



**Ukraina  
Situasjons - og risikobilde  
Mars 2022**

## **Politiets formål:**

Å gi en orientering om og momenter til refleksjon, kvalitetssikring og forebygging av mulige sårbarheter i egen virksomhet knyttet til krigen i Ukraina.

## **Situasjonsbilde:**

Den sikkerhetspolitiske situasjonen i Europa fremstår som utfordrende, og det er uavklart hvordan situasjonen vil påvirke Norge og norske interesser.

Noe representerer likevel en forhøyet risiko er i denne sammenheng, og man anmoder om at man er særlig oppmerksom på:

- Nye nettverksoperasjoner vil sannsynligvis ramme norske mål i året som kommer. Virksomheter knyttet til forsvar, beredskap, politikkutforming eller teknologi hvor Norge er langt fremme, vil være særlig utsatt.
- Russiske etterretningsoffiserer vil fortsatt forsøke å rekruttere kilder og kontakter som har tilgang til informasjonen de søker.
- Norsk næringsliv og norske kunnskapsmiljøer vil oppleve fordekte anskaffelsesforsøk fra aktører involvert i militær modernisering og opprustning. Aktører knyttet til Russland, Kina, Iran og Pakistan vil representere en særskilt utfordring.

## **Videre vil man tillate seg å anmode om at man retter oppmerksomheten mot følgende risiko:**

- Vis ekstra varsomhet overfor samarbeidspartnere og virksomheter fra land som Norge ikke er alliert eller har sikkerhetspolitisk samarbeid med. Anbefalt litteraturer er trusselvurderinger for 2022 fra PST, ETJ og NSM.
- Bedriftene anbefales å tilpasse seg risikobildet og spesielt være oppmerksom på økt risiko for digitale trusler. Eksempler, økonomisk svindel, sabotasje eller kartlegging for fremtidige operasjoner
- For næringslivet i Nordland er politiet ikke kjent med at det foreligger en konkret risiko for målrettede angrep, men næringslivet kan rammes via samarbeidspartnere og/eller underleverandører.
- Forsvarlig digital grunnmur kreves, jfr. NSM grunnprinsipper for cybersikkerhet. Kontakt IT-leverandør.
- Datatilsynet advarer om økt risiko for nettverksangrep. Man bør ta ekstra forholdsregler knyttet til informasjonssikkerhet, personopplysninger, datasikkerhet på tjenestereiser og private reiser der man bruker datautstyr med tilgang til bedriften.
- Oppdaterte beredskapsplaner, tiltak: fysisk sikring og digitale angrep. Tåler bedriften dataavbrudd?

- Vestlige sanksjoner vil få en omfattende innflytelse på næringslivet. Dette forsterkes av vestlige selv-sanksjonering. Videre må man være forberedt på mot-sanksjonering fra russisk side.
- Flyktningstrømmen er på gang. I migrasjonskriser vil man risikere at andre nasjonaliteter blande seg i asylstrømmen for å komme inn til Europa på uriktig grunnlag. Videre er flyktingene sårbare for å bli utsatt for ulike former for arbeidslivskriminalitet etter at de har ankommet til Norge.
- Politiet og PST følger situasjonen i Europa nøye og vurderer løpende betydningen for den sivile beredskapen.

## **Forslag til tiltak:**

- Gjennomgå og styrke IKT sikkerheten i organisasjonen/bedriften/kommunen.
- Gjennomgå og styrke personell- og informasjonssikkerheten i organisasjonen/bedriften/kommunen.
- Lav terskel for å melde fra til politiet om mistenkelige hendelser og personer.
- Være spesielt årvåken mot personer som etterspør sensitiv informasjon uten legitim grunn.
- Bygg sikkerhets- og samarbeidskultur både internt og med samarbeidspartnere.
- Ikke stå alene, diskuter med dine samarbeidspartnere og bransjeorganisasjon.

Vi står nå i en spesiell situasjon, og da er det godt å vite at vi med forholdsvis enkle grep kan redusere sårbarheten for både virksomheten og samfunnet. Lykke til.

## **Politiet i Nordland er tilgjengelig, og kan kontaktes på:**

Nordland politidistrikt, tlf. 02800, 75 58 90 00 eller [post.nordland@politiet.no](mailto:post.nordland@politiet.no)

Næringslivskontakten, tlf. 918 83 382 eller [havard.fjarli@politiet.no](mailto:havard.fjarli@politiet.no)

**Ukraina – situasjon og risikobilde**

Utgitt: mars 2022

Utgiver: Nordland politidistrikt