Riksrevisjonen

Modeller og maskinlæring
Revisjon, risiko og muligheter

NOKIOS 2023

Jan Roar Beckstrøm
chief data scientist, Riksrevisjonen

Riksrevisjonen

Velferdsstaten er under press

- Kunstig intelligens åpenbart en del av løsningen

- Antallet over 67 år vil øke fra 0,8 millioner i 2020 til 1,1 millioner i 2030 og 1,6 millioner i 2060. Andelen vil da øke fra 16 prosent til 26 prosent.
- Andelen i yrkesaktiv alder (20-66 år) vil avta. I 2060 blir det 2,3 yrkesaktive per person over 67 år. I dag er tallet 4,3.
- Antallet over 80 år vil mer enn dobles, fra 200 000 personer i 2020, til 400 000 i 2030 og 700 000 i 2060. Andelen av totalbefolkningen som er i denne aldersgruppen, vil da øke fra 4 prosent til 12 prosent.

Kilde: Folkehelseinstituttet

Riksrevisjonen

Riksrevisjonen

Dokument 3

Bruk av kunstig intelligens i staten

Riksrevisjonen undersøker hvordan myndighetene sikrer ansvarlig og pålitelig bruk av kunstig intelligens. Vi regner med å offentliggjøre undersøkelsen våren 2024.

Riksrevisjonen

https://english.rekenkamer.nl/publications/reports/2022/05/18/an-audit-of-9-algorithms-used-by-the-dutch-government

POLITICO Enter keyword EXPLORE NEWSLETTERS & PODCASTS POLITICOPRO

FROM POLITICOPRO

Dutch scandal serves as a warning for Europe over risks of using algorithms

The Dutch tax authority ruined thousands of lives after using an algorithm to spot suspected benefits fraud – and critics say there is little stopping it from happening again.

https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/

Auditing machine learning algorithms

A white paper for public auditors

by the Supreme Audit Institutions of Finland, Germany, the Netherlands, Norway and the UK

27 april 2023

Abstract

This paper discusses audits of machine learning (ML) algorithms by Supreme Audit Institutions (SAIs). The paper aims to help SAIs and individual auditors to perform audits on ML algorithms that have been applied by government agencies. It is designed for auditors with some knowledge of quantitative methods. Expert level knowledge of ML-models is not assumed.

We include an audit catalogue - a set of guidelines including suggested audit topics based on risks, as well as methodology to perform audit tests. The paper is accompanied by an Excel helper tool that sums up and guides through different parts of the audit.

First version: 14.10.2020. *auditingalgorithms.net* is maintained by The Office of the Auditor General of Norway (Riksrevisjonen). For inquiries, please contact machinelearning@riksrevisjonen.no.

www.auditingalgorithms.net

Riksrevisjonen

Risiko…
- et enormt tema

Derfor:

Noen mer eller mindre tilfeldige eksempler som jeg håper dere ikke hører om andre steder på NOKIOS ☺

Hvordan sørge for «Meaningful Human Control» med KI-baserte autonome drapsroboter?

AI BUSINESS

STAY UPDATED

ML | NLP | Data | Automation | Verticals | Responsible AI | Companies | More

Pentagon's Replicator: 'Small, Smart, Cheap and Many' Autonomous Systems

In a race with China, DoD takes a page from Ukraine's use of drones to successfully counter Russia's traditional military advantage

Ben Wodecki
September 7, 2023

3 Min Read

https://aibusiness.com/responsible-ai/pentagon-s-replicator-small-smart-cheap-and-many-autonomous-systems

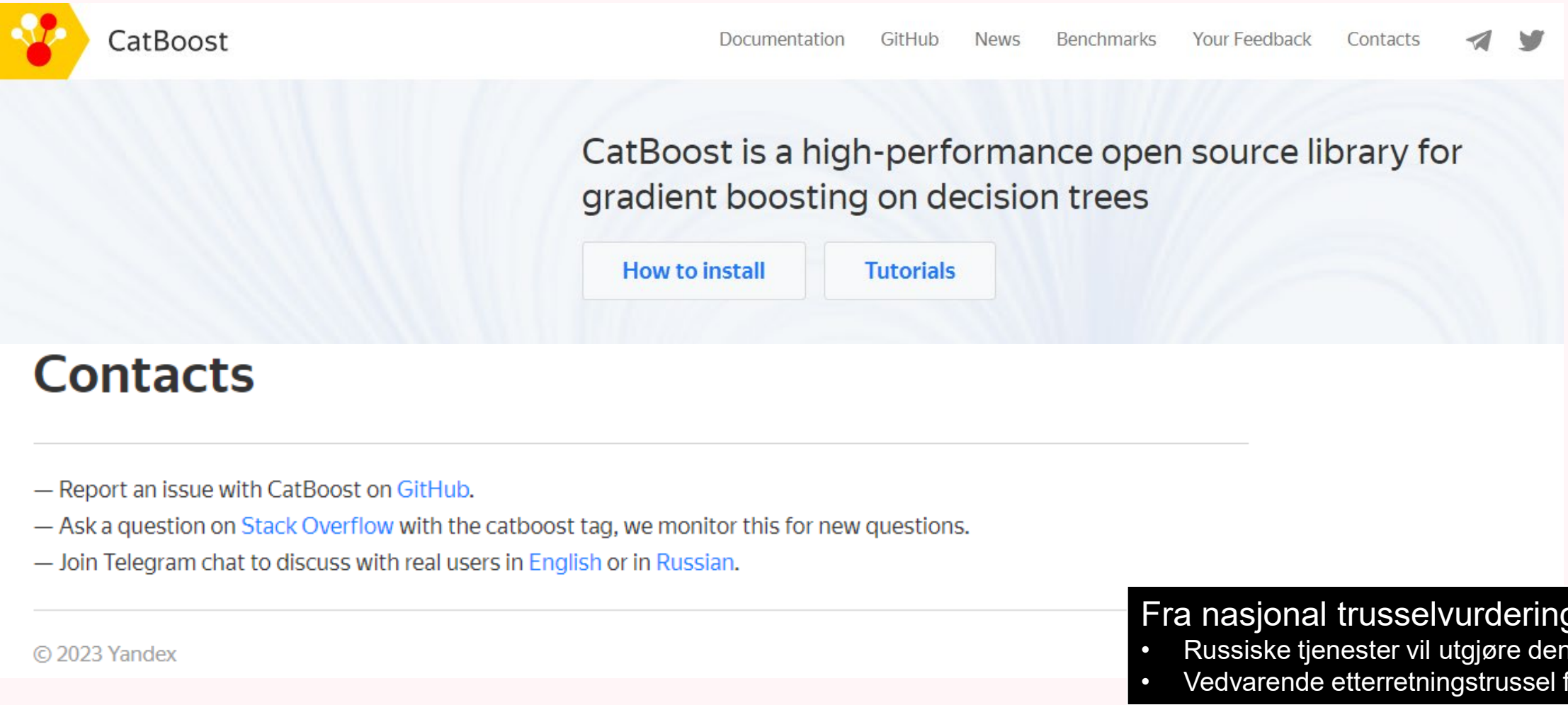
Forsvarsdepartementet

Strategi

Strategi for kunstig intelligens for forsvarssektoren

ML-algos: Hvor kommer de fra...

https://catboost.ai/



Fra nasjonal trusselvurdering 2023:

- Russiske tjenester vil utgjøre den største trusselen
- Vedvarende etterretningstrussel fra Kina

Forgiftning av data

ISJ INTERNATIONAL SECURITY JOURNAL

HOME NEWS PRODUCTS INDUSTRY SECTORS MAGAZINE VIDEOS COMPANIES

Categories: AI & Deep Learning, Cyber Security, Featured News
Tags: Devin Partida

Exclusive: What is data poisoning and why should we be concerned?

September 13, 2021 8:55 am

Data poisoning involves tampering with machine learning training data to produce undesirable outcomes. An attacker will infiltrate a machine learning database and insert incorrect or misleading information. As the algorithm learns from this corrupted data, it will draw unintended and even harmful conclusions.

Kilde: https://internationalsecurityjournal.com/what-is-data-poisoning/

«Fairness through unawareness»

(Også kjent som «prøve å fikse noe, og så blir det bare verre»)

Kjønn → Bias → Diskriminering

Fjern kjønn → problem solved

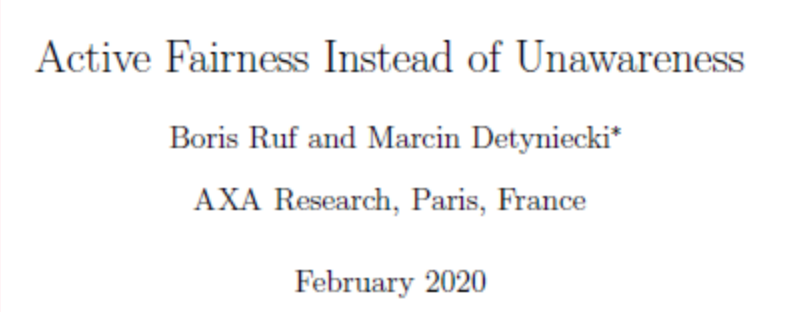
…not

Problemet er multicollinearitet

Typisk en rekke variabler som er korrelert med kjønn (og med hverandre)

Kjønns*dimensjonen* er til stede i data, selv om du fjerner kjønns*variabelen*

Resultat: Du har bare rotet det mer til, og har enda mindre kontroll på bias


Active Fairness Instead of Unawareness

Boris Ruf and Marcin Detyniecki*

AXA Research, Paris, France

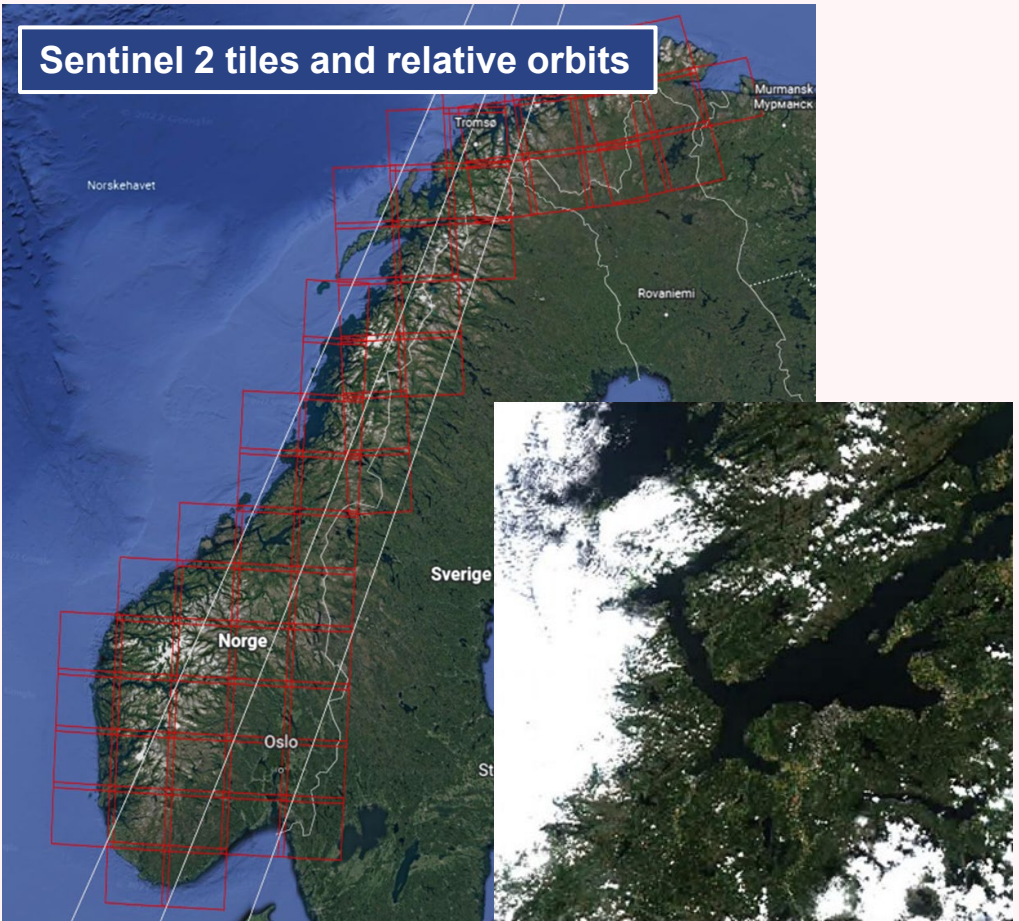
February 2020

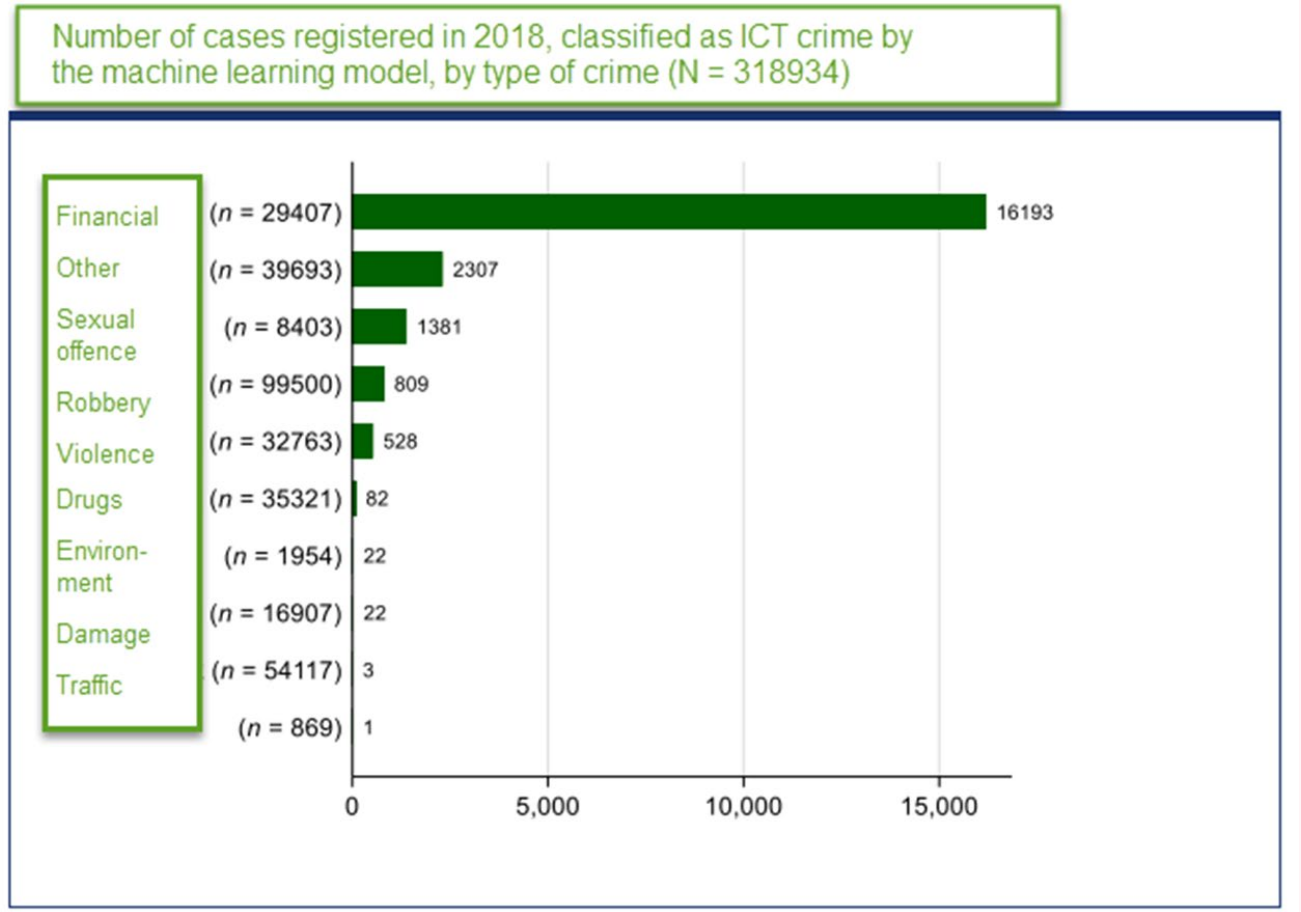
https://arxiv.org/abs/2009.06251

Bruk av ML i revisjonen

To eksempler:

1. Support Vector Machine for å kategorisere kriminalsaker - funket bra
2. Deep Learning på satellittbilder – funket ikke så bra





Og det var det!

Takk for oppmerksomheten!

Epost: jrb@riksrevisjonen.no