


# Konflikten mellom Russland og Ukraina – sikkerhet i et næringslivsperspektiv



NHO webinar 9. mars 2022  
Odin Johannessen

# Uoversiktlige utfordringer og usikkerhet fører til økt risiko generelt og innenfor noen områder spesielt:

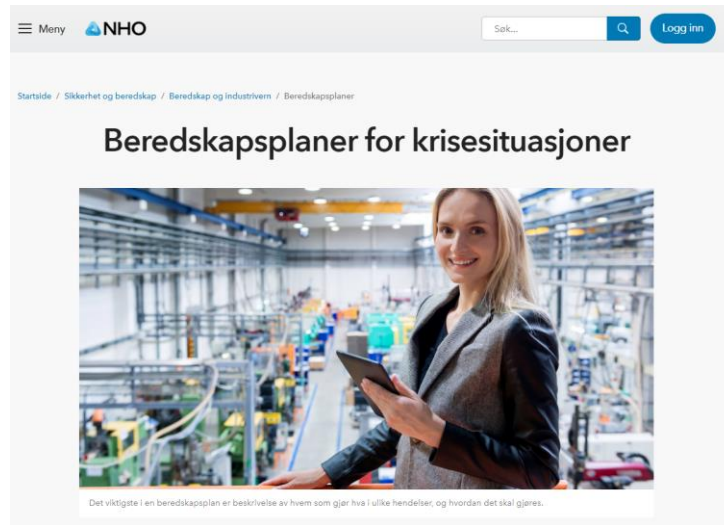
- Makro:
  - Verdier vs. pragmatisme – sanksjoner og viljen til å etterleve disse – treffer de som intendert?
  - Råvaretilgang – økte priser på mat, energi, råvarer – sosial uro?
  - Konkurransen om knapphetsgoder - økt sannsynlighet for konflikt (vann, energi, metaller, korn)?
  - Økt prisstigning – økt sosial uro – mindre stabile samfunn/markeder?
  - Økt press på enigheten blant allierte - sanksjonene rammer ulikt internt i hvert land?
  - **Digitale nettverk – ramme med effekt uten attribusjon – lav risiko!**
  - **Cybersikkerhet – IT – OT - høy effekt – lav risiko?**
  - **Demokratiets kår – falske nyheter og konspirasjonsteorier – utfordrer samhold og tillit!**
- Mikro:
  - **Økt risiko knyttet til digital kriminalitet – verdikjeden - lav risiko – høy fortjeneste**
  - **Økt risiko for spionasje – får ikke kjøpe – må ha det likevel!**
  - **Økt risiko for sabotasje – hvordan påvirke et liberalt demokrati?**
  - **Økt risiko for å bli rammet av sanksjoner – verdikjeder og sårbarheter.**
  - **Økt risiko for mangel på kompetanse – digitalisering og digital kompetanse.**



Foto: NYTimes

# Tiltak som kan redusere digital risiko:

- Makro:
  - Evne til geopolitisk analyse – identifisere flaskehalser og håndtere risiko – dele med næringslivet.
  - **Evne til nasjonalt forsvar av digitalt nettverk styrkes gjennom samarbeid nasjonalt og internasjonalt.**
- Mikro:
  - **Beredskapsplaner herunder styrket fokus på digital sikkerhet i eget nettverk og i verdikjeden – IT og OT**
  - **Personellsikkerhet** – alle ansatte - hele ansettelsesforholdet – håndtere risiko.
  - **Kompetanse** sikkerhet og kompetanseutvikling – utvikle og beholde.



## Beredskapsplaner må inneholde :

- Hvem som skal varsles?
- Hva skal iverksettes av tiltak?
- Hvem har ansvar for iverksetting og samordning (ledelse) av tiltakene?
- Hvem skal bidra og hvilket materiell og utstyr skal benyttes (f.eks. verneutstyr)?
- Hvilke rutiner gjelder for bistand/samvirke?
- Andre relevante faktorer avhengig av virksomhet og hendelse.

## Sårbarhetsreducerende tiltak kan være:

- Sikkerhetskultur
- Sterke passord
- To-faktorpålogging
- Sikkerhetsovervåking
- Logiske tiltak

## Håndtering av rest-risiko (ikke uttømmende):

- Ekstern backup
- Beredskapsplaner
- Segregering (IT - OT)
- Reserveløsninger
- Beredskapsavtaler

Last ned her: <https://www.nsr-org.no/aktuelt/nodplakat>

Løpene: Oppstart 14. januar 2023

# NØDPLAKAT FOR DIGITALE ANGREP

## VARSLER

Varsle ICT driftsorganisasjon, og mobiliser beredskapsorganisasjon i egen virksomhet.

### 23 20 80 00

Varsle politiets nasjonale cybersikkerhetscenter (NCS) via den dagdrøne skranken til Kripos. Dette varselet er egnet for innmeldelse, men NCS ønsker å få tilstrekkelig informasjon tidlig, uavhengig av om saken er anmeldt eller ikke.

## HÅNTERER

Be om akutt bistand fra leverandører som tilbyr tjenester for håndtering av dataangrep. Disse har dagdrøne alarmtelefoner. Se liste over til høyre. Inneholdt råd om umiddelbare tiltak, og verksett dette.

Gi gjernne hendelse/håndteringsleverandøren fullmakt til å ha direkte kontakt med myndighetene (NCS/NCCSC), og å dele relevante informasjon med disse fortløpende.

### 02800

Anmeld saken til lokalt politidistrikt. Hvis du lokalt politi til eventuell fortløpende kontakt med NCS/NCCSC.

Politiet kan også fiseses om forhold, dersom man ikke ønsker å innmelde. Les mer om anmeldelse og tips til politiet om datakriminalitet ved å scanne QR-koden, eller besøk <https://www.politiet.no/rad/datakriminalitet> og -bedrageri

Politiets næringslivskontakter har ingen operativ funksjon ved hendelser, men kan bistå med råd og veiledning.

## GJENOPPRETTE

Verksett beredskapsplaner for neddrift. Etter et dataangrep kan det ta mange uker å gjenopprette normal drift, så det er viktig å utvikle alternative driftsmodeller tidlig.

Godkjente leverandører: Leverandørene under her dagdrøne alarmtelefoner for håndtering av dataangrep, og er godkjent av NSM i henhold til deres kvalitetskrav.

**Defendable**  
91 80 80 30  
post@defendable.no

**mnemonic**  
23 20 47 41  
23 20 28 25  
mr@mnemonic.no

**ATGA**  
03060  
it@atga.no

**Netsecurity**  
92 24 73 65  
it@netsecurity.no

**sopra steria**  
24 14 04 56  
no.it@soprasteria.com

Vil gjerne oppmerksom på at flere andre aktører tilbyr tilsvarende tjenester, slik som de ikke er nevnt på den tidligere kvalitetsvurderingen til NSM.

### Politiets næringslivskontakter:

Oslokriv:	Torstein Edset	96 75 964	torstein.edset@politiet.no
Kripos:	Vakant		
Oslo PD:	Christina T. Booth	434 34 545	christina.booth@politiet.no
Aglia PD:	Jani Kåre Erikson	959 46 303	j.eriksen@politiet.no
Sør Øst PD:	Kyrre Lindanger	996 71 726	kyrre.lindanger@politiet.no
Vest PD:	Sorja Lund	924 97 728	Sorja.Lund@politiet.no
Tromsø PD:	Terje Lunde	481 61 669	terje.lunde@politiet.no
Møre og Romand PD:	Merethe Samuelsen	915 17 939	merethe.samuelsen@politiet.no
Nordland PD:	Iggil Arne Hestad	926 06 045	hestad@politiet.no
Øst PD:	Håvard Færø	918 83 282	havard.farero@politiet.no
Trøndelag PD:	Jani Kevin Brunvoll	976 77 266	jani.kevin.brunvoll@politiet.no
Finnmark PD:	Lene Espelund	958 99 554	Lene.Espelund@politiet.no
	Jani Arne Pettersen	900 95 960	jani.arne.pettersen@politiet.no

Næringslivets sikkerhetsråd er stiftet av Finans Norge, NHO, Virke, Spekter, Rederiforbundet og Den Norske Krigsforbund for skibs- og bærer kontinuerlig med å kartlegge, forny og og belønne tilknyttede sikkerhetsaktører mot norsk næringsliv. Se våre nettsider [www.nsr-org.no](https://www.nsr-org.no) for flere detaljer.

Plakaten er utarbeidet i samarbeid med

**POLITIET**  
NASJONAL  
Sikkerhetsmyndigheten



**Takk for  
oppmerksomheten**