



Utenriksdepartementet

Strategi

# Internasjonal cyberstrategi for Norge

2017



# Internasjonal cyberstrategi for Norge

2017

# Forord av statsminister Erna Solberg

Utviklingen i det digitale rom – cyberdomenet – skjer raskt. Internettets globale karakter gir enorme muligheter. Betydningen av det digitale rom for nasjoners økonomi, sikkerhet, vekst og utviklingsmuligheter er stor og økende.

Samtidig gjør vår avhengighet av digitale løsninger oss sårbare. Det digitale rom åpner for nye og alvorlige grenseoverskridende trusler fra både statlige og andre aktører. Hele det norske samfunnet er i dag avhengig av sikre, stabile og robuste digitale nettverk. Et alvorlig cyberangrep kan ramme samfunnets kritiske infrastruktur.

For å oppnå best mulig beskyttelse er Norge avhengig av et bredt samarbeid både nasjonalt og internasjonalt. På det digitale området er det behov for økt nasjonal samordning når det gjelder sikkerhet og for å understøtte norske interesser i videreutviklingen av internasjonal praksis og regelverk på cyberområdet.

Flere aspekter i utviklingen av det digitale rom vil kreve vår oppmerksomhet fremover. Ett eksempel er at et bærekraftig internett er avhengig av den riktige balansen mellom åpenhet, sikkerhet, robusthet og frihet. Norge arbeider for et digitalt rom som fremmer innovasjon og internasjonal handel, som bidrar til internasjonal stabilitet og sikkerhet og som ivaretar demokratiske verdier og universelle menneskerettigheter.

Det er enighet internasjonalt om at den alminnelige folkeretten i utgangspunktet også gjelder i det digitale rom. Samtidig er det behov for internasjonal dialog om hvordan folkeretten kommer til anvendelse i cyberdomenet. Det er i dag ingen FN-konvensjoner eller globale avtaler som særskilt regulerer staters bruk av det digitale rom. Viktige beslutninger om utvikling og forvaltning av internettet blir i stor grad fattet av kommersielle og andre aktører, uten direkte påvirkning fra myndigheter eller samfunnsborgere. Også på disse områdene er det ulike synspunkter globalt om retningen videre.

For regjeringen er det viktig at Norge har en helhetlig og koordinert politikk for å påvirke utviklingen av det globale digitale rom der dette er mulig. Regjeringen legger derfor vekt på tett samordning mellom relevante myndighetsorganer som representerer Norge på de arenaer hvor internasjonale rammevilkår og spilleregler for det digitale rom utformes. I Stortingsmelding 37 (2014-2015) redegjør regjeringen for globale sikkerhetsutfordringer i utenrikspolitikken. Som en oppfølging av meldingen etablerte Utenriksdepartementet i 2016 en nasjonal cyberkoordineringsgruppe for å koordinere norske standpunkter på cyberområdet i internasjonale fora.

Vår internasjonale cyberpolitikk skal tjene Norge og norske interesser, sikre gode og forutsigbare rammevilkår, og bidra til forebygging av og beskyttelse mot utfordringer og trusler i det digitale rom. Bedre nasjonal samordning vil øke effekten av vår politikk, og bidra til å heve vår anseelse internasjonalt på dette feltet. Denne internasjonale cyberstrategien er et viktig første steg til bedre nasjonal koordinering på feltet.



Oslo, 31. august 2017

# Innholdsfortegnelse

Forord av statsminister Erna Solberg. ....	3
Bakgrunn. ....	5
Styrende prinsipper. ....	6
Norges strategiske prioriteringer . . . . .	7
Cybersikkerhet: Fremme sikre, stabile og robuste digitale nettverk . . . . .	7
Innovasjon og økonomi: Fremme innovasjon, utvikling og markedstilgang. ....	8
Bekjempe kriminalitet: Internasjonalt samarbeid mot organisert IKT-kriminalitet og annen alvorlig kriminalitet i det digitale rom . . . . .	8
Cyberdomenet i sikkerhetspolitikken. ....	9
Global forvaltning av internett: Bidra til effektive, stabile og inkluderende strukturer. ....	10
Utvikling: Tilgang til internett og utvikling av kapasitet for å utnytte det digitale roms potensiale for å fremme vekst, velstand og sikkerhet for alle. ....	11
Frihet på nett: Universelle rettigheter gjelder også online. ....	12

## Innledning

Det digitale rom har på kort tid endret det globale landskapet Norge befinner seg i. Internett har utviklet seg til å bli verdens viktigste infrastruktur og utgjør i dag ryggraden i den globale flyten av varer, tjenester og informasjon. Om få år antas internett å være den superstrukturen som all annen infrastruktur er avhengig av. Betydningen av det digitale rom for nasjoners økonomi, sikkerhet, vekst og utviklingsmuligheter er stor og økende.

Det har ført til at stater har intensivert sitt arbeid for å fremme nasjonale interesser i utviklingen og bruken av det digitale rom. Det pågår prosesser multilateralt blant annet i FN, Nato og OSSE, og bilateralt mellom enkeltland knyttet til bruk og regulering. I tillegg diskuteres dette mellom våre allierte i sikkerhetspolitiske fora, på globale arenaer hvor internasjonal handelspolitikk, justispolitikk og samferdselspolitikk utvikles. Dessuten er kontakt og samarbeid med private aktører sentralt.

I dag er det ingen FN-konvensjoner eller globale avtaler som regulerer særskilt staters bruk av det digitale rom. Dette er ulikt andre områder av stor betydning for global økonomi og sikkerhet. Det er imidlertid internasjonal enighet om at den alminnelige folkeretten i utgangspunktet også gjelder i det digitale rom. Samtidig er det i noen tilfeller tvil og uenighet om hvordan og når folkeretten kommer til anvendelse.

Et velfungerende globalt internett og en robust global digital infrastruktur er avgjørende for Norges økonomi og sikkerhet. Vi har en grunnleggende og langsiktig interesse av å bidra til å skape gode rammevilkår for fremtidig utvikling og bruk av det digitale rom.

Forsvar mot digitale trusler blir stadig viktigere. Men forsvar alene skaper ikke sikkerhet. Som i den analoge verden er det nødvendig også å håndtere de bakenforliggende årsakene til truslene og å avveie tiltak mot trusler opp mot de mange fordeler og muligheter det digitale rom gir. Vi må finne en riktig balanse mellom sikkerhet på den ene siden og åpenhet på den andre. Et velfungerende digitalt rom er avhengig av begge deler.

## Bakgrunn

Det digitale rom har lagt grunnlaget for innovasjon, vekst og utvikling både nasjonalt og globalt. Med en stabil og robust digital infrastruktur er det nesten ingen grenser for hvilke muligheter internett åpner for. Internett har endret vår hverdag på de fleste områder de siste 20 årene. Produksjon, handel, underholdning, utdanning, finans, helsetjenester, landbruk, kommunikasjon, politisk mobilisering, transport, medier, sikkerhet, og kontakt med offentlige etater er noen eksempler. Internettets betydning for sosial og økonomisk utvikling vil ikke bli mindre i årene fremover. I utviklingsland gir det digitale rom spesielt store muligheter for vekst og utvikling.

Statlige myndigheters rolle i *utviklingen* av det digitale rom er begrenset. Staten har likevel en viktig rolle som *tilrettelegger* for utvikling, eksempelvis gjennom reguleringer og gjennom fremme av innovasjon, forskning og undervisning, og i noen tilfeller som eier og beskytter av kritisk infrastruktur. Internasjonalt spiller statlige myndigheter en viktig rolle i normutvikling i det digitale rom, politisk som operativt. Utvikling av internett og digitale tjenester og produkter foregår imidlertid i all hovedsak gjennom private selskap og forsknings- og utviklingsmiljøer. I tillegg er selve ryggraden i internettet, den globale digitale infrastrukturen, i hovedsak i privat eie. Regjeringens holdning er at dette i utgangspunktet er positivt og bidrar til konkurranse, fortsatt innovasjon og utvikling. Samtidig betyr det at viktige beslutninger om utvikling og sikkerhet i det digitale rom i stor grad blir fattet av kommersielle og ikke-statlige aktører utenfor de tradisjonelle mellomstatlige arenaene vi kjenner.

I kombinasjon med samfunnets voksende avhengighet av det digitale rom opplever vi en kraftig økning av digitale sikkerhetsutfordringer og digitale sårbarheter<sup>1</sup>. IKT-kriminalitet og nettverksoperasjoner fra både statlige og ikke-statlige aktører utgjør svært alvorlige trusler mot Norges sikkerhet og økonomi. Dette må gjenspeiles i vårt internasjonale samarbeid og vår sikkerhets- og utenrikspolitikk. Regjeringens internasjonale cyberstrategi gjør rede for våre styrende prinsipper og strategiske prioriteringer på dette området.

---

<sup>1</sup> Jfr. bl.a. Melding til Stortinget nr. 38 (2016-2017) *IKT-sikkerhet. Et felles ansvar*, og NOU 2015:13, *Digital sårbarhet – sikkert samfunn* (Lysne I utvalget).

## Styrende prinsipper

Norge arbeider for et digitalt rom som fremmer innovasjon og internasjonal handel, som bidrar til internasjonal stabilitet og sikkerhet og som ivaretar demokratiske verdier og universelle menneskerettigheter. Det gjør vi i samarbeid med andre stater og internasjonale organisasjoner, men også med partnere fra ikke-statlige aktører som akademia og forskningsmiljø, næringslivet og sivilsamfunnet.

Et bærekraftig globalt internett er avhengig av den riktige balansen mellom *åpenhet, sikkerhet, robusthet og frihet*. For å opprettholde dette er vi avhengig av internasjonalt samarbeid.

Det digitale rom påvirker alle deler av samfunnet. Regjeringen legger derfor vekt på tett koordinering mellom relevante myndighetsorganer som representerer Norge på internasjonale arenaer hvor internasjonal cyberpolitikk skapes og utvikles.

### **Åpenhet**

Internettets suksess skyldes interoperabilitet som gir tilgang for alle og internasjonale standarder basert på konsensus. Det er avgjørende at både de offentlige og private forvalterne av internettet holder tritt med utvikling og innovasjon. Myndigheters inngripen for å regulere må sikre fortsatt åpenhet og ikke hindre innovasjon og begrense kreativiteten hos utviklere, gründere og andre.

### **Sikkerhet**

Norge skal beskytte sine digitale nettverk, og sammen med andre stater arbeide for et sikkert digitalt rom som innbyr til tillit hos myndigheter, næringsliv og individer. Sikkerhet i det digitale rom gir handlefrihet. Det gjelder å finne den rette balansen mellom hva vi *kan* gjøre og hva vi *bør* gjøre for å redusere samfunnets og individers sårbarhet.

### **Robusthet**

Det nettverk av nettverk som til sammen utgjør internett går på tvers av geografiske grenser. Stabilitet i og tillit til digitale nettverk er avgjørende for global utvikling. Sikkerhet i disse nettverkene er ikke utelukkende et teknisk spørsmål. Vi må avklare ansvar mellom myndigheter og privat sektor. Vi må skape global forståelse og respekt for betydningen av digital infrastruktur. Vi må ansvarliggjøre sluttbrukere og virksomheter slik at digitale enheter håndteres og opereres på en sikker måte.

### **Frihet**

Samtidig som vi skal ivareta våre digitale sikkerhetsinteresser, må vi også ivareta våre demokratiske verdier og rettigheter for individer.

Universelle menneskerettigheter gjelder også online. Det er viktig at menneskerettigheter som ytringsfrihet, forsamlingsfrihet og religionsfrihet har den samme beskyttelse i det digitale rom som i det analoge.

# Norges strategiske prioriteringer

## *Cybersikkerhet: Fremme sikre, stabile og robuste digitale nettverk*

Hele det norske samfunnet er i dag avhengig av sikre, stabile og robuste digitale nettverk for å fungere godt. Det gjelder også grunnleggende funksjoner i samfunnet, som energiforsyning, vannforsyning, helsetjeneste, samferdsel, beredskap og finansvesen. Arbeidet med cybersikkerhet krever et bredt samspill mellom aktører på tvers av nasjonale grenser. For å fremme sikkerhet, stabilitet og økt robusthet i digitale nettverk vil regjeringen:

- **Fremme internasjonalt samarbeid om cybersikkerhet og enighet om statlig oppførsel i det digitale rom.** I dag deltar Norge på viktige arenaer i regi av EU, FN, Nato, OECD (Organisasjonen for økonomisk samarbeid og utvikling) og OSSE (Organisasjonen for sikkerhet og samarbeid i Europa), Europarådet samt i dialoger med andre stater både bilateralt og regionalt, herunder Nordisk samarbeid.
- **Bidra til global forståelse for at man må se personrelaterte, teknologiske og organisatoriske sikkerhetstiltak i sammenheng:** Norge skal være et eksempel for andre stater som vil tilrettelegge for god samhandling mellom tilbydere av digital tilgang, varer og tjenester og regulerende myndigheter for å identifisere digitale trusler, redusere sårbarheter og håndtere cyberhendelser. Det er myndighetenes ansvar å bidra til å tilrettelegge for en god sikkerhetskultur og forsvarlig opptreden i det digitale rom.
- **Videreutvikle det internasjonale samarbeidet for å styrke vår evne til å forebygge, oppdage, varsle og håndtere alvorlige cyberhendelser.** Digitale angrep og hendelser strekker seg over landegrenser og krever derfor internasjonalt samarbeid for å forebygges og håndteres. Regjeringen vil fortsette å utvikle samarbeidet med andre stater for å styrke egen og andre staters evne til å forebygge og håndtere digitale angrep.
- **Fremme internasjonale standarder og samarbeid.** Elektronisk kommunikasjon er global. Tjenester og produkter vi bruker i Norge er som oftest produsert og utviklet i andre deler av verden. Det er derfor i vår interesse å arbeide for gode internasjonale standarder. På europeisk nivå er European Network and Information Security Agency (Enisa) og European Telecommunications Standards Institute (ETSI) og deres Technical Committee Cyber (TC Cyber) viktige samarbeidspartner. Globalt er Den internasjonale standardiseringsorganisasjonen (ISO) og Den internasjonale telekommunikasjonsunionen (ITU) sentrale aktører for internasjonalt samarbeid.
- **Arbeide for et grunnleggende felleseuropeisk sikkerhetsnivå:** Produksjon av norske elektroniske kommunikasjonstjenester avhenger i stor grad av fysisk infrastruktur og av innsatsfaktorer fra leverandører utenfor landets grenser. Norge skal være en pådriver for å etablere en hensiktsmessig regulering på europeisk nivå som møter sikkerhetsutfordringene knyttet til utkontraktering og internasjonalisering, og som blant annet omfatter tilsyn og kontroll av leverandører og samarbeid på tvers av landegrensene.
- **Styrke samarbeidet med EU.** Samarbeidet med EU om cybersikkerhet er av stor betydning for Norge. Regjeringen vil fortsette å arbeide for å optimalisere dette samarbeidet blant annet gjennom oppfølging av direktivet om nettverks- og informasjonssikkerhet (NIS-direktivet) og European Network Information Security Agency (Enisa). Vi vil også delta i det europeiske kontraktuelle offentlig-private partnerskapet om cybersikkerhet (cPPP Cybersecurity).

## *Innovasjon og økonomi: Fremme innovasjon, utvikling og markedstilgang*

Den digitale økonomien er fortsatt i rask utvikling og er en av de viktigste drivere for verdiskaping, innovasjon, konkurranseevne og vekst. Det digitale rom bidrar til vekst og sysselsetting ved å skape grunnlag for investeringer og innovasjon, øke tilgangen til større markeder og redusere betydningen av geografisk lokalisering. Selv små bedrifter kan nå kunder hvor som helst i verden uten betydelige merkostnader. For å sikre at det digitale rom også i fremtiden vil støtte opp under norsk økonomi og innovasjon vil regjeringen:

- **Fremme global åpenhet på internett.** Norge skal samarbeide med andre stater for å sikre at internett forblir en åpen og ikke-diskriminerende plattform for kommunikasjon hvor forbrukerne har tillit til digitale markeder.
- **Tilrettelegge for digital innovasjon,** både i privat og offentlig sektor innenfor EØS-området. Samtidig vil vi arbeide for økt digital kompetanse og digitale ferdigheter for framtidens arbeidsmarked.
- **Beskytte åndsverk.** Sammen med andre stater skal Norge bidra til å beskytte åndsverk og sensitiv informasjon mot tyveri og plagiering. Norske informasjonssikkerhetsmiljø oppfordres til å knytte seg til European Cyber Security Organisation (ECSSO).
- **Fremme norsk forskning globalt** og bidra til at norske forskningsmiljøer er i forkant innenfor informasjons- og kommunikasjonssikkerhet. Regjeringen vil legge til rette for samarbeid mellom norske og internasjonale forskningsmiljøer og kunnskapsinstitusjoner. Forskningen skal bidra til å finne nye løsninger på sentrale samfunnsutfordringer knyttet til cyberfeltet, og styrke muligheten til offentlig sektor og næringsliv for å adoptere og utnytte både nasjonale og internasjonale forskningsresultater.
- **Sammen med OECDs medlemsstater arbeide for å fremme digital økonomi.** Gjennom å styrke mulighetene for tilgang til digitale tjenester globalt; redusere barrierer for investering i og anvendelse av digitale teknologier; fremme omforente globale standarder for et åpent, stabilt og tilgjengelig internett; bidra til utvikling av nasjonale og internasjonale strategier for personvern og databeskyttelse; utvikle og ta i bruk teknologinøytrale reguleringer som fremmer konkurranse om infrastruktur; redusere hindringer for utviklingen av e-handel globalt, med vekt på styrket tillit blant forbrukere, og forbedre utdanningssystemer for å møte behovet for IKT-kompetanse. Vi vil også delta i den koordinerte forsknings- og innovasjonsinnsatsen innenfor IKT-sikkerhet som inngår i vårt samarbeid med EU.

## *Bekjempe kriminalitet: Internasjonalt samarbeid mot organisert IKT-kriminalitet og annen alvorlig kriminalitet i det digitale rom*

Digitaliseringen av samfunnet har skapt nye arenaer for kriminelle handlinger slik som for økonomisk vinning, sabotasje, overgrep eller oppfordring til voldelig ekstremisme. Norske virksomheter og norske interesser er under økende press. Digitale nettverk kan både være en bærer av kriminelle handlinger i cyberdomenet eller være mål i seg selv.

Norge skal bidra i det internasjonale arbeidet for å bekjempe kriminalitet i det digitale rom ved å:

- **Bidra til utforming av normer, konvensjoner og tiltak for å bekjempe IKT-kriminalitet.** Norge har en langsiktig strategisk interesse av å påvirke utviklingen av internasjonale konvensjoner, internasjonale normer og andre tiltak som former rammene for hvordan IKT-kriminalitet skal bekjempes globalt. I denne sammenheng er det viktig å sikre en effektiv internasjonal straffesaksbehandling. Norge vil arbeide for at flere stater slutter seg til prinsippene i Europarådets konvensjon om datakriminalitet (Budapestkonvensjonen). Vi ønsker internasjonal harmonisering av lovverk for IKT-kriminalitet, samt effektive virkemidler for bistand og beredskap over landegrensene.



- **Delta aktivt i internasjonalt politisamarbeid mot IKT-kriminalitet.** Norge deltar i samarbeid innen Europol, Interpol og det nordiske samarbeid om kompetanse, kapasitet- og informasjonsutveksling. Norge vil løpende vurdere behovet for å ha en tilstedeværelse av liaisoner i de store internasjonale satsingene i Europol og Interpol og delta i tidsbegrenset utveksling av personell med spesialkompetanse. Virtuelle IKT-tjenester og spredning av data og dataprogrammer over landegrenser muliggjør etablering av fristeder for kriminelle på nett. Regjeringen vil løpende vurdere behovet for et tettere samarbeid med andre stater for å forhindre slike fristeder.
- **Styrke og videreutvikle det forebyggende arbeidet mot radikaliserings og rekruttering på internett.** For å lykkes med å forebygge radikaliserings og voldelig ekstremisme, vil Norge i samarbeid med andre stater utvikle målrettede tiltak mot plattformene der den ekstremistiske propagandaen spres. Norge vil samarbeide tett med stater som håndterer tilsvarende utfordringer og sørge for at våre tiltak holder en høy internasjonal standard.
- **Aktivt delta på internasjonale arenaer som utveksler informasjon og erfaringer og utformer gode løsninger for å forebygge og bekjempe IKT-kriminalitet.** Deltakelse i slike fora gir verdifull erfaringsutveksling som er viktig for norsk politikktutforming på området og for å bekjempe IKT-kriminalitet i Norge. Samtidig kommer våre erfaringer andre land til gode. Blant de aktuelle internasjonale arenaer er FNs kontor for bekjempelse av narkotika og kriminalitet (UNODC), Europarådet, EU, Internet Corporation for Assigned Names and Numbers (Icann), Enisa og Eurojust.

### *Cyberdomenet i sikkerhetspolitikken*

Norge skal beskyttes mot alvorlige digitale trusler fra statlige og ikke-statlige aktører. Handlefrihet i det digitale domenet skal sikres både gjennom det vi gjør nasjonalt og gjennom internasjonalt samarbeid, særlig innenfor Nato, OSSE og FN. Nato er et viktig forum for erfaringsutveksling og ekspertise, felles standarder, øvelser og trening som gir allierte evne til å operere sammen i kriser, og er viktig for å videreutvikle det digitale rom som et operasjonsdomene. I OSSE arbeides det med «kjøreregler» og tillitsbygging, mens det innenfor FN-systemet pågår diskusjoner om folkerettens anvendelse og en gryende internasjonal diskusjon om dilemmaene og problemstillinger utvikling av «cybervåpen» stiller oss overfor. Norge skal gjennom nasjonal og internasjonal innsats ivareta våre sikkerhetspolitiske interesser ved å:

- **Fortsette å utvikle god beskyttelse mot cybertrusler nasjonalt, herunder gjennom bredt sivilmilitært og offentlig-privat samarbeid. Norge skal investere ytterligere i etterretning.** God beskyttelse mot digitale angrep i fred, krise og væpnet konflikt forutsetter evne til å oppdage, motstå og håndtere trusler, samt evne til mottiltak mot digitale angrep, i tråd med internasjonal rett. Dersom en motstander hindres i å oppnå den effekten vedkommende er ute etter, vil slike cyberangrep miste noe av sin nytteverdi.
- **Sammen med likesinnede land videreutvikle evnen til forsvar mot digitale angrep.** Nato-samarbeidet samt bilateralt og flernasjonalt samarbeid med nære allierte skal prioriteres. Norge skal beskytte egne styrkebidrag i internasjonale operasjoner mot digitale angrep. Videre skal Norge samarbeide med partnerland der det gagnar norske interesser. Vi skal bidra til at Natostyrker sin samlede evne til å møte digitale trusler gjennom utvikling av nasjonale kapabiliteter, flernasjonalt alliert samarbeid og støtte til Nato-prosesser for økt robusthet, utnyttelse av teknologiske muligheter samt evne til krisehåndtering. Samtidig skal vi **bidra til bevissthet om de dilemmaene og problemstillingene utviklingen av militære cyberkapasiteter stiller**, herunder spørsmål rundt rustningskontroll, eksportkontroll, avgrensning mellom statlige og ikke-statlige aktører og attribusjon.
- **Bidra i å utvikle forståelsen for hvordan folkeretten kommer til anvendelse i det digitale rom.** Det er enighet internasjonalt om at folkeretten også gjelder i det digitale rom, men det er fortsatt behov for større grad av internasjonal enighet rundt hvordan og når folkeretten kommer til anvendelse i det digitale domenet. Arbeidet i FNs mellomstatlige ekspertgruppe og Nato Cooperative Cyber Defence Centre of Excellence i Tallinn er viktig i så måte.

## *Global forvaltning av internett: Bidra til effektive, stabile og inkluderende strukturer*

Internett er en kompleks infrastruktur. Det finnes ingen overordnet aktør som styrer all infrastrukturen globalt. Det eksisterer heller ingen internasjonale bindende avtaler som regulerer hvordan nasjonalstatene skal håndtere spesifikke utfordringer knyttet til utvikling av internett. Det er imidlertid en stadig økende interesse for å få etablert prinsipper for god ressursforvaltning og administrasjon innenfor de verdensomspennende organisasjonene som sitter på nøkkelressursene på Internett og mellom relevante myndigheter. Både private aktører og myndigheter deltar i dette arbeidet som er viktig for å hindre at internett blir fragmentert og mister sin globale karakter.

God ressursforvaltning og prinsipper for styring og utvikling av internett - Internet Governance - blir derfor stadig viktigere. Tillit til at tjenestene som leveres over internett er stabile og sikre er grunnleggende for fortsatt utvikling av nett og tjenester. For å fremme en robust global forvaltning av internett som sikrer effektive, stabile og inkluderende strukturer vil regjeringen:

- **Bidra til å sikre internett som en åpen, tilgjengelig og robust plattform for vekst og sosial og kulturell utvikling.** Sammen med andre stater fremme en global internettpolitikk som stimulerer til innovasjon og utvikling av innhold, applikasjoner og tjenester. Norge skal delta aktivt på internasjonale arenaer med dette siktemålet.
- **Fremme prinsippet om rolleavklaringer.** I samarbeid med andre stater og næringsliv fremme prinsippet om at næringslivet i all hovedsak bør ha det operative ansvaret for drift og utvikling av internett, mens forvaltningen legges til det såkalte "Multistakeholder Community" som inkluderer både myndigheter, næringsliv, det sivile samfunn og akademia.
- **Fremme god forvaltning.** I samarbeid med andre stater søke å forbedre flerinteressent/multistakeholder-modellen samt vektlegge og fremme gode forvaltningsprinsipper som åpenhet, ansvarlighet, transparens, representativitet og habilitet i de organisasjoner som kontrollerer grunnleggende internettressurser.
- **Unngå unødig statlig inngripen.** Vi vil sammen med andre stater arbeide for å unngå at statlig regulering av internett bremser utvikling, innovasjon og kommunikasjon eller misbrukes til sensur eller propaganda.
- **Fremme åpenhet og frihet.** I samarbeid med andre stater arbeide for at internett også i fremtiden forblir en åpen og fritt tilgjengelig arena hvor enhver fritt kan gi og motta informasjon og hvor grunnleggende menneskerettigheter blir beskyttet. Internettforvaltning globalt eller nasjonalt kan aldri legitimere brudd på universelle rettigheter.

## *Utvikling: Tilgang til internett og utvikling av kapasitet for å utnytte det digitale roms potensiale for å fremme vekst, velstand og sikkerhet for alle*

Norge kan spille en viktig rolle globalt gjennom bistand til kapasitetsbygging på cyberfeltet i andre land og regioner i tråd med flere av FNs bærekraftsmål (Agenda 2030). Utviklingsland må i større grad gis mulighet til å dra nytte av mulighetene internett åpner for og samtidig evne å håndtere digitale utfordringer og digitale trusler.

For å få til dette vil regjeringen:

- **Fremme og støtte kapasitetsbygging innen cybersikkerhet i utviklingsland.** Kapasitetsbygging i denne forstand inkluderer institusjonsbygging, eksempelvis nasjonale telekommyndigheter og nasjonale CERT<sup>2</sup>, elektronisk myndighetsutøvelse (e-government), etterforskningskapasitet relatert til IKT-kriminalitet, utvikling av nasjonale lover for elektronisk kommunikasjon, innovative løsninger for bistand til helse og utdanning, utvikling av digital infrastruktur og etablering av varslingsystemer. Som del av dette arbeidet vil vi Intensivere samarbeidet og dialogen med EU om cyber kapasitetsbygging i land utenfor EØS-området.
- **Legge større vekt på robust infrastruktur og sikkerhet og åpenhet i det digitale rom som del av den bærekraftige utviklingsagendaen,** som del av regjeringens globale arbeid med fattigdomsbekjempelse, handel, sosial og økonomisk utvikling, utdanning, helse, samt menneskerettigheter og demokrati. Samtidig vil vi bidra til å oppnåelse av FNs bærekraftsmål om infrastruktur og innovasjon.
- **I samarbeid med internasjonale institusjoner arbeide for at flere utviklingsland i større grad skal kunne benytte de muligheter internettet gir for økonomisk og sosial utvikling,** herunder jobbskaping og tilgang til utdanning og helsetjenester. Det inkluderer å bistå utviklingsland med tilgang til internett, å styrke kompetansen og evnen til å forebygge, oppdage og håndtere digitale trusler, samt å bekjempe IKT-kriminalitet og ulovlig kapitalflyt ved hjelp av det digitale rom. Med dette bidrar vi også til oppnåelse av FNs bærekraftsmål om fredelige og inkluderende samfunn. Norge skal samarbeide med andre om å lukke gapet mellom kvinners og menns tilgang og bruk av internett, slik at kvinner få lik mulighet til økonomisk og politisk deltakelse i samfunnsutviklingen.

---

<sup>2</sup> CERT: Computer Emergency Response Team

## *Frihet på nett: Universelle rettigheter gjelder også online*

Norge skal bidra til at internasjonale menneskerettigheter respekteres i det globale digitale rom ved å:

- **Støtte aktører som gjennom det digitale rom kjemper for ytringsfrihet.** I samarbeid med likesinnede stater og det sivile samfunn bidra til å opprettholde og utvikle plattformer som muliggjør frie ytringer og forsamlinger i det digitale rom.
- **Bidra til økt forståelse for betydningen av cybersikkerhet.** Sikre kommunikasjonsløsninger og cybersikkerhet er viktig for menneskerettighetsaktivister, journalister og andre som kan tenkes å bli overvåket som følge av sine meninger og ytringer.
- **Sammen med andre stater, næringslivet og andre ikke-statlige aktører arbeide for at flest mulig mennesker globalt har tilgang til et fritt og sikkert internett.** Blant annet gjennom fortsatt deltagelse og engasjement i *Freedom Online Coalition*.
- **Arbeide for å fremme global forståelse for betydningen av å sikre retten til privatliv i det digitale rom.** Det inkluderer å fremme prinsippet om lovmessig forankret og forholdsmessig overvåking.

Utgitt av:  
Utenriksdepartementet

Offentlige institusjoner kan bestille flere eksemplarer fra:  
Departementenes sikkerhets- og serviceorganisasjon  
Internett: [www.publikasjoner.dep.no](http://www.publikasjoner.dep.no)  
E-post: [publikasjonsbestilling@dss.dep.no](mailto:publikasjonsbestilling@dss.dep.no)  
Telefon: 222 40 000  
Publikasjonskode: E-969 B  
Forsidefoto: Scanpix/Shutterstock  
Trykk: Departementenes sikkerhets- og serviceorganisasjon  
09/2017 – opplag 200

