Næringslivets sikkerhets-råd

Oslo, 2. november 2020

Stortingets justiskomite

Næringslivets Sikkerhetsråds høringsinnspill Meld.St.27 Politimeldingen – et politi for fremtiden

Innledning
Næringslivets Sikkerhetsråd (NSR) viser til ovennevnte melding. Våre innspill har til hensikt å gjøre politiet best mulig i stand til å møte kriminalitetsutviklingen for å beskytte både samfunn og næringsliv, i det tiårsperspektiv meldingen omfatter.

Næringslivets Sikkerhetsråd skal legge til rette for effektivt og tillitsfullt samarbeid på tvers av sektorer og bransjer. Formålet med virksomheten er å gjøre næringslivet best mulig rustet til å kartlegge, forebygge og bekjempe moderne kriminalitet sammen med politiet og andre myndigheter. I en verden preget av kompleksitet, ustabilitet, tvetydighet og usikkerhet[1] er egen evne til å forebygge kriminalitet et stadig viktigere, og gjennomgående tema.

Forebygging starter hos den enkelte, og bygger på god situasjonsbevissthet, helhetlige verdivurderinger, et oppdatert trusselbilde, kunnskap om egne sårbarheter, og planer for å beskytte disse. Myndighetene bidrar med viktige innspill knyttet til situasjonsbildet og trussel aktørene. Først og fremst gjennom sine årlige trusselvurderinger, men også i økende grad gjennom daglig kontakt mellom næringslivet og politiets næringslivskontakter.

Næringslivskontakt ordningen er mottatt meget positivt, og vil om den får utvikle seg både regionalt og sentralt, være et svært godt redskap i det forbyggende arbeid. Næringslivet får kjennskap og kunnskap om politiet, og omvendt. Slik heves kvaliteten i det forebyggende arbeidet gjennom en nærhet som styrker virksomhetsforståelsen og øker innsikten i hverandres utfordringer.

Næringslivets Sikkerhetsråd vil derfor takke for de prioriteringer som er foretatt for å få på plass denne ordningen. Dette er et meget godt utgangspunkt for fortsatt utvikling av samarbeidet, både i et privat-offentlig og et totalforsvars perspektiv. Gjennom godt samarbeid styrkes samvirkeevnen, og vi utnytter alle tilgjengelige ressurser til det beste for mennesker, næringsliv og samfunn.

Grunnlaget
St.Meld. 27 er en invitasjon til fortsatt styrking av politiet. Styrkingen vil skje etter fire prioriteter. Det er styrking sett i lys av kriminalitetsutviklingen, nåsituasjonen i politiet og utvikling av beredskapsevnen etter 22. juli 2011 angrepene, arbeidet med å gjennomføre nærpolitireformen og politiets fremtidige kompetansebehov.

Næringslivets Sikkerhetsråd gjennomfører regelmessig undersøkelser knyttet til kriminalitet i og mot næringslivet. Grunnlaget for dette høringsinnspillet er blant annet hentet fra Kriminalitets- og sikkerhetsundersøkelsen i Norge i 2019 (KRISINO 2019), Hybride trusler og hendelser mot norsk

[1] VUCA = volatility, uncertainty, complexity, ambiguity se Harvard Business Review https://hbr.org/2014/01/what-vuca-really-means-for-you

næringsliv i 2019 (Hybridundersøkelsen 2019) og Mørketallsundersøkelsen 2020.

Mørketallsundersøkelsen 2020 er den 12. undersøkelsen om den digitale sikkerhetstilstanden i norsk næringsliv og noen offentlige virksomheter. Undersøkelsen ble i år også utvidet til å beskrive digital sikkerhet under den innledende delen av Covid-19 pandemien.

Hybride eller sammensatte trusler er en betegnelse på en fremgangsmåte der en trusselaktør bruker flere ulike virkemidler for å oppnå sine mål eller hensikter. Metodene varierer og påvirkningsoperasjoner, digitale angrep, spionasje, desinformasjon, sosial manipulering, og undergraving står sentralt. Målet med Hybridundersøkelsen 2019 var å kartlegge utbredelsen av hybride trusler mot næringslivet.

Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO) har siden 2006 vært et viktig bidrag til kunnskap om kriminalitet og sikkerhet i næringslivet for næringsliv og myndigheter. Undersøkelsen gir alene og sammen med de ovennevnte undersøkelser et godt bilde at kriminalitetsutfordringer som rammer næringslivet.

NSR har ikke et grunnlag for å kommentere politiets gjennomføring av nærpolitireformen og utvikling av beredskapsevnen etter 22. juli angrepene, og vil derfor ikke kommentere disse punktene ytterligere.

Generelt synes bekjempelse av kriminalitet i og mot næringslivet ikke å være trukket frem som et synlig satsningsområde i denne meldingen. Det er et satsningsområde NSR mener bør tydeliggjøres fordi et vel fungerende effektivt næringsliv er grunnlaget for vår nasjonale velferd og trygghet. Vi vil i det etterfølgende begrunne vårt syn:

Kriminalitetsutviklingen
I næringslivet oppleves kriminalitetsutviklingen på samme måte som i samfunnet ellers. Det foregår en tydelig dreining bort fra den fysiske- og over til den digitale kriminaliteten. Fortsatt betyr også fysiske kriminalitet mye for lønnsomheten i noen sektorer. Spesielt gjelder dette vare- og detaljhandelen hvor butikktyverier er et problem som ikke blir prioritert når de anmeldes.
I bygg, eiendom- og anleggssektoren (BEA) er tyveri av kostbart anleggsmateriell fra byggeplasser et fenomen som kommer og går, men som for de som rammes kan ha store forretningsmessige konsekvenser.

Arbeidslivskriminalitet (akrim) forbindes ofte med svart arbeid, hvitvasking og sosial dumping. En fellesnevner er at useriøse aktører undergraver norske samfunnsstrukturer og virker konkurransevridende. Samarbeid og samlokalisering av ressurser mellom etatene i akrimsentrene, har gitt positive resultater. På bakgrunn av felles kunnskap, prioriteres innsats og bruk av virkemidler. Det har gitt positive resultater til støtte for et seriøst arbeidsliv hvor arbeidslivets spilleregler følges, og arbeidslivskriminalitet forhindres og bekjempes. Slik sikres samfunnets verdiskapning.

NSR mener at arbeidet med akrim bekjempelse bør videreføres. Tett og integrert samarbeid mellom ulike komplementære kompetanseområder, kan sikre god situasjonsforståelse og tidsriktig prioritering av innsats og virkemidler. Gjennom fleksibel organisering avhengig av trusselbildet kan vi unngå at noen næringer eller sektorer oppfattes som uregulerte mulighetsområder for vel organiserte og ressurssterke kriminelle.

Digital kriminalitet varierer hva angår mål og metode, men rammer alle sektorer. Metoder og verktøy er under stadig utvikling, og har blitt så troverdige at de er meget vanskelig å avsløre. Bare i løpet av det siste året har digitale svindelforsøk tappet to norske virksomheter for flere hundre millioner kroner.

Mens den fysiske kriminaliteten oppleves som lokal eller regional, er den digitale kriminaliteten global i sin natur. Det betyr at en liten bedrift fra et lite lokalsamfunn i Norge kan utsettes for internasjonale kriminalitet drevet av kriminelle syndikat og/eller nasjonalstater.

De digitale hendelsene vi har hørt om i Norge det siste året representerer trolig bare toppen av isfjellet. Vi vet fra de etablerte CERT-ene (Cyber Emergency Response Teams) og andre foretaks- eller sektorvise responsmiljø at disse daglig beskytter sin del av vår digitale infrastruktur mot cyberangrep.

Kriminaliteten er etterretningsdrevet. Muligheter undersøkes, sårbarheter prøves og sannsynligheter vurderes, før den kriminelle operasjonen iverksettes. Samfunnet og næringslivet taper flere milliarder kroner årlig på grunn av utspekulert, smart svindel og bedrageri.

Det er meget positivt av vi har fått en nasjonal enhet i politiet for bekjempelse av digital kriminalitet (NC3). Den næringsdrivende som utsettes for slik kriminalitet må imidlertid innledningsvis forholde seg til sitt lokale politi. Det er her forhold skal anmeldes, og det er her fra etterforskningen skal starte. Støtten politiet gir næringslivet ved digital kriminalitet oppleves svært mangelfull. Det styrker heller ikke opplevelsen når de fleste sakene henlegges etter kun kort tid.

I opplistingen av hovedprioriteter i tiden fremover fremgår det ikke tydelig at digital kriminalitet er et satsningsområde for politiet. Det presiseres at kriminaliteten skjer i økende grad med bruk av digitale løsninger og i den digitale verden. Men kriminalitetsutfordringene løses ikke ved at "politiet derfor må være til stede på internett og andre digitale plattformer", eller "gjennom å kunne kommunisere med innbyggerne på andre måter enn ved fysisk oppmøte". Intensjonene må tydeliggjøres i samsvar med PST, KRIPOS, NSM og Etterretningstjenestens trusselvurderinger. Det er sikkert bra med to politifolk pr 1000 innbygger, men det hjelper lite om de er på feil sted eller mangler kompetanse for å håndtere den digitale trusselen næringsliv og folk flest opplever.

Prosedyrene for å inngi anmeldelse oppleves meget omfattende og ressurskrevende. Når sannsynligheten for at saken blir henlagt er stor, velger svært mange å ikke anmelde forholdet til politiet.[2] Over tid har denne praksis festet seg. Den fornærmede bedriften mangler en god grunn til å anmelde forholdet. Selvfølgelig er det forståelse for at ikke alle anmeldte saker av ressurshensyn kan etterforskes, men i stedet for å la det bli som det er, må forholdet søkes løst. Ingen er tjent med at eksisterende praksis fortsetter, bortsett fra de kriminelle.

NSR mener utvikling av politiets evne til å forebygge og bekjempe den digitale kriminaliteten bør styrkes betydelig, og i takt med Regjeringens strategi for å digitalisere samfunnet. Styrkingen bør gjøres både lokalt og nasjonalt, og bør skje i samvirke med andre offentlige myndigheter og med næringslivet etter samme prinsipp som akrim arbeidet. Politiet må settes i stand til å håndtere hele spekteret av moderne, sammensatte trusler. Dette er primært en myndighetsoppgave, og er en konsekvens av den samfunnssikkerhets utviklingen regjeringen selv har beskrevet over flere år.

Politiets fremtidige kompetansebehov

Kompetanse er sentralt i forståelsen av et helhetlig trusselbilde. I ØKOKRIMs truselvurdering fra i år fremheves at nasjonale grenser har fått mindre betydning på mange områder. Videre heter det:

"*Grenseoverskridende virksomhet blir mer utbredt og finansielle transaksjoner går raskere……Kriminaliteten i det virtuelle rom skjer i økende grad uten fysisk kontakt, på nye arenaer og gjerne gjennom en identitet som skiller seg fra den fysiske personen. Det daglige kriminalitetsbildet preges i dag av kriminalitet innen virtuell- og kryptovaluta, massebedragerier i virtuelle rom, misbruk av personopplysninger og persondata, nettovergrep og trusler på nett"*.[3]

Det grunn til å stille spørsmål om vi forstår verdien av digital informasjon.

I forhold til personvern og innføringen av et nytt personvernregelverk er verdien av digitalisert informasjon reflektert i lovverk og strafferammer. Det skjedde 20. juni 2018 når EUSs nye personvernforordning (GDPR) ble en del av norsk lovgivning.

[2] Krisino 2019 og Mørketallsundersøkelsen 2020.
[3] https://www.okokrim.no/trusselvurdering-2020.6304950-411472.html

Når det gjelder andre former for digital informasjon, for eksempel næringslivets digitaliserte intellektuelle eiendom, henger trolig forståelsen noe etter. Dette er et fenomen som gjelder hele samfunnet, og som blant annet speiles i Mørketallsundersøkelsen 2020. Beskrivelsen av hva som har gått tapt er mangelfull og konsekvensene begrensede.[4] Svært mange hendelser oppdages ved en tilfeldighet, og mange sliter med å kostnads sette hendelsene. Samtidig vet vi fra de virksomheter som har valgt å være åpen om hendelsene at tapene kan fastsettes i milliardbeløp når vi legger dem sammen. Dette er penger som brukes til å finansiere annen illegal virksomhet og terrorisme globalt.

Vi er nå inne i det noen kaller den fjerde industrielle revolusjon, en revolusjon som blant annet tar bort skillene mellom fysiske, digitale og biologiske sfærer. På samme måte som de tre første industrielle revolusjonene, vil den fjerde også endre økonomi, arbeidsmarked og samfunn på grunn av nye teknologier og prosesser. I motsetning til tidligere, skjer den fjerde industrielle revolusjonen i rekordfart. Den vil med kombinasjonen av hurtig utvikling og økt globalisering, gi muligheter og utfordringer vi aldri har sett.

Norge er alt et av verdens mest digitaliserte land, og Regjeringens digitaliseringsstrategi understreker viktigheten av at denne utviklingen skal fortsette. Det er bra. Vi er avhengig av teknologiutvikling dersom vi skal løse de globale og nasjonale utfordringene knyttet til bærekraftig utvikling. Men for vår nasjonale sikkerhets skyld må også statens regulatoriske evne holde tritt med utviklingen. Usikkerhet om denne evnen kan ha svært negativ effekt på norsk næringsliv og verdiskapning, ved at Norge gjøres til et digitalt fristed for omfattende grenseoverskridende kriminell aktivitet. Konsekvensene kan bli som beskrevet for akrim.

Politiets kapabilitet til å utøve statens maktmonopol spiller en betydelig rolle. Skal man jobbe forbyggende handler dette ikke utelukkende om å være varsom og passe på i forkant. Det handler også om å kunne motta anmeldelser, etterforske, pågripe og få straffedømt de skyldige i våre domstoler. Å bryte loven må ha en åpenbar konsekvens, også på det digitale området.

I et digitalisert samfunn må kompetanse, lovgivning og strafferammer utvikles i takt med den digitale samfunnsutviklingen. Hvis ikke vil vi bli et fristende mål for kriminelle trusselaktører som utnytter vårt åpne tillitsbaserte samfunn og våre næringsområder på grunn av utdatert lovgivning og svak rettshåndhevelse. Er risikoen for å bli tatt lav fordi politiet mangler ressurser eller kompetanse, konsekvensene av å bli tatt håndterbare og gevinstpotensialet stort for de kriminelle, blir vi nettopp et slikt mål. Derfor er det lave antallet anmeldelser innenfor det digitale kriminalitetsområde bekymringsfullt, ikke bare for næringslivet, men også for samfunnet.

Næringslivets Sikkerhetsråd mener krav til politiets satsning på både å forebygge og bekjempe digital kriminalitet bør uttrykkes sterkere og tydeligere enn beskrevet i denne meldingen om fremtidens politi. Den fremtidsrettede holdningen Regjeringen viser i sin digitaliseringsstrategi, må speiles i arbeidet med å kunne håndheve og dømme etter norske lover og bestemmelser på det samme området.

Satsingen som har funnet sted med etableringen av Nasjonalt Cyber-krim senter (NC3) en meget positiv og bør fortsette. Vi mener imidlertid at også politidistriktenes kompetanse innenfor dette området bør styrkes betydelig for at fremtidens politi skal kunne møte publikums forventninger om trygget. Som en begynnelse på dette arbeidet foreslår NSR at ordningen med næringslivskontakter innen politiet styrkes med en egen næringslivskontakt for digital kriminalitet.

Kombinasjonen av to næringslivskontakter med komplementær kompetanse vil sikre relevant støtte fra politiet til virksomheter som opplever digital kriminalitet. Grunnleggende fenomenkunnskap og næringslivskunnskap vil tilføres politiets regionale og sentrale organer. Ordningen vil bidra til et forbedret situasjonsbilde og situasjonsforståelse på alle nivå. Ikke minst kan et slikt tiltak styrke bedre det forebyggende arbeidet i betydelig grad.

[4] NSR: Mørketallsundersøkelsen 2020, ss 33, 49.

Oppsummert

Næringslivets Sikkerhetsråd vil takke for denne muligheten til å bidra til utviklingen av et politi for fremtiden. Vi mener Politimeldingen gir et godt grunnlag for utviklingen av politiet i årene som kommer, men meldingen burde utrykt satsingen for å forebygge og bekjempe digital kriminalitet noe tydeligere. For å avbøte på dette fremmer NSR følgende forslag:

NSR mener at prinsippet for organisering av akrim bekjempelse bør videreføres. Tett og integrert samarbeid mellom ulike komplementære kompetanseområder, sikrer god situasjonsforståelse og tidsriktig prioritering av innsats og virkemidler. Gjennom fleksibel organisering avhengig av trusselbildet kan vi unngå at noen næringer eller sektorer oppfattes som uregulerte mulighetsområder for velorganiserte og ressurssterke kriminelle.

NSR mener utvikling av politiets evne til å forebygge og bekjempe den digitale kriminaliteten bør styrkes betydelig, og i takt med Regjeringens strategi for å digitalisere samfunnet. Styrkingen bør gjøres både lokalt og nasjonalt, og bør skje i samvirke med andre offentlige myndigheter og med næringslivet etter samme prinsipp som akrim arbeidet. Politiet må settes i stand til å håndtere hele spekteret av moderne, sammensatte trusler. Dette er primært en myndighetsoppgave, og en konsekvens av den samfunnssikkerhets utviklingen regjeringen selv har beskrevet over flere år.

Næringslivets Sikkerhetsråd mener krav til politiets kompetanse og evne til å forebygge og bekjempe digital kriminalitet bør uttrykkes tydeligere enn beskrevet i denne meldingen om fremtidens politi. Satsningene bør skje sentralt og lokalt. NSR mener ordningen med lokalenæringslivskontakter innen politidistriktene bør styrkes med en egen næringslivskontakt for digital kriminalitet i hvert distrikt. Grunnleggende fenomenkunnskap og lokal næringslivskunnskap vil tilføres politiets regionale og sentrale organer. Ordningen vil bidra til et forbedret situasjonsbilde og situasjonsforståelse på alle nivå. Ikke minst kan et slikt tiltak styrke det forebyggende arbeidet i betydelig grad.

Vennlig hilsen

Odin Johannessen
Direktør