UTSYN - FORUM FOR UTENRIKS OG SIKKERHET

PÅVIRKNINGSOPERASJONER:
FORSTERKENDE OG SPLITTENDE MEKANISMER
THESE GO TO 11

«These go to 11» henviser til en velkjent scene i den fiktive dokumentarfilmen *This is Spinal Tap* fra 1984, der gitaristen viser frem forsterkerne sine med volumknapper som går fra 0 til 11, i stedet for 0 til 10 som var vanlig. Gitaristen mener at denne nummereringen øker forsterkernes høyeste volum, og forklarer det med at 11 «er et hakk høyere». Når reporteren spør hvorfor ikke bare innstillingen 10 på forsterkerne kan settes til å være høyere, nøler gitaristen før han svarer: «Disse går til 11». Visstnok begynte virkelige band og musikere etter dette å kjøpe utstyr med volumknapper som gikk opp til 11 på grunn av filmen.

Innen moderne risikostyring er risikopersepsjon det narrativet som et individ, en gruppe eller et samfunn har, hvor deres personlige følelser og emosjoner reflekterer deres oppfatning av trusler og/eller muligheter. Et eksempel på virkemiddel for å påvirke offentlig opinion og meninger er en såkalt «synkronisert angrepspakke»[1]med en kombinasjon av både *kinetiske* og *ikke-kinetiske* verktøy. Referansen til filmen *This is Spinal Tap* er et bilde på en strategi innen påvirkningsoperasjoner, som handler om å kombinere ulike former for makt for å **forsterke** en oppfatning og skape et offentlig narrativ.

HOVEDPUNKTER

- Forskning peker på hybride trusler og hybrid krigføring rettet mot privat sektor som den mest sannsynlige formen for fremtidig konflikt i Europa – og at hybride trusler, og dermed implisitt påvirkningsoperasjoner, allerede er utbredt.[2]
- Hensikten med dette fagnotatet er å tydeliggjøre hva som er grunnleggende ved påvirkningsoperasjoner, og vise til eksempler på hvordan påvirkningsoperasjoner kan se ut og bli forsterket i privat og sivil sektor.

PÅVIRKNINGSOPERASJONER

En omforent forståelse av hva som utgjør begrepet «påvirkningsoperasjoner» finnes ikke. Ironisk nok er påvirkningsoperasjoner tett koblet til begrepet «hybride trusler», hvor eksperter har uttalt at «den internasjonale konsensus om «hybrid krigføring» er tydelig: ingen forstår hva det er, men alle, inkludert NATO og EU, er enige om at det er et problem».[3]

Såkalte «hybride trusler» og «hybrid krigføring» anses som en kombinasjon av kinetiske (konvensjonelle) og hybride (ikke-konvensjonelle) verktøy for å utøve makt.

Til tross for at ikke-konvensjonelle maktmidler er dominerende i hybrid krigføring, inkluderer også hybrid krigføring kinetiske trusler, for eksempel attentater (se figur 1).

I kategoriseringen av hybride trusler kan cybertrusler skilles fra cyberoperasjoner i a) det operative domenet, som ondsinnet programvare (*malware*) rettet mot kritisk infrastruktur, og b) informasjonsdomenet, for å skape et narrativ som støtter operasjonen og/eller for å påvirke beslutninger eller meninger.[4] I dette fagnotatet fokuserer vi på kombinasjonen av kinetiske og ikke-kinetiske maktmidler som forsterkere i påvirkningsoperasjoner.

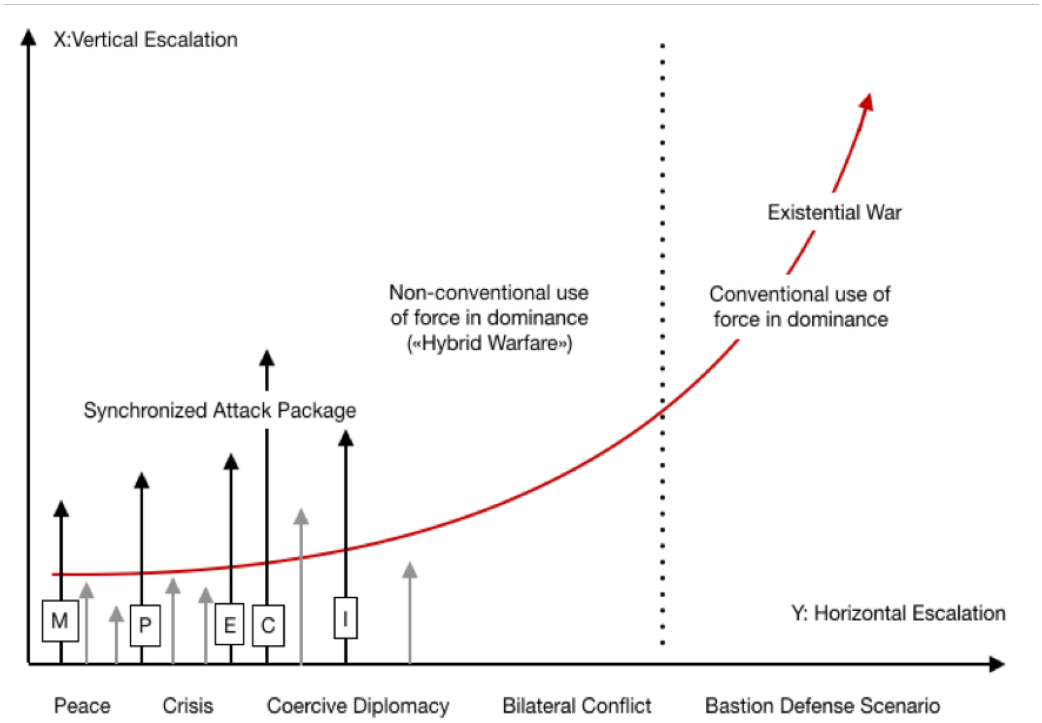
	Kinetisk	**Ikke-kinetisk**
Kan tilskrives bestemt faktor	Mindre kinetiske operasjoner utformet for å underbygge eller styrke et troverdig strategisk narrativ, flytting av konvensjonelle styrker, uanmeldte militære øvelser («snap øvelser») osv.	Åpenlyse operasjoner utformet for å påvirke målrettede gruppers meninger og atferd gjennom kanaler som medier, nasjonale informasjonskampanjer, trusler om atomstyrker, press på økonomi og energiforsyning, propaganda og desinformasjon, cyberforstyrrelser, cyberoperasjoner rettet mot kritisk infrastruktur, politisk destabilisering osv.
Kan ikke tilskrives bestemt faktor	Skjulte kinetiske operasjoner som sabotasje, attentater og «terror»-angrep, utført av spesialstyrker uten uniformer eller i umerkede uniformer («små grønne menn») og stedfortredere i form av militser, opprørsgrupper, kriminelle organisasjoner, selvforsvarsorganisasjoner, ideelle organisasjoner osv.	Manipulering av nyheter og skjulte påvirkningsoperasjoner gjennom alle typer medier og plattformer, politisk destabilisering, oppfordring til demonstrasjoner, utnyttelse av ikke-voldelige sympatisørgrupper og «nyttige idioter» osv.

***Figur 1**: FFI sin kategorisering av hybride trusler.[5] Figuren viser at påvirkningsoperasjoner kan komme til uttrykk både som kinetiske og ikke-kinetiske hybride trusler og bestå av både tilskrivbare og ikke-tilskrivbare maktmidler: militært, politisk, økonomisk, sivilt og informasjon (MPECI).[6]*

«Hybrid krigføring» kan forstås som en fase der hyppigheten av hybride trusler over tid går over en grense for hva som kan betraktes som enkelthendelser. Det kan imidlertid ikke defineres hvilket nivå effekten av truslene har på den grunnleggende funksjonsevnen til samfunnskritisk infrastruktur,[7] så man kan skille hendelsene ut fra den «vanlige støyen».

For å forstå differensieringen mellom «hybride trusler» og «hybrid krigføring» er det to ganske like begreper som kan skape forvirring: *MPECI* og *PMESII*. Figur 2 illustrerer at hybride trusler er det som utføres av en motpart med bruk av militære, politiske økonomiske, sivile, informasjonsverktøy (MPECI: Military – Political – Economic – Civil – Information). Disse faktorene regnes som maktmidler,[8] som kan brukes for å skape både en horisontal og vertikal eskalering (figur 2) – og som sannsynligvis vil inkludere et bredt utvalg av inngrep og operasjoner som vist i figur 1.

En «synkronisert angrepspakke» (SAP)[9] rettes mot sårbarheter i samfunnet på tvers av politikk, forsvar, økonomi, sosiale forhold, informasjon og infrastruktur (PMESII: Political – Military – Economic – Social – Information – Infrastructure), og er også forbundet med begrepet «hybrid krigføring», eller «lavintensitets-konflikt». Påvirkningsoperasjoner med et strategisk mål om å ta eierskap til narrativet i samfunnet, for å skifte det strategiske tyngdepunktet til fordel for motparten, vil sannsynligvis være et viktig element i hybrid krigføring. Dermed må påvirkningsoperasjoner fokusere på spesifikke sårbarheter i samfunnet, ofte som et resultat av eller en del av, langvarig spionasje og innhenting av kunnskap, eller gjennom å sondere sårbarheter i samfunnet.



Figur 2: *Den synkroniserte angrepspakken (svarte piler) er ment å illustrere hvordan hybride trusler kan være vanskelig å skille fra «normale» uønskede hendelser (grå piler). Hybride trusler kan brukes over hele freds-/krigsspekteret og eskaleres både vertikalt og horisontalt.*

DEN SIKKERHETSPOLITISKE DIMENSJONEN AV PÅVIRKNINGSOPERASJONER

I Norge er de viktigste kritiske samfunnsfunksjonene styresett og suverenitet, befolkningens sikkerhet, og samfunnets funksjonalitet. Implisitt er disse kritiske samfunnsfunksjonene også viktig for befolkningens tillit til myndighetenes evne til å ivareta befolkningen. En tillit som kan undergraves hvis disse funksjonene ikke fungerer som de skal. Innenfor de kritiske samfunnsfunksjonene finnes ulike typer tjenester basert på forsyning og infrastruktur som betjener befolkningen, og som samtidig utgjør innsatsfaktorer for virksomheter som er ansvarlige for andre kritiske samfunnsfunksjoner. Hvis denne kategorien svikter kan det altså forplante seg til andre deler av samfunnet.

Eksempler her er manglende energiforsyning som kan føre til tap av vann og avløp, forstyrrelser i finansielle tjenester og elektronisk kommunikasjon som gir betydelige utfordringer for helse- og omsorgssektoren og for krisehåndtering. Alvorlig funksjonssvikt i denne kategorien kan føre til sosial uro og problemer i hverdagen med konsekvenser for folks sikkerhet, samt skade viktige samfunnsinteresser.[10]

Cyberangrep som forårsaker skade, ødeleggelse eller forstyrrelse i privat sektor er fremdeles relativt sjeldent, men «cybertrusselen» og digitale angrep mot kritisk infrastruktur er en raskt voksende bekymring. En rapport fra Forsvarets forskningsinstitutt (FFI) konkluderte imidlertid med at oppfatningen om at cybertrusselen er en avgjørende faktor i konflikter, for permanent å lamme en motstander med spektakulære digitale angrep på samfunnets infrastruktur, neppe er realistisk.[11] I stedet må cybertrusselen sees på som et maktmiddel som brukes *sammen med* andre koordinerte hendelser, der hovedmålet er å vinne dominans over informasjons-domenet, å ta eierskap til narrativet, og forskyve et strategisk tyngdepunkt til fordel for ikke å oppnå en enighet om represalier eller for å identifisere hvor god beredskapen er, og/eller på hvilket nivå myndighetene identifiserer at de har et avgjørende ansvar for å beskytte samfunnets motstandskraft (for eksempel som en del av langvarig spionasje).

En synkronisert angrepspakke, der effekten av flere typer maktmidler samles opp, anses i sum å gi en mer kostnadseffektiv samfunnsskade enn effekten av ett enkelt konvensjonelt angrep.

Et eksempel kan være skadelig programvareangrep på et kraftverk for å skape strømbrudd. Effekten av denne handlingen kan forsterkes i synergi med (for eksempel) ekstreme temperaturer. Befolkningsgrupper vil i et slikt scenario få et ressursbehov, særlig innen sårbare grupper som eldre- og hjemmesykepleie. Kombinert med en desinformasjonskampanje kan sosiale medier fungere som en plattform for å forsterke mistillit til myndighetene. Et narrativ kan lages ved å spre falske nyheter til flere personer og gjenta en melding helt til den slår sprekker i «det sosiale limet», for eksempel ved å slå mynt på populistiske antakelser som «oss og dem». Man kan skape et falskt narrativ om en regjering som har ignorert den sårbare befolkningsgruppen og kreve politisk endring.

I sosiale medier blir denne strategien ofte referert til som mikromålretting, gjennom at kontoer for påvirkning lages og deltar i eksisterende (virkelige) sosiale grupper og kun engasjerer seg med et fåtall forskjellige personer. Eller gjennom «influencer influencing», hvor disse kontoene bare prøver å påvirke noen veldig få stedfortredere, enten journalister eller andre innflytelsesrike mennesker, som kan bære budskapet for den som står bak.[12] Her kan det strategiske narrativet *forsterkes* med ulike maktmidler tilpasset etter hva man observerer av resultater.

Under årets kommunevalg i Kristiansand skiftet en Facebook-side (finansiert for å skape kontinuerlig engasjement) det politiske landskapet til fordel for en mindre opposisjon.[13] Selv om dette eksempelet *ikke* er knyttet til hybride trusler fungerer det som et eksempel for å vise hvordan sosiale medier kan bidra til å forsterke et budskap. Til tross for denne opposisjonens program på ytre høyre plasserte de seg selv nært alle de større partiene, og hevdet de ønsket å samarbeide («vi kommer i fred»). En slik tilsiktet posisjonering kan påvirke demokratiske og konsensusbaserte beslutnings-miljøer fordi disse er forutsigbart basert på gjennom-snittsvelgerens posisjon. Å påvirke denne gruppen vil

dermed sannsynligvis være den mest ønskelige strategien for å maksimere effekten av politiske kampanjer.[14] I Kristiansand ble narrativet fra Facebook-kampanjen sannsynligvis forsterket på grunn av tre store politiske, sivile og økonomiske hendelser i byen: Et stort infrastrukturprosjekt, en offentlig investering i et kunstsenter og en kontroversiell flytting av byens viktigste havn.

I sitt fagmilitære råd som grunnlag for ny langtidsplan for Forsvaret gikk Forsvarssjefen i år inn for en historisk satsning på å gjenoppbygge forsvarskapasiteter. Til tross for avstanden mellom partiene på venstre- og høyresiden har Forsvarssjefens budskap blitt møtt med enighet langs hele det politiske spekteret. Partiene kan likevel ha ulike motiver for å støtte hans forslag. Mens noen partier ønsker å vise NATO at Norge trapper opp for å møte alliansens mål om å bruke to prosent av BNP på forsvar, mener andre partier at dette er et riktig skritt for å styrke nasjonal forsvarsevne uten å være avhengig av alliert støtte. Dermed trenger ikke motstand mot endring nødvendigvis komme utenfra, men den indre motstanden kan kultiveres.

Problemstillingen rundt kultivering og politisk påvirkning ble utfordret i øvelsen «Forgotten Waters» utført av *The Centre for a New American Security* (CNAS) i 2017. Deltakerne i øvelsen ble testet på deres manglende kjennskap til hybride trusler, særlig når det gjaldt den geopolitisk viktige nordatlantiske passasjen mellom Grønland, Island og Storbritannia, kjent som «GIUK-gapet». Under øvelsen ble deltakerne fortalt at en desinformasjonskampanje på Island hadde endret utfallet av landets nasjonale valg, og en regjeringsmakt som ville redusere amerikansk militær tilstedeværelse på Island hadde blitt innsatt. I øvelsen sto deltakerne overfor en rekke kompliserte utfordringer: Behovet for å avdekke og motvirke desinformasjonskampanjer, behovet for å opprettholde og styrke samhold i NATO-alliansen, og behovet for å finne alternative baser til de amerikanske maritime overvåkningsflyene P-8 Poseidon. Øvelsen viste deltakerne hvordan påvirknings-operasjoner som har en effekt på den interne politikken i et NATO-alliert land kan skape en stor bekymring for alliansens sikkerhet. Dette eksempelet med høyt kompleksitetsnivå ble presentert i øvelsen for å adressere hvor avhengig det transatlantiske samholdet er av å kunne svare på hybride trusler med raske beslutninger og effektive mottiltak.[15]

HVORDAN PÅVIRKES PRIVAT SEKTOR OG HVORDAN STYRKER VI EVNEN TIL Å OPPDAGE PÅVIRKNINGSOPERASJONER OG REAGERE?

Ressurser og kritisk infrastruktur er viktige komponenter for vitale samfunnsfunksjoner. I dag er det privat sektor som i hovedsak er eier og driver av disse komponent-ene. Forskning peker på at hybride trusler rettet mot kritisk infrastruktur, sivilsamfunnet og den private sektoren vil være en *sannsynlig hovedfaktor i enhver fremtidig konflikt i Europa*.[16]

I mars 2019 presenterte Næringslivets Sikkerhetsråd (NSR) en studie om hybride trusler rettet mot det norske næringslivet. Studien inkluderte 354 intervjuer av norske virksomheter i offentlig og privat sektor med 100 eller flere ansatte, og fant at:

- 67% av virksomhetene mente at det å ha en sentral og veletablert posisjon i samfunnet gjorde dem til potensielle mål for hybride trusler
- 70% mente at manglende evne til å gjenkjenne forsøk på å påvirke deres drift, kamuflert som vanlige henvendelser, er en tilstand som gjør bedriftene sårbare mot hybride trusler[17]

Funnene gjenspeiler at det å beskytte kritisk infra-struktur mot påvirkningsoperasjoner i stor grad er et ansvar som faller på privat sektor, snarere enn at det offentlige tar ansvar i tradisjonell forstand. Dette er et viktig aspekt av hvordan påvirkningsoperasjoner påvirker privat sektor, særlig fordi 63% av virksomhetene i studien mente at deres sårbarhet for hybride trusler skyldtes manglende situasjonsbevissthet om hvordan hybride trusler kan rettes mot organisasjonen.

I 2017 ble den ukrainske regjeringen angrepet av løse-pengeviruset «NotPetya». Fra Ukraina spredte viruset seg til private enheter, blant disse den København-baserte shippinggiganten *A.P. Moller-Maersk* og *Mondolez*. Dette eksempelet viser at det å motvirke hybride trusler mot private virksomheter i stor grad er et

ansvar som faller på den private sektoren alene, i stedet for militær beredskap i tradisjonell forstand. En nyhets-artikkel påpekte treffende at de som stod bak utsendingen av «NotPetya» ikke erklærte krig mot den ukrainske regjeringen, og det gjorde heller ikke Russland når de invaderte Krimhalvøya. Artikkelen konstaterte faktisk at de fleste væpnede konflikter siden andre verdenskrig ikke har inneholdt krigserklæringer i det hele tatt.[18]

Hvorfor bør dette være en bekymring for private virksomheter spesielt? Et eksempel er *Zurich*, et verdensledende forsikringsselskap som hevder at «NotPetya» er en krigshandling, mens en av deres kunder, *Mondolez*, argumenterer for det motsatte. Årsaken til uenigheten er at *Mondolez* tapte millioner av dollar på grunn av «NotPetya». Dermed er det private selskaper som nå debatterer definisjonen av krig, og dermed ansvar for forsikringsutbetaling i retten.

Påvirkningsoperasjoner kan utformes slik at de ikke kan tilskrives en bestemt faktor, slik at man holder seg under det nivået hvor «normale» uregelmessigheter kan påvises. Påvirkningsoperasjoner kan også dukke opp i et tempo utformet for å holde seg under en grense som normalt ville økt bevisstheten om skiftende forhold, og utfordrer dermed den tradisjonelle bipolare oppfatningen av krig og fred.

Hvor lang tid vil det ta før vi blir så vant til det uvanlige at det uvanlige blir normalt? Er det noe som kan fungere som *forsterkere* i påvirkningsoperasjoner og som har påvirket vår oppfatning av politikk og samfunn?

Har GPS-forstyrrelser i nordområdene gradvis blitt så vanlig at vi ikke lenger hever et øyenbryn når det skjer? Hva med andre lands militære tilstedeværelse i våre nærområder og farvann? Hva med cyberangrep på vårt helsevesen? Når ble phishing-forsøk på arbeidsplassen din normalt? Og hva med de tingene vi ikke ser? Uforklarlige sykdommer som forsvinner like raskt som de oppstår og kun innenfor landets grenser? I en konstant skiftende verden kan det være utfordrende å identifisere et avvik fra hva som er normalt når referansene for det som er normalt konstant endres, og alle deler av samfunnssikkerhetens grunnleggende funksjoner blir berørt. Lignelsen om den kokende frosken brukes ofte for å forklare hvorfor mennesker reagerer raskt på nye hendelser, men ikke reagerer på sakte endrede forhold før det er for sent: Hvis du er en frosk hopper du ut fra en kjele med kokende vann, men hvis du blir plassert i en kjele med lunkent vann som gradvis varmes opp, reagerer du ikke og vil til slutt dø av det varme vannet.

På grunn av den høye graden av plausibel benektelse som er gjeldende ved påvirkningsoperasjoner bør derfor avvik som kan registreres i *PMESII-spekteret* balansere usikkerhet med tillit basert på for eksempel føre-var eller forsiktighetsprinsippet. Det innebærer også et offentlig ansvar om å handle når det er en sannsynlig risiko mot kritiske samfunnsfunksjoner. En offentlig utredning (NOU) er nå på høring for en ny lov som kan gi en tverrsektoriell fullmakt i fredstid, i tilfeller der ekstraordinære situasjoner kan oppstå, hvor det er et behov for å handle raskt og hvor nåværende lovgivning ikke sørger for nok fleksibilitet.

"There's a feeling among many states that other states are carefully calibrating their cyber-aggressions, so they fall below the threshold of war," said Gary Brown, a former U.S. Air Force judge advocate who now teaches cyberlaw at the National Defence University in Washington. "That makes it challenging for the targeted country to respond. It's neither war nor peace—it's constant competition."

- Elisabeth Braw: Can Courts Clear the Fog of War? (Foreign Policy, 2019)

Hybride trusler mot kritisk infrastruktur er eksempler på hendelser der denne loven anses som relevant. På hvilket nivå kritiske samfunnsfunksjoner må rammes før tiltak iverksettes, og hvem som skal bestemme den tverrsektor-ielle terskelen for overskridelse, forblir imidlertid et åpent spørsmål. En betydelig utfordring for å iverksette mottiltak er å oppnå enighet hvis det ikke finnes en åpenbar trussel eller motstander, men at situasjonen

oppfattes som en vanlig fredsfase. Måter å forbedre robusthet og motstandsdyktighet i samfunnssikkerheten er dermed ikke begrenset til mekanismer for å motvirke hybride trusler og påvirkningsoperasjoner. Det inkluderer også formidling av kunnskap til det systemet som blir berørt. Da kan denne kunnskapen fungere som sensorer for tidlig varsling, og aktivere eksisterende forebyggende mekanismer.

Å bygge motstandsdyktighet i dag innebærer dermed ikke bare å styrke digital og fysisk infrastruktur, men det handler også om å styrke kunnskap og bevissthet om det trussellandskapet vi har. Private bedrifter og sivilsamfunnet spiller en viktig rolle i å motvirke påvirkningsoperasjoner og hybride trusler. Den nye trusselsituasjonen betyr også at gamle skillelinjer mellom det offentlige, private, sivile og militære gradvis viskes ut og derfor trenger vi samarbeid vi ikke har hatt før på tvers av ansvarsområder.

Hvordan skal befolkning og virksomheter så bli oppmerksomme på og rapportere om falske nyheter og påvirkningsoperasjoner? Neste år skal *Direktoratet for samfunnssikkerhet og beredskap* (DSB) lede en øvelse kalt «Øvelse Digital 2020» som forener næringslivet, offentlige organisasjoner, og sivile og militære myndigheter. Det er store forventninger til at læringsutbyttet vil kunne identifisere og utvikle ytterligere tiltak basert på funn fra øvelsen. Forhåpentligvis vil øvelsen bidra til å øke bevisstheten rundt det nye trusselbildet, samt hvilke tiltak vi bør prioritere for å forhindre angrep som har som mål å destabilisere vårt samfunn. Prosessen fremover med sikring av kritisk infrastruktur bør inkludere «alle» med et fokus på bevisstgjøring året rundt, som kontinuerlig oppdateres i henhold til trusselbildet og som er kommunisert i åpne trusselvurderinger fra myndigheter som PST, NSM og Forsvaret.

I dag kan internasjonal sikkerhetspolitikk like lett ramme en kommune i Norge. Eksempelvis som nevnt i form av hacking av et lokalt kraftselskap, som i neste sving skaper en debatt og påvirker folks tillit til myndighetene. Det er derfor viktig at alle innbyggere, virksomheter og myndigheter har en felles forståelse av trusselbildet. Jo mer bevisst og ansvarlig enhver del av samfunnet reagerer på avvik, jo mer er vi i stand til å bygge et robust samfunn mot påvirkningsoperasjoner. Mer kunnskap betyr også økt rapportering av mistenkelige hendelser til myndigheter, og kan styrke det offentlige-private samarbeidet vi trenger innen sikkerhetsspørsmål vedrørende hybride trusler. Det bidrar også til dokumentasjon av et mer nøyaktig situasjonsbilde av trusler, og gjør det lettere for relevante myndigheter å kartlegge hendelser, sette dem i system og svare med mottiltak.

Kunnskap og bevissthet om hybride operasjoner og hvilke myndigheter man skal rapportere til må integreres inn i samfunnets ryggrad for at vi skal være i stand til å reagere og rapportere, slik som mekanismene for varsling i privat sektor har fungert i årevis. Kunnskap og bevissthet om hybride trusler og påvirkningsoperasjoner, falske nyheter og splittende stemmer bør derfor være like relevant for privat sektor som det er for Forsvarets situasjonssenter (SITSEN) i Oslo.

OM FORFATTERNE

Richard Utne er seniorrådgiver for Fylkesmannen i Agder. Han har bred internasjonal erfaring i risikostyring og sikkerhetsledelse, både i privat og offentlig sektor. Utne har lang tjenesteerfaring fra Forsvaret og deltar i ulike forum og ekspertgrupper knyttet til samfunnssikkerhet. Han har også vært bidragsyter til Hybridundersøkelsen gjennomført av Næringslivets Sikkerhetsråd.

Birgitte Førsund er direktør i Junglemap som jobber med digital sikkerhet. Hun har de siste 20 årene jobbet som bindeledd mellom sikkerhetsmiljøer og næringsliv via flere offentlig-private prosjekter med fokus på forebyggende digital sikkerhet. Førsund har siden 2017 samarbeidet tett med Næringslivets Sikkerhetsråd på vegne av KPMG Cyber og bidratt til arbeidet med Mørketallsundersøkelsen 2018 og Hybridundersøkelsen 2019.

Fagnotatet er en del av et prosjekt for å løfte sentrale problemstillinger knyttet til den kommende langtidsplanen for Forsvaret.

FOTNOTER

Bildet på første side er hentet fra Scott Myers (2017) *Great Scene: "This is Spinal Tap"*: https://gointothestory.blcklst.com/great-scene-this-is-spinal-tap-b22e7f5b2b60

1. Cullen. P & Reichborn-Kjennerud, E. (2017). Understanding Hybrid Warfare. The Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare Project (Norsk utenrikspolitisk institutt, NUPI).
2. Diesen, S. (2018). Lavintensivt hybridangrep på Norge i en fremtidig konflikt (Forsvarets forskningsinstitutt, FFI).
3. Cullen. P & Reichborn-Kjennerud, E. (2017). Understanding Hybrid Warfare. The Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare Project (NUPI).
4. Diesen, S. (2018). Lavintensivt hybridangrep på Norge i en fremtidig konflikt (FFI).
5. Ibid.
6. Akronymet brukt mest i USA er DIMEFIL: Diplomatic, Information, Military, Economic, Financial, Intelligence, Law enforcement.
7. Som beskrevet i NOU 2019:13 Når krisen inntreffer, seksjon 4.2 – 4.5.
8. Cullen. P & Reichborn-Kjennerud, E. (2017). Understanding Hybrid Warfare. The Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare Project (NUPI).
9. Ibid.
10. DSB (2016). Samfunnets kritiske funksjoner.
11. Diesen, S. (2018). Lavintensivt hybridangrep på Norge i en fremtidig konflikt (FFI).
12. Schneier, B. (2019). 8 Ways to Stay Ahead of Influence Operations (Foreign Policy).
13. Dagens Næringsliv (10.10.2019). Spillet om Sørlandsnyhetene.
14. Hotelling, H. (1929). Stability in competition.
15. Smith, J & Hendrix, J. (2017). FORGOTTEN WATERS. Minding the GIUK Gap: A Tabletop Exercise (Center for a New American Security, CNAS).
16. Diesen, S. (2018). Lavintensivt hybridangrep på Norge i en fremtidig konflikt (FFI).
17. Næringslivets Sikkerhetsråd (2019). Hybridundersøkelsen.
18. Braw, E. (2019). Can Courts Clear the Fog of War? (Foreign Policy).

UTSYN - FORUM FOR UTENRIKS OG SIKKERHET

Stortorvet 3
0155 Oslo

www.prosjektutsyn.no

post@prosjektutsyn.no

I SAMARBEID MED:

NOF

NTL Forsvaret

Fellesforbundet