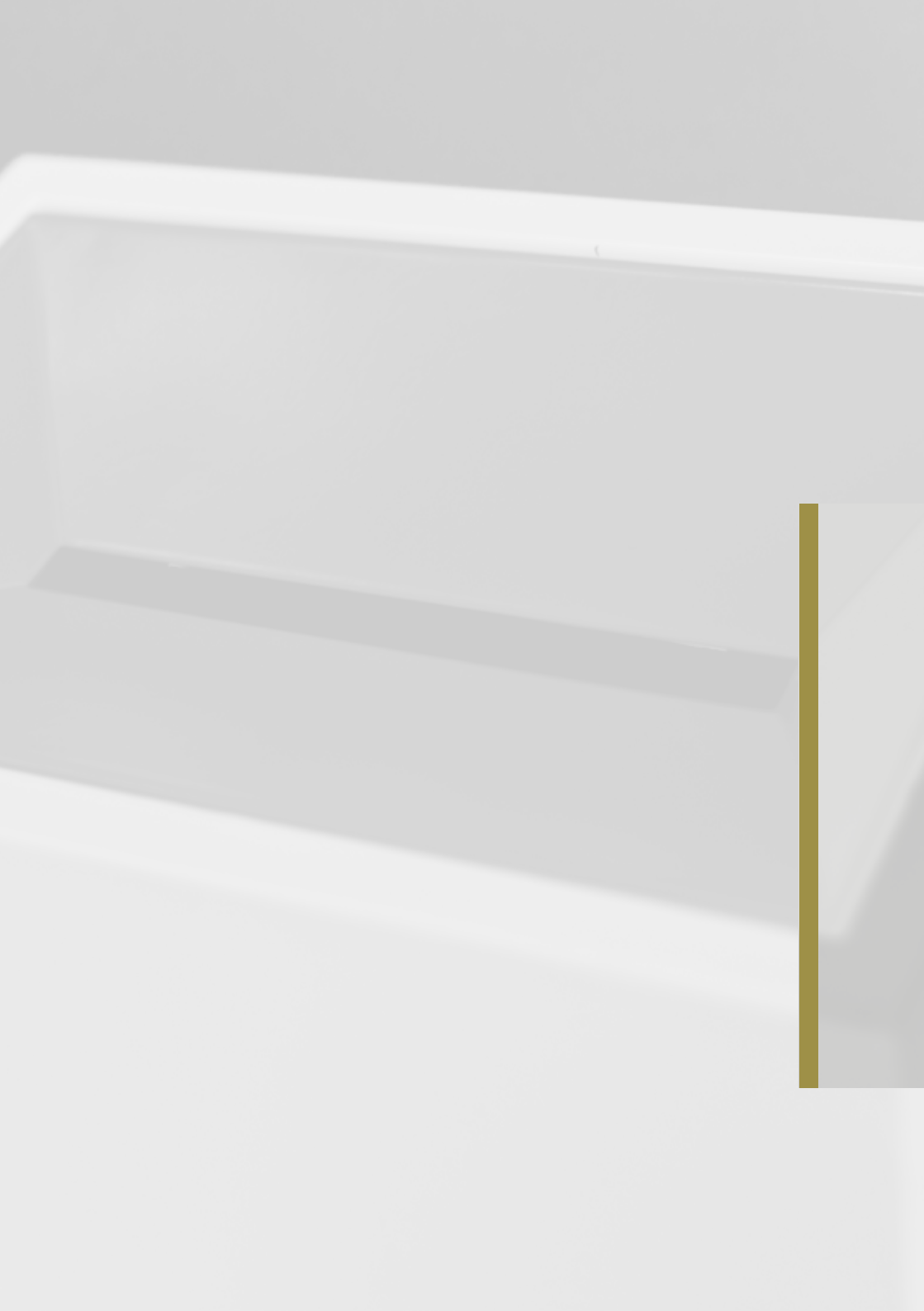
VAL

Nynorsk

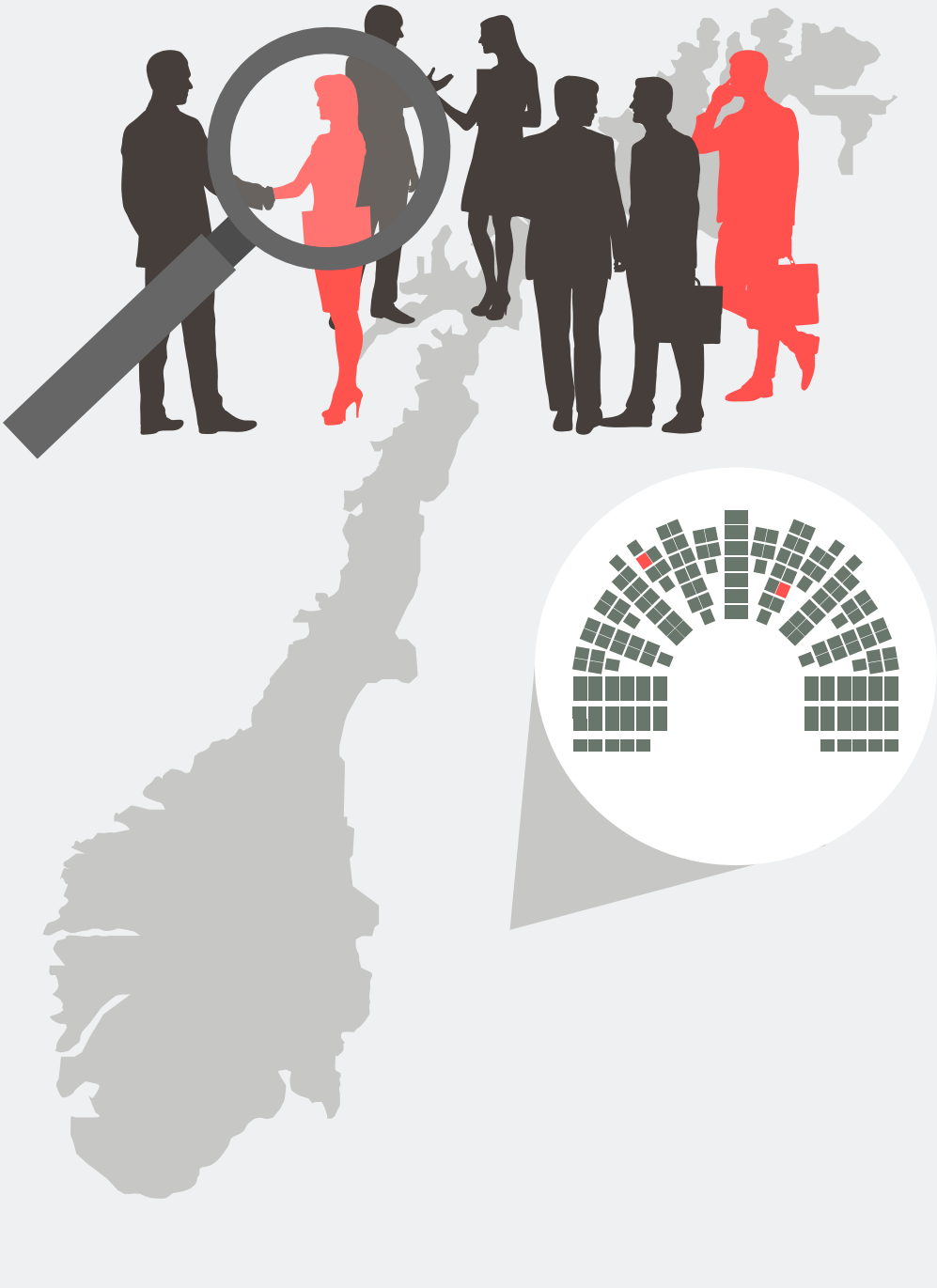
Du er av interesse –

Gode råd til deg som stiller til val

Utarbeidd av
Etterretningstenesta,
Nasjonalt tryggingsorgan
og Politiets
tryggingsteneste



Innhald



Noreg – eit tillitsbasert samfunn

Det siste året har det vore auka merksemd rundt faren for at framande statar prøver å påverke politiske prosessar i andre land. Påverknad kan i denne konteksta definerast som ein utanlandsk, statleg initiert, fordekt og tilsikta aktivitet for å oppnå eit mål som på kort eller lang sikt kan svekkje norske interesser til fordel for ein annan stat. Slik påverknad kan rettast mot valsystemet og gjennomføringa av valet, mot politiske aktørar eller mot veljarane og haldningar i befolkninga.

Vi har eit velfungerande og stabilt demokratisk system og eit samfunn prega av openheit. Det bidreg til å gjere både institusjonane og enkeltpersonar med politiske verv robuste. Noreg har dermed eit godt utgangspunkt for å stå imot forsøk på slik påverknad av innanrikspolitiske prosessar. Samstundes skal vi ikkje vere naive.

Framande statar kan søkje informasjon om og påverke norske politikarar, politiske prosessar eller forhold. Her kan kvar og ein av oss bidra til å sikre sensitiv informasjon om oss sjølv og om politiske prosessar og dessutan bidra til å handtere eventuell slik påverknad.

Informasjonen din – ansvaret ditt

Du må sjølv bidra til å beskytte eigen informasjon og dei verktøya du bruker for å kommunisere. Kva du sjølv gjer har betydning for din eigen integritet og evna til å kommunisere trygt og sikkert. Det er viktig at du har kunnskap om korleis du kan handtere situasjonar som kan innebere risiko. Dette kan vere situasjonar knytte til menneskelege relasjonar og bruk av digitale verktøy.

Du er av interesse

Etterretningstenestene til framande statar driv målretta operasjonar i Noreg – særleg der ein har motstridande eller konkurrerande interesser. Som politikar betyr det at du må rekne med at etterretningstenestene til framande statar kan vere interesserte i deg som eit ledd i verksemda si. For å nå måla sine bruker dei både opne og skjulte metodar. Detaljert kunnskap om deg, både som privatperson og politikar, kan ha høg verdi. Etterretningstenestene er dyktige til å skape relasjonar mellom menneske,

blant anna gjennom hyggjelege og naturlege møte. Noko så tilsynelatande banalt som kontaktlista di på telefonen kan interessere etterretningstenester. Seinare kan denne relasjonen utnyttast negativt.

FALSK E-POST

Det blir stadig sendt ut e-post som gir seg ut for å kome frå kjende selskap, til dømes kan det sjå ut som om det blir sendt ut ein faktura. I nokre tilfelle vil det installerast skadevare på maskina viss du klikkar på ei lenkje eller opnar vedlegg, medan i andre tilfelle er dei ute etter å skaffe seg informasjon om deg, til dømes påloggingsinformasjon og annan informasjon som kan utnyttast vidare.

MENNESKELEG TILNÆRMING

Ein norsk politikar kjem i snakk med ein diplomat, ein delegasjonsmedlem eller ein næringsdrivande. Seinare blir politikaren invitert på lunsj. Lunsjen blir opp følgd med fleire møte over ein lengre periode. Politikaren blir beden om informasjon om andre i partiet eller i eit konkurrerande parti. Det kan vere av personleg karakter eller jobbrelatert. Vedkomande ber òg politikaren leggje til rette for møte med leiinga i partiet eller med andre interessante partar. Utanlandske aktørar som nemnt i dømet kan vere knytte til eller utnytta av etterretningstenesta i landet. Dette er ein vanleg måte å operere på i Noreg.

Sårbarheiter blir utnytta

Framande statar prøver kontinuerleg å ta seg inn i datasystem for å hente ut informasjon eller ta kontroll over system. Sentralt i slike verkemiddel står ofte såkalla innsidarar. Dette er personar som allereie har ein lovleg tilgang til informasjonen og systema. Det å lure menneske til å skaffe seg slik tilgang er noko som skjer dagleg.

Den enklaste metoden for å ta seg inn i datasystem er å få mottakarar av e-postar til å opne vedlegg eller lenkjer som startar det teknologiske angrepet. Kunnskap om til dømes sensitiv og privat informasjon eller politiske standpunkt kan utnyttast.

Kjenn verdiane dine

Vit kva som er sensitiv informasjon for deg og partiet ditt

- Kva informasjon har den største verdien og den mest alvorlege konsekvensen viss andre fekk tilgang?
- Kven kan du dele slik informasjon med, og kven skal han ikkje delast med?

Behandle sensitiv informasjon med varsemd

- Tenk over kva du seier og kven som lyttar – både på telefon og i det offentlege rommet.
- Forsikre deg om identiteten til dei du kommuniserer med.
- Enkelte tema eller saker bør ikkje diskuterast på telefon eller sendast via vanleg e-post eller SMS.
- Når noko er sensitivt, bør møte bli gjennomførte utan PC, mobil, og smartklokker til stades.
- Bruk krypteringsløysingar for elektronisk kommunikasjon.

Beskytt eigen mobiltelefon, nettbrett og PC

- Ikkje lån bort det elektroniske utstyret ditt til andre.
- Hald elektronisk utstyr oppdatert med siste versjon av programvara.
- Ikkje gi andre tilgang til PC-en din, mobiltelefonen din, minnepinnane dine eller anna elektronisk utstyr.

Beskytt dei digitale tenestene dine

- Bruk fleirfaktorautentisering (bruk av passord i kombinasjon med SMS, kodebrikke eller liknande) der det blir tilbode.
- Bruk ulike passord for kvar teneste.

E-post

- Ver kritisk til lenkjer og vedlegg i e-post som du får.
- Er du uviss på om du bør opne eit vedlegg eller ein link, vurder om det er strengt nødvendig.
- Ta kontakt med avsendar via telefon/anna om du er i tvil.
- Gjer gjerne eit internettsøk på informasjonen utan å opne lenkja/vedlegget.
- Rapporter mistenkjelege e-postar til eigen partiorganisasjon, tillitsvald for lista di eller arbeidsgivaren din.

Sosiale medium

- Bruk personverninnstillingane til å beskytte tilgang og synlegheit etter behovet ditt.
- Ver medviten om kva du legg ut om deg sjølv og andre.
- Ver kritisk til det som kan vere falske nyheiter – unngå å spreie vidare.
- Slå av informasjon om kvar du er om du absolutt ikkje treng å bruke det.
- Sei frå til andre at du ikkje ønskjer at dei skal tagge/merkje deg på sosiale medium.
- Søk om verifisering av Twitter-kontoar og andre tilsvarande tenester som tilbyr dette. Det aukar truverdet til kontoen betrakteleg. Hugs å nytte eit svært sterkt passord.

På reise

- Unngå å kople deg opp til offentlege trådlause nett. Bruk mobildata eller mobilt breiband.
- Dersom du reiser til utsette land, bør du ikkje ta med den vanlege mobiltelefonen din, PC-en din eller nettbrettet ditt. Dette er til dømes land som Noreg ikkje har tryggingspolitisk samarbeid med.

Når bør du be om rådgivning?

Ta kontakt med partiorganisasjonen din, tillitsvald eller arbeidsgivaren din om du skulle oppleve hendingar som

- mottak av e-postar som er mistenkjelege
- tekniske irregularitetar i digitalt utstyr
- tap av mobiltelefon, PC og nettbrett
- tap av sensitiv informasjon
- målretta tilnærming
- misbruk av profilane dine i sosiale medium
- spreiing av falsk informasjon

Dersom du trur du er utsett for eit digitalt angrep, påverknad eller tilnærming frå framande statar, bør du så raskt som mogleg informere og diskutere saka med den næraste leiaren din. Om du framleis er bekymra?

Ta kontakt med relevante styresmakter som Politiets tryggingsteneste (PST), Nasjonalt tryggingsorgan (NSM) eller lokalt politi.

MISTENKJELEG E-POST

- Sjekk om avsendaren er riktig. Døme: feilstava, sluttar på .com i staden for .no, bruker gmail eller yahoo i staden for jobb-e-post.
- Viss du kjenner avsendar, men er uviss – ring vedkomande og sjekk om dei faktisk har sendt deg noko.
- Er det for godt til å vere sant, så er det gjerne det – bruk sunn fornuft!

Denne brosjyren er utarbeidd av Etterretningstenesta, Nasjonalt tryggingsorgan og Politiets tryggingsteneste på oppdrag frå Forsvarsdepartementet og Justis- og beredskapsdepartementet, koordinert og finansiert av Kommunal- og moderniseringsdepartementet.