FFI Forsvarets forskningsinstitutt

25/003

FFI-RAPPORT

Valgpåvirkning i 2023 og 2024

– en trendstudie

Paul M. H. Buvarp
Eskil Grendahl Sivertsen

Valgpåvirkning i 2023 og 2024
– en trendstudie

Paul M. H. Buvarp
Eskil Grendahl Sivertsen

Forsvarets forskningsinstitutt (FFI) 21. januar 2025

Emneord
Påvirkningsoperasjoner
Desinformasjon
Digital påvirkning
Demokrati
Valg

FFI-rapport
25/003

Prosjektnummer
1582

Online ISSN
2704-2383

Engelsk tittel
Election Interference in 2023 and 2024 – A trend study

Godkjennere
Stig Rune Sellevåg, *forskningsleder*
Janet M. Blatny, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Denne rapporten sammenstiller litteratur og casestudier fra de seneste års påvirkningsforsøk for å beskrive hvordan valgpåvirkning arter seg i dag. Vi har brukt en rekke metoder og sikret et bredt og godt tilfang av litteratur til studien. Vi har lagt vekt på materialer publisert i hovedsak de seneste to år for å sikre rettidigheten av innholdet.

Vi finner at aktørene som er mest relevante i valgpåvirkning i dag, er Russland, Kina og Iran, selv om vi også ser en rekke andre internasjonale aktører som forsøker seg på dette feltet. I 2023 og 2024 ble det gjennomført mange valg globalt, og det har blitt rapportert flere tilfeller av forsøk på valgpåvirkning i Europa denne perioden. Taktikkene, teknikkene og fremgangsmåtene som benyttes, følger i takt med den teknologiske utviklingen, særlig innen bruk av nye plattformer og kunstig intelligens. Utviklingen av fremgangsmåtene peker også på en økende strategisk forståelse av hvordan man kan benytte informasjonspåvirkning for å oppnå mål. Aktørene integrerer i større grad informasjonspåvirkning med andre strategiske mål og virkemidler, og viser seg tilpasningsdyktige og opportunistiske.

Som casestudier beskriver vi a) påvirkning mot presidentvalget og EU-parlamentsvalget i Frankrike sommeren 2024, b) påvirkning mot OL i Paris i 2024, og c) den utbredte kinesiske påvirkningskampanjen Spamouflage Dragon. Disse casestudiene er valgt fordi de danner et bredt og tidsriktig bilde av påvirkning som rammer ulike typer valg og begivenheter som kan ha politiske ringvirkninger. I tillegg rommer disse flere metoder og fremgangsmåter som gir et mer helhetlig bilde av påvirkningsaktørers verktøykasse. Vi ser en økende grad av kompleksitet og tilpasningsdyktighet i alle tilfellene. Vi ser også en utbredt bruk av verktøy som er gjort mulig av kunstig intelligens, spesielt for å produsere troverdig innhold.

Den samlede analysen av litteraturen og casestudiene peker mot at fremtiden innen påvirkning vil preges av enda mer effektiv bruk av kunstig intelligens, som kan vise seg å utfordre nåtidens metoder for å avdekke desinformasjon. Fremtiden vil sannsynligvis også by på enda mer avanserte spredningsmetoder som utnytter en kombinasjon av menneskelige og automatiserte systemer, og bidrar til enda mer tilpasset målrettelse. Spesielt casestudiene indikerer at langsiktigheten og den strategiske forankringen av påvirkningsoperasjoner er i en styrkningsprosess. Samtidig blir det vanskeligere å tilegne seg data fra plattformer for sosiale medier, og viktige forsknings- og kontringsorganisasjoner er under sterkt politisk press, spesielt i USA. Vi gjennomgår også foreslåtte tiltak på tvers av mange spor: det teknologiske, regulatoriske, utdanningsrettede, journalistiske, beredskapsmessige og plattformspesifikke.

Vår konklusjon er at trusselen for valgpåvirkning er økende. Ikke bare ser vi bruk av valgpåvirkning mot mål i Europa, men aktørene ser ut til å bruke påvirkning mer strategisk, til å evne å bruke nye teknologier, og til å gjennomføre stadig mer komplekse operasjoner.

Summary

This report compiles literature and case studies from recent years' influence operations to describe how election interference manifests today. We have used a range of methods and ensured a broad selection of literature for the study. Emphasis has been placed on materials published within the past two years to ensure the content remains current and relevant.

We find that the actors most relevant to election influence and interference today are Russia, China, and Iran, although several other international actors are also active in this field. In 2023 and 2024, numerous elections were held globally. Several attempts at election interference in Europe have been observed during this period. The tactics, techniques, and procedures employed have evolved alongside technological advancements, particularly in the use of new platforms and artificial intelligence. These developments point to an increasing strategic understanding of how influence operations can be used to achieve objectives. The actors integrate to a greater degree than before the use of influence and disinformation together with other strategic aims and tools, and prove themselves adaptable and opportunistic.

As case studies, we describe: a) influence efforts targeting the presidential and European Parliament elections in France during the summer of 2024, b) influence operations aimed at the 2024 Paris Olympics, and c) the widespread Chinese influence campaign known as Spamouflage Dragon. These case studies were selected because they offer a broad and up-to-date perspective on influence operations affecting several types of elections and events that could have an impact on electoral outcomes. Moreover, they encompass multiple methods and approaches, offering a comprehensive view of the tools available to influence actors. In all cases, we observe increasing complexity and adaptability. Additionally, there is extensive use of tools enabled by artificial intelligence, particularly for producing credible content.

The combined analysis of the literature and case studies suggests that the future of influence operations will likely be characterised by even more effective use of artificial intelligence, potentially challenging current methods for detecting disinformation. The future is also expected to feature increasingly advanced dissemination methods that utilize a combination of human and autonomous systems,and contributes to more tailored targeting strategies. Notably, the case studies indicate that the long-term focus and strategic grounding of influence operations are becoming stronger. At the same time, access to data from social media platforms is becoming more restricted, and key research and countermeasure organisations are under significant political pressure, particularly in the United States. Our report also contains an overview of proposed measures from the literature across multiple fronts: technological, regulatory, educational, journalistic, preparedness, and platform-specific.

Our conclusion is that the threat of election interference is increasing. Not only do we observe influence operations targeting elections in Europe, but actors also appear to employ influence more strategically, leverage recent technologies effectively, and carry out increasingly complex operations.

Innhold

Forord

Denne rapporten er skrevet på oppdrag for Kommunal- og distriktsdepartementet (KDD) som en del av oppdraget med å kartlegge uønsket påvirkning i forbindelse med norske valg i perioden 2023 til og med 2025.

Hensikten med rapporten er å etablere et oppdatert kunnskapsgrunnlag om utviklingen av påvirkningsoperasjoner generelt, og i forbindelse med valg spesielt. Rapporten vil dermed bli viktig når vi skal vurdere hvilke analyser vi skal gjennomføre når vi skal kartlegge eventuell utenlandsk påvirkning i forbindelse med stortingsvalget i 2025.

Vi vil rette en stor takk til sommerstudent Astrid Utheim Aune, som bidro med mye og grundig grunnforskning som innspill til denne rapporten sommeren 2024.

Kjeller, 21. januar 2025
Paul Magnus Hjertvik Buvarp og Eskil Grendahl Sivertsen

1 Innledning

Denne rapporten skal gi en oppdatert oversikt over hvordan ulike aktører bruker sosiale medier og internett til å gjennomføre påvirkningsoperasjoner i forbindelse med valg.

Studien kartlegger de viktigste aktørene og deres målsettinger, i tillegg til taktikkene og virkemidlene de tar i bruk. Rapporten dekker spesielt perioden 2023 til og med desember 2024, selv om også publikasjoner fra tidligere år er tatt med for å bidra til en større kontekst. Perioden 2023–2024 kjennetegnes av både økt sikkerhetspolitisk spenning og utbredelsen av generativ kunstig intelligens (generativ KI). Rapporten har derfor et spesielt søkelys på betydningen av dette for påvirkningsoperasjoner.

Rapporten dreier seg hovedsakelig om valgpåvirkning, men påvirkningsoperasjoner i sin helhet er også av betydning. Det er viktig å merke seg at dette skillet ofte er komplekst og ikke alltid relevant fordi det kan være vanskelig å fastslå den faktiske intensjonen bak påvirkningsforsøk. Mange påvirkningsoperasjoner kan ha bredere samfunnsmessige mål som indirekte kan påvirke valg og demokratiske prosesser. Spesielt er dette viktig å påpeke med tanke på at 2024 var et stort valgår.[1]

Rapporten er strukturert for å gi en omfattende forståelse av påvirkningsoperasjoner og utviklingen de siste to årene. Den begynner med en gjennomgang av metodene for studien og noen vurderinger rundt disse i kapittel 2. I kapittel 3 redegjør vi for noen av de mest sentrale kildene brukt i rapporten. Kapittel 4 samler funnene, deriblant de viktigste påvirkningsaktørene, observasjoner fra nasjonale valg i Europa i 2023 og 2024, og påvirkningsoperasjoners taktikker, teknikker og fremgangsmåter. I kapittel 5 beskriver vi tre casestudier av påvirkningsoperasjoner i 2024. I kapittel 6 gjennomføres analysen, hvor vi behandler og syntetiserer funn fra litteraturen og casestudiene. I kapittel 7 går vi gjennom noen utvalgte trender og utviklinger vi ser for oss fremover. I kapittel 8 drøftes en rekke tiltak anbefalt av forskjellige kilder, og i kapittel 9 kommer vi med en oppsummering og konkluderende bemerkninger.

[1] EEAS (2024, januar). *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence*. European Union External Action Service. s. 4.

2 Metode

Studien kombinerer systematisk litteraturgjennomgang med casestudieanalyse for å kartlegge og analysere utviklingen innen valgpåvirkning og påvirkningsoperasjoner. For å sikre en strukturert og etterprøvbar analyse av påvirkningsoperasjoner benyttet vi ABCDE-rammeverket utviklet av James Pamment.[2]

2.1 Datainnsamling

Datainnsamlingen ble gjort gjennom strukturerte søk på engelsk og norsk (for å fange opp kilder direkte relevant for Norge) på Google og i akademiske søketjenester som Google Scholar og Oria, supplert med målrettede søk i rapporter fra sikkerhetstjenester og ledende analyseselskaper (se vedlegg A for søkeord). For å sikre bred dekning brukte vi snøballmetoden (*snowballing*) både forlengs og baklengs fra identifiserte nøkkelpublikasjoner. Som støtte i litteratursøket benyttet vi KI-verktøyene Perplexity og Elicit. Bruken av KI, og dessuten begrensninger, validitet og reliabilitet, beskrives senere i dette underkapittelet.

Utvalgskriterier

Kildematerialet ble valgt basert på et sett definerte kriterier for å sikre kvalitet og relevans. Primært inkluderte vi materiale publisert mellom 2022 og 2024 som direkte omhandler påvirkningsoperasjoner og valgpåvirkning. Kildene måtte komme fra etablerte aktører som statlige institusjoner, forskningsinstitusjoner eller anerkjente analyseselskaper (se vedlegg B). All litteratur måtte være enten fagfellevurdert eller grundig kvalitetssikret. Det siste er vanskelig å vite, og derfor benyttet vi bare kilder fra etablerte aktører som statlige institusjoner, forskningsinstitusjoner eller anerkjente analyseselskaper (se vedlegg B), som trolig holder høy kvalitet. Som supplement inkluderte vi også tekniske analyser av spesifikke operasjoner, relevante policydokumenter og empiriske studier av konkrete hendelser. Materiale med uklar metodikk, manglende dokumentasjon eller åpenbar politisk slagside ble ekskludert.

Bruk av KI-baserte språkmodeller

Vi benyttet anledningen denne studien ga, til å eksperimentere med bruk av kunstig intelligens i form av store språkmodeller (*large language models* – LLM-er) for å finne, sortere, systematisere, sammenstille og presentere informasjon.

Ifølge regjeringens nye digitaliseringsstrategi skal offentlig sektor anvende KI for å utvikle bedre tjenester og løse oppgaver mer effektivt, med mål om at alle statlige virksomheter skal bruke KI i sin oppgaveløsning innen 2030.[3] Videre setter strategien som ambisjon at Norge skal

[2] Pamment, J. (2020, september). *The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework.* Carnegie Endowment for International Peace (Working Paper).
[3] Digitaliserings- og forvaltningsdepartementet (2024). *Fremtidens digitale Norge: Nasjonal digitaliseringsstrategi 2024-2030.*

være ledende på verdiskaping med data og på datadrevet forskning.[4] FFI skal ligge i forkant av utviklingen, og vi har derfor eksperimentert med å bruke KI-baserte språkmodeller i arbeidet for å opparbeide oss kunnskap og erfaring. I dette har vi sett til Europakommisjonens anbefalinger om hvordan KI kan brukes til vitenskapelige forskningsformål.[5]

Vi gjorde forsøk på bruk av et utvalg av de mest populære modellene: ChatGPT fra OpenAI, Claude fra Anthropic, Elicit (fra Elicit), NotebookLM fra Google og Perplexity (fra Perplexity). En kort beskrivelse og vurdering av dette finnes i vedlegg C.

2.2 Casestudier

Casestudiene beskriver hvordan de mest relevante aktørene har brukt ulike virkemidler og metoder i praksis. Formålet er å vise en operasjonalisering av konsepter og handlemåter slik at det skal bli lettere å forstå hvordan påvirkningsoperasjoner kan bli utført.

Utvalgskriterier

Utvalget av casestudier styres av flere kriterier. Casene må ha tilstrekkelig dokumentasjon for grundig analyse, de må være representative for ulike typer påvirkningsoperasjoner og virkemidler, de må være relevante for vestlige demokratier, og de må være fra perioden 2023–2024.

Vi valgte å beskrive tre caser, alle fra 2024. De to første er presidentvalget og EU-parlamentsvalget i Frankrike (casestudie 1) og De olympiske lekene (OL) i Paris (casestudie 2). Alle tre begivenhetene foregikk i det samme landet og mer eller mindre innenfor det samme tidsrommet sommeren 2024. De illustrerer hvordan valgpåvirkning spiller sammen med påvirkningsoperasjoner generelt og i forbindelse med konkrete hendelser, hvordan virkemidler brukes, og hvordan hensikter og effekter overlapper og kan være komplekse å analysere. I disse to casene er Russland den mest aktive aktøren.

Den tredje casestudien handler om Spamouflage Dragon (casestudie 3), med vekt på Kina som aktør. Til sammen viser de tre casene en bredde som skal være godt egnet til å illustrere påvirkningsoperasjoner anno 2024.

Analysemetode

Analysen av casene er gjennomført systematisk ved hjelp av James Pamments ABCDE-rammeverk.[6] Funnene er validert gjennom kryss-sjekking mot flere kilder. ABCDE-rammeverket er et analytisk verktøy designet for å systematisk undersøke og forstå påvirkningsoperasjoner. Rammeverket består av fem hovedelementer:

[4] Ibid.
[5] European Commission (2024, mars). *Living guidelines on the responsible use of generative AI in research*.
[6] Pamment (2020, september).

- **A – Actor (aktør):** identifisere hvem som står bak operasjonen
- **B – Behavior (atferd):** analysere de spesifikke handlingene og taktikkene som brukes
- **C – Content (innhold):** undersøke innholdet som spres
- **D – Degree (omfang):** vurdere operasjonens rekkevidde og intensitet
- **E – Effect (effekt):** evaluere operasjonens effekter

Dette rammeverket brukes også av EUs utenrikspolitiske tjeneste (European External Action Service – EEAS) og er spesielt egnet for å analysere påvirkningsoperasjoner fordi det gir en helhetlig tilnærming til å forstå kompleksiteten i slike operasjoner. Det gjør at forskere kan dekonstruere påvirkningshendelser på en systematisk måte, noe som gir både dybdeanalyse av individuelle operasjoner og sammenlignende analyser på tvers av ulike hendelser.

2.3 Metodiske begrensninger

Studien har flere metodiske begrensninger. Én av dem er at datagrunnlaget i hovedsak er hentet fra offentlig tilgjengelige kilder. Dette utelukker informasjon fra graderte kilder, som kan inneholde mer detaljert innsikt.

Som en kvalitativ undersøkelse av trender møter denne studien naturlige utfordringer med validitet og reliabilitet. Trendstudier er i sin natur tolkningsøvelser som krever subjektive valg under både datainnsamling og analyse. For å forsøke å minimere risikoen for blindsoner og bias ble dataene samlet inn gjennom en kombinasjon av forlengs og baklengs snøballmetode (*snowballing*). Denne metoden gjorde det mulig å dekke et bredere spekter av relevante kilder og rapportering, men det kan fortsatt ikke garanteres at all relevant litteratur er inkludert. KI-verktøy som Elicit og Perplexity ble brukt for å identifisere relevante kilder basert på semantisk forståelse uavhengig av språk, men reduserer kun delvis utfordringene med språkbaserte begrensninger, som for eksempel å finne forskningsresultater på språk forskerne ikke kan eller å finne aktuelle forskningsresultater som benytter alternativ terminologi for påvirkningsoperasjoner.

Rapportens tidsmessige avgrensning til 2023–2024 utelukker grundige analyser av hendelser etter senhøsten 2024, inkludert det amerikanske presidentvalget den 5. november. Innen rapportens ferdigstilling er ikke slike analyser klare og tilgjengelige. Selv om det amerikanske valget var en betydelig begivenhet med allerede dokumentert informasjonspåvirkning, mener vi at utviklingstrekk innen valgpåvirkning i 2024 belyses grundig i rapporten selv uten at dette valget er tatt med.

Casestudiene i rapporten utgjør et utvalg av hendelser som skal illustrere et bredt spekter av aktører og virkemidler innen informasjonspåvirkning og påvirkningsoperasjoner rettet mot vestlige demokratier. Utvalget har naturlige begrensninger i både antall og innhold, og utvalget går nødvendigvis på bekostning av andre relevante eksempler. Spesielt har ferske hendelser ofte begrenset dokumentasjon, ettersom undersøkelser og vurderinger krever tid. Dette gjør det utfordrende å inkludere slike hendelser med mindre det finnes tilstrekkelig tilgjengelig

informasjon. Likevel er sammensetningen av casestudier designet for å balansere bredde, aktualitet og representativitet.

Tilgangen til primærdata er en betydelig begrensning. Mange rapporter gir ikke full innsikt i metode, datagrunnlag eller funn, noe som reduserer muligheten til å vurdere hvor pålitelig informasjonen er. For å redusere denne reliabilitetsutfordringen har vi basert oss på kilder fra anerkjente institusjoner og, i casene, brukt ABCDE-rammeverket for å sikre konsistens og avdekke eventuelle mangler i kildegrunnlaget. Likevel ligger det utfordringer i å sammenfatte informasjon fra kilder som bruker ulike beskrivelser, metodikker og analyseteknikker.

Selv om KI-verktøy har vært brukt for å støtte enkelte deler av arbeidet, har vi vært tilbakeholdne med å stole på KI-språkmodeller. Disse anses ikke som tilstrekkelige for å oppnå høy reliabilitet og validitet. Deres rolle i arbeidet har vært begrenset til å støtte søk etter relevant litteratur, vurdere struktur og, i noen tilfeller, foreslå tekstlig rammeverk. All output fra KI-verktøy har blitt manuelt kontrollert og bearbeidet.

3 Litteratur

Dette kapittelet gir vi en kortfattet oversikt over litteraturen som er brukt i denne rapporten. En komplett kildehenvisning ligger til slutt, under «Referanser». Kildene er valgt ut for å sikre en bred og balansert dekning av påvirkningsoperasjoner generelt og i forbindelse med valg spesielt. De er kategorisert i tre hovedgrupper: teoretiske rammeverk, empiriske analyser og teknologisk litteratur.

3.1 Teoretiske rammeverk og metodiske tilnærminger

Teoretiske rammeverk er metodiske verktøy for å systematisere analyser av påvirkningsoperasjoner. Blant de mest sentrale er James Pamments ABCDE-rammeverk, som dekonstruerer påvirkningsoperasjoner gjennom å beskrive aktører, atferd, innhold, omfang og effekt. Dette rammeverket er spesielt nyttig for å dekonstruere komplekse påvirkningsoperasjoner og sammenligne dem på tvers av ulike casestudier. Et annet viktig rammeverk er Ben Nimmos fire D-er – *dismiss*, *distract*, *distort* og *dismay* (avvise, forvrenge, distrahere og skremme) – som er spesielt velegnet for å analysere russiske desinformasjonsoperasjoner. Rapporter om tiltak for beskyttelse mot påvirkning er hentet fra blant annet Institute for Strategic Dialogue[7], The International Foundation for Electoral Systems[8] og The Carnegie Endowment for International Peace[9].

3.2 Empiriske analyser og kartleggingsrapporter

Rapportens empiriske grunnlag er hentet fra en rekke rapporter som dokumenterer faktiske påvirkningsoperasjoner og -trender. En av de mest omfattende er den andre rapporten fra European External Action Service (EEAS), som gir en helhetlig oversikt over hvordan aktører som Russland, Kina og Iran bruker manipulasjon og desinformasjon til å påvirke politiske prosesser i Europa.[10] Den franske overvåkningstjenesten VIGINUM har skrevet detaljerte analyser av påvirkningsforsøk blant annet i forbindelse med valg i Frankrike og OL i Paris i 2024, hvor den russiske Doppelgänger-operasjonen har vært aktiv. Videre har blant annet Graphika skrevet dyptgående studier av kinesiske operasjoner, inkludert Spamouflage Dragon. Andre analysebyråer som Recorded Future, Digital Forensics Research Laboratory (DFRLab), The European Digital Media Observatory og EEAS-teamet EUvsDisinfo er også viktige kilder til empiriske analyser.

[7] Rolfe, T., Schwertheim, H., Döring, M., og Jacobs, E. (2024). *Safeguarding Elections in the Digital Age: Assessing Evolving Electoral Risks and their Mitigation for Online Electoral Integrity*. The Institute for Strategic Dialogue.
[8] North, D.A., Levine, D., Sikora, K., og Diossy, N. (2024). Building Resilience Against Election Influence Operations: Preparing for the European Elections in 2024 and Beyond – Case-studies. *The International Foundation for Electoral Systems*.
[9] Bateman, J., og Jackson, D. (2024). *Countering Disinformation Effectively: An Evidence-Based Policy Guide*. The Carnegie Endowment for International Peace.
[10] EEAS (2024, januar).

3.3 Teknologisk litteratur og innovasjon

Rapporten trekker på flere kilder som beskriver den teknologiske utviklingen innen påvirkningsoperasjoner. For eksempel har Microsoft Threat Analysis Center (MTAC) dokumentert hvordan generativ kunstig intelligens brukes til å produsere og spre desinformasjon i operasjoner som Doppelgänger. Artikler fra blant annet Hunter et al. i *Defense & Security Analysis*[11] og Łabuz og Nehring i *European Political Science*[12] undersøker hvordan KI endrer både metodene og de strategiske mulighetene for aktører som driver med informasjonspåvirkning. Meta sine trussel-rapporter gir også verdifull innsikt i koordinert inautentisk atferd, særlig i kinesiske og russiske operasjoner, og illustrerer hvordan teknologi brukes for å manipulere informasjonsmiljøet.

Mange flere kilder er brukt, blant annet faglitteratur, annen rapportering, avisartikler og lovverkskilder. I sum trekker rapporten på et bredt utvalg av kilder som gir et godt grunnlag for å forstå hvordan påvirkningsoperasjoner har blitt utført i perioden 2023–2024.

[11] Hunter, L. Y., Albert, C. D., Rutland, J., Topping, K., & Hennigan, C. (2024). 'Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations'. *Defense & Security Analysis*, 40(2), 235-269.
[12] Łabuz, M., og Nehring, C. (2024). 'On the way to deep fake democracy? Deep fakes in election campaigns in 2023'. *European Political Science*.

4 Funn fra litteraturen

I dette kapittelet beskriver vi funn fra trendstudien. Vi har delt opp funnene i tre kategorier: aktører (i delkapittel 4.1); observasjoner av informasjonspåvirkning i nasjonale, europeiske valg i 2023–2024 (i delkapittel 4.2); og taktikker, teknikker og fremgangsmåter (*tactics, techniques, and procedures* – TTP-er, i delkapittel 4.3). Eksempler bidrar til å sette funnene i kontekst. Mer kontekst finnes også i casestudiene i kapittel 5.

4.1 Aktører og pågående operasjoner

Denne delen gir en oversikt over de viktigste statlige aktørene involvert i påvirkningsoperasjoner og over målsettingene og organiseringen deres. Vi nevner også noen av de kjente påvirkningsoperasjonene aktørene står bak (disse beskrives i mer detalj i casestudiene i kapittel 5).

4.1.1 Russland og deres største operasjoner

Russlands påvirkningsaktiviteter er en integrert del av Russlands maktpolitiske verktøykasse.[13] Gjennom påvirkningsoperasjoner forsøker Russland aktivt å rettferdiggjøre sin angrepskrig mot Ukraina og undergrave demokratiske institusjoner i Vesten. Andre mål inkluderer å svekke tilliten til media, polarisere offentlig debatt og skape interne splittelser i målstatene. I tillegg ønsker de å avlede oppmerksomheten fra sine egne innenrikspolitiske utfordringer.[14]

Påvirkningsoperasjonene utføres av en rekke ulike aktører i og rundt det russiske statsapparatet. Disse utgjør til sammen infrastrukturen i et globalt økosystem for påvirkning og propaganda.[15] Aktørene kan grovt deles i tre grupper: offentlige myndigheter, statskontrollerte medier og proxy-kilder, der innholdet spres gjennom falske profiler, bots og falske nettaviser/nyhetsportaler på ca. 30 språk.[16]

Den russiske militære utenlandsetterretningstjenesten GRU har en sentral rolle i Russlands påvirkningsoperasjoner.[17] Den russiske staten samarbeider også tett med private, russiske selskaper som Structura Digital Technologies og Social Design Agency, som er sentrale i blant

[13] Ajir, M., og Vailliant, B. (2018). 'Russian Information Warfare: Implications for Deterrence Theory'. *Strategic Studies Quarterly,* 12(3), 70-89; Riehle, K. (2022). 'Russia and Information Power'. *The Journal of Intelligence, Conflict, and Warfare*, *4*(3), 261–265.
[14] EEAS (2024, januar); Insikt Group (2023, 5. desember); Bradshaw, S., og Howard, P. N. (2018). *The global organization of social media disinformation campaigns*. Journal of International Affairs, 71(1.5), 23-32.
[15] EEAS (2024, januar).
[16] U.S. Department of State. (2020, august). *Pillars of Russia's disinformation and propaganda ecosystem.* Global Engagement Center (GEC); VIGINUM (2024, februar). *Portal Kombat: A structured and coordinated pro-Russian propaganda network.* Secrétariat general de la défense et de la sécurité nationale; EU Disinfo Lab (2020, juni).
[17] Bradshaw og Howard (2018).

annet den kjente Doppelgänger-operasjonen. Disse selskapene er eid av personer med nære forbindelser til president Putin, og de rapporterer direkte til Kreml.[18]

Doppelgänger benytter seg av avanserte metoder som URL-kapring og domene-kloning, hvor falske versjoner av kjente europeiske nyhetsnettsteder opprettes.[19] I tillegg brukes generativ KI til å produsere falske nyhetsartikler og manipulerte bilder i stort omfang.[20] Operasjonen har blitt observert i flere europeiske land, inkludert Frankrike, Tyskland og Ukraina, og har vist seg å være særlig aktiv i forbindelse med betydningsfulle hendelser som OL i Paris 2024.[21]

Parallelt med Doppelgänger har Russland drevet **Matryoshka**, også kjent som **Operation Overload**, siden 2023.[22] Denne operasjonen retter seg spesifikt mot å diskreditere vestlige mediehus og faktasjekkere. Matryoshka har omfattet over 90 separate aktiviteter siden september 2023, hvor falskt innhold produseres og faktasjekkere kontaktes direkte i et forsøk på å undergrave tilliten til disse institusjonene.[23] Operasjonen viser Russlands ønske om å svekke troverdigheten til vestlige informasjonskilder.

I 2024 ble **Bad Grammar**-operasjonen avdekket. Denne representerer en ny fase i russisk bruk av KI i påvirkningsoperasjoner. Operasjonen bruker ChatGPT til å produsere innhold på russisk og engelsk, som deretter spres via Telegram. Målgruppen er primært russisk-, ukrainsk-, amerikansk-, moldovsk- og baltisktalende publikum, noe som viser Russlands interesse i å påvirke både innenlandske og utenlandske målgrupper.[24]

Portal Kombat er enda en pågående russisk operasjon. Den benytter et nettverk av 193 pro-russiske informasjonsportaler for å spre pro-russiske narrativer og kritisere Vesten og Ukraina. Operasjonen bruker avanserte SEO-teknikker for å øke synligheten til innholdet i søkeresultater. Dette demonstrerer Russlands evne til å utnytte tekniske aspekter ved moderne informasjonsspredning.[25]

Den nylig oppdagede **Copy Cop**-operasjonen representerer en ny taktikk, hvor innhold fra legitime medie-kilder plagieres og modifiseres for å spre pro-russiske narrativer. Denne operasjonen er aktiv i Frankrike, USA og Storbritannia og viser Russlands evne til å tilpasse eksisterende innhold til sine formål.[26]

---

[18] EU DisinfoLab (2020). *How two information portals hide their ties to the Russian News Agency Inforos*. EU DisinfoLab.; U.S. Department of Justice. (2024, 4, september). *Justice Department disrupts covert Russian government-sponsored foreign malign influence operation targeting audiences in the United States and elsewhere*. U.S. Department of Justice.
[19] EEAS (2024, juni).
[20] Insikt Group (2023, 5. desember). 'Obfuscation and AI Content in the Russian Influence Network "Doppelgänger" Signals Evolving Tactics'. *Recorded Future*.
[21] *Ibid.;* Bond, S. (2024, juni 6). 'This is what Russian propaganda looks like in 2024'. *NPR Transcript*.
[22] VIGINUM (2024, juni). *Matryoshka: A pro-Russian campaign targeting media and the fact-checking community*. Secrétariat general de la défense et de la sécurité nationale.
[23] *Ibid.*
[24] OpenAI (2024, mai). *AI and Covert Influence Operations: Latest Trends*. OpenAI.
[25] VIGINUM (2024, februar)
[26] Insikt Group (2024, 9. mai). *Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale*. Recorded Future.

Disse nyere operasjonene bygger på erfaringer fra tidligere kampanjer som **Secondary Infektion** (2014–2020) og **Project Lakhta** (2014–pågående), som ønsket å så splid mellom vestlige land og polarisere det amerikanske samfunnet.[27] Russland har konsekvent vist evne til å utvikle og tilpasse sine påvirknings-teknikker over tid, med økt bruk av KI og sofistikerte tekniske metoder i de senere årene.

4.1.2 Kina og deres største operasjoner

Kinas påvirkningsoperasjoner støtter Kommunistpartiets strategiske mål om global innflytelse, et stabilt regime og motvirkning av kritikk mot Kina.[28] Gjennom blant annet doktrinen «Tell the China story well» søker Kina å projisere et positivt bilde av Kina som en fredelig ledernasjon, samtidig som de forsøker å undertrykke kritikk av Kina, undergraving av kinesiske interesser og omtale om sensitive temaer som Taiwan og Xinjiang.[29] I tillegg arbeider Kina for å promotere sitt eget politiske og økonomiske system som et alternativ til vestlige demokratier.[30]

Påvirkningsarbeidet gjennomføres av en rekke aktører, inkludert statlige organer, som Kommunistpartiets propaganda-avdeling, Departementet for statssikkerhet og Folkets frigjøringshær (PLA), private og statseide selskaper og ulike cybergrupper.[31] I utlandet mobiliserer Kina sine diaspora-nettverk, Confucius-institutt og frontorganisasjoner for å fremme partiets interesser. Videre benyttes ulike teknikker som manipulering av informasjon gjennom falske kontoer på sosiale medier, kjøp av medieinnflytelse og økonomisk press på selskaper og stater.[32]

Den mest fremtredende kinesiske påvirkningsoperasjonen er **Spamouflage Dragon**, først oppdaget i 2019 og fortsatt aktiv (se casestudie 3 i kapittel 5.3). Denne operasjonen opererer på tvers av over 50 ulike plattformer og nettsider. Spamouflage Dragon har som hovedmål å generere positiv omtale av Kina og kritisere vestlig politikk. Operasjonen benytter seg av automatisert innholdsproduksjon for å spre pro-kinesisk propaganda og retter seg mot både vestlige land og regioner av spesiell interesse for Kina, som Taiwan.[33]

Kina har også vist en økende interesse for å påvirke valg, særlig i Taiwan. I forbindelse med Taiwan-valget i 2024 rapporterte Microsoft Threat Intelligence om bruken av KI-genererte nyhetsankere, videoer og memes i kinesiske påvirkningsoperasjoner.[34] Dette representerer en

[27] Nimmo, B., Francois, C., Eib, C.S., Ronzaud, L., Ferreira, R., Hernon, C., og Kostelancik, T. (2020). *Secondary Infektion*. Graphika; Hanlon, B. (2018). 'Target USA: Key Takeaways from the Kremlin's 'Project Lakhta'.' *The German Marshall Fund*.
[28] Etterretningstjenesten (2024). *Kinas globale ambisjoner.* I Fokus 2024 (Kapittel 3). Etterretningstjenesten; Hunter et al. (2024).; EEAS (2024, januar).
[29] Zhang, X. (2024). '*Telling China's Story Well' as propaganda campaign slogan: A critical analysis.* Media, Culture & Society, 46(5), s. 1237–1254.; Hunter et al. (2024).
[30] Charon, P., & Jeangène Vilmer, J.-B. (2021). *Chinese influence operations: A Machiavellian moment.* Institute for Strategic Research (IRSEM), Ministry for the Armed Forces. ISBN: 978-2-11-155519-8.
[31] Hunter et al. (2024); Nimmo, B., Torrey, M., Franklin, M., Agranovich, D., Milam, M., Hundley, L., og Flaim, R. (2023, august). 'Second Quarter Adversarial Threat Report'. *Meta*.
[32] *Ibid.*
[33] OpenAI (2024, mai); Nimmo et al. (2023).
[34] Microsoft Threat Intelligence (2024, april). *Same targets, new playbooks: East Asia threat actors employ unique methods*. Microsoft.

betydelig utvikling i hvordan Kina bruker visuelt innhold i sine påvirkningsoperasjoner, og viser en økende kompleksitet i deres tilnærming.

Videre har kinesiske operasjoner vært målrettet spesifikt mot Taiwans yngre befolkning, med mål om å påvirke holdninger til en mulig gjenforening.[35] Dette viser Kinas langsiktige strategiske tenkning i sine påvirkningsoperasjoner.

Det er også rapportert om kinesiske påvirkningsforsøk rettet mot det amerikanske valget i 2024, hvor falske grasrotbevegelser ble skapt for å påvirke politiske diskusjoner.[36] Dette indikerer en utvidelse av Kinas påvirkningsoperasjoner til å omfatte bredere geopolitiske mål utover deres umiddelbare regionale interesser.

4.1.3 Iran og deres største operasjoner

Iran styrer blant annet den Quds-lenkede internett-gruppen International Union of Virtual Media (IUVM) for å spre manipulerende innhold.[37] Irans målsettinger med påvirkningsoperasjoner inkluderer å manipulere og påvirke målgrupper ved å øke polarisering og svekke tilliten til regjeringer.[38] En stor del av Irans innsats er rettet mot Israel og USA. Irans påvirkningsoperasjoner tar også sikte på å utnytte aktuelle hendelser og kriser for å så forvirring og mistillit i vestlige samfunn. Denne tilnærmingen gjør at Iran opportunistisk kan fremme sine egne narrativer og undergrave troverdigheten til motstanderne sine.[39]

Den mest fremtredende iranske operasjonen i de senere år er **Emerald Divide**, oppdaget i 2024. Denne operasjonen hadde som hovedmål å skape splittelse i det israelske samfunnet og benyttet seg av cirka 250 koordinerte falske kontoer for å spre polariserende innhold rettet mot ulike grupper i Israel.[40] Operasjonen viser Irans ønske om å utnytte og forsterke eksisterende samfunnsspenninger i mållandene.

Iran har også rettet påvirkningsoperasjoner mot befolkningen i Canada[41], USA[42] og Israel[43], med mål om å skape splittelse mellom jøder og muslimer. Disse operasjonene har benyttet seg av falske profiler på sosiale medier og falske aktivistgrupper for å spre polariserende innhold.[44] Dette demonstrerer Irans evne til å operere på tvers av flere land og målgrupper samtidig.

[35] Hunter et al. (2024).
[36] Watts, C. (2024, 4. august). 'China tests US voter fault lines and ramps AI content to boost its geopolitical interests'. *Microsoft On the Issues*.
[37] DFRLab (2018, 29. august. 29. august). '#TrollTracker: An Iranian Messaging Laundromat'. *Medium*.
[38] Insikt Group (2024, 8. mai). 'Iran-Aligned Emerald Divide Influence Campaign Evolves to Exploit Israel-Hamas Conflict'. *Recorded Future*.
[39] *Ibid.*
[40] Nelson, N. (2024, 9. mai). '3-Year Iranian Influence Op Preys on Divides in Israeli Society'. *DarkReading*; Insikt Group (2024, 8. mai).
[41] Yates, J., Rogers, K., og Rocha, R. (2019, 24. mai). 'How a suspected Iran-based campaign tried to get Canadian media to spread fake news'. *CBC News*.
[42] Myers, S.L., Hsu, R., og Fassihi, F. (2024, 4. september). 'Iran Emerges as a Top Disinformation Threat in U.S. Presidential Race'. *The New York Times*.
[43] Insikt Group (2024, 8. mai).
[44] *Ibid.*

4.2 Observasjoner av valgpåvirkning i 2023 og 2024

I årene 2023 og 2024 ble det gjennomført svært mange valg globalt.[45] Særlig 2024 var et stort valgår, og flere institusjoner advarte mot utilbørlig påvirkning.[46] Vi gjennomførte derfor et overfladisk søk i rapportering fra institusjoner eller fra media rundt europeiske valg ved hjelp av nøkkelord som «disinformation», «fake news», og «påvirkningsoperasjoner». Observasjoner fra utvalgte valg i Europa i 2023 og 2024 gjennomgås kort under.

Merk at disse observasjonene ikke har blitt vurdert eller analysert av FFI og ikke kan regnes som konkluderende for om valgene er utsatt for utenlandsk påvirkning. Allikevel tegner de et bilde av rapporterte hendelser i europeiske valg i perioden.

4.2.1 Europeiske valg i 2023

Bulgaria gjennomførte valg for sin nasjonalforsamling i 2023.[47] Landets informasjonsmiljø er betegnet som et springbrett for russisk påvirkningsoperasjoner videre inn i Balkan og Europa.[48] I 2023 bemerket eksperter at to pro-russiske partier (Revival og BSP) økte eller befestet sine sterke posisjoner i den bulgarske nasjonalforsamlingen, og at disse sprer russisk narrativer.[49] I tillegg er det rapportert om forbindelser mellom russiske påvirkningsoperasjoner og den bulgarske digitale reklameplattformen AdRain.bg.[50]

Estland gjennomførte valg for sin nasjonalforsamling i 2023.[51] Som nabo til Russland og hjemlandet til en betydelig russisk diaspora er landet godt kjent med russisk påvirkningsoperasjoner.[52] Generelle desinformasjonsnarrativer som ble spredt i sammenheng med valget, inkluderte krigen i Ukraina – spesifikt om våpenleveranser, politiske forbindelser og ukrainske flyktninger –, klima, forholdet til EU og økonomien.[53]

Hellas hadde et parlamentsvalg i flere runder i 2023.[54] Det er observert desinformasjon i tilknytning til valget, men dette er rapportert mer som et internt anliggende enn utenlandsk innblanding.[55] Noen av temaene som ble spredt under valgperioden, handlet om LGBTQ+-saker

[45] IFES (2024). 'ElectionGuide'. *International Foundation for Electoral Systems*.
[46] Se, for eksempel: UNDP (2024). 'A 'Super Year' for Election'. United Nations Development Programme; WEF (2024, 10. januar). 'Global Risks 2024: Disinformation Tops Global Risks 2024 as Environmental Threats Intensify'. *World Economic Forum*.
[47] IFES (2024).
[48] Georgiev, G., Petrova, V, og Trabala, K. (2023. 19. april). *Breaking the Code: Tackling the Interlocking Nexus of Russian and Chinese Disinformation and Illicit Financial Flows in Southeast Europe*. Center for the Study of Democracy.
[49] *Ibid*.
[50] Wesolowsky, T. (2024, 6. april). ''Mushroom Websites' Spread a Deluge Of Disinformation In Bulgaria'. *RadioFreeEurope*.
[51] IFES (2024).
[52] Walsh, S., og Thompson, D. (2023, 13. august). 'Combatting Russian Disinformation: Estonia's Response to the War in Ukraine'. *Democratic Erosion Consortium.*
[53] EDMO (2023, november). *Disinformation narratives during the 2023 elections in Europe*. Red. Panizio, E. European Digital Media Observatory.
[54] IFES (2024).
[55] Scott, F. (2023, 19. mai). 'The role of misinformation in Greece's upcoming elections'. *Logically Facts*.

og immigrasjon[56], men også krigen i Ukraina og energikrisen.[57] De siste temaene er av og til frontet med pro-russiske narrativer, som ifølge EU Disinfo Lab kan peke i retning av russisk innblanding.[58]

Montenegro avholdt valg både for president (i flere runder) og for nasjonalforsamlingen i 2023.[59] I forbindelse med presidentvalget ble det avdekket informasjonspåvirkning fra serbiske nettsider og medier som handlet om relasjoner med Serbia og Albania og påstått ekskludering av etniske grupper fra regjeringen.[60] Andre narrativer var sentrert rundt påstander om falske meningsmålinger og uriktige opplysninger om stemmeprosessen.[61]

Polen hadde et sejm- og senatsvalg og en folkeavstemning i 2023.[62] Eksperter mener valget var gjenstand for mye desinformasjon i form av fotomanipulasjon, feilpresentasjon av videoer og anti-europeiske, anti-vestlige narrativer som ble spredt gjennom alle medieplattformer.[63] Samtidig påpekes det at desinformasjonen ikke ser ut til å stamme fra utlandet, men at det heller var et resultat av tidligere mangeårig informasjonspåvirkning fra Russland som har gjennomsyret den interne diskursen, og at Russland ser det som unødvendig å blande seg inn videre.[64]

Serbia gjennomførte et valg for nasjonalforsamlingen i 2023.[65] Landet har over tid vært en av Russlands sterkeste støttespillere i Europa, og dette preger valgene i landet.[66] Russisk-styrte medier som RT og Sputnik var i dette valget for eksempel ute med påstander om at opposisjonen til den russisk-vennlige presidenten var finansiert av USA og George Soros – en velbrukt fiendefigur i konspirasjonsteorier.[67]

Slovakia hadde valg for sitt nasjonalråd og en folkeavstemning i 2023.[68] Valget var i stor grad preget av russisk informasjonspåvirkning og russiske narrativer spredt av slovakiske politikere.[69] Flere enn 365 000 valgrelaterte desinformasjonsinnlegg ble funnet på slovakiske sosiale medier i ukene før valget, med mer eksponering enn vanlige innlegg.[70] Narrativene som ble spredt, handlet mye om Ukraina-krigen og konsekvensene av den, men også om LGBTQ+-saker og immigrasjon.[71] I tillegg ble det spredt KI-genererte lydfiler som skulle være opptak av lederen for et liberalt opposisjonsparti som snakket om eget, fiktivt valgfusk og kontroversielle

[56] EDMO (2023, november).
[57] Dimitriadis, D. (2023, juni). *Disinformation Landscape in Greece*. EU Disinfo Lab.
[58] *Ibid*.
[59] IFES (2024).
[60] EDMO (2023, november).
[61] *Ibid.*
[62] IFES (2024).
[63] Czarnecka, M. (2023, 10. oktober). 'Polish Election Campaign 'Drowning In Disinformation'. *Barron's*.
[64] *Ibid*.
[65] IFES (2024).
[66] Brey, T. (2023, 14 desesmber).
[67] *Ibid*.
[68] IFES (2024).
[69] Sauvage, G. (2023, 28. september). 'Slovakia swamped by disinformation ahead of parliamentary elections'. *France24*.
[70] *Ibid*.
[71] EDMO (2023, november).

forslag.[72] Klippet ble delt de siste dagene før valgdagen, da en regel som forhindret valgomtale i media, gjorde det vanskelig å avkrefte de falske påstandene.[73]

Spania avholdt senats- og deputertkammervalg i 2023.[74] I forkant av valget ble det spredt desinformasjon om valgprosessen og valgfusk, spesielt forsterket av støttespillere til ytre-høyre partiet Vox.[75] Ved siden av slik direkte valgrelatert desinformasjon var også klima, immigrasjon, LGBTQ+-saken og EU gjenstand for desinformasjon under det spanske valget.[76] Det er bemerket at noen av narrativene, spesielt om tillit til demokratiet, EU og NATO, er i tråd med kjente russiske narrativ.[77]

Tsjekkia gjennomførte presidentvalg i 2023 over flere runder.[78] Valget var plaget av betydelige mengder desinformasjon, ofte relatert til militære og forsvarsrettede temaer med likhetstrekk til kjente russiske narrativer.[79] I ett tilfelle ble falske tekstmeldinger sendt ut til media og privatpersoner med påstanden om at den ledende kandidaten i valget var død.[80] Meldingen lenket også til en nettside som etterlignet nettsiden til kandidatens parti og bar tegn på å tilhøre russiske aktører.[81]

Tyrkia avholdt presidentvalg over flere runder i 2023.[82] Det rapporteres om bruk av desinformasjon i valget, men kun med løse påstander om utenlandsk påvirkning.[83] Eksperter peker også på en systematisk blokade av den politiske opposisjonens innhold i media og på sosiale medier.[84] Det som kom gjennom blokaden, var i stor grad manipulert eller misvisende.[85] Narrativer som dominerte i Tyrkia, handlet ofte om religion, anti-LGBTQ+-holdninger, politiske bindinger (spesielt til den kurdiske bevegelsen) og immigrasjon.[86] Det ble også observert bruk av KI-genererte videoer og bilder for å fremme falske påstander.[87]

[72] Atherton, D. (2023, 7. oktober). 'Incident 573: Deepfake Recordings Allegedly Influence Slovakian Election'. *AI Incident Database*.
[73] *Ibid*.
[74] IFES (2024).
[75] Klepper, D. (2023, 19 juli). 'Voting fraud claims spread ahead of Spain's pivotal election'. *AP News*.
[76] EDMO (2023, november).
[77] EU vs Disinfo (2023, 1 august). 'Disinfo: Elections in Spain don't matter as EU and NATO are real bosses'. *EU vs Disinfo*.
[78] IFES (2024).
[79] EDMO (2023, november).
[80] Khatsenkova, S. (2023, 27 januar). 'A fake death, bullet casings and threats: Czech elections are marred by disinformation'. *Euro News*.
[81] *Ibid*.
[82] IFES (2024).
[83] Khatsenkova, S. (2023, 16 mai). 'Turkey's disinformation elections: Fake videos and wildly misleading claims'. *Euro News*.
[84] Sarı, M. S. (2023, 11. juli). 'Turkish elections 2023 in the shadow of disinformation'. *Heinrich Böll Stiftung*.
[85] *Ibid*.
[86] EDMO (2023, november).
[87] *Ibid*.

4.2.2 Europeiske valg i 2024

Bulgaria avholdt to valg for nasjonalforsamlingen i 2024.[88] Disse var gjenstand for forsøk på informasjonspåvirkning fra Russland ved bruk av nettverk av desinformasjonsagenter på sosiale medier og støtte til pro-russiske politiske partier.[89] Det har også blitt meldt at påvirkningsoperasjoner som Doppelgänger er svært aktive i Bulgaria med flere hundre nettsteder opprettet for å spre desinformasjon.[90]

EU-land gjennomførte valg for Europaparlamentet sommeren 2024.[91] Påvirkningsoperasjoner knyttet til dette valget gjennomgås i casestudie 1 (delkapittel 5.1).

Frankrike avholdt valg for sin nasjonalforsamling i flere runder sommeren 2024.[92] Påvirkningsoperasjoner knyttet til dette valget gjennomgås i casestudie 1 (delkapittel 5.1).

Georgia gjennomførte parlamentsvalg høsten 2024.[93] Landet har over tid beveget seg i retning av EU-medlemskap, men dette ble utfordret ved valget, et resultat blant annet av russisk informasjonspåvirkning.[94] Narrativene som ble observert under valgperioden, var knyttet til blant annet NATO, Ukraina, liberalisme, NGO-er, EU og Europa, Vesten og USA, og dessuten Russland. Med unntak av Russland ble alle disse presentert i negativt eller konspiratorisk lys.[95]

Irland avholdt et valg til sitt representanthus og en folkeavstemning i 2024, i tillegg til at de deltok i EU-parlamentsvalget.[96] Rapporter indikerer at Irland var gjenstand for falske, russiske nettsider etablert av Portal Kombat, da rettet mot EU-valget.[97] I oppløpet til det nasjonale valget ble det også rapportert om økende desinformasjon, ofte innen temaer som valgjuks og utenlandsk påvirkning.[98]

Kroatia gjennomførte valg for nasjonalforsamlingen i april 2024 og presidentvalg før årsslutt.[99] Det er observert regulær desinformasjon og bruk av KI-generert desinformasjon som falske

[88] IFES (2024).
[89] Simeonova, M. (2024, 8. november). 'Fool me thrice: The pattern of political instability in Bulgaria, Georgia, and Moldova'. *European Council on Foreign Relations*.
[90] Wesolowsky (2024, 6. april).
[91] IFES (2024).
[92] *Ibid.*
[93] *Ibid*.
[94] White, A. L.-I. (2024, 27. oktober). 'Georgian elections raise further concerns about democratic backsliding'. [Presse konferanse]. *Europaparlamentet*.
[95] EDMO (2024, 27. november). 'Anti-Western Propaganda and Disinformation Amid the 2024 Georgian Parliamentary Elections'. *European Digital Media Observatory*.
[96] IFES (2024).
[97] Gallagher, C. (2024, 11 mai). 'France warns Department of Foreign Affairs about Russian disinformation targeting Irish voters'. *The Irish Times*.
[98] Irish Independent (2024, 27. november). 'The Indo Daily: Election misinformation and disinformation on the rise in Ireland'. *Irish Independent*.
[99] IFES (2024).

videoer, bilder og lyd.[100] Samtidig finnes det ikke eksplisitte indikasjoner på at denne påvirkningen er av utenlandsk opprinnelse, men er heller av innenriks opphav.[101]

Litauen hadde to valg i 2024, for president og parlament, begge utført gjennom flere runder.[102] I sammenheng med presidentvalget ble det avdekket en belarusisk påvirkningsoperasjon som brukte en oppdiktet journalist for å iscenesette intervjuer som senere ble klippet for å fremme falske narrativer og kringkastet over flere plattformer og språk.[103]

Moldova avholdt et presidentvalg over flere runder og en folkeavstemning i 2024.[104] Folkeavstemningen er et eksempel på den typen avstemninger som kan tiltrekke informasjonspåvirkning, i og med at dette var en avstemning om hvorvidt Moldovas grunnlov skulle inkorporere pro-europeiske intensjoner.[105] Russiske offentlige medier og sosiale medier drev i tilknytning til valget og folkeavstemningen informasjonspåvirkning med falske påstander om at presidenten var korrupt, angrep mot opposisjonen, eliter som overstyrer folket, og tapt suverenitet.[106] KI-genererte bilder har også blitt brukt.[107]

Nord-Makedonia gjennomførte et presidentvalg gjennom flere runder og valg for nasjonalforsamlingen i 2024.[108] Nord-Makedonia er i en langvarig prosess for å bli medlem av EU, og dette er noe Russland tar i bruk i sin informasjonspåvirkning rettet mot landet.[109]

Romania avholdt både et presidentvalg og et senat- og deputertkammervalg i 2024.[110] Etter sterke anklager om informasjonspåvirkning fra Russland og en overraskende seier til ytre-høyre-kandidaten i første runde ble resultatene av presidentvalgets første runde annullert.[111] Avgraderte dokumenter publisert av den utgående presidenten i Romania viser en omfattende og godt organisert russisk påvirkningsoperasjon som utnyttet TikTok for å eksponere og fremme en pro-russisk kandidat.[112] Operasjonen var også koblet til flere cyberangrep på valgrelatert infrastruktur.[113]

[100] Brautović, M., og Roško, M. (2024, mai). *Generative AI Use and Disinformation During the Croatian Parliament Elections 2024.* Adria Digital Media Observatory.
[101] *Ibid*.
[102] IFES (2024).
[103] Daukšas, V. (2024, 27. mai). 'Doppelganger journalist FIMI incident from Belarus National State TV against Lithuanian president elections 2024 candidates'. *Debunk.org.*
[104] IFES (2024).
[105] EU vs Disinfo (2024, 24. oktober). 'Disinformation Review: Moscow's anger and plan for Moldova'. *EU vs Disinfo*.
[106] *Ibid*.
[107] *Ibid.*
[108] IFES (2024).
[109] Jones, M. G. (2024, 24. january). 'Russia trying to 'hijack' frustration with EU accession delay – North Macedonia FM'. *Euronews*.
[110] IFES (2024).
[111] Higgins, A., og Barbulescu, M. (2024, 6. desember). 'Romanian Court Annuls Presidential Election Results and Orders a New Vote'. *The New York Times*.
[112] Rainsford, S: (2024, 4. desember). 'Romania hit by major election influence campaign and Russian cyber-attacks'. *BBC*.
[113] *Ibid*.

Slovakia hadde et presidentvalg i 2024 over flere runder.[114] Som ved nasjonalrådsvalget året før mener eksperter at russisk informasjonspåvirkning var sterkt til stede under presidentvalget.[115] Det ble observert mye aktivitet fra russiske medier og proxy-aktører, for eksempel NewsFront og Voice of Europe, i tillegg til slovakiske aktører som spredte russisk desinformasjon.[116] Disse påsto blant annet at opposisjonen var krigshissere og ville sende slovakiske soldater til Ukraina for å kjempe mot Russland, og at de var USAs og NATOs marionetter.[117]

Storbritannia gjennomførte valg for underhuset i 2024.[118] Eksperter peker på noen tilfeller av desinformasjon i Storbritannia, selv om pågangen av påvirkningsoperasjoner og desinformasjon mot valget var forventet å være høyere, spesielt bruken av KI.[119] Journalister avdekket også et knippe med pro-russiske Facebook-sider som brukte desinformasjon, KI-generert innhold og målrettede reklamekampanjer for å kritisere hovedpartene i valget til fordel for det populistiske ytre-høyre-partiet Reform UK.[120] Disse operasjonene knyttes til russiske Doppelgänger.[121]

Tsjekkia avholdt senatsvalg over flere runder i 2024.[122] Det tidligere nevnte Voice of Europe, en russisk-affiliert desinformasjonskanal, har sitt hovedkvarter i Praha i Tsjekkia og ble anklaget for å spre usanne narrativer om store folkemengder som protesterte mot korrupsjon, militær støtte til Ukraina og regjeringen som sådan.[123] Et annet narrativ rapportert spredt i landet var konspirasjonsteorier om flommen som rammet regionen tidligere på året.[124]

4.2.3 Valgene i 2023 og 2024 sett under ett

Disse observasjonene rundt europeiske valg i 2023 og 2024 danner et bilde av aktiv informasjonspåvirkning som rammer valg. Selv om FFI ikke har vurdert eller konkludert rundt disse observasjonene, peker de på mulige påvirkningsoperasjoner.

Det kan også merkes at det synes å være flere observasjoner om informasjonspåvirkning av valg i 2024 enn i 2023. Det er tilfelle ikke bare totalt sett, men også når vi tar høyde for at det var flere valg i 2024 enn i 2023. En grundig gjennomgang av disse valgene kan anbefales når rapporteringen og valideringen av hendelsene har modnet. Inntil da er det verdt å dokumentere påvirkningsoperasjonenes taktikker, teknikker og fremgangsmåter på et mer generelt nivå.

[114] IFES (2024).
[115] Hockenos, P. (2024, 17. april). 'Russia Just Helped Swing a European Election'. *Foreign Policy*.
[116] *Ibid*.
[117] *Ibid*.
[118] IFES (2024).
[119] Johnston, J. (2024, 27. september). 'Why Britain's 'deepfake election' never happened'. *Politico*.
[120] Workman, M., og Nguyen, K. (2024, 29. juni). 'UK Conservatives say ABC analysis that points to foreign interference operation 'highly alarming'. *ABC News*.
[121] *Ibid*.
[122] IFES (2024).
[123] Vock, I. (2024, 28. mars). 'Russian network that 'paid European politicians' busted, authorities claim'. *BBC*.
[124] CEDMO (2024, 29. november). 'What disinformation narratives took over Central Europe in the third quarter of 2024?'. *Central European Digital Media Observatory*.

4.3 Taktikker, teknikker og fremgangsmåter (TTP-er)

Metoder og teknikker i påvirkningsoperasjoner har blitt mer teknologisk avanserte og komplekse de siste to årene. Under beskrives de viktigste, og de brukes ofte i kombinasjon for å maksimere effekten og minimere risikoen for deteksjon.

Kunstig intelligens, spesielt generativ KI som store språkmodeller (*large language models* – LLM-er) og deepfake-teknologi, har spilt en nøkkelrolle i utviklingen av nye teknikker og forbedringen av eksisterende metoder. Samtidig fortsetter aktørene å benytte mer tradisjonelle metoder som falske nettsider og lett manipulert innhold (*cheapfakes*), ofte i en hybrid tilnærming som kombinerer menneskelig og KI-generert innhold.[125]

4.3.1 Tidsløpet for operasjoner

EEAS har definert et generelt tidsløp for de 33 hendelsene de observerte under nyere europeiske valg:[126]

Måneder før valget (opptil 1 år – eller mer): I denne fasen etablerer aktører infrastruktur, utvikler målgrupper og forbereder narrativer. Vanlige aktiviteter inkluderer å opprette nettsider og kontoer på sosiale medier, drive målrettet annonsering og spre polariserende innhold.

Den siste måneden før valget: Etter som valgkampen intensiveres, øker påvirkningsaktiviteten og blir mer variert. Angrep på kandidater, utbredelse av desinformasjon og cyberoperasjoner blir mer fremtredende. Aktører utnytter oppmerksomheten rundt valget for å forsterke narrativene sine.

De siste 72 timene og valgdagen: I sluttfasen søker aktørene å påvirke velgernes atferd gjennom å fremme budskap om å avstå fra å stemme, spre forvirring om prosedyrer eller påstå valgfusk. Falske eller misvisende «avsløringer» lanseres for maksimal effekt, med minimal tid for motreaksjon.

Perioden etter valget: Påvirkningsaktører utnytter usikkerheten i timene og dagene etter at stemmene er avgitt, for å så tvil om resultatene. Påstander om feil, manipulasjon eller utenlandsk innblanding brukes for å utfordre legitimiteten til utfallet og provosere frem protester.

4.3.2 Innhold

Påvirkningsaktører benytter seg av en rekke ulike innholdstyper for å oppnå sine mål:

Falske narrativer kan beskrives som fullstendig oppdiktede historier eller ideer skapt for å villede publikum og etablere alternative forståelser av hendelser. Et nylig eksempel på dette er den russiske Doppelgänger-operasjonen, oppdaget i 2022, som har skapt og spredt falske nyhetshistorier for å undergrave støtten til Ukraina i vestlige land. Operasjonen har blant annet

[125] Franklin, M., Hundley, L., Torrey, M., Agranovich, D., og Dvilyanski, M. (2024, mai). 'First Quarter Adversarial Threat Report'. *Meta*.; Insikt Group (2024, 8. mai).
[126] EEAS (2024, januar).

spredt narrativer om at støtte til Ukraina og sanksjoner mot Russland vil få negative konsekvenser for vestlige samfunn.[127]

Forvridde fakta kan forstås som manipulerte fremstillinger av reelle hendelser eller informasjon som tas ut av kontekst eller presenteres selektivt for å forme en bestemt oppfatning. Under Israel–Hamas-konflikten i 2023 ble dette tydelig demonstrert da eldre bilder fra konflikten og andre konfliktsoner ble presentert som samtidige hendelser på sosiale medier.[128] Denne taktikken utnytter ofte store internasjonale hendelser for å skape forvirring og mistillit.

Visuell feilrepresentasjon har blitt stadig mer sofistikert med fremveksten av KI-teknologi. I 2024 rapporterte Microsoft Threat Intelligence om bruken av KI-genererte nyhetsankere, KI-genererte videoer og memes i kinesiske påvirkningsoperasjoner rettet mot Taiwan-valget.[129]

Emotive narrativer kan tenkes å være utformet for å vekke sterke emosjonelle reaksjoner. Et eksempel på dette er de russiske narrativene som ble spredt i forkant av OL i Paris 2024, hvor det ble skapt frykt rundt økt terrortrussel i Frankrike. Dette var en del av den bredere Doppelgänger-operasjonen (se casestudie 2).[130]

Konspiratorisk innhold kan beskrives som innhold som fremmer mistillit til institusjoner eller autoriteter ved å antyde skjulte agendaer eller maktstrukturer. Ett eksempel er fra 2022, da russiske aktører spredte konspiratorisk innhold om amerikanske biologiske laboratorier på ukrainsk territorium, med mål om å rettferdiggjøre invasjonen i Ukraina.[131]

Polariserende kommentarer forstås her som innhold som er utformet for å overdrive skiller i et samfunn. Ett eksempel er den iranske Emerald Divide-operasjonen, oppdaget i 2024, som utnyttet eksisterende sosiale og politiske spenninger i Israel for å skape ytterligere polarisering.[132]

Humor og satire med politisk brodd kan brukes for å formidle politisk ladede budskap på en mer subtil måte. Ett eksempel er under det franske presidentvalget i 2024, da russiske aktører spredte memes og satiriske videoer som latterliggjorde president Macron og hans kone, ofte med homofobiske og transfobiske undertoner.[133]

Håndplukking av informasjon (eller *cherrypicking*) er en taktikk som innebærer selektiv utvelgelse av fakta eller data som støtter et bestemt synspunkt, mens motstridende informasjon

[127] EU Disinfo Lab (2024). 'What is the Doppelgänger Operation? List of Resources'. *EU Disinfo Lab.*
[128] Bellingcat (2023, 11. oktober). 'Hamas Attacks, Israel Bombs Gaza and Misinformation Surges Online'. *Bellingcat*..
[129] Watts (2024, 4. august).
[130] Watts, C. (2024, 2. juni). 'How Russia is trying to disrupt the 2024 Paris Olympic Games'. *Microsoft On the Issues*.
[131] EU vs Disinfo (2023, 8. mars). 'Disinfo: The Russian special military operation in Ukraine uncovered US biological laboratories'. *EU vs Disinfo*.
[132] Nelson (2024, 9. mai, 9. mai).
[133] EU vs Disinfo (2024, 3. mai).

ignoreres. Et eksempel er da russiske aktører forsterket historier om økte levekostnader og energiutfordringer i EU for å beskrive en kommende systemkollaps.[134]

Forsterking av sann informasjon kan betegnes som en teknikk hvor faktisk korrekt informasjon overdrives eller tas ut av proporsjoner for å støtte et bestemt narrativ. Under OL i Paris 2024 ble for eksempel falske bilder brukt for å overdrive hvor forurenset elven Seinen var.[135]

Disse innholdstypene brukes ofte i kombinasjon for å skape et overbevisende og mangefasettert narrativ som kan være vanskelig å motbevise eller gjennomskue for målgruppen.

4.3.3 Produksjonsmetoder

Produksjonen av innhold i påvirkningsoperasjoner har blitt stadig mer sofistikert, særlig med introduksjonen av verktøy basert på kunstig intelligens.

Bruk av kunstig intelligens

KI har revolusjonert måten desinformasjon produseres på:

- **Store språkmodeller (LLM-er)** brukes nå til å produsere og forbedre innhold og til å øke produktiviteten i påvirkningsoperasjoner. Et eksempel på dette er den russiske Bad Grammar-operasjonen, oppdaget i 2024, som brukte OpenAIs ChatGPT til å produsere innhold på russisk og engelsk som senere ble lagt ut som kommentarer på Telegram.[136]
- **Generativ KI for innholdsproduksjon** har blitt et viktig verktøy for å skape overbevisende falskt eller manipulert innhold. For eksempel bruker den russiske Doppelgänger-operasjonen KI for å fabrikkere nyhetsartikler i høyt tempo.[137] I 2023 ble det avdekket at en kinesisk operasjon brukte KI-genererte nyhetsankere, videoer og memes for å påvirke den yngre befolkningen i Taiwan før valget.[138]
- **Deepfake-teknologi** brukes til å manipulere bilder, video og lyd. Under presidentvalget i Slovakia i 2023 ble en audio-deepfake av en presidentkandidat som angivelig diskuterte valgfusk, spredt på sosiale medier.[139]
- **KI-assistert personalisering** av innhold blir brukt for å skreddersy budskap til spesifikke målgrupper basert på deres atferd på nett. Dette ble observert i russiske påvirkningsforsøk rettet mot det amerikanske valget i 2024.[140]

[134] EU vs Disinfo (2024, 5. juni). 'Elections are battlefields for the Kremlin: Drag everyone down into the mud'. *EU vs Disinfo*.
[135] Buziashvili, E. og Châtelet, V. (2024, 1. august). 'Russia-linked operations target Paris 2024 Olympics'. *DFRLab*.
[136] OpenAI (2024, mai).
[137] Insikt Group (2023, 5. desember).
[138] Watts (2024, 4. august); Hunter et al. (2024).
[139] Łabuz, og Nehring (2024).
[140] Hunter et al., (2024).

Tradisjonelle metoder

Til tross for fremveksten av KI fortsetter tradisjonelle produksjonsmetoder å spille en viktig rolle:

- **Manuell innholdsproduksjon** utført av mennesker forblir viktig, spesielt for å skape nyansert og kontekstuelt relevant innhold.
- **Photoshopping og enkel videomanipulasjon**, kjent som «cheapfakes», utgjør fortsatt en betydelig del av visuell desinformasjon.[141]

Sammensatte tilnærminger

I påvirkningsoperasjoner, for eksempel russiske Doppelgänger eller kinesiske Spamouflage, kombineres mange av de beskrevne virkemidlene, metodene og teknikkene for å maksimere effekten.[142]

4.3.4 Plattformer og kanaler

Påvirkningsoperasjoner utnytter en rekke ulike plattformer og kanaler for å spre innholdet sitt:

Sosiale medier: Plattformene Facebook, X (Twitter), Instagram, TikTok, LinkedIn og YouTube er de mest brukte sosiale mediene for påvirkningsoperasjoner. Bruk og utbredelse varierer og er tilpasset målgruppene som forsøkes nådd.[143]

Falske nyhetsnettsteder: I Doppelgänger-operasjonen i 2024 ble det opprettet falske versjoner av kjente europeiske nyhetsnettsteder for å spre desinformasjon.[144]

Meldingstjenester: Meldingstjenester som WhatsApp og Telegram blir brukt. Spesielt Telegram har fått en sentral rolle i russiske påvirkningsoperasjoner, både til å plante og forsterke innhold, koordinere cyberangrep og omgå vestlige restriksjoner av russiske statskanaler.[145]

Informasjonsportaler: Disse brukes av spesielt russiske aktører. For eksempel avdekket VIGINUM i 2024 Portal Kombat-nettverket, som består av 193 pro-russiske informasjonsportaler som spredte desinformasjon.[146]

[141] Dan, V., Paris, B., Donovan, J., Hameleers, M., Roozenbeek, J., van der Linden, S., og von Sikorski, C. (2021). 'Visual Mis- and Disinformation, Social Media, and Democracy'. *Journalism & Mass Communication Quarterly*, 98(3), 641-664.
[142] EU Disinfo Lab (2024); Franklin et al. (2024, mai).
[143] TrustLab (2023, september). 'Code of Practice on Disinformation: A Comparative Analysis of the Prevalence and Sources of Disinformation across Major Social Media Platforms in Poland, Slovakia, and Spain.' *TrustLab*.
[144] EEAS (2024, juni). 'Doppelgänger strikes back: FIMI activities in the context of the EE24'. *European Union External Action Service*.
[145] Buziashvili og Châtelet (2024, 1. august, 1. august).
[146] VIGINUM (2024, februar).

4.3.5 Spredning

Påvirkningsoperasjoner benytter seg av en rekke sofistikerte metoder for å spre og forsterke innholdet sitt:

Koordinert inautentisk atferd (*coordinated inauthentic behavior* – CIB) involverer nettverk av falske kontoer som samarbeider for å spre desinformasjon. Den iranske Emerald Divide-operasjonen, oppdaget i 2024, brukte cirka 250 koordinerte falske kontoer for å skape splittelse i det israelske samfunnet.[147]

Bruk av bots (automatiserte brukerkontoer eller programmer) er en utbredt metode. I 2024 ble det avdekket at russiske aktører brukte avanserte bots på TikTok som utnyttet RAG-teknologi (*retrieval-augmented generation*) for å generere kontekstrelevante kommentarer og spre desinformasjon om Ukraina-krigen.[148]

Falske forsterkere er falske kontoer som koordinert liker, deler og kommenterer på innhold for å gi inntrykk av popularitet og relevans. Dette ble observert i den russiske Doppelgänger-operasjonen i 2024, hvor forsterkere – tusenvis av falske kontoer – ble brukt til å dele innhold for å øke dets synlighet.[149]

Emneknagg-manipulasjon innebærer koordinert bruk av bestemte emneknagger for å få temaer til «å trende» (altså bli fremhevet av plattformen som populære temaer). Dette ble observert iblant annet kinesiske påvirkningsoperasjoner knyttet til Taiwan-valget i 2023.[150]

«Usynlig blekk»-teknikken (*invisible ink*) går ut på at falske brukere deler innhold gjennom å dele rene URLer til desinformasjonsmeldinger, som gjør spredningen vanskeligere å detektere da de ikke bærer noe tekst som kan gjenkjennes. Dette ble observert i russiske påvirkningsoperasjoner i 2024, spesielt i forbindelse med forsøk på å påvirke EU-valget og valget i USA.[151]

Kunstig grasrotbevegelse (*astroturfing*) er forsøk på å skape inntrykk av grasrotengasjement for en sak. Dette ble observert i kinesiske påvirkningsoperasjoner rettet mot det amerikanske valget i 2023–2024.[152]

[147] Nelson (2024, 9. mai).
[148] Morris, S., Gurzick, D., Guillory, S., og Borsky, G. (2024, 16. mai). 'Countering Cognitive Warfare in the Digital Age: A Comprehensive Strategy for Safeguarding Democracy against Disinformation Campaigns on the TikTok Social Media Platform'. *Information Professionals Association*.
[149] EEAS (2024, juni).
[150] Bond, S. (2023, 13. desember). 'Fake social media accounts are targeting Taiwan's presidential election'. *NPR*.
[151] Alethea Team (2024, 27. mars). *Writing with Invisible Ink*. Alethea; EEAS (2024, juni).
[152] Watts (2024, 4. august).

4.3.6 Manipulasjonsmetoder

Påvirkningsoperasjoner benytter seg av flere ulike manipulasjonsmetoder:

Rekontekstualisering av innhold innebærer at ekte bilder eller videoer tas ut av sin opprinnelige sammenheng. Under Israel–Hamas-konflikten i 2023 ble eldre bilder fra konflikten og andre konfliktsoner presentert som samtidige hendelser.[153]

URL-kapring og domene-kloning innebærer å opprette falske nettsider som etterligner legitime mediekilder. Den russiske Doppelgänger-operasjonen i 2024 opprettet falske versjoner av kjente europeiske nyhetsnettsteder.[154]

Søkemotoroptimalisering (*search engine optimisation* – SEO) brukes for å øke synligheten av desinformasjon i søkeresultater. Dette ble observert i den russiske Portal Kombat-operasjonen, hvor et nettverk av 193 informasjonsportaler brukte SEO-teknikker for å spre pro-russisk propaganda.[155]

Falsk flagg-operasjoner er når en aktør utfører handlinger under dekke av å være en annen aktør. I Frankrike i 2023 ble russiske aktører mistenkt for å ha tagget davidsstjerner på bygninger som en del av en slik operasjon.[156]

Phishing og spearphishing brukes for å stjele sensitiv informasjon eller få uautorisert tilgang til kontoer. Under det franske presidentvalget i 2017 ble Emmanuel Macrons valgkampanje utsatt for et hackerangrep attribuert til russisk etterretningstjeneste.[157]

4.3.7 Angrepsvektorer

Påvirkningsoperasjoner utnytter ulike angrepsvektorer for å maksimere effekten:

Opportunistisk utnyttelse av hendelser er en taktikk hvor aktører raskt utnytter aktuelle hendelser eller kriser til sin fordel. Eksempler på dette inkluderer koronapandemien, hvor flere aktører spredte desinformasjon om virusets opprinnelse, effekten av vaksiner og konspirasjonsteorier egnet til å undergrave tilliten til vestlige lands myndigheter.[158] Et annet eksempel er under OL i Paris, hvor spesielt russiske aktører forsøkte å spre frykt og undergrave president Macron (se casestudie 2, kapittel 5.2).[159]

[153] Bellingcat (2023, 11. oktober).
[154] EEAS (2024, juni).
[155] VIGINUM (2024, februar).
[156] Schofield, H. (2023, 8. november). 'Star of David graffiti in Paris – the Russian connection'. *BBC*.
[157] North et al. (2024).
[158] Bradshaw og Howard (2018).
[159] EU vs Disinfo (2024, 3. mai).

Personangrep rettes ofte mot politikere, journalister eller andre offentlige personer for å undergrave troverdigheten deres. Et eksempel på dette er spredningen av en manipulert video av Nancy Pelosi som fikk henne til å fremstå beruset.[160]

Undergraving av tillit til institusjoner og prosesser er en sentral strategi. Strategien skiller seg også fra de andre fordi den ofte undergraver hele det demokratiske systemet, i motsetning til for eksempel å støtte opp under eller sverte én av flere kandidater.[161] Russiske påvirkningsoperasjoner har konsekvent forsøkt å svekke tilliten til demokratiske institusjoner i vestlige land.[162]

Forsterking av splittelse i samfunnet er en annen vanlig taktikk. Den iranske Emerald Divide-operasjonen utnyttet eksisterende sosiale og politiske spenninger i Israel for å skape ytterligere polarisering.[163]

4.3.7.1 Valgspesifikke vektorer

I EEAS' gjennomgang av 33 påvirkningshendelser fra nylige europeiske valg identifiseres fem hovedkategorier av vektorer som er mest relevante for valg, med noen overlapp til det over:[164]

1. **Påvirkning av informasjonskonsum**: Påvirkningsaktører søker å kontrollere informasjonsflyten og sette agendaen ved å etablere infrastruktur for å distribuere målrettet innhold og engasjere målgrupper i forkant av valget.
2. **Påvirkning av borgernes evne til å stemme**: Gjennom å oppfordre til boikott av valget eller å avgi ugyldige stemmer, søker aktører å senke valgdeltakelsen og representativiteten til valgresultatet. Dette kan involvere falske sikkerhetsadvarsler, forvirring om prosedyrer eller fremstilling av boikott som en protesthandling.
3. **Angrep på kandidater og politiske partier**: Ved å undergrave omdømmet til bestemte kandidater eller så tvil om uavhengigheten til partier søker aktører å polarisere velgere og fremme bestemte politiske utfall. Vanlige taktikker inkluderer personangrep, konspirasjonsteorier og påstander om utenlandsk innblanding.
4. **Undergraving av tilliten til demokratiet**: Påvirkningsaktører angriper selve legitimiteten til valgsystemet ved å fremstille det som svakt, korrupt eller åpent for manipulasjon. Dette kan involvere falske påstander om valgfusk, forhåndsbestemte resultater eller system-svikt.
5. **Påvirkning av valgrelatert infrastruktur**: Cyberangrep mot fysisk eller digital infrastruktur kan forstyrre gjennomføringen av valget og så tvil om resultatene. Selv om

[160] Labuz og Nehring (2024); Dan et al. (2021).
[161] Funk, A., Vesteinsson, K, og Baker, G. (2024). *Freedom on the Net 2024: The Struggle for Trust Online*. Freedom House.
[162] Microsoft Threat Analysis Center (2024, 17. april). *Nation-states engage in US-focused influence operations ahead of US presidential election*. MTAC.
[163] Nelson (2024, 9. mai).
[164] EEAS (2024, januar).

reelle angrep er sjeldne, kan både reelle og påståtte cyberoperasjoner utnyttes for å skape en atmosfære av usikkerhet.[165]

4.3.8 Målgrupper og effekter

Påvirkningsoperasjoner retter seg mot ulike målgrupper og søker å oppnå bestemte effekter:

Ulike målgrupper inkluderer

- hele befolkningen i mållandet, som observert i russiske påvirkningsoperasjoner rettet mot USA og europeiske land[166]
- bestemte demografiske grupper, som demonstrert av kinesiske påvirkningsoperasjoner rettet mot Taiwans yngre befolkning[167]
- radikale miljøer på ytterkantene i det politiske spektrum, for eksempel Russlands forsterking av høyreradikale narrativer i Tyskland[168]
- politikere og beslutningstakere, som sett under det franske presidentvalget i 2017[169]
- journalister og media, som i Matryoshka-operasjonen rettet mot faktasjekkere[170]

Tilsiktede effekter og observerte konsekvenser kan i mange tilfeller analyseres gjennom Ben Nimmos fire D-er. Disse er utviklet for å kategorisere russiske påvirkningsoperasjoner, men er nyttige kategorier for å forstå påvirkning i bredt.[171]

1. **Dismiss (avvise)**: Aktører forsøker å diskreditere kilder til motstridende informasjon. Dette ble observert i russiske forsøk på å undergrave troverdigheten til vestlige medier som rapporterte om situasjonen i Ukraina.[172]
2. **Distort (forvrenge)**: Fakta forvrenges for å passe et ønsket narrativ. Dette var tydelig i den russiske Doppelgänger-operasjonen, som spredte forvrengte fortellinger om konsekvensene av støtte til Ukraina.[173]
3. **Distract (distrahere)**: Oppmerksomheten ledes bort fra uønskede temaer. Kinesiske påvirkningsoperasjoner har for eksempel forsøkt å avlede oppmerksomhet fra situasjonen i Xinjiang ved å sette søkelys på påståtte menneskerettighetsbrudd i vestlige land.[174]

[165] Se, for eksempel Delkapittel 4.3.2. Scenario 2 – Undergraving av tilliten til valget i: Bjørgul, L., Sivertsen, E. G., og Sellevåg, S. R. (2022, 17. juni). *Scenarioer for uønsket påvirkning i forbindelse med norske valg*. FFI-Rapport 22/01424. Forsvarets forskningsinstitutt.
[166] EEAS (2024, januar).
[167] Hunter et al. (2024).
[168] EEAS (2024, juni).
[169] North et al. (2024).
[170] VIGINUM (2024, juni).
[171] Corp (2022, 8. mars).
[172] Watts, C. (2024, 17. april). 'Russian US election interference targets support for Ukraine after slow start'. *Microsoft On the Issues*.
[173] EU Disinfo Lab (2024).
[174] Hunter et al. (2024).

4. **Dismay (skremme)**: Trusler eller skremmende retorikk brukes for å påvirke atferd. Dette ble observert i russiske narrativer spredt før OL i Paris 2024, som forsøkte å skape frykt for terrorangrep.[175]

4.3.9 Narrativer og tematikk

Dominerende narrativer og tematiske trender i nyere påvirkningsoperasjoner inkluderer

- anti-Ukraina-narrativer, spesielt fremtredende etter den russiske invasjonen i 2022[176]
- kritikk av vestlig politikk, ofte brukt i kinesiske påvirkningsoperasjoner[177]
- narrativer som fremmer splittelse, observert i flere påvirkningsoperasjoner fra både Russland, Kina og Iran[178]
- konspirasjonsteorier relatert til globale hendelser, som påstander om amerikanske bio-laboratorier i Ukraina[179]
- anti-EU-narrativer, som har vært fremtredende i russiske påvirkningsoperasjoner – for eksempel har Doppelgänger-operasjonen spredt narrativer som hevder at EU-sanksjoner mot Russland skader europeiske land mer enn Russland, og at EU-institusjoner er korrupte og udemokratiske[180]
- narrativer som undergraver legitimiteten til valgsystemet, enten gjennom å så tvil rundt institusjoner eller valgfunksjonærer eller å fremme påstander om at valget er «rigget» i noens favør[181]
- påstander om at politikere er korrumperte eller påvirket av andre stater eller institusjoner[182]

4.3.10 Kombinasjon av teknikker for maksimal effekt

Påvirkningsoperasjoner kombinerer ofte flere teknikker og plattformer for å oppnå maksimal effekt. Doppelgänger-operasjonen er et godt eksempel på dette:

1. Den benyttet seg av **falske nyhetsnettsteder** som etterlignet legitime mediekilder.[183]
2. Innholdet ble produsert ved hjelp av **generativ KI** for rask og omfattende artikkelgenerering.[184]

[175] Watts (2024, 2. juni).
[176] Watts (2024, 17. april); EEAS (2024, juni); EU vs Disinfo (2023, 8. mars).
[177] Watts (2024, 4. august); Microsoft Threat Analysis Center (2024, 17. april).
[178] Nelson (2024, 9. mai); Insikt Group (2024, 8. mai).
[179] EU vs Disinfo (2023, 8. mars).
[180] EEAS (2024, juni).
[181] Funk et al. (2024).
[182] *Ibid*.
[183] EEAS (2024, juni).
[184] Insikt Group (2023, 5. desember).

3. Spredningen ble forsterket gjennom bruk av **falske forsterkere** på sosiale medier og en avansert fire-trinns prosess for å spre innholdet: Utgivelses-kontoer publiserte originalinnhold, forsterkings-kontoer forsterket innholdet gjennom deling, innholdet ble delt som kommentarer på innlegg fra kontoer med mange følgere, og komplekse URL-omdirigeringsteknikker ble brukt for å unngå plattformrestriksjoner.[185]
4. Operasjonen utnyttet **aktuelle hendelser** som OL i Paris for å skape frykt og mistillit.[186]
5. Den kombinerte **sanne fakta med forvridde narrativer** for å øke troverdigheten.[187]

Andre eksempler inkluderer den kinesiske Spamouflage Dragon-operasjonen, som kombinerte bruk av en rekke sosiale medieplattformer med sofistikert innholdsproduksjon,[188] og den iranske Emerald Divide-operasjonen, som utnyttet eksisterende samfunnssplittelser gjennom målrettet innhold spredt via koordinerte falske kontoer.[189]

Disse eksemplene illustrerer hvordan moderne påvirkningsoperasjoner utnytter et bredt spekter av teknikker og plattformer i komplekse, lagvise kampanjer for å maksimere sin påvirkningskraft og minimere risikoen for deteksjon.

4.4 Delkonklusjon

Funnene avdekker flere viktige utviklingstrekk ved påvirkningsoperasjoner i 2023–2024. For det første domineres landskapet av tre hovedaktører – Russland, Kina og Iran – med egne målsettinger og operasjonsmønstre. Russland fremstår som den mest aktive aktøren, med omfattende operasjoner som Doppelgänger, Matryoshka og Portal Kombat. Disse operasjonene viser økende teknologisk driv, særlig i bruken av kunstig intelligens og automatiserte systemer.

I Europa i 2023 og 2024 er det observert flere forsøk på informasjonspåvirkning knyttet til valg. Dette kan tyde på at valg stadig er målskiver for fremmedstatlig påvirkning. Taktikker, teknikker og fremgangsmåter har blitt mer sofistikerte, med kunstig intelligens og teknologi-utvikling som sentrale drivere for innovasjon. Aktørene kombinerer ofte tradisjonelle metoder med nye teknologiske verktøy og opererer på tvers av flere plattformer og kanaler, gjerne i kombinasjon og selvforsterkning. Samlet sett indikerer funnene at påvirkningsoperasjoner blir stadig mer komplekse og strategiske, med økt bruk av teknologi og mer målrettede påvirkningsforsøk.

[185] EEAS (2024, juni).
[186] Watts (2024, 2. juni).
[187] *Ibid.*
[188] Graphika (2023, februar). *Deepfake It Till You Make It: Pro-Chinese Actors Promote AI-Generated Video Footage of Fictitious People in Online Influence Operation*. Graphika.
[189] Nelson (2024, 9. mai).

5 Casestudier

For å videre demonstrere hvordan aktørene benytter påvirkningsoperasjoner, går vi gjennom tre casestudier. Disse skal gi et bredt innblikk i moderne påvirkningsoperasjoner og er valgt ut for å spenne ulike aktører, tilnærminger og målvalg. Casestudiene er som nevnt også systematisert gjennom ABCDE-rammeverket, og en rekke lærdommer er trukket ut av hver.

5.1 Casestudie 1: To valg i Frankrike i 2024

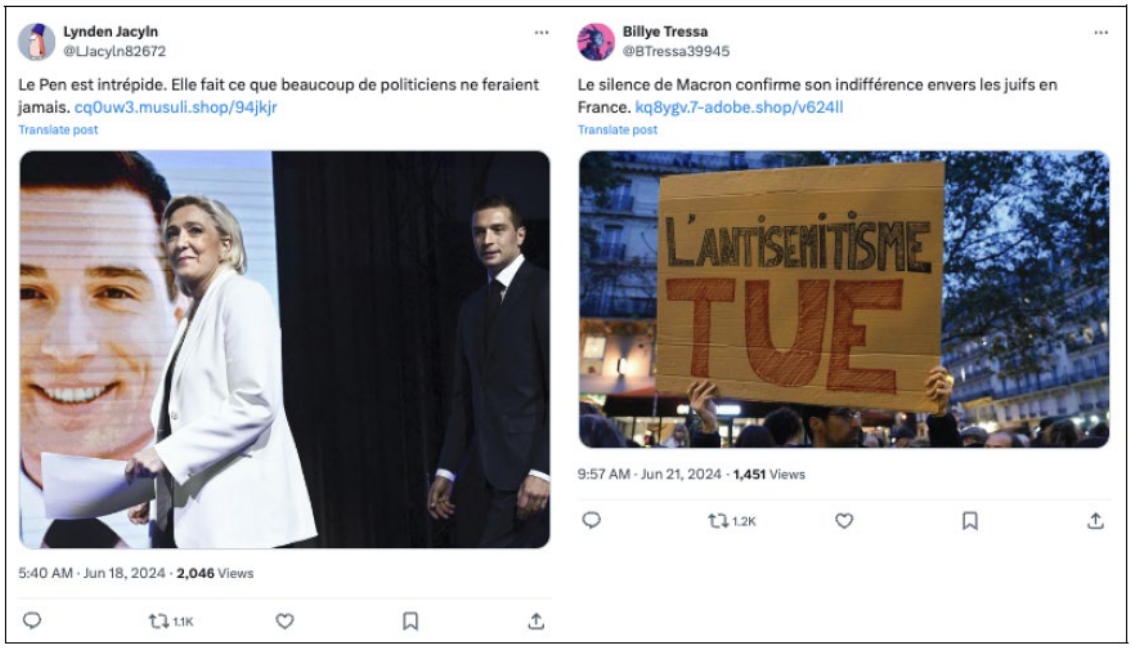
Sommeren 2024 bød på to store valgbegivenheter i Frankrike: EU-parlamentsvalget (6.–9. juni) og et presidentvalg (30. juni–7. juli). Disse var gjenstand for påvirkningsforsøk fra flere aktører, i hovedsak Russland og Iran. I denne casestudien legger vi vekt på fire operasjoner fra russiske aktører og en aktør fra Iran.

De fire russiske operasjonene er kjent som Doppelgänger, CopyCop, Pravda-nettverket og Portal Kombat. Den iranske aktøren er kjent som The International Union of Virtual Media (IUVM).[190]

Doppelgänger-operasjonen brukte flere tusen falske kontoer på sosiale medier for å spre politiske budskap på X og Facebook. Russiske aktører etablerte i tillegg klonede nettsider som etterlignet kjente franske nyhetssider som Le Parisien og Le Point med tilnærmet like nettadresser.[191] Hovedtemaet for Doppelgängers innhold var narrativer som beskrev migrasjon som en destabiliserende kraft i Frankrike og at president Macron var uegnet til å håndtere migrasjonsspørsmål. Videre pekte de på Frankrikes deltakelse i NATO og Macrons utenrikspolitikk.[192]

CopyCop-operasjonen brukte store språkmodeller til å masseprodusere artikler som etterlignet legitime artikler, men med en fordreining i retning av russiske interesser. Over 19 000 artikler ble generert og publisert på falske nyhetssider.[193] Et av delmålene til operasjonen synes å ha vært å undergrave franske myndigheters evne til å sikre valget og å ha en troverdig stemme i det offentlige ordskiftet.[194] Artiklene hadde ofte tematikk som kritiserte Macron og Frankrikes støtte til Ukraina.[195]

[190] EEAS (2024, juni); Insikt Group (2024, 9. mai); VIGINUM (2024, februar); DFRLab (2018, 29. august).
[191] EEAS (2024, juni).
[192] Insikt Group (2024, 28. juni). *Sombres Influences: Russian and Iranian Influence Networks Target French Elections*. Recorded Future.
[193] Insikt Group (2024, 9. mai).
[194] *Ibid.*
[195] *Ibid*.



Figur 5.1 Doppelgänger-attribuerte sosiale mediekontoer som promoterer Marine Le Pen (til venstre; teksten sier «Le Pen er fryktløs. Hun gjør det som mange politikere aldri gjør»,) og som kritiserer Macron (til høyre; teksten sier «Macrons stillhet bekrefter likegyldigheten hans til jødene i Frankrike», mens plakaten sier «Antisemitisme dreper»). Lenkene ledet til Doppelgänger-nettsider.[196]

Portal Kombat-operasjonen etablerte franskspråklige informasjonsportaler hvor de promoterte russisk-vennlig innhold. Ved hjelp av søkemotoroptimalisering ble disse sidene rangert høyt i søkeresultater.[197]

Utenfor disse tre operasjonene brukte russisk-affilierte aktører også etablerte markedsførings-metoder for å publisere 275 politiske reklamer uten merking. Disse reklamene støttet russiske narrativer og nådde over tre millioner kontoer i EU, hvorav nesten en tredjedel var franske kontoer.[198] Narrativene dreide seg i stor grad om økonomisk ustabilitet. Spesielt var stigende energipriser og prislappen på Macrons støtte til Ukraina i fokus. Operasjonen hadde som mål å posisjonere Russland som et mer stabilt alternativ og å undergrave befolkningens støtte til regjeringens politikk.[199] I tillegg spredte disse aktørene memes og satiriske videoer som latterliggjorde president Macron og hans kone, ofte med homofobiske og transfobiske undertoner.[200]

[196] Insikt Group (2024, 28. juni).
[197] VIGINUM (2024, februar).
[198] AI Forensics (2024). *Supporting Evidence: Pro-Russian Ads Campaigns Approved by Meta from May 1 to May 27, 2024 in Italy, Germany, France & Poland.* AI Forensics.
[199] *Ibid.*
[200] EU vs Disinfo (2024, 3. mai).

Det iranske IUVM-nettverket brukte falske kontoer på sosiale medier for å spre politiske budskap.[201] Mye av innholdet pekte på fransk utenrikspolitikk. I dette tilfellet var både Macron og Le Pen gjenstand for nettverkets informasjonsoperasjoner, hvor de begge ble koblet til NATO og til Israels krigføring i Midtøsten.[202] Trolig dreide dette seg om et forsøk på å undergrave fransk tiltro til egne politikere på tvers av den politiske skalaen. Irans kampanje var av beskjeden skala i forhold til den russiske.[203]

Effekten av disse operasjonene var begrenset, på tross av sofistikerte forsøk, spesielt fra Russland.[204] Meta og X jobbet sammen med de franske myndighetene for å motvirke dem.[205] Meta fjernet også de 275 falske reklamene fra Facebook, selv om de først rakk å nå over tre millioner kontoer.[206]

5.1.1 ABCDE-matrise

For å gi en oversikt over casestudien på en håndterlig måte er hovedelementene her beskrevet i en ABCDE-matrise (tabell 5.1). Dette skal også gjøre det mulig å raskt sammenligne elementer på tvers av casestudiene.

Tabell 5.1 ABCDE-matrise for casestudie 1.

Aktør	**Atferd**	**Innhold**	**Omfang**	**Effekt**
Russland • Doppelgänger • CopyCop • Portal Kombat Iran • IUVM	• koordinert inautentisk atferd • nettside-kloning • falske informasjons-portaler • KI-generert innhold • betalt reklame på sosiale medier • skjult innholds-distribusjon	• migrasjon • økonomisk ustabilitet • NATO og utenriks-politikk • sikkerhets-risikoer • undergraving av Macron	• flere inautentiske nettsider • tusenvis av falske kontoer • tusenvis av artikler • flere hundre reklamer	Lite nedslag

[201] Insikt Group (2024, 28. juni).
[202] *Ibid.*.
[203] *Ibid*.
[204] *Ibid*.
[205] Franklin et al . (2024, mai); Louis, L. (2024, 12. april). 'France fights disinformation as Olympics, elections loom'. *Deutsche Welle*.
[206] AI Forensics (2024).

5.1.2 Erfaringer fra hendelsene

Fire erfaringer fra casestudie 1 peker seg ut:

1. **Aktørene forbereder seg for påvirkningsoperasjoner i forkant:** Russiske påvirkningsaktører starter sine kampanjer tidlig for å forme informasjonsmiljøet i forkant av valg. Myndigheter bør være tidlig i gang med å forebygge og utvikle responsopsjoner.

2. **Operasjonene koordineres på tvers av plattformer:** Ettersom aktørene benytter seg av flere vektorer og plattformer for å oppnå spredning (for eksempel bot-nettverk på X og søkemotoroptimalisering) er det viktig å etablere gode samarbeid mellom plattformene og myndighetene. Dette vil bidra til tidlig varsling og fjerning av desinformasjon.

3. **Påvirkningen har begrenset nedslag til tross for stor skala:** Selv om nettverkene, spesielt de russiske, produserte enorme mengder desinformasjon og påvirkningsmateriale, var det forholdsvis lite nedslag hos den franske befolkningen. Det må allikevel antas at myndighetenes forberedelser og rask fjerning av falske brukere og nettsider hadde noe å si for dette resultatet.

4. **Aktørene utnytter samtidige hendelser:** Aktørene benyttet seg godt av at flere hendelser hadde sammenheng i tid og sted for å effektivisere budskapene sine og oppnå kumulative effekter. I denne casestudien var det spesielt EU-valget og presidentvalget som var fokus, men OL i Paris var også under opptrapping i samme periode (dette behandles som en egen casestudie i kapittel 5.2). Slike sammenfall av flere hendelser og angrepsflater kompliserer muligheten til å effektivt kontre påvirkningsoperasjoner. Det kan derfor tenkes at myndigheter bør vurdere desinformasjonsfaren ved å gjennomføre større begivenheter som avstemminger samtidig.

5.2 Casestudie 2: OL i Paris 2024

Samme sommeren som de to valgene var Frankrike vertsland for OL. Dette førte til en enorm internasjonal oppmerksomhet og dermed også en unik anledning for påvirkningsaktører. Det er vanskelig å skille påvirkningsoperasjoner i forbindelse med OL fra de to valgene som foregikk i Frankrike, og som er beskrevet i casestudie 1, ikke minst fordi de foregikk tett opptil hverandre. Det er også sannsynlig at flere aktører som ønsket å påvirke franske eller generelt vestlige publikum, ikke skilte spesielt på påvirkningsoperasjoner rettet mot valg eller mot OL. OL er likevel verdt en studie i seg selv, siden det bød på mye større, global oppmerksomhet, med publikum fra alle verdenshjørner, og siden mange aktører var involvert – både i å utføre og å motvirke påvirkning.

VIGINUM, den franske overvåkingstjenesten, fant 43 påvirkningsoperasjoner med mål om å undergrave tilliten til at Frankrike kunne forvalte sin vertsrolle sikkert.[207] NewsGuard fulgte 36 desinformasjonsnarrativer, spredt over 17 språk[208] fordelt i tur på 83 nettsider, 25 av dem tidligere kjent for pro-russisk propaganda.[209] Microsoft Threat Analysis Center (MTAC) pekte på to sentrale mål for disse operasjonene: å undergrave tilliten til den internasjonale olympiske komité (IOC) globalt og å fostre en forventning om voldshendelser under lekene.[210]

Aktørene som var mest aktive i disse kampanjene, var Russland, Kina, Iran, og pro-palestinske og pro-aserbajdsjanske nettverk.

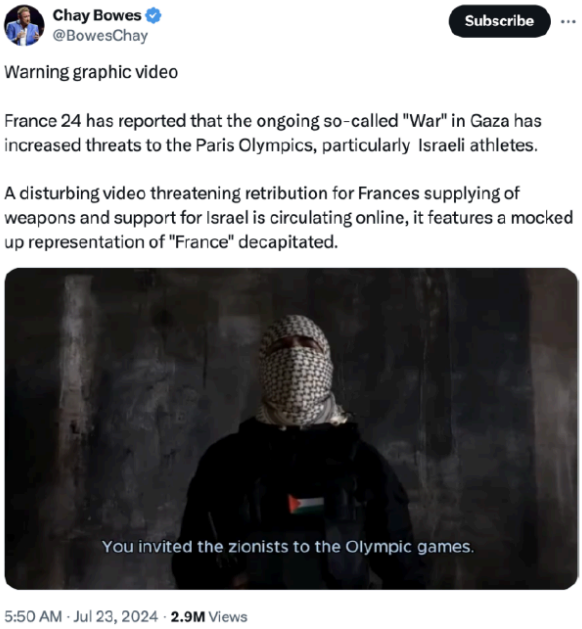
Fra Russland var aktører tilknyttet Doppelgänger og Matryoshka-operasjonene aktive gjennom gruppene Storm-1679 og Storm-1099,[211] samt restene av det gamle Internet Research Agency (IRA)[212] [213] Doppelgänger-gruppen Storm-1099 opprettet minst 15 unike, franskspråklige nettsider, deriblant det sentrale Reliable Recent News (RRN), for å spre påstander om IOCs korrupsjon og advarsler mot vold under lekene. Automatiserte brukerprofiler (bots) ble også brukt for å fremme både emneknagger (som JOPourris2024 – «råttent OL 2024») og egne narrativer på Telegram, X og Facebook.[214]

Betegnelsen «Storm-xxxx», hvor xxxx representerer et firesifret tall, er ikke et selvoppnevnt navn for påvirkningsaktører. Storm-betegnelsen stammer fra en nomenklatur utviklet av Microsoft Threat Intelligence som gir oppdagede trusselaktører navn basert på gitte karakteristikker. «Storm-xxxx» er en midlertidig betegnelse der Microsoft har nylig avdekket en ukjent trusselaktivitet i en løs konstellasjon, eller en gruppe som ser ut til å være under utvikling eller utfoldelse. Se: Microsoft Defender (2024, 19. desember). 'How Microsoft names threat actors'. *Microsoft*.

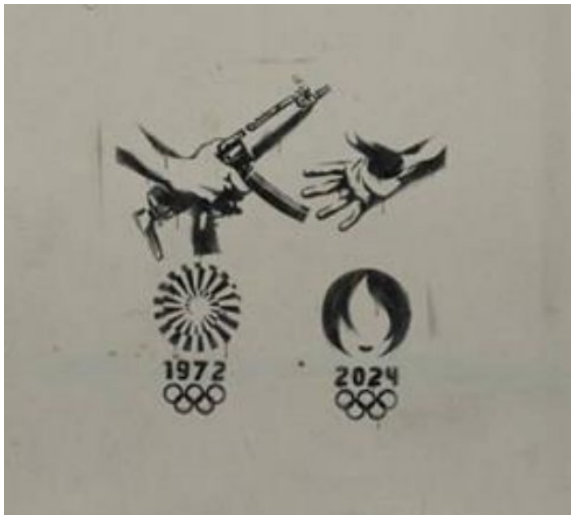
En video sluppet bare dager før åpningsseremonien viste en angivelig Hamas-kriger som direkte truet med å angripe lekene.[215] Videoen ble delt bredt og sett over 25 millioner ganger.[216] Videoen var ikke ekte og ble senere attribuert til gjenværende elementer av det russiske Internet Research Agency.[217] En annen Doppelgänger-kampanje begynte sent i 2023 å spre falske bilder av graffiti i Paris som antydet trusler mot israelske borgere som besøkte lekene, med referanser til angrepene mot OL i

[207] VIGINUM (2024, september). *Summary of the Information Threat to the Paris 2024 Olympic and Paralympic Games*. Secrétariat general de la défense et de la sécurité nationale.
[208] Arabisk, engelsk, fransk, gresk, italiensk, kinesisk, nederlandsk, persisk, polsk, portugisisk, rumensk, russisk, slovensk, spansk, tyrkisk, tysk og ungarsk.
[209] Blachez, I, og Labbé, C. (2024, 21. august). '2024 Paris Olympics Misinformation Tracking Center'. *NewsGuard*.
[210] Watts (2024, 2. juni).
[211] *Ibid.*
[212] Buziashvili og Châtelet (2024, 1. august, 1. august).
[213] VIGINUM (2024, juni).
[214] Buziashvili og Châtelet (2024, 1. august, 1. august).
[215] *Ibid.*
[216] *Ibid.*
[217] *Ibid.*

München i 1972.[218] MTAC vurderte bildene som digitalt genererte. Bildene ble videre delt gjennom RRN og inautentiske brukerkontoer.



Figur 5.2 Skjermbilde fra kontoen @BowesChay som deler den falske videoen av en Hamas-kriger som truer med å angripe OL i Paris.[219]



Figur 5.3 Bilde som viser digitalt generert graffiti med trusler mot OL i Paris.[220]

[218] Watts (2024, 2. juni).
[219] Buziashvili og Châtelet (2024, 1. august, 1. august).
[220] Watts (2024, 2. juni).

Russiske aktører tok flittig i bruk kunstig intelligens til å generere innhold. Ett merkverdig eksempel er den falske dokumentaren «Olympics Has Fallen», hvor Storm-1679 genererte stemmen til Tom Cruise gjennom kunstig intelligens og fikk denne til å lese en tekst som kritiserte IOCs lederskap.[221] Filmen demonstrerte en sterk produksjonsevne, med imponerende, datagenererte spesialeffekter, gjennomført markedsføring med en forfalsket Netflix-intro og forfalskede anbefalinger fra vestlige medier. Den ble distribuert først gjennom Telegram og så videre til andre plattformer.[222]

Figur 5.4 Et stillbilde fra den falske dokumentaren «Olympics Has Fallen».[223]

Samme gruppe, Storm-1679, produserte i tillegg en serie med videoer som utga seg for å stamme fra legitime nyhetskilder. For eksempel produserte de en video som angivelig kom fra det belgiske Euro News, hvor de påsto at parisere kjøpte eiendomsforsikring for å verne seg mot terror knyttet til lekene. En annen video utga seg for å være fra France24, som hevdet at 24 prosent av OL-billettene som hadde blitt kjøpt, hadde kommet i retur av personer som fryktet terrorangrep.[224]

Slike fiktive eller oppblåste sikkerhetstrusler var hyppige temaer for russiske aktører. I et tilfelle ble det spredt falske medierapporter om at CIA advarte mot å bruke metroen i Paris, eller at CIA anbefalte folk å holde seg unna lekene på grunn av terrortrusselen.[225]

[221] *Ibid.*
[222] *Ibid.*
[223] Watts (2024, 2. juni).
[224] *Ibid.*
[225] Watts (2024, 2. juni); Buziashvili og Châtelet (2024, 1. august, 1. august).

Kinesiske aktører benyttet seg av de kinesiske plattformene Weibo, Douyin og WeChat.[226] Her spredte disse aktørene narrativer som kritiserte vestlige verdier og klimaspørsmål. For eksempel lagde en kjent kinesisk influenser en video som kritiserte OL. Videoen ble sett over 2 millioner ganger over bare fire dager.[227]

Iranske og pro-palestinske nettverk målrettet sine kampanjer mest mot israelske utøvere med innhold spredt på Telegram, Facebook og Instagram.[228] Dette innebar blant annet å lekke personlig og identifiserende informasjon (såkalt doxxing) av israelske utøvere og anklage dem for å ha begått krigsforbrytelser.[229]

Pro-aserbajdsjanske nettverk opprettet det de kalte OLIMPIYA-kampanjen, som knyttet lekene til påstått fransk etterretningsvirksomhet og israelsk krigføring. De oppfordret til bruk av emneknaggener som #BoycottParis2024 og #NoParis2024.[230] Emneknaggene ble også forsterket gjennom kunstige grasrotbevegelser der narrativene ble delt og innholdet koordinert fra flere falske kontoer.[231]

Flere aktører bidro til å motvirke disse forsøkene på påvirkning. VIGINUM identifiserte raskt mange av kampanjene.[232] De sosiale medieplattformene tok også grep selv. Flere kontoer som spredte falsk informasjon på X (deriblant den falske Hamas-videoen), ble sperret.[233] EUs European Digital Media Observatory (EDMO) spilte en viktig rolle i å motvirke desinformasjon knyttet til OL gjennom koordinert faktasjekkinnsats på tvers av medlemsland og regelmessige oppdateringer om desinformasjonstrender.[234]

Effekten av disse forsøkene var begrensede, med lite tilfang i det franske informasjonsmiljøet, til dels på grunn av aktive kontringsmetoder.[235] Samtidig må det påpekes at enkelte kampanjer fikk delvis gjennomslag, som den fiktive Hamas trussel-videoen, fordi den økte følelsen av utrygghet.[236] Selv om flere institusjoner var aktive i å motbevise falske påstander, kunne det observeres en såkalt Streisand-effekt – at forsøk på å dempe en sak bidrar til å fremme den.[237] Man kunne også se at offentlige personer og influensere bidro til spredningen av desinformasjon, ofte uten å være klar over det selv.[238]

[226] VIGINUM (2024, september).
[227] *Ibid.*
[228] *Ibid.*
[229] VIGINUM (2024, september).
[230] *Ibid.*
[231] *Ibid*.
[232] *Ibid.*
[233] Buziashvili og Châtelet (2024, 1. august).
[234] EDMO (2024, 22. august).
[235] VIGINUM (2024, september).
[236] Buziashvili og Châtelet (2024, 1. august); VIGINUM (2024, september).
[237] VIGINUM (2024, september).
[238] *Ibid.*.

5.2.1 ABCDE-matrise

Som ved casestudie 1 gis det her en oversikt over casestudien på en håndterlig måte med hovedelementene beskrevet i en ABCDE-matrise (tabell 5.2). Dette skal også gjøre det mulig å raskt sammenligne elementer på tvers av casestudiene.

Tabell 5.2 ABCDE-matrise for casestudie 2.

Aktør	Atferd	Innhold	Omfang	Effekt
Russland • Doppelgänger • Internet Research Agency • Matryoshka Kina Pro-Palestina Iran Pro-Aserbajdsjan	• etterligning av medier • doxxing • bot-nettverk • falske hendelser • koordinert inautentisk atferd	• sikkerhets-trusler • undergraving av tillit • anti-Israel • IOC-korrupsjon	• mange inautentiske nettsider • millioner av visninger	Lite nedslag, men til noen grad vellykket med virale øyeblikk

5.2.2 Erfaringer fra hendelsene

Syv erfaringer fra casestudie 2 peker seg ut:

1. **Koordinering mellom flere aktører øker effekten av desinformasjon:** Informasjonspåvirkning som blir spredt av flere statlige og ikke-statlige aktører, kan betydelig øke effekten av falske narrativer. Slike kampanjer når ikke bare flere brukere, men gjør også kontringsarbeidet mer utfordrende fordi det ofte må overvåkes på tvers av plattformer, språk og brukergrupper.

2. **Avanserte teknologier bidrar til mer sofistikerte påvirkningsoperasjoner:** Bruken av KI-generert innhold og deepfakes øker troverdigheten og rekkevidden til påvirkningsoperasjoner. Det er viktig å følge med på den teknologiske utviklingen for å utvikle relevante kontringsmetoder.

3. **Bruken av eksisterende engstelser og splittelser øker desinformasjonens troverdighet:** Der desinformasjon utnytter reelle forhold, for eksempel uro rundt klima og miljø eller sikkerhet, blir den mer troverdig og vanskeligere å avkrefte. Proaktiv kommunikasjon (*prebunking*) rundt slike temaer kan svekke muligheten til å utnytte dem.

4. **Utilsiktet spredning gjennom influensere peker på verdien av medieforståelse:** Influensere og offentlige personer kan spre falsk informasjon uten å mene det, noe som øker spredningen kraftig. Kursing og utdanning om viktigheten av kildekritikk og

medieforståelse for befolkningen generelt, men også målrettet mot offentlige personer, er kritisk for å hindre utilsiktet amplifikasjon.

5. **Hurtige og koordinerte responser bidrar til å begrense spredning:** Der myndigheter kan agere raskt, sammen med plattformer og andre instanser, kan man hindre effekten av påvirkningsoperasjoner. Tidlig kontring er verdifullt for å hindre spredning.

6. **Forsiktige avkreftelsesstrategier kan hindre utilsiktede effekter:** Å aktivt identifisere og omtale desinformasjon kan virke mot sin hensikt hvis det bidrar til økt oppmerksomhet. Måten disse avsløres og motarbeides på, må derfor være nøye gjennomtenkt i hvert tilfelle.

7. **Vedvarende utfordringer ved uregulerte plattformer:** Plattformene håndterer krav om å fjerne innhold eller kontoer på forskjellige måter og til forskjellige grader. Noen plattformer responderer ikke på slike krav i det hele tatt. Effektiv håndtering av påvirkningsforsøk avhenger derfor av planer for hvordan uregulerte plattformer skal håndteres.

5.3 Casestudie 3: Spamouflage Dragon

Spamouflage Dragon, også kjent som Dragonbridge eller Storm-1376, er en storskala påvirkningsoperasjon attribuert til Kina.[239] Operasjonen er ifølge amerikanske rettsdokumenter styrt av Kinas Departement for offentlig sikkerhet.[240] Operasjonen bruker flere tusen inautentiske kontoer på flere enn 40 plattformer på nett med innhold på mange språk.[241]

Kampanjen viser regionale variasjoner i fremtoningen og er tilpasningsdyktig i møte med uforutsette globale hendelser. I USA og Taiwan har kampanjen vært mest fokusert på valgpåvirkning, mens den i Japan og Sør-Korea utnytter regionale uenigheter. I Europa undergraver kampanjen tilliten til demokratiske prosesser.[242] Overordnet kan målsettingen til Spamouflage sies å være å promotere pro-kinesiske narrativer og å undergrave påståtte motstandere, i hovedsak USA.[243]

Operasjonen har endret karakter de seneste årene. Tidligere var kampanjen i hovedsak rettet mot å promotere pro-kinesiske narrativer og å motsi kritikk rettet mot de kinesiske styresmaktene.[244] Operasjonen begynte å ekspandere i 2019 i tråd med Hongkong-protestene som fikk internasjonal oppmerksomhet, og ytterligere i 2020 som følge av covid-19-utbruddet.

[239] Watts (2024, 4. august).
[240] O'Sullivan, D., Devine, C., og Gordon, A. (2023, 13. november). 'China is using the world's largest known online disinformation operation to harass Americans, a CNN review finds.' *CNN*.
[241] Graphika (2024, september). '*The #Americans: Chinese State-Linked Influence Operation Spamouflage Masquerades as U.S. Voters to Push Divisive Online Narratives Ahead of 2024 Election*'. Graphika.
[242] Microsoft Threat Intelligence (2024, april).
[243] Graphika (2024, september).
[244] Graphika (2019, september). *Cross-Platform Spam Network Targeted Hong Kong Protests: "Spamouflage Dragon" used hijacked and fake accounts to amplify video content*'. Graphika.

Operasjonen har etter hvert også i større grad rettet seg mot amerikanske publikum og mot valg.[245] I 2023 tok operasjonen enda et steg og begynte med mer sofistikerte metoder som bruk av generativ KI. Et markant eksempel i så måte er en serie KI-genererte memes laget av Spamouflage rettet mot den taiwanske presidentkandidaten William Lai i desember 2023.[246]

I tilknytning til presidentvalget i USA i 2024 rettet Spamouflage kampanjer mot president Joe Biden, tidligere president Donald Trump og visepresident Kamala Harris.[247] Målet synes å ha vært å undergrave det amerikanske politiske systemet, og politikere på både demokratisk og republikansk side.[248] Narrativer som er brukt, har vært våpenlovgivning, hjemløshet, misbruk av narkotika, raseproblematikk og Israels krigføring mot Hamas.[249] Operasjonen har også vist evnen til rask omstilling, for eksempel da den brukte KI-genererte bilder i august 2023 for å påstå at den amerikanske regjeringen var innblandet i Hawaiis pågående skogbrann.[250] Ved siden av stadig mer sofistikert bruk av KI bruker Spamouflage inautentiske kontoer for å etterligne amerikanske velgere og spre innhold koordinert på tvers av flere plattformer.[251]

Taiwan er tett knyttet til Kinas strategiske mål, og Spamouflage har her fokusert på valgpåvirkning. I Taiwans presidentvalg i 2024 brukte operasjonen KI-genererte videoer og lydklipp for å spre desinformasjon gjennom sosiale medier på Taiwan. Et godt eksempel er et lydklipp av Terry Gou, en tidligere presidentkandidat, som gir sin støtte til en annen presidentkandidat. Lydklippet var KI-generert av Spamouflage, og det viser både evnen og viljen til å påvirke valg.[252]

I Japan og Sør-Korea viser Spamouflage en annen side av operasjonen. Her har Spamouflage for eksempel spredt narrativer som kritiserer Japans håndtering av radioaktivt vann fra Fukushima, for å skape spenninger i regionen knyttet til miljø og sikkerhet. Spamouflage ble også knyttet til innhold i Sør-Korea som forsterket lokale protester mot Japans handlinger. Denne kreative bruken av begge sider for å øke regional uro viser tydelig en økende modenhet i kinesisk påvirkning.[253]

Selv om operasjonen har utviklet seg i en stadig modnere og mer sofistikert retning, er det lite som tilsier at Spamouflage har klart å påvirke målene sine. Til tross for enkelte virale øyeblikk er det lite av operasjonens narrativer som florerer organisk i reelle fora.[254] Samtidig kan man ikke avskrive en kontinuerlig utvikling og forbedring av operasjonen som sannsynligvis vil få støtte av KI-verktøy for å gjøre kampanjene mer slagkraftige for publikummet det er rettet mot.

[245] Graphika (2024, september).
[246] Microsoft Threat Intelligence (2024, april).
[247] Graphika (2024, september).
[248] *Ibid*.
[249] Graphika (2024, september).
[250] Microsoft Threat Intelligence (2024, april).
[251] Graphika, (2024).
[252] Microsoft Threat Intelligence (2024, april).
[253] *Ibid.*
[254] Graphika (2024, september).

5.3.1 ABCDE-matrise

Som ved de andre casene gis det her en oversikt over casestudien på en håndterlig måte med hovedelementene beskrevet i en ABCDE-matrise (tabell 5.3). Dette skal også gjøre det mulig å raskt sammenligne elementer på tvers av casestudiene.

Tabell 5.3 ABCDE-matrise for case-studie 3

Aktør	Atferd	Innhold	Omfang	Effekt
Kina • Spamouflage	• koordinert inautentisk atferd • falske videoer • KI-generert innhold • skjult innholds-distribusjon	• pro-Kina • undergraving av tillit til valg • aktuelle saker • klima og miljø	• mange falske kontoer • millioner av visninger	Lite nedslag

5.3.2 Erfaringer fra hendelsene

Fire erfaringer fra casestudie 3 peker seg ut:

1. **Påvirkningsaktører eksperimenterer og lærer:** Selv om en avslørt operasjon kan virke useriøs og lite slagkraftig, vil den sannsynligvis gi læring til aktøren, som dermed kan utvikle seg videre.

2. **KI som en universaloversetter:** KI gir en rekke muligheter til påvirkningsaktører. Foruten å generere falskt innhold vil KI også kunne hjelpe aktører med å skape og oversette innhold med mye mer troverdighet, både språklig og kulturelt. Norsk språk og særtrekk antas å bli en mindre terskel å krysse med KI.

3. **Aktører kan skreddersy kreative kampanjer for å nå sine mål:** En kampanje kan være tilpasset regionale eller lokale mål og kan sees forskjellig ut fra område til område. Noen steder ønsker en aktør å skape mistillit eller kaos rundt valg, andre steder ønsker de å promotere meningsfellene sine eller undergrave meningsmotstanderne sine.

4. **Globale interesser skaper insentiver for globale operasjoner:** Særlig Spamouflage Dragon viser at påvirkning ikke bare kan ansees som et våpen i konflikt eller konkurranse, men også som et maktpolitisk virkemiddel som brukes med ulik hensikt mot ulike mål over hele verden. Den lave kostnaden ved slike operasjoner gjør påvirkning til et variert verktøy.

5.4 Delkonklusjon

Disse casestudiene gir et tydelig innblikk i hvordan påvirkningsoperasjoner har utviklet seg både teknologisk og strategisk, med en økende kompleksitet og variert tilnærming. Gjennom analysen av valgpåvirkningen i Frankrike, påvirkningsoperasjoner knyttet til OL i Paris, og Spamouflage Dragon-operasjonen finner vi flere fellesindikasjoner.

For det første er det tydelig at aktørene i økende grad utnytter kunstig intelligens til å generere troverdig og skreddersydd innhold, noe som hever presisjonen og effekten av operasjonene. For det andre viser studiene viktigheten av tidlig og koordinert respons fra myndigheter og plattformer for å begrense skadevirkningene. Samlet sett peker dette mot at påvirkningsoperasjoner rettet mot valg og tilknyttede begivenheter har blitt et lavkostnads- og høyverdiverktøy for strategiske aktører.

6 Analyse

Dette kapittelet samler og analyserer vi de generelle observasjonene fra funnene og casestudiene og gir et helhetlig bilde av påvirkningsoperasjoner i dagens informasjonslandskap. Her drøftes også den teknologiske utviklingen og dens betydning for operasjonenes kompleksitet og gjennomslagskraft. I det neste kapittelet, kapittel 7, vil vi diskutere trender og videreutviklinger innen påvirkningsfeltet.

6.1 Operasjonene blir stadig mer komplekse

Påvirkningsoperasjoner, både generelle og valgsentrerte, er komplekse, tilpasningsdyktige og mangfoldige verktøy som brukes av en rekke aktører med ulike formål og metoder. Disse operasjonene har ikke én enkelt taktikk eller enhetlig strategi; snarere benyttes et bredt spekter av taktikker, teknikker og fremgangsmåter (*tactics, techniques, and procedures* – TTP-er) som tilpasses både mål og kontekst. Teknologiske fremskritt, særlig innen kunstig intelligens (KI), har vært drivende i denne utviklingen, og vi kan forvente stadig flere og mer sofistikerte utfordringer fra aktører som ønsker å påvirke informasjonslandskapet.

6.2 Mangfoldet av aktører øker

Russland, Kina og Iran er blant de mest kjente statlige aktørene innen påvirkningsfeltet i et vestlig perspektiv. Allikevel peker litteraturen også på et økende antall andre aktører, både statlige og ikke-statlige, som utnytter disse verktøyene. Terskelen for å iverksette påvirkningsoperasjoner har blitt senket på grunn av modningen av sosiale medier og andre digitale plattformer, som i dag gir relativt rimelige og effektive kanaler for manipulasjon. Lavere produksjonskostnader, særlig grunnet utviklingen av generativ KI, har gjort det enklere for aktører å skalere opp operasjonene sine. Vellykkede operasjoner har også fungert som kraftfulle demonstrasjoner som kan inspirere og legge til rette for fremtidige operasjoner fra ulike aktører.

6.3 Operasjonene strekker seg over tid med forskjellige faser

For påvirkningsoperasjoner rettet mot valg er det et tydelig tidsløp som strekker seg fra tidlig planlegging til påvirkning etter valget. Operasjonene starter ofte måneder eller år før valget,[255] med oppbygging av infrastruktur og etablering av målrettede nettsider og kontoer på sosiale medier. I den siste måneden intensiveres påvirknings-aktiviteten, inkludert angrep på kandidater og utbredelse av desinformasjon. I de siste 72 timene og på valgdagen ser vi ofte forsøk på å spre forvirring og oppfordringer til å avstå fra å stemme, mens perioden etter valget preges av

[255] Bjørgul et al. (2022, 17. juni).

narrativer som utfordrer legitimiteten til utfallet. Dette viser hvor viktig det er for mottiltak å være strategisk tilpasset operasjonenes ulike faser.

6.4 Forskjellige målgrupper påvirkes med forskjellige metoder

Påvirkningsoperasjoner er målrettet for å maksimere den psykologiske og sosiale effekten. Ulike målgrupper, som brede befolkningsgrupper, spesifikke demografiske grupper, radikale miljøer eller beslutningstakere, påvirkes med utvalgte narrativer og innholdstyper.

Ved å analysere disse gjennom Ben Nimmos fire D-er – *dismiss*, *distract*, *distort* og *dismay* (avvise, forvrenge, distrahere og skremme)[256] – ser vi at operasjoner kan fungere på flere nivåer, som å diskreditere kilder, forvrenge fakta, lede oppmerksomheten bort fra kritiske emner eller skremme publikummet til en ønsket reaksjon.

6.5 Påvirkningsoperasjoner har blitt et statlig, strategisk verktøy

Statlige aktørers påvirkningsoperasjoner er ofte strukturert og målrettede, med spesifikke strategiske målsetninger som tydelig skiller seg fra sporadiske eller opportunistiske innblandinger.

Russland bruker sine påvirkningsoperasjoner for å rettferdiggjøre angrepskrigen mot Ukraina, svekke tilliten til demokratiske institusjoner og polarisere samfunnsdebatten. Kinas operasjoner, derimot, legger vekt på å fremme narrativer som underbygger Kinas politiske og økonomiske interesser, men også til å skape splittelse i vestlige samfunn og avlede oppmerksomhet fra kritikk av Kinas behandling av minoriteter. Iran bruker lignende strategier, med hovedvekt på å utnytte eksisterende splittelse i samfunn de ønsker å påvirke, som Israel og USA.

Disse strategiske målsettingene understreker at påvirkningsoperasjoner fungerer som integrerte deler av statlige utenrikspolitiske verktøy.

6.6 Taktikker og innhold er tilpasset kontekst og mål

Funnene og casene viser at påvirkningsaktører benytter taktikker, teknikker og fremgangsmåter (TTP-er) tilpasset både kontekst og målgruppe. Effektive påvirkningsoperasjoner retter seg ofte mot allerede eksisterende skillelinjer og konflikter i målgruppen, for eksempel sosiale, politiske eller kulturelle spenninger.

Vanlige innholdstyper inkluderer falske narrativer, visuell feilrepresentasjon og polariserende kommentarer. Aktørene utnytter dyptgripende følelser som frykt, angst, mistillit og identitets-problematikk for å appellere til primitive responser og omgå rasjonelle, kognitive filtre. Slike

[256] Corp (2022, 8. mars).

taktikker tilrettelegger for emosjonelt ladet informasjon som får stor gjennomslagskraft, og som kan være vanskelig å motvirke gjennom tradisjonelle, faktaorienterte strategier.

6.7 Valgpåvirkning følger bestemte angrepsvektorer og strategier

For valgrelaterte operasjoner ser vi særlig fem angrepsvektorer: påvirkning av informasjonskonsum, manipulering av borgeres evne til å stemme, angrep på kandidater og partier, undergraving av tilliten til demokratiet, og påvirkning av valgrelatert infrastruktur. Disse vektorene skaper en flerfasettert påvirkningsstrategi, der formålet er å redusere tillit til valgsystemet og forsterke eksisterende sosiale skillelinjer.

Disse spesifikke strategiene viser hvordan påvirkningsoperasjoner målrettes mot kjernefunksjoner i demokratiske prosesser. Casestudie 1 viser gode eksempler på denne typen operasjoner rettet mot valg i 2024 (kap. 5.1).

6.8 Generativ KI er brukt, men ikke mestret

En av de mest transformative teknologiene i denne sammenhengen er generativ KI. Selv om de mest pessimistiske prognosene for valgpåvirkning gjennom KI ikke har materialisert seg i 2024, er KI allerede en integrert del av påvirkningsoperasjoner.

Samtidig er generativ KI fortsatt en umoden teknologi. Det er imidlertid sannsynlig at vi vil se en mer omfattende utnyttelse av KI i fremtidige operasjoner, et tema som vil bli utforsket i delkapittel 7.1. Denne teknologien gir aktører muligheten til å skalere og tilpasse påvirkningsoperasjoner på måter som kan være vanskeligere å avdekke og motvirke.

6.9 Aktørene bruker flere kanaler og selvforsterkende informasjonsmiljøer

En vesentlig lærdom fra casene er bruken av flere kanaler og selvforsterkende informasjonsmiljøer. Påvirkningsoperasjoner opererer på tvers av kanaler og utnytter ofte falske nettsider, klonede nyhetskilder og automatiserte kontoer for å bygge et økosystem av selvbekreftende informasjon. Disse økosystemene gir en informasjonsteknologisk gjenklang, hvor falske narrativer forsterkes på tvers av plattformer og gir publikum inntrykk av at narrativene er bredt støttet og troverdige.

Slike strukturer, som opererer på tvers av ulike nettsteder og plattformer med forskjellig juridisk og modererende praksis, skaper komplekse utfordringer for dem som forsøker å identifisere og demme opp for påvirkningsoperasjonene.

6.10 Bruken av plattformer og kanaler avhenger av modereringen deres

Plattformer varierer sterkt i sin regulering og respons på krav om å fjerne innhold, og flere operasjoner har vist at uregulerte eller uoversiktlige plattformer brukes bevisst for å spre påvirkningsinnhold. Eksempler fra casene viser hvordan meldingstjenester som Telegram benyttes for å både koordinere og spre desinformasjon. Når modererte plattformer som Facebook og Twitter implementerer mottiltak, kan innhold derfor lett migrere til andre plattformer. Dette utfordrer myndighetenes og plattformenes evne til å følge og begrense Påvirkningsoperasjoner som flyter mellom kanaler og plattformer.

6.11 Delkonklusjon

Påvirkningsoperasjoner er dynamiske og tilpasningsdyktige verktøy som utnytter en rekke taktikker og teknikker for å påvirke ulike målgrupper og kontekster. Operasjonene er preget av en høy grad av kompleksitet og utnytter eksisterende sosiale og politiske skillelinjer for å maksimere effekten. Påvirkningsaktører benytter lavkostnadsstrategier og teknologiske fremskritt (særlig KI) til å skalere opp operasjonene sine. Operasjonene er ofte strukturert rundt klare mål, enten det handler om å svekke tilliten til demokratiske institusjoner, polarisere samfunn eller fremme strategiske interesser. Ved å operere på tvers av flere plattformer og kanaler skaper de selvforsterkende informasjonsmiljøer som utfordrer både myndigheter og plattformer i arbeidet med å begrense spredningen av desinformasjon. Variasjonen i plattformenes respons og regulering bidrar til å gjøre mottiltakene mer komplekse og krevende.

7 Fremtidige trender og utviklinger

Påvirkningsoperasjoner er, som vist, under hurtig utvikling. Teknologisk utvikling har en formidabel fremdrift som kan tenkes å muliggjøre nye metoder og nye taktikker, teknikker og fremgangsmåter (*tactics, techniques, and procedures* – TTP-er). Den teknologiske utviklingen kan også gjøre at nye aktører kommer til. Her belyser vi noen av de mest kritiske trendene som vi tror kan ha en effekt i fremtiden.

7.1 Økt bruk av kunstig intelligens

Påvirkningsoperasjoner er i rask utvikling, drevet fremover av teknologiske fremskritt, særlig innen kunstig intelligens. En av de mest betydningsfulle trendene er den økte bruken av store språkmodeller for å produsere og forbedre innhold i kampanjer. Denne utviklingen øker ikke bare produktiviteten, men også troverdigheten av påvirkningsoperasjoner.[257]

Parallelt med dette kan vi forvente en mer avansert bruk av deepfake-teknologi, spesielt innen audio. Denne trenden kan gjøre det enda vanskeligere å skille ekte fra falskt innhold.[258] Videre ser vi en økende tendens til KI-assistert personalisering av påvirkning, hvor innhold skreddersys for spesifikke målgrupper basert på atferden deres på nettet og preferansene deres.[259]

I det visuelle domenet har bruken av KI-genererte nyhetsankere, videoer og memes økt i påvirkningsoperasjoner. Denne trenden representerer en betydelig utvikling i hvordan visuelt innhold brukes for å manipulere og påvirke.[260]

7.2 Mer komplekse spredningsmetoder og taktikker

Mens teknologien bak innholdsproduksjonen utvikler seg, ser vi også en utvikling i hvordan dette innholdet spres. Det er en økende trend mot mer avanserte hybride spredningsstrategier som kombinerer automatiserte systemer med menneskelige operatører. Denne tilnærmingen gjør påvirkningsoperasjoner mer fleksible og vanskeligere å oppdage.[261]

Samtidig har bruken av strategier på tvers av plattformer økt. Aktørene bak påvirkningsoperasjoner sprer innholdet sitt over flere plattformer samtidig, noe som gjør det vanskeligere for enkeltplattformer å effektivt motvirke spredningen.[262]

[257] OpenAI (2024, mai); EEAS (2024, januar); Dan et al. (2021); Hunter et al. (2024).
[258] Labuz og Nehring (2024).
[259] Hunter et al. (2024).
[260] Microsoft Threat Intelligence (2024, april).
[261] Insikt Group (2023, 5. desember).
[262] Nimmo et al. (2023); EEAS (2024, januar).

Som respons på økte mottiltak fra plattformer og myndigheter ser vi også en utvikling av nye teknikker for å omgå deteksjonsmekanismer. Dette inkluderer økt bruk av såkalte usynlig blekk -teknikker (*invisible ink*) og andre metoder for å skjule koordinert aktivitet.[263]

7.3 Målrettede kampanjer mot spesifikke grupper

En annen fremtredende trend er bevegelsen mot mer målrettede kampanjer. Påvirkningsaktører fokuserer i økende grad på bestemte demografiske grupper eller regioner, snarere enn brede, generelle kampanjer.[264] Denne trenden går hånd i hånd med en økende tendens til å utnytte og forsterke eksisterende sosiale og politiske spenninger i mållandene.[265]

Det er også økt aktivitet rundt valg og andre betydningsfulle politiske hendelser.[266] Denne trenden understreker den mulige innvirkning påvirkningsoperasjoner kan ha på demokratiske prosesser og nasjonale sikkerhetsspørsmål.

7.4 Langsiktig strategisk og geopolitisk tenkning

Det er også en tydelig trend mot mer langsiktig strategisk tenkning i påvirkningsoperasjoner, kanskje best belyst i casestudie 3 om Spamouflage Dragon. Dette er spesielt relevant i forsøk på å påvirke yngre demografiske grupper, noe som antyder et fokus på langsiktig opinionsforming.[267]

Parallelt med dette har de geopolitiske målene for påvirknings-aktiviteter blitt bredere. Operasjoner strekker seg nå ofte utover umiddelbare regionale interesser til å omfatte globale mål.[268] Denne trenden indikerer en økende kompleksitet og rekkevidde for påvirkningsoperasjoner som et geopolitisk verktøy.

7.5 Vanskeligere å forske på og motarbeide påvirkningsoperasjoner

To negative trender innen forskning på påvirkning har gjort seg gjeldende i 2024. De sosiale mediene har hevet terskelen for forskeres tilgang til data, og ledende amerikanske institusjoner som jobber med temaet, har blitt svekket eller lukket. Dette kan vise seg å være langvarige utfordringer for arbeidet mot valgpåvirkning, også i Norge.

7.5.1 Redusert tilgang til data fra plattformene

Som følge av Elon Musks overtakelse av Twitter (nå X) har plattformen nedprioritert tiltak som styrker tillit og sikkerhet (*trust and safety*), og for alle praktiske formål stengt ned tilgangen til

[263] Aletha Team (2024); EEAS (2024, januar).
[264] Hunter et al. (2024); EEAS (2024, januar).
[265] Nelson (2024, 9. mai); Insikt Group (2024, 8. mai).
[266] North et al. (2024).
[267] Hunter et al. (2024); EEAS, (2024, januar).
[268] Watts (2024, 4. august); EEAS (2024, januar).

data for forskere. For å få tilgang til data må en forskningsinstitusjon nå gjennom en søknadsprosess hvor man kan få innvilget tilgang til et begrenset datasett. Det minste datasettet i denne kategorien koster per nå 42 000 USD i måneden.[269] Det er bred enighet i forskningsmiljøene om at dette representerer en nedstenging av forskning på påvirkning på X.[270]

Det er ikke bare på Musks X at data blir vanskeligere å samle. Metas populære verktøy for Facebook- og Instagram-data, CrowdTangle, ble stengt i 2024.[271] Det blir erstattet av et nytt produkt, Meta Content Library (MCL), som krever at den som søker, er en ikke-kommersiell forskningsinstitusjon.[272] Det er uklart hvordan Meta forholder seg til statlige forskningsinstitusjoner og forsvars- og sikkerhetssektoren. Nedstengingen av CrowdTangle har ført til protester blant påvirkningsforskere som mener MCL er langt fra en god erstatter.[273]

TikTok og Reddit har også gjort tilgang til data dyrere og vanskeligere.[274]

EU har lenge vært proaktive i å pålegge plattformene reguleringer som skal gjøre det lettere for forskning, overvåking og sikkerhetsarbeid på sosiale meder. Nylig, gjennom forordningen om digitale tjenester (Digital Services Act – DSA), har EU pålagt «veldig store nettplattformer» å gi tilgang til data til utvalgte forskere.[275] Det er enn så lenge ikke en utprøvd prosess, og det gjenstår å se hvor smidig den er. Det skal merkes at DSA ikke ennå er tatt inn i EØS-avtalen, så det er ikke per nå en mulig vei å gå for norske forskere og myndigheter.[276]

7.5.2 Kampen mot kampen mot påvirkning

Påvirkning, og særlig valgpåvirkning, har over tid vært et betent tema i amerikansk politikk. Siden det amerikanske presidentvalget i 2016, som også ble kroneksempelet på spesielt russisk valgpåvirkning, har konservative politikere anklaget både private og statlige institusjoner som har søkelys på problemstillingen, for sensur, bias og brudd på ytringsfriheten.

Det mest prominente eksempelet på dette er kvelningen av Stanford Internet Observatory (SIO). På bakgrunn av sterk motgang og juridiske utfordringer presset frem av republikanske kongressmedlemmer har Stanford University, som eier SIO, avviklet deler av SIO som driver med forskning på påvirkningsoperasjoner, og flere anerkjente eksperter har forlatt eller mistet jobben ved SIO. Selv om universitetet sier at SIO ikke er lagt ned, tyder utviklingen på at

[269] X Corp. (2024). 'X Enterprise API Interest Form'. *X Developer Platform*.
[270] Dang, S. (2024, 6. november). 'Exclusive: Elon Musk's X restructuring curtails disinformation research, spurs legal fears'. *Reuters*.
[271] Ortutay, B. (2024, 15. august). 'Meta kills off misinformation tracking tool CrowdTangle despite pleas from researchers, journalists'. *AP*.
[272] Meta (2024, 24. oktober). 'Meta Content Library and API'. *Meta Transparency Center*.
[273] Kerr, D. (2024, 14. august). 'Meta shutters tool used to fight disinformation, despite outcry'. *NPR*.
[274] UoB Communications (2023, 2. november). 'Study warns API restrictions by social media platforms threaten research'. *University of Bath*.
[275] Windwehr, S., og Selinger, J. (2024, 27. mars). 'Can we fix access to platform data? Europe's Digital Services Act and the long quest for platform accountability and transparency'. *Internet Policy Review*.
[276] Regjeringen (2024, 19. november). 'Forordning om digitale tjenester (Digital Services Act – DSA)'. *Regjeringen.no*.

mandatet og budsjettet tynnes kraftig ned og omdirigeres til å handle om andre problemer enn valgpåvirkning, desinformasjon og påvirkningsoperasjoner.[277]

Et lignende trykk rettes også mot det statlige Global Engagement Center (GEC), en underdivisjon av det amerikanske utenriksdepartementet, som overvåker og kjemper mot utenlandsk påvirkning. På samme måte som SIO er GEC under press fra søksmål, budsjettkutt og politisk motbør fra republikanere i kongressen.[278]

Også en rekke universiteter, ikke-kommersielle organisasjoner og private aktører i kampen mot påvirkning (for eksempel Graphika) er nevnt som mål for søksmål og politiske angrep.[279] Det er fryktet at forskning og overvåking av påvirkningsoperasjoner og valgpåvirkning i USA blir nøytralisert i en påstått kampanje mot sensur og bias. Dette vil være et betydelig tap for kampen mot utenlandsk påvirkning internasjonalt.

7.6 Delkonklusjon

Teknologisk utvikling, spesielt innen kunstig intelligens, forventes å fortsette å forme operasjonenes natur, med økt bruk av personaliserte og visuelle elementer for å skape mer overbevisende og målrettet innhold. Samtidig synes det å være en parallell utvikling i spredningsmetoder, der hybride strategier og operasjoner på tvers av plattformer skaper nye barrierer for deteksjon og mottiltak. Operasjonene blir i tillegg stadig mer strategiske og langsiktige, med aktører som målretter mot spesifikke demografiske grupper og jobber mot bestemte geopolitiske mål. Denne utviklingen understreker hvordan påvirkningsoperasjoner i økende grad tvinnes inn i statlige strategier.

En bekymringsverdig utvikling kan tilskrives krympende tilgang til data og forskningsmiljøers kapasitet. Plattformenes økte restriksjoner på forskertilgang, kombinert med politisk press mot nøkkelinstitusjoner i USA, kan svekke det globale arbeidet med å forstå og motvirke påvirkningsoperasjoner. Selv om EU har tatt skritt for å regulere plattformene gjennom forordningen om digitale tjenester, er implementeringen fortsatt usikker og ufullstendig.

Disse trendene peker på behovet for en samlet innsats på tvers av teknologi, politikk og forskning for å møte fremtidens utfordringer innen påvirkningsoperasjoner.

[277] Newton, C., og Schiffer, Z. (2024, 13. juni). 'The Stanford Internet Observatory is being dismantled'. *Platformer*.
[278] Myers, S. L. (2023, 14. desember). 'State Dept.'s Fight Against Disinformation Comes Under Attack'. *The New York Times*.
[279] Myers, S. L., og Frenkel, S. (2023, 19. juni). 'G.O.P. Targets Researchers Who Study Disinformation Ahead of 2024 Election'. *The New York Times*.

8 Tiltak fra litteraturen

I litteraturen finnes også forslag til tiltak fra både europeiske og andre internasjonale aktører. Disse er generelle og ikke nødvendigvis tilpasset norske forhold. FFI har tidligere utarbeidet en rapport som beskriver tiltak og anbefalinger som kan støtte den norske forsvarssektoren i kampen mot påvirkningsoperasjoner.[280]

8.1 Utvikle og utnytte teknologi

En viktig del av innsatsen mot påvirkningsoperasjoner ligger i å utvikle og utnytte teknologi for å identifisere og motvirke desinformasjon. Til det formålet bør det investeres i avanserte deteksjonsalgoritmer som kan oppdage koordinerte informasjonsoperasjoner, spesielt med tanke på den økende bruken av KI-generert materiale.[281]

Generativ KI representerer både en risiko og en ressurs; selv om KI kan produsere realistisk desinformasjon, kan god overvåkning med KI også bidra til å styrke faktasjekking og raskt kategorisere falske påstander.[282] I litteraturen anbefales det også at disse tiltakene kombineres med regelverk som pålegger plattformer økt ansvar for datatilgang og transparens for at forskere og reguleringsmyndigheter kan vurdere tiltakene i sanntid.[283] Dette bør motvirke den svekkede tilgangen til data fra plattformene.

8.2 Internasjonalt samarbeid om regulering

Regulatoriske rammeverk spiller en avgjørende rolle i å begrense utenlandsk påvirkning, spesielt gjennom sosiale medier. Dette bør utvikles gjennom økt samarbeid mellom EU-medlemsland, NATO og G7 for å koordinere mottiltak.[284] EU har vedtatt forordningen om digitale tjenester, som legger strenge krav til plattformer for håndtering av desinformasjon og politisk annonsering.[285] Norge bør undersøke muligheter for å stille krav til plattformer og andre relevante aktører.

Det finnes flere regulatoriske tiltak under utarbeidelse. For eksempel jobber EU-kommisjonen med streng regulering om transparens i politiske annonser, slik at velgere får innsyn i hvem som står bak slike kampanjer.[286] Sammen med de teknologiske tiltakene bør reguleringsmyndigheter

[280] Sivertsen, E. G., og Buvarp, P. (2024, 5. april). *Forsvar mot fremmedstatlige påvirkningsoperasjoner – etablering av funksjon i forsvarssektoren*. FFI-Rapport 23/01897. Forsvarets forskningsinstitutt.
[281] Microsoft Corporate Blogs (2023, 16. mai). 'Defending the information space from cyber-enabled influence operations'. *Microsoft EU Policy Blog*.
[282] Bateman og Jackson (2024).
[283] Clapp, S. (2024, mars). *Combatting foreign interference in elections.* European Parliamentary Research Service.
[284] *Ibid*.
[285] European Commission (2024). 'The Digital Services Act'. *European Commission.*
[286] European Commission (2023, 7. november). 'Commission welcomes political agreement on transparency of political advertising regulation'. *European Commission*.

arbeide for å sikre datatilgang for forskere, spesielt i valgperioder, for bedre å kunne vurdere effekten av tiltak.[287]

8.3 Utdanning i mediekunnskap og økt mediekompetanse

Utdanning i mediekunnskap er en kritisk komponent for å øke samfunnets motstandskraft mot påvirkningsoperasjoner. Forskning viser at mediekunnskap bidrar til kritisk tenkning og evnen til å gjenkjenne falsk informasjon.[288] Slike tiltak bør utvides regionalt slik at de når ut til sårbare befolkningsgrupper som kanskje ikke har samme tilgang til digital opplæring.[289]

En annen anbefaling fra litteraturen er å utvikle tiltak som styrker individers følelse av kontroll, eller *locus of control*, slik at de aktivt oppsøker troverdig informasjon i stedet for å stole blindt på innhold som presenteres på nettet.[290]

8.4 Samarbeid og informasjonsdeling på tvers i samfunnet

Samarbeid mellom myndigheter, teknologiselskaper og sivilsamfunn er en åpenbar forutsetning for å bekjempe påvirkningsoperasjoner.[291] Litteraturen anbefaler å undersøke det EU kaller et hurtig varslingssystem (*rapid alert system*), som gjør det mulig for medlemsland å dele informasjon om potensielle trusler i forkant av valg.[292] Det bør også etableres tydelige kommunikasjonskanaler mellom forskere og reguleringsmyndigheter, slik at innsikter og data kan deles raskt og effektivt under valgperioder, noe som styrker valgsikkerheten.[293]

Ifølge Carnegie bør beslutningstakere handle som «investorer» og bruke en «porteføljetilnærming» der ulike tiltak mot påvirkningsoperasjoner kombineres og justeres over tid.[294] Dette tillater løpende tilpasning til trusselbildet, samtidig som man minimerer risiko for tilbakeslag.

8.5 Styrking av lokale medier

En styrket lokaljournalistikk er et kritisk, men underprioritert tiltak for å motvirke påvirkningsoperasjoner.[295] Lokale nyhetsmedier spiller en viktig rolle i å opprettholde offentlig

[287] Rolfe et al. (2024).
[288] EDMO (2024). 'The Importance of Media Literacy In Countering Disinformation'. *European Digital Media Observatory*.
[289] Rolfe et al. (2024).
[290] Bateman og Jackson (2024).
[291] EEAS (2024, januar).
[292] Clapp (2024, mars); EEAS (2024, januar).
[293] Rolfe et al. (2024).
[294] Bateman og Jackson (2024).
[295] *Ibid.*

tillit og opplyst samfunnsdiskurs. Støtte til lokale medier kan bidra til å begrense spredningen av desinformasjon ved å skape et pålitelig informasjonsmiljø.[296] [297]

8.6 Forbedret beredskap rundt valg

Det bør utvikles målrettede strategier for å beskytte valg mot påvirkningsoperasjoner, med spesiell vekt på økt overvåking i kritiske perioder før valg.[298] Det er svært viktig at teknologiplattformer samarbeider med nasjonale myndigheter for å identifisere og respondere på trusler som kan påvirke valgutfall.[299]

I tillegg finnes det et behov for forbedrede cybersikkerhetstiltak knyttet til valg og kampanjer. Bedre sikkerhetsrutiner kan redusere risikoen for operasjoner der noen stjeler informasjon og strategisk lekker den (*hack-and-leak operations*), noe som kan påvirke demokratisk tillit og valgdeltakelse.[300]

8.7 Plattformenes rolle og ansvar

Identifisering og fjerning av koordinert inautentisk atferd på sosiale plattformer er essensielt for å redusere påvirkningsoperasjoners rekkevidde.[301] Allikevel, som beskrevet i delkapittel 7.5 virker det som om plattformene tar mer og mer avstand fra slike tiltak, og gjør det vanskeligere å utføre faktasjekking eller overvåkning for tredjeparter.

Dessuten bidrar algoritmer som fremmer engasjement til å intensivere spredningen av desinformasjon.[302] For stor tillit til teknologiske løsninger kan gjøre at vi overser de strukturelle og psykologiske faktorene som driver påvirkningsoperasjoner. Det anbefales derfor en tilnærming som inkluderer faktasjekking, innholdsmerking og regulatoriske tiltak.

8.8 Faktasjekking og avkrefting (*debunking*)

EU-kommisjonen anbefaler å styrke uavhengige faktasjekkingsorganisasjoner, slik at desinformasjon raskt kan avkreftes.[303] Vi kan anbefale at plattformer samarbeider med forskere og sivilsamfunnet for å sikre at faktasjekkere har tilgang til nødvendige data og verktøy for å identifisere og avkrefte falske påstander effektivt.[304]

[296] *Ibid*.
[297] EESC (2023, 12. juni). 'Strong civil society and independent media are the firewall against disinformation'. *The European Economic and Social Committee*; Bateman og Jackson (2024).
[298] North et al. (2024).
[299] Rolfe et al. (2024).
[300] Bateman og Jackson (2024).
[301] Franklin et al. (2024, mai).
[302] Bateman og Jackson (2024).
[303] European Commission (2021, 8. mars). 'Action Plan against Disinformation'. *European Commission*.
[304] Rolfe et al. (2024).

Allikevel må det erkjennes at selv om publikum kan justere sine meninger om bestemte påstander, fører det sjeldent til atferdsendringer.[305] Effekten av faktasjekking varierer avhengig av hvordan informasjonen presenteres og mottas.

8.9 Delkonklusjon

I litteraturen foreslås det flere tiltak for å styrke motstandskraften mot påvirkningsoperasjoner, selv om mange av disse er generelle og ikke nødvendigvis tilpasset norske forhold.

Teknologiske løsninger som avanserte deteksjonsalgoritmer og kunstig intelligens nevnes som essensielle verktøy for å identifisere og motvirke desinformasjon, men teknologi alene er ikke nok. Den må støttes av politiske og regulatoriske tiltak som sikrer transparens og datatilgang, særlig i valgperioder.

Utdanning i mediekunnskap og kritisk tenkning foreslås som langsiktige løsninger for å styrke samfunnets motstandsdyktighet, mens styrket lokaljournalistikk kan bidra til å sikre et pålitelig informasjonsmiljø.

Økt samarbeid mellom myndigheter, teknologiselskaper og sivilsamfunn, i tillegg til tidlige varslingssystemer for informasjonsdeling, fremheves som avgjørende for å bekjempe påvirkningsoperasjoner. Fakta-sjekking og avkrefting av falsk informasjon (*debunking*) er nyttige elementer, men har begrenset effekt uten en bredere strategi.

Samlet peker litteraturen på behovet for et helhetlig rammeverk som kombinerer teknologi, regulering, utdanning og samarbeid for å møte de økende utfordringene med påvirkningsoperasjoner.

[305] Bateman og Jackson (2024).

9 Oppsummering og konklusjon

9.1 Oppsummering

Rapporten begynte med en gjennomgang av konteksten (kapittel 1), metodene (kapittel 2) og litteraturen (kapittel 3) som ligger til grunn for studien. Vi fant (i kapittel 4) at etablerte aktører som Russland, Kina og Iran fortsatt er de mest aktive innen påvirkningsoperasjoner, men så også andre aktører bruke disse virkemidlene. Flere valg i Europa viser tegn til forsøk på valgpåvirkning, ifølge medier og overvåkingsinstitusjoner. Vi gjennomgikk også påvirkningsoperasjoners taktikker, metoder og effekter, inkludert bruken av kombinerte teknikker for å forsterke påvirkningen.

Gjennom tre casestudier (beskrevet i kapittel 5) belyste vi moderne påvirkningsoperasjoner. Den første handlet om valgene i Frankrike sommeren 2024, der operasjoner fra Russland og Iran forsøkte å svekke tilliten til valget og sverte ledende kandidater. Den andre tok for seg OL i Paris, der flere aktører brukte ulike strategier for å fremme politiske og sikkerhetsmessige narrativer. Den tredje casestudien undersøkte Kinas Spamouflage Dragon-operasjon, som demonstrerer at Kina har både ambisjoner og fleksibilitet i informasjonsdomenet.

Analysen (i kapittel 6) bygget videre på funnene og pekte på økende kompleksitet i operasjonene, mer presis målretting og en utvikling der påvirkningsoperasjoner blir et langsiktig strategisk verktøy for stater. Vi forventer (som beskrevet i kapittel 7) at kunstig intelligens og spredningsteknikker vil spille en stadig viktigere rolle fremover, samtidig som tilgang til plattformdata og forskningsmuligheter begrenses, noe som kan svekke fremtidig innsats mot påvirkningsoperasjoner. Allikevel finnes det anbefalte tiltak fra litteraturen og fra FFI (oppsummert i kapittel 8), selv om det heller ikke her kommer frem noen klar, helhetlig løsning på utfordringen.

9.2 Konklusjon

Det er en krevende oppgave å forsøke å holde seg oppdatert på de nyeste utviklingene og trendene innen valgpåvirkning. Dette er et felt i hurtig utvikling, ikke minst med fremveksten av nye teknologier, men også ettersom året har bydd på et rekordantall valg rundt hele verden. Når vi også ser at mange nasjonale, europeiske valg rapporteres som utsatt for informasjons-påvirkning i 2024, er det viktig å kartlegge nåtidens versjon av fenomenet. Dette understrekes av at Romania i desember annullerte et valg på grunn av informasjonspåvirkning.[306]

Et sentralt funn i denne trendstudien er økende kompleksitet i operasjonene. Det kan virke som om påvirkningsoperasjonene som fikk mye oppmerksomhet rundt 2016, var nokså primitive, og at aktører har brukt tiden siden den gang til å modne teknikker og hurtig ta i bruk teknologier. Det skal ikke glemmes at den grunnleggende teknologien som muliggjør mye av dagens

[306] Higgins og Barbulescu (2024, 6. desember).

informasjonspåvirkning, altså internettet og sosiale medier, er relativt nyanskaffede teknologier. Hvordan man bruker slike nye vektorer og kapabiliteter mest effektivt, er noe som kan ta tid å forstå.

Det samme mønsteret kan peke på at den store frykten for KI-baserte påvirkningsoperasjoner inn i 2024 – som ikke materialiserte seg som fryktet – kanskje ikke var direkte overdrevet, men heller noe prematurt. Det virker uansett klokt å begynne å tenke på utfordringene som KI bringer med seg, før de blir fullendt. Da sosiale medier kom for fullt rundt 2005–2010, var det lite debatt og tenkning rundt hvordan de kunne brukes innen påvirkning, og tiltakene har dermed vært forsinket. **Det finnes nå en mulighet for å øke forskning og å utvikle tiltak som kan sikre en fremtid der KI brukes ansvarsfullt.** Arbeid med dette foregår, for eksempel gjennom NATOs KI strategi.[307] Den nasjonale norske KI strategien[308] har generelt behov for en oppdatering siden 2020, og bør ta høyde for påvirkningstrusselen.

Taktikkene, teknikkene og fremgangsmåtene for påvirkningsoperasjoner har blitt mer komplekse og mer integrerte og brukes oftere i sammenheng med hverandre. Der man før kanskje så en mengde av inautentiske, automatiserte brukere som flommet fora med uriktige påstander, ser man nå nettverk av brukere, falske nettsider og spesialiserte meldingsgrupper. Disse bygger opp et komplekst og selvbekreftende økosystem av påstander og narrativer som gir en ny dybde. Dette gir påvirkningsaktørene tre fordeler. **Målgruppene de sikter på, kan falle inn i økosystemet på flere punkter i nettverket, narrativene virker mer troverdige fordi de bekreftes på tvers av tjenester og plattformer, og ikke minst gjør et slikt oppsett arbeidet med å finne, flagge og fjerne desinformasjon vanskeligere.**

Det er også påfallende at det virker som om det også foregår en strategisk modning samtidig som teknikkene og taktikkene innen påvirkning modnes. **Flere aktører virker å ha formet et syn på offensive påvirkningsoperasjoner som et strategisk verktøy, på tilnærmet lik linje med handelspolitikk og diplomati.** Og på samme måte som handelspolitikk og diplomati er kontekstuelle verktøy – som brukes tilpasset for ulike problemsett og mål – så er også den strategiske bruken av informasjonspåvirkning målrettet og kontekstuell. Det peker mot at denne typen påvirkning vil fortsette og kan bli en mer kontinuerlig og integrert del av ulike aktørers forhold til den internasjonale sfæren.

Det har tidligere vært en tendens til å se på påvirkning av valg som en begrenset operasjon, både innen hvilke påstander og argumenter påvirkningsaktørene løfter, og innen målsettinger. I dag kan man se tegn til at aktører påvirker andre land kontinuerlig, med en større forståelse for hvordan påvirkningsoperasjoner passer inn i den helhetlige verktøykassen. Operasjonene er strategiske og integrerte, men også tilpasningsdyktige og opportunistiske.

Vi mener at teknologiutviklingen, den økende kompleksiteten og den strategiske integreringen av påvirkningsoperasjoner kan peke mot en økt trussel for valgpåvirkning, også i Norge.

[307] NATO (2024, 10. juli). 'Summary of NATO's revised Artificial Intelligence (AI) strategy'. *NATO*.
[308] Kommunal- og moderniseringsdepartementet (2020, 14. januar). *Nasjonal strategi for kunstig intelligens*.

Vedlegg

A Søkeord til datainnsamling

Primære søkeord

- election interference
- election influence operations
- foreign influence
- FIMI
- disinformation campaigns
- information operations
- influence operations
- digital propaganda
- voter manipulation
- election integrity
- election security
- informasjonspåvirkning
- påvirkningsoperasjoner
- informasjonsoperasjoner
- desinformasjon
- valgpåvirkning
- velgerpåvirkning

Aktørspesifikke søkeord

- Russian influence operations
- Chinese influence operations
- Spamouflage Dragon
- Doppelganger
- Portal Kombat

Teknologirelaterte søkeord

- AI influence operations
- deepfake election interference
- artificial intelligence disinformation
- LLM disinformation
- AI propaganda

Eksempler på søkestrenger

For FIMI og påvirkningsoperasjoner generelt: ("foreign information manipulation" OR "FIMI" OR "influence operations") AND (Russia OR China OR Iran) AND 2022..2024

For spesifikke aktører og operasjoner: (Russia OR China) AND ("Spamouflage Dragon" OR "Doppelganger" OR "Portal Kombat" OR "Secondary Infektion") AND 2022..2024

For valgpåvirkning: ("election interference" OR "election influence" OR "valgpåvirkning") AND (Russia OR Russland OR China OR Kina) AND 2024

For teknologi og påvirkning: ("artificial intelligence" OR "AI" OR "deepfake") AND ("disinformation" OR "influence operations") AND 2022..2024

For hendelser i 2024: ("French election" OR "Paris Olympics" OR "German election") AND ("interference" OR "influence" OR "disinformation") AND 2024

For norskspråklige kilder: ("informasjonspåvirkning" OR "påvirkningsoperasjoner" OR "valgpåvirkning") AND (Russland OR Kina) AND 2022..2024

B Eksempler på kilder

Med **myndigheter** menes vestlige, demokratiske staters myndigheter og tilknyttede enheter, for eksempel European External Action Service (EEAS), VIGINUM (Frankrike), Global Engagement Center (US State Department) og EU vs Disinfo.

Med **analyseselskaper** menes etablerte, anerkjente selskaper, for eksempel: Microsoft Threat Analysis Center (MTAC), Recorded Future, Graphika, DFRLab, EU DisinfoLab, Institute for Strategic Dialogue og NewsGuard.

Med **forskningsinstitusjoner** menes anerkjente akademiske institusjoner som kjente universiteter eller enheter, for eksempel Stanford Internet Observatory.

Med **organisasjoner** menes anerkjente fora, tenketanker, konsortium og lignende, for eksempel Freedom House, Atlantic Council, World Economic Forum og European Digital Media Observatory (EDMO).

C Kommentarer til bruk av KI-baserte verktøy

Perplexity var et nyttig verktøy til å kjapt finne og sammenstille kilder og informasjon. Den tilførte likevel lite verdi for å løse denne oppgaven hvor vi allerede hadde god oversikt over kilder og inngående kunnskap om temaet.

Elicit og NotebookLM var svært nyttige til å identifisere og sammenstille relevant informasjon fra et omfattende kildegrunnlag. Disse modellene er imidlertid ikke egnet til å produsere forslag til tekst.

ChatGPT og Claude, modeller som skal være egnet til å produsere forslag til tekst, fant vi ikke tilfredsstillende for dette formålet per i dag. Prosessen med å trene opp modellenes «forståelse» ble for tidkrevende, og resultatene i varierende grad ikke til å stole på.

Basert på vår erfaring, kan vi anbefale Elicit til det den er god på: finne kilder og syntetisere informasjon fra store kildegrunnlag. LM Notebook var nyttig til å finne og sammenstille informasjon fra mange kilder, men også den kunne gjøre feil. ChatGPT og Claude fungerer fint til enklere oppgaver, som å foreslå struktur, vurdere tekster og lage sammendrag, men vi klarte ikke å bruke dem til å bearbeide større kildegrunnlag eller produsere god nok tekst basert utelukkende på kildene de fikk. Vi anbefaler å utvise forsiktighet ved bruk av språkmodeller til forskningsarbeid, men vi ser et klart potensial i fremtiden.

Referanser

AI Forensics (2024). *Supporting Evidence: Pro-Russian Ads Campaigns Approved by Meta from May 1 to May 27, 2024 in Italy, Germany, France & Poland.* AI Forensics. https://cmsbackend.aiforensics.org/uploads/Meta_Ads_Follow_up_27_May_24_46d87a3953.pdf

Ajir, M., og Vailliant, B. (2018). 'Russian Information Warfare: Implications for Deterrence Theory'. *Strategic Studies Quarterly,* 12(3), 70-89. https://www.jstor.org/stable/26481910

Alethea Team (2024, 27. mars). *Writing with Invisible Ink*. Alethea. https://ink-alethea.s3.us-east-2.amazonaws.com/Alethea-Writing-With-Invisible-Ink.pdf

Atherton, D. (2023, 7. oktober). 'Incident 573: Deepfake Recordings Allegedly Influence Slovakian Election'. *AI Incident Database*. https://incidentdatabase.ai/cite/573/

Bateman, J., og Jackson, D. (2024). *Countering Disinformation Effectively: An Evidence-Based Policy Guide*. The Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/Carnegie_Countering_Disinformation_Effectively.pdf

Bellingcat (2023, 11. oktober). 'Hamas Attacks, Israel Bombs Gaza and Misinformation Surges Online'. *Bellingcat*. https://www.bellingcat.com/news/2023/10/11/hamas-attacks-israel-bombs-gaza-and-misinformation-surges-online/

Bjørgul, L., Sivertsen, E. G., og Sellevåg, S. R. (2022, 17. juni). *Scenarioer for uønsket påvirkning i forbindelse med norske valg*. FFI-Rapport 22/01424. Forsvarets forskningsinstitutt. https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3074/22-01424.pdf

Blachez, I, og Labbé, C. (2024, 21. august). '2024 Paris Olympics Misinformation Tracking Center'. *NewsGuard*. https://www.newsguardtech.com/special-reports/2024-paris-olympics-misinformation-tracking-center/

Bond, S. (2024, 6. juni). 'This is what Russian propaganda looks like in 2024'. *NPR Transcript*. https://www.npr.org/transcripts/g-s1-2965

Bond, S. (2023, 13. desember). 'Fake social media accounts are targeting Taiwan's presidential election'. *NPR*. https://www.npr.org/2023/12/13/1219080681/fake-social-media-accounts-are-targeting-taiwans-presidential-election

Bradshaw, S., og Howard, P. N. (2018). *The global organization of social media disinformation campaigns*. Journal of International Affairs, 71(1.5), 23-32.

https://ora.ox.ac.uk/objects/uuid:67cd8a98-8b3c-45c0-b07f-5e25b25ea67a/files/madb637c676fc7e1c0d8bd552a32751bc

Brautović, M., og Roško, M. (2024, mai). *Generative AI Use and Disinformation During the Croatian Parliament Elections 2024.* Adria Digital Media Observatory. https://edmo.eu/wp-content/uploads/2024/06/ADMO_report_8.pdf

Buziashvili, E. og Châtelet, V. (2024, 1. august). 'Russia-linked operations target Paris 2024 Olympics'. *DFRLab*. https://dfrlab.org/2024/08/01/russia-linked-operations-target-paris-2024-olympics/

CEDMO (2024, 29. november). 'What disinformation narratives took over Central Europe in the third quarter of 2024?'. *Central European Digital Media Observatory*. https://cedmohub.eu/what-disinformation-narratives-took-over-central-europe-in-the-third-quarter-of-2024/

Charon, P., & Jeangène Vilmer, J.-B. (2021). *Chinese influence operations: A Machiavellian moment*. Institute for Strategic Research (IRSEM), Ministry for the Armed Forces. https://www.irsem.fr/report.html

Clapp, S. (2024, mars). *Combatting foreign interference in elections.* European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/759612/EPRS_ATA(2024)759612_EN.pdf

Corp, S. (2022, 8. mars). *Combatting Disinformation With the Four D's*. Center for Academic Innovation, University of Michigan. https://ai.umich.edu/blog-posts/spotting-fake-news-ben-nimmo-disinformation-misinformation-fake-news-teach-out/

Czarnecka, M. (2023, 10. oktober). 'Polish Election Campaign 'Drowning In Disinformation'. *Barron's*. https://www.barrons.com/news/polish-election-campaign-drowning-in-disinformation-3653f131

Dan, V., Paris, B., Donovan, J., Hameleers, M., Roozenbeek, J., van der Linden, S., og von Sikorski, C. (2021). 'Visual Mis- and Disinformation, Social Media, and Democracy'. *Journalism & Mass Communication Quarterly*, 98(3), 641-664. https://doi.org/10.1177/10776990211035395

Dang, S. (2023, 6. november). 'Exclusive: Elon Musk's X restructuring curtails disinformation research, spurs legal fears'. *Reuters*. https://www.reuters.com/technology/elon-musks-x-restructuring-curtails-disinformation-research-spurs-legal-fears-2023-11-06/

Daukšas, V. (2024, 27. mai). 'Doppelganger journalist FIMI incident from Belarus National State TV against Lithuanian president elections 2024 candidates'. *Debunk.org*. https://www.debunk.org/doppelganger-journalist-FIMI-incident-from-belarus-national-state-tv-against-lithuanian-president-el

DFRLab (2018. 29. august). '#TrollTracker: An Iranian Messaging Laundromat'. *Medium*. https://medium.com/dfrlab/trolltracker-an-iranian-messaging-laundromat-218c46509193

Digitaliserings- og forvaltningsdepartementet (2024). *Fremtidens digitale Norge: Nasjonal digitaliseringsstrategi 2024-2030*. https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/no/pdfs/nasjonal-digitaliseringsstrategi_ny.pdf

Dimitriadis, D. (2023, juni). *Disinformation Landscape in Greece*. EU Disinfo Lab. https://www.disinfo.eu/wp-content/uploads/2023/06/20230623_GreeceDisinfoFS.pdf

EDMO (2024, 27. november). 'Anti-Western Propaganda and Disinformation Amid the 2024 Georgian Parliamentary Elections'. *European Digital Media Observatory*. https://edmo.eu/publications/anti-western-propaganda-and-disinformation-amid-the-2024-georgian-parliamentary-elections/

EDMO (2024, 22. august). 'Disinformation About Politics and the Olympics Takes the Stage in July'. *European Digital Media Observatory*. https://edmo.eu/wp-content/uploads/2024/08/EDMO-Horizontal-.pdf

EDMO (2024). 'The Importance of Media Literacy In Countering Disinformation'. *European Digital Media Observatory*. https://edmo.eu/areas-of-activities/media-literacy/the-importance-of-media-literacy-in-countering-disinformation/

EDMO (2023, november). *Disinformation narratives during the 2023 elections in Europe*. Red. Panizio, E. European Digital Media Observatory. https://edmo.eu/wp-content/uploads/2023/10/EDMO-TF-Elections-disinformation-narratives-2023.pdf

EEAS (2024, juni). 'Doppelganger strikes back: FIMI activities in the context of the EE24'. *European Union External Action Service*. https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf

EEAS (2024, januar). *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence*. European Union External Action Service. https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

EESC (2023, 12. juni). 'Strong civil society and independent media are the firewall against disinformation'. *The European Economic and Social Committee.* *https://www.eesc.europa.eu/en/news-media/press-releases/strong-civil-society-and-independent-media-are-firewall-against-disinformation*

Etterretningstjenesten. (2024). *Kinas globale ambisjoner*. I Fokus 2024 (Kapittel 3). Etterretningstjenesten. https://www.etterretningstjenesten.no/publikasjoner/fokus/Fokus24_innhold/Fokus24_kapittel_3

EU Disinfo Lab (2024). 'What is the Doppelganger Operation? List of Resources'. *EU Disinfo Lab.* https://www.disinfo.eu/doppelganger-operation/

EU Disinfo Lab (2020, juni). *How two information portals hide their ties to the Russian News Agency Inforos*. EU Disinfo Lab. https://www.disinfo.eu/wp-content/uploads/2020/06/20200615_How-two-information-portals-hide-their-ties-to-the-Russian-Press-Agency-Inforos.pdf

EU vs Disinfo (2024, 24 okt.) 'Disinformation Review: Moscow's anger and plan for Moldova'. *EU vs Disinfo*. https://euvsdisinfo.eu/moscows-anger-and-plan-for-moldova/

EU vs Disinfo (2024, 5. juni). 'Elections are battlefields for the Kremlin: Drag everyone down into the mud'. *EU vs Disinfo*. https://euvsdisinfo.eu/elections-are-battlefields-for-the-kremlin-drag-everyone-down-into-the-mud/

EU vs Disinfo (2024, 3. mai). 'Elections are battlefields for the Kremlin: Go after the leaders'. *EU vs Disinfo*. https://euvsdisinfo.eu/elections-are-battlefields-for-the-kremlin-go-after-the-leaders/

EU vs Disinfo (2023, 1. august). 'Disinfo: Elections in Spain don't matter as EU and NATO are real bosses'. *EU vs Disinfo*. https://euvsdisinfo.eu/report/elections-in-spain-dont-matter-as-eu-and-nato-are-real-bosses/

EU vs Disinfo (2023, 8. mars). 'Disinfo: The Russian special military operation in Ukraine uncovered US biological laboratories'. *EU vs Disinfo*. https://euvsdisinfo.eu/report/the-russian-special-military-operation-in-ukraine-uncovered-us-biological-laboratories/

European Commission (2024, mars). *Living guidelines on the responsible use of generative AI in research*. https://research-and-innovation.ec.europa.eu/document/download/2b6cf7e5-36ac-41cb-aab5-0d32050143dc_en?filename=ec_rtd_ai-guidelines.pdf

European Commission (2024). 'The Digital Services Act'. *European Commission.* https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

European Commission (2023, 7. november). 'Commission welcomes political agreement on transparency of political advertising regulation'. *European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4843

European Commission (2021, 8. mars). 'Action Plan against Disinformation'. *European Commission*. https://digital-strategy.ec.europa.eu/en/library/action-plan-against-disinformation

Franklin, M., Hundley, L., Torrey, M., Agranovich, D., og Dvilyanski, M. (2024, mai). 'First Quarter Adversarial Threat Report'. *Meta*. https://transparency.fb.com/sr/Q1-2024-Adversarial-threat-report

Funk, A., Vesteinsson, K, og Baker, G. (2024). *Freedom on the Net 2024: The Struggle for Trust Online*. Freedom House. https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf

Gallagher, C. (2024, 11. mai). 'France warns Department of Foreign Affairs about Russian disinformation targeting Irish voters'. *The Irish Times*. https://www.irishtimes.com/politics/2024/05/11/france-warns-department-of-foreign-affairs-about-russian-efforts-to-extend-disinformation-activities-into-ireland/

Georgiev, G., Petrova, V, og Trabala, K. (2023, 19. apr). *Breaking the Code: Tackling the Interlocking Nexus of Russian and Chinese Disinformation and Illicit Financial Flows in Southeast Europe*. Center for the Study of Democracy. https://csd.eu/fileadmin/user_upload/publications_library/NED_Report_WEB.pdf

Graphika (2024, september). '*The #Americans: Chinese State-Linked Influence Operation Spamouflage Masquerades as U.S. Voters to Push Divisive Online Narratives Ahead of 2024 Election*'. Graphika. https://22006778.fs1.hubspotusercontent-na1.net/hubfs/22006778/graphika-report-the-americans.pdf

Graphika (2023, februar). *Deepfake It Till You Make It: Pro-Chinese Actors Promote AI-Generated Video Footage of Fictitious People in Online Influence Operation*. Graphika. https://public-assets.graphika.com/reports/graphika-report-deepfake-it-till-you-make-it.pdf

Graphika (2019, september). *Cross-Platform Spam Network Targeted Hong Kong Protests: "Spamouflage Dragon" used hijacked and fake accounts to amplify video content*'. Graphika. https://public-assets.graphika.com/reports/graphika_report_spamouflage.pdf

Hanlon, B. (2018). 'Target USA: Key Takeaways from the Kremlin's 'Project Lakhta'.' *The German Marshall Fund*. https://www.gmfus.org/news/target-usa-key-takeaways-kremlins-project-lakhta

Higgins, A., og Barbulescu, M. (2024, 6. desember). 'Romanian Court Annuls Presidential Election Results and Orders a New Vote'. *The New York Times*. https://www.nytimes.com/2024/12/06/world/europe/romania-election-court.html

Hockenos, P. (2024, 17. april). 'Russia Just Helped Swing a European Election'. *Foreign Policy*. https://foreignpolicy.com/2024/04/17/slovakia-president-pellegrini-russia-election-interference-disinformation/

Hunter, L. Y., Albert, C. D., Rutland, J., Topping, K., & Hennigan, C. (2024). 'Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations'. *Defense & Security Analysis*, 40(2), 235-269. https://doi.org/10.1080/14751798.2024.2321736

IFES (2024). 'ElectionGuide'. *International Foundation for Electoral Systems*. https://www.electionguide.org/

Insikt Group (2024, 28. juni). *Sombres Influences: Russian and Iranian Influence Networks Target French Elections*. Recorded Future. https://go.recordedfuture.com/hubfs/reports/TA-2024-0628.pdf

Insikt Group (2024, 9. mai). *Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale*. Recorded Future. https://go.recordedfuture.com/hubfs/reports/cta-2024-0509.pdf

Insikt Group (2024, 8. mai). 'Iran-Aligned Emerald Divide Influence Campaign Evolves to Exploit Israel-Hamas Conflict'. *Recorded Future*. https://www.recordedfuture.com/research/iran-aligned-emerald-divide-influence-campaign-evolves-to-exploit-israel-hamas-conflict

Insikt Group (2023, 5. desember). 'Obfuscation and AI Content in the Russian Influence Network "Doppelgänger" Signals Evolving Tactics'. *Recorded Future*. https://www.recordedfuture.com/research/russian-influence-network-doppelgangers-ai-content-tactics

Irish Independent (2024, 27. november). 'The Indo Daily: Election misinformation and disinformation on the rise in Ireland'. *Irish Independent*. https://www.independent.ie/podcasts/the-indo-daily/the-indo-daily-election-misinformation-and-disinformation-on-the-rise-in-ireland/a599409120.html

Johnston, J. (2024, 27. september). 'Why Britain's 'deepfake election' never happened'. *Politico*. https://www.politico.eu/article/britain-deepfake-election-never-happened-artificial-intelligence-online-content-misinformation/

Jones, M. G. (2024, 24. januar). 'Russia trying to 'hijack' frustration with EU accession delay – North Macedonia FM'. *Euronews*. https://www.euronews.com/my-europe/2024/01/24/russia-trying-to-hijack-frustration-with-eu-accession-delay-north-macedonia-fm

Kerr, D. (2024, 14. august). 'Meta shutters tool used to fight disinformation, despite outcry'. *NPR*. https://www.npr.org/2024/08/14/nx-s1-5074143/meta-shutters-tool-used-to-fight-disinformation-despite-outcry

Khatsenkova, S. (2023, 16. mai). 'Turkey's disinformation elections: Fake videos and wildly misleading claims'. *Euro News*. https://www.euronews.com/2023/05/16/turkeys-disinformation-election-fake-videos-and-wildly-misleading-claims

Khatsenkova, S. (2023, 27. januar). 'A fake death, bullet casings and threats: Czech elections are marred by disinformation'. *Euro News*. https://www.euronews.com/my-europe/2023/01/27/a-fake-death-bullet-casings-and-threats-the-czech-elections-marred-by-disinformation

Klepper, D. (2023, 19. juli). 'Voting fraud claims spread ahead of Spain's pivotal election'. *AP News*. https://apnews.com/article/spain-election-misinformation-trump-25add18d4bacb5a90e423b1925673006

Kommunal- og moderniseringsdepartementet (2020, 14. januar). *Nasjonal strategi for kunstig intelligens*. https://www.regjeringen.no/contentassets/1febbbb2c4fd4b7d92c67ddd353b6ae8/no/pdfs/ki-strategi.pdf

Łabuz, M., og Nehring, C. (2024). 'On the way to deep fake democracy? Deep fakes in election campaigns in 2023'. *European Political Science*. https://doi.org/10.1057/s41304-024-00482-9

Louis, L. (2024, 12. april). 'France fights disinformation as Olympics, elections loom'. *Deutsche Welle*. https://www.dw.com/en/france-fights-disinformation-as-olympics-elections-loom/a-68759644

Meta (2024, 24. oktober). 'Meta Content Library and API'. *Meta Transparency Center*. https://transparency.meta.com/researchtools/meta-content-library

Microsoft Corporate Blogs (2023, 16. mai). 'Defending the information space from cyber-enabled influence operations'. *Microsoft EU Policy Blog*. https://blogs.microsoft.com/eupolicy/2023/05/16/tech-talk-cyber-influence-cybersecurity-ai-dtac/

Microsoft Defender (2024, 19. desember). 'How Microsoft names threat actors'. *Microsoft*. https://learn.microsoft.com/en-us/defender-xdr/microsoft-threat-actor-naming

Microsoft Threat Analysis Center (2024, 17. april). *Nation-states engage in US-focused influence operations ahead of US presidential election*. MTAC. https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2024/04/MTAC-Report-Elections-Report-Nation-states-engage-in-US-focused-influence-operations-ahead-of-US-presidential-election-04172024.pdf

Microsoft Threat Intelligence (2024, april). *Same targets, new playbooks: East Asia threat actors employ unique methods*. Microsoft. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-East-Asia-Report.pdf

Morris, S., Gurzick, D., Guillory, S., og Borsky, G. (2024, 16. mai). 'Countering Cognitive Warfare in the Digital Age: A Comprehensive Strategy for Safeguarding Democracy against Disinformation Campaigns on the TikTok Social Media Platform'. *Information Professionals Association*. https://information-professionals.org/countering-cognitive-warfare-in-the-digital-age/

Myers, S. L. (2023, 14. desember). 'State Dept.'s Fight Against Disinformation Comes Under Attack'. *The New York Times*. https://www.nytimes.com/2023/12/14/technology/state-department-disinformation-criticism.html

Myers, S. L., Hsu, R., og Fassihi, F. (2024, 4. september). 'Iran Emerges as a Top Disinformation Threat in U.S. Presidential Race'. *The New York Times*. https://www.nytimes.com/2024/09/04/business/media/iran-disinformation-us-presidential-race.html

Myers, S. L., og Frenkel, S. (2023, 19. juni). 'G.O.P. Targets Researchers Who Study Disinformation Ahead of 2024 Election'. *The New York Times*. https://www.nytimes.com/2023/06/19/technology/gop-disinformation-researchers-2024-election.html

NATO (2024, 10. juli). 'Summary of NATO's revised Artificial Intelligence (AI) strategy'. *NATO*. https://www.nato.int/cps/en/natohq/official_texts_227237.htm

Nelson, N. (2024, 9. mai). '3-Year Iranian Influence Op Preys on Divides in Israeli Society'. *DarkReading*. https://www.darkreading.com/threat-intelligence/three-year-iranian-influence-op-preys-divides-israeli-society

Newton, C., og Schiffer, Z. (2024, 13. juni). 'The Stanford Internet Observatory is being dismantled'. *Platformer*. https://www.platformer.news/stanford-internet-observatory-shutdown-stamos-diresta-sio/

Nimmo, B., Francois, C., Eib, C.S., Ronzaud, L., Ferreira, R., Hernon, C., og Kostelancik, T. (2020). *Secondary Infektion*. Graphika. https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf

Nimmo, B., Torrey, M., Franklin, M., Agranovich, D., Milam, M., Hundley, L., og Flaim, R. (2023, august). 'Second Quarter Adversarial Threat Report'. *Meta*. https://transparency.fb.com/sr/Q2-2023-Adversarial-threat-report

North, D.A., Levine, D., Sikora, K., og Diossy, N. (2024). 'Building Resilience Against Election Influence Operations: Preparing for the European Elections in 2024 and Beyond – Case-studies'. *The International Foundation for Electoral Systems*. https://www.ifes.org/pub/building-resilience-against-election-influence-operations-/case-studies

O'Sullivan, D., Devine, C., og Gordon, A. (2023, 13. november). 'China is using the world's largest known online disinformation operation to harass Americans, a CNN review finds.' *CNN*. https://edition.cnn.com/2023/11/13/us/china-online-disinformation-invs/index.html

Ortutay, B. (2024, 15. august). 'Meta kills off misinformation tracking tool CrowdTangle despite pleas from researchers, journalists'. *AP*. https://apnews.com/article/meta-crowdtangle-research-misinformation-shutdown-facebook-977ece074b99adddb4887bf719f2112a

OpenAI (2024, mai). *AI and Covert Influence Operations: Latest Trends*. OpenAI. https://downloads.ctfassets.net/kftzwdyauwt9/5IMxzTmUclSOAcWUXbkVrK/3cfab518e6b10789ab8843bcca18b633/Threat_Intel_Report.pdf

Pamment, J. (2020, september). *The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework*. Carnegie Endowment for International Peace (Working Paper). https://carnegie-production-assets.s3.amazonaws.com/static/files/Pamment_-_Crafting_Disinformation_1.pdf

Rainsford, S: (2024, 4. desember). 'Romania hit by major election influence campaign and Russian cyber-attacks'. *BBC*. https://www.bbc.com/news/articles/cgq18w507dko

Regjeringen (2024, 19. november). 'Forordning om digitale tjenester (Digital Services Act – DSA)'. *Regjeringen.no*. https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/forordning-om-digitale-tjenester-digital-services-act-dsa/id2860429/

Riehle, K. (2022). 'Russia and Information Power'. *The Journal of Intelligence, Conflict, and Warfare*, *4*(3), 261–265. https://doi.org/10.21810/jicw.v4i3.4206

Rolfe, T., Schwertheim, H., Döring, M., og Jacobs, E. (2024). *Safeguarding Elections in the Digital Age: Assessing Evolving Electoral Risks and their Mitigation for Online Electoral Integrity*. The Institute for Strategic Dialogue. https://www.isdglobal.org/wp-content/uploads/2024/09/Safeguarding-Elections-in-the-Digital-Age.pdf

Sarı, M. S. (2023, 11. juli). 'Turkish elections 2023 in the shadow of disinformation'. *Heinrich Böll Stiftung*. https://tr.boell.org/en/2023/07/11/turkish-elections-2023-shadow-disinformation

Sauvage, G. (2023, 28. september). 'Slovakia swamped by disinformation ahead of parliamentary elections'. *France24*. https://www.france24.com/en/europe/20230928-disinformation-swamps-slovakia-ahead-of-parliamentary-elections

Schofield, H. (2023, 8. november). 'Star of David graffiti in Paris – the Russian connection'. *BBC*. https://www.bbc.com/news/world-europe-67360768

Scott, F. (2023, 19. mai). 'The role of misinformation in Greece's upcoming elections'. *Logically Facts*. https://www.logicallyfacts.com/en/article/misinformation-greek-elections

Simeonova, M. (2024, 8. november). 'Fool me thrice: The pattern of political instability in Bulgaria, Georgia, and Moldova'. *European Council on Foreign Relations*. https://ecfr.eu/article/fool-me-thrice-the-pattern-of-political-instability-in-bulgaria-georgia-and-moldova/

Sivertsen, E. G., og Buvarp, P. (2024, 5. april). *Forsvar mot fremmedstatlige påvirkningsoperasjoner – etablering av funksjon i forsvarssektoren*. FFI-Rapport 23/01897. Forsvarets forskningsinstitutt. https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3287/23-01897.pdf

Sivertsen, E. G., Buvarp, P. M. H., Lundberg, H., Madsen, L., Albrechtsen, T., Andersen, M. K. K., og Ili, A. S. (2023, 11. desember). *Kartlegging av utenlandsk informasjonspåvirkning på sosiale medier før, under og etter kommunestyre- og fylkestingsvalget 2023*. FFI-Rapport 23/02392. Forsvarets forskningsinstitutt. https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3253/23-02392.pdf

TrustLab (2023, september). *Code of Practice on Disinformation: A Comparative Analysis of the Prevalence and Sources of Disinformation across Major Social Media Platforms in Poland, Slovakia, and Spain.* TrustLab. https://disinfocode.eu/wp-content/uploads/2023/09/code-of-practice-on-disinformation-september-22-2023.pdf

UNDP (2024). 'A 'Super Year' for Election'. *United Nations Development Programme*. https://www.undp.org/super-year-elections

UoB Communications (2023, 2. november). 'Study warns API restrictions by social media platforms threaten research'. *University of Bath*. https://www.bath.ac.uk/announcements/study-warns-api-restrictions-by-social-media-platforms-threaten-research/

U.S. Department of State. (2020, august). *Pillars of Russia's disinformation and propaganda ecosystem*. Global Engagement Center (GEC). https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

U.S. Department of Justice. (2024, 4. september). *Justice Department disrupts covert Russian government-sponsored foreign malign influence operation targeting audiences in the United States and elsewhere*. U.S. Department of Justice. https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

VIGINUM (2024, september). *Summary of the Information Threat to the Paris 2024 Olympic and Paralympic Games*. Secrétariat general de la défense et de la sécurité nationale. https://www.sgdsn.gouv.fr/files/files/Publications/20240919_NP_SGDSN_VIGINUM_Summary%20information%20threat%20Paris2024Games_EN_0.pdf

VIGINUM (2024, juni). *Matryoshka: A pro-Russian campaign targeting media and the fact-checking community*. Secrétariat general de la défense et de la sécurité nationale. https://www.sgdsn.gouv.fr/files/files/20240611_NP_SGDSN_VIGINUM_Matriochka_EN_VF.pdf

VIGINUM (2024, februar). *Portal Kombat: A structured and coordinated pro-Russian propaganda network.* Secrétariat general de la défense et de la sécurité nationale. https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf

Vock, I. (2024, 28. mars). 'Russian network that 'paid European politicians' busted, authorities claim'. *BBC*. https://www.bbc.com/news/world-europe-68685604

Walsh, S., og Thompson, D. (2023, 13. august). 'Combatting Russian Disinformation: Estonia's Response to the War in Ukraine'. *Democratic Erosion Consortium. https://www.democratic-erosion.com/2023/08/13/combatting-russian-disinformation-estonias-response-to-the-war-in-ukraine/*

Watts, C. (2024, 4. august). 'China tests US voter fault lines and ramps AI content to boost its geopolitical interests'. *Microsoft On the Issues*. https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/

Watts, C. (2024, 2. juni). 'How Russia is trying to disrupt the 2024 Paris Olympic Games'. *Microsoft On the Issues*. https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/

Watts, C. (2024, 17. april). 'Russian US election interference targets support for Ukraine after slow start'. *Microsoft On the Issues*. https://blogs.microsoft.com/on-the-issues/2024/04/17/russia-us-election-interference-deepfakes-ai/

WEF (2024, 10. januar). 'Global Risks 2024: Disinformation Tops Global Risks 2024 as Environmental Threats Intensify'. *World Economic Forum*. https://www.weforum.org/press/2024/01/global-risks-report-2024-press-release/

Wesolowsky, T. (2024, 6. april). ''Mushroom Websites' Spread a Deluge Of Disinformation In Bulgaria'. *RadioFreeEurope*. https://www.rferl.org/a/bulgaria-disinformation-mushroom-websites/32893788.html

White, A. L.-I. (2024, 27. oktober). 'Georgian elections raise further concerns about democratic backsliding'. [Pressekonferanse]. *Europaparlamentet*. https://www.europarl.europa.eu/resources/library/media/20241027RES24997/20241027RES24997.pdf

Windwehr, S., og Selinger, J. (2024, 27. mars). 'Can we fix access to platform data? Europe's Digital Services Act and the long quest for platform accountability and transparency'. *Internet Policy Review*. https://policyreview.info/articles/news/can-we-fix-access-to-platform-data

Workman, M., og Nguyen, K. (2024, 29. juni). 'UK Conservatives say ABC analysis that points to foreign interference operation 'highly alarming'. *ABC News*. https://www.abc.net.au/news/2024-06-29/uk-election-pro-russian-facebook-pages-coordinating/104038246

X Corp. (2024). 'X Enterprise API Interest Form'. *X Developer Platform*. https://developer.x.com/en/products/x-api/enterprise/enterprise-api-interest-form

Rogers, K., og Rocha, R. (2019, 24. mai). 'How a suspected Iran-based campaign tried to get Canadian media to spread fake news'. *CBC News*. https://www.cbc.ca/news/science/how-a-suspected-iran-based-campaign-tried-to-get-canadian-media-to-spread-fake-news-1.5143913

Zhang, X. (2024). *Telling China's Story Well' as propaganda campaign slogan: A critical analysis*. Media, Culture & Society, 46(5), s. 1237–1254. https://doi.org/10.1177/01634437241237942

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan, med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs formål

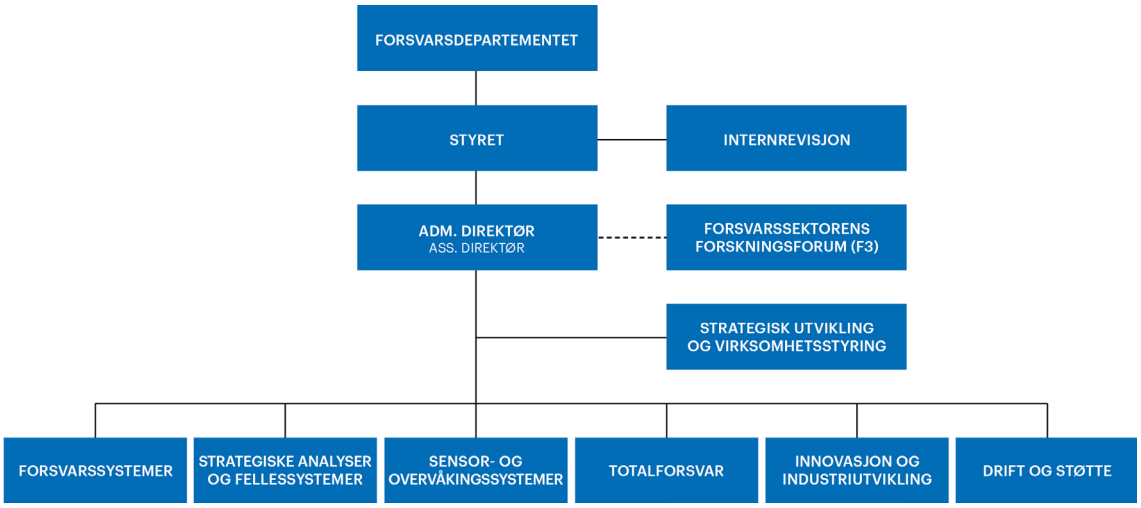
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

FFIs visjon

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs verdier

Skapende, drivende, vidsynt og ansvarlig.



Forsvarets forskningsinstitutt (FFI)
Postboks 25
2027 Kjeller

Besøksadresse:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telefon: 91 50 30 03
E-post: post@ffi.no
ffi.no

Norwegian Defence Research Establishment (FFI)
PO box 25
NO-2027 Kjeller
NORWAY

Visitor address:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telephone: +47 91 50 30 03
E-mail: post@ffi.no
ffi.no/en