KRONIKK

Tekst:
Stein Schjølberg, sorenskriver (pensj.), forfatter av boken ”Cyberkriminalitet” Universitetsforlaget (mai 2017)

Et nytt trussel- og risikobilde i cyberspace

Vi må ha en best mulig cybersikkerhet og vern mot terrorangrep og cyberangrep på vårt samfunn i fremtiden. Cyberangrep er i ferd med å skape et nytt trussel- og risikobilde hvor våre vitale nasjonale interesser kan være truet. Ikke minst er det alvorlig når det kan synes som om andre statlige aktører utgjør en vesentlig del av risikobildet. Som et eksempel vises til at President Obama den 29. desember 2016 besluttet tiltak overfor Russland, og uttalte blant annet: *In response to the Russian government's aggressive harassment of U.S. officials and cyber operations aimed at our election. Russia´s cyber activities were intended to influence the election, erode faith in U.S. democratic institutions, sow doubt about the integrity of our electoral process, and undermine confidence in the institutions of the U.S. government. These actions are unacceptable and will not be tolerated.*

Trusselbildet er også beskrevet i Etteretningstjenestens rapport FOKUS 2016 slik: *Teknologisk kompetente aktører har mulighet for tilgang til vitale deler av det norske samfunnets digitale infrastruktur, noe som kan nyttes til å hente ut informasjon om politiske beslutningsprosesser, militære forhold, økonomi og høyteknologi. Den teknologiske utviklingen gjør at metodene er i rask utvikling og bidrar til at det er stadig vanskeligere å avsløre og identifisere stater, grupper og personer som opererer i det digitale rom.*

Store utfordringer
Norge er et av verdens mest digitaliserte land og står overfor store utfordringer i behovet for å gjennomføre tiltak for å forebygge og verne landet, både for forsvaret av Norge mot og krigslignende cyberangrep, og mot alvorlige cyberangrep og annen cyberkriminalitet. Et større cyberangrep kan sette ut av spill viktige samfunnsfunksjoner, for eksempel innen olje- og kraftforsyning, telekommunikasjon, finans, kringkasting, transport, og helsevesen. Nasjonal Sikkerhetsmyndighet (NSM) har høsten 2015 avgitt sin rapport ”Sikkerhetsfaglige råd”, og presenterer 72 anbefalte tiltak. NSM uttaler i rapporten på side 5-6 blant annet: *Sikkerhetsarbeidet har i for stor grad fokusert på usammenhengende organisatoriske og tekniske løsninger, som er fragmentariske og suboptimale. Dette blir mer utfordrende desto mer nettverksorientert samfunnet blir.*

Forebyggende tiltak
Forebyggende tiltak mot cyberkriminalitet er meget viktig. De forbyggende tiltak som i dag kan være nødvendige mot globale cyberangrep og annen alvorlig cyberkriminalitet som opererer helt uavhengig av nasjonale landegrenser kan deles inn i fire hovedområder. Det er for det første nødvendig å tilføre politi og institusjoner for cybersikkerhet kunnskap om kjente former for cyberkriminalitet. For det andre er det nødvendig å oppdatere eller innføre særskilte straffebestemmelser, hvor straffelovgivningen ikke gir et tilstrekkelig vern. For det tredje er det nødvendig å

utvikle hensiktsmessige internasjonale cybersikkerhetstiltak for styring og kontroll av lagring og kommunikasjon av data og informasjon både nasjonalt og internasjonalt. For det fjerde en mulighet til forsikring mot cyberkriminalitet, slik at forsikringsselskapene gir økonomisk trygghet til forsikringstageren, og setter samtidig standarder for hva som kreves av forebyggende cybersikkerhetstiltak.

Cybersikkerheten på det offentlige operative nivå i Norge er god, med virksomheten til Nasjonal Sikkerhetsmyndighet (NSM), Forsvarets Sikkerhetstjeneste, PST, Kripos, og enkelte bedrifters cybersikkerhet. Center for Cyber and Information Security, NTNU, er et av de fremste forskningsinstitusjoner for cybersikkerhet i Norge, direktør Sofie Nystrøm har i juli 2016 blant annet uttalt følgende: *Landegrenser er for lengst visket ut i det digitale rom og gjør at samarbeid det satses på i NATO, EU, FN og Interpol er ekstra viktig. Dette er den eneste måten å takle de massive problemstillingene vi står ovenfor på tvers av myndighetene, leverandører og private virksomheter.*

Statsministerens kontor
Først og fremst foreslår jeg at Statsministerens kontor bør styrkes. Det er Statsministeren som er regjeringens øverste politiske leder og som sitter med det overordnede ansvar for Norges cybersikkerhet og beredskap. Jeg foreslår at Statsministerens kontor bør få et mer direkte ansvar og rolle i tiltak som omfatter å styrke den nasjonale cybersikkerheten og vernet mot cyberangrep og annen alvorlig cyberkriminalitet. Dette arbeidet bør ledes av en statssekretær for å få en effektiv politisk gjennomslagskraft. Det bør også kunne vurderes en "nasjonal sikkerhetsrådgiver", istedenfor en statssekretær. Jeg viser til at i flere land har Statsministerens kontor de senere år økt sin innflytelse og posisjon som regjeringsleder. Det skapes således et mer robust ledelsesapparat for krisehåndtering. Australia har utviklet en Cyber Security Strategy i 2016. Statsminister Malcolm Turnbull uttalte blant annet følgende: *"The Government will show leadership locally, regionally and globally. I will designate a Minister Assisting the Prime Minister on cyber security and appoint a Special Adviser on Cyber Security in my Department, the Government's lead on cyber security policy."*

Et Sikkerhets- og beredskapsdepartement
Det bør også pånytt vurderes å etablere et Sikkerhets- og beredskapsdepartement som bør få ansvaret for den nasjonale cybersikkerheten, og Nasjonal Sikkerhetsmyndighet (NSM) bør være hoveddelen av et nytt departement. Jeg foreslår at anbefalingene fra Sårbarhetsutvalget av 2000 (Willoch-utvalget) nå vurderes i et cybersamfunn av i dag, og eventuelt legges til grunn. Det globale cybersamfunn har skapt en helt annen situasjon i 2016 og klargjort behovet for en vesentlig bedre sikkerhets- og beredskapspolitikk, som også omfatter cybersikkerhet. Andre land har etablert et særskilt departement for sikkerhet- og beredskap, blant annet USA med *Department of Homeland Security*.
Justis-og beredskapsdepartementet bør etter min mening deles i to departementer, og departementet bør pånytt får betegnelsen Justisdepartement. Jeg foreslår at Norge også bør få sin versjon av *Department of Homeland Security*. Dette vil medføre en samordnet og effektiv nasjonal cybersikkerhet- og beredskap. Utviklingen av cyberspace har ført til at internasjonale tiltak for cybersikkerhet, samtidig blir en vesentlig del av våre nasjonale cybersikkerhetstiltak. Nasjonal Sikkerhetsmyndighet (NSM) har i sin rapport også uttalt følgende om Justis- og beredskapsdepartementets

koordineringsrolle: *Justis- og beredskapsdepartementets koordinerende rolle innenfor forebyggende sikkerhet i sivil sektor er ikke i tilstrekkelig grad operasjonalisert slik at departementet kan ta sin rolle med den kraft som er nødvendig.*
Riksrevisjonen har også kritisert at ansvarlige departementer ikke har fulgt opp IKT sikkerheten godt nok, og at det er store svakheter i behandlingen av samfunnsviktige data.

Politiadministrasjonen
Det bør etter min mening nå vurderes om politiet skal få sin Politiadministrasjon på samme måte som Domstoladministrasjonen, direkte underlagt Statsråden i Justisdepartementet og undergitt Stortingets styring og kontroll, og ledet av en Rikspolitisjef slik som i andre nordiske land. Det har nå gått femten år side Politidirektoratet (POD) ble opprettet. Virkningen ved å ha en administrative enhet også i Justisdepartementet, har ført til en administrativ dobbeltbehandling og til en uklar rolle- og arbeidsfordeling. I tillegg har en form for sekretariatfunksjon medført omfattende detaljstyring av POD. Jeg foreslår at det oppnevnes et nytt utvalg til å utrede behovet for en eventuell omorganiseringen av den sentrale politiforvaltning, som også bør inkludere en utredning om påtalemyndigheten i politiet skal underlegges Riksadvokatens administrasjon. Utvalget bør ledes av Riksadvokaten.

Straffelovgivning
For å kunne etablere strafferettslige standarder i cyberspace, må straffebestemmelser bli utformet så klare, entydige og presise som mulig. Rettsanvendelsen må ikke baseres på utflytende tolkinger av eksisterende straffebestemmelser som ble vedtatt for å omhandle andre formål enn informasjons- og kommunikasjonsteknologien, eller som rammer bare tilfeldig og perifer atferd i cyberspace. En av de viktigste formål med straffelovgivningen er å forebygge straffbare handlinger, som også gjelder for lovgivning om cyberkriminalitet. De prosessuelle elementer i etterforskingen og påtale av cyberkriminalitet må også inkludere virkemidler som tar vare på fundamentale rettigheter til personvern og menneskerettigheter, og at disse samsvarer med forpliktelsene i de internasjonale lovverk om menneskerettigheter. Forebyggende virkemidler, etterforsking, påtale og domstolsbehandling må baseres på lovgivning og være under domstolskontroll, og de rettigheter som har et vern offline må også få anvendelse som et vern online.

Internasjonale tiltak
Vi står her overfor cyberangrep og annen cyberkriminalitet som opererer helt uavhengig av nasjonale og regionale grenser. Lov og orden må også sikres og utvikles i cyberspace, som i det globale samfunn for øvrig. Et hovedproblem er at handlinger i cyberspace kan finne sted uten at det eksisterer internasjonal lovgivning eller en domstol som kan stille aktørene til ansvar med rettsforfølging og straff. Cyberspace er i dag den siste gjenværende arena der globale straffbare handlinger kan gjennomføres uten nevneverdig risiko. Alle andre områder, det være seg på land, til sjøs, og i luften er underlagt internasjonale lover og regelverk. Det er i dag bare innenfor bilaterale og multilaterale avtaler at cyberkriminalitet over landegrensene vil kunne straffes, og dette vil ikke være tilstrekkelig for en global cybersikkerhet. Den seneste utvikling av alvorlige cyberangrep mot enkeltlandenes kritiske informasjonsinfrastruktur har vist nødvendigheten av å etablere tiltak i internasjonale regelverk som vern mot cyberangrep og annen alvorlig global cyberkriminalitet. Tiltak for etterforsking og straffeforfølgning må derfor organiseres på internasjonal basis, der verdenssamfunnet

samordner sine interesser. Norge som fredsnasjon bør spille en viktig rolle. Det er nødvendig at forslag om globale tiltak for fred, cybersikkerhet og rettsikkerhet i cyberspace på FN-nivå stadig fremmes og drøftes.

INTERPOL

INTERPOL har bygget opp sin avdeling, INTERPOL Global Complex for Innovation (IGCI) i Singapore. Et samarbeid gjennom INTERPOL kan være helt avgjørende for gjennomføringen av en etterforsking, slik som avdelingens direktør Noboru Nakatani, uttalte i januar 2016: *Due to bilateral relations between Russia and USA, a joint task force is not feasible, but through Interpol, it happened. Under the umbrella of Interpol, people are motivated to work together to combat cybercrime. Combating cybercrime is not about competition, its about cooperation and collaboration.*
INTERPOL forstår at cybereksperten i fremtiden ikke vil finnes i politiorganisasjoner, men i akademia og den private sektor. INTERPOL World 2017 ble arrangert i Singapore 5-7. Juli 2017. Mer enn 250 selskaper fra hele verden deltok. Men enkelte store globale selskaper som Google, Facebook, og Apple var invitert, men møtte ikke.

A Geneva Convention or Declaration for Cyberspace

Et initiativ for å utvikle en konvensjon eller erklæring bør bli utarbeidet og bli vedtatt slik som tidligere Geneve konvensjoner eller erklæringer (Declarations). Geneve er en helt spesiell by med hovedkvarter for flere FN-institusjoner. De felles standarder og normer for handlinger og kommunikasjon i cyberspace som bør diskuteres i et slikt rammeverk kunne være følgende: standarder for internasjonale tiltak for cybersikkerhet, internasjonal koordinering og samarbeid for etterforsking av internasjonal alvorlig cyberkriminalitet gjennom INTERPOL, standarder for et globalt partnerskap med den private sektor i etterforsking og påtale av alvorlig cyberkriminalitet, harmonisering av landenes straffelovgivning mot cyberkriminalitet, og etablere en internasjonal kriminaldomstol eller tribunal for cyberspace *A Third Pillar for Cyberspace*

Public-Private Partnerships

Forebyggelse og bekjempelse av den globale cyberkriminalitet krever også et samarbeid og koordinering med global privat sektor, de såkalte *"Public-Private Partnerships".* Slike samarbeidsavtaler med den globale private sector bør baseres på et internasjonalt avtalegrunnlag, slik som *A Memorandum of Understanding (MoU).* Samarbeidet må unngå å behandle sikkerhetsgradert informasjon. INTERPOL forstår at cybereksperten i fremtiden ikke vil finnes i politiorganisasjoner, men i akademia og den private sektor. INTERPOL World 2017 ble arrangert i Singapore 5-7. Juli 2017. Mer enn 250 selskaper fra hele verden deltok. Men enkelte store globale selskaper som Google, Facebook, og Apple var invitert, men møtte ikke. Europol organiserte i Haag den tredje *Europol-INTERPOL Cybercrime Conference* i 2015. Det deltok flere enn 350 cyber eksperter fra hele verden, som også inkluderte mange fra privat sektor og akademia.
Statsministeren og regjeringen i Japan organiserte i november 2015 en stor konferanse med flere enn 400 nasjonale og internasjonal deltagere. Japan er en av verdens største produsenter av smart-teknologi innenfor "Internet of Things (IoT)". Konferansen som hadde tittelen *Cyber3Conference Okinawa 2015* omfattet tre hovedelementer som er forbundet innbyrdes, og som det globale cybersamfunnet står overfor:

cybertilknytning, cybersikkerhet, og cyberkriminalitet. Konferansens inneholdt diskusjoner om hvordan det globale cybernettverket kunne sikres og styrkes, med spesiell fokus på ”public-private partnerships”.
Microsoft har etablert Digital Crimes Unit (DCU), som er en internasjonal ekspertgruppe med juridisk og teknisk ekspertise og samarbeider med kunder og partnere over hele verden. Microsoft Cybercrime Center i Seattle organiserte i februar 2015 *Cybercrime Enforcement Summit*, som hadde deltagelse fra INTERPOL, Europol, FBI, Secret Service i USA, og politiorganisasjoner fra mange land.
Etter min mening bør Microsoft Cybercrime Center og Digital Crimes Unit kunne være en modell for andre globale IT selskaper som ønsker et ”public-private partnership”.

For mer informasjon, se www.cybercrimelaw.net