Næringslivets sikkerhetsråd

Hybridundersøkelsen

Hybride trusler og hendelser mot norsk næringsliv

Gjennomført av Opinion AS for Næringslivets Sikkerhetsråd

Forord

Det offentlige ordskiftet tatt for seg temaer knyttet til hybride trusler og hendelser. Hybride hendelser kan være rettet mot både stater og næringsliv, og identifiseres ut i fra de irregulære og ukonvensjonelle virkemidlene som tas i bruk.

Hybride operasjoner kan utføres via påvirkningsoperasjoner, cyberangrep, spionasje og operasjoner hvor desinformasjon, nettmanipulering, og undergraving står sentralt, Med dette initiativet vil Næringslivets Sikkerhetsråd (NSR) kartlegge utbredelsen av hybride trusler mot næringslivet.

NSR står også bak de nasjonale undersøkelsene Mørketallsundersøkelsen - 2018, og KRISINO - 2017. Det betyr at NSR har komplementerende undersøkelser og dokumentasjon, som gjør at hybrid undersøkelsen kan spisses ytterligere. Det gir også grunnlag for å gjenta hybrid undersøkelsen i årene som kommer for å kunne sammenligne og følge utviklingen. Samlet vil Hybrid, Mørketall og KRISINO - undersøkelsene dermed sikre svært viktig dokumentasjon og være grunnlag for videre sikkerhetsarbeid, også knyttet til forebyggende og bevisstgjørende tiltak i Norge. Undersøkelsen vil også fange opp eksisterende grad av samarbeid mellom næringslivet og ansvarlige myndigheter. Eksempelvis, hvilke myndigheter rapporterer næringslivet hendelser til og i hvor stor utstrekning rapporteres det.

Undersøkelsen er utarbeidet med utgangspunkt fra en finsk undersøkelse fra 2018 og skaper dermed et visst sammenligningsgrunnlag mellom Norge og Finland.

Takk til alle som har støttet undersøkelsen og gitt bidrag til rapporten.

Jack Fischer Eriksen
Direktør i Næringslivets Sikkerhetsråd

NORGES BANK

KPMG

mnemonic

Nordea

VISMA

ONE VOICE

ONE WORLD

DEN NORSKE KRIGSFORSIKRING FOR SKIB
GJENSIDIG FORENING
The Norwegian Shipowners' Mutual
War Risks Insurance Association

AkerBP

equinor

Innhold

Forord 2
Sammendrag 5
Om undersøkelsen 6

1. Sikring og sårbarheter 8
1.1 Virksomhetens sårbarheter for hybride trusler 10
1.2 Sannsynlighet for hybride trusler 10

2. Forberedelser og forebygging 12
2.1 Virksomhetense forbyggende tiltak 14
2.2 16

3. Tilfeller og konsekvenser 18
3.1 Hendelser 20
3.2 Arenaer for hendelser 21
3.3 Følger og håndtering av hendelser

4. Samarbeid mellom næingsliv/myndigheter 24
4.1 Rapportering 26
4.2 Samarbeid mellomm næringsliv/myndigheter 28

5. Evne til å tåle forstyrrelser i tilgang til ressurser 30
5.1 Endringer som følge av GDPR 32
5.2 Økt sikkerhetsbevissthet 32

6. Analyse 34

7. Trender 40

8. Forebyggende aktiviteter/tiltak 48

9. Etterord 54

Sammendrag

67 prosent av virksomheter med 100 ansatte eller flere mener det å ha en sentral og veletablert posisjon i samfunnet gjør at de er potensielle mål for hybride trusler.

70 prosent av virksomhetene mener manglende evne til å gjenkjenne påvirkningsforsøk kamuflert som andre henvendelser er et forhold som gjør virksomheten sårbar for hybride trusler. Videre er det 63 prosent som mener manglende sikkerhetsbevissthet i organisasjonen gjør dem sårbare. 48 prosent mener det er usannsynlig at de blir utsatt for hybride trusler, mens 24 prosent mener det er sannsynlig at de blir utsatt for slike trusler. Samtidig er det seks av ti som mener det er vanlig at virksomheter generelt blir utsatt for hybride trusler.

Datavirus og phishing-operasjoner ses som de største sårbarhetene som kan gi trusselaktører kontroll over virksomhetens informasjonssystemer (37 og 27 prosent). En av ti mener at den mest sannsynlige metoden en trusselaktør får kontroll over informasjonssystemene, er at trusselaktøren utnytter ansatte via blackmail, bestikkelse eller sosial manipulering, mens 5 prosent mener det mest sannsynlige er at en insider blir plassert i virksomheten.

Dersom man utsettes for hybride trusler, ses tap av konfidensiell informasjon, driftsforstyrrelser og tap av omdømme som ses som de mest alvorlige potensielle konsekvensene.

Det er 32 prosent av virksomhetene som har merket former for unormal aktivitet som kan utgjøre en hybrid operasjon. *Samtidig er det 14 prosent som har opplevd økt aktivitet i tidsrommet NATO-øvelsen Trident Juncture foregikk.*

Det er ikke et entydig svar på hvem virksomhetene ville kontaktet dersom man ble utsatt for hybride trusler. 63 prosent vil kontakte politiet, 33 prosent Nasjonal sikkerhetsmyndighet, 28 prosent PST, 14 prosent NorCert og 12 prosent Kripos (kan svare flere alternativ).

Om undersøkelsen

Bakgrunn
Opinion har gjennomført Hybridundersøkelsen på oppdrag fra Næringslivets Sikkerhetsråd.

Populasjon
Populasjonen for denne undersøkelsen er norske virksomheter i privat og offentlig sektor med 100 ansatte eller flere. Undersøkelsens utvalg er trukket fra Bisnodes database som henter informasjon fra Enhetsregisteret.
Det er gjennomført 354 intervju i undersøkelsen.

Datainnsamling
Datainnsamling er gjennomført ved hjelp av telefonintervjuer (CATI), i perioden 15. november til 4. desember 2018.

Feilmarginer
Opinion gjør oppmerksom på at enhver undersøkelse vil være beheftet med feilmarginer. Feilmarginene knytter seg i hovedsak til statistisk usikkerhet. Dette er utvalgsskjevheter som medfører at utvalget ikke er identisk med universet eller målgruppen. Ulikheter kan knytte seg til bestemte kjennetegn eller atferd.

Ved 354 respondenter eller intervjuer (n=354) kan vi med 95 % sannsynlighet si at det riktige resultatet ligger innenfor ± 2,3 og ± 5,2 prosentpoeng, avhengig av prosentresultatets størrelse. Usikkerheten er størst ved et prosentresultat på 50 % og minst ved prosentresultater på 5% / 95%.

Definisjon av Hybride trusler og angrep

Hybride angrep kan være rettet mot både stater og næringsliv, og identifiseres ut i fra de irregulære og ukonvensjonelle virkemidlene som tas i bruk. Dette kan blant annet være påvirkningsoperasjon, cyberangrep, spionasje og operasjoner hvor desinformasjon, nettmanipulering, undergraving står sentralt.

Karakteristikker

Respondentene i undersøkelsen har følgende fordeling mellom privat og offentlig sektor:

Sektor	Antall (n)	Andel Intervju
Privat	187	53 %
Offentlig	167	47 %
Totalt	354	100,0 %

Geografi

Under er en oversikt over respondentenes fylkesvise tilhørighet:

Fylke	Antall Intervju (n)	Andel Intervju
Oslo	58	16%
Østlandet for øvrig	126	36 %
Sør-/Vestlandet	99	28 %
Midt-Norge	49	14 %
Nord-Norge	22	6 %
Totalt	354	100 %

Virksomhetsstørrelse

Undersøkelsen omfatter virksomheter i følgende størrelsesgrupper:

Virksomhets-størrelse	Antall Intervju (n)	Andel Intervju
100 til 199 ansatte	216	61 %
200 ansatte eller flere	138	39 %
Totalt	354	100%

Bransje

Undersøkelsen omfatter virksomheter i følgende bransjer:

Bransje	Antall Intervju (n)	Andel Intervju
Industri etc.	52	15 %
Bygg og anleggsvirksomhet, transport og lagring	40	11 %
Varehandel, overnatting og servering	24	7 %
Tjenesteytende næringer	76	21 %
Offentlig administrasjon	33	9 %
Undervisning	34	10 %
Helse og sosial	95	27 %
Totalt	354	100 %

1. Virksomheter som mål for hybride trusler

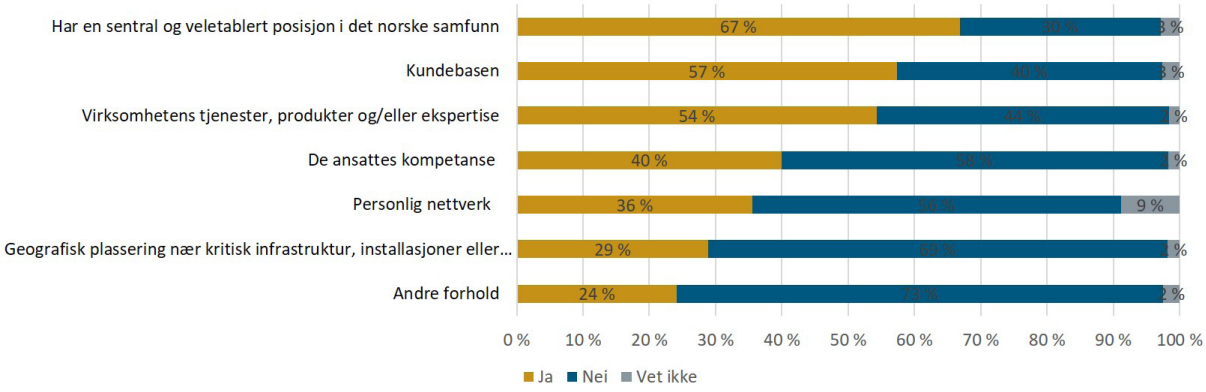
Dette kapitlet dekker spørsmål knyttet til virksomhetenes sårbarheter for hybride trusler

1. Virksomheter som mål

1.1 Potensielle mål for hybride trusler

På spørsmål om ulike forhold som potensialet kan utgjøre en trussel mot bedriften, er det 9 prosent som mener de ikke er et potensielt mål for noen av truslene. 3 prosent opplever at alle forhold spurt om er trusler som kan ramme dem.

Figur 1 Jeg vil nå lese opp noen ulike forhold og ber deg svare ja eller nei på om disse potensielt kan gjøre din virksomhet til et mål for hybride trusler? (n=354)



67 prosent av virksomheter med 100 ansatte eller flere mener det er at de har en sentral og veletablert posisjon i samfunnet som gjør at de er potensielt mål for hybride trusler. Det er noe mer vanlig å ha dette synet i offentlig enn i privat sektor (76 vs. 59 prosent), og det er mer spesifikt virksomheter inne offentlig administrasjon som mener dette. Blant virksomheter som anser seg som en del av kritisk infrastruktur er det 82 prosent som mener deres sentrale posisjon i samfunnet gjør dem til et potensielt mål for hybride trusler.

Nær 6 av 10 mener deres kundebase gjør dem til et potensielt mål for hybride trusler. Dette er et syn som fordeler seg likt uavhengig av undergruppe.

Når det gjelder produkter, tjenester og/eller ekspertise, er det 54 prosent som mener det gjør dem til et potensielt mål for hybride trusler. Virksomheter som ser seg som en del av kritisk infrastruktur (78 prosent), har dette synet i størst grad.

Fire av ti mener de ansattes kompetanse gjør dem til et mulig mål for hybride trusler. Dette er noe mer tilfelle i virksomheter med 200 ansatte eller flere enn i mindre virksomheter (48 vs. 35 prosent) og blant de som er en del av kritisk infrastruktur (50 vs. 35 prosent).

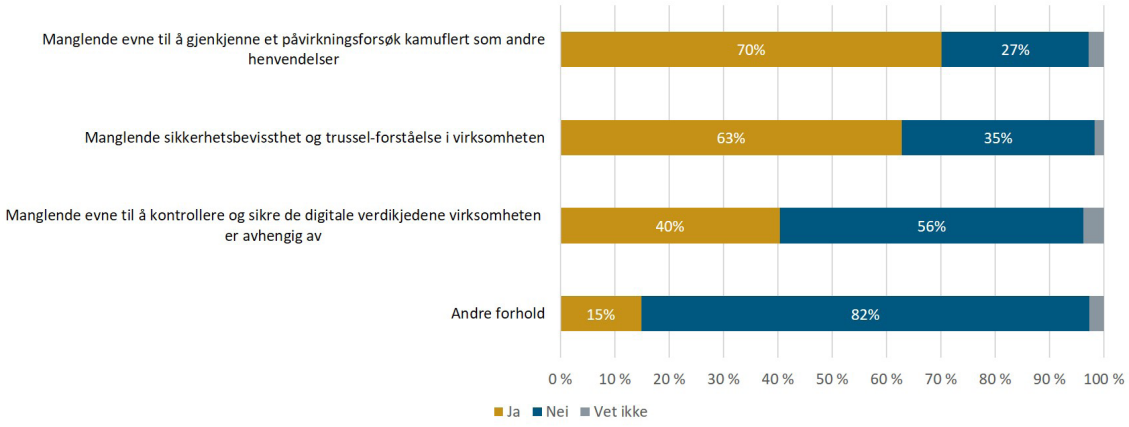
Personlige nettverk ses som en mulig årsak til at man er et mål for hybride trusler av 36 prosent av virksomhetene. De som er en del av kritisk infrastruktur mener dette i større grad enn andre (44 vs. 30 prosent). På andre bakgrunnsvariabler er det ingen forskjell.

Tre av ti mener geografisk plassering bidrar til at de kan være et mål for hybride trusler. 40 prosent av de som er en del av kritisk infrastruktur mener dette mot 35 prosent av andre. Det er også et mer utbredt syn i offentlig sektor enn i privat (37 vs. 21 prosent)

1.2 Forhold som kan gjøre virksomheten sårbar for hybride trusler

70 prosent mener en manglende evne til å gjenkjenne påvirkningsforsøk gjør dem sårbare for hybride trusler. Samtidig er det hele 63 prosent som mener manglende sikkerhetsbevissthet og trusselforståelse i virksomheten gjør dem sårbare for hybride trusler.

Figur 2 Tror du følgende interne forhold kan gjøre virksomheten sårbar for hybride trusler? (n=354)



Når det gjelder manglende evne til å gjenkjenne påvirkningsforsøk er det noe mer utbredt syn i offentlig virksomheter enn i private (79 vs. 62 prosent). Utover dette er det ingen forskjeller. Manglende sikkerhetsbevissthet og trusselforståelse som en årsak til sårbarhet, fordeler seg jevnt uavhengig av undergrupper med unntak av at det er mer utbredt i offentlige virksomheter som hører innunder offentlig administrasjon.

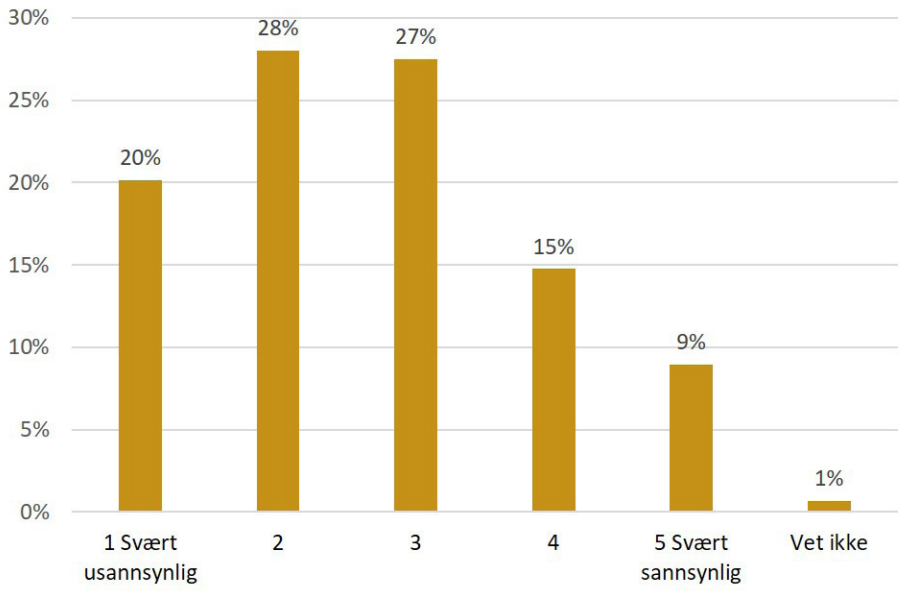
Fire av ti mener manglende evne til å kontrollere og sikre digitale verdikjeder virksomheten er avhengig av, kan gjøre dem sårbare for hybride trusler. Offentlige virksomheter mener dette er tilfelle i større grad enn private (48 vs. 34), men det ikke er andre forskjeller mellom undergrupper.

1. Virksomheter som mål

1.3 Sannsynlig å bli utsatt for hybride trusler?

Nær halvparten mener det er usannsynlig at de blir utsatt for hybride trusler, mens det er en av fire som mener der er sannsynlig at det skjer.

Figur 3 Hvor sannsynlig eller usannsynlig mener du det er at din virksomhet blir utsatt for Hybride trusler? (n=354)

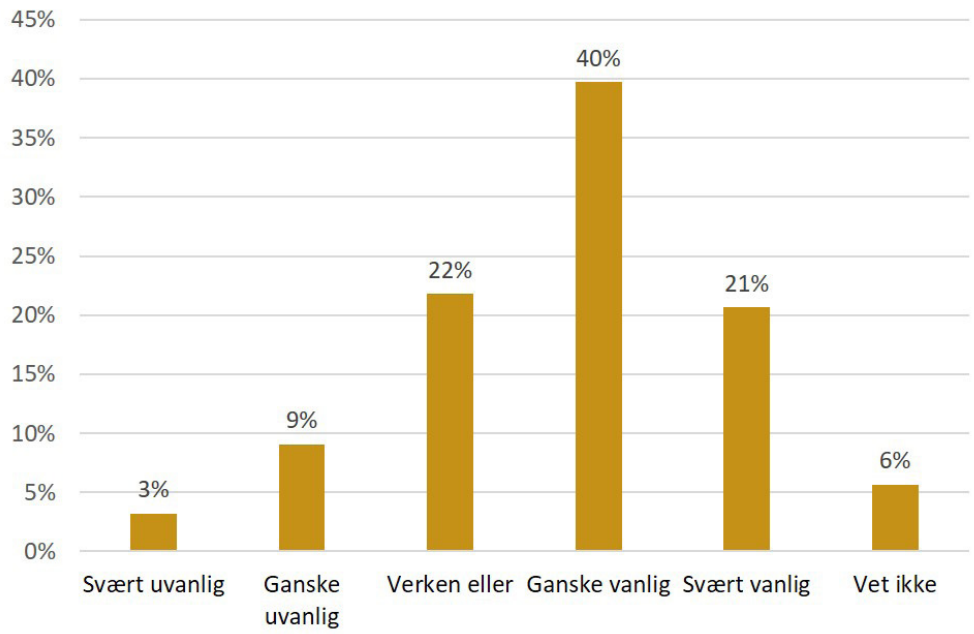


9 prosent mener det er svært sannsynlig at virksomheten blir utsatt for hybride trusler, mens ytterligere 15 prosent svarer verdien 4 på skalaen fra 1 til 5. Det er ikke forskjell på undergrupper, med unntak av at virksomheter i offentlig administrasjon i større grad enn andre mener det er sannsynlig at det skjer, hele 26 prosent sier det er svært sannsynlig. Det er imidlertid ikke forskjell på offentlig og privat sektor.

1.4 Tror det er vanlig å bli utsatt for hybride trusler

Seks av ti mener det er vanlig med hybride trusler, mens 12 prosent tror det er uvanlig.

Figur 4 Hvor vanlig eller uvanlig tror du det er at virksomheter blir utsatt for hybride trusler i Norge?



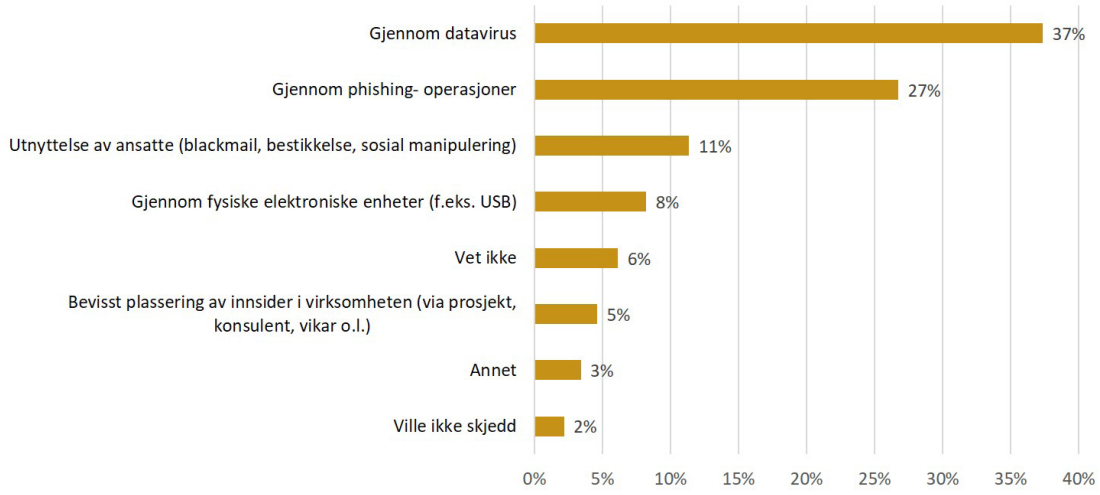
Offentlige virksomheter innen offentlig administrasjon mener i større grad enn andre at det er vanlig (78 prosent svarer svært eller ganske vanlig). Det samme er tilfelle blant de som leverer til offentlig sektor (71 prosent svarer svært eller ganske vanlig). Utover dette er det ikke forskjeller mellom ulike undergrupper.

1.5 Mest sannsynlige svakhet

Dersom en trusselaktør skulle få tilgang til virksomhetens informasjonssystemer, er det 37 prosent som mener at det vil ha skjedd via datavirus og 27 prosent som ser det som mest sannsynlig at det skjer via et phishing-angrep. En av ti mener at utnyttelse av ansatte er den mest sannsynlige metoden en trusselaktør benytter for å få tilgang, mens 5 prosent ser det som mest sannsynlig at en insider blir plassert i virksomheten. Kun 2 prosent svarer at det ikke ville skjedd.
På dette spørsmål er det ikke store forskjeller mellom ulike undergrupper.

1. Virksomheter som mål

Figur 5 Tenk deg en situasjon der en trusselaktør får tilgang til virksomhetens informasjonssystemer. Hvordan ville trusselaktøren mest sannsynlig fått denne tilgangen? (n=354)



De som svarer annet har de blant annet notert forhold som uredelige ansatte og at det skjer via andre parter som for eksempel via banken.

Ordskyen under viser de åpne svarene.

2. Virksomhetens forberedelser og forebygging

I dette kapitlet har

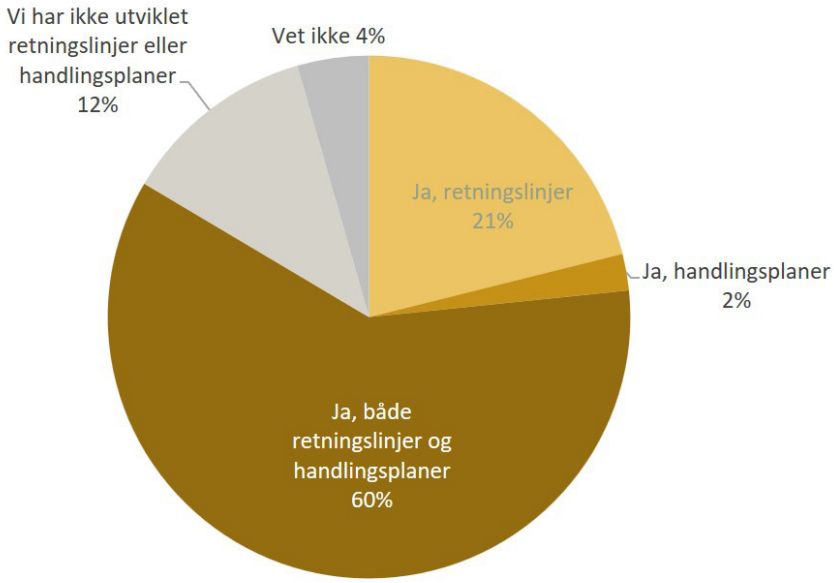
Ctrl

2. Forberedelser og forebygging

2.1 Retningslinjer eller handlingsplaner

Seks av ti har både retningslinjer og handlingsplaner for å beskytte virksomhetens verdier mot hybride trusler. 12 prosent har ikke utviklet retningslinjer eller handlingsplaner.

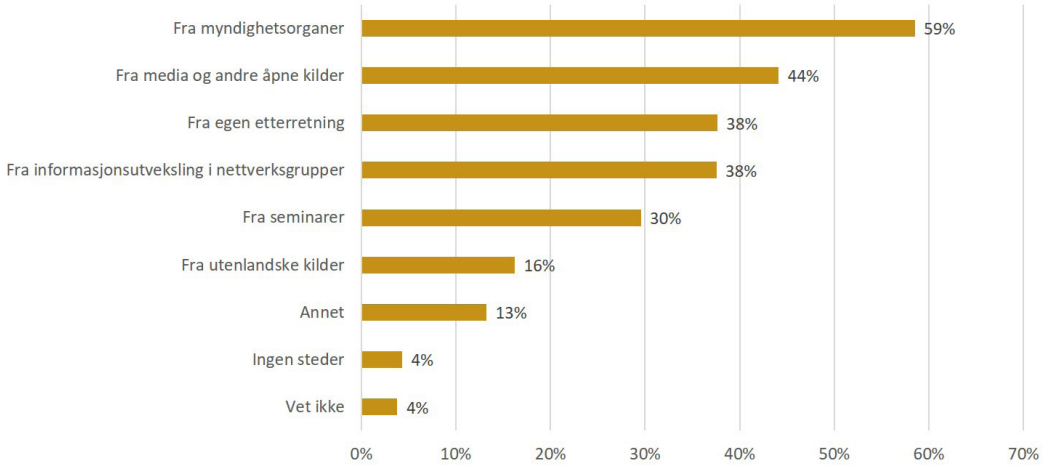
Figur 6 Har din virksomhet retningslinjer eller handlingsplaner for å beskytte virksomhetens verdier mot hybride trusler? (n=354)



Det er i noe større grad virksomheter i privat sektor som ikke har retningslinjer eller handlingsplaner. 16 prosent av private virksomheter har ikke slike retningslinjer eller planer mot 7 prosent av offentlige virksomheter. Tilnærmet samme forholdet er det mellom virksomheter som er del av kritisk infrastruktur og de som ikke er det. 15 prosent av de som ikke er del av kritisk infrastruktur har ikke retningslinjer eller planer, mens 7 prosent av de som er del av kritisk infrastruktur er i samme situasjon.

2.2 Informasjonskilder

Myndighetsorganer er den vanligste informasjonskilden for hybride trusler. Seks av ti mottar informasjon om hybride trusler, operasjoner og aktiviteter fra denne kilden.



Offentlige virksomheter mottar slik informasjon i større grad fra myndighetsorgan enn tilfelle er for private virksomheter (67 vs. 51 prosent). Private virksomheter får informasjon i større grad fra media (50 vs. 38 prosent) og utenlandske kilder (23 vs. 9 prosent) enn tilfellet er med offentlige virksomheter. De som er en del av kritisk infrastruktur får informasjon fra myndighetsorgan i større grad enn andre (68 vs. 53 prosent).

Blant de som svarer andre kilder har de notert er rekke ulike mulige informasjonskilder.

3. Tilfeller og konsekvenser av hybride trusler

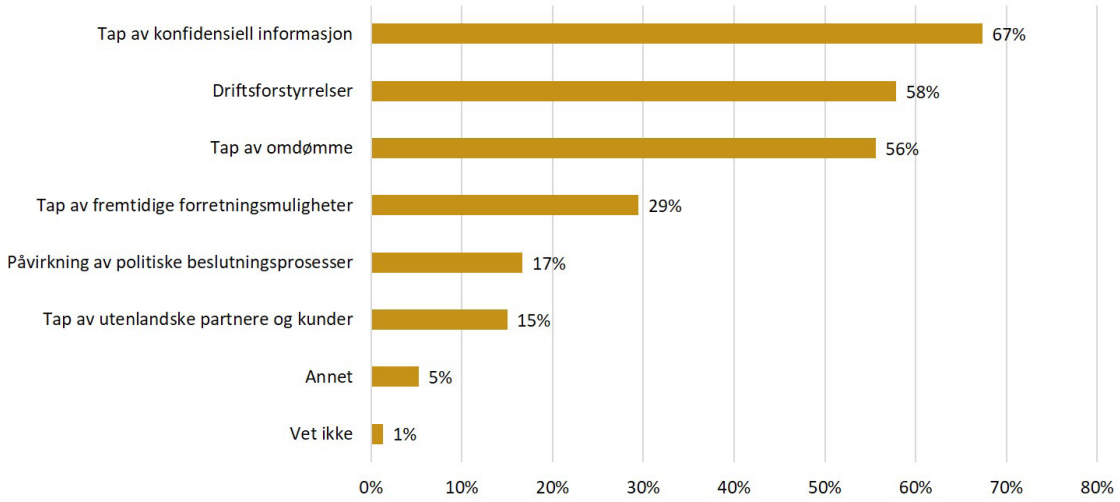
Det er

3. Tilfeller og konsekvenser

3.1 Konsekvenser

Tap av konfidensiell informasjon er den konsekvensen flest ser for seg som et resultat av å bli utsatt for hybride trusler.

Figur 7 Hva anser du som de mest alvorlige konsekvensene av hybride trusler? (n=354)

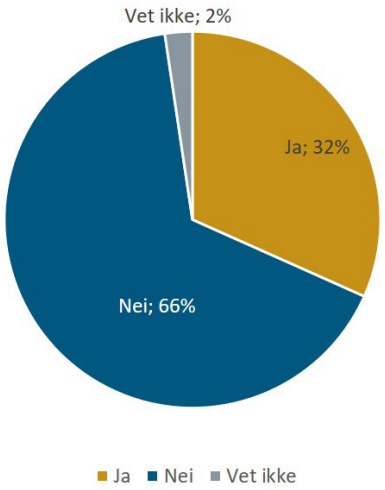


Virksomheter i offentlig sektor svarer tap av konfidensiell informasjon i større grad enn private virksomheter (79 vs. 57 prosent). Private på sin side mener i større grad enn offentlige at tap av fremtidige forretningsmuligheter og tap av utenlandske partnere er konsekvenser. De som er del av kritisk infrastruktur ser i større grad enn andre driftsforstyrrelser som den mest alvorlige konsekvensen.
Virksomheter med 200 ansatte eller mer ser i større grad enn mindre virksomheter tap av konfidensiell informasjon og tap av fremtidige forretningsmuligheter som en alvorlig konsekvens.
Virksomheter innen offentlig administrasjon ser i større grad enn virksomheter i andre bransjer at påvirkning av politiske beslutningsprosesser er en alvorlig konsekvens (39 prosent). Tap av konfidensiell informasjon trekkes mer fram som en alvorlig konsekvens i offentlig administrasjon og helse og sosial enn i andre bransjer (83 og 79 prosent).
De som har svart annet har blant annet notert økonomisk tap som en mulig konsekvens.

3.2 Unormal aktivitet

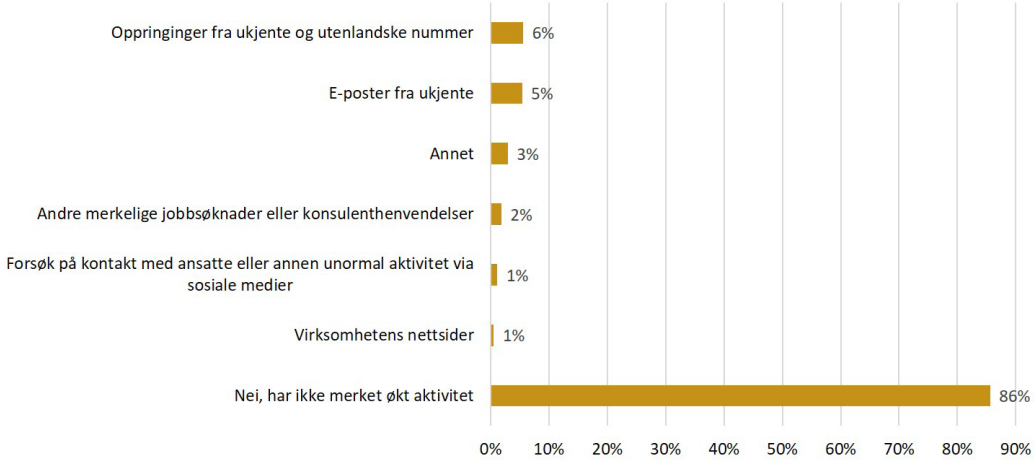
Tre av ti har opplevd unormal aktivitet som kan utgjøre en hybrid operasjon. På dette spørsmålet er det ikke forskjell mellom virksomheter i ulike undergrupper.

Figur 8 Har du merket noe form for unormal aktivitet rettet mot din eller andres virksomhet som kan utgjøre en hybrid operasjon eller deler av en slik operasjon? (n=354)



Mens det er 32 prosent som har opplevd unormal aktivitet mot virksomheten en eller annen gang, er det 14 prosent som sier de har opplevd økt aktivitet som kan være hybride trusler i tidsrommet NATO-øvelsen Trident Juncture foregikk (svarer en eller flere av alternativene under).

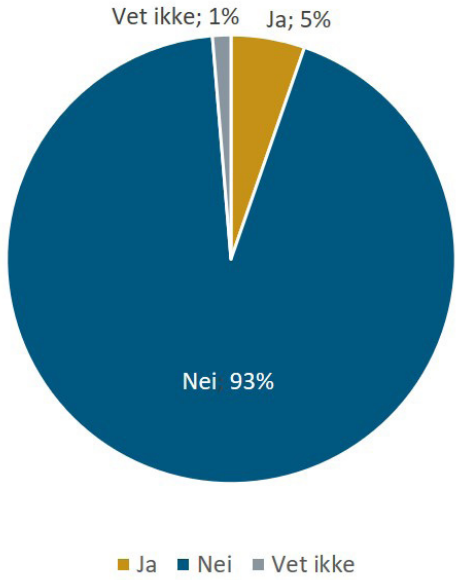
Figur 9 NATO-øvelsen Trident Juncture ble gjennomført i Norge høsten 2018. Har din virksomhet i dette tidsrommet merket økt aktivitet på følgende områder? (n=354)



3. Tilfeller og konsekvenser

Blant de som har opplevd aktivitet i tidsrommet NATO-øvelsen foregikk, er det oppringninger og eposter som er mest vanlig. Hhv. 6 og 5 prosent av virksomhetene har opplevd dette. Videre er det 2 prosent som har opplevd merkelige jobbsøknader eller konsulenthenvendelser, mens 1 prosent har opplevd forsøk på å kontakte ansatte via sosiale medier og aktiviteter mot virksomhetens nettsider.
5 prosent av virksomhetene har hørt om at andre virksomheter i eget nettverk har blitt utsatt for økt aktivitet som kan utgjøre hybride trusler i tidsrommet NATO-øvelsen foregikk.

Figur 10 Har du hørt om andre i ditt nettverk som har opplevd økt aktivitet på nevnte områder i dette tidsrommet? (n=354)



Det er ikke forskjeller på virksomheter i ulike undergrupper når det gjelder spørsmålene om aktiviteter under NATO-øvelsen.

4. Samarbeid mot hybride trusler

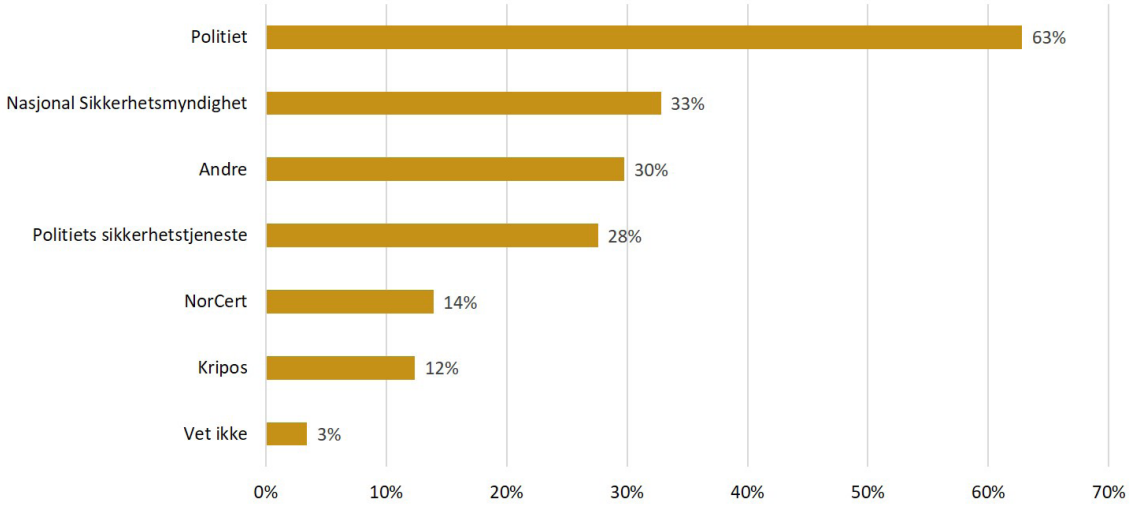
Dette kapitlet handler om

4. Samarbeid

4.1 Hvilke myndighetsorgan blir kontaktet

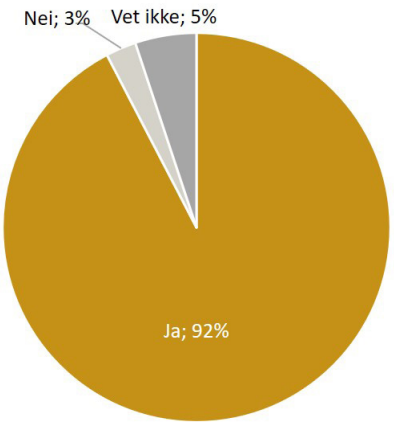
Dersom man blir utsatt for hybride trusler, vil virksomheter først og fremst ta kontakt med politiet.

Figur 11 Dersom din virksomhet skulle blitt utsatt for hybride trusler, hvilke myndighetsorganer ville dere kontaktet? (n=354)



63 prosent vill tatt kontakt med politiet dersom de blir utsatt for hybride trusler, mens det er relativt store ander som også ville kontaktet andre aktører.
En stor del av virksomhetene vil dele informasjon med norske myndigheter dersom det oppdages mistenkelig aktivitet rettet mot virksomheten. Dette er en holdning som er gjeldende uavhengig av undergruppe.

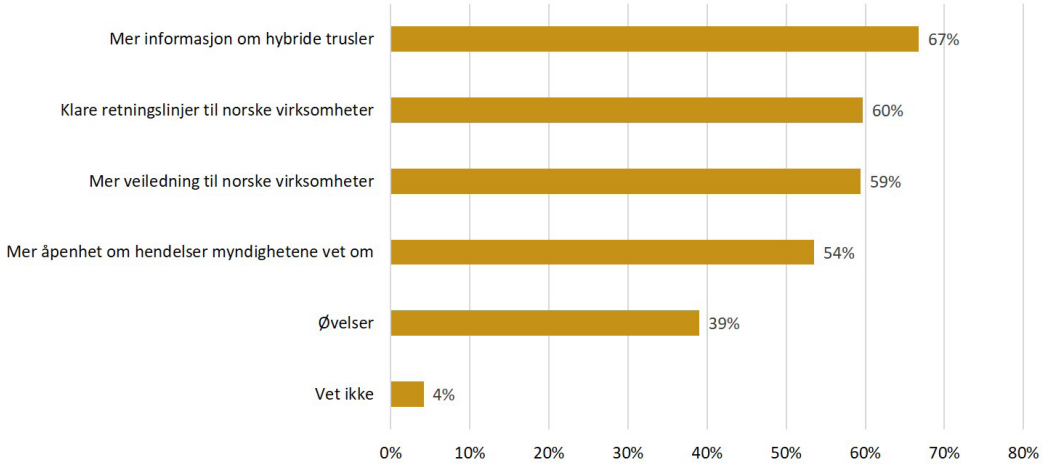
Figur 12 Ville din virksomhet delt informasjon med norske myndigheter dersom det oppdages mistenkelig aktivitet rettet mot virksomheten enten utenlands eller i Norge? (n=354)



4.2 Opplyse om hybride trusler

Mer informasjon fra myndighetene om hybride trusler er etterlyst fra virksomhetene.

Figur 13 Av følgende alternativer, hvilke mener du at norske myndigheter bør bidra med for å opplyse om hybride trusler? (n=354)



67 prosent etterlyser mer informasjon om hybride trusler. Ellers er det verdt å merke seg at 54 prosent mener større åpenhet om hendelser myndighetene kjenner til vil være et godt opplysningstiltak. Det er spesielt virksomheter med 200 ansatte eller mer og bygg/anlegg- og transportvirksomheter som mener dette (hhv. 63 og 76 prosent).

5. Evne til å tåle forstyrrelser i tilgang til ressurser

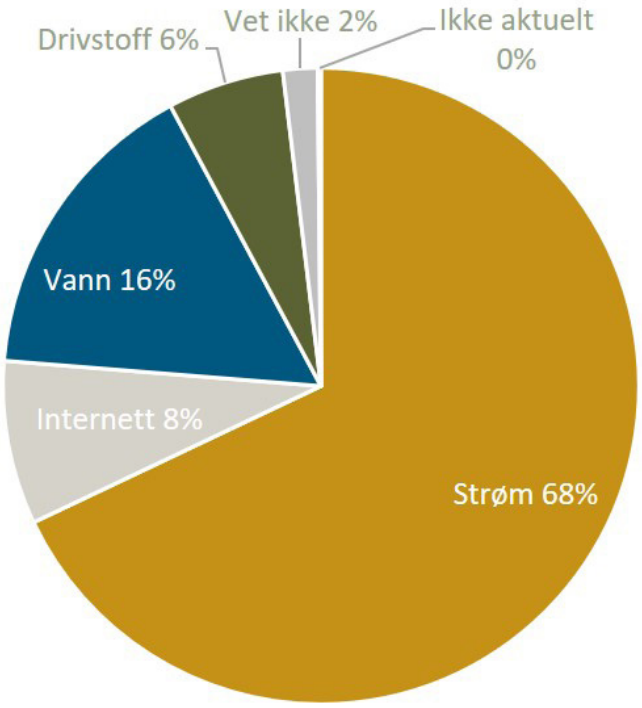
Dette kapitlet ser på

5. Evne til å tåle forstyrrelser

5.1 5.1 Bortfall av ressurser

Dersom strøm, internett, vann og drivstoff ikke er tilgjengelig, er det bortfall av strøm som vil merkes i størst grad.

Figur 14 Tenk deg at strøm, internett, vann og drivstoff ikke er tilgjengelig. Hvilke av de fire ville ha størst negativ effekt på din virksomhet? (n=354)



Virksomheter innen bygg/anlegg- og transport mener naturlig nok i større grad enn andre at bortfall av drivstoff vil ha størst negativ påvirkning (33 prosent). Virksomheter innen offentlig administrasjon mener i større grad enn andre at bortfall av internett vil være alvorlig (22 prosent), mens bortfall av vann vil være mest merkbart i inne undervisning og helse og sosial (26 og 34 prosent).

6. Analyse

I dette kapitlet har vi analysert noen av funnene i undersøkelsen.

6. Analyse

6.1 Hybride trusler – vanlig, men usannsynlig?

Virksomheter som tror det er vanlig at virksomheter blir utsatt for hybride trusler i Norge, anser det som lite sannsynlig å selv bli utsatt.

En høy prosentandel av respondentene, 60 prosent, mener det er vanlig at virksomheter blir utsatt for hybride trusler. Samtidig oppgir 48 prosent at de mener det er usannsynlig at sin egen virksomhet blir utsatt for hybride trusler. Trenden ser vi på tvers av sektorer, geografi og virksomhetenes størrelse.

Funnene peker dermed på en interessant tendens; næringslivet anser det som vanlig å bli utsatt for hybride trusler, samtidig som de mener sannsynligheten er liten for at det skal skje med egen virksomhet. Dette henspiller muligens på en felles oppfatning om at hybride angrep er noe utenkelig og fjerntliggende. Det er uklarhet og uenighet rundt begrepet hybride angrep. Begrepet fremstilles og anvendes forskjellig i ulike bransjer, miljøer og områder. En antagelse er at flere tror hybride trusler er hendelser som tar mye oppmerksomhet og som uten tvil oppleves som et angrep av alle involverte. Erfaringer viser derimot at hendelser kan være små og vanskelig å oppdage, og ta form som kartlegging, samarbeids- og kontaktinitiativ og påvirkningsforsøk.

Av virksomheter som oppgir at de er en del av kritisk infrastruktur, oppgir 67 prosent at de tror det er vanlig at virksomheter blir utsatt for hybride trusler. Samtidig oppgir 48 prosent av de samme respondentene at de anser det som usannsynlig at sin virksomhet blir utsatt for hybride trusler. Ikke-attribuerbare cyberoperasjoner[1] rettet mot offentlig tjenesteyting og infrastruktur presenteres av FFI som en av de viktigste utfordringene myndighetene kan stå overfor ved et hybridangrep.

Det kan være utfordrende å se hvordan hybride trusler vil påvirke eller utfordre egen bransje. Innenfor offentlig administrasjon mener 78 prosent at det er vanlig at virksomheter blir utsatt for hybride trusler i Norge. Videre oppgir 48 prosent at de anser det som sannsynlig at egen virksomhet blir utsatt for hybride trusler. En mulig forklaring på fokuset fra denne bestemte bransjen kan være at de nettopp er styrt at politiske prosesser og dermed i større grad informert om trusler som kan møte dem.

6.2 Virksomhetens posisjon i samfunnet – spiller det en rolle?

Tillit er en nøkkelvariabel i beskyttelse mot hybride trusler. Sosial tillit fremmer en sikkerhetsfølelse og bidrar til samarbeid og samhandling. Sosial tillit betyr at mennesker stoler på hverandre, strukturene i samfunnet og på autoritetene. Dette forbedrer vår mulighet til å forberede og beskytte flere kritiske funksjoner og daglige operasjoner. Nettopp derfor er tillit et mål for hybride operasjoner[2].

Virksomheter med en veletablert posisjon i samfunnet har gjerne stor tillit i befolkningen. Undersøkelsen viser at 67 prosent av respondentene oppgir at deres sentrale og veletablerte posisjon i det norske samfunn er et forhold som potensielt kan gjøre virksomheten til et mål for hybride trusler. For eksempel vil et angrep mot datasystemene til et sykehus ville være et ledd i et forsøk på å svekke befolkningens tillitt til en svært viktig institusjon.

Fra offentlig sektor svarer 76 prosent at deres sentrale og veletablerte posisjon i det norske samfunn er et forhold som potensielt kan gjøre virksomheten til et mål for hybride trusler. Fra privat sektor oppgir 69 prosent fra industri-, 62 prosent fra bygg og anlegg og 59 prosent fra

1 Ikke-attribuerbare angrep vil si at aktøren bak er ukjent og umuliggjør dermed et motangrep (FFI-Rapport 18/00080)
2 (HyWbrid CoE, 2018).

tjenesteytende -bransje at deres sentrale og veletablerte posisjon potensielt kan gjøre virksomheten til et mål.
Av virksomheter som er leverandører av kritisk infrastruktur oppgir 78 prosent at virksomhetens tjenester, produkter og/eller ekspertise gjør virksomheten til et potensielt mål for hybride trusler. Dette kan tyde på at virksomhetene er innforstått med at sin virksomhet er et attraktivt mål for trusselaktører. Overraskende er det da at 48 prosent fra samme gruppe anser det som usannsynlig at egen virksomhet blir utsatt for hybride trusler.

Henholdsvis 91 prosent og 83 prosent av offentlig administrasjon oppgir virksomhetens tjenester, produkter og ekspertise, samt de ansattes kompetanse som forhold som potensielt kan gjøre dem til mål for hybride trusler.

Svak sikkerhetskultur – en sårbarhet?
En oppfatning kan være at hybrid aktivitet kun foregår på et statlig nivå; ved at en stat påvirker standpunktet til en annen stat. Gjennom å studere de ulike virkemidlene som hybride operasjoner kan ta i bruk, er det tydelig at befolkningen, lokalsamfunnet og næringslivet spiller en signifikant rolle både som et mål, men også i rollen som god forebygger ved hjelp av en god sikkerhetskultur.

83 prosent av respondentene fra offentlig administrasjon oppgir at de ansattes kompetanse potensielt kan gjøre virksomheten til et mål for hybride trusler. Funnene er interessante sammenlignet med Kriminalitets- og sikkerhetsundersøkelsen i Norge (Krisino) 2017, som viser at bare halvparten av norske virksomheter foretar identitetssjekk i forbindelse med ansettelsesprosesser, og ca. 30 prosent foretar ekthetskontroll av vitnemål. En utro tjener kan enkelt utnytte og misbruke de ansattes kompetanse.
I årets undersøkelse ble det også stilt spørsmål ved hvordan en trusselaktør mest sannsynlig ville fått tilgang til virksomhetens informasjonssystemer. 5 prosent svarte her gjennom bevisst plassering av innsider i virksomheten (gjennom for eksempel prosjekt, konsulenttjenester eller vikar).

Undersøkelsen viser også at 70 prosent tror manglende evne til å gjenkjenne et påvirkningsforsøk kan gjøre virksomheten sårbar for hybride trusler. Mens 63 prosent tror manglende sikkerhetsbevissthet og trussel-forståelse i virksomheten utgjør en sårbarhet.
Innen offentlig administrasjon oppgir hele 96 prosent at manglende evne til å gjenkjenne et påvirkningsforsøk kan gjøre virksomheten sårbar for hybride trusler og 91 prosent tror manglende sikkerhetsbevissthet og trussel-forståelse kan gjøre virksomheten sårbar for hybride trusler. I Mørketallsundersøkelsen 2018 rapporterte 39 prosent om at mangel på sikkerhetsbevissthet blant de ansatte var en årsak til at sikkerhetsbrudd oppstod. Dette viser at forholdene næringslivet tror gjør virksomheten sårbar faktisk stemmer. Interessant er det også å sammenligne med tall fra Krisino 2017 hvor kun 16 prosent oppgir å lese PSTs trusselvurdering, og kun 11 prosent leser NSMs risikovurdering. Dette sender et sterkt signal om hva som bør forbedres og hva som er et enkelt tiltak.

40 prosent oppgir manglende evne til å kontrollere og sikre de digitale verdikjedene virksomheten er avhengig av som et forhold som kan gjøre virksomheten sårbar for hybride trusler. I Mørketallsundersøkelsen 2018 oppgir 8 prosent at problemer som skyldes outsourcingpartner var en årsak til at sikkerhetsbrudd oppstod.

6. Analyse

På spørsmål om hvordan en trusselaktør mest sannsynlig ville fått tilgang til virksomhetens informasjonssystemer oppgir 37 prosent gjennom datavirus og 27 prosent gjennom phishing-operasjoner. Mørketallsundersøkelsen 2018 bekrefter denne antagelsen og peker på at virus eller malwareinfeksjon er mest alvorlige hendelsen som forekommer. Phishing-operasjoner utnytter og bedrar personer i virksomhetene og forekomsten har økt kraftig fra 2016 til 2018.

6.3 Alvorlige konsekvenser

Når det gjelder de mest alvorlige konsekvensene av hybride trusler er det tap av konfidensiell informasjon som flest oppgir som mest alvorlig. Videre er det driftsforstyrrelser med 58 prosent og tap av omdømme med 56 prosent som anses som de mest alvorlige konsekvensene.

17 prosent av respondentene oppgir påvirkning av politiske beslutningsprosesser som en av de mest alvorlige konsekvensene av hybride trusler. Respondenter fra offentlig administrasjon anser 39 prosent påvirkning av politiske beslutningsprosesser som en av de mest alvorlige konsekvensene. Dette er urovekkende fordi en påvirkningsoperasjon kan medføre enorme konsekvenser og kan sette sentrale demokratiske prinsipper i spill.

6.4 Hendelser

32 prosent av respondentene har opplevd noen form for unormal aktivitet rettet mot sin egen eller andres virksomhet som kan utgjøre en hybrid operasjon eller deler av en slik operasjon. 40 prosent innenfor industribransjen, 42 prosent i offentlig administrasjon og 37 prosent innenfor undervisning svarte ja på dette spørsmålet. Geografisk ser vi en større forekomst i Nord-Norge hvor 40 prosent svarer at de har opplevd unormal aktivitet.
NATO-øvelsen Trident Juncture ble gjennomført i Norge høsten 2018. Undersøkelsen viser at 14 prosent av respondentene opplevde økt aktivitet eller henvendelser i dette tidsrommet. Dette tydeliggjør det faktum at trusselbildet kan endres i takt med vår egen aktivitet. Dette er et forhold det er viktig å signalisere til både myndigheter, næringsliv og samfunnet forøvrig.

6.5 Om samarbeidet mellom myndigheter og næringslivet

På spørsmål om hvilket myndighetsorgan en virksomhet ville kontaktet ved en hybrid hendelse, svarer 63 prosent at de ville kontaktet Politiet, mens 33 prosent sier de vil kontakte NSM, 30 prosent svarer "andre", og 28 prosent svarer PST.

Svarene viser at det ikke er entydig for næringslivet hvem de skal rapportere eller melde ifra til når de opplever noe mistenkelig som kan knyttes til en hybrid hendelse. For mange oppleves "politi" eller ansvarlig myndighet som fragmentert og uklart hvem som har ansvar for hva.

Fra å ha ett politi med ett tydelig nasjonalt ansvar, har utviklingen innen teknologi og digitalisering av samfunnet de siste ti årene gitt oss en samfunnsstruktur og organisering med spesialiserte enheter som er underlagt ulike departement og myndighetsorganer. Noen myndighetsorganer kan også ha overlappende funksjoner, og ansvarsfordelingen blir derfor uklar for næringsliv og samfunn.

6.4 Deling av informasjon mellom myndigheter og næringsliv

På spørsmål om fra hvilke informasjonskilder næringslivsaktører mottar informasjon innen cyber- sikkerhet, svarer 59 prosent at de får den fra myndigheter på ulikt vis, 44 prosent svarer media og 38 prosent sier de får nødvendig informasjon fra egen etterretning.
I vårt digitaliserte samfunn er informasjon og kompetanse innen sikkerhet blitt nødvendig ferskvare.

I tillegg til mengden av informasjon som blir digitalisert, er det heller ikke begrensninger på tilgang til all type teknologi, hvilket betyr at myndighetene ikke alltid har et "teknologisk forsprang" overfor kriminelle. Samlet medfører dette at vi alle, både næringsliv, myndigheter, politi og forsvar må holde oss oppdatert om trusselbildet 24/7 og dele mer av egne hendelser, etterretning og erfaringer enn noen gang før.

På spørsmål om virksomhetene er villige til å dele informasjon med myndighetene, svarer hele 92 prosent at de ønsker det, 3 prosent sier nei og 5 prosent svarer "vet ikke". At det er en så høy andel som svarer at de ønsker å dele informasjon med myndighetene samsvarer med at nesten 90 prosent av digital infrastruktur i Norge er i private hender. Det viser også et ønske fra næringslivet om å ta ansvar og samarbeide bedre enn det som er tilfellet i dag.

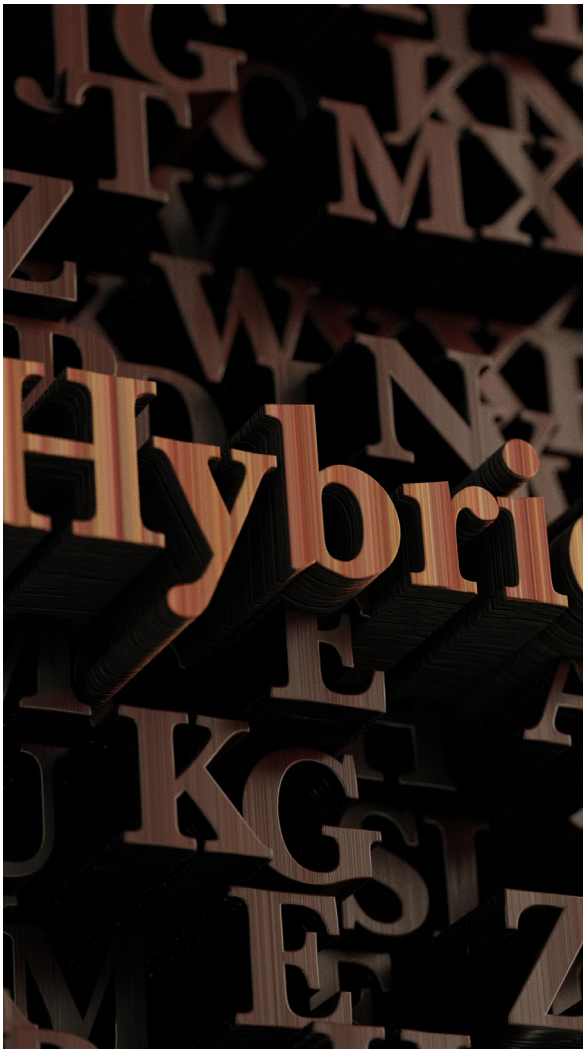
På spørsmål om mer informasjon fra myndighetene om hybride trusler, svarer 76 prosent at de ønsker mer informasjon, 60 prosent ønsker mer retningslinjer, 59 prosent vil ha veiledninger og 54 prosent ønsker mer åpenhet fra myndighetene.

En positiv utvikling er at E-tjenestene de siste 3 årene har utgitt åpne trusselvurderinger. Det å omsette informasjon til konkrete og riktige tiltak, er en utfordring som ikke er løst godt nok per dags dato. I følge Kriminalitets- og sikkerhetsundersøkelsen i Norge – 2017 (KRISINO) i regi av Næringslivets sikkerhetsråd, var det i privat sektor 14 prosent som hadde lest PSTs trusselvurdering, mot 26 prosent i offentlig sektor. Tilsvarende for NSMs risikovurdering er 8 og 21 prosent.

6.4 Samarbeid mellom sivile og forsvar

Skillet mellom militær og sivil sektor viskes gradvis ut ved digitalisering. Et hybrid angrep kan komme fra en statlig aktør, organiserte kriminelle, terrororganisasjon eller via en enkeltperson. Eller det kan være en kriminell organisasjon som utfører cyber angrep for en statlig aktør. Eksempelvis "Night Wolfes" – en russisk motorsykkelklubb som støttes av Putin, og som blant annet har vært aktiv i Ukraina: https://en.wikipedia.org/wiki/Night_Wolves . Hybride angrep kan bli rettet mot samfunnets svake sider, spesielt via digitale sårbarheter. Man bør derfor tenke nytt innen sårbarheter og ikke bare fokusere på kritisk infrastruktur.

Hybride trusler krever proaktivitet og samhandling på tvers av sektorer, departement og ansvarsområder. Det krever også en forankret og felles situasjonsforståelse. Mer om dette utdypes under kapittelet om "tiltak".



7. Trender

I dette kapitlet presenterer vi trender sett fra ulike myndigheter og private aktører.

Delata

7. Risikobildet/trender

7.1Hybride virkemidler- en uforutsigbar trussel

Jan Ivar Botnan, forskningssjef, Forsvarets forskningsinstitutt

Innledning

I 2018 ble NATO-øvelsen Trident Juncture gjennomført med stort engasjement fra involverte i både Forsvaret og det sivile samfunn. Samspillet mellom flere sektorer innen rammene for det revitaliserte Totalforsvaret ble øvet i lys av alliertes behov, regelverk og trusselbilde. Øvelsen bedømmes som svært vellykket, men selve totalforsvarskonseptet reiser flere viktige problemstillinger som må få oppmerksomhet i det videre arbeid med landets beredskap. Når Forsvaret gjennom bruk av beredskapslovene og beredskapskontrakter gjør bruk av sivile leverandører til sine operasjoner, kan disse bli lovlige krigsmål. Dessuten vil kritisk sivil infrastruktur kunne angripes under krise eller krig for å svekke forsvarsevnen og viljen til å motstå politisk press. Dette er kjente metoder fra krigshistorien. Offentlige og private virksomheter som bidrar til å ivareta samfunnskritiske funksjoner, kan bli utsatt for spionasje, sabotasje og terrorisme. Terrorbombingen av England 1940 og av Tyskland i 1945 er slike eksempler, selv om formålet med bombingen ikke ble oppnådd; motstandsviljen ble ikke svekket, snarere tvert imot. Dette viser at det er vanskelig å forutsi de psykologiske konsekvensene av anslag mot et samfunn, noe også reaksjonene etter 22. juli 2011 viste. Landet samlet seg i solidaritet i stedet for å jakte på skyldige.

I årets trusselvurdering fra PST står det. «Statlig styrte nettverksoperasjoner representerer en vedvarende trussel mot norske verdier. Metodene er billige, effektive og i konstant utvikling, og angriperne finner stadig nye sårbarheter de kan utnytte.» Dette er riktig, men for å være til nytte for det daglige beredskapsarbeidet må utsagnet nyanseres og konkretiseres.

Vi må åpenbart arbeide strukturert for å bygge en bred beredskap mot ondsinnede handlinger fra terrorister og fremmede makter. Dette vil selvfølgelig foregå i samarbeid med allierte og nære venner, men historien viser at selv de nærmeste kan fordreie virkeligheten av politiske grunner. Derfor finnes det ikke noe alternativ til nasjonal kompetanse.

Russlands operasjonsmønster i Ukraina har satt begrepet hybridkrig på dagsorden i vår beredskapsplanlegging. Selv om hybridkrig i prinsipp ikke er noe nytt, så har samfunnsutviklingen og trusselbildet åpnet for nye, og tidligere ukjente, utfordringer for sivil sektor. Det er derfor fortjenestefullt at Næringslivets Sikkerhetsråd har kartlagt forståelsen og opplevelsen av hybride angrep. Vi skal innledningsvis merke oss at hele 67 % av respondentene ønsker mer informasjon om hybride trusler, og at 54 % mener myndighetene må vise mer åpenhet om hendelser som har funnet sted.

Hybridkrig

Begrepet hybridkrig ble introdusert i 2007 av Frank Hoffman. Han analyserte hvordan Taliban, Al-Qaida og Hezbollah hadde hatt fremgang mot konvensjonelt sterkere motstandere, og betegnet deres vellykkede operasjoner som hybridkrig.

Russlands operasjoner i Ukraina i 2014 overraskket og satte begrepet hybridkrig for alvor på dagsorden. Under sin folkerettsstridige annektering av Krim og støtte til opprøret i Donbass, gjennomførte Russland sabotasje, spredte falske nyheter som fant klangbunn hos den etnisk russiske befolkningen, og brukte irregulære styrker. Dette viste seg å være svært effektivt, og Russland tok kontroll på Krim med lite bruk av

tradisjonell militærmakt. Erfaringene i Donbass var mer blandede. Operasjonene stod i sterk kontrast til krigene i Tsjetsjenia og Georgia som var unødvendig voldelige, utført med gammelt materiell og under dårlig ledelse.

Det ble hevdet at Russland hadde utviklet et nytt strategisk konsept (hybridkrig) som skulle kompensere for landets underlegenhet overfor NATO i konvensjonelle militære styrker. Støtte for denne påstanden ble funnet i en artikkel av general Gerasimov fra 2013. Gerasimov bruker imidlertid ikke begrepet hybridkrig. Hans artikkel dreier seg om hvor effektivt Vesten har veltet sittende regimer uten bruk av militære virkemidler. Eksemplene hans er Den arabiske våren (2010-11), Orangebevegelsen i Ukraina (2004) og Roserevolusjonen i Georgia (2003). Artikkelen er bygget på et foredrag han holdt for militære ledere som han beskylder for ikke å ha «fulgt med i timen». Gerasimov kan nok ha rett i noen av sine analyser, men han overdriver, spesielt hva gjelder deler av Den arabiske våren der amerikanerne viste liten vilje til å støtte demokratibevegelsene, og har blitt kritisert for det. Allikevel bør selve konseptet hybridkrig, eller bruk av hybride virkemidler, vies oppmerksomhet. I en fremtidig konflikt må vi være forberedt på å bli eksponert for alle relevante virkemidler en motstander rår over, også kjernevåpen, som riktignok vanskelig kan defineres inn under begrepet hybridkrig. Spesielt for operasjonene i Ukraina var at Russland kunne spille på landets historie, avsettingen av den lovlig valgte presidenten og den store russiske minoriteten som følte seg diskriminert av Kiev. Slike forhold vil man ikke finne i Norge, men det er god grunn til at de baltiske land, med betydelig russisk minoritetsbefolkning, føler seg urolige. I disse landene er det rapportert om anslag mot infrastrukturen, uten at dette har blitt fulgt opp med andre virkemidler.

Hybride virkemidler kan være effektive. Det er etterretnings- og sikkerhetsmyndighetenes oppgave å overvåke andre lands øvelser, kartlegge kapasiteter og egne sårbarheter, og vurdere hvilke nye teknologier som kan bli benyttet. For å illustrere spennet i hybride virkemidler, vil det bli gitt noen eksempler. Grunnlaget bør være at en motstander vil vurdere alle muligheter.

De seneste tiår har det foregått en eksplosiv utvikling i bioteknologien. Det menneskelige genom er for lengst sekvensert, og nye muligheter for påvirkning av livsprosessene er utviklet, i forskningens og medisinens tjeneste. Men i dette ligger også en ny trussel. Under den kalde krigen var biologiske våpen bygget på naturlig forekommende mikroorganismer. Nå kan mikroorganismer genmodifiseres, slik at de kan forårsake til nå ukjente sykdommer og for eksempel være resistente overfor tilgjengelig vaksine og antibiotika. Nye narkotiske stoffer som virker sløvende og påvirker dømmekraften, utvikles stadig. Det er ikke vanskelig å forestille seg at slike virkemidler kan benyttes til å svekke beredskapen ved at nøkkelpersonell settes ut av funksjon. Det kan være enklere enn fysisk å slå ut kraftforsyningen, sprenge en bro eller hacke seg inn i prosesskontrollsystemet på en terminal for gasseksport. Denne trusselen er dessverre lite påaktet; det er lettere å forstå og forholde seg til kuler og eksplosiver.

Et virkemiddel som derimot har fått mye oppmerksomhet i form av offentlige utredninger og styrking av kompetansemiljøer, er cyberangrep. Satsning på bedre mottiltak er nødvendig i lys av den raske teknologiske trusselutviklingen. Nye og mer effektive systemer har blitt introdusert uten at sikkerheten overfor cyberangrep har vært tilstrekkelig utredet. Dette arbeides det nå aktivt med i mange miljøer, men fortsatt avdekkes det tekniske sikkerhetshull og utilstrekkelig organisasjonsmessig sikring.

7. Risikobildet/trender

Dette inviterer til kriminelle anslag som påfører næringslivet store tap. Det er derfor naturlig at det settes inn betydelige ressurser for å sikre egen virksomhet. I enkelte bransjer samarbeides det godt med bransje-CERTer, med støtte fra nasjonale ressurser.

Spørsmålet i denne sammenheng er om det også gjennomføres eller planlegges hybride angrep mot sentrale private og offentlige virksomheter. Hensikten vil da være å svekke det norske samfunnet i krise og krig. Her står man oppe i et problem: Hvordan skiller man slike anslag fra kriminalitet og avanserte «guttestreker»? De som arbeider med hybride virkemidler, kan også være interessert i spionasje med rent økonomiske motiver. I det praktiske sikkerhetsarbeidet spiller det kanskje ingen rolle hva motivet er, man må uansett sikre seg. Det er imidlertid et faktum at de gruppene som i statlig regi forbereder hybridkrig, er svært dyktige og ressurssterke. De kan operere slik at det knapt er mulig for den enkelte virksomhet å oppdage og avverge anslag. Derfor må vi ha sterke nasjonale ressurser som kan støtte sikkerhetsarbeidet i de mest utsatte bransjene, slik sikkerhetsloven legger opp til.

Det er viktig at det nasjonale trusselbildet er nøkternt og balansert. Bare motstanderen tjener på neglisjering og overdrivelser. Mange virksomheter i Norge er godt sikret, og det vil være ekstremt vanskelig å trenge inn i og overta styringen av prosesskontrollsystemene. I den åpne litteratur finner man svært få veldokumenterte eksempler på at dette har funnet sted. Et ekstremt unntak er Stuxnet, dataviruset som fikk Irans sentrifuger for urananrikning til å løpe løpsk. Dette var imidlertid en svært ressurskrevende operasjon, hvor de mest avanserte stater sto bak og brukte flere år på utviklingen. Det er lite sannsynlig at noen vil prioritere slike satsninger for annet enn de høyest prioriterte målene. Denne forståelsen må reflekteres i beredskapsarbeidet.

Av forståelige grunner er virksomheter lite åpne om sikkerhetshendelser, dels for ikke å fremstå som enkle mål og dels for at ikke tilliten i aksjemarkedet skal svekkes. Likevel er kunnskapen om hendelser det viktigste grunnlaget for god beredskap. Derfor må det arbeides for mer systematisk innrapportering av hendelser, slik at de kan inngå i grunnlaget for sikkerhetsmyndighetens rådgivning. Mer åpenhet om hendelser er ønsket av 54 % av respondentene i undersøkelsen.

Hybridundersøkelsen er et godt tilskudd til det ellers gode arbeidet som gjøres for å sikre norske virksomheter mot cyberangrep, herunder forsvar mot hybride virkemidler. Det er imidlertid ett element i trusselbildet som bør få mer oppmerksomhet; sosial medier. Det mest vellykkede hybridangrep er når man kan nå sine mål uten bruk av militære ressurser. Eksempelvis kan den svenske opinionen ved en mulig fremtidig folkeavstemning om NATO-medlemskap bli påvirket av en fremmed makt. Dette har klare paralleller til det som kan ha funnet sted under presidentvalgene i Frankrike (2017) og USA (2016), og ved Brexit-avstemningen i Storbritannia (2016). Denne type påvirkning er ikke noe nytt; propaganda har vært benyttet i de fleste konflikter. Det nye er at internett og spesielt sosiale medier samler enorme mengder personopplysninger til promotering av avsenderen og underholdning for vennekretsen. Noe kan også være straffbart eller i det minste ubehagelig for den det gjelder.

Påvirkning av valg

Den ultimate effekten av hybride virkemidler er å endre utfallet av demokratiske valg. Mest effektivt gjennomføres dette i samarbeid med politiske grupperinger som har sammenfallende interesser med fremmede makter eller av andre grunner ser seg tjent med støtte utenfra. Under Den kalde krigen mottok flere politiske partier i Vest-Europa finansiell støtte fra Moskva.

En merkbart mer offensiv russisk utenrikspolitikk har igjen satt spørsmålet om påvirkning av demokratiske valg på dagsorden. I første rekke har det vært mistanke om innblanding ved presidentvalget i USA og Brexit-avstemningen, som begge ga svært uventede resultat. Senere rådet det bekymring for at Russland aktivt skulle påvirke valgene i Tyskland og Frankrike (2017), spesielt fordi fremgang for EU-skeptiske partier ville være i Russlands interesse. I kjølvannet av flyktningestrømmen fra Syria lå det godt til rette for at voldsepisoder, ensidig nyhetsfokus, spredning av kompromitterende informasjon og falske nyheter ville påvirke store velgergrupper.

Det amerikanske presidentvalget

La oss gå tilbake til den vestlige fortolkningen av general Gerasimov. Hensikten med hybride virkemidler er å nå politiske mål for lavest mulig pris, helst uten å bli avslørt og med minst mulig maktanvendelse og tap. Fra vestlig side fremheves de russiske operasjonene i Ukraina som skremmende eksempler på at russerne har lært raskt, og har evne og vilje til anslag mot naboland. Når støvet har lagt seg i Washington og forhåpentligvis alle forhold rundt presidentvalget i 2016 har kommet på bordet, kan russisk samspill med enkelte amerikanske politikere og tyveri av sensitiv informasjon fremstå som det ultimate eksempel på vellykket bruk av hybride virkemidler, et skoleeksempel for dem som planlegger slikt.

Etter presidentvalget i USA 2016 har amerikanerne trukket seg ut av internasjonale avtaler og samarbeid, og dermed åpnet for at land som Kina og Russland kan styrke sine posisjoner. Presidenten har signalisert mindre amerikansk tilstedeværelse i Midtøsten og i perioder skapt tvil om forholdet til NATO. For tiden er det kjølig forhold mellom president Trump og mange av hans europeiske allierte, mens han tilsynelatende har et langt mer positivt forhold til president Putin, førstesekretær Kim Jong-un, kronprins bin Salman og statsminister Netanyahu. Det kan bli konflikter av slikt. Sett fra Moskva kan dette oppleves som gode muligheter for å gjenskape status og innflytelse fra sovjettiden.

Hvordan kunne dette skje; er russerne ekstremt dyktige eller er det samfunnsutviklingen og tilgangen på nye virkemidler som har gjort det enkelt? Med tanke på vår egen beredskap vil det være nyttig å rekapitulere hendelsene rundt presidentvalget, slik vi nå oppfatter dem.

USA var i 2016 et polarisert samfunn. Middelklasse-amerikanere følte seg glemt av eliten i Washington, som ble oppfattet å ivareta egne interesser med utbetaling av enorme lønninger og bonuser. Bruk av føderale midler for å redde bank- og bilindustrien under finanskrisen i 2008, ble oppfattet som et svik mot alle dem som mistet sine boliger. Mens partiene i Kongressen tidligere kunne finne frem til kompromisser i vanskelige saker, var frontene nå steile. Kompromissvilje ble straffet hardt av kjernevelgerne. Dette var bakteppet for Trumps vellykkede kampanje. Hans opptreden under og etter valgkampen har bidratt til ytterligere polarisering.

7. Risikobildet/trender

President Trump kom raskt i konflikt med maktapparatet i Washington. Hans omgang med sannheten var lemfeldig. Opptelling i Washington Post viser at han i 2018 i gjennomsnitt løy 15 ganger om dagen (i det offentlige rom). Når presidenten setter en slik standard, blir det lettere å få gjennomslag for falske nyheter som kan tjene en fremmed stats interesser. Grensen mellom sannhet og løgn viskes ut. Makthavernes troverdighet svekkes.

Amerikansk etterretning konkluderte i januar 2017 med at den russiske regjeringen hadde påvirket det amerikanske presidentvalget ved å trenge inn i datasystemet til det demokratiske partiet og stjele den personlige e-posten til Hillary Clintons kampanjeleder John Podesta, for så å videreformidle den til WikiLeaks. I tillegg hadde de spredt falske nyheter på sosiale medier og forsøkt å trenge inn i valgsystemer og databaser i flere amerikanske delstater. Påstandene ble bekreftet av nederlandsk etterretning, som i 2014 og 2015 skal ha fulgt russiske nettoperasjoner.

Forholdet kompliseres av mistanke om at Trump-kampanjen samarbeidet tett med russerne. Dette gjør saken sterkt politisk, noe som kommer tydelig til uttrykk i Kongressen og reflekteres i pressen. Spesialetterforsker Mueller er satt på saken, med vide fullmakter. I påvente av hans konklusjon, preges saken av lekkasjer og spekulasjoner. I 2017 rapporterte New York Times at etterforskningen hadde avdekket kontakt mellom russisk etterretning og medlemmer av Trumps valgkampstab. Flere personer er dømt for å ha løyet for FBI. Så langt er det imidlertid uavklart hva Trumps kontakter bestod i, om det utelukkende var sammenblanding av ulike roller, eller om det ble etablert relasjoner som har brakt Trump i et avhengighetsforhold til Putin. Enkelte av Trumps opptredener har bidratt til disse spekulasjonene.

I januar 2017 ble en sikkerhetsgradert rapport lekket til pressen. Christopher Steele, britisk russlandsekspert og tidligere etterretningsoffiser, hevdet at Moskva sitter på kompromitterende informasjon om Trump, blant annet skal han være filmet med prostituerte på et Moskva-hotell i 2013. Rapporten ble finansiert av Clinton-kampanjen og det demokratiske partiet. Det er knyttet stor spenning og forventing til spesialetterforsker Muellers rapport, om den vil gi grunnlag for riksrett mot presidenten. Noen konklusjoner kan vi imidlertid allerede trekke. Russerne forsøkte å påvirke valgutfallet og resultatet ble som de ønsket. Saken har svekket presidentembetet og skapt mistanke om at Trump har en skjult agenda. Trolig har det vært relativt enkelt å få tilgang til demokratenes servere, da passord ble lekket. Påvirkningen gjennom sosiale medier er langt mer interessant. Dette er et hovedpunkt i Muellers etterforskning. Selskapet Cambridge Analytica står her sentralt. Det ble stiftet i 2013, og Breitbart-redaktør og Trump-medarbeider Steve Bannon var i en periode viseadministrerende direktør i selskapet. Forretningsidéen er å samle informasjon om velgere, slik at deres holdninger og preferanser kan kartlegges. Dette gjør det mulig å skreddersy et politisk budskap for å gi det størst mulig gjennomslag.

Cambridge Analytica

Dr Michal Kosinski er amanuensis i psykologi ved Stanford University, USA. I perioden 2008 til 2014 studerte han ved Cambridge University, der han utviklet en metode for å bestemme folks viktigste karaktertrekk på grunnlag av «likes» gitt på Facebook. Dette er en interessant og potensielt skremmende anvendelse av det vi kaller maskinlæring ved bruk av store mengder data. Sammen med kolleger lagde han en Facebook-app og inviterte brukere til å fylle ut et spørreskjema som skulle brukes til å fastlegge

respondentens personlighetstrekk.

Dette var en standardtest. Tre millioner samtykket og ga opplysninger. Det ble til tre millioner profiler som ble brukt i forskningen. Deretter utviklet han algoritmer som på grunnlag av personens gitte «likes», skulle fastlegge de samme personlighetstrekkene. Resultatet var forbløffende. Basert på et relativt lite antall «likes», kunne han med stor treffsikkerhet beregne samme personlighetstrekk som ble funnet ved tradisjonell analyse av spørreskjemaene. Flere «likes» ga sikrere svar. Maskinen viste seg å kunne sammenstille og fortolke informasjonen som ligger i tilsynelatende ustrukturerte sympatierklæringer (likes) langt bedre enn et menneske. Her var det forretningsmuligheter.

Kosinski gikk videre og testet om metoden kunne brukes til effektiv markedsføring der kunden får reklamen tilpasset sin personlighet. Han gjennomførte flere reklamekampanjer på Facebook, én gjaldt kosmetikk. Reklamen ble utformet på to måter, én for å slå an hos introverte og én for å slå an hos ekstroverte personer. Reklamen ble sendt til 3 millioner personer. Den virket. Mottakerne var 50% mer tilbøyelige til å kjøpe kosmetikken når den var rettet mot deres personlighetstype.

I 2014 signerte firmaet Cambridge Analytica en avtale med Aleksandr Kogan, en av Kosinskis kolleger ved Cambridge University. 270 000 amerikanere besvarte en ny undersøkelse av personlighetstrekk og politiske preferanser, mot en økonomisk kompensasjon på 2-5$. Det krevdes at respondenten tidligere hadde benyttet seg av stemmeretten og at han/hun måtte logge seg inn med sin Facebook-konto, som Kogan dermed også fikk tilgang til. Cambridge Analytica betalte. Ved å samle inn data, også om respondentenes venner, satt Cambridge Analytica med informasjon om mange millioner velgere. Facebook hevder kontrakten bare åpnet for å hente informasjon om dem som hadde samtykket og fått betalt. Kogan bestrider dette.

Alt var lagt til rette for å drive personlig rettet valgkamp for Donald Trump. Cambridge Analytica har bistått i en rekke valgkamper i flere land. Det er godt kjent at senator Tom Cruz benyttet seg av selskapet, men brøt kontakten etter at forventet fremgang uteble. Det tyder på at Kosenskis metode ikke er noe vidundermiddel som alltid gir suksess. Bare når andre forutsetninger er oppfylt, vil den gi uttelling.
Selv om metoden først og fremst har blitt omtalt fordi man søker forklaring på Trumps overraskende valgseier, kan den benyttes for mange andre formål enn å påvirke velgere. Den har vist seg effektiv til å fastlegge seksuell legning, rase, intelligens, traumer, politiske holdninger og anlegg for rusavhengighet, bare på grunnlag av «likes». Det er grunn til å være bekymret. Det er fortsatt et uavklart spørsmål om opplysninger fra Cambridge Analytica ble lagt til grunn for russiske nettverksoperasjoner, men det kan ikke utelukkes.

Presidentvalget i Frankrike 2017.
Resultatene av presidentvalget i USA og Brexit-avstemningen i Storbritannia kom svært uventet og skapte uro i innflytelsesrike miljøer. Det ble søkt etter forklaringer, og det oppsto berettiget mistanke om at Russland hadde spilt en fordekt rolle, spesielt i USA. NSA-sjef Mike Rodgers advarte mot russisk innblanding i det kommende franske presidentvalget.

Etter krisene i Ukraina var det åpenbart at Russland ønsket å svekke NATO og EU, og få opphevet de økonomiske sanksjonene mot landet.

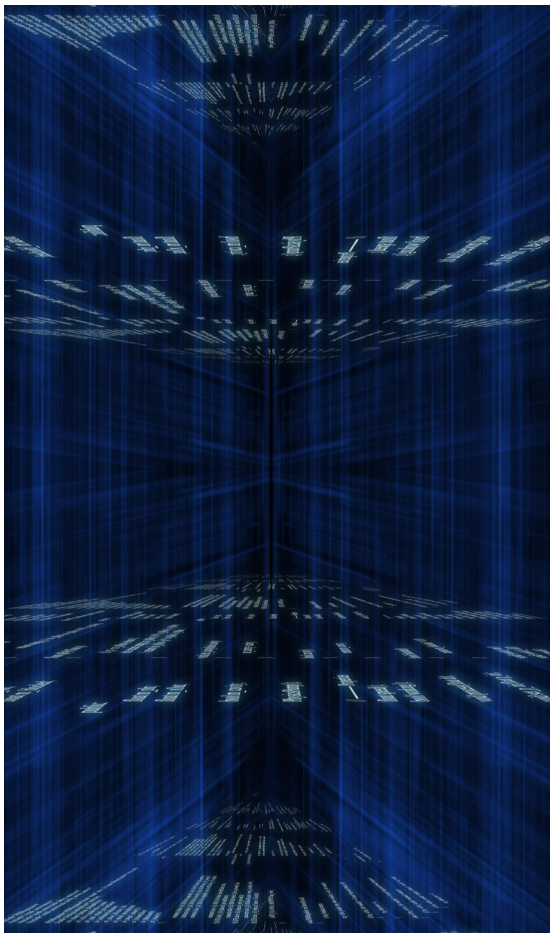
7. Risikobildet/trender

Lederen for Nasjonal Front, Marie le Pen, var sterkt kritisk til fransk innvandringspolitikk, NATO og EU. De russiske nettstedene RT og Sputnik fremstilte henne konsekvent positivt i valgkampen. Den senere valgte presidenten, Emmanuel Macron, betegnet dem som propagandaagenter for Nasjonal Front. I et møte med president Putin uttalte le Pen at hun støttet Russlands annektering av Krim og ville heve de økonomiske sanksjonene. Hun var åpenbart Putins favoritt ved presidentvalget. Etter at franske banker nektet Nasjonal front lån på grunn av rasistiske holdninger, fikk de i 2014 russiske lån til sin valgkamp. Det hersket betydelig uro for at Russland skulle prøve å påvirke valget. Det ble spekulert i flere typer fremstøt.

To dager før første valgrunde, ble titusener av e-poster fra Macrons kampanjeorganisasjon lekket. E postene ble delt på sosiale medier av WikiLeaks og av mange amerikanske aktivister. Lekkasjene fikk voldsom medieoppmerksomhet, men Macron kom godt ut av det hele. For det første avslørte ikke e-postene spesielt kritikkverdige forhold, snarere tvert i mot. De bekreftet inntrykket av at Macron hadde spilt med åpne kort i valgkampen. Riktignok hadde enkelte e-poster kompromitterende innhold, men de var åpenbart forfalskede og dessuten svært amatørmessig utført.

Valgresultatet tyder på at lekkasjen hadde liten effekt, Emmanuel Macron vant andre runde med dobbelt så mange stemmer som Marie le Pen. Det store spørsmålet er nå hvem som sto bak hackingen av e-postene.

Flashpoint, et amerikansk cybersikkerhetsselskap, konkluderte med «moderat konfidens» at Fancy Bear, en hackergruppe med kontakter til russisk militær etterretning, sto bak hackingen. Guillaume Poupard, sjef for fransk cybersikkerhet, uttalte til Associated Press at hackingen var så generisk og enkel at nesten enhver kunne utført den. Bildet er dermed fortsatt noe uklart.
Det var åpenbart at Russland støttet le Pen, og hun signaliserte støtte til Russland i viktige saker. Russland hadde derfor sterke motiver for å få henne valgt. Likevel var lekkasjen av e-poster amatørmessig og i strid med forestillingen om dyktige russiske hackere. Det var ikke foretatt noen kartlegging av store velgergrupper i Frankrike, slik teknologien bak Cambridge Analytica åpner for. De mest virkningsfulle verktøy for påvirkning var kanskje ikke tilgjengelige, men situasjonen kan være en annen ved fremtidige valg. Eller kanskje var le Pens situasjon så håpløs at Putin ikke ville vise kortene sine.



Konklusjon

Det er viktig at den nasjonale beredskapen tar hybride trusler på alvor. Samfunnsendringen og teknologiutviklingen gjør livet bedre for store folkegrupper, men de skaper også sårbarheter som kan utnyttes i en konfliktfylt verden. Fredsoptimismen fra 90-tallet er erstattet av en rekke nye og uklare konfliktlinjer. Russland har vist vilje og evne til å bruke folkerettsstridige virkemidler for å sikre sine interesser og har videreført arven fra Sovjetunionen med satsning på teknologi og naturvitenskap for politiske og militære formål. Samtidig tillater ikke økonomien like store forsvarsinvesteringer som i USA og Kina. De må være kreative, og de må være smartere politisk og teknologisk enn sine motstandere. Derfor er det viktig at vi ikke bare konsentrerer oss om de trusler som er kjente, men leter systematisk etter nye farer før vi blir eksponert for dem.

Det er åpenbart at cyberkriminalitet har kommet for å bli, fra den mest trivielle til den avanserte. Offentlig og privat virksomhet vil måtte benytte betydelige ressurser på robuste teknologiske løsninger, opplæring og organisering for å sikre sine verdier. Dette er forstått hos de ansvarlige og vil bli gjort. Når det derimot gjelder alvorlige hybride trusler mot landets selvstendighet og sikkerhet, står vi overfor ressurssterke og kreative aktører. Kreative virkemidler vil trolig ikke avsløres før det er alvor, og da er det for sent å lære. Hybridundersøkelsen avdekker behov for informasjon, veiledning og retningslinjer. Det er viktig og riktig at den nye sikkerhetsloven pålegger sikkerhetsmyndigheten å skape bedre forståelse av hva som kan ramme av sabotasje, spionasje og terrorisme.

Hvis spesialetterforsker Mueller kommer til bunns i alle mistenkelige forhold rundt presidentvalget i USA, kan det overraskende valgresultatet tre frem som tidenes mest vellykkede hybridoperasjon. E postlekkasjen mot Macron i det franske presidentvalget hadde derimot liten effekt, men det er flere forhold som skiller de to sakene. En viktig forskjell er innholdet i e-postene som ble lekket. En annen var at Cambridge Analytica hadde kartlagt holdninger og preferanser til millioner av velgere i USA, spesielt i vippestatene. Dette gjorde det mulig å tilpasse individuelt det politiske budskapet, både på nettet og i presidentkandidatens taler. Trump lyktes med dette, men Cruz fikk det ikke til.

Hva bør vi lære av dette? Grunnleggende sett bygger Cambridge Analytica på fagområdene matematikk, maskinlæring, stordata, psykologi og markedsføring. Forskningsmiljøet på Cambridge University viste at en maskin med langt større presisjon enn et menneske kan fastsette en velgers personlighet, med preferanser og antipatier, på grunnlag av spredt og tilsynelatende tilfeldig informasjon. Dette vil selvfølgelig videreutvikles for markedsføring av lovlige produkter, men i USA etterforskes fortsatt et mulig komplisert samspill mellom en fremmed makt og en valgkamporganisasjon. Dette stiller krav til tradisjonelt datasikkerhetsarbeid for å hindre at skjermingsverdig informasjon kommer på avveie, men det er ikke nok. Når falske nyheter spres for å svekke en stat, er det viktig at offisiell informasjon blir trodd, og at myndighetene har tillit, slik vi opplevde det 22. juli 2011. Derfor har vi en felles interesse av, og ansvar for, å videreutvikle det norske tillitssamfunnet, slik at vi stoler også på de politikerne vi ikke stemte på.

7. Risikobildet/trender

7.1 Hybride trusler, hva nå?

Richard Utne, Forsvaret

"The international consensus on 'hybrid warfare' is clear: no one understands it, but everyone, including NATO and the European Union, agrees it is a problem".

- Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare (CHW): Understanding Hybrid Warfare (2017).

I 2017 presenterte et norskledet multinasjonalt kapasitets- og utviklingsprosjekt rapporten Understanding Hybrid Warfare. Rapporten mener at for å løse et problem må man først forstå det, og påpeker at det ikke finnes en overordnet konsistent definisjon på begrepet hybride trusler. Innledningsvis er det derfor viktig å etablere en helhetlig tilnærming til begrepet. Hybride trusler er representert av et bredt spekter av militære, politiske, økonomiske, sivile og informasjons- instrumenter som rettes mot det sivile samfunnet og den private sektor. Tilsynelatende kan små angrep isolert sett, være synkroniserte angrep der bruk av hele spekteret av hybride trusler i sum skaper effekt som langt overstiger effekten av et konvensjonelt militært angrep. Forskning peker på at slik lav-intensitetskonflikt er den mest sannsynlige formen for fremtidig krigføring på den vestlige halvkule, der kampen i overveiende grad vil være knyttet til narrativet. Signaturen til hybride trusler er at de er utformet for å forårsake effekt, mens de samtidig holder seg under alarmterskelen til eksisterende forsvarsmekanismer. Med stor grad av troverdighet lar de seg dermed ikke knytte til en aktør, noe som også gjør det vanskelig å oppnå konsensus for kollektiv reaksjon.

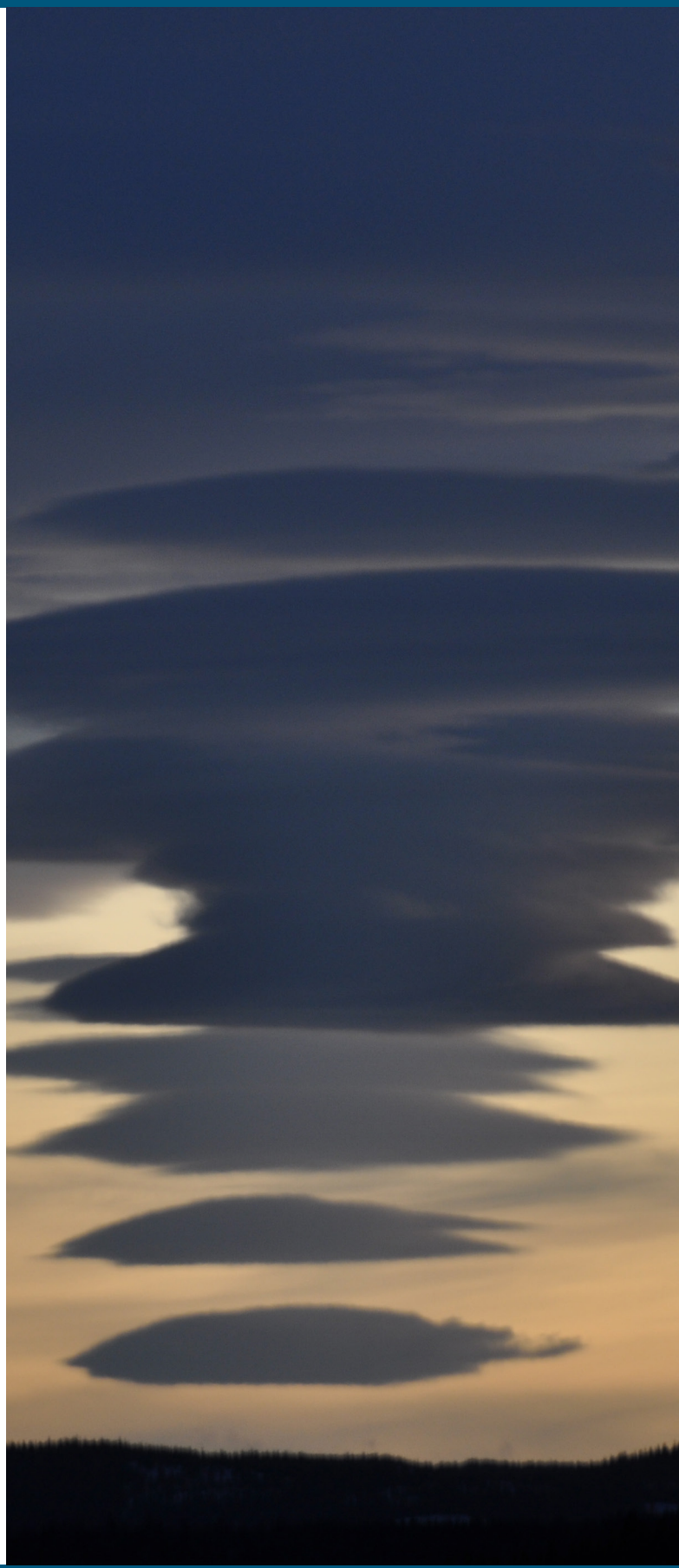
En aktør som retter hybride trusler mot norske interesser kan tenkes å ha langsiktige politiske strategier som går langt utenfor våre egne politiske tidsrammer. Dermed kan vår oppfatning av hva som er normalt gradvis forskyves og føre til at vi etterhvert etablerer en oppfattelse av en ny normaltilstand. Internasjonale sosiale nettverk med investeringer i kritisk infrastruktur oppfattes som naturlige i vår globaliserte verden. Dette er relevant for næringslivet, for totalforsvaret og for NATO, fordi ressurser og kritisk infrastruktur som er viktige komponenter for det sivile samfunnet så vel som for totalforsvaret i stor grad er eiet og drevet av privat sektor. I gjennomsnitt er mer enn 50 prosent av satellittkommunikasjon som brukes til forsvarsformål fra privat sektor og om lag 75 prosent av vertsnasjonsstøtte til NATO-operasjoner og øvelser hentet fra kommersiell infrastruktur og tjenester.

Forholdet mellom typiske operatører i næringslivet er gjensidig avhengig av at de ulike støttefunksjonene, leverandørene og forsyningssegmentene er tilstrekkelig robuste til å motstå et hybrid angrep, det være seg politisk, økonomisk eller omdømme-messig. Artikkel 3 i Atlanterhavstraktaten beskriver sivil beredskap og resiliens som grunnleggende forutsetninger for individuelt og kollektivt forsvar. Nettopp fordi hybride trusler er rettet mot sivil og privat sektor er kostnader knyttet til robusthet og resiliens et ansvar som påligger næringslivet i stedet for militær beredskap i tradisjonell forstand.

Fordi sivil og militær beredskap og krisehåndtering er gjensidig avhengig av hverandre, beskriver regjeringens strategi for totalforsvaret («Støtte og samarbeid 2018»), at løpende samarbeid er nødvendig for å utnytte samfunnets samlede ressurser best mulig og dermed bidra til god samfunnsøkonomi.

Ansvar, nærhet, likhet og samvirke er nasjonale prinsipper for samarbeid i beredskap og krisehåndtering. Men fordi det ikke finnes tilstrekkelig distribusjon av sensorer i næringslivet som kan identifisere (mulige) hybride trusler, risikerer nettopp ansvar, nærhet og likhet å hindre rapportering til et (hittil ikke-eksisterende) overordnet organ som kan sammenstille hendelser i hele spekteret av virkemidler for å identifisere og om mulig utstede en tidlig varsling om et pågående synkronisert hybrid angrep. En av våre største utfordringer knyttet til hybride trusler i dag er derfor ikke mangel på evnen til samarbeid eller barrierer og mottiltak, men at samarbeid, barrierer og mottiltak blir reaktive og ikke proaktive. Hybridundersøkelsen til Næringslivets Sikkerhetsråd er derfor et viktig bidrag til at ansvarlige myndigheter investerer i proaktive tiltak i næringslivet for støtte og samarbeid. Det er god samfunnsøkonomi og et stykke på vei mot 2%.

Richard Utne har lang og bred internasjonal erfaring i risikostyring og sikkerhetsledelse, både i privat og offentlig sektor. I 2018 var Utne prosjektleder for NATOs sivile komite Transport Group Ocean Shipping: Kinetic and Hybrid Threats to the Maritime Community in the North Atlantic Ocean and the North Sea. Denne artikkelen representerer bare Utnes egne synspunkter.



7. Risikobildet/trender

7.2 Norges Bank og hybride trusler

Carl-Axel Hagen, sikkerhetsdirektør, Norges Bank

Med et globalt trusselbilde preget av etterretning, organisert kriminalitet og terror, skal Norges Bank gjennomføre sine oppgaver med en høy grad av sikkerhet for sitt personell, sine funksjoner og sine systemer. Norges Bank forvalter en rekke kritiske funksjoner, blant annet betalingssystemet, kontantforsyningen, finansiell krisehåndtering og statens pensjonsfond utland.

Det har skjedd en endring i hvordan konflikter utspiller seg i vår tid. Det har utviklet seg en preferanse for bruk av hybride virkemidler som i større grad også rammer sivile institusjoner. Samtidig er det geopolitiske landskapet i endring som kan føre til at Norges Bank som sentralbanken i Norge ufrivillig kan oppfattes som en politisk og diplomatisk aktør. I Ukraina har man observert cyberangrep, inkludert spionasje og sabotasje, også mot finansiell sektor. I andre land har man observert påvirkningsoperasjoner mot sentralbankledelsen i sannsynlige forsøk på å svekke omdømme til finanssektoren.

Hybride trusler har som hensikt å redusere politisk handlingsrom ved å bruke forskjellige maktmidler mot svakheter og sprekker i samfunnet. Myndighetene som sitter på helhetsoversikten er de som best kan vurdere om Norge er utsatt for hybride trusler.

Norges Bank understøtter myndighetene i denne oppgaven gjennom fire konkrete tiltak. For det første har banken et etterretningsmiljø som kontinuerlig overvåker det globale trusselbildet og identifiserer hendelser som kan påvirke Norges Bank.

For det andre er det tett samhandling mellom bankens fysiske- og cybersikkerhetsmiljøer. Det gjør at Norges Bank evner å se sammenhengen i tilsiktede uønskede hendelser som skjer i det fysiske og logiske domenet.

For det tredje har sikkerhetsmiljøet i banken drevet aktiv og målrettet kunnskapsformidling om hybride trusler til toppledelsen og systemeiere av Norges Banks verdier slik at de har en forståelse for hvordan sikkerhetshendelser knyttet til bankens objekter, infrastruktur og informasjonssystemer kan ha politiske konsekvenser.

Til slutt har banken en tett dialog med myndighetene og rapporterer jevnlig på relevante sikkerhetshendelser som berører Norges Bank.

Gjennom disse fire tiltakene er Norges Bank i stand til å vurdere i hvilken grad tilsiktede uønskede hendelser kan benyttes for å ramme politisk handlefrihet og til å rapportere til relevante myndigheter.

EIGEBRET

8. Forebyggende aktiviteter/tiltak

Gode forebyggende aktiviteter og tiltak bidrar til redusert sårbarhet og reduserte konsekvenser. Vi har derfor innhentet gode råd og veiledninger fra ulike aktører.

8. Forebyggende aktiviteter/tiltak

Fem tiltak for næringslivet

Inkluder sikkerhetsrelaterte tema på jevnlige samtaler med ansatte, som tema i prosjekter og i daglig operasjon. Gjennom regelmessige samtaler med ansatte og bevisstgjøring vil man etablere en kultur med rom for å snakke om sikkerhetsrelaterte utfordringer og hendelser. Dette gir virksomheten en mulighet til å iverksette sikringstiltak proaktivt.

Regelmessige påminnelser om tiltak, samt å bruke styringssystemene effektivt til å vurdere om tiltakene tjener formålet. Gjennom jevnlig vurdering og oppfølging av iverksatte tiltak vil virksomheten ha et oppdatert bilde av egen sikkerhetsbevissthet og sikkerhetsarbeid.

Verdi- og sårbarhetsforståelse – er en grunnstein i god bedriftskultur. Hybride trusler rettes ikke nødvendigvis etter de som har mest penger i banken. Sosialt nettverk, geografisk plassering eller virksomhetens kompetanse er forhold man bør sette seg inn i for å vurdere virksomhetens verdier og sårbarhet.

Trusselforståelse – på lik linje som at virksomheter har god kjennskap til sitt marked, sektor eller bransje, bør de holde seg oppdatert på trender, aktører og hendelser som utgjør trusselbildet. PST, E-tjenesten, DSB og NSM publiserer hvert år ulike trusselvurderinger med gratis informasjon om hvilke trusler din virksomhet kan stå overfor.

Globale trender – gjennom å sette seg inn i globale trender vil man i større grad forstå det trusselbildet som hybride trusler representerer. Det er viktig å forstå at man er en brikke i et større

10. Etterord

Bidragsytere til undersøkelse og rapport, utover utvalget

Næringslivets sikkerhetsråd har flere samarbeidsprosjekter som pågår til enhver tid, men som alle omhandler sikkerhet på ulikt vis. Det gir oss bedre breddeforståelse, samt tilgang til ressurser og kunnskap som bidrar til høy kvalitet på våre produkter. I forbindelse med analyser knyttet til Mørketallsundersøkelsen 2018 ønsker vi derfor å takke følgende bidragsytere:

Birgitte Førsund – Senior Manager, KPMG
Ingunn Kolberg Vedeld– Associate, KPMG
Magdalena Agata Szwiec – Associate, KPMG
Espen Johansen – Operations & Security Manager, Visma Software International
Isabel Quiroga Arkvik – Fraud management, Nordea.
Hege Ossletten – Nestleder UNINETT Norid AS

www.nsr-org.no

Næringslivets sikkerhetsråd

Mot kriminalitet - for næringsliv og samfunn