MAKT OG TILLIT I KRISETID

FAGNOTATER 2020

UTSYN – FORUM FOR UTENRIKS OG SIKKERHET

MAKT OG TILLIT I KRISETID

Denne publikasjonen består av 3 tekster, og er en en del av et prosjekt for å løfte nye problemstillinger knyttet til makt, demokrati og tillit i lys av koronakrisen. Hensikten er å bidra til en opplyst debatt og kunnskapsbasert diskurs om samfunnssikkerhet, politiske veivalg, og krisehåndtering i ulike ledd.

I lys av det digitale skiftet velger globale aktører ulike strategier. Mens Kina har satset stort på digital infrastruktur, har vestlige teknologiselskaper vektlagt persondata. I begge tilfeller oppstår reelle dilemmaer og utfordringer med hensyn til samfunnssikkerhet og demokratiutvikling. Overordnet handler dette om teknologiens betydning for demokrati, tillit og sikkerhet.

I en krise er vi også mer sårbare for desinformasjon og påvirkningskampanjer fra aktører som har som mål å polarisere og destabilisere. Vanlige borgeres kunnskap og motstandskraft mot desinformasjon som florerer er derfor viktig.

For å styrke ordskiftet og ytringskjulturen på disse spørsmålene er det viktig å bringe inn faglig baserte analyser og vurderinger. Det er også avgjørende for å styrke beslutningsgrunnlaget for norske beslutningstakere på potensielt svært sensitive og polariserte spørsmål. Denne publikasjonen er et bidrag til dette.

Prosjektet er støttet av Fritt Ord.

Publisert: Juni 2020.

FRITT ORD

UTSYN – FORUM FOR UTENRIKS OG SIKKERHET

Stortorvet 3, 0155 Oslo

post@prosjektutsyn.no | www.prosjektutsyn.no

INNHOLD

HVORDAN KAN MAKTFORHOLD PÅVIRKE SAMFUNNSSIKKERHET I KRISETID?

RICHARD UTNE

Samfunnssikkerhet handler om vår kollektive evne til å verne oss mot og håndtere hendelser som truer grunnleggende verdier og funksjoner – og som setter liv og helse i fare. Hvordan påvirker så koronakrisen samfunnssikkerheten vår?

I løpet av svært kort tid har pandemien ført til betydelig inngripen i borgernes liv og handlefrihet, unntakstilstand i politikken med endringer av de parlamentariske spillereglene, og dramatisk nedgang i økonomien. Samtidig som milliarder i kompensasjoner bevilges for at samfunnet skal normaliseres, opplever et stort antall mennesker høy grad av usikkerhet. Dette fagnotatet belyser hvordan samfunnssikkerhet er et dynamisk begrep og at samfunnssikkerheten kan påvirkes av forholdet mellom makt og tillit i krisetid.

SAMFUNNSSIKKERHETSBEGREPET OG UTVIKLING I NORGE

Begrepet *samfunnssikkerhet* handler om vår kollektive evne til å verne oss mot og håndtere hendelser som truer grunnleggende verdier og funksjoner – og som setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil, eller bevisste handlinger. Begrepet sikkerhet er sentralt som forklaring på atferd og motivasjon for menneskets søken etter trygghet. Sikkerhet er den mest grunnleggende verdien av de menneskelige behov etter fysiske behov, og defineres ofte som fravær av fare (Kaufman, 2013), eller som opplevelse av trygghet, stabilitet og forutsigbarhet (Maslow, 1943).

Direktoratet for samfunnssikkerhet og beredskap (DSB) beskriver samfunnets kritiske funksjoner som funksjoner samfunnet ikke kan klare seg uten i syv døgn eller kortere, uten at dette truer befolkningens sikkerhet og/eller trygghet. Disse samfunnssfunksjonene, mener DSB, ivaretar grunnleggende verdier og kan derfor betraktes som «grunnpilarer for samfunnets robusthet». Grunnpilarene er delt i tre overordnede kategorier som igjen består av totalt 14 underkategorier vi kjenner som samfunnets kritiske funksjoner.

Kategorien styringsevne og suverenitet inneholder de grunnleggende ramme-betingelsene for at andre samfunnsfunksjoner skal kunne ivaretas. Kontroll over norsk territorium er en forutsetning for myndighetene til å ivareta *befolkningens sikkerhet og trygghet*, opprettholde normal styring og møte kriser med nødvendige ressurser. Samfunnssikkerhet handler derfor også om vern om demokratiet. I kategorien styringsevne og suverenitet ligger ivaretakelse av Norges politiske system, opprettholdelse av nasjonal beredskap og Forsvarets oppgaver i forebyggende sikkerhet med overvåkning, etterretning og evne til avskrekking. Dette krever politisk tillit til de som

Kilde: DSB, Samfunnets kritiske funksjoner (2016).

skal forvalte makten; Stortinget, regjeringen og domstolene.

En viktig faktor som bidro til å forme begrepet *samfunnssikkerhet* var uforutsigbarheten som oppstod etter Berlinmurens fall. I 1993 beskrev langtidsplanen for det sivile beredskap at trusselbegrepet, som tradisjonelt hadde omfattet Forsvarets vurdering av Norges sikkerhetspolitiske situasjon i forhold til definerte motstandere, var for snevert grunnlag for videre dimensjonering av en sivil beredskap som skulle planlegge og utføre innsats ved kriser og katastrofer i fred (St.meld. nr. 48). Et knapt tiår senere fant Sårbarhetsutvalget at Norge var sårbart for endringer som kunne påvirke teknologisk og samfunnsmessig utvikling. Utvalget introduserte begrepet *samfunnssikkerhet* for å samordne sikkerheten i samfunnet (NOU 2000:24, «Et sårbart samfunn»). Siden den gang har begrepet blitt utfordret både i form av hvordan det skal forstås og om hvem det angår.

Tradisjonelt har sikkerhetsstyring knyttet til samfunnssikkerhet vært hendelsesbasert, og ikke risikoorientert. Forskjellen er vesentlig: Hendelsesbasert sikkerhetsstyring er reaktiv. Med dette menes at forebyggende tiltak iverksettes etter at en uønsket hendelse har inntruffet. Risikobasert sikkerhetsstyring er proaktiv og handler om å identifisere uønskede hendelser og iverksette forebyggende og konsekvensreduserende tiltak *før* hendelsene oppstår. Men eksempler viser at investeringsviljen i vern mot uønskede hendelser har basert seg på hendelser i fortid og at investeringsviljen er proporsjonal med grad av kollektiv utrygghet.

Siden slutten på den kalde krigen har hvert tiår blitt definert av innsats mot uønskede hendelser etter at de har skjedd. Den kalde krigens sikkerhetspolitiske trussel som tidligere hadde påvirket allmenn risikopersepsjon, ble erstattet av frykt for endringer i klima. Samfunnet var kanskje allerede oppmerksom på endringer i klimaet, men flommen i 1995 gjorde oss oppmerksomme på det moderne samfunnets sårbarhet mot naturhendelser som følge av klimaendringene. Senere ble Forsvaret reorganisert til mer internasjonal innsats i kampen mot terror. Etter hvert som støvet fra tvillingtårnene la seg ble det jakt på ensomme ulver og innsats mot skoleskyting. Tradisjonelt hadde antiterror i bred forstand vært en politioppgave frem til terroren 22. juli, men blomsterkasser på Karl Johan i Oslo og evakueringsøvelser på skoler inkluderte nå også allmenn ansvarliggjøring. Russlands intervensjon i Ukraina revitaliserte den transatlantiske alliansen, totalforsvaret og det sivile samfunnets rolle i kampen mot såkalte *hybride trusler*.

Hva kan være årsaken til at samfunnssikkerheten i Norge i stor grad har vært hendelsesbasert?

Moderne risikostyring utfordrer den etablerte oppfatningen av sammenheng mellom uønskede hendelser og historiske data. *Risiko* handler om fremtidige konsekvenser av en aktivitet og usikkerhet knyttet til hva konsekvensen kan bli. Ved dimensjonering av forebyggende beredskap bør vi derfor ikke legge for stor vekt på historiske data. Vi kan simpelthen ikke benytte historiske data utelukkende til å predikere fremtiden, fordi fremtidige hendelser vil alltid ha et nytt element av sårbarhet knyttet til for eksempel ny teknologi. Begrepet risiko er ofte assosiert med trusler, men kan også bety muligheter. Når vi foretar en investering eller når vi velger å gjøre noe, så tar vi risiko. Vi ønsker å oppnå en gevinst på en eller annen måte. I risikostyring vil dette si å balansere motsetningsforholdet mellom å utforske muligheter og unngå tap. En utfordring er at risiko tilhører fremtiden og ikke kan beskrives med et objektivt tall. Prognoser må derfor sees i sammenheng med at tilgjengelig kunnskap og forutsetning for beslutning alltid vil ha en tilhørende grad av usikkerhet, og som kan påvirkes av oppfatninger.

Risikopersepsjon er knyttet til et *narrativ*, som er en oppfatning (tro, vurdering), som holdes av et individ, gruppe eller et samfunn om risiko. Et narrativ er den logiske strukturen for å formidle en historie eller en fortelling i en eller annen form, eller som når skikkelsen Erasmus Montanus i Ludvig Holbergs (1684-1754) «Jeppe på bjerget» viser oss at risikopersepsjon kan påvirkes av falske slutninger. I moderne krigføring foregår kampen om narrativet i stor grad i det digitale domenet. Et eksempel er ofte referert til som «trollfabrikker», nært assosiert med begrepet *hybrid krigføring*, og som benyttes som del av en strategi for å påvirke opinion og oppfatning (som i forkant av et valg) gjennom for eksempel å plante falske nyheter i sosiale medier eller i nyhetskilder.

Så, hva med tillit?

MAKT, TILLIT OG SAMFUNNSSIKKERHET I KRISETID

Norge er et tillitssamfunn. Transaksjonskostnaden ved maktoverføring i demokratiet er basert på valutaen tillit. I samfunnsøkonomi vil valutakurs påvirke tilbud, etterspørsel og produksjonskostnader. Et eksempel er Norges Banks pengepolitikk som i dag er rettet mot stabilitet i kronens verdi mot utenlandsk valuta, definert som euro. Krisesituasjoner og trusler langt borte kan påvirke valutaen for oss her hjemme og skape usikkerhet knyttet til lønnsomhet i fremtidige investeringer. I samfunnsøkonomi er det en grunnregel at nåverdien må være positiv for at en investering skal være lønnsom. Men hva skjer med investeringsviljen når valutaen svekkes og fremtiden er uforutsigbar?

I et demokrati er det viktig at vi har tillit til de som er delegert makt til å investere i trygghet. Alle kan ikke være eksperter, vi må ha tillit til at ekspertise og drøftinger ligger til grunn for beslutninger. Like viktig for tilliten er det å ha et åpent samfunn som tillater å stille spørsmål ved forutsetningene som ligger til grunn for vurderingene. Sosiologen Max Weber (1864-1920) definerte makt som «enhver sjanse til å gjennomføre sin vilje innenfor en sosial relasjon, også på tross av motstand, uansett hva denne sjansen beror på». I vår fredelige avkrok av verden virker definisjonen kanskje mer fjern, enn hva den nasjonen hele forsvarskonseptet til Norge, og NATO for den saks skyld, legger til grunn.

Maktrelasjoner kan være både formelle og uformelle, og bundet av psykologiske kontrakter. Bilateralt kan makt sees som et virkemiddel for å oppnå tillit gjennom for eksempel nødhjelp, som et virkemiddel gjennom misbruk av tillit ved oppkjøp av eiendom i et tredjeland («we come in peace»), eller ved å påvirke balansen mellom tilbud og etterspørsel. Det er for eksempel naivt å tro at Russland slutter å eksportere korn fordi de behøver det selv.

Professor Harald Grimen (1955-2011) pekte på tre mulige faktorer som påvirker balansen mellom makt og tillit; tvang til lojalitet, aksept av legitimitet, og tro på effektivitet. I Norge er tillit en grunnleggende forutsetning for styringsevne og suverenitet. Vi har en parlamentarisk styringsform som reguleres av forholdet mellom makt og tillit, det vil si at en regjering sitter så lenge flertallet på Stortinget tillater det. Forutsetningen er basert på tillit – eller mistillit, om du vil. Styrken på tillit kan variere med grad av og grunnlaget for opplevd legitimitet, og kan dermed styres av faktorer som påvirker vår risikopersepsjon.

Nettopp med bakgrunn i en gryende legitimitetskrise i vestlige demokratier, bestilte regjeringen i 2019 en rapport fra Institutt for samfunnsforskning. Hensikten var å kartlegge politisk tillit i Norge, og i slutten av april 2020 forelå den første av to rapporter med en analyse av ulike samfunnsgruppers tillit til lokaldemokratiet. Politisk tillit er ifølge rapporten et sammensatt fenomen som ikke lar seg forklare av én enkeltfaktor. Velgernes tillit til politiske institusjoner og aktører ansees som et resultat av deres vurdering knyttet til politikkens virkemåte og organisering (Hausgjerd og Segaard, 2020). Rapporten viser at innbyggerne i Norge har høy tillit til politikere og politiske institusjoner sammenliknet med andre land, men at tilliten har sunket de siste årene. Tilliten er også til en viss grad skjevt sosialt fordelt. Arbeidsledige og de som mottar trygdeytelser har systematisk lavere tillit til politikere enn resten av befolkningen, og de som ikke stemmer ved valg har også lavere tillit til lokaldemokratiet enn de som stemmer ved valg.

Studier av risikopersepsjon viser at det lett oppstår uoverensstemmelser mellom vanlige menneskers vurdering av risiko på den ene siden, og vitenskapelig tilnærming til risiko på den andre. Den subjektive oppfatningen av risiko, hva mennesker er tilbøyelig til å betrakte som trygt eller utrygt, kan variere mye. Mange oppfatter nye, ukjente stoffer og teknologier, som for eksempel en ny vaksine, som farlig. En kontrollert aktivitet som for eksempel å kjøre bil kan oppleves som tryggere enn en du selv ikke kan påvirke, som det å sitte i fly. Dersom vi knytter vurderinger til noe som har verdi for oss kan en akseptabel risiko for en person være en uakseptabel risiko for en annen. En årsak kan være at individer ofte trekkes mot en bias kalt «risikopersepsjon», som knytter vurderingen til følelser som for eksempel handler om ting som kan ramme oss personlig og som har personlig verdi for oss, eller frykt for endring.

Den tyske sosiologen Ulrich Beck (1944-2015) beskriver risikosamfunnet som frykt for endringer som følge av teknologisk eller samfunnsmessig utvikling. I det moderne samfunnet er det mennesket som driver frem endringer gjennom vitenskapelig og teknologisk utvikling, men frykter samtidig konsekvensene av endringene de selv skaper. Risikosamfunnet er dermed ikke knyttet til teknologi i «hardware» forstand, men må forstås som et uttrykk for sosial medvirkning til utvikling av metoder for å løse problemstillinger. En forutsetning for et bærekraftig teknologisk samfunn er at motivasjonen, eller investeringsviljen, ligger i den dominerende gruppen av befolkningen. En befolkningsgruppe som er konsentrert rundt behov for sikkerhet vil dermed kunne tenkes å ha en mer samlet motivasjon og investeringsvilje for trygghet, enn dersom alle grunnleggende behov var dekket, selv om opplevelsen av utrygghet viser seg å være basert på gale forutsetninger.

I beskrivelsen av samfunnets kritiske funksjoner viser DSB også til suverenitetshevdelse som en grunnleggende rammebetingelse for at andre samfunnsfunksjoner skal ivaretas: «Norske myndigheter må ha kontroll over norsk territorium for å kunne ivareta befolkningens sikkerhet og trygghet, samt ha evne til å opprettholde normal styring og til å møte ekstraordinære situasjoner med nødvendige ressurser.» I tillegg til konstitusjonelle organers ivaretakelse av styring og kriseledelse, har Forsvaret en utøvende rolle. I dette ligger overvåkning og etterretning, forebyggende sikkerhet og militær respons.

Covid-19 aktualiserer et betent tema i den nye sikkerhetsloven som sier at myndighetene blant annet kan samle metadata om IKT-trafikk til og fra virksomheter knyttet til det nasjonale varslingssystemet for digital infrastruktur. Under Covid-19 har det vært en betydelig økning av falske nyheter i sosiale media. Eksempler er alt fra råd om inntak av medikamenter som kan ha en rekke uheldige bivirkninger, til teorier om at stråling fra 5G-nettet er årsaken til pandemien. Lavintensive konflikter, eller hybrid krigføring, er ofte forbundet med begrenset maktbruk mellom grupperinger eller såkalte «failed states», ofte dominert av irregulære kinetiske virkemidler. Men Forsvarets forskningsinstitutt (FFI) mener at oppfatningen om den klassiske asymmetriske krigen ikke gjelder for det fremtidige trusselbildet i Vesten. Våre politiske, økonomiske og sosiale betingelser er divergerende fra regioner vi tradisjonelt har assosiert til begrepet, og en lavintensiv konflikt i Vesten vil sannsynligvis domineres av kampen om narrativet, snarere enn av små grønne menn (Diesen, 2018). FFI mener et dominerende virkemiddel i slik krigføring er påvirkningsoperasjoner rettet mot privat sektor, og at dette allerede er utbredt. Sanntidsrapportering og spredning av informasjon når «en enorm mengde strategiske tilhørere, som spesielt i vestlige samfunn består av alle de enkeltindivider og grupper som i kraft av enten personlig posisjon eller organisatorisk styrke har mulighet for å påvirke politiske beslutninger» (Diesen, 2018).

I forbindelse med Covid-19 snakker vi om en normalisering av et samfunn der en stor befolkningsgruppe opplever, eller kan komme til å oppleve, usikkerhet. Hva skjer med deg når alt går tilbake til normalen, men du ikke har noen normal hverdag å gå tilbake til? Ufrivillig tap av forutsetninger for trygghet skaper økte forskjeller i samfunnet. Vestlige land står nå foran en historisk høy arbeidsledighet. Opplevd utrygghet kan skape krav om proteksjonisme, føre til mindre samarbeid og splittelse i etablerte felleskap. Dette kan føre til at stabiliteten i vår politiske tillitsvaluta kan bli påvirket målt mot utenlandsk valuta. Samfunn med vesentlig sosial skjevfordeling gjenspeiler ofte lavere grad av politisk tillit enn land der dekningsgraden av befolkningens og samfunnets grunnleggende behov er jevnt fordelt. Der en stat feiler å ivareta slik fordeling kan mistillit til myndighetene bli resultatet. Bare se til USA.

Den engelske psykologen Marie Jahoda beskriver konsekvenser av arbeidsledighet som en av de største sosiale utfordringer. Kostnaden både for enkeltindividet og samfunnet er svært høy, ikke bare økonomisk men også knyttet til følelsen av forutsigbarhet for trygghet og følelse av en meningsfull tilværelse. Den høye arbeidsledigheten som fulgte depresjonen i 1930-årene la grunnlaget for oppslutning om krefter verden siden har markert seieren over. Det er ikke det samme som å si at det samme kan skje igjen, men bør minne oss på at koronaviruset kan føre til konsekvenser som ikke knyttes til samfunnssikkerhetsbegrepet i tradisjonell forstand.

Vern mot uønskede hendelser krever ofte spesialisering innenfor gitte fagfelt, men vi behøver også spesialister som kan se ting i sammenheng og lage en overordnet *risikoorientert* situasjonsforståelse. Ikke minst, det er nødvendig å forstå at begrepet samfunnssikkerhet ikke kan beskrives statisk, men at det må sees i sammenheng med utviklingen i sårbarhetsbildet. Akkurat som suverenitetshevdelse i alle domener, er tiltak mot høy arbeidsledighet og utenforskap en viktig innsatsfaktor for ivaretakelse av samfunnets grunnleggende funksjoner – og må tas på alvor.

Motivasjonen og investeringsviljen i trygghet er proporsjonal med usikkerhet knyttet til våre grunnleggende verdier, og det er i en krise vi kjenner på verdiene i særlig grad. For å skape trygghet må vi ha tillit til at gevinsten er verdt innsatsen. Verdien av tillit lar seg ikke tallfeste. Det gjør for eksempel heller ikke frihet, men vi er villige til å betale mye for den.

KILDER/ANBEFALING TIL ANDRE TEKSTER OM TEMAET

- Diesen, Sverre (2018): *Lavintensivt hybridangrep på Norge i en fremtidig konflikt*. FFI rapport 18/00080.
- Direktoratet for samfunnssikkerhet og beredskap (2016): *Samfunnets kritiske funksjoner*.
- Grimen, Harald (2001): *Tillit og makt – tre samanhengar*. Tidsskrift for Den norske legeforening 2001:121, 3617–9.
- Hausgjerd, Atle & Segaard, Signe (2020): *Politisk tillit, lokaldemokrati og legitimitet*. Institutt for samfunnsforskning. Rapport 2020:6.
- Jahoda, Marie (1982): *Employment and Unemployment: A Social-Psychological Analysis*. Cambridge University.
- Kaufmann, Mareile (2013): *Emergent self-organization in emergencies: resilience rationales in interconnected societies*. Resilience: International Policies, Practices and Discourses 1:1, 53-68.
- Maslow, Abraham H. (1943): *A theory of human motivation*. Psychological Review 50(4), 370–396.

OM FORFATTEREN

Richard Utne har bred internasjonal erfaring i risikostyring og sikkerhetsledelse, både i privat og offentlig sektor. Han har lang tjenesteerfaring fra Forsvaret og har deltatt som rådgiver i flere internasjonale operasjoner. Utne har en master i risikostyring og sikkerhetsledelse fra Universitetet i Stavanger (UiS), med fordypning i sikkerhetsledelse i konfliktområder.

ET DIGITALISERT SAMFUNN OG ET UOVERSIKTLIG TRUSSELBILDE

SIMEN BAKKE

Digitaliseringen stiller staten og samfunnet ovenfor mer utfordrende problemstillinger enn i det tradisjonelle, fysiske domenet. Spesielt gjør dette seg gjeldende på grunn av internettets grenseløse kompleksitet, og det faktum at flere av våre tjenester, også samfunnskritiske funksjoner, kan rammes av cyberangrep. Trusselaktørene er flere og de kan enklere utføre trusselrettet aktivitet og cyberangrep, uten at staten nødvendigvis er i posisjon til å nøytralisere og inkapasiterer motstanderen. Geografiske og juridiske grenser som forhindrer trusselaktivitet i det fysiske rom, er i mindre grad tilgjengelig i det digitale domenet.

Av denne årsak, må sikkerhetsarbeidet i det digitale rom også organiseres annerledes enn i det fysiske domenet. Teknologien gir oss mulighet til å bedrive masseovervåkning i en helt annen skala enn tidligere i historien, men må i demokratiske rettsstater samtidig utføres på måter som ivaretar grunnleggende menneskerettigheter. Derfor bør det forebyggende IKT-sikkerhetsarbeidet i det digitale rom, prioriteres høyere. På denne måten forhindrer beskyttelsestiltakene en trusselaktør å ramme våre samfunnskritiske funksjoner, samtidig som demokratiske verdier og rettsstatsprinsipper opprettholdes. Også i den digitale tidsalder.

INNLEDNING

Trusler og beskyttelsestiltak i det 21. århundre, skiller seg vesentlig fra tidligere historiske epoker. Det er naturligvis også flere fellesnevnere med tidligere historiske perioder. Likevel er det noen sentrale særegenheter knyttet til den globale digitale infrastrukturen, som i dag utfordrer oss på helt nye måter. Den økende digitaliseringen og økt datatrafikk over internett, muliggjør aktivitet, trusler og angrep av en helt annen skala sammenliknet med tilsvarende aktivitet i det fysiske domenet. Det er flere årsaker til utviklingen, men noen viktige hovedtrekk må her trekkes frem:

1. Digitaliseringen medfører sentrale verdier og kritiske innsatsfaktorer, koblet til internett.
2. Internett forholder seg i liten grad til fysiske skillelinjer og geografiske avstander.
3. Internett er et lite regulert domene, og rettshåndhevende myndigheter har liten kontroll.
4. Aktivitet og angrep skalérer, slik at trusselaktører kan angripe flere mål samtidig.
5. Muligheten for å avdekke illegitim aktivitet forutsetter tilstrekkelig deteksjonskapasitet.

De nevnte punktene er særdeles sentrale for cyberrelatert aktivitet. I tillegg til cyberaktivitet, kommer tradisjonell trusselaktivitet begått i det fysiske domenet. Der *bruken* av tjenester, og i særdeleshet kommunikasjonstjenester – benytter internett som infrastruktur. Sistnevnte skiller seg fra rene cybertrusler og såkalte nettverksangrep, med at det eksempelvis kan være personer med tilknytning til terrorgrupper, organiserte kriminelle eller statlige etterretningsorganisasjoner som opererer i «den virkelige verden», i tillegg til i cyberverdenen. Selv om noen av de ovenfornevnte punktene bidrar til at aktivitet fra trusselaktører er mer utfordrende å detektere og håndtere, er det også elementer i cyberverdenen som gjør det enklere for en kompetent aktør å beskytte seg. Dette skyldes blant annet at dataene som sendes over infrastrukturen, er verifiserbare og i mange tilfeller også etterprøvbare. Det legges igjen *digitale spor* fra aktiviteten, så lenge det er satt opp funksjoner i IKT-sikkerhetsregimet som loggfører denne aktiviteten. Unormal aktivitet i nettverket kan detekteres ved bruk av anomalideteksjon (mønstergjenkjenning) basert på maskinlæring og kunstig intelligens. Dermed kan automatisert varsling om pågående nettverksoperasjoner finne sted. Hendelsen kan varsles uten behov for, eller med et minimum av, menneskelig innblanding. På denne måten er det også mulig å etablere automatiserte beskyttelsesmekanismer på et helt annet nivå i det digitale domenet, sammenliknet med tradisjonelt sikkerhets- og beredskapsarbeid i den fysiske verden.

Kombinasjonen mellom trusler i det fysiske og det digitale domenet, hvor angrep kan utføres av enkeltindivider, kriminelle aktører, terrorgrupper og selv statlige aktører – der det ikke nødvendigvis er tydelig hvem som står bak aktiviteten, utfordrer norske myndigheters organisering. Sektorprinsippet i Norge, i kombinasjon med de fire prinsippene for samfunnsikkerhet- og beredskap; ansvar, nærhet, likhet og samvirke, tilsier at den aktøren som forvalter ansvaret i det daglige, også skal håndtere en krise mest mulig likt når en slik hendelse inntreffer.**1** Dette er imidlertid et utgangspunkt. Behovet for samvirke for å respondere på cyberhendelser og hybride trusler, utfordrer imidlertid de andre prinsippene. I særdeleshet gjelder dette nærhetsprinsippet som *kan* fremstå som uhensiktsmessig i tilfeller hvor *sentralisert* beskyttelse og respons kan være bedre egnet mot cybertrusler. Dette er likevel en balansegang, der også lokale tiltak må iverksettes.

De senere årene har utviklingen medført et behov for å tenke annerledes, og spesielt rundt *gråsoneaktivitet* og såkalte *hybride trusler*. Skillet mellom fred, krise og krig er ikke like tydelig i dagens digitale trusselbilde, sammenliknet med hva det er ved eksempelvis konvensjonell krigføring ved bruk av kinetisk militærmakt og tradisjonelle militære styrker.**2** Dette utydelige skillet mellom fred, krise og krig, blir desto mer utfordrende når man ikke er sikker på hvilken aktør som står bak eksempelvis et cyberangrep. Er det unggutter bosatt i Norge, internasjonale kriminelle aktører som er betalt for å utføre en tjeneste på vegne av andre, eller er det en statlig aktør som står bak? Dette utydelige bildet gjør det utfordrende for myndighetene å respondere adekvat på aktivitet i cyberdomenet. Dermed fremkommer gråsoneproblematikken tydeligere i det digitale domenet.

CYBERANGREP OG HYBRIDE TRUSLER

Vi har flere eksempler på hendelser i Norge, hvor cyberaktivitet har rammet sentrale samfunnsinstitusjoner. Operasjonene mot Helse Sør-Øst og Hydro, hvor store mengder personopplysninger fra førstnevnte kom på avveie**3** og sistnevntes datasystemer ble stengt ned på grunn av skadelig kode,**4** er blant to av de mer kjente eksemplene. I nyere tid, har vi også eksempelet på investeringsfondet Norfund som ble rammet av det som tilsynelatende kan fremstå som en phishing-kampanje, hvor fondet ble lurt til å overføre 100 millioner kroner til feil kontonummer.**5** Dette kan fremstå som

tradisjonell, internasjonal kriminalitet. På en annen side ville man ikke nødvendigvis vært klar over det dersom en statlig aktør stod bak. I eksempelet med Helse Sør-Øst, konkluderte PSTs etterforskning med at det var sannsynlig at en statlig aktør stod bak, uten at de hadde tilstrekkelig med spor til å ettergå aktiviteten for å identifisere trusselaktøren.**6** Det er i dette kompliserte og utydelige bildet, myndigheter med ansvar for cybersikkerhet nå skal operere.

Etterretningstjenesten og PSTs trussel-vurderinger for 2020, trekker Russland og Kina frem som aktører hvilket bedriver stor grad av spionasje, samt kartlegging- og cyberaktivitet mot Norge, norske virksomheter, politiske institusjoner, myndighetsapparat og annen sentral infrastruktur. Iran nevnes også spesifikt av tjenestene. Situasjonen beskrives av Etterretningstjenesten som en periode med stormaktsrivalisering hvor det pågår et våpenkappløp, der makt nå går fremfor internasjonal rett.**7** Cyberaktivitet, trusler og angrep foregår utelukkende i det digitale domenet. *Hybrid krigføring*, er derimot en betegnelse for bruk av ulike virkemidler, både i det fysiske og i det digitale domenet.

Erklæring av *krigsskueplass* er noe som hører forrige århundre til. Starten av det 21. århundret kan sies å være preget av en mer kontinuerlig strøm med ulike former for trusselrelatert aktivitet. Det mest kjente eksempelet når det gjelder hybrid krigføring i nyere tid, finner vi Øst-Ukraina. Hendelsen omtales ofte som en «game changer» innen området, og påvirket forholdet mellom EU, NATO og Russland vesentlig. I konflikten som frem til nå har tatt rundt 13 000 liv fra begynnelsen av 2014, har russisk-støttede separatister brukt en rekke ulike virkemidler for å destabilisere regionen. Væpnede, uorganiserte soldater, spesialstyrker kamuflert som separatister, cyberangrep mot kritisk infrastruktur som strømforsyning og banker, utpressing av militære offiserer, samt desinformasjonskampanjer mot befolkningen, var blant de mange virkemidlene som ble brukt.**8**

For ukrainske myndigheter var dette naturligvis en utfordrende situasjon å besvare. Dette var ingen tradisjonell krig ved bruk av konvensjonelle militære maktmidler. Det var heller ikke en situasjon som kunne løses av det sivile maktapparatet. Gråsoneproblematikken gjorde seg gjeldende. Selv om det i ettertid viste seg å være en operasjon som var sentralstyrt fra Moskva, var det i den innledende fasen stor usikkerhet om hva slags aktør Ukraina her stod overfor. Konflikten om Krim-halvøya har riktignok en lang og betent historie mellom Ukraina og Russland. Et tilsvarende scenario kan være relevant også i andre deler av Europa med historisk tilknytning til den tidligere Sovjetunionen.

Samtidig vil det kunne være nærliggende å tenke seg at tilsvarende problematikk kunne funnet sted i andre landområder som grenser mot Russland. Herunder tidligere Sovjet-stater, de baltiske landene og selv vårt eget fylke Finnmark. Landområder med større deler russisk-tilknyttet befolkning, vil således kunne være mer sårbare for slik aktivitet. Hendelsen i Øst-Ukraina er en konkret situasjon som har utspilt seg i Europa i nyere tid – og som i stor grad har skapt presedens for hvordan trusselbildet i Europa skal forstås. Hva som er det reelle trusselbildet som vestlige stater står overfor, er en vesentlig større og bredere diskusjon som ikke skal utdypes nærmere her.

VERDIORIENTERT OG TRUSSELORIENTERT TILNÆRMING TIL IKT-SIKKERHET

Kombinasjonen av et mer uoversiktlig og utfordrende trusselbilde, mer kompetente og potente trusselaktører i det digitale domenet, økt grad av digitalisering i det norske samfunnet, flere sentrale verdier og tjenester koblet til internett – gjør oss sårbare for angrep. En trusselaktør som ønsker å ramme det norske samfunnet på negative måter trenger ikke bevege seg med stridsvogner, kampfly og

infanteritropper over landegrensene, men kan ved bruk av mer kostnadsbesparende metoder i cyberdomenet tilegne seg kontroll over datasystemer. I beste fall avdekkes disse forsøkene på datainnbrudd. I verste fall oppdages de ikke, og kritiske funksjoner som vann- og avløpssystemer, bankers betalingssystemer, nødetatenes meldingssystemer og liknende kritiske systemer, blir påvirket. I ytterste konsekvens blir de sabotert. Dette er en utvikling som bør tas på stort alvor, hvor det finnes flere ulike tilnærminger for å beskytte samfunnet mot cyberaktivitet og -angrep.

De fleste virksomheter benytter en *verdiorientert* tilnærming til sikkerhetsarbeidet. En slik tilnærming finner vi blant annet i Nasjonal Sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet.**9** Grunnprinsippene har til hensikt å sørge for at norske IKT-systemer er tilstrekkelig sikret. Hensikten med grunnprinsippene er at alle de viktigste tiltakene for å *redusere sårbarheter* i IKT-systemene, implementeres. Slike tiltak gjør det mer utfordrende for en trusselaktør å tilegne seg innpass i datasystemer til offentlige og private virksomheter. Sannsynligheten reduseres for at informasjon eller andre sensitive verdier kommer på avveie, blir endret eller utilgjengeliggjøres. Sikringstiltakene ligger fysisk og logisk nært de verdiene som skal beskyttes. Trusselaktøren må forsere en rekke tekniske, logiske og organisatoriske barrierer for å oppnå urettmessig tilgang til datasystemet. En slik tilnærming har få negative sider for samfunnet i stort – foruten at de enkelte tiltakene kan være økonomisk kostnadsdrivende. Likevel er det slik at mange av de viktigste tiltakene, vil medføre liten eller ingen kostnad. Oppdatert programvare, kryptering av datatrafikk, streng tilgangsstyring og kontroll med leverandører, for å nevne noen spesifikke tiltak.

En slik tilnærming som den beskrevne ovenfor, *beskytter* mot aktivitet, trusler og angrep fra uvedkommende, enten de er statlige, organiserte kriminelle eller enkeltindivider. Metodene og kapasitetene til de nevnte aktørene vil selvsagt variere. Likevel vil det være slik at beskyttelsestiltak mot en type aktør, også i stor grad vil beskytte mot nettverksaktivitet og inntrengningsforsøk fra andre aktører. Svært mange av de vellykkede spionasje- og sabotasjeoperasjonene som utføres mot datasystemer, skyldes dårlige rutiner for IKT-sikkerhet i virksomheten. Til tross for at mange av de sårbarhetsreduserende sikringstiltakene er tilgjengelige, billige og svært nyttige – er det ikke uvanlig at et vellykket inntrengningsforsøk skyldes at en virksomhet har forsømt sine oppdateringsrutiner.

En annen tilnærming til sikkerhetsarbeidet, er en *trusselorientert* tilnærming. Ofte er det ønskelig med en kombinasjon av begge disse to tilnærmingene i sikkerhetsarbeidet. For å benytte et lett tilgjengelig eksempel, bedriver politiet i stor grad med sikkerhetsarbeid ved en trusselorientert tilnærming i det fysiske domenet, innenfor norsk jurisdiksjon. Politiet avdekker lovbrudd, etterforsker saken, legger den frem for domstolen – og trusselaktøren (i dette tilfellet lovbryteren), inkapasiteres ved domfellelse. Trusselaktøren er satt ut av spill for å foreta nye lovbrudd. Den individualpreventive effekten sikres igjennom fengselsoppholdet og den allmennpreventive effekten sikres igjennom at handlingen, eksempelvis datainnbrudd, er belagt med straff. Enkelt forklart kan man si at kun et fåtall vil utføre innbrudd, ettersom risikoen for å bli tatt og dermed straffeforfulgt i liten grad veier opp for det potensielle utbyttet. I cyberdomenet er derimot saken nokså annerledes.

Trusselaktørene som tidligere nevnt, består blant annet av statlige aktører og organiserte kriminelle som befinner seg på geografiske områder utenfor norsk jurisdiksjon. Mange av disse også i land som norske myndigheter ikke har et sikkerhetspolitisk samarbeid, og utleveringsavtaler, med. Blant annet Russland, Kina og Iran, som nevnt i Etterretningstjenestens og PSTs trusselvurderinger. Dette betyr at norske myndigheter ikke kan straffeforfølge trusselaktørene for lovbrudd som begås i cyberdomenet. Selv om norske myndigheter

avdekker at en av de nevnte statlige aktørene, eller aktører som igjen er tilknyttet de statlige aktørene (for eksempel hackergrupper) står bak, er det lite de kan foreta seg for å nøytralisere eller inkapasitere trusselen. Det er fremdeles i den enkelte virksomhets IKT-system at responstiltakene må iverksettes, for å forhindre aktøren i å operere.

Når den fremmede aktøren oppdages, er det ofte for sent. Informasjon kan allerede være kompromittert. Virksomheten som har blitt rammet, trenger ikke engang vite at datainnbruddet har vært et faktum. Dersom sabotasje utføres, for eksempel ved bruk av kryptovirus som «låser» maskinene i nettverket, vil *konsekvensene* for virksomheten bli tydelige – selv om de ikke oppdaget det forutgående inntrengningsforsøket. Sistnevnte kan komme i noe så enkelt som et vedlegg i en e-post eller ved at en ansatt i virksomheten klikket på en ukjent lenke, som igjen eksekverte skadelig kode. Så enkelt er det altså i dag å utføre digitale angrep, dersom ikke beskyttelsestiltakene er tilstrekkelige. De ansatte er ofte en av de viktigere beskyttelsesmekanismene i en virksomhets IKT-sikkerhetsregime. Til tross for at det ofte fokuseres mye på tekniske og fysiske sikringstiltak, kan det være nok at en ansatt ikke klarer å skille mellom en korrekt og en falsk nettside for pålogging til virksomhetens tjenester. Slike forsøk på *phishing* for å hente ut innloggingsinformasjon, er en enkel form for sosial manipulasjon som benyttes med svært stor suksessrate.

TOTALFORSVAR OG STYRKET NASJONALT SAMARBEID

Totalforsvaret er et konsept som var godt kjent under den kalde krigens dager. I tiden etter Berlinmurens fall og Sovjetunionens kollaps, har det i lengre tid vært en periode med stabilitet for Norges del hva gjelder sikkerhetspolitiske forhold.**10** Dette bildet har imidlertid endret seg, og det har oppstått en ny «kald front» mellom flere NATO-land på den ene siden, og Russland og Kina på den andre. Dette har medført et behov for å revitalisere totalforsvarskonseptet. Norske myndigheter har brukt vesentlig tid og ressurser på revitaliseringen de senere årene. Blant annet som vertskap for NATO-øvelsene Trident Javelin (2017), og Trident Juncture (2018). Under øvelsene deltok de fleste offentlige aktører med nasjonalt beredskapsansvar, i tillegg til en rekke sentrale private aktører.**11**

Totalforsvaret kan i Norge langt på vei sies å ha styrket båndene mellom de sivile og de militære aktørene. I tillegg har det kommet på plass en *bistandsinstruks* mellom Forsvaret og Politiet som gjør det tydeligere når, hvordan og på hvilke kriterier etatene kan utnytte hverandres ressurser.**12** I tillegg til videreutviklingen av totalforsvarskonseptet, eksisterer det både et Felles kontraterrorsenter (FKTS) og et Felles cyberkoordineringssenter (FKCS). I de nevnte sentre, deltar både sivile og militære aktører. Etterretningstjenesten, PST, NSM og KRIPOS, er blant deltakerne.**13** I tillegg har NSM opprettet et Nasjonalt cybersikkerhetssenter (NCSC), og det eksisterer en rekke computer emergency response teams (CERT), tilhørende ulike sektorer som helse, justis, finans med flere. Samarbeidet, informasjonsutvekslingen og hendelseshåndteringen mellom aktørene, er styrket.

Enkelte av aktørene, har en *offensiv trusselorientert* tilnærming. Dette er i særdeleshet Etterretningstjenesten, PST og Politiet. De nevnte aktørene skal innhente informasjon, analysere og utarbeide etterretningsrapporter og trusselvurderinger. PST og Politiet skal med påtalemyndigheten i spissen også etterforske og straffeforfølge lovbrudd.**14** Den nevnte virksomheten utføres for å avdekke trusselaktører, og for å iverksette mottiltak. Aktører som NSM og de nevnte CERT-ene, har i større grad en *defensiv verdiorientert* tilnærming. Disse aktørene skal bidra til at virksomhetene iverksetter tilstrekkelige sikringstiltak, slik at beskyttelsesmekanismer er implementert og sårbarheter blir redusert.**15** Arbeidet utføres for at en trusselaktør ikke skal kunne lykkes med

sine angrep, dersom de forsøker seg på datainnbrudd, nettverksoperasjoner eller annen cyberaktivetet.

Skillet mellom de offensive trusselorienterte aktørene, og de defensive verdiorienterte aktørene, er viktig. Spesielt gjelder dette i situasjoner hvor straffeforfølging kan være aktuelt, noe som kun er Politiet (og PST) med påtalemyndigheten i spissen sine oppgaver. Dette er en virksomhet som er langt mer lovregulert sammenliknet med andre former for informasjonsinnhenting, hvor rettsstatens maktfordelingsprinsipp forankret i Grunnloven står sentralt. Samtidig er det slik i cyberdomenet at både aktørene som står bak og hvilket land de oppholder seg i, er mer utydelig og komplisert sammenliknet med i det fysiske domenet. Dette utfordrer statens myndighet, med Politiet og PST i spissen, fordi påtalemyndighetene i liten grad kan straffeforfølge personer som befinner seg i land Norge ikke har et sikkerhetspolitisk samarbeid med. Denne utviklingen er blant annet noe av årsaken til at både FKTS og FKCS har blitt opprettet, da samarbeid med Etterretnings-tjenesten er nødvendig.

Selv om samarbeidet mellom aktørene er styrket, har de likevel ulike ansvarsområder og mandater. Dette gjør at informasjon mellom aktørene ikke kan deles ukritisk. Eksempelvis er Etterretningstjenestens mandat å innhente informasjon og utarbeide trusselvurderinger om fremmede stater, organisasjoner og individer.**16** Oppdraget til E-tjenesten er altså ikke rettet mot norske borgere. PST derimot, skal forebygge og etterforske ulovlig etterretningsvirksomhet, spredning av masseødeleggelsesvåpen, sabotasje og politisk motivert vold eller tvang på norsk jord.**17** Dette oppdraget retter seg både mot norske borgere, og borgere fra annen stat som befinner seg i Norge. Det tradisjonelle Politiet, skal primært etterforske lovbrudd begått på norsk jord, uavhengig av borgerens statstilknytning.**18** NSM er norske myndigheters fagorgan for forebyggende sikkerhet, og skal gi informasjon, råd og veiledning til offentlige og private virksomheter om forebyggende sikkerhet.**19** Til tross for de svært ulike mandatene og enkelte skranker for informasjonsdeling, er trenden de senere årene likevel at samarbeidet må være sterkt for at aktørene i fellesskap skal kunne beskytte staten, norske virksomheter og norske interesser.

VEIEN VIDERE – HVORDAN SKAL VI SIKRE OSS I DET DIGITALE LANDSKAPET?

Til tross for at trusselbildet i det digitale domenet kan oppleves som uoversiktelig og komplisert, er det samtidig viktig å erkjenne at det ikke finnes noen enkel løsning eller en quick-fix. Skal man klare å sikre samfunnet på en god måte, må man innledningsvis erkjenne at truslene i det digitale domenet *er* flere, de *kan* enklere angripe, de *kan* være vanskeligere oppdage og det *kan* være vanskeligere å ettergå angrepene. Etter at dette er erkjent, må aktørene som har ansvar for å sikre staten, samfunnet og næringslivets IKT-systemer mot trusselaktivitet og angrep – prioritere IKT-sikkerhet i bred forstand. Dette innebærer at fysisk sikring av IKT-systemer, personellsikkerhet og hvem som har tilgang til IKT-systemer, kontroll på leverandører og underleverandører av utstyr til IKT-systemer, må være kartlagt og kontrollert. Og det må i tillegg benyttes systemer for automatisert avdekking, varsling, respons og håndtering av unormal aktivitet i datasystemer – som kan komme fra trusselaktører. På denne måten kan den verdiorienterte forebyggende tilnærmingen, sikre både samfunnskritiske funksjoner og enkeltindividers personopplysninger. Dette uten å komme i konflikt med demokratiske prinsipper.

I disse dager er den nye loven for Etterretningstjenesten under stortingsbehandling med et konsept for «tilrettelagt innhenting». Det nevnte konseptet har til hensikt å beskytte staten og norske interesser mot trusler utenfra, ved masseinnsamling og -lagring av metadata som krysser den norske grensen i fiberkabler.**20** Utfordringen med lovforslaget er imidlertid at denne tilnærmingen også vil innhente og lagre

kommunikasjon fra og til norske borgere. Dette oppstår fordi datatrafikken i sin natur i dag er global. Således vil store deler av norske borgeres kommunikasjon med hverandre, transporteres via servere i utlandet. Lovforslaget vil dermed bidra til å endre det norske samfunnets tilnærming til og forståelse av kommunikasjonsfrihet. Frem til i dag har dette prinsippet handlet om fravær av statlig inngrep i borgernes kommunikasjon, med mindre borgeren er underlagt en konkret mistanke for å ha begått en handling som Stortinget har belagt med straff. Altså et lovbrudd. Innsamlingen fra nordmenn vil være en *utilsiktet* konsekvens av lovforslaget, som fra Etterretningstjenestens ståsted handler om å samle inn data om borgere tilknyttet fremmede stater. Hvor stor andel av norske borgeres datatrafikk som vil samles inn, er foreløpig ukjent og vil avhenge av filtreringsteknologien.

Forsvarsdepartementet som har utarbeidet lovforslaget, har lagt inn rettsstatlige mekanismer som domstolskontroll før søk i dataene og forbud mot bruk av dataene i tilknytning til straffesaker (med unntak av de mest alvorlige lovbruddene). Likevel representerer lovforslaget et inngrep i borgernes frihetssfære, som er mer drastisk enn noe annet lovforslag siden EUs Datalagringsdirektiv. Sistnevnte ble vedtatt innført i norsk rett av Stortinget i 2011, men ble i 2014 stanset av EU-domstolen ettersom inngrepet i borgernes privatliv ble betraktet som uforholdsmessig av domstolen.**21** I etterkant av dette, fikk imidlertid politiet i 2016 tilgang på metoden «dataavlesning», som er et mer målrettet virkemiddel for å tilegne seg informasjon fra datasystemer til personer som mistenkes for alvorlige lovbrudd.**22**

Det er viktig å huske på at trusseletterretning er et *virkemiddel* for å bidra til å skape sikkerhet. Sikkerhet, som består av et mangfold ulike virkemidler (noen av dem omtalt i dette fagnotatet), er nødvendig for å opprettholde demokratiet og rettsstaten. De to sistnevnte er imidlertid styringsformer som bør betraktes som *mål* i seg selv. Dette er fordi de kan anses som forutsetninger for at mennesker i vår del av verden skal kunne leve gode liv, på den måten de selv ønsker. Demokrati og rettsstat sikrer individene tilstrekkelig grad av både frihet og selvbestemmelse. Derfor må man være ytterst forsiktig med virkemidler som skal skape sikkerhet, men som samtidig kan undergrave demokratiske verdier.

En tilnærming som i mindre grad har vært diskutert, men som i større grad bør vurderes – er hvorvidt det er hensiktsmessig og mulig å skille infrastruktur som næringsliv, stat og borgere benytter for datakommunikasjon, fra hverandre. I dag går store deler av internett-trafikken over den samme digitale infrastrukturen. Dette gjør at trusselaktører, enten de er kriminelle grupperinger eller statlige aktører, potensielt kan få tilgang til det meste av våre verdier i det digitale domenet – over den samme digitale infrastrukturen. En konsekvens av dagens tilstand er at det er vanskeligere å sikre *samfunnsfunksjoner* og *kritisk infrastruktur* mot angrep fra trusselaktører, samtidig som vi forsøker å ivareta grunnleggende borgerrettigheter og friheter over den samme digitale infrastrukturen. Med strengere sikkerhetskrav og større grad av overvåkning utelukkende rettet mot digital infrastruktur som stat og næringsliv benytter seg av, desto mindre ville behovet vært for konsepter som «tilrettelagt innhenting». I møte med samfunnets stadig økende overvåkning, kan en slik tilnærming fungere mer målrettet, den kan tilby bedre sikkerhet og den er i større grad forenlig med demokratiske verdier.

En sentral utfordring med dagens tilnærming for å beskytte både samfunnet og staten mot cybertrusler og -angrep, er at det ofte argumenteres for at det pågår en kontinuerlig «kamp» mellom stater i cyberdomenet. Logikken fra et sikkerhetsperspektiv, vil dermed være at også sikkerhetstiltak må samsvare med det trusselbildet som den pågående «kampen» representerer. Dette gjør at aktørene som definerer trusselbildet, også dermed definerer

hva som de-facto *er* den reelle situasjonen «der ute». Jo mer alvorlig trusselbildet i cyberdomenet beskrives, desto lengre vil aktører tilknyttet forsvar og sikkerhet ofte hevde at staten må strekke seg for å møte trusselbildet. Dersom man ikke er tydelig på hvor langt denne grensen skal kunne gå i en demokratisk rettsstat, er det en fare for at vi faller for logikken om at man som minimum må ha tilsvarende kapasiteter som mer autoritære stater. Dermed risikerer vi at sistnevnte setter premissene for demokratiske staters maktbruk. I så tilfelle kan vi gå en farlig tid i møte. Spesielt gjelder dette i overvåkningsteknologiens tidsalder, hvor sanntidssporing og analyse av all tilgjengelig datatrafikk – i teorien vil være mulig.

Når det gjelder aktivitet, trusler og angrep i cyberdomenet fra statlige aktører, må disse motvirkes også i andre diplomatiske og politiske kanaler. Ettersom de statlige aktørene vanligvis besitter vesentlig mer ressurser og kompetanse til å gjennomføre avansert angrep sammenliknet med andre aktører, er det desto viktigere å sørge for gode relasjoner med fremmede stater. Overnasjonale reguleringer og lovverk som sørger for at cyberdomenet ikke blir et anarkistisk fristed, hvor det til syvende og sist er de sterkeste statene som hevder sin rett – er også viktig å få på plass. Dette må samtidig utføres på en måte hvor de mange private plattformaktørene som i dag har vesentlig innflytelse i cyberdomenet, for eksempel Facebook, Twitter og Google, også involveres. Propaganda og desinformasjon i sosiale medier representerer en vesentlig utfordring for demokratiske stater, men kan kun bekjempes på lag med plattformeierne. Statlige sikkerhets- og overvåkningstiltak vil ha minimal effekt dersom plattformeierne hvor budskapene spres, ikke er delaktige i slike samarbeid.

Dersom vi ser noen år frem i tid, vil vi antakeligvis ha en annerledes tilnærming til sikkerhet i det digitale cyberdomenet, sammenliknet med i dag. Behovet for å ha større kontroll på den digitale infrastrukturen, hvor datatrafikk i større grad separeres basert på staten og samfunnets beskyttelsesbehov – bør presse seg frem. Det faktum at det meste av vår infrastruktur i dag er tilkoblet internett, og fordi tjenestene våre i dag eksponeres for det komplekse trusselbildet der ute – gjør at vi må tenke nytt om sikring av IKT-systemer. Behovet for større grad av enhetlige krav og føringer fra statlige og politiske myndigheter, som bidrar til at sikkerhets- og beskyttelsesbehov går fremfor andre hensyn som for eksempel frihandel og markedsliberalisme, må vurderes. På denne måten vil det være mulig å sikre IKT-systemene til stat og næringsliv i tillegg til kritisk infrastruktur, samtidig som våre demokratiske verdier og frihetsidealer opprettholdes. De immaterielle demokratiske verdiene har ikke nødvendigvis en økonomisk prislapp, men er likevel avgjørende for videreutviklingen av våre frie samfunn. De immaterielle verdiene må derfor også tas med i dette sikkerhetsregnskapet.

Vi er i dag kun i starten av overvåkningens tidsalder. Konsekvensene av tilnærmingen vi i dag velger, vil sette varige spor de neste tiårene. La oss derfor foreta noen grundig gjennomtenkte og kloke valg.

FOTNOTER

1. St. Meld. 10. (2017). *Risiko i et trygt samfunn*, s. 20.
2. NUPI. (2016). *Hybrid krigføring – hva er det?*
3. NRK. (2019). *Dataangrepet mot helse Sør-Øst*.
4. NRK. (2019). *Slik fungerer løsepengeviruset som rammet Hydro*.
5. NRK. (2020). *Politiet på bar bakke i Norfund-saken*.
6. PST. (2018). *PST innstiller etterforskingen av datainnbruddet i Helse Sør-Øst RHF og Sykehuspartner*.
7. Etterretningstjenesten. (2020). *Fokus 2020*, s. 9.
8. NSR. (2018). *Hybridundersøkelsen*.
9. NSM. (2019). *Grunnprinsipper for IKT-sikkerhet*.
10. Store Norske Leksikon. (2020). *Totalforsvaret*.
11. NATO, JWC. (2018). *Trident Juncture 2018 Command Post Exercise*.
12. Regjeringen. (2017). *Har fastsatt ny instruks for Forsvarets bistand til politiet*.
13. Regjeringen. (2018). *Oppfølgingen etter 22. juli: De viktigste tiltakene*.
14. Forskrift om ordningen av påtalemyndigheten. (1986). *Påtaleinstruksen*.
15. NSM. (2019). *Nasjonalt cybersikkerhetssenter*.
16. Lov om Etterretningstjenesten. (1998). *Etterretningstjenesteloven*.
17. Lov om Politiet. (1995). *Politiloven*.
18. Lov om Politiet. (1995). *Politiloven*.
19. NSM. (2014). *Om NSM*.
20. St. Prop. 80L (2019 – 2020). *Lov om Etterretningstjenesten (etterretningstjenesteloven)*.
21. EU. (2020). *Data Retention Directive*.
22. Regjeringen. (2016). *Nye regler om dataavlesing trer i kraft*.

OM FORFATTEREN

Simen Bakke har bakgrunn fra Forsvaret, Politiet og Røde Kors på både operativt og strategisk nivå. I dag er han ansatt hos Politiets IKT-tjenester. Bakke har politiutdanning og en mastergrad i risikostyring og sikkerhetsledelse fra Universitetet i Stavanger (UiS).

PERSONVERN VERSUS STATSSIKKERHET: ER BALANSEN RIKTIG FOR Å IVARETA BEGGE OMRÅDENE?

BIRGITTE FØRSUND

INNLEDNING

Vi har i skrivende stund delvis lagt bak oss den verste globale pandemien i nyere tid. En krise som har rammet både i form av sykdom, død og et enormt press på helsevesenet. I tillegg har det også medført en kraftig negativ påvirkning på økonomi, arbeidsledighet og samfunnet generelt. De virksomhetene innen både offentlig og privat sektor som har holdt det gående gjennom hele krisen, har utvidet og digitalisert verdikjedene eksempelvis via økt bruk av hjemmekontor. Så en krise betyr også muligheter for de som vil bygge og skape mer og nytt, basert på erfaringene som ble gjort underveis i pandemien. Men det er også de med ondsinnede hensikter som ser muligheter via en krise til å agere, påvirke og splitte et samfunn som er under sterkt press.

Allerede før pandemien sto Norge og våre allierte overfor endringer i det sikkerhetspolitiske landskapet. Trender som stormaktrivalisering, nasjonalisme og proteksjonisme har gitt negative konsekvenser for samarbeid og allianser – og økt usikkerhet nasjonalt og internasjonalt. De sikkerhetspolitiske endringene i kombinasjon med digitalisering av vårt samfunn under stress, press og pandemiens prøvelser, har derfor medført en økt sårbarhet innen både stats- og samfunnssikkerhet som vi bør være oppmerksom på.

De siste hendelser knyttet til politivold, demonstrasjoner, opptøyer og hard retorikk via media og digitalt, har gitt USA en ny krise i pandemikrisen. De aktører og land som tjener på å splitte USA innenfra, antas å bidra aktivt til ytterligere polarisering, påvirkning og splittelse, spesielt via det digitale rom. Maktmidlene som vi før knyttet til krig, er flyttet til det digitale rom med mål, regi og gjennomføringsevne som minner om krigføring. En motstander eller fiende kan via en aktiv etterretningstjeneste forsterke, påvirke og muliggjøre en tilstedeværelse og maktutøvelse i USAs gater som vi aldri før har opplevd, uten geografiske hindringer. Dette muliggjøres via digitaliseringen. De digitale verdikjedene og arenaene er der vår tids krigføring utkjempes.

OM ETTERRETNINGSTRUSSELEN

Etterretningstrusselen er nærmest som en evigvarende pandemi. En usynlig trussel for de fleste av oss og derfor vanskelig å forholde seg til. Ved koronapandemiens utbrudd, var vi alle enige om trusselbildet og tiltak. Den samme konsensus har vi ikke når det gjelder etterretningstrusselen i det digitale rom.

Dette fordi etterretningstrusselen blir omtalt ulikt av myndigheter, Stortinget og politikere, samt at de heller ikke er enige om en definisjon på eksempelvis *hybride trusler* – eller har etablert en felles og samlende situasjons-/trusselforståelse. I tillegg er det enda ikke enighet om hvilke verktøy vår etterretning skal ha i det digitale rom, knyttet til et såkalt digitalt grenseforsvar.

Etterretningstrusselen blir påpekt i alle de åpne trusselvurderingene fra våre hemmelige tjenester som PST, NSM og E-tjenesten, men dessverre blir ikke disse trusselvurderingene lest av mange nok. Spesielt ikke av næringslivet som til tross for at de står for 90% av den digitale infrastrukturen i Norge, ikke har en samlende

CERT (Computer Emergency Response Team) slik som eksempelvis helse-, kraft- og kommunesektoren.

Utfordringen er derfor at vi ikke har en samlende og felles situasjonsforståelse om trusselbildet, noe som gjør forebygging, hendelseshåndtering og rapportering vanskeligere. Det gir ringvirkninger som igjen gjør at vi ikke har et godt nok dokumentert overordnet bilde av trusselsituasjonen. Et eksempel er rapportering fra næringslivet til ansvarlige myndigheter om de opplever noe uregelmessig som de ønsker å rapportere, fordi de vet ikke alltid hva de skal være observante på. Dette er vi avhengige av for å fatte beslutninger knyttet til sikkerhet, også med hensyn til internasjonalt sikkerhetssamarbeid hvor vi er forpliktet til å bidra via våre allianser.

KONSEKVENSER AV ET STERKT PERSONVERN VERSUS STATSSIKKERHET

Informasjon om trusselaktører er de hemmelige tjenestenes viktigste arbeidsredskap. Men som Datatilsynet påpeker kan innsamlingsmetodene samtidig være og oppleves som negative, knyttet til befolkningens krav og forventninger om fravær av overvåkning og et sterkt personvern.

Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger. Dette sikres gjennom blant annet lover og regler som eksempelvis menneskerettigheter og personvernforordningen.

Sikkerhetspolitikkens hovedmål er å ivareta Norges suverenitet, territorielle integritet, demokratiske styresett og politiske handlefrihet. Dette sikres gjennom et bredt sett av politiske, militære, folkerettslige, diplomatiske og økonomiske virkemidler.

Men, kan samspillet mellom personvern og statssikkerhet bli bedre balansert i henhold til det trusselbildet vi faktisk må forholde oss til? Kan nettopp vår tolkning av et sterkt personvern muliggjøre enda mer ufrivillig kontroll, overvåkning og inngripen i våre liv fra *andre* krefter vi ikke har kontroll på og som ikke vil oss godt? Hvilket handlingsrom gir vi våre hemmelige tjenester når de ikke møter fienden i det digitale rom med samme verktøy?

Et digitalt grenseforsvar er nødvendig for Norges evne til å kartlegge, varsle og motvirke alvorlige trusler, både i fredstid og i sikkerhetspolitiske krisesituasjoner. En risikobasert tilnærming er proaktiv og fokuserer på å identifisere uønskede hendelser og iverksette forebyggende og konsekvensreduserende tiltak før hendelser oppstår. Tradisjonelt har vi i stor grad basert oss på hendelsesbasert tilnærming til sikkerhet. Sistnevnte vil i så fall i vår digitale tid være en gavepakke til motkrefter som vil skade landet, infrastrukturen og befolkningen vår. Sikkerhet i dag er ikke statisk og krever en proaktiv tilnærming for å sikre vår suverenitet på alle måter. Et personvern må derfor også sees i denne sammenheng – og hvilke konsekvenser det gir for sikkerheten samlet sett om vi styrer nasjonens sikkerhet med størst vekting av personvernprinsippet.

Slik Norges sikkerhet står i dag uten et digitalt grenseforsvar – så kan i prinsippet kritiske samfunnsfunksjoner være under cyberangrep lenge, uten at vi vet det.

VÅRT INTERNASJONALE ANSVAR INNEN SIKKERHET

Norge har også et ansvar om å bidra til forebygging og økt sikkerhet via våre internasjonale samarbeidsavtaler og allianser. Norsk utenrikspolitisk institutt (NUPI) fremmer et viktig poeng med tanke på det internasjonale aspektet og ansvaret Norge har: *Å basere nasjonal sikkerhet på andre lands velvilje vil være direkte uansvarlig. I tillegg kan et bevisst valg om ikke å styrke nasjonal etterretning på feltet digital kommunikasjon sende et uheldig signal om at Norge tar lett på slik sikkerhet. Norge kan i verste*

fall bli et svakt ledd i det vestlige sikkerhetssamarbeidet (sitat Karsten Friis, forsker ved NUPI i en kronikk i DN, 4. februar 2019).

Norge er et av de få landene i NATO, EU og EØS-samarbeidet, som ikke har digitalt grenseforsvar. Som NUPI fremhever, så sender det også et signal om hvordan Norge forvalter og prioriterer sikkerhet. Dette har betydning for våre internasjonale relasjoner, gjennomslag og ikke minst tilliten vi er avhengig av via internasjonale samarbeidsprosjekter fremover.

ÅPENHET OG KONTROLL AV DIGITALT GRENSEFORSVAR

Kontroll av etterretningen har vi en sterk forankring for i vårt land og med tilhørende kontrollmekanismer på ulike nivå i henhold til det å bevare tillit og sikre åpenhet (som EOS-utvalget og Høyesterett). Vi har også kultur for åpenhet og det å stille spørsmål. Vi bør derfor også kunne stille spørsmål og belyse bedre hva som er konsekvensene av at vår etterretning ikke har samme verktøy i det digitale rom som motpartene, og hva det medfører for vår nasjons sikkerhet i dag og fremover.

Balansen mellom personvern og statssikkerhet bør korrigeres slik at vi møter truslene med riktig verktøy og kontroll. Å sitte alene i en båt med personvernflagget til topps verken redder eller sikrer vårt lands suverenitet eller borgernes personvern. Det svekker også den internasjonale tilliten til oss i de sikkerhetssamarbeid og allianser vi har forpliktet oss til.

Internett brukes av oss alle, uavhengig av landegrenser, og er dermed et sted for alle med gode og onde hensikter. Nettet brukes ikke bare til underholdning, media og andre tjenester vi setter pris på. Nettet brukes også til etterretning, sabotasje for å ødelegge, påvirkning for å skape splid, endre holdninger, fremprovosere handlinger, og til kommunikasjon og samarbeid mellom internasjonale terrorister for å rekruttere, koordinere, finansiere og planlegge terrorhandlinger. Et digitalt grenseforsvar gir E-tjenesten tilgang til å utføre målrettede søk i dette «digitale rom».

Som NUPI fremhever må det antas at norsk digital kommunikasjon allerede er samlet opp av andre lands etterretningstjenester, primært i Sverige og Storbritannia, og av kommersielle aktører som driver systemene. Spørsmålet er altså ikke om vår digitale kommunikasjon skal kunne samles opp eller ikke. Det blir den allerede.

Som det fremkommer via høringer, så vil ikke E-tjenesten overvåke norske borgeres kommunikasjon. Det inkluderer pasient- og helseopplysninger, kommunikasjon mellom journalister og kilder, eller mellom advokater og klienter. Digitalt grenseforsvar vil derimot kunne gi Norge et verktøy i det digitale rom som gir oss mulighet til å forebygge, håndtere og sikre verdier og rettigheter som nasjonen og borgere er avhengig av i et velfungerende demokrati.

Et digitalt grenseforsvar kan bidra til å sikre eksempelvis norsk næringsliv og ansatte, som er en forutsetning for både totalforsvarskonseptet og NATOs kollektive forsvarsprinsipp. I en digitalisert tid med nye trusler i konstant endring som kan ramme oss alle, bør ikke personvern alene være det dominerende sikkerhetsaspekt vi styrer etter og med det gi alvorlige konsekvenser for det å ivareta kollektiv sikkerhet og vår suverenitet.

Som påpekt av regjeringen så er norsk utenlandsetterretning en grunnstein for Norges forsvar og sikkerhet. Ved å styrke vår etterretningsevne vil forslag til ny lov bidra til å beskytte landet vårt og rettighetene vi setter så høyt. Det inkluderer også personvernet.

KILDER

- Regjeringen (2020): *Nei, E-tjenesten får ikke tilgang til all digital kommunikasjon mellom norske borgere*.
- Regjeringen (2020): *Foreslår ny lov om Etterretningstjenesten.*
- Regjeringen (2020): *Prop. 80 L (2019–2020) Lov om Etterretningstjenesten (etterretningstjenesteloven).*
- NUPI (2019): *Digitalt grenseforsvar: Å gjøre ingenting er uansvarlig*.
- Regjeringen (2017): *Vi trenger et digitalt grenseforsvar.*

OM FORFATTEREN

Birgitte Førsund har de siste 20 årene jobbet som bindeledd mellom sikkerhetsmiljøer og marked/media/ledelse via flere offentlige/private prosjekter med fokus på forebyggende digital sikkerhet. Siden 2019 har hun vært Director of Communications and Alliances for Junglemap, med fokus på bevisstgjørende og forebyggende tiltak for bedre digital sikkerhet. Første prosjekt ble samarbeidet mellom NSR, PST og Junglemap om å tilby næringslivet et gratis introduksjonskurs om digital sikkerhet.

MAKT OG TILLIT I KRISETID

PROSJEKT UTSYN – FORUM FOR UTENRIKS OG SIKKERHET

Stortorvet 3, 0155 Oslo

post@prosjektutsyn.no | www.prosjektutsyn.no