom att det generellt finns främst just icke-bindande vägledningar snarare än klara regler för vad som gäller för cyberoperationer i praktiken.

[7] Rapportens innehåll har också presenterats i form av ett webbinarium, se avsnitt 3.12.

3.2 Modellering och simulering av effekter

Memot *Implementing cyber effects in M&S. An overview of FOI research modeling and simulation of the effects of cyber operations* (Granåsen, 2019) beskriver hur FOI arbetat med modellering och simulering av de effekter statsstödda cyberoperationer kan ge. Memot togs fram i samband med Natos arbetsgrupp för modellering och simulering (MSG-170). FOI:s arbete har gjorts dels med hjälp av en simulator för ledningskrigföring, dels med hjälp av cyberanläggningen CRATE.[8] En slutsats var att simulering av tidigare genomförda operationer typiskt inkluderar tillvägagångssätt som redan är för gamla för att kunna vara verksamma i skarpt läge. Samtidigt drogs slutsatsen att metodernas effekter förmodligen är desamma som de som skulle ges med modernare metoder.

3.3 Offensiv modell

I forskningsartikeln *The Offensive Cyber Operations Playbook* (Granåsen och Jaitner, 2019) beskrivs USA:s, Storbritanniens och Rysslands syn på cyberoperationer. Ländernas syn skiljer sig bland annat i vad som är offensivt och defensivt samt vad som är tillåtet respektive otillåtet agerande. En annan skillnad är att Storbritannien kategoriserar cyberoperationer enligt *vad som utförs* medan USA kategoriserar utifrån *vilka effekter* som uppnås. Vidare är en skillnad att Ryssland placerar cyberoperationer inom ramen för informationsoperationer och ser dem som mer integrerade med övriga militära operationer än vad USA och Storbritannien gör.

I cyberangreppsmodellen *Cyber kill chain* (framtagen av Lockheed Martin) finns ett steg som går ut på manuell styrning under angreppet. Det noteras i artikeln att det bara ibland finns behov av sådan manuell styrning under operationer (snarare än *fire-and-forget*). Det argumenteras därför för att det finns bättre sätt att modellera på och att ett bättre sätt vore att modellera cyberoperationer i enhetlighet med hur andra typer av militära operationer modelleras med faserna infiltrering, utförande och exfiltrering.

[8] Båda beskrivs också i avsnitt 2.2.5.

3.4 Attribution, tillvägagångssätt och sofistikation

I rapporten *Cyberoperationers attribution, tillvägagångssätt och sofistikation* (Karlzén, 2019)[9] beskrivs databaser med cyberoperationer, hur den som utfört en cyberoperation kan identifieras (genom så kallad attribution), hur cyberoperationer utförs och hur sofistikerade de är.

Analysen utgår från en databas framtagen av amerikanska tankesmedjan CFR[10]. Databasen har beskrivningar och källhänvisningar för cyberoperationer (som rubricerats som statsstödda). Utifrån en mängd databaser valdes den specifika databasen baserat på kriterier som detaljrikedom, stats- och operationsfokus samt tillförlitlighet. En begränsning med databasen är att dess källor i huvudsak är engelskspråkiga (snarare än exempelvis kinesiska eller ryska).

Utifrån databasen drogs några slutsatser om angripare, offer och effekter. De vanligast beskrivna angriparna är Kina, Ryssland, Nordkorea och Iran medan Sverige inte alls syns som angripare. För en enskild operation ligger generellt bara ett land bakom som angripare, men det finns ett fåtal undantag där samarbete verkar ha skett. Offer är typiskt privata företag snarare än myndigheter, men fokus låg på vilket land offret hörde till. Bland de vanligaste offren (vad gäller nationell hemvist) syns USA i absoluta tal. Per capita är istället Israel vanligast (med Sverige en bit ner på listan, men före USA). Med

[9] Rapporten har också lett fram till en akademisk forskningsartikel (Karlzén, 2020).

[10] Databasen går under benämningen Cyber Operations Tracker och nås på https://www.cfr.org/cyber-operations/. Databasen är den mest kompletta vad gäller statsstödda operationer. Databasen bygger på källor som till stor del utgörs av nyhetsartiklar och cybersäkerhetsföretags rapporter.

tanke på att databasen bara inkluderar några hundratal operationer är det dock vanskligt att dra slutsatser om vilka länder som är mest eller minst drabbade.

De allra flesta operationerna i databasen kategoriseras som underrättelseinhämtning, med resten fördelad på kategorierna destruktion av data, *doxing* (inhämtning och offentlig publicering av känslig information), *defacement* (där webbplatser vandaliseras) samt *denial of service* (blockering av tjänst, till exempel genom överbelastningsattacker). Det finns även en liten andel sabotage. Att underrättelseinhämtning överväger medan exempelvis sabotage är mycket ovanligt kan bero på att inhämtning av information är enklare att göra i cyberdomänen medan sabotage är enklare att genomföra utanför cyberdomänen.

Direkta tekniska effekter av operationer beskrivs främst i tekniska utredningar av cybersäkerhetsföretag. För sekundära (operativa) effekter är de främsta källorna expertutlåtanden och anonyma källor i nyhetsartiklar. Att källorna skiljer sig åt gör att det blir svårt att se en tydlig koppling mellan en operation som utförs på ett visst sätt och att den har en viss typ av effekt. Dessutom är de tekniska systemen komplexa, vilket gör det komplicerat för angripare att ta reda på exakt vad det avsedda offret har för system och det är svårt att se till att bara det avsedda offret drabbas. Ett behov av framtida forskning som nämns är därför att utforska hur enkelt det är att begränsa ett cybervapens verkan till ett fåtal system och hur det kan avgöras hur riktad en operation var tänkta att vara. På liknande sätt nämns behov av studier av hur riktade cyberoperationer stater vill utföra och i vilken utsträckning de bryr sig om sidoskador i cyberdomänen.

Vad gäller attribution finns ofta långa och svaga beviskedjor där motbevis ibland till och med ignoreras. Det finns bland annat problem med politisk färgning, fokus på vissa (engelskspråkiga) källor, överdrifter och tekniska begränsningar i att spåra agerande på internet. Detta gäller även attributionen som görs i databasens källor. Det noterades också att attribution är svårt, bland annat på grund av angriparens försök att dölja sig (bl.a. med så kallade falska flaggor som vilseleder) och subjektivitet (bias) hos den som försöker identifiera angriparen. Vidare noterades det att teoretiska modeller för attribution och faktisk attribution i praktiken skiljer sig åt i vilka variabler som används för identifieringen. Ett förslag på mer forskning om attribution som nämndes var att studera hur enkelt det är att avslöja någons identitet, exempelvis baserat på dennes programmeringsstil.

Inom ramen för tillvägagångssätt beskrev rapporten olika sätt att modellera cyberoperationer. Ett exempel på en modell är Lockheed Martins Cyber kill chain. Det finns också andra exempel på modeller såsom de framtagna av Mitre, HP samt amerikanska försvarsdepartementet. Vilken modell som är lämpligast att använda beror på vilka detaljer som behövs, som exempelvis tidsaspekter i form av hur snabbt saker sker och i vilken ordning. Vad gäller tillvägagångssättens sofistikation (svårighetsgraden eller vilken färdighet som krävs) håller de beskrivna operationernas tillvägagångssätt generellt en relativt

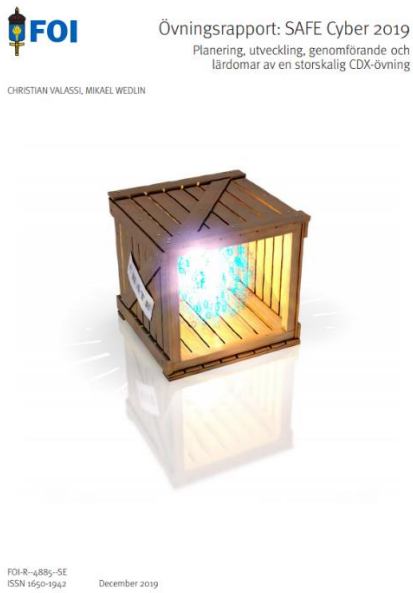
låg sofistikationsgrad. Vad som av olika tyckare framhålls som ett sofistikerat angreppssätt är sällan särskilt imponerande. Å andra sidan är det möjligt att operationer som använder mer avancerade verktyg eller utnyttjar okända sårbarheter inte upptäcks.

Vad gäller sofistikation finns det baserat på öppna källor en hel del som talar för att det inte krävs så mycket för att utföra cyberoperationer. Exempelvis bygger operationerna oftast på rättfram rekognoscering, grundläggande nätfisketekniker och enkla ledningsinfrastrukturer. Vidare återanvänds verktyg från tidigare operationer (egna eller andras) och det går till och med att köpa in cybervapen vilket minskar kraven på teknisk förmåga. Angripare verkar sällan bry sig om att rikta in vapnen så att de inte även slår mot andra än avsett offer. Sannolikheten för att bli identifierad som upphovsman verkar också låg, likaså de möjliga konsekvenserna. Mot denna bakgrund är det inte förvånande att även mindre resursstarka stater rapporteras ha legat bakom cyberoperationer.

Men det finns också saker som talar för att det faktiskt krävs en hel del sofistikation för att utföra cyberoperationer. Först och främst kan det vara så att operationer verkar enkla eftersom det bara är just de enkla cyberoperationerna som upptäcks. På liknande sätt upptäcks kanske inte mer resurskrävande och smartare rekognoscering medan avancerade tekniska metoder kan vara alltför svåranalyserade för att förstås och beskrivas. Vidare kräver införskaffandet av cybervapen att man vet vad man behöver och vid köp krävs finansiella muskler. Det är också möjligt att statsaktörer är noggranna med att deras vapen minimerar risken för indirekta skador varför de måste lägga betydande arbete på att målinrikta vapnen. Vad gäller identifieringen av angripare är det möjligt att underrättelsetjänster lyckas väl men helt enkelt inte talar högt om det. Dessutom har stater vissa maktmedel gentemot varandra, som exempelvis sanktioner. Upptäckta operationer kan dessutom avslöja vilka metoder som använts och därmed göra använda cybervapen verkningslösa i framtiden. Avslutningsvis tyder källorna på att det alltjämt främst är resursstarka länder som utför operationer vilket indikerar att det trots allt krävs större mängder tid, möda, personella resurser och organisatorisk färdighet för att utföra cyberoperationer.

För att vidare utreda vad som krävs för att utföra cyberoperationer föreslog rapporten att det undersöks hur väl typiska cyberoperationer stoppas av standardskydd och om hela operationer stoppas av enskilda skydd. Dessutom föreslogs studier av att köpa cyberoperationsförmåga. Till sist frågades det även vad som kan sägas om mörkertalet av operationer, det vill säga de som inte upptäckts och som förmodligen är de mer sofistikerade cyberoperationerna.

3.5 Övningen SAFE Cyber 2019



Rapporten *Övningsrapport: SAFE Cyber 2019. Planering, utveckling, genomförande och lärdomar av en storskalig CDX-övning* (Valassi och Wedlin, 2019) beskriver FOI:s övningsverksamhet på området med de huvudsakliga uppdragsgivarna Myndigheten för Samhällsskydd och beredskap (MSB) samt Försvarsmakten. Rapporten beskriver hur cyberförsvarsövningar brukar planeras och genomföras.[11]

Rapporten förklarar att övningar brukar gå ut på att de övande deltagarna ska försvara och/eller angripa IT-system. Syftet är att de övande ska lära sig hantera den typ av situationer och incidenter som de utsätts för i övningen. Övningar kan också vara prövande och därmed gå ut på att utvärdera de övandes kunskapsnivå eller att testa ny utrustning. Tekniska simuleringsövningar är dock idag sällan av en prövande karaktär i Sverige.

Rapportens tonvikt ligger på den senaste övningen SAFE Cyber 2019, vilken utfördes i samarbete med Försvarsmakten, med övande deltagare från många olika Försvarsmaktsnära myndigheter och företag.

SAFE Cyber 2019 gick ut på att de övande skulle försvara sina cybersystem och bestod av en teknisk simuleringsdel och en diskussionsbaserad delövning med fokus på ledning. Delarna genomfördes främst var för sig men med viss kommunikation mellan delarna. Rapporten beskriver hur övningarna planerades och vilka utmaningar som fanns. Vidare beskrivs hur övningarna genomfördes, från administrativa aspekter kring lokaler och lunch till tekniska detaljer.

Vidare utvärderades övningarna och förbättringsförslag togs fram. Det beskrivs exempelvis hur förberedelserna hos övningsledningen kunde varit bättre och mer ekonomiskt effektiva. Det beskrivs också att övningsdeltagarna behövde mer information om de tekniska system, den fiktiva organisation de skulle försvara och den incidentrapporteringsmall som användes, samt vilka ramar som fanns för

[11] Tidigare övningar beskrivs utifrån denna källa i avsnitt 2.2.6.

försvarande lag. Det fanns också brister i överföring av information mellan den tekniska delen av övningen till den ledningsbaserade delen. Det noterades också vara svårt för ledningsdelen att föra samman tekniska incidentrapporter som rörde samma incident. En övergripande reflektion var att beroende på roll fanns det behov av olika lägesbilder.

3.6 Cyberoperationer som genomfördes 2019

I memot *Omvärldsbevakning statsattribuerade cyberoperationer 2019* (Lindahl, 2019b) sammanfattas kortfattat 2019 års statsstödda cyberoperationer som beskrivits i databasen framtagen av amerikanska tankesmedjan CFR. Generella slutsatser om operationerna är att de i huvudsak är tekniskt enkla och att de ofta är i form av politiska påtryckningskampanjer. Dessutom noteras att det fortsatt är svårt att verkligen veta vem som ligger bakom en operation. Attributionsproblematiken kvarstår alltså. Överhuvudtaget är det som media publicerar om cyberoperationer ofta svårt att belägga i andra källor.

3.7 Standardisering för modellering och simulering

I rapporten *Final Report for the Cyber Modeling and Simulation (M&S) Study Group (SG)* (SISO m.fl., 2020) beskrivs ett försök att standardisera cybermodellering och cybersimulering. Rapporten togs fram i samband med en arbetsgrupp i den internationella organisationen Standardiseringsorganet för interoperabilitet vid simuleringar (fritt översatt från eng. Simulation Interoperability Standards Organization) vilken samarbetar med Nato. Rapporten utgår från hur modellering och simulering sker i dagsläget och från litteratur om hur modellering och simulering bör byggas. Dessutom undersöktes hur träning inom området normalt utförs och hur den skulle kunna utföras.

3.8 Svenska definitioner

I rapporten *De svenska definitionerna inom aktivt cyberförsvar* (Zouave, 2020) klarläggs svensk policy på området, samt vilken betydelse och vilka begränsningar policyn medför för begreppsapparaten. Rapporten ger en överblick över svenska myndigheters begreppsanvändning på området baserat på svensk policy, strategi och militär doktrin. Begrepp som avhandlas är bland annat aktiv förmåga, cyber, cyberoperation samt de svenska översättningarna av termerna engelskans *cyber network operation, cyber network defence, cyber network attack* och *cyber network exploitation*. Den huvudsakliga slutsats som dras i

rapporten är att de svenska begreppen (och deras betydelse) är i ett formativt stadium och att de därmed kan komma att förändras i framtiden. Rapporten visar också att det aktiva cyberförsvaret är tänkt att omfatta både defensivt agerande såväl som proaktivt agerande med offensiva inslag.

3.9 Simulering av effekter

I rapporten *Top Ten Cyber Effects for Campaign and Mission Simulations* (Nato, 2020) beskrivs en metod för att bedöma vilka av cyberoperationers effekter som är intressantast att öva för de som inte är cyberexperter. Rapporten togs fram i samband med Natos arbetsgrupp för modellering och simulering (MSG-170). Metoden utgår ifrån hur sannolikt det skulle vara att en viss effekt skedde i skarpt läge, hur lätt det är att öva och upptäcka effekten, hur väl effekten kan simuleras givet tidsramarna samt i vilken mån simuleringen av effekten inte förstör för resten av övningen.

3.10 Informationselement i incidentrapporter

I forskningsartikeln *Evaluation of Information Elements in a Cyber Incident Report* (Lif m.fl., 2020) studeras vilka informationselement som bör ingå i incidentrapporter om cyberincidenter. Olika mallar och ramverk för incidentrapportering gås igenom och en egen variant utvärderas inom ramen för cyberövningen SAFE Cyber 2019. Slutsatser från utvärderingen är att de tekniska cyberförsvararna hade svårt att relatera till organisatoriska konsekvenser av angreppen, samt att bedömningar av konsekvenser kan behöva göras av ledningen snarare än av tekniker. Det betonades även att framtida incidentrapporteringsmallar bör förbättras vad gäller entydighet i definitioner.

3.11 Cyberoperationer som genomfördes 2020

I memot *Omvärldsbevakning statsattribuerade cyberoperationer 2020* (Lindahl, 2020) sammanfattas kortfattat statsstödda cyberoperationer som skett sedan den förra omvärldsbevakningen i avsnitt 3.6. Generella slutsatser om operationerna är att de i huvudsak är tekniskt enkla, men att svårare angrepp också förekommer. Det noteras också att syftena i huvudsak handlar om informationsinhämtning. Dessutom noteras problematik vad gäller en sorts legosoldater i cyberdomänen.

3.12 Webbinarier

Projektet genomförde fyra webbinarier, det vill säga online-föreläsningar med video och ljud, där tittare fick möjlighet att ställa frågor. Webbinarierna gavs ut i en FOI-kanal på Youtube. Det första webbinariet *Cyberoperationer - Vem gör vad mot vem?* (Lindahl, 2019a) beskrev grunderna för cyberoperationer och vem som gör vad mot vem i cyberdomänen. Vid skrivande stund (november 2020) har webbinariet visats över 2 700 gånger vilket gör det till det videoklipp med klart flest visningar av FOI:s alla videoklipp i plattformen. Det andra webbinariet *Folkrätt vid aktiva operationer på cyberdomänen* (Zouave och Lindahl, 2019) utgick från den rapport som beskrevs i avsnitt 3.1 och handlade om folkrätt. Även denna sändning blev populär. Det tredje webbinariet *I skuggan av pandemin: cyberattackerna ökar* (Lindahl och Liljedahl, 2020) beskrev cyberhot mot sjukvården i samband med pandemin orsakad av Covid-19. Webbinariet togs fram i samband med ett annat projekt vid FOI. Det fjärde webbinariet *Säkerhet vid videomöten* (för tillfället opublicerat) rörde säkerheten för videokonferenser, vilka ökat under pandemin. I webbinariet deltog tre personer: den förre chefen för Militära underrättelse- och säkerhetstjänsten (MUST), cybersäkerhetskonsulten Robert Malmgren samt en projektmedlem.

3.13 Samarbeten

Projektet har samarbetat med flera organisationer utanför FOI. I detta avsnitt nämns dessa samarbeten.

Projektgruppen genomförde övningen SAFE Cyber 2019 tillsammans med (uppdragsgivaren) Försvarsmakten. Som övande deltog många olika Försvarsmaktsnära myndigheter och företag (se avsnitt 3.5).

Projektgruppen var med som stöd i flera övningar under namnet Locked Shields vilka sker med främst europeiska myndigheter som deltagare. Övningarna leds av Nato-ackrediterade cyberförsvarscentret CCDCOE i Tallinn, men alla medverkande lag förväntas bidra med stöd för genomförandet.

Projektgruppen utvärderade ett ramverk för cyberoperationer som tagits fram av FHS. Detta beskrivs mer i avsnitt 3.14.

En av projektmedlemmarna deltog i arbete vid internationella Standardiseringsorganet för interoperabilitet vid simuleringar (SISO). Arbetet bestod av att standardisera cybermodellering och cybersimulering (se avsnitt 3.7). Samma projektmedlem deltog också i Natos arbetsgrupp för modellering och simulering vilken samarbetar med SISO. Som en del av detta studerades hur cyberoperationers effekter bör modelleras och simuleras (se avsnitt 3.2). Arbetsgruppen tog dessutom fram en metod för att bedöma vilka av cyberoperationers effekter som är intressantast att öva (se avsnitt 3.9).

På initiativ av en projektmedlem skrev Nato-ackrediterade cyberförsvarcentret i Estland en rapport (De Tomas Colatin och Väljataga, 2020) som analyserar folkrätten om utvecklingen och användningen av cybervapen, cyberoperationer och cyberförmåga. En slutsats är att utvecklingen av cybervapen kräver mycket underrättelser, varför även folkrätten relaterat till underrättelseinhämtning blir relevant gentemot cybervapen.

Det kan också nämnas att (inom ramen för ett annat projekt) var en av projektmedlemmarna medförfattare till epilogen (Jaitner och Sommestad, 2019) för en antologi om rysk målbild i cyberdomänen. Antologin gavs ut av finska myndigheten Försvarsmaktens forskningsanstalt, som bjudit in FOI att delta i antologiarbetet.

3.14 Kommande resultat

När den här rapporten trycks är två resultat i projektet fortfarande under färdigställande.

Det första resultatet kommer att bli en rapport om en övningsmiljö som byggts upp i CRATE. Övningsmiljön syftar till att ge Försvarsmakten möjlighet att genomföra cyberförsvarsövningar i en miljö som efterliknar deras interna datornätverk FMIP. Övningsmiljön modelleras därför efter FMIP även om likheten inte är så hög att övningsmiljön omfattas av försvarssekretess. Övningsmiljön kan användas för att skapa enskilda övningar. Övningsmiljön förenklar därför det tekniska arbetet inför en övning, vilket är en stor fördel då utvecklingen och genomförandet av övningar visat sig vara komplicerat och tidsödande.

Det andra resultatet kommer att bli ett memo som beskriver hur ett ramverk för cyberoperationer utvärderats i en mindre övning inom ramen för SAFE Cyber 2020 under hösten 2020. Ramverket togs fram av bland andra FHS (se Huskaj och Iftimie, 2020).

4 Slutsatser

Forskningsområdet cyberoperationer är relativt nytt och saknar tydliga gränser. Akademiska forskningsartiklar inom området publiceras brett och av författare från många olika discipliner. Samtidigt är det ganska få forskare som publicerar öppet om militära cyberoperationer. Vidare finns det mer än tjugo databaser över genomförda cyberoperationer. Databaserna och deras källor är öppna, men i huvudsak knapphändiga och otillförlitliga. Exempelvis uppvisar många källor drag av partiskhet eller sensationalism. Det är samtidigt inte konstigt att öppna källor är ofullständiga eftersom få offer för cyberoperationer vill dela med sig av hur de drabbats och få angripare vill avslöja sin förmåga. Det är med andra ord svårt att få tag i tillförlitliga data varför forskningsresultat inom området behöver tolkas med viss försiktighet.

De slutsatser som dragits från projektets resultat och vad som vore intressant att studera vidare återfinns nedan med ett avsnitt per forskningsfråga (1–6). När hänvisningar till projektens resultat görs indikeras det med korsreferenser (på formen 2.x eller 3.x) till tidigare avsnitt som beskriver resultatet.

4.1 Hur modelleras aktiv cyberförmåga?

Forskningen om modellering på området är ganska begränsad (Huskaj och Iftimie, 2020) men det finns trots allt flera olika sätt att modellera cyberoperationer (se avsnitt 3.4). Ett exempel är Lockheed Martins Cyber kill chain (3.4) som är inriktad på enskilda cyberangrepp. Vilken modell som är lämpligast att använda beror på i vilket syfte den ska användas. Exempelvis kan tekniska operatörer behöva andra modeller än chefer, medan angripare kan behöva andra modeller än försvarare. En viktig aspekt är vilka detaljer som behövs och vilken typ av operation det rör sig om. I operationer sker enskilda steg ofta mycket snabbt. Därtill ingår i operationer ofta att agerande sker i cykler, exempelvis där angriparen tar sig in i system efter system. En modell kan därför behöva avspegla att saker kan ske snabbt och i cykler (3.4). Ibland finns behov av manuell styrning av cybervapen. I andra fall räcker det med *fire-and-forget.* En modell kan därför behöva tillåta båda dessa varianter (3.3). Ofta vill den som utför en operation agera dolt och utan upptäckt (2.5). I andra fall är det irrelevant för angriparen om den blir upptäckt eller inte. Det kan till och med vara så att angriparen vill bli upptäckt för att bevisa sin förmåga (2.5). Vilken modell som är lämplig beror på vilka av dessa alternativ som behöver kunna modelleras. Ytterligare en aspekt är vilket syfte som ska uppnås med operationen och i vilken utsträckning syftet behöver modelleras (2.5; 3.3). Slutligen behöver valet av modell bero på i vilken utsträckning integrering med agerande i andra domäner krävs och hur väl olika modeller återspeglar detta (3.3).

I projektet utvärderades ett ramverk för cyberoperationer som tagits fram av bland andra FHS. Utvärderingen genomfördes i en mindre övning under hösten 2020 (3.14).

Framtida forskning bör besvara följande:

- Vilka modeller av cyberoperationer är lämpliga för vilka cyberoperationer?
- Vilka detaljer behövs i modellerna i olika situationer?

4.2 Hur ska situationsförståelse som möjliggör effektivt beslutsfattande kopplat till cyberoperationer uppnås?

Under projektets början noterades det att situationsförståelseområdet till stor del var outforskat. Utmaningar som särskilt noterades var exempelvis att de olika sensorer som finns i cyberdomänen är heterogena samt att situationsförståelse behöver läras ut och tränas i realistiska miljöer som FOI:s cyberanläggning CRATE. I senare resultat (2.5) nämndes vikten av informationsdelning mellan försvarare.

En svårighet i att uppnå situationsförståelse gäller identifieringen av cyberangripare (attribution). I avsnitt 3.4 noterades det att teoretiska modeller för attribution och faktisk attribution i praktiken skiljer sig åt i vilka variabler som används för identifieringen. Det noterades också att attribution är svårt, bland annat på grund av angriparens försök att dölja sig (bl.a. med så kallade falska flaggor som vilseleder) och ens egen subjektivitet. Offentliga utpekande av angripare görs ofta på till synes svag grund och utan att tala om vilken ovisshet som finns i bedömningen av vem som angrep. I avsnitt 3.4 noterades det dock också att cybersäkerhetsföretag med sina många kunder har god insikt i vad som sker i olika nät. Det nämndes också att det finns forskare som hävdar att staters underrättelsetjänster har goda möjligheter att attribuera men att de inte diskuterar sådant öppet.

I övningen SAFE Cyber 2019 (3.5) upplevde de övande att de hade varit betjänta av mer förståelse av den mall de använde för incidentrapportering och av den fiktiva organisation de skulle försvara. Vidare upptäcktes svårigheter i att överföra information mellan den tekniska delen av övningen och den ledningsbaserade delen. Det noterades också att det var svårt för ledningsdelen att föra samman tekniska incidentrapporter som rörde samma incident. En övergripande reflektion var att det fanns behov av olika lägesbilder för olika roller. Dessutom var en slutsats att de tekniska cyberförsvararna hade svårt att relatera till organisatoriska konsekvenser av angreppen och att bedömningar av konsekvenser därför kan behöva göras av ledningen snarare än av tekniker

(3.10). Vad gäller övningarna finns också visst överlapp med forskningsfråga 5 (om utbildning och övning).

Framtida forskning bör besvara följande frågor:

- Hur kan incidentrapporteringsmallar förbättras, exempelvis med mer entydiga definitioner? (3.10)
- Hur enkelt är det att avslöja någons identitet, exempelvis baserat på dennes programmeringsstil? (3.4)
- Hur kan en teknisk cyberförsvarare kommunicera relevanta delar av sin cyberlägesbild till ledningen som bättre förstår organisatoriska konsekvenser?
- Hur kan vanliga användares situationsförståelse förbättras så att de inte är så benägna att gå på nätfiske och liknande vilseledning?
- Hur kan man öka sin sikt i cyberdomänen, exempelvis genom utplacering av sensorer på strategiska platser?
- Hur kan man minska motståndarens förmåga till målsökning i cyberdomänen, exempelvis genom att dölja sådant som utmärker ens system?
- Vilka typer av cyberoperationer sker i Sverige och omvärlden och vad bör räknas som olika typer av cyberoperationer?

Parallellt med projektet studerades också situationsförståelse inom ramen för andra FOI-projekt. Mest närliggande är en förstudie om cyberlägesbild som också togs fram i ett FoT-projekt och som publiceras i en samlingsrapport (Bildsten m.fl., 2020) om förstudier i slutet av 2020.

4.3 Vad kan man förvänta sig för effekt av en typisk cyberoperation?

För att avgöra vilken effekt man kan förvänta sig av en typisk cyberoperation är det rimligt att utgå från kunskap om effekterna som genomförda cyberoperationer haft. Även om tillvägagångssätt blir förlegade när de avslöjas och sårbarheter täpps till, består förmodligen de typiska effekterna (3.2). Vilka de förväntade effekterna är utgår därför från den mest omfattande databasen över statsstödda cyberoperationer: amerikanska tankesmedjan CFR:s databas. I databasen kategoriseras de allra flesta av databasens operationer som underrättelseinhämtning (3.4). Operationerna har alltså främst effekter på angriparens underrättelsenivå. Databasen innehåller också ett mindre antal operationer som kategoriseras som destruktion av data, *doxing* (inhämtning och offentlig publicering av känslig information), *defacement* (där webbplatser vandaliseras), *denial of service* (blockering av tjänst, till exempel genom

överbelastningsattacker) och ett fåtal procent sabotage[12]. Tidigare forskning (från 2012) har kommit fram till att ingen cyberoperation någonsin skadat vare sig byggnader eller människor (2.5). Detta går delvis tvärtemot den bild som ibland målas upp i media om att omfattande cybersabotage eller cyberkrig är nära förestående. Det finns dock exempel på hur cyberoperationer stört ut kritisk infrastruktur. I september 2020 rapporterades det om att vård fördröjts på grund av att ett sjukhus datorsystem tagits ner av angripare (Eddy och Perlroth, 2020). När angriparna uppmärksammades på att sjukhuset drabbats avslutade de angreppet.

Att underrättelseinhämtning överväger medan exempelvis sabotage är mycket ovanligt kan bero på att inhämtning av information är enklare att göra i cyberdomänen medan sabotage är enklare att genomföra utanför cyberdomänen (3.4). Det kan också tänkas att sabotage visserligen är ovanligt, men att det får mycket fokus med tanke på att det skulle kunna få spektakulära effekter.

Vad gäller vilka länder som oftast drabbas av operationerna syns USA som det vanligaste offret (i en fjärdedel av operationerna) i absoluta tal i CFR-databasen (se avsnitt 3.4). Att databasen räknar USA som det vanligaste offret beror förmodligen delvis på att databasens källor i huvudsak är engelskspråkiga (snarare än exempelvis kinesiska eller ryska) (3.4). Det kan också bero på att amerikanska mål är attraktiva. Statistiken indikerar i alla fall att det går att tämligen framgångsrikt slå mot resursstarka och tekniskt välutvecklade motståndare. Det bör dock noteras att operationerna i huvudsak riktar sig mot privata företag snarare än (direkt) mot myndigheter, så detta behöver inte säga något om den amerikanska militärens motståndskraft.

Vad gäller direkta tekniska effekter beskrivs sådana främst i tekniska utredningar av cybersäkerhetsföretag som sannolikt saknar kunskap om bakomliggande motiv (3.4). För sekundära effekter är de främsta källorna istället expertutlåtanden och anonyma källor i nyhetsartiklar (3.4). Det gör det svårt att se en tydlig koppling mellan en operation som utförs på ett visst sätt och en viss typ av effekt. Detta försvårar helhetsbilden av en cyberoperation. Dessutom är de tekniska systemen komplexa, det är svårt att veta exakt vad det avsedda offret har för system och det är en utmaning att se till att bara det avsedda offret drabbas. Exempelvis kan använda cybervapen oftast återanvändas. Sammantaget är det alltså svårt att (åtminstone med öppna källor) förutsäga vilken effekt en typisk cyberoperation får.

[12] Att cyberoperationer bara till ett fåtal procent utgörs av sabotage stämmer väl med andra källor (Maness m.fl., 2017; Kjaerland, 2006).

Framtida forskning bör besvara följande frågor:

- Vilka politiska och militära mål brukar cyberoperationer ha och vilka andra mål vore lämpliga? (2.5)
- Hur enkelt är det att begränsa ett cybervapens verkan till ett fåtal system och hur kan det avgöras hur riktad en operation var tänkt att vara? (3.4)
- Hur riktade operationer vill stater utföra och i vilken utsträckning bryr de sig om sidoskador i cyberdomänen? (3.4)
- Varför finns så få cybersabotage beskrivna i källorna? Uppnås konsekvenserna av cybersabotage enklare på annat vis?

4.4 Vilka kompetenser, metoder, tekniker och verktyg krävs för att utföra cyberoperationer?

Det råder olika meningar om vad som krävs för att utföra cyberoperationer (2.5). Baserat på de cyberoperationer som finns beskrivna i öppna källor finns det en hel del som talar för att det inte krävs så mycket sofistikation för att utföra cyberoperationer. Exempelvis bygger operationerna oftast på enkel rekognoscering, grundläggande nätfisketekniker och enkla ledningsinfrastrukturer. Vidare återanvänds verktyg från tidigare operationer (egna eller andras) och det går till och med att köpa in cybervapen, vilket minskar kraven på teknisk förmåga. Baserat på tillgängliga källor verkar angripare sällan bry sig om att rikta in vapnen så att de inte även slår mot andra än avsett offer. Sannolikheten för att bli identifierad som upphovsman verkar också låg, likaså de möjliga konsekvenserna för upphovsmannen. Mot denna bakgrund är det inte förvånande att även mindre resursstarka stater rapporteras ha legat bakom cyberoperationer. (återgivet från avsnitt 3.4)

Men det finns också saker som talar för att det faktiskt krävs en hel del sofistikation för att utföra cyberoperationer. Först och främst verkar kanske operationer enkla eftersom det bara är de enkla som är lätta nog att upptäcka. På liknande sätt upptäcks kanske inte mer resurskrävande och smartare rekognoscering medan avancerade tekniska metoder kan vara alltför svåranalyserade för att förstås och beskrivas. Vidare kräver införskaffandet av cybervapen att man vet vad man behöver och vid köp krävs finansiella muskler. Det är också möjligt att statsaktörer är noggranna med att deras vapen bara slår mot avsett mål, varför de måste lägga betydande arbete på att målinrikta vapnen. Vad gäller identifieringen av angripare är det möjligt att underrättelsetjänster lyckas väl, men helt enkelt inte talar högt om det. Dessutom har stater vissa maktmedel gentemot varandra, som exempelvis sanktioner. Upptäckta operationer kan dessutom avslöja vilka metoder som använts och därmed rendera använda cybervapen verkningslösa i framtiden. Avslutningsvis tyder källorna på

att det alltjämt främst är resursstarka länder som utför operationer, vilket indikerar att det trots allt krävs större mängder tid, möda, personella resurser och organisatorisk färdighet för att utföra cyberoperationer. (återgivet från avsnitt 3.4)

Framtida forskning bör besvara följande frågor:

- Vad kan man säga om operationer som inte upptäckts, det vill säga mörkertalet som förmodligen är de mest sofistikerade cyberoperationerna? (3.4)
- Hur väl stoppas typiska cyberoperationer av standardskydd? Hindras hela operationer av enskilda skydd eller kan operationernas detaljer ändras och fortgå? (3.4)
- I vilken utsträckning kan cyberoperationsförmåga köpas? (3.4)
- Hur kan man öka sin sikt i cyberdomänen, exempelvis genom utplacering av sensorer på strategiska platser? (se även 4.2)
- Hur enkelt är det att avslöja någons identitet, exempelvis baserat på dennes programmeringsstil? (3.4) (se även 4.2)
- Vilket behov finns av att göra cyberoperationer mer riktade och hur enkelt är det att möta behovet? (3.4) (se även 4.3)

4.5 Hur kan tester, övningar och utbildningar nyttjas för att öka, utveckla, vidmakthålla och värdera önskade förmågor i cybermiljön?

Med hjälp av övningar kan människors cyberoperationsförmåga utvärderas och höjas samt utrustning testas (3.5). I de tekniska simuleringsövningar som används i Sverige ligger fokus på att höja människors förmåga (3.5). FOI har arrangerat flera sådana cyberövningar. Under projektet genomförde projektgruppen övningen SAFE Cyber 2019 där många olika Försvarsmaktsnära myndigheter och företag deltog som övande (3.5). I samband med övningen studerades bland annat forskningsfråga 2 om situationsförståelse (se 3.10). Projektgruppen har också varit delaktig i genomförandet av de årliga övningar som går under namnet Locked Shields. I Locked Shields deltar i huvudsak europeiska myndigheter och övningen leds av Nato-ackrediterade cyberförsvarscentret CCDCOE i Tallinn, Estland (3.13).

Ingen övning är den andra lik och det finns gott om administrativa utmaningar för planering och utförande av övningar. Det är också överhuvudtaget svårt att få tag i tillräckliga data för att kunna återskapa eller simulera operationer som skett, varför realistiska övningar är svårgenomförda (2.5). Utförandet av övningar underlättas dock av FOI:s cyberanläggning CRATE. Dessutom kan övningar som

fokuserar på effekter vara lättare att genomföra eftersom effekterna är mindre varierade än operationernas utförandesätt (3.2). Det är en utmaning att kombinera tekniska övningar med övningar på ledningsnivå (3.5). Det finns dessutom administrativa utmaningar med att utföra övningar med många människor inblandade (3.5).

För att genomföra kostnadseffektiva övningar bör det som ska övas väljas ut baserat på vissa kriterier. Kriterier som föreslagits i projektet är hur sannolikt det skulle vara att en viss effekt förekom i skarpt läge, hur lätt det är att öva och upptäcka effekten, hur väl effekten kan simuleras givet tidsramarna, samt i vilken mån simuleringen av effekten inte förstör för resten av övningen (3.9).

Framtida forskning bör besvara följande frågor:

- Vilka delar av cyberoperationer bör övas i cyberanläggningar respektive skrivbordsövningar?
- Vilka tillvägagångssätt och vilka effekter går att öva och vad är alltför kostsamt i form av tidsåtgång, skador och annat?
- Vilka typer av forskning är möjliga att förena med lärandet hos övningsdeltagare och deras organisationer?

4.6 Vad finns det för problematik kopplat till etik, juridik och folkrätt avseende operationer i cyberdomänen?

Folkrättsligt saknas klara regler för vad som är tillåtet i cyberdomänen och istället finns skillnader i olika länders syn (3.1; 3.3). De folkrättsliga normerna är klarare i sammanslutningar med likasinnade stater såsom EU och Nato (3.1). Det finns också icke-bindande vägledningar såsom Tallinnmanualen (3.1). Vidare kan folkrätten på angränsande områden som yttre rymd, autonoma vapensystem och artificiell intelligens visa hur folkrätten för cyberoperationer kommer utvecklas (3.1). Det råder dock olika meningar om det är en framkomlig väg att utgå från angränsande områdens folkrätt för att skapa folkrätt för cyberdomänen (2.5).

Förutom att det behöver finnas tydliga överenskomna regler måste det också gå att utkräva ansvar av den som bryter mot rätten. I praktiken begränsas dock effekten av folkrätten av svårigheten att avgöra vem som utförde en cyberoperation (attribueringen) (3.4).

En aspekt som folkrätten behöver reglera är vad militär verksamhet får agera mot. I cyberdomänen finns inte alltid klara distinktioner mellan vad som är militärt och vad som är civilt. På många sätt är istället militära och civila system sammanflätade (2.5). Exempelvis kan militär verksamhet bygga på civil infrastruktur och cybervapentillverkare kan komma att räknas som militärer om

de gör uppdateringar av vapnen strax före vapnen används (2.5). Sammanflätningen gör det svårt att säga när en operation är riktad mot militära eller civila mål. Det är också oklart i vilken utsträckning det ens är tillåtet att skicka cybervapen via civila nät (2.5).

En annan aspekt folkrätten behöver reglera är vilket agerande i cyberdomänen som anses utgöra vapenanvändning, alltså hur och när suveräna stater får agera med våld mot andra suveräna stater. Enligt Natos regler kan cyberangrepp föranleda kollektivt självförsvar (3.1). Cyberangrepp kan alltså likt kinetiska angrepp betraktas som en form av aggression och väpnat angrepp (3.1). Förmodligen finns det ett samband mellan styrkan i cyberangrepps effekter och deras legalitet (2.5). En del röster har ansett användningen av cybervapen så allvarlig att den bör minimeras med icke-spridningsavtal likt de för kärnvapen (2.5). I samband med detta finns också idéer om att skapa etiskt stigma kring användningen av cybervapen på motsvarande sätt som för kemiska, biologiska, radiologiska och nukleära vapen (2.5).

Framtida forskning bör besvara följande frågor:

- Hur kan sidoskador undvikas på neutrala och civila? (2.5) (se även 4.2 och 4.3)
- Var går skiljelinjen mellan civila och militära mål? (2.5)

5 Referenser

Referenserna är indelade i två avsnitt, där första avsnittet (5.1) utgörs av referenser till det som publicerats i projektet. Övriga referenser återfinns i ett andra avsnitt (5.2).

5.1 Publicerat i projektet

Granåsen, D. 2019. Implementing cyber effects in M&S. An overview of FOI research modeling and simulation of the effects of cyber operations. FOI Memo 6780. Totalförsvarets forskningsinstitut.

Granåsen, D., Jaitner, M. 2019. The Offensive Cyber Operations Playbook. European Conference on Cyber Warfare and Security. (FOI-S--6150--SE. Totalförsvarets forskningsinstitut.)

Karlzén, H. 2018. Operationer i cyberdomänen. En inventering av internationell forskning. FOI-R--4614--SE. Totalförsvarets forskningsinstitut.

Karlzén, H. 2019. Cyberoperationers attribution, tillvägagångssätt och sofistikation. FOI-R--4834--SE. Totalförsvarets forskningsinstitut.

Karlzén, H. 2020. Usefulness of Cyber Attribution Indicators. European Conference on Cyber Warfare and Security.

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

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

Karlzén, H., Wedlin, M. 2018. Inventering av svensk forskning inom cyberförsvar. FOI Memo 6451. Totalförsvarets forskningsinstitut.

Lif, P., Varga, S., Wedlin, M., Lindahl, D., Persson, M. 2020. Evaluation of Information Elements in a Cyber Incident Report. IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).

Lindahl, D. 2019a. Cyberoperationer - Vem gör vad mot vem?. Youtube. (3 juni.) https://youtube.com/watch?v=ArDc538mv2Y

Lindahl, D. 2019b. Omvärldsbevakning statsattribuerade cyberoperationer 2019. FOI Memo 6963. Totalförsvarets forskningsinstitut.

Lindahl, D. 2020. Omvärldsbevakning statsattribuerade cyberoperationer 2020. Totalförsvarets forskningsinstitut. FOI Memo 7422.

Lindahl, D., Liljedahl, B. 2020. I skuggan av pandemin: cyberattackerna ökar. Youtube. (5 maj.) https://www.youtube.com/watch?v=YRJdr5MCRSM

Nato. 2020. Top Ten Cyber Effects for Campaign and Mission Simulations.

SISO. 2020. SISO-REF-070-2020. Final Report for the Cyber Modeling and Simulation (M&S) Study Group (SG). Simulation Interoperability Standards Organization.

Valassi, C., Wedlin, M. 2019. Övningsrapport: SAFE Cyber 2019. Planering, utveckling, genomförande och lärdomar av en storskalig CDX-övning. FOI-R--4885--SE. Totalförsvarets forskningsinstitut.

Wedlin, M., Granåsen, D., Brynielsson, J., Zuoave, E., Varga, S., Wesslau, K., Lindahl, D., Luotsinen, L. 2017. Utveckling av forskningsområde Operationer i cyberdomänen. FOI Memo 6248. Totalförsvarets forskningsinstitut.

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

Zouave, E. 2020. De svenska definitionerna inom aktivt cyberförsvar. FOI-D--0981--SE. Totalförsvarets forskningsinstitut.

Zouave, E., Lindahl, D. 2019. Folkrätt vid aktiva operationer på cyberdomänen. (24 juni.) Youtube. https://youtube.com/watch?v=lGiVaRYPQuM

5.2 Övriga referenser

Arquilla J., Ronfeldt, D. 1993. Cyberwar is Coming!, Comparative Strategy, vol. 12:2.

Bildsten, C., Karlzén, H., Westerdahl, L., Lundholm, K., Eidenskog, E., Karresand, M. 2020. Förstudier inom informationssäkerhet. Cyberlägesbild, virtualiserade referensmiljöer och datacentrerad säkerhet. FOI-R--5068--SE. Totalförsvarets forskningsinstitut.

Boleng J., Schweitzer, D., Gibson, D.S. 2008. Developing cyber warriors, 3rd International Conference on Information Warfare and Security.

Brynielsson J., Franke U., Varga S. 2016. Cyber Situational Awareness Testing. Combatting Cybercrime and Cyberterrorism. (FOI-S--5619--SE. Totalförsvarets forskningsinstitut.)

CCDCOE. 2020. About Us. https://ccdcoe.org/about-us/

De Tomas Colatin, S., Väljataga, A. 2020. Data as a weapon: refined cyber capabilities under weapon reviews and international human rights law. CCD COE, Nato.

Eddy, M., Perlroth., N. 2020. Cyber Attack Suspected in German Woman's Death. NY Times. 18 september. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

Englund, J. 2019. Kinas industriella cyberspionage. FOI Memo 6698. Totalförsvarets forskningsinstitut.

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

Fiorenza N. 2007. NATO considers response to cyber warfare following attacks on Estonia, Jane's International Defence Review, vol. juni.

Franke, U. 2015. War by non-military means: Understanding Russian information warfare. FOI-R--4065--SE. Totalförsvarets forskningsinstitut.

Franke, U., Brynielsson, J. 2014. Cyber situational awareness - A systematic review of the literature. Computers & Security vol. 46. (FOI-S--4736--SE. Totalförsvarets forskningsinstitut.)

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

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

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

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

Försvarets radioanstalt och Försvarsmakten. 2016. Överenskommelse om gemensamma begrepp för cyberområdet. Bilaga 1 till FM 2016-12950.

Försvarsberedningen. 2013. Vägval i en globaliserad värld. Ds 2013:33. Försvarsdepartementet.

Försvarsdepartementet. 2015. Inriktning för Försvarsmaktens verksamhet för åren 2016 till och med 2020. Fö2015/00953/MFI.

Försvarsmakten. 2018. Inriktning av Försvarsmaktens plan för forskning och teknikutveckling. FM2016-23660:3.

Försvarsmakten. 2020. Doktrin för Gemensamma operationer. DGO 20. FM2018-18369:30.

Försvarsutskottet. 2015. 2014/15:FöU11 Försvarspolitisk inriktning – Sveriges försvar 2016–2020.

Giles, K., Hagestad, W. 2013. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. 5th International Conference on Cyber Conflict.

Grennert, J., Tham Lindell, M. 2002. Cyberterrorism. Öppnar IT för nya möjligheter för terrorism?. FOI-R--0626--SE. Totalförsvarets forskningsinstitut.

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

Hagström Frisell, E., Zetterlund, K. 2013. Getting it Right in Uncertain Times. The Defence Priorities of the United States, the United Kingdom and France. FOI-R--3695--SE. Totalförsvarets forskningsinstitut.

Hammervik, M., Klum, P., Lif, P., Johansson, B., Castor, M., Tydén, L. 2009. Slutrapport LKS. Metodutveckling. FOI-R--2843--SE. Totalförsvarets forskningsinstitut.

Harrington C. 2008a. USAF doctrine pushes cyber warfare as kinetic alternative, Jane's Defence Weekly, vol. april.

Harrington C. 2008b. USAF creates new career track for cyber experts, Jane's Defence Weekly, vol. juli.

Heickerö, R. 2006. Informationskrig i cyberrymden. Elektronisk och digital krigföring i en breddad hotbild. FOI-R--2028--SE. Totalförsvarets forskningsinstitut.

Heickerö, R. 2008. Utveckling av strategier och förmåga till informationskrigföring och informationsoperation i Kina. FOI-R--2556--SE. Totalförsvarets forskningsinstitut.

Heickerö, R. 2010. Emerging Cyberthreats and Russian Views on Information Warfare and Information Operations. FOI-R--2970--SE. Totalförsvarets forskningsinstitut.

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

Huskaj, G., Iftimie, I.A. 2020. Toward an ambidextrous framework for offensive cyberspace operations: a theory, policy and practice perspective. Proceedings of the 15th International Conference on Cyber Warfare and Security.

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

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

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

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

Kindvall, G. 2005. Effektbaserade operationer. FOI-R--1454--SE. Totalförsvarets forskningsinstitut.

Kindvall, G., Nordstrand, E. 2003. FoRMA IW – Sammanfattning av genomfört arbete. FOI-R--0795--SE. Totalförsvarets forskningsinstitut.

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

Jaitner, M., Sommestad, T. 2019. I: Kukkola, J., Ristolainen, M., Nikkarila, J.P. 2019. Game Player. Facing the structural transformation of cyberspace. Försvarsmaktens forskningsanstalt.

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

Lif, P., Granåsen, M., Sommestad, T. 2017. Development and validation of technique to measure cyber situation awareness. International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). (FOI-S--5779--SE. Totalförsvarets forskningsinstitut.)

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

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

Lundholm, K., Löfvenberg, J., Hunstad, A., Karlzén, H. 2011. Lägesbild på informationsarenan. Översikt och diskussion. FOI-R--3240--SE. Totalförsvarets forskningsinstitut.

Maness, R.C., Valeriano, B., Jensen, B. 2017. Dyadic Cyber Incident and Dispute Data. file.prio.no/journals/JPR/2014/51/3/Valeriano%20&%20Maness%202014%20replication%20&%20codebook.zip

Mittermaier, E., Westrin, P. 1999. Infrastrukturens sårbarhet med avseende på logiska, IT-relaterade hot. FOA-R--99-01052-240--SE. Försvarets forskningsanstalt.

Nakashima, E., Warrick, J. 2012. Stuxnet was work of U.S. and Israeli experts, officials say. The Washington Post. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Regeringen. 2017. Nationell strategi för samhällets informations- och cybersäkerhet. Regeringens skrivelse. 2016/17:213.

Schubert, J., Clausen Mork, J., Johansson, R., Sommestad, T., Svensson, M., Thorell, H. 2016. Vilseledning av lägesbild. FOI-D--0717--SE. Totalförsvarets forskningsinstitut.

Severin, M. 2018. Tidig förvarning och icke-militära angreppssätt. FOI-R--4577--SE. Totalförsvarets forskningsinstitut.

Sommestad, T., Hallberg, J. 2012. Cyber security exercises and competitions as a platform for cyber security experiments. Proceedings of NordSec. (FOI-S--4218--SE. Totalförsvarets forskningsinstitut.)

U.S. Cyber Command. 2020. U.S. Cyber Command History. https://www.cybercom.mil/About/History/

Vendil Pallin, C. 2017. Rysslands långsiktiga informationssäkerhetsstrategi. FOI Memo 6309. Totalförsvarets forskningsinstitut.

Vendil Pallin, C. 2019a. Ryssland nationaliserar internet - lagförslaget om ett ”suveränt internet”. FOI Memo 6680. Totalförsvarets forskningsinstitut.

Vendil Pallin, C. 2019b. Russian information security and warfare. I Routledge Handbook of Russian Security. (FOI-S--6016--SE. Totalförsvarets forskningsinstitut.)

Vidström, A. 2002. Analys av Insider Virus. FOI-R--0750--SE. Totalförsvarets forskningsinstitut.

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

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

Wedlin, M., Nilsson, P., Komulainen, A., Kamrani, F., Svensson, J., Krona, M., Bengtsson, J. 2019. Polisiära cyberhot. Tekniska möjligheter. FOI-R--4739--SE. Totalförsvarets forskningsinstitut.

Wedlin, M., Westring, E. 2017. Internet som militär arena – en utmaning i totalförsvaret. I Hull Wiklund, C., Faria, D., Johansson, B. Öhrn-Lundin, J. (red.). 2017. Strategisk utblick 7. Närområdet och nationell säkerhet. FOI-R--4454--SE. Totalförsvarets forskningsinstitut.

Westerdahl, L. 2020. Metodik för övning i cybermiljö – en statusrapport. FOI Memo 7001. Totalförsvarets forskningsinstitut.

Wiener, N. 1948. Cybernetics: Or Control and Communication in the Animal and the Machine. MIT Press.

Zouave, E., Colde, K. 2020. Cyberövningar i det svenska och europeiska policylandskapet. FOI Memo 7291. Totalförsvarets forskningsinstitut.

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

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