

# Metoderapport til SKUP 2026

## «Den russiske forbindelsen»

### 1. Innsendere

**Mediehus:** Gjengangeren og Nettavisen i samarbeid med NRK Vestfold Telemark.

#### **Journalister:**

- Kjetil Stormark (Gjengangeren)
- Tormod Malvin Sæther (Nettavisen)
- Erik Andreassen (NRK Vestfold Telemark)
- Lars-Christian A. Lofstad (Gjengangeren)
- Morten Rød (reportasjeleder, NRK)
- Ståle Hansen (NRK)

#### **Redaktører:**

- Torgeir Lorentzen, Gjengangeren
- Charlotte Sundberg Østby, Nettavisen
- Kristin Monstad, NRK Vestfold Telemark
- Kathrine Strøm, setteredaktør NRK i saker vedrørende PST

#### **Djervlens advokater / redaksjonelle revisorer:**

- Stig Finslo, Amedia
- Per Arne Kallbakk, NRK

#### **Prosjektkoordinatorer/rådgivere:**

- Richard Aune, redaksjonssjef NRK Vestfold/Telemark
- Lars Kristiansen, gravesjef NRK
- Erik H. Sønstelie, gravesjef Amedia

#### **Fotografer/illustratører (utvalg):**

- Sigrid Moe (illustratør, Nettavisen)
- Lars Tore Endresen (fotograf, NRK)
- Håvard Hjorthaug Vege (fotograf, Nettavisen)
- Philip Hofgaard (fotograf, NRK)
- Oskar Rennedal (fotograf, NRK)
- Arne Frank Solheim (fotograf, NRK)

**Finansiering:** Prosjektet er finansiert av mediehusene og med støtte fra Amedias Gravefond.

**Spørsmål om prosjektet:** Kan rettes til en av redaktørene.

## 2. Sammendrag / oppsummering

Prosjektet startet januar 2025. Målet var å undersøke om det private selskapet Vissim AS i Horten hadde brutt sikkerhetsloven, ved å bruke russiske utviklere til å utvikle graderte systemer for Forsvaret og de norske spesialstyrkene. Dersom dette stemte, var neste spørsmål om russiske myndigheter kunne ha fått innsyn i norske hemmeligheter på en måte som har betydning for rikets sikkerhet.

Teamet definerte tidlig en minimums- og maksimumshistorie. Minimumshistorien var at militære eksperter mener det kan sette rikets sikkerhet i fare at Vissim har brukt russiske utviklere til å utvikle systemer for Forsvaret og Equinor. Maksimumshistorien var mer dramatisk: at russiske spioner kunne ha bygget inn bakdører som ga innsyn i eller kontroll over kritiske systemer. Ut fra sakens kompleksitet og tiden til rådighet valgte vi å prioritere minimumshistorien, samtidig som vi la en plan som ikke ødela for muligheten til å etterprøve maksimumssporet.

Gjennom publiseringer 3. juni og 18. juni 2025 avdekket Gjengangeren, Nettavisen og NRK følgende hovedforhold:

- I 15 år hadde det norske Forsvaret et tett samarbeid med Vissim om utvikling og leveranser av samband- og kommunikasjonssystemet som Sjøforsvaret og andre deler av Forsvaret benytter. Vesentlige deler av systemene ble i realiteten utviklet ved en avdeling firmaet hadde i St. Petersburg, og russere i Norge har vært involvert i utviklingsarbeidet.
- Equinor har siden 1997 kjøpt programvareløsninger utviklet av Vissim, som i perioden 2003–2023 hadde egen utviklingsavdeling i St. Petersburg. I 2018 fikk selskapet blant annet en kontrakt på 100 millioner kroner for å levere løsninger for overvåking av sikkerheten på olje- og gassinstallasjoner på norsk sokkel.

Prosjektet fant ikke grunnlag for å publisere at systemene var kompromittert av russisk etterretning, eller at russiske myndigheter faktisk hadde fått innsyn i graderte hemmeligheter via konkrete «bakdører». Arbeidet etterlot likevel vesentlige spørsmål om risiko, sårbarhet og myndighetenes håndtering av bekymringsmeldinger og sikkerhetsvurderinger gjennom årene.

Arbeidet reiste grunnleggende spørsmål om hvordan norske myndigheter og store samfunnsaktører har vurdert risiko knyttet til utvikling av sikkerhetskritiske systemer i Russland, og om disse vurderingene er tilpasset dagens sikkerhetspolitiske situasjon.

### **3. Bakgrunn: Slik kom arbeidet i gang**

Allerede i 2022 mottok frilanser Kjetil Stormark de første tipsene om mulig bruk av russiske utviklere i utvikling av systemer med betydning for norsk sikkerhet, knyttet til Vissim. I årene som fulgte gjennomførte han en rekke kildesamtaler og innledende research for å kartlegge påstandene nærmere. En sentral del av dette arbeidet var å bygge tillit, vurdere kildemotiver og forsøke å få tilgang til skriftlig dokumentasjon, samtidig som kildebeskyttelse var et gjennomgående hensyn.

Høsten 2024 ble funn, spor og problemstillinger samlet og presentert for Amedias gravesjef. Dette utløste arbeidet med å etablere et redaksjonelt samarbeid og løfte prosjektet inn i en større undersøkelse.

I denne fasen ble det utarbeidet et kortfattet notat som oppsummerte spor og påstander knyttet til mulige svakheter og sikkerhetsbrudd i marine- og sambandssystemer, samt mulig russisk involvering i utviklingsarbeid. Etter interne vurderinger ble det arbeidet videre med å finne en redaksjonell konstellasjon som kunne prioritere en kompleks og sensitiv sak.

NRK Vestfold Telemark ble med før jul 2024. Gjengangeren vurderte saken som viktig fordi selskapet lå i Horten og hadde lokal tilstedeværelse, samtidig som tematikken hadde nasjonal betydning. Nettavisen kom inn i prosjektet etter et møte 11. februar 2025.

### **4. Organisering og arbeidsform**

#### **4.1 Team og roller**

I januar 2025 ble Morten Rød fra gravegruppen NRK Sørøst satt inn som reportasjeleder. Det ble besluttet å engasjere Kjetil Stormark som frilanser, blant annet ut fra hans kjennskap til feltet og forarbeidet. Gjengangeren og NRK Vestfold Telemark stilte med reporter. Etter februar 2025 bidro også Nettavisen med reporter, og senere ble også illustratør og fotograf koblet på etter behov.

Kjerneteamet som jobbet kontinuerlig med saken besto i perioder av reportasjeleder og tre reportere, med støtte fra redaktører og graveledelse i de involverte mediehusene.

#### **4.2 Metodikk og struktur**

Ved oppstart ble det holdt forberedende møte (24. januar) og oppstartsverksted (28. januar), der roller, ansvar, sikkerhet, etikk, hypoteser, metoder, mulige kilder og fremdriftsplan ble avklart. Vi ble enige om å følge en verkstedbasert arbeidsform med oppstartsverksted, midtverksted og sluttverksted, og etablerte en felles mappestruktur for dokumentasjon, med dokumentoversikt og arbeidslogg.

#### **4.3 Sikkerhetstiltak**

På grunn av sakens karakter ble det gjennomført møter om sikkerhetstiltak. Vi valgte en forsiktighetslinje: nye private kontoer med alias, felles samarbeidsplattform i skyløsning, og

kryptert kommunikasjon via Signal. Sikkerhetsavdelinger i de involverte mediehusene fulgte ekstra med på utstyr for å avdekke mistenkelig aktivitet. Det ble ikke avdekket noe som tydet på kompromittering, men vi tok enkelthendelser på alvor og kontaktet sikkerhetsmiljø ved mistanke.

#### **4.4 Premortem**

Vi gjennomførte en premortem-øvelse for å identifisere hva som kunne få prosjektet til å havarere, og hvilke tiltak som kunne redusere risikoen. Formålet var å forebygge feil i en sak med stor konsekvensradius og betydelig risiko for pressetiske og juridiske fallgruver.

### **5. Hypoteser, minimum–maksimum og metodiske valg**

Ved oppstart arbeidet vi ut fra to hovedhypoteser:

1. Vissim har brukt russiske utviklere til å lage graderte systemer til Forsvaret og de norske spesialstyrkene, og dette ville etter 2022 være i strid med sikkerhetslovens intensjon og praksis.
2. Den russiske involveringen kan ha gitt russiske myndigheter mulighet til innsyn i norske hemmeligheter av betydning for rikets sikkerhet.

Som del av dette arbeidet tok vi kontakt med New York Times og Dossier Center for å få bistand til å sjekke russiske navn vi avdekket, blant annet med sikte på å avklare om noen var kjent i relevante miljøer eller registre.

### **6. Metoder, kilder og datainnsamling**

#### **6.1 Feltarbeid og observasjoner (identifisering)**

Vi la en plan for å identifisere russiske ansatte og dokumentere hvem som kunne knyttes til utviklingsarbeid. Det ble prøvd ulike kameraoppsett fra Gjengangerens lokaler i Horten. Vi fant en løsning der en fotograf satt i en privat bil med sotede vinduer. Hvis vi ble oppdaget, skulle vi presentere oss og forklare ærendet; vi skulle ikke lyve.

Ved ett tilfelle mente vi at vi ble oppdaget fra et vindu i kontorbygget. Etter dette besluttet redaktørene å stanse videre fotografering av ansatte som vi brukte til identifisering. I en periode kartla vi også biler parkert hos Vissim for å identifisere medarbeidere. Dette ga navn som senere ble undersøkt i databaser og åpne kilder.

#### **6.2 Innsynsbegjæringer og dokumentanalyse**

Vi gjorde systematiske søk etter relevante dokumenter i offentlig postjournal. Vi ventet i starten noe med innsyn, for at ulike aktører ikke skulle bli varslet om arbeidet vårt for tidlig. Vi brukte også Innsyn.no (Faktisk.no) for bedre søkefunksjonalitet og oversikt over tid, men

opplevde tekniske utfordringer knyttet til kommunikasjon med enkelte etater og innsending/mottak av meldinger.

### **6.3 OSINT og digitale verktøy**

Vi gjennomførte omfattende kartlegging av personer og selskaper gjennom:

- Norske kilder og registre (bl.a. folkeregisteropplysninger, telefon-/adresseregistre og brønnøysunddata)
- Sosiale medier og åpne nettkilder (LinkedIn, Facebook m.m.) og nettbaserte B2B-tjenester
- Russiske datakilder, herunder selskapsregistre, ved bruk av oversettelsesverktøy og VPN
- Russiske sosiale medier (VK m.m.)
- Wayback Machine for historisk innhold fra Vissims nettsider om russiske utviklere og avdelingskontor i Russland

I fase 2 brukte vi et spesialverktøy fra Osint Industries til å gjøre dypere kartlegging av digitale fotavtrykk. Metoden var iterativ: små funn (ny e-post, brukernavn eller telefonnummer) kunne gi grunnlag for nye søk og nye koblinger. Kartleggingen av hver enkelt person var tidkrevende, og i minst ett tilfelle avdekket vi flere parallelle online-identiteter knyttet til samme person.

### **6.4 Samarbeid med Dossier Center**

Dossier Center bidro til å kartlegge russiske borgere opp mot flere lukkede datakilder og databaser, blant annet russiske telefonregistre, folkeregisteropplysninger, passopplysninger (inkludert passnumre) og russiske firmaregistre. Det ble også gjort kartlegging av nær familie (ektefelle, foreldre, barn, søsken) for å se etter mulige direkte eller indirekte koblinger til russisk etterretning eller andre statlige myndigheter.

### **6.5 Kilder, bakgrunnssamtaler og intervjuer**

Vi satte opp lister over nåværende og tidligere ansatte, militære eksperter, forskere på sikkerhet og samfunnsberedskap, politikere og andre relevante kilder. Samtaler ble tatt opp og transkribert. Alt materiale ble samlet i en sikker arbeidsmappe med begrenset tilgang for team og nøkkelpersoner i prosjektet.

Vi konfronterte Equinor og Vissim løpende med funn for å få motforestillinger og avdekke feil eller misforståelser, men også for å hente nye opplysninger som kunne foredle researchen. Dette skapte frustrasjon hos de vi gransket, men bidro til kvalitet og til at berørte parter fikk god tid til å benytte sin rett til samtidig imøtegåelse.

Vi bygget ikke egne databaser eller kjørte automatiserte dataspøringer/skraping; det var ikke nødvendig gitt persongalleriets størrelse i prosjektet.

## 7. Kildekritikk, verifisering og kildehåndtering

Vi diskuterte motivene til sentrale kilder, særlig der opplysningene kom fra anonyme kilder med forbindelser til Vissim, Equinor eller Forsvaret. Et bærende prinsipp i verifiseringsarbeidet var at vi kun ville bruke opplysninger som var dokumentert skriftlig eller bekreftet av flere uavhengige kilder.

Vi vurderte også informasjon fra et privat sikkerhetsselskap anbefalt av en sikkerhetsekspert, og gjennomførte flere samtaler. Dette ble likevel tatt ut av publisert materiale fordi vi ikke kunne utelukke at selskapet kunne ha kommersielle interesser, eller at vi kunne bli kritisert for å gi en slik kilde definisjonsmakt.

Når saken utviklet seg og både funn og premisser endret seg, ble det nødvendig å kontakte kilder på nytt. Vi redegjorde for hva vi faktisk hadde avdekket, hva vi ikke hadde grunnlag for å publisere, og ga mulighet til å justere uttalelser gitt på et tidligere tidspunkt. Dette var viktig for at alle kilder skulle uttale seg på like premisser.

Kildevernet ble ivaretatt. I researchfasen ba Vissims daglige leder tidlig om å få vite hvilke kilder vi hadde, og forlangte navn på militære ekspertkilder. Vi oppga etter redaksjonell vurdering, og i forståelse med kildene, navnene på to ekspertkilder vi ønsket å bruke. Etterpå tok Vissim kontakt med dem, noe kildene reagerte negativt på. Vi opplevde også at andre forsøkte å kartlegge hvem som hadde snakket med oss. Dette skjerpet vår håndtering av kildepor og kildebeskyttelse.

## 8. Etske problemstillinger

Prosjektet reiste flere etiske avveininger som ble diskutert og håndtert løpende:

1. Belastning for enkeltpersoner og risiko for stempling  
De russiske ansatte som bodde i Horten med sine familier kunne bli utsatt for utilbørlig belastning. Det var ikke grunnlag for å hevde at enkeltansatte hadde gjort noe galt. Vi besluttet derfor tidlig at bilder av russiske ansatte på vei til og fra jobb ikke skulle benyttes, og vi valgte å rette hovedfokus mot det systemkritiske: hva systemene var, hvordan de var utviklet, og hvordan ansvarlige aktører vurderte risiko.
2. Habilitet og redaksjonelle roller  
En redaktørs habilitet ble vurdert ved to anledninger fordi hun var gift med PSTs sjef for deler av perioden vi gransket. Vi fulgte habilitetsspørsmålet tett. Da det ble relevant å kontakte PST-sjefen om opplysninger som dukket opp, flyttet vi all research knyttet til PST til setterredaktør, som et føre-var-tiltak.
3. Fremferd under identifiseringsarbeid  
I planleggingen diskuterte vi også metoder som kunne bli oppfattet som skjulte. I felt hadde vi en klar linje: hvis vi ble oppdaget, skulle vi presentere oss og forklare hva vi gjorde; vi skulle ikke lyve. Da vi mente vi kunne ha blitt oppdaget, stanset vi videre fotografering av ansatte.

## 9. Motstand, kvalitetssikring og endring av premiss

Vi møtte betydelig motstand og kritikk fra Vissim og Equinor. Flere aktører ønsket ikke å uttale seg, og deler av sakskomplekset inneholdt «sorte hull», blant annet knyttet til hva Forsvaret og sikkerhetsmyndigheter hadde gjort med bekymringsmeldinger.

Før publisering hadde vi avtale om juridisk rådgivning og gjennomgang av materiale med mediejussekspertise, og vi hadde også advokat til å lese siste versjon før publisering.

Som et bevisst metodisk grep besluttet redaktørene, etter reaksjoner fra berørte parter og eget kvalitetssikringsarbeid, å ta en time-out i april for en mer omfattende redaksjonell revisjon. Revisorene fikk tilgang til arbeidsmapper, arbeidslogger og dokumenter og gikk gjennom kildebredde, sitater, meningsinnhold og sakens klarhet.

Revisjonen avdekket at prosjektet hadde bygget på et narrativ som ikke lot seg verifisere fullt ut. Vi endret derfor grunnpremisset og gikk over til et strengere dokumentasjonskrav, der vi fokuserte på beviselig korrekte forhold og reduserte avhengigheten av anonyme enkeltkilder eller opplysninger som ikke kunne underbygges av flere. Vi gikk også en ny runde med sentrale kilder for å sikre like premisser.

Denne prosessen førte til endret fremdriftsplan og utsatt publisering. Under en senere «linje-for-linje»-gjennomgang ble publisering igjen stanset fordi vi oppdaget at Forsvaret etter redaksjonens vurdering ikke hadde fått samtidig imøtegåelse på enkelte spørsmål. Dette utløste ny runde før publisering.

Bruken av redaksjonelle revisorer som en integrert del av metoden var avgjørende i slutfasen. Den tvang fram en systematisk gjennomgang av premisser, dokumentasjon og kildebruk, og avdekket svakheter som gjorde at prosjektet ble omarbeidet før publisering. Metoden førte til utsatt publisering, men resulterte i et mer presist, bedre dokumentert og presseetisk tryggere sluttprodukt.

## 10. Publisering og formidling

Publiseringsstrategi ble diskutert tidlig i prosjektet. Samarbeidet mellom en abonnementsdrevet lokalavis, en åpen nettavis og NRK reiste spørsmål om åpenhet versus betalingsmur. Underveis ble det vurdert som viktig at sakene var allment tilgjengelige, fordi de handlet om nasjonal sikkerhet og kritisk infrastruktur. Sakene gikk derfor åpent i alle kanaler.

Begge hovedsakene ble publisert samtidig kl. 07.00 på nettsidene til Gjengangeren, Nettavisen og NRK Vestfold og Telemark, henholdsvis 3. juni og 18. juni 2025. Begge dagene ble publiseringene fulgt opp med større innslag i NRKs Nyhetsmorgen, videre dekning i NRKs løpende nyhetsflater og senere oppfølging i kveldsendingene.

I forkant av publisering laget redaksjonene en felles publiserings- og oppfølgingsplan og en felles FAQ for håndtering av forventet kritikk og spørsmål. Dette var et bevisst grep for å sikre samordnet formidling og ryddig, konsistent oppfølging av en kompleks og sensitiv sak.

## 11. Avsløringer, funn og avgrensninger

Prosjektet innfridde minimumskravene ... Vi fant heller ikke grunnlag for å publisere at systemet var kompromittert av russisk etterretning. Dette var et bevisst redaksjonelt resultat av revisjonsarbeidet og de skjerpede dokumentasjonskravene vi satte oss, og innebar en tydelig avgrensning bort fra påstander vi ikke kunne underbygge fullt ut.

Vi fikk bekreftet at flere av de russiske ansatte hadde bakgrunn og forbindelser til russisk forsvarsindustri. Vi kartla totalt 17 russiske statsborgere som hadde arbeidet for Vissim. Samtidig etterlot arbeidet seg nye spørsmål og hypoteser som det på tidspunktet for rapportskriving ikke var avklart om eller hvordan vi skulle gå videre med.

## 12. Konsekvenser (kjent status)

Publiseringene utløste politiske reaksjoner. Det kom krav om gjennomgang, risikovurderinger og gransking fra flere politikere. Flere tidligere forsvarssjefer ble intervjuet, og enkelte ga uttrykk for at de ville ha reagert dersom de hadde visst om russisk utviklerinvolvering i modernisering av kritiske systemer.

Per rapporttidspunkt var det ikke kjent at sakene hadde ført til konkrete endringer i politikk, praksis eller regelverk. Cyberforsvarets sjef har uttalt at systemet har hatt svakheter som er avdekket og lukket, men at taushetsregler hindrer detaljer. Vi hadde kilder som sa mer om dette, men vi hadde ikke tilstrekkelig faktagrunnlag til å publisere.

## 13. Dokumentasjon

Vi etablerte en felles mappestruktur for all dokumentasjon i prosjektet, med dokumentoversikt og arbeidslogg. Samtaler og intervjuer ble tatt opp og transkribert, og alt materiale ble samlet i en sikker arbeidsmappe med begrenset tilgang. Under revisjonsfasen fikk revisorene tilgang til arbeidsmapper og logger for å kunne etterprøve kildegrunnlag, sitater og arbeidsprosess.

## 14. Hva som er nytt metodisk (oppsummert)

Vi mener prosjektet har overføringsverdi på flere punkter:

1. Hypotese- og minimum/maksimum-styring som verktøy for å sikre publisierbarhet uten å miste mulige spor
2. Sikkerhetsopplegg i en sensitiv sak: alias, tilgangsstyring, kryptert kommunikasjon og sikkerhetsoppfølging
3. Iterativ OSINT som metode: små identitetsfunn som driver nye søk og nye koblinger
4. Redaksjonell revisjon som metode: stans, gjennomgang med full tilgang, endring av premiss og ny kilderunde før publisering

5. Etisk risikostyring i felt: stopp av identifiserende fotografering og bevisst valg om å vri fokus fra enkeltpersoner til systemkritikk

## 15. Læring

Prosjektet ga flere læringspunkter:

- Team og tidsrammer må være realistiske, og teamet bør settes etter kompetanse og kildenettverk
- Det er viktig å jobbe systematisk etter hypoteser og justere når hypoteser falsifiseres
- Mapestruktur, faste redaktørmøter, kildebredde og «djevlels advokater» er avgjørende
- Historiefortelling og visuell planlegging bør inn tidlig, men med riktig timing
- Det menneskelige i lange løp må ivaretas
- Manus bør være klare før linje-for-linje
- «Kill your darlings» for å sikre effektivitet og fremdrift

## 16. Vedlegg: publisert materiale

Vedlegget består av en fullstendig liste over publiseringer med tittel, dato og medium (inkludert publiseringene 03.06.2025 og 18.06.2025 i Gjengangeren, Nettavisen og NRK, samt relevante oppfølgingspubliseringer og innslag).

Dato	Tittel artikkel	Fil eller lenke til artikkel	Mediehuset
03.06.2025	Horten-firma utviklet forsvarssystemer - brukte russere	<a href="https://www.gjengangeren.no/forsvarsrets-russiske-forbindelse/f/5-60-1145574">https://www.gjengangeren.no/forsvarsrets-russiske-forbindelse/f/5-60-1145574</a>	Gjengangeren
03.06.2025	Redd Russland er på innsiden: - Det må ut	<a href="https://www.nettavisen.no/nyheter/forsvarets-russiske-forbindelse/f/5-95-2451752">https://www.nettavisen.no/nyheter/forsvarets-russiske-forbindelse/f/5-95-2451752</a>	Nettavisen
03.06.2025	Sikkerhetsskandalen må få konsekvenser	<a href="https://www.nettavisen.no/norsk-debatt/sikkerhetsskandalen-norske-militarhemmeligheter-utviklet-av-russere/s/5-95-2463637#am-comments">https://www.nettavisen.no/norsk-debatt/sikkerhetsskandalen-norske-militarhemmeligheter-utviklet-av-russere/s/5-95-2463637#am-comments</a>	Nettavisen

03.06.2025	Forsvarets russer-kobling: – Lett å få helt noia	<a href="https://www.nettavisen.no/nyheter/tidligere-forsvarssjef-lett-a-fa-helt-noia/s/5-95-2464305">https://www.nettavisen.no/nyheter/tidligere-forsvarssjef-lett-a-fa-helt-noia/s/5-95-2464305</a>	Nettavisen
03.06.2025	Krever gransking etter avsløring om Forsvaret: – Forventer ny vurdering	<a href="https://www.nettavisen.no/nyheter/krever-gransking-etter-avsloring-om-russisk-utvikling-av-forsvarets-sambandsystem/s/5-95-2464064">https://www.nettavisen.no/nyheter/krever-gransking-etter-avsloring-om-russisk-utvikling-av-forsvarets-sambandsystem/s/5-95-2464064</a>	
03.06.2025	Dagsrevyen - helt bakerst i sendingen	<a href="https://tv.nrk.no/serie/dagsrevyen/sesong/202506/episode/NNFA19060325">https://tv.nrk.no/serie/dagsrevyen/sesong/202506/episode/NNFA19060325</a>	NRK
03.06.2025	Kveldsnytt - forsvarssaken er nr 5	<a href="https://tv.nrk.no/serie/kveldsnytt/sesong/202506/episode/NNFA23060325">https://tv.nrk.no/serie/kveldsnytt/sesong/202506/episode/NNFA23060325</a>	NRK
04.06.2025	Ny sikkerhetsblemme av Forsvaret	<a href="https://www.adressa.no/debatt/i/LMBQ51/ny-sikkerhetsblemme-i-naive-norge">https://www.adressa.no/debatt/i/LMBQ51/ny-sikkerhetsblemme-i-naive-norge</a>	Adresseavisen
05.06.2025	EU-politiker: – Risiko for at norsk forsvarsteknologi er infiltrert	<a href="https://www.nettavisen.no/nyheter/eu-politiker-mika-altola-risiko-for-at-norsk-forsvarsteknologi-er-infiltrert/s/5-95-2466698">https://www.nettavisen.no/nyheter/eu-politiker-mika-altola-risiko-for-at-norsk-forsvarsteknologi-er-infiltrert/s/5-95-2466698</a>	
05.06.2025	Avsløring om Forsvarets russiske forbindelse: – Høy risiko for at det kan finnes en bakdør	<a href="https://www.nrk.no/vestfoldogtelemark/avsloring-om-forsvarets-russiske-forbindelse--ho-y-risiko-for-at-det-kan-finnes-en-bakdor-1.17443910">https://www.nrk.no/vestfoldogtelemark/avsloring-om-forsvarets-russiske-forbindelse--ho-y-risiko-for-at-det-kan-finnes-en-bakdor-1.17443910</a>	NRK Vestfold
11.06.2025	Tidligere forsvarssjef: – Jeg hadde reagert	<a href="https://www.nrk.no/vestfoldogtelemark/tidligere-forsvarssjef-bruun-hansen-kjente-ikke-til-russiske-utviklere-i-vissim-1.17450918">https://www.nrk.no/vestfoldogtelemark/tidligere-forsvarssjef-bruun-hansen-kjente-ikke-til-russiske-utviklere-i-vissim-1.17450918</a>	<a href="https://www.nrk.no">NRK.no</a>



