Kapittel 1

Stuxnet – et paradigmeskifte?

Claudia Emilie Aanonsen, Eskil Jakobsen og Niels Nagelhus Schia

Natanz, Iran, 2008. På en øde plass står et anlegg for anrikning av uran, et materiale som brukes i fremstillingen av atomkraft og atomvåpen. Fra 2008 opplever forskere og operatører ved anlegget Natanz at sentrifugene, som er vitale for anrikningsprosessen, fra tid til annen svikter i stor skala. Ingen forstår hvorfor når monitorene i kontrollrommet viser at alt fungerer som det skal. Gjentatte utskiftinger av sentrifuger gjøres over flere år før de avdekker en godt skjult digital skadevare i systemene sine, senere kjent som Stuxnet.

Minsk, Hviterussland, 2010. I kontorene til det lille hviterussiske IT-selskapet VirusBlokAda sitter Sergey Ulasen og hans kollega Oleg Kupreev en alminnelig arbeidsdag i juni. De analyserer en skadevare som har infisert datamaskinen til en kunde i Iran. De avdekker en eller flere nulldagssårbarheter av sjeldent kaliber. Var det noe mer enn typisk cyberkriminalitet? Ulasen skriver et innlegg som spres raskt på et IT-sikkerhetsforum.

Washington D.C., USA, 2010. Kort tid etter at innlegget til Ulasen publiseres, ankommer CIA-direktør Leon Panetta situasjonsrommet i Det hvite hus. President Barack Obama får beskjed om at operasjon Olympic Games kan være avslørt. Skadevaren rettet mot Natanz har gått viralt og spres til datamaskiner over hele verden. IT-miljøer har fått nyss om angrepet og døpt skadevaren Stuxnet. De har foreløpig ikke fått oversikt over angrepets omfang eller herkomst, men koden ligger fritt tilgjengelig og kan havne i feil hender. For Obama er det først og fremst avgjørende at angrepet ikke blir attribuert til USA.

Innledning

Da Stuxnet ble offentlig kjent i 2010, viste de store fysiske, eller *kinetiske*, skadevirkningene at digital skadevare kunne sabotere funksjonaliteten til

infrastruktur, forårsake alvorlige ødeleggelser og ikke minst fungere som et politisk pressmiddel. Dette representerte noe helt nytt. Dette kapittelet belyser hvordan Stuxnet har påvirket hvordan stater benytter seg av cyberkapabiliteter i konflikt, og hvordan cyberoperasjoner oppfattes.

Vi forfekter at angrepet representerer et *paradigmeskifte*, og bygger denne argumentasjonen på en analyse av angrepet og dets etterspill. Utviklingen i cyberdimensjonen av konflikten mellom USA og Israel versus Iran, og dessuten andre staters opprustning av cyberkapasiteter, er også viktige bestanddeler i analysegrunnlaget.[4] Skiftet gjelder bruk av cyberoperasjoner i konfliktsituasjoner og utvikling av offensive og defensive cyberkapabiliteter etter Stuxnet. Paradigmeskiftet innebar at cyberoperasjoner *kan* benyttes som en alternativ måte å hevde sikkerhetspolitiske interesser på. Ikke bare i gråsonen som et supplement mellom diplomati og militære virkemidler, men også som et *substitutt* til konvensjonell militærmakt (Maschmeyer, 2021; Kostyuk & Gartzke, 2022).

Argumentasjon rundt den strategiske betydningen av cyberoperasjoner omhandler i stor grad spesifikke konfliktscenarioer og bygger på klassisk strategisk teori. For å belyse måten Stuxnet har påvirket staters oppfatning av cyberoperasjoner og cyberdomenet generelt, supplerer vi med et konstruktivistisk perspektiv. En slik forståelse av cybertrusler viser hvordan hendelser blir fremstilt av eksperter og i medier, og kontekstualiserer endringer i staters sikkerhetspolitiske disposisjoner i cyberdomenet. Tilnærmingen illustrerer at det er flere teoretiske perspektiver som kan bidra til økt forståelse av hvordan stater benytter og forstår cyberoperasjoner i konflikt.

I takt med digitaliseringen har de fleste stater i verden utviklet defensiv cyberkapasitet. Med digitale løsninger for å drifte kritisk infrastruktur – alt fra tilgang til rent vann, strømnett, telekommunikasjon, transport til betalingssystemer – er det blitt avgjørende for stater å beskytte egne systemer og nettverk. Cyberdomenet ble ved NATO-toppmøtet i Warszawa i 2016 erklært som et femte domene for krigføring på lik linje med land, sjø, luft og verdensrom (Libicki & Tkacheva, 2020). Mange stater har også satset på å utvikle offensive cyberkapabiliteter som ledd i avskrekkingsstrategier (se også Aannøs kapittel 4) eller som våpen for oppnåelse av sikkerhetspolitiske mål (Fanelli, 2016). Denne typen opprustning er derfor betydningsfull for hvordan mellomstatlig konflikt og eskalering forstås i det 21. århundret.

4 Thomas Kuhns konseptualisering av paradigmeskifter innebærer en totalomveltning av grunnleggende dogmer innenfor en vitenskapelig disiplin (Kuhn, 1996). Her benyttes begrepet imidlertid for å beskrive utvikling som er mindre omfattende enn Kuhns konseptualisering.

For å forstå cyberoperasjoner er det viktig å skille mellom *cyberkriminalitet* som sivile datainnbrudd og *cyberangrep* med sannsynliggjort statlig opphav.[5] Cyberangrep som blir utført av stater, skjer som regel i form av spionasje eller sabotasje (Schulze et al., 2020). Stuxnet faller inn under sistnevnte kategori som statlig maktbruk gjennom en operasjon ved navn Olympic Games. Skadevaren ble i hovedsak utviklet av USA og Israel med mål om å svekke Irans atomprogram gjennom flerårig digital sabotasje. Da operasjonen ble allment kjent, skapte det stor bekymring verden rundt. Det spredte seg en forestilling om at vi ville oppleve et cyber-Pearl Harbor, og at vi sto overfor en cyberkrig (Buchanan, 2020; Lindsay, 2013, s. 373; Sanger, 2012; 2018; Zetter, 2014). Selv om denne bekymringen har mildnet, og frykten for cyberkrig er dempet (Smeets & Soesanto, 2020; Maschmeyer, 2021), forstår mange i dag skadepotensialet i cyberoperasjoner og -angrep som langt mer alvorlig enn det man trodde før 2010.

Fordi Stuxnet forårsaket kinetiske ødeleggelser, forekom det et betraktelig opprykk i offentlig diskurs om hvordan cyberangrep bør håndteres. I forlengelsen bidro dette også til å endre staters oppfatning av spillereglene for bruk av cyberkapabiliteter i konfliktsituasjoner (Jervis, 2016). For å undersøke hvorvidt operasjonen innebærer et paradigmeskifte i denne sammenheng, anser vi det som nødvendig å vurdere om Olympic Games endret cyberoperasjoners strategiske betydning i mellomstatlig konflikt. I kapittelets første del beskrives statlige cyberoperasjoner og den politiske bakgrunnen for Stuxnet. I andre del presenteres en gjennomgang av hendelsesforløpet under planleggingen og gjennomføringen av operasjonen. Deretter beskrives etterspillet, som danner grunnlaget for den påfølgende analysen av paradigmeskiftet.

Gjennom dokument- og diskursanalyse har vi identifisert paradigmeskiftet som tredelt: 1) et skifte i den strategiske betydningen av cyberoperasjoner, 2) et skifte i staters forestilling om sikkerhetstrusler i cyberdomenet og 3) et skifte mot økt sikring av industrielle kontrollsystemer (IKS) som del av strategier for å ivareta nasjonal sikkerhet.

Veien til Stuxnet

Cyberoperasjoner med statlig opphav var ikke noe nytt fenomen da Stuxnet ble oppdaget i 2010. Det mange regner som den første mellomstatlige cyber-

5 *Cyberkriminalitet* er et samlebegrep for ulike typer dataangrep og innbrudd i cyberdomenet utført av ikke-statlige aktører. *Løsepengevirus*, eller digital utpressing, er en fremtredende form for cyberkriminalitet og utføres gjerne av aktører ute etter finansiell vinning. *Cyberangrep* med statlig opphav er angrep utført eller støttet av stater, som regel for å svekke motstandere med sikte på å hevde egne sikkerhetspolitiske interesser.

operasjonen, blir kalt Moonlight Maze. Fra 1996 til 1998 stjal hackere tusenvis av sensitive dokumenter fra det amerikanske forsvaret og andre offentlige institusjoner. USA har beskyldt Russland for å stå bak denne operasjonen (Buchanan, 2020, s. 318). Et annet eksempel er da store deler av den amerikanske våpenindustrien og myndighetsapparatet ble rammet av en rekke datainnbrudd mellom 2003 og 2006. Operasjonene fikk kallenavnet Titan Rain og ble attribuert til kinesisk etterretning (Council on Foreign Relations, u.å.k; Buchanan, 2017, s. 51–52). I 2007 ble en rekke estiske organisasjoner og statlige organer utsatt for vedvarende alvorlige tjenestenektangrep med sannsynliggjort opphav fra russiske sikkerhetsmyndigheter (Council on Foreign Relations, u.å.g; Lawson, 2013, s. 87–89). Disse angrepene hadde konsekvenser for sikkerhetstilstanden i USA og Estland, men var imidlertid begrenset til lekkasje av gradert informasjon og manglende funksjonalitet i IKT-systemer. Tradisjonell skadevare som benyttes til *tjenestenektangrep*, *trojanske hester*, *tasteloggere* og *spionprogramvare*, har i utgangspunktet ikke evnet å forvolde kinetisk skade.[6] Stuxnet skiller seg tydelig fra tidligere angrep fordi skadevaren var utformet med mål om fysisk sabotasje, med egenskaper som gjør det hensiktsmessig å betrakte den som såkalt *weaponized malware* eller *cybervåpen* (Knapp & Langill, 2014; Vega et al., 2017). På grunnlag av dette har den blitt beskrevet som «verdens første digitale våpen» (Zetter, 2014).

USA og Israels relasjon til Iran var i årene før Stuxnet preget av vedvarende spenninger grunnet daværende president Mahmoud Ahmadinejads ambisjoner om å videreutvikle atomprogrammet til Iran gjennom blant annet høyanrikning av uran.[7] Det ble ansett som lite sannsynlig at anrikningen utelukkende hadde til hensikt å bygge opp et sivilt atomprogram for kraftutvinning (Buchanan, 2020). Da USA invaderte Irak i 1991, økte spenningene i regionen, særlig mellom Israel og Iran. Iran brakte atomvirksomheten sin under jorda og testet for første gang urananrikning. Omtrent på samme tid som Natanz ble bygget i 2000, anerkjente det internasjonale samfunnet Iran som en atomstat (Zetter, 2014).

6 *Distribuerte tjenestenektangrep* (distributed denial-of-service (DDoS)) er angrep med hensikt å hindre tilgang til informasjon eller ressurser i datasystemer. *Trojanske hester* er skadevare med tiltak som kan skape «kaos» på brukerens datamaskin, for eksempel ved å blokkere, stjele, endre eller slette data, eller kompromittere maskinen og nettverket. Skadevaren er som regel avhengig av å aktiveres av en bruker og fremstår derfor som tilsynelatende legitim, derav navnet «trojansk hest». *Tasteloggere* (keylogger) er programvare som brukes for å registrere og loggføre tasketrykk på datamaskiner. *Spionprogramvare* (spyware) er skadevare som kan overvåke brukerens aktivitet på en datamaskin.

7 Anrikning er prosessen hvor man skiller ut det fissile stoffet uran-235 i sentrifuger som spinner i høy hastighet. Uran er stoffet som brukes for å utvikle atomvåpen gjennom høyanrikning (Heireng, 2015, s. 22–23; Zetter, 2014, s. 75).

Frykten for at atomprogrammets fremgang skulle føre til våpenkappløp, og i verste fall atomkrig, gjorde det vesentlig for USA å gjøre et forsøk på å stanse utviklingen. Etter etterretningsfiaskoen i Irak 2003 hadde USA verken politisk handlingsrom eller støtte til å invadere et nytt land i Midtøsten basert på indisier. Samtidig økte presset fra den israelske presidenten Benjamin Netanyahu, som indikerte at Israel var forberedt på å gå til angrep mot anrikningsanlegget i Natanz (Buchanan, 2020, s. 130; Sanger, 2018, s. 39; Lindsay, 2013, s. 398). President Bush sto i en krevende situasjon. USA kunne risikere å bli involvert i en krig med Iran. Forsøk på diplomatisk løsning eller fravær av handling ville falt i dårlig jord hos israelerne og potensielt legge til rette for iranernes utvikling av atomvåpen. Bush fortalte staben sin at han trengte et tredje alternativ. US Strategic Command presenterte en løsning som kunne både avverge et israelsk luftangrep på anrikningsanlegget, bremse det iranske atomprogrammet og få Iran til forhandlingsbordet: en cyberoperasjon, som over flere år skulle sabotere urananrikningen ved Natanz. Operasjonen ble iverksatt og fikk navnet Olympic Games (Sanger, 2012; 2018).

Operasjon Olympic Games

Planleggingen av Olympic Games foregikk over flere år som et samarbeid mellom National Security Agency (NSA), United States Cyber Command (USCYBERCOM) og den israelske signaletterretningsenheten Unit–8200, i tillegg til etterretning fra britiske Government Communications Headquarters (GCHQ). USAs Central Intelligence Agency (CIA) hadde overordnet myndighetsansvar for operasjonen (Sanger, 2018, s. 27, 174; Zetter, 2014).

I planleggingsfasen bygget personell fra NSA og Unit–8200 replikaer av Natanz. Dette muliggjorde grundig testing før de tok seg inn i anrikningsanleggets kontrollsystem med skadevare (Buchanan, 2020, s. 134; Sanger, 2012, s. 176–177). Allerede mot slutten av Bushs presidentperiode hadde tidlige versjoner av Stuxnet infiltrert og gjort skade på Natanz. I 2009, da Barack Obama skulle innsettes som ny president, ble han i en orienteringssamtale med Bush introdusert for den graderte operasjonen. Iranerne var på dette tidspunktet fullstendig uvitende om at de var offer for digital sabotasje. For å fortsette bremsingen av Irans atomprogram autoriserte Obama videreføringen av operasjonen (Buchanan, 2020; Sanger, 2012, s. 9, 171).

En utfordring for operasjonen var at kontrollsystemet for anrikningssentrifugene var fullstendig adskilt fra eksterne nettverk. Denne praksisen kalles *air-gapping* og benyttes preventivt for viktige datasystemer (Lindsay, 2013, s. 380–381; Zetter, 2014). For å infiltrere anlegget måtte Stuxnet smugles

inn fysisk via en USB-pinne og deretter gjennomføre oppgavene sine på egen hånd.[8] Skadevarens selvstendige funksjonalitet gjorde at angrepet ikke kunne avblåses etter iverksetting. Oppgavene besto blant annet av å identifisere, infiltrere og overvåke riktig mål, for deretter å manipulere dets kommandoer (Sanger, 2012; Zetter, 2014). Den mangefasetterte planleggingsprosessen gjør at operasjonen må betraktes som en kompleks og sammensatt effektoperasjon og et digitalt angrep. Dette skiller Stuxnet fra heldigitale statlige cyberoperasjoner.

Sentrifugene ved anrikningsanlegget benyttet et industrielt kontrollsystem (IKS) overvåket av Supervisory Control and Data Acquisition (SCADA). For å styre mekanismene som regulerte sentrifugenes innstillinger, ble programmerbar logisk styring (PLS) benyttet. Tidlig på 2000-tallet inneholdt IKS-systemer sjelden integrerte sikkerhetsløsninger (Applegate, 2013; Sanger, 2012). Mangel på slike sikkerhetsløsninger gjorde det enklere for Stuxnet å utnytte flere *nulldagssårbarheter* for å forårsake store ødeleggelser.[9]

På samme måte som med konvensjonelle våpen er cyberangrep bygget opp med et leveringssystem som overbringer nyttelast til et mål. Nyttelasten til Stuxnet besto blant annet av et *rootkit* som muliggjorde infiltrasjon av PLS-systemet Siemens S7-315-2.[10] Operasjonen var første kjente anledning hvor et slikt rootkit ble benyttet til å infiltrere et PLS-system (Applegate, 2013; Lindsay, 2013). Operatørene ved Natanz overvåket og sendte kommandoer til PLS-systemet gjennom Siemens-programvaren Step7 (Zetter, 2014, s. 52). Med rootkitet og en velplassert DLL-fil[11] kunne Stuxnet derfor tilegne seg administratorrettigheter og manipulere kommandoene som ble fôret til PLS-systemet gjennom Step7 slik at den gjennomførte uønskede justeringer av sentrifugene (Vega et al., 2017, s. 171; Applegate, 2013).

Da Stuxnet ble installert på PLS-systemet, var skadevaren programmert til å vente to uker før iverksetting av sabotasjen. I denne perioden registrerte og lagret Stuxnet all normal aktivitet som ble overført fra sensorene. Etter

8 Selve leveransemetoden av skadevaren gjør at Olympic Games må betraktes som en operasjon utført med ulike metoder, en kombinasjon av HUMINT (menneskebasert innhenting av etterretning) og programmering.

9 *Nulldagssårbarheter* (zero-day vulnerabilities) er ukjente sårbarheter i programvare. Disse hullene kan utnyttes av angripere før sårbarheten eventuelt oppdages av systemeier, og lukkes.

10 *Rootkit* er skadevare som bruker administratortilgang for å installeres og utføre handlinger.

11 *Dynamisk lenkebibliotek.*

to uker i passiv tilstand begynte Stuxnet å manipulere sentrifugenes omdreiningshastighet. Sentrifugene spant på det meste med en hastighet på 86 400 omdreininger per minutt. Senere senket skadevaren farten, tidvis ned til 120 omdreininger per minutt (Buchanan, 2020; Sanger, 2012). Angrepet hadde til hensikt å uoppdaget sabotere for urananrikningen, men endringene i omdreiningshastigheten over tid forårsaket at metallet i sentrifugene vibrerte ukontrollert og ristet i stykker. På grunn av skadevarens evne til å manipulere sensorenes rapportering var ledelsen ved Natanz overbevist om at det var menneskelige feil som var årsaken til skadene (Sanger, 2012, s. 169, s. 177). Det er anslått at skadevaren til sammen forårsaket destruksjon av over tusen sentrifuger (Vega et el., 2017, s. 157; Albright et al., 2010).

Sommeren 2010 ble Obama informert av CIA-direktør Leon Panetta og lederne for Olympic Games om at kopier av skadevaren var ute i det fri. Den spredte seg som ild i tørt gress – hovedsakelig i Iran, India og Indonesia, men også tilbake til USA. Dette var overraskende fordi skadevaren i utgangspunktet var bygget slik at den kun forplantet seg i Siemens PLS-systemer i Natanz (Sanger, 2012, s.181; 2018, s. 40).

Den globale spredningen ble forårsaket av at en arbeider ved Natanz koblet datamaskinen sin til sentrifugenes kontrollsystem og deretter tilbake på nettverket. Plutselig lå koden i hendene på «alle», ikke minst cybermaktene Iran, Nord-Korea, Russland og Kina (Sanger, 2018, s. 40). Det gikk ikke lang tid før den ble oppdaget og oppsporet av IT-selskaper, og på ulike nettforum begynte det å summe. Etter kort tid annonserte også Microsoft at de hadde iverksatt arbeidet med å lukke sikkerhetshull i Windows. Skadevaren fikk på dette tidspunktet kallenavnet Stuxnet av analytikere ved programvareselskapet Symantec. Det gikk likevel over et år før det ble fastslått at Stuxnets hovedmål var det spesifikke Siemens PLS-systemet ved anrikningsanlegget i Natanz (Zetter, 2014).

Etterspill

I kjølvannet av Stuxnet ble både botemidler mot cyberangrep og utvikling av offensive cyberkapabiliteter viktige prioriteringer for iranske sikkerhetsmyndigheter (Libicki, 2012; 2019; Uskowi, 2016). Et *våpenkappløp* i cyberdomenet hadde begynt. Under to år etter at iranerne forsto hva de hadde blitt rammet av, deployerte de en potent wiper-skadevare som fikk kallenavnet Shamoon. Angrepets hovedmål var det saudiarabiske statlige

petroleumsselskapet Saudi Aramco.[12] I 2012 aktiverte iranske operatører en overskrivningskomponent som kompromitterte og ødela data på over 35 000 av selskapets maskiner (Buchanan, 2020, s. 149–151).

I 2012 og 2013 gjennomførte Iran et koordinert tjenestenektangrep mot en rekke amerikanske finansinstitusjoner. De mistet evnen til å drifte tjenestene sine normalt.[13] Operasjonen, som fikk kallenavnet Ababil, har blitt beskrevet som en respons på amerikanske økonomiske sanksjoner mot Iran (Council on Foreign Relations, u.å.e). Den har også blitt beskrevet som en direkte reaksjon på Stuxnet (Libicki, 2019). Disse ulike tolkningene viser at det kan være hensiktsmessig å se cyberoperasjoner i lys av det overordnede konfliktbildet og ikke isolert kun til cyberdomenet.

I 2013 utvidet iranerne atomprogrammet sitt. Samtidig som Obama-administrasjonen forsøkte å forhandle med Iran, uttalte kasinomogulen Sheldon Adelson at USA heller burde gå til krig. Iran reagerte kraftig, og i løpet av et par måneder utførte iranske operatører et cyberangrep mot Adelsons selskap Sands Corp som forårsaket betydelige økonomiske tap. Angrepet har blitt tolket som motivert av Irans ønske om å demonstrere at også de var i besittelse av evnen til å skape destruksjon i cyberdomenet på linje med amerikanerne (Buchanan, 2017, s. 82–84).

Utover de beskrevne angrepene er det nærliggende å også se senere angrep i sammenheng med Stuxnet. Det påfølgende tiåret var preget av en rekke cyberoperasjoner med utgangspunkt i en amerikansk og israelsk offensiv mot Iran (Schulze et al., 2020). Antallet kjente operasjoner oversteg femti per begynnelsen av 2022. I tabellen under beskrives de mest alvorlige kjente operasjonene som inntraff etter Stuxnet.[14]

---

12 Skadevaren spredte seg aktivt mellom datamaskiner og nettverk før den iverksatte overskrivning av alle data på tilkoblede harddisker. De iranske operatørene lot Shamoon spre seg over store deler av Saudi Aramcos nettverk og lot den ligge i dvale inntil de hadde funnet et passende tidspunkt for å aktivere en overskrivningskomponent som slettet all data (*wiper*) ved aktivering fra iranske operatører. Rapporteringskomponenten transmitterte logg av hva viruset foretok seg til operatørene, slik at de kunne overvåke operasjonens virkning.

13 En gruppe ved navn Izz ad-Din al-Qassam Cyber Fighters påtok seg ansvaret. De rammede finansinstitusjonene var blant annet Bank of America, JPMorgan Chase, Citigroup og Wells Fargo.

14 Utvelgelsen er gjort basert på en metodikk for klassifisering av cyberoperasjoners alvorlighetsgrad utarbeidet av Kostyuk et al. (2018). Metodikken oppfatter eskalering i likhet med Herman Kahn som en stige av konfliktnivåer. De syv nivåene går fra *forberedelser til handling* til *eksistensielt angrep* (egen oversettelse). Nivåene kobles til ulike typer handlinger med konvensjonelle maktmidler og cyberkapasiteter. På grunnlag av kriteriene i stigen kan Stuxnet klassifiseres som *svært ødeleggende angrep*.

Tabell 1: Alvorlige cyberoperasjoner av Iran, Israel og USA (2010–2022)[15]

Angriper	Offer	År	Angrepsmål	Konsekvenser
USA og Israel	Iran	2010	Natanz anrikningsanlegg	1000 sentrifuger ødelagt, forsinkelser i teknologisk utvikling
Iran	Saudi-Arabia	2012	Saudi Aramco	Ødeleggelse av store mengder data
Iran	USA	2012–2013	Amerikanske banker	Manglende funksjonalitet i finansielle tjenester
Iran	USA	2013	Sands Casino	Stengt kasino, finansielle tap
USA	Iran	2019	Det iranske forsvaret	Informasjonssikkerhetsbrudd i militære datasystemer
Iran	USA	2019	Amerikanske myndigheter og kritisk infrastruktur	Informasjonssikkerhetsbrudd
Iran	Israel	2020	Israelske vannrensnings-anlegg	Risiko for klorforgiftning og tap av system for irrigasjon
Israel	Iran	2020	Shahid Rajaee-havnen	Tap av funksjonalitet i datasystemer, forsinkelser i forsyninger
Israel	Iran	2021	Natanz anrikningsanlegg	Strømbrudd, sentrifuger ødelagt

Angrepene som inntraff to til tre år etter 2010, er naturlige å se i direkte sammenheng med Stuxnet. Den senere utviklingen er imidlertid også interessant fordi Stuxnet kan oppfattes som et startskudd for en langvarig *tit for tat*-relasjon i cyberdomenet.[16]

Operasjonen som rammet det iranske forsvarets datasystemer i 2019 (Tabell 1), er iøynefallende sett i lys av cyberoperasjoners strategiske betydning, deres potensial som det tredje alternativ, og i ytterste konsekvens *substitutt* for konvensjonell militærmakt. Operasjonen var en motreaksjon fra USA mot Irans angivelige bidrag til angrep på en oljetanker og nedskytning av en amerikansk drone. Etter flere ukers planlegging gjennomførte USCYBERCOM flere angrep mot iransk etterretning og militære datasystemer. Det har blitt hevdet at operasjonen fikk klarsignal fra daværende president Trump fordi

15 Data hentet fra Council on Foreign Relations – Cyber Operations Tracker, Vega et al. (2017), Barnes og Gibbons-Neff (2019) og Chulov (2021).

16 *Tit for tat* er et begrep som beskriver en relasjon mellom stater som utfører angrep mot hverandre av gjensidig proporsjonalitet, som ikke nødvendigvis eskalerer eller de-eskalerer konflikt.

den ble bedømt til å befinne seg under terskelen for væpnet konflikt (Barnes og Gibbons-Neff, 2019). Angrepene inntraff samme dag som presidenten avviste et angrep med konvensjonell militærmakt. Operasjonen har derfor blitt beskrevet som et eksempel på en form for *trykkavlastning* hvor cyberoperasjoner fungerer som et mindre eskalerende substitutt for militærmakt (Barnes og Gibbons-Neff, 2019; Healey & Singh, 2022).

I delkapittelet presenteres et tredelt paradigmeskifte tuftet på Stuxnet, etterspillet og staters oppfatning av disse. Argumentasjonen bygger i første del på strategisk teori og undersøker endringer i de aktuelle statenes sikkerhetspolitiske disposisjoner. I andre del problematiseres scenarioer fremstilt av eksperter og medier om fremtidens bruk av cyberkapabiliteter som grunnlag for en *trussel-inflasjon*. Avslutningsvis belyses utvikling i sikringen av IKS som inntraff i kjølvannet av Stuxnet.

Paradigmeskiftet

Del 1: den strategiske betydningen av cyberoperasjoner

Staters strategiske ønske om å *avskrekke* fiender fra å gjennomføre angrep, kobles ofte sammen med både defensive og offensive cyberkapabiliteter. I tråd med tradisjonell strategisk teori øker defensiv kapasitet motstandsdyktigheten. Slik blir det vanskeligere og mer ressurskrevende for en fiende å angripe. Offensiv kapasitet muliggjør effektive motangrep som kan straffe en eventuell angriper. Et sentralt mål bak utvikling av defensiv og offensiv kapasitet er altså å øke kostnaden ved å angripe slik at det blir lite attraktivt for en motpart (Fanelli, 2016). Hvorvidt effektiv avskrekking av motstandere i cyberdomenet er mulig, har vært gjenstand for betydelig debatt (se for eksempel Aannøs kapittel 4 i denne boken eller Jervis, 2016; Libicki, 2009; Schulze et al., 2020; Smeets & Soesanto, 2020).

I analyse av tradisjonell militær opprustning er *sikkerhetsdilemmaet* et fremtredende konsept. Dilemmaet dikterer at stater vil ruste opp når de blir klar over en motstanders opprustning og demonstrert kapasitet, som potensielt også kan eskalere til konflikt (Jervis, 1978; Glaser, 2000). *Eskalering* forstås som disposisjoner som bidrar til en økning i intensitet i konflikt mellom parter (Schulze et al., 2020). Herman Kahns eskaleringsstige illustrerer et hierarki av konfliktnivåer, hvor stater kan klatre både opp og ned på «stigen» (Kahn, 1965). Stater kan også holde seg på et gjensidig proporsjonalt nivå, også kjent som *tit for tat* (Schulze et al., 2020). Med dette utgangspunkt kan Stuxnets signaleffekt til Iran og resten av verden oppfattes som opphav til cyberrelaterte sikkerhetsdilemmaer med påfølgende opprustning og mulig eskalering

(Uskowi, 2016; Healey & Singh, 2022). Cyberdomenet som stridsteater er imidlertid grunnleggende vesensforskjellig fra de konvensjonelle domenene land, sjø og luft. Sammenlignet med for eksempel et luftangrep kan intensjon bak cyberangrep være vanskelig å tolke. Forvirring om og feiltolkning av angrepets mål og hensikt kan oppstå, og angripers intensjon harmonerer ikke alltid med oppfatningen til den rammede (Libicki & Tkacheva, 2020; Schulze et al., 2020).

Jason Healey og Robert Jervis argumenterer for at cyberangrep under noen omstendigheter kan fungere som såkalt *trykkavlastning* (Healey & Jervis, 2020).[17] Dette kan innebære at cyberoperasjoner inntreffer *istedenfor* angrep med konvensjonelle våpen. Dersom alternativet til Olympic Games var totalødeleggende bombing av Natanz, kan Stuxnet hypotetisk sett ha vært de-eskalerende. At president Trump ga det amerikanske angrepet mot iranske militære datasystemer grønt lys i 2019, understøtter oppfatningen av at cyberoperasjoner potensielt kan være et substitutt til konvensjonell militærmakt. Men cyberoperasjoner fungerer tilsynelatende svært sjelden på denne måten, og enkelte oppfatter dem som lite egnet som et slikt substitutt (Maschmeyer, 2021).

Når vi ser nærmere på den geopolitiske dyaden USA og Israel versus Iran, vitner opprustningen og de mange angrepene i tiåret etter Stuxnet om eskalering. Det er imidlertid usikkert om offensivene i cyberdomenet har bidratt til eskalering i det overordnede konfliktbildet. På den ene siden kan de avanserte og kraftfulle angrepene fra Iran peke på utvikling av cyberkapasitet for å matche USA og Israel, noe som tilsier at Stuxnet førte til et sikkerhetsdilemma og potensielt inspirerte motangrep. På den andre siden bør man ikke vurdere cyberangrep som uavhengig av et øvrig konfliktbilde. Dersom vi tolker Stuxnet og følgende cyberoffensiver mellom USA, Israel og Iran som virkemidler i det bredere konfliktbildet, kan Stuxnet ikke antas å ha bidratt til eskalering uten videre.

Herman Kahn ser på ikke-kinetiske operasjoner mellom stater som tilhørende såkalt *subcrisis maneuvering*. Det vil si handlinger som foregår på et lavere konfliktnivå og ikke nødvendigvis bidrar til å eskalere konflikt (Kahn, 1965). Hvis cyberoperasjoner vurderes i sammenheng med det øvrige konfliktbildet, kan de ikke sies å være eskalerende eller de-eskalerende i seg selv på en eventuell eskaleringsstige (Schulze et al., 2020; Libicki, 2020). De kan i stedet betraktes som del av et slags *rutenett* hvor *ringvirkninger* mellom ulike domener for krigføring foregår parallelt med eventuell eskalering (Libicki,

17 Egen oversettelse, opprinnelig: *pressure-release.*

2020).[18] Et fremtredende eksempel blir, i henhold til dette, Irans betydelige opprustning offensivt og defensivt i årene etter Stuxnet-angrepet. Før Stuxnet var Irans militære cyberkapasitet av begrenset omfang, men i etterkant iverksatte de en storstilt satsning som inkluderte utvikling og deployering av skadevare (Uskowi, 2016; Healey & Singh, 2022).

Analyse av angrepene listet i Tabell 1 tilsier at konflikten i cyberdomenet har hatt varierende spenningsnivå, og følgelig ikke fulgt en klassisk stige av eskalering. Stuxnet kan heller oppfattes som et startskudd for en lang rekke *tit-for-tat*-angrep i cyberdomenet isolert, og ikke nødvendigvis eskalerende for konfliktsituasjonen mellom USA, Israel og Iran. Enkelte hevder at Stuxnet bidro til at iranerne kom til forhandlingsbordet med USA og P5 + 1 (Zetter, 2014).[19] Dette illustrerer hvordan Stuxnet også fungerte som et politisk pressmiddel. Da iranerne forsto hvor langt USA og Israel var villige til å gå for å stanse anrikningsvirksomheten deres, kunne de også bruke det som forhandlingskort (Sanger, 2018, s. 42). Forhandlingene ledet frem til avtalen *Joint Comprehensive Plan of Action*, inngått i 2015. Det tredje alternativet som president Bush, og senere Obama, ga grønt lys, kan ha bidratt til å oppfylle deres strategiske mål om å forhindre Irans atomvåpenkapasitet uten å ty til konvensjonell militærmakt. Olympic Games blir da et veiskille for bevissthet rundt cyberoperasjoners potensial som sikkerhetspolitisk virkemiddel. Operasjonen er en høyst effektiv form for *subcrisis maneuvering* på et nivå som befinner seg mellom diplomati og konvensjonell militærmakt. Denne oppfatningen er understøttet av det teoretiske konseptet *trykkavlastning* siden Stuxnet også kan tenkes å ha fungert som et substitutt for et konvensjonelt militærangrep.

Teorier forankret i klassisk strategisk tenkning kan være egnet til å forstå staters handlemåte i cyberdomenet under konflikt. Deres forklaringskraft kan imidlertid være begrenset når det gjelder måten Stuxnet preget forestillingene om (fremtidige) cybertrusler og følgelig diskursen blant både eksperter og i det offentlige ordskiftet. Disse forestillingene problematiseres i neste del. Analysen viser et skifte i måten stater oppfatter cyberoperasjoner på, og hvilken betydning det kan ha for disposisjoner i cyberdomenet.

Del 2: staters oppfatning av sikkerhetstrusler i cyberdomenet

Konsekvensene av Stuxnet strekker seg tilsynelatende langt utover konfliktsituasjonen mellom USA, Israel og Iran. Her følger en analyse av hvorvidt

18 I Martin Libicki og Olesya Tkachevas artikkel «Cyberspace Escalation: Ladders or Lattices?» (2020) presenteres ideen om cyberoperasjoners ringvirkninger (*spill-over effect*) over et rutenett (*lattice*) som alternativ til eskaleringsstigen.

19 P5 + 1 er de faste medlemmene i FNs sikkerhetsråd og Tyskland.

Stuxnet preget diskursen omkring sikkerhetstrusler i cyberdomenet, og hvordan det bidro til et skifte i staters sikkerhetspolitiske handlingsmønster.

Statlig bruk av cyberoperasjoner under konflikt bør ikke forstås som isolerte hendelser, men snarere i sin historiske og politiske kontekst. En slik forståelse retter oppmerksomheten mot hvordan vår *forestilling* av trusler mot samfunnet konstrueres. I kritisk sikkerhetslitteratur argumenteres det for at oppfatningen om hva som utgjør en trussel mot samfunnet, kommuniseres via makthavere som styrer vår idé om *hvem* og *hva* som utgjør trusselen. Dette legger igjen føringer for hva som anses som nødvendig respons (Buzan et al., 1998; Dunn Cavelty, 2013). Stuxnet er et godt eksempel på en hendelse som fremprovoserte forestillinger om en ny og fremtidig type eksistensiell trussel i et domene hvor det er vanskelig å begripe nettopp hva som truer, mot hvem og hvilken effekt det kan ha (Lawson & Middleton, 2019; Sandvik, 2016, s. 177–176).

Stuxnets skadeomfang forvandlet måten man forestilte seg og snakket om cybertrusler blant IT-sikkerhetsmiljøer, politikere, media, forskning, populærkultur og i det øvrige samfunnet på 2010-tallet. Mange fryktet at skadevarens kode kunne spres uhemmet på internett mellom aktører med hensikt om å forvolde lignende skade (Lindsay, 2013, s. 366). Særlig i amerikanske medier og blant politikere ble det spekulert i dommedagsscenarioer som cyber-Pearl Harbor i frykt for totalødeleggelse av kritiske samfunnsfunksjoner (Lawson & Middleton, 2019, s. 1–2; Lawson, 2013).

Metaforiske sammenligninger har militarisert cyberdomenet gjennom analogier. Flere argumenterte for å forberede seg på det verst tenkelige og slik unngå angrep med fatale konsekvenser for samfunn (Sandvik, 2016, s. 179; Wirtz, 2018). Den tidligere amerikanske forsvarsministeren og CIA-direktøren Leon Panetta hevdet at cyberkrig var på fremmarsj, og at USA kunne forvente et angrep på linje med 9/11. Barack Obama skrev i 2012 at risikoen for cyberangrep mot USA ble regnet som en av de største truslene mot landets sikkerhet (Lindsay, 2013, s. 367). Enkelte sammenlignet skadepotensialet av cybervåpen med atombomber (The Economist, 2010, s. 11). Ringvirkningene som følge av diskursen om påkommende cyberkrig og cyberrevolusjon iverksatte trussel-inflasjon i form av oppskalering av cyberkapasitet i USA og blant stormaktene Kina og Russland (Mazanec & Shamai, 2009, s. 224; Lawson & Middleton, 2019). Forsvarsbudsjetter ble økt, nye cybersikkerhetsetater etablert, og IT-sikkerhetsselskaper opplevde kraftig kommersiell vekst for å imøtekomme det nye domenet for strid (Lindsay, 2013, s. 367; Sandvik, 2016, s. 179).

I løpet av det siste tiåret har man observert at offensive hendelser i cyberdomenet har økt i hyppighet og rammer oftere flere mål samtidig enn

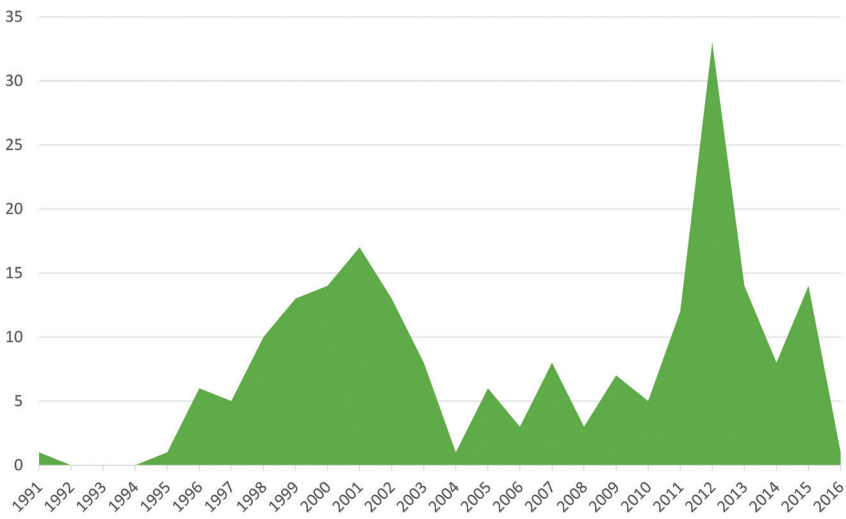
tidligere (Nasjonal sikkerhetsmyndighet, 2021). Men når det gjelder bruk av cyberangrep med høy alvorlighetsgrad i mellomstatlig konflikt, er bildet betraktelig mer fredelig enn det de dystre spådommene tilsa.

Stuxnet var riktignok det første kjente cyberangrepet som førte til kinetisk skade, etterfulgt blant annet av angrepene på strømnettet i Ukraina i 2015 og 2016, amerikanske Colonial Pipeline i 2021 og angrepet på Viasat-satellitten under den russiske invasjonen av Ukraina tidlig i 2022.[20] Likevel observerer vi at alvorlighetsgraden i kinetiske cyberangrep ikke har økt i den grad det ble forespeilet. Bekymringen for at Stuxnet forsynte andre aktører med kode som kunne kopieres og instruere lignende angrep, var misledende. Koden i seg selv oppga eksempelvis ikke mer infiltrasjonsveiledning enn tidligere funnet skadevare som Conficker.[21] I tillegg var nyttelasten i Stuxnet såpass tilpasset målet at den ikke anses som spesielt nyttig til andre formål (Lindsay, 2013, s. 388).

Satsningen på å bygge kapasitet mot tenkelige cyberangrep med kinetisk skadeevne på infrastruktur har kostet dyrt og ekspandert våpenindustrien (Sandvik, 2016, s. 179). I realiteten har andre former for cyberangrep florert det siste tiåret, også som offensivt virkemiddel mellom stater. Slik som figur 1.1 viser, var det viktigste vendepunktet for den dominerende, og særlig amerikanske, oppfatningen av sikkerhetstrusler i cyberdomenet det amerikanske presidentvalget i 2016. Russisk påvirkningskampanje gjennom informasjonslekkasje og informasjonspåvirkning via sosiale medier demonstrerte en ny form for cyberkapabilitet. Fikseringen på dommedagsscenarioer hadde satt amerikanerne på et annet spor når russerne hevdet sine interesser overfor supermakten (Lawson & Middleton, 2019, s. 1–2).

20 Cyberangrep som enten direkte eller indirekte utgjør fysisk skade, regnes som kinetiske cyberangrep (Applegate, 2013). I desember 2015 og igjen i 2016 ble Ukrainas strømnett hacket av aktører som deaktiverte kontrollsystemene og etterlot hovedstaden og den vestlige delen av landet uten strøm i flere timer. Angrepet var det første kjente tilfellet av cyberangrep som forårsaket strømbrudd (Kostyuk & Zhukov, 2017). Det amerikanske selskapet Colonial Pipeline ble etter et løsepengevirus tvunget til å stenge rørledningene som frakter nesten halvparten av bensinen til USAs østkyst (Walsh, 2021). Et cyberangrep mot infrastrukturen til satellitten KA-SAT brøt internettforbindelsen til tusenvis av mennesker i Ukraina, og satte i tillegg, blant annet, en vindmøllepark i Tyskland ute av spill (Burgess, 2022).

21 Conficker er en skadevare som spredte seg til millioner av PC-er verden over før den ble oppdaget i 2008. Skadevarens hovedmål var å utnytte svakheter på PC-er med Microsoft-operativsystemer.

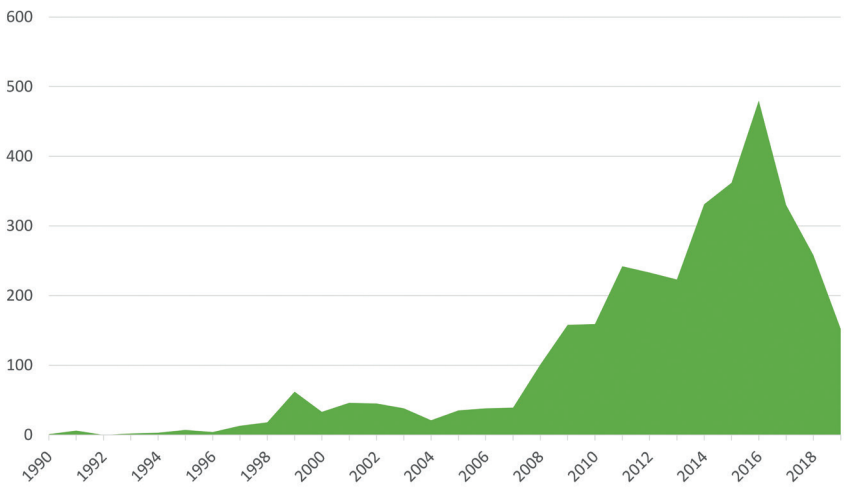


Figur 1.1: Omtaler av «cyber-Pearl Harbor» i store amerikanske aviser, 1991–2015[22]

Max Smeets og Stefan Soesanto illustrerer en lignende trend i sin forskning på diskursen om cyberrevolusjon og andre skrekkscenarioer (Smeets & Soesanto, 2020). Cyberkrig hadde sin gullalder i litteraturen fra 2013, kort tid etter Stuxnet. Brått etter 2016 ble det mindre populært å analysere for eksempel avskrekkingsstrategier i cyberdomenet. Dette kan forklares med at forestillingen om at den primære trusselen i cyberdomenet var kinetiske skadevirkninger, ble avkreftet da amerikanerne måtte håndtere russisk påvirkning under valget. Både politikere og forskere måtte utvide forståelsen av cyberoperasjoner og følgelig den intellektuelle tilnærmingen til mellomstatlig konflikt.

En slik utvidelse i forståelsen av handlingsrommet i cyberdomenet illustrerer hvorfor man bør forstå cybertrusler som sammensatte og på tvers av ulike domener. Ulike staters trusselpersepsjon vil avvike, ergo vil staters operasjonsmønstre variere ut ifra strategiske kulturer (Schulze et al., 2020, s. 5). Denne anerkjennelsen hjelper oss å forstå utfordringen ved å undersøke om handlinger i cyberdomenet kan være eskalerende eller de-eskalerende. Informasjonsoperasjoner underbygger det Maschmeyer beskriver som *subversjon*, nemlig bruk av cyberrelaterte virkemidler for å undergrave politisk stabilitet (Maschmeyer, 2021).

22 Mentions of cyber Pearl Harbor in major U.S. newspapers. Fra «Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991–2016» av S. Lawson og M.K. Middleton, 2019, *First Monday*, *24*(3), s. 12.



Figur 1.2: Tidsskriftartikler, bokkapitler og forskningsrapporter om cyberavskrekking, 1990–2020[23]

Som nevnt omtales Stuxnet som «verdens første cybervåpen». Angrepet skapte dog ingen cyberrevolusjon og forårsaket heller ikke cyber-Pearl Harbor. Etterspillet viser imidlertid at Stuxnet var et teknisk underverk som beviste at cyberangrep *kan* forvolde kinetisk skade og potensielt fungere som et substitutt til konvensjonelle maktmidler i gråsonen mellom diplomati og militære virkemidler (Lindsay, 2013, s. 402). I tillegg finner vi at Stuxnet også har hatt betydning for stater og virksomheters oppfatninger av *defensive* cyberkapabiliteter. Bevisstheten som Stuxnet frembrakte, førte til økt satsning på sikring av industrielle kontrollsystemer (IKS) som utgjør den tredje bestanddelen av paradigmeskiftet (Karnouskus, 2011; Secarma, u.å.).

Del 3: Industrielle kontrollsystemer

Defensiv cyberkapasitet omhandler staters evne til å sikre konfidensialitet, integritet og tilgjengelighet i sine nettverk og sin digitale infrastruktur (Fanelli, 2016). Sikring av kritisk infrastruktur blir gjerne oppfattet som særlig viktig, og industrielle kontrollsystemer (IKS) er en viktig del av det teknologiske fun-

23 Journal articles, book chapters, and research reports on cyber deterrence, Jan 1990–Jan 2020. Fra *Cyber Deterrence is Dead. Long Live Cyber Deterrence!* av M. Smeets og S. Soesanto, 2020, Council on Foreign Relations.

damentet til digitaliserte samfunn. De spiller en sentral rolle i vareproduksjon og forsyning av grunnleggende tjenester som vann og strøm (ENISA, u.å.).

Stuxnet viste verden at IKS kunne angripes og manipuleres. Før Stuxnet var det en utbredt oppfatning at PLS-systemer ikke trengte betydelige sikringstiltak, siden programvaren ikke var ansett som relevant angrepsmål for trusselaktører (Karnouskos, 2011; Knapp & Langill, 2014; Buchanan, 2020). Stuxnet viste at dette var en uholdbar oppfatning, og førte til en helt ny tilnærming til sikringstiltak (Vega et al., 2017). En viktig lærdom i kjølvannet av Stuxnet var at selv *air-gappede* PLS-systemer ikke nødvendigvis er sikre.

Et viktig sikringstiltak for IKS som er koblet på nettverk, er bruk av Intrusion Detection Systems (IDS) og Intrusion Detection and Prevention Systems (IDPS). IDS er programvareløsninger som overvåker nettverkstrafikk og rapporterer til systemadministrator dersom en trussel oppdages. Mange IDPS-er har også en aktiv komponent som kan iverksette sikringstiltak i sanntid og potensielt stoppe uønsket aktivitet. Dette kan skje gjennom endringer av innstillinger i brannmur eller rekonfigurering av oppdaget skadevare (Knapp & Langill, 2014; Vega et al., 2017).[24]

Sikker utviklingsmetodikk av fastvare er også viktig for sikkerheten til PLS-systemer.[25] Det har blitt anslått at det i gjennomsnitt forekommer 15–50 «bugs» per 1000 linjer kode, også for programvare som inngår i IKS (Vega et al., 2017). Gjennom bedre utviklingsmetodikk kan utviklere forhindre sårbarheter i IKS-systemene de produserer. Dette var et viktig læringspunkt etter Stuxnet og preger utvikleres arbeid den dag i dag (Skopik & Smith, 2015; ENISA, u.å.). Et annet fremtredende sikringstiltak er utvikling av prosessorarkitektur for PLS-systemer med økt grad av sikringsmekanismer. Et prosjekt med sikte på å oppnå dette ble igangsatt allerede i 2010 av amerikanske Defense Advanced Research Projects Agency (DARPA) (Vega et al., 2017).

Utvikling og anskaffelse av sikkerhetsløsninger helt ned på maskinvarenivå er ressurskrevende og kostbart. Søkelys på sikring av IKS i staters nasjonale sikkerhetsstrategier understøtter resonnementet om at Stuxnet bidro til betydningsfull utvikling. Behovet for disse sikringstiltakene kan også oppfattes som et viktig skifte innenfor programvareutvikling fordi det endret måten dataingeniører forholder seg til sikkerhetshensyn på.

24 Et eksempel på IDS-programvare er SecureNOK (SNOK). Selskapet bak denne samarbeider blant annet med NIST og Siemens i sitt arbeid med å sikre IKS (SecureNOK, u.å.).

25 Fastvare (*firmware*) er programvare som styrer de grunnleggende funksjonene til maskinvare (*hardware*).

Konklusjon

Paradigmeskiftet som forekom etter Olympic Games og Stuxnet, må tolkes i lys av hvor eksepsjonell operasjonen var. Planleggingen og gjennomføringen var svært ressurskrevende og foregikk over flere år. Dette ble gjort av velfinansiert og kompetent personell fra tre verdensledende aktører innenfor offensive cyberkapabiliteter og etterretning – USA, Israel og Storbritannia. Det er derfor ikke en type operasjon som er enkel for andre aktører å etterligne. Dette har imidlertid ikke hindret andre stater fra å la seg inspirere og endre sin tilnærming til cyberkapabiliteter. Irans endrede disposisjoner og gjennomføring av offensive cyberoperasjoner mot USA og Israel illustrerer dette. På grunnlag av utviklingen har vi postulert at Stuxnet representerer et paradigmeskifte med tre bestanddeler.

Den første bestanddelen omhandler cyberoperasjoners strategiske betydning. Stuxnet var i utgangspunktet et angrep som skulle hindre unødvendig eskalering. Operasjonen kan ha hatt stabiliserende effekt på konfliktnivået i henhold til teorien om trykkavlastning og cyberangrep som substitutt. Denne muligheten er betydningsfull siden den utfordrer tradisjonelle oppfatninger av forholdet mellom bruk av makt og eskalering.

Den andre bestanddelen viser hvordan staters oppfatning av sikkerhetstrusler i cyberdomenet endret seg i kjølvannet av Stuxnet. Forestillinger om et cyber-Pearl Harbor ble forsterket gjennom ekspertuttalelser og forårsaket oppsving i forsvarsbudsjetter og staters satsning på cyberkapabiliteter. Selv om Stuxnet viste at cyberangrep kan fungere som alternativt virkemiddel i mellomstatlig konflikt, har frykten for totalødeleggende og kinetiske cyberangrep mildnet, og utvidet seg til et mer politisk søkelys på cyberkriminalitet og statlig subversjon.

Den tredje bestanddelen relaterer seg også til bevissthet om cyberoperasjoners skadepotensial. IKS som det Stuxnet rammet, er en viktig del av funksjonaliteten og sikkerheten til digitaliserte stater og kritisk infrastruktur. Operasjonen viste at disse systemene kan være sårbare for angrep. Dette førte til et betydningsfullt skifte i hvordan stater, virksomheter og programvareutviklere forholder seg til sikkerhetsstyring.

Samlet sett har vi argumentert for at Stuxnet frembrakte et betydningsfullt skifte i staters forståelse av cyberkonflikt og cyberkapabiliteter. Cyberoperasjoner representerer et tredje alternativ som *kan* benyttes der diplomati ikke fører frem, men hvor bruk av militærmakt ikke fremstår som formålstjenlig. Selv om vi ikke har sett mange operasjoner med avgjørende påvirkningskraft på konfliktsituasjoner, er vissheten om at utvikling i mellomstatlige forhold kan påvirkes av cyberoperasjoner svært betydningsfull.

Referanser

Albright, D., Brannan, P. & Walrond, C. (2010). *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* (ISIS Report). Institute for Science and International Security.

Applegate, S. D. (2013). The Dawn of Kinetic Cyber. *2013 5th International Conference on Cyber Conflict (CYCON 2013*), 1–15.

Barnes, J. E. & Gibbons-Neff, T. (2019, 22. juni). U.S. Carried Out Cyberattacks on Iran. *The New York Times.* https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html

Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, trust, and fear between nations.* NY Oxford University Press.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics.* Harvard University Press.

Burgess, M. (2022, 23. mars) A Mysterious Satellite Hack Has Victims Far Beyond Ukraine. *Wired*. https://www.wired.com/story/viasat-internet-hack-ukraine-russia/

Buzan, B., Wæver, O. & de Wilde J. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

Chulov, M. (2021, 11. april). Israel appears to confirm it carried out cyberattack on Iran nuclear facility. *The Guardian*. https://www.theguardian.com/world/2021/apr/11/israel-appears-confirm-cyberattack-iran-nuclear-facility

Council on Foreign Relations CFR (u.å.a). *Attack on Iranian computer systems.* Council on Foreign Relations. https://www.cfr.org/cyber-operations/attack-iranian-computer-systems

Council on Foreign Relations CFR (u.å.b). *Attack on Israeli water utilities.* Council on Foreign Relations. https://www.cfr.org/cyber-operations/attack-israeli-water-utilities

Council on Foreign Relations CFR (u.å.c). *Compromise of Saudi Aramco and RasGas*. Council on Foreign Relations. https://www.cfr.org/cyber-operations/compromise-saudi-aramco-and-rasgas

Council on Foreign Relations CFR (u.å.d). *Compromise of the Sands Casino.* Council on Foreign Relations. https://www.cfr.org/cyber-operations/compromise-sands-casino

Council on Foreign Relations CFR (u.å.e). *Denial of service attacks against U.S. banks in 2012–2013*. Council on Foreign Relations. https://www.cfr.org/cyber-operations/denial-service-attacks-against-us-banks-2012-2013

Council on Foreign Relations CFR (u.å.f). *Disruption of operations at Shahid Rajee Port.* Council on Foreign Relations. https://www.cfr.org/cyber-operations/disruption-operations-shahid-rajaee-port

Council on Foreign Relations CFR (u.å.g). *Estonian denial of service incident*. Council on Foreign Relations. https://www.cfr.org/cyber-operations/

Council on Foreign Relations CFR (u.å.h). *Stuxnet*. Council on Foreign Relations. https://www.cfr.org/cyber-operations/stuxnet

Council on Foreign Relations CFR (u.å.i). *Targeting of industrial control systems*. Council on Foreign Relations. https://www.cfr.org/cyber-operations/targeting-industrial-control-systems

Council on Foreign Relations CFR (u.å.j). *Targeting of U.S. government and private entities and other victims*. Council on Foreign Relations. https://www.cfr.org/cyber-operations/targeting-us-government-and-private-entities-and-other-victims

Council on Foreign Relations. CFR (u.å.k). *Titan Rain*. Council on Foreign Relations. https://www.cfr.org/cyber-operations/titan-rain

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, *15*(1), 105–122.

ENISA (u.å.). *ICS SCADA*. ENISA. https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada

Fanelli, R. (2016). Cyberspace Offense and Defense. *Journal of Information Warfare*, *15*(2), 53–65.

Falliere, N., O'Murchu, L. O. & Chien, E. (2011). W32.Stuxnet dossier version 1.4 (February 2011) (Vol. 4).

Healey, J. & Jervis, R. (2020). The Escalation Inversion and Other Oddities of Situational Cyber Stability. *Psychology of War*, *3*(4), 30–53.

Healey, J. & Singh, V. V. (2022). Situational Cyber Stability and the Future of Escalating Cyber Conflict. I P. Pernik (red.), *Cyberspace Strategic Outlook 2030: Horizon Scanning and Analysis* (s. 16–26). NATO Cooperative Cyber Defence Centre of Excellence.

Heireng, H. S. (2015). *Uranets vei til kjernekraft og kjernevåpen – en innføring i kjernefysisk flerbruksteknologi* (2015/01688). Forsvarets forskningsinstitutt.

Jervis, R. (1978). Cooperation under the Security Dilemma. *World Politics*, *30*(2), 167–214.

Jervis, R. (2016). Some Thought on Deterrence in the Cyber Era. *Journal of Information Warfare*, *15*(2), 66–73.

Kahn, Herman (1965). *On Escalation: Metaphors and Scenarios*. Praeger.

Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. *IECON 2011 – 37th Annual Conference of the IEEE Industrial Electronics Society*, 4490–4494. https://doi.org/10.1109/IECON.2011.6120048

Knapp, E. D. & Langill, J. (2014). *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems* (2. utg.). Syngress.

Kostyuk, N., & Gartzke, E. (2022). Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine (Summer 2022). *Texas National Security Review*.

Kostyuk, N., Powell, S. & Skach, M. (2018). Determinants of the Cyber Escalation Ladder. *Cyber Defense Review*, *3*(1), 123–133

Kostyuk, N. & Zhukov, Y. M. (2017). Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution*, *63*(2), 317–347.

Kuhn, T. S. (1996). *The structure of scientific revolutions*. University of Chicago Press.

Lai, D. & Roccu, R. (2019). Case study research and critical IR: the case for the extended case methodology. *International Relations*, *33*(1), 67–87.

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics*, *10*(1), 86–103.

Lawson, S. & Middleton, M. K. (2019). Cyber-Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991–2016. *First Monday*, *24*(3).

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar.* RAND Corporation.

Libicki, M. C. (2012). *Crisis and Escalation in Cyberspace.* RAND Corporation.

Libicki, M. C. (2015). The Cyberwar that wasn't. I K. Geers (red.), *Cyber war in perspective: Russian aggression against Ukraine* (s. 49–54). NATO Cooperative Cyber Defence Centre of Excellence.

Libicki, M. C. [Norsk Utenrikspolitisk Institutt NUPI] (2019, 3. juni). *Peace, war and alliances in cyberspace*. [Video]. Youtube, 35:50–36:35. https://www.youtube.com/watch?v=EU0mIyxQ5EYogt=2202sogab_channel=NorskutenrikspolitiskinstituttNUPI

Libicki, M. C. (2020). Cyberwar is what states make of it. *Cyber Defense Review*, *5*(2), 77–87.

Libicki, M. C. & Tkacheva, O. (2020). Cyber Escalation: Ladder or Lattice? I T. Stevens, K. Floyd & P. Pernik (red.), *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* (s. 60–73). NATO Cooperative Cyber Defence Centre of Excellence.

Lin, H. (2012). Escalation Dynamics and Conflict Termination in Cyberspace. *Strategic Studies Quarterly*, *6*(3), 46–70.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404.

Maness, R. C. & Valeriano, B. (2016). Cyber Spillover Conflicts: Transitions from Cyber Conflict to Conventional Foreign Policy Disputes? I K. Friis & J. Ringsmose (red.), *Conflict in Cyber Space: Theoretical, strategic and legal perspectives* (s. 45–64). Routledge.

Maschmeyer, L. (2021). The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *International Security*, *46*(2), 51–90.

Mazanec, B. M. & Shamai, P. (2020). Stigmatizing Cyber and Information Warfare – Mission Impossible? I C. Whyte, A. T. Thrall & B. M. Mazanec (red.), *Information warfare in the age of cyber conflict* (1. utg.). (s. 215–228). Routledge.

Nasjonal sikkerhetsmyndighet NSM (2021). *Nasjonalt digitalt risikobilde 2021*. Nasjonal sikkerhetsmyndighet. https://nsm.no/aktuelt/nasjonalt-digitalt-risikobilde-2021

Sandvik, K. B. (2016). Law in the Militarization of Cyberspace: Framing a Critical Research Agenda. I K. Friis og J. Ringsmose (red.), *Conflict in Cyber Space: Theoretical, strategic and legal perspectives* (s. 175–197). Routledge.

Sanger, D. E. (2012). *Confront and conceal: Obamas Secret Wars and Surprising Use of American Power.* Crown.

Sanger, D. E. (2018). *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age.* Crown.

Schulze, M., Kerscher, J. & Bochtler, P. (2020). *Cyber Escalation: The conflict dyad USA/Iran as a test case*. (Working Paper NR. 01). Stiftung Wissenschaft und Politik: German Institute for International and Security Affairs.

Secarma (u.å.). Stuxnet: The Day Industial Control Systems Became a Target. Secarma. https://secarma.com/stuxnet-the-day-industrial-control-systems-became-a-target/

SecureNOK (u.å.). Cyber Security for OT. https://www.securenok.com/

Segal, A. (2016). *Cyber Conflict After Stuxnet: Essays from the Other Bank of the Rubicon.* Cyber Conflict Studies Association.

Skopik, F. & Smith, P. (red.) (2015). *Smart Grid Security: Innovative Solutions for a Modernized Grid.* Syngress.

Smeets, M. & Soesanto, S. (2020, 18. februar). Cyber Deterrence Is Dead. Long Live Cyber Deterrence! *Council on Foreign Relations.* https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence

The Economist (2010, 3. juli). The threat from the internet: Cyberwar. *The Economist*, 396(8689), s. 11. https://www.economist.com/leaders/2010/07/01/cyberwar

Uskowi, N. (2016). Iran's Reaction to Stuxnet. I A. Segal, *Cyber Conflict After Stuxnet: Essays From the other Bank of the Rubicon*. CCSA.

Vega, A., Bose, P. & Buyuktosunoglu, A. (2017). *Rugged Embedded Systems: Computing in Harsh Environments.* Morgan Kaufmann.

Walsh, J. (2021, 8. mai). Ransomware Attack Shuts Down Massive East Coast Gasoline Pipeline. *Forbes.* https://www.forbes.com/sites/joewalsh/2021/05/08/ransomware-attack-shuts-down-massive-east-coast-gasoline-pipeline/?sh=6e7266746625

Wirtz, J. J. (2018). Cyber Pearl Harbor redux: helpful analogy or cyberhype? *Intelligence and National Security*, *33*(5).

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and launch of the world's first digital weapon.* Crown Publishers.