Defensie Materieel Organisatie
Ministerie van Defensie

Defensie Innovatie Competitie 2017

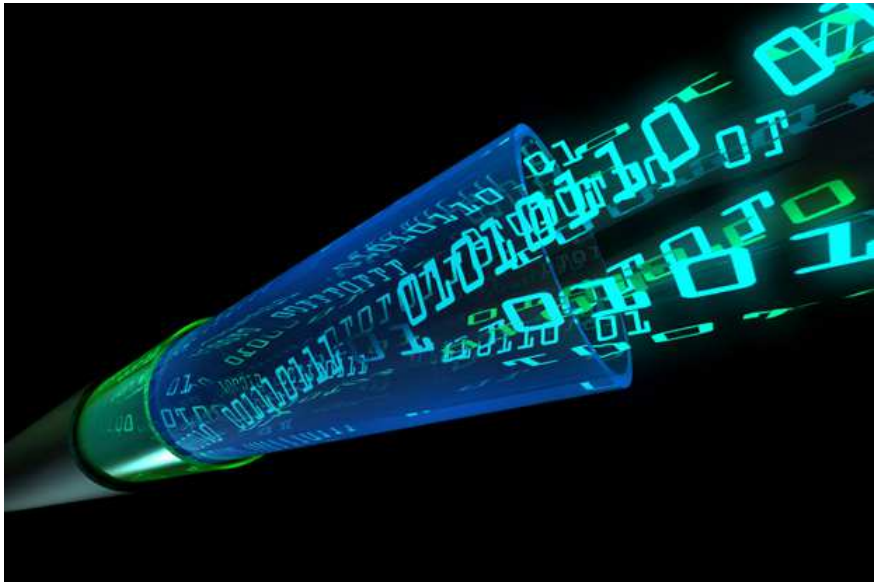
Correlatiealgoritmen & anomaliedetectie

DMO
JIVC / KIXS

17 juli 2017

Overzicht

- Cyber data analytics: wat is het?
  (correlatiealgoritmen en anomaliedetectie)
- Huidige situatie
- Toekomstbeeld
- Uitdagingen

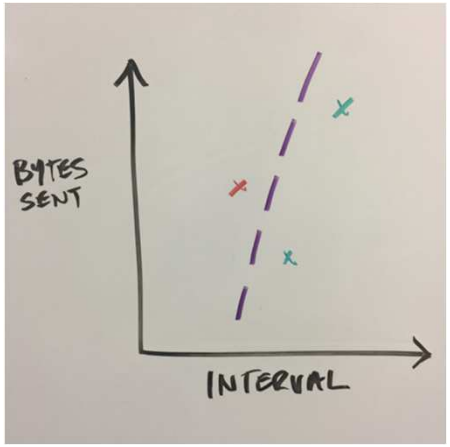


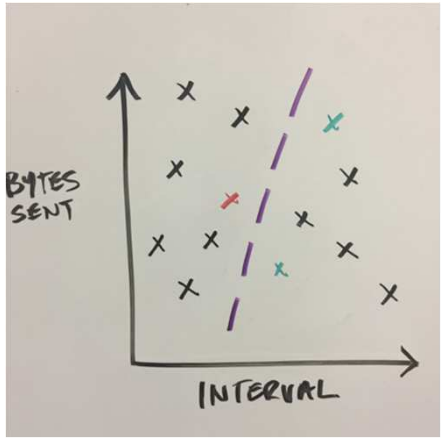

富嶽三十六景
神奈川沖
浪裏

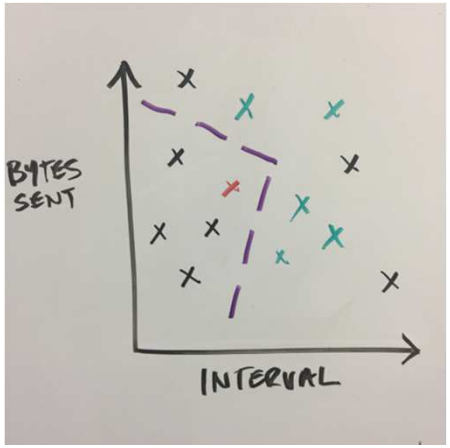
Wat is het?

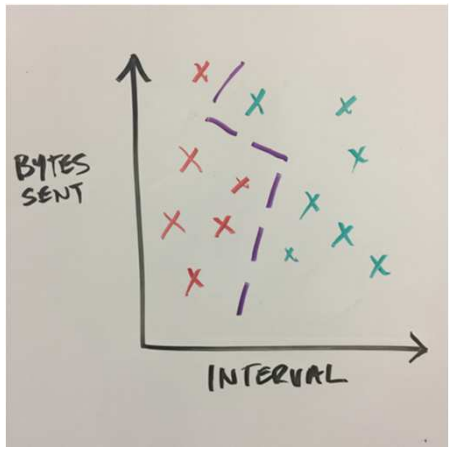
- M&T voor het detecteren van zinvolle samenhangen in dataverzamelingen
- Meer-dimensionale datapresentatie en –analyse
- Ontdekken van aan het oog onttrokken verbanden
- Het gaat om oorzakelijke verbanden
- Oorzaak ‘is ongelijk aan’ correlatie
- Presentatie van de gevonden patronen
- Validatie en verificatie van de resultaten

Supervised learning

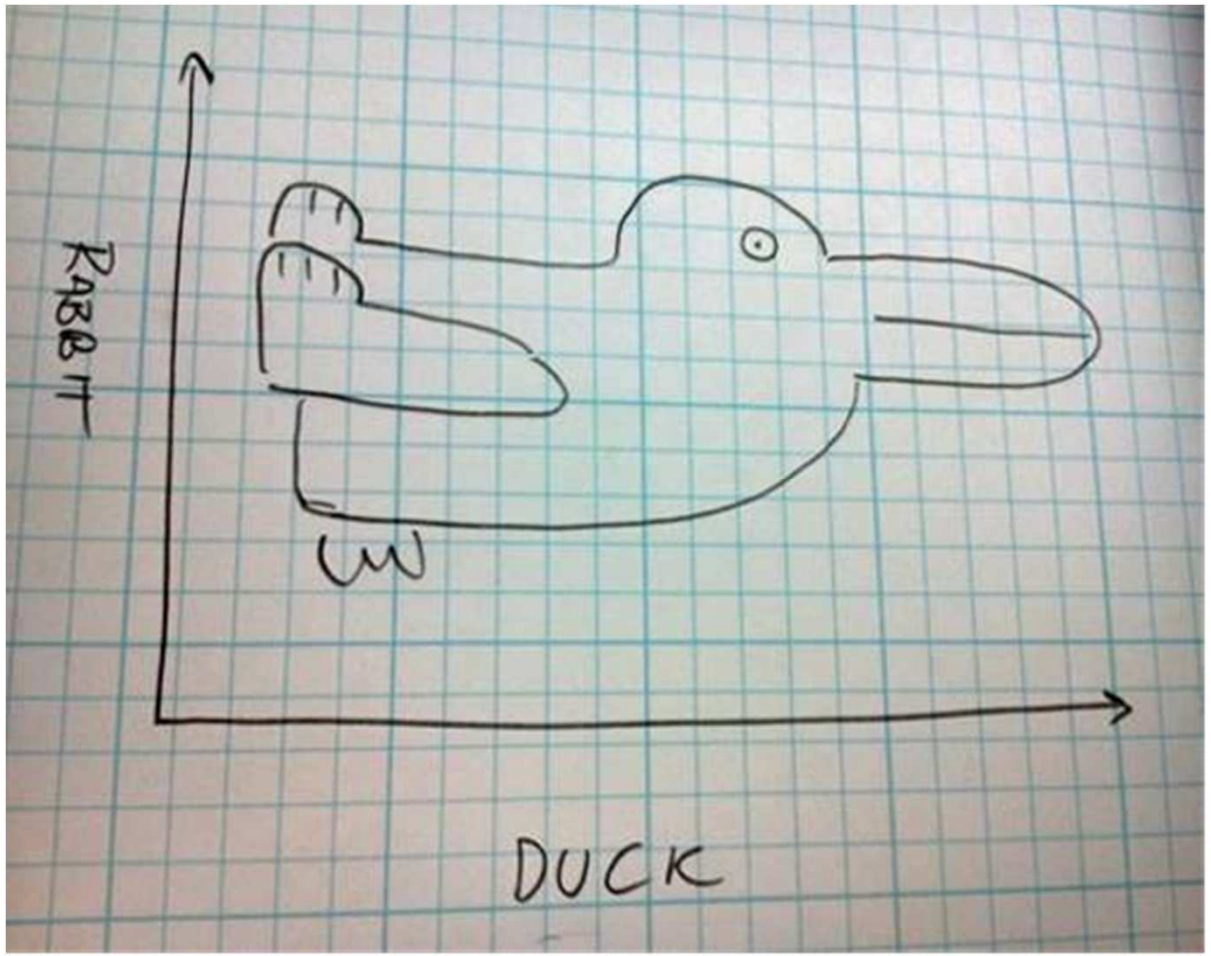








Supervised learning?

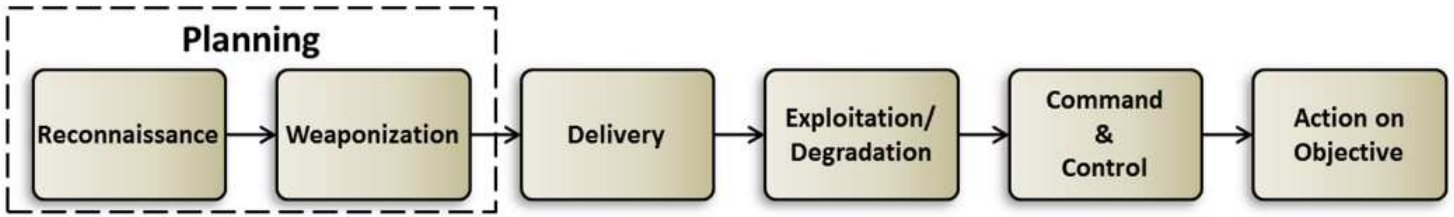


Huidige situatie

- We maken o.a. gebruik van Intrusion Detection Systemen (IDS)
- Er zijn veel gegevens, maar hoe hou je zicht op betekenisvolle patronen?
- Kunnen teruggrijpen op de rauwe gegevens
- Aandacht voor herleidbaarheid
- Is het wenselijk om zowel binnen als buiten onze infrastructuur te kijken?
- Welke rol spelen gedragspatronen?

Huidige situatie 2

- Cyberaanval verloopt in fasen, waarin verschillende activiteiten waarneembaar zijn



- Nieuwe patronen zijn moeilijk detecteerbaar
- Forensisch onderzoek is noodzakelijk
- Technische informatie (infrastructuur) en activiteiten en gedrag van actoren zijn mogelijk afleidbaar uit openbare bronnen
- Welke indicatoren zeggen iets over intenties van actoren?

Huidige situatie 3

- Meer sensoren op meer plekken, gerichter inzetten, sneller verwerken en op basis van ‘beperkte kennis’ bij analisten beter kunnen analyseren
- De resultante van dit proces is onder meer de basis voor cyber situational awareness

Typen cyberincidenten

Cyber Event Type	Description
Unauthorized Access	An individual gains logical access without permission to a network, system, application, data, or other resource.
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources.
Malicious Code	Successful installation of malicious software that infects an operating system or application.
Scans/Probes/ Attempted Access	Activity that seeks to access or identify a computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.

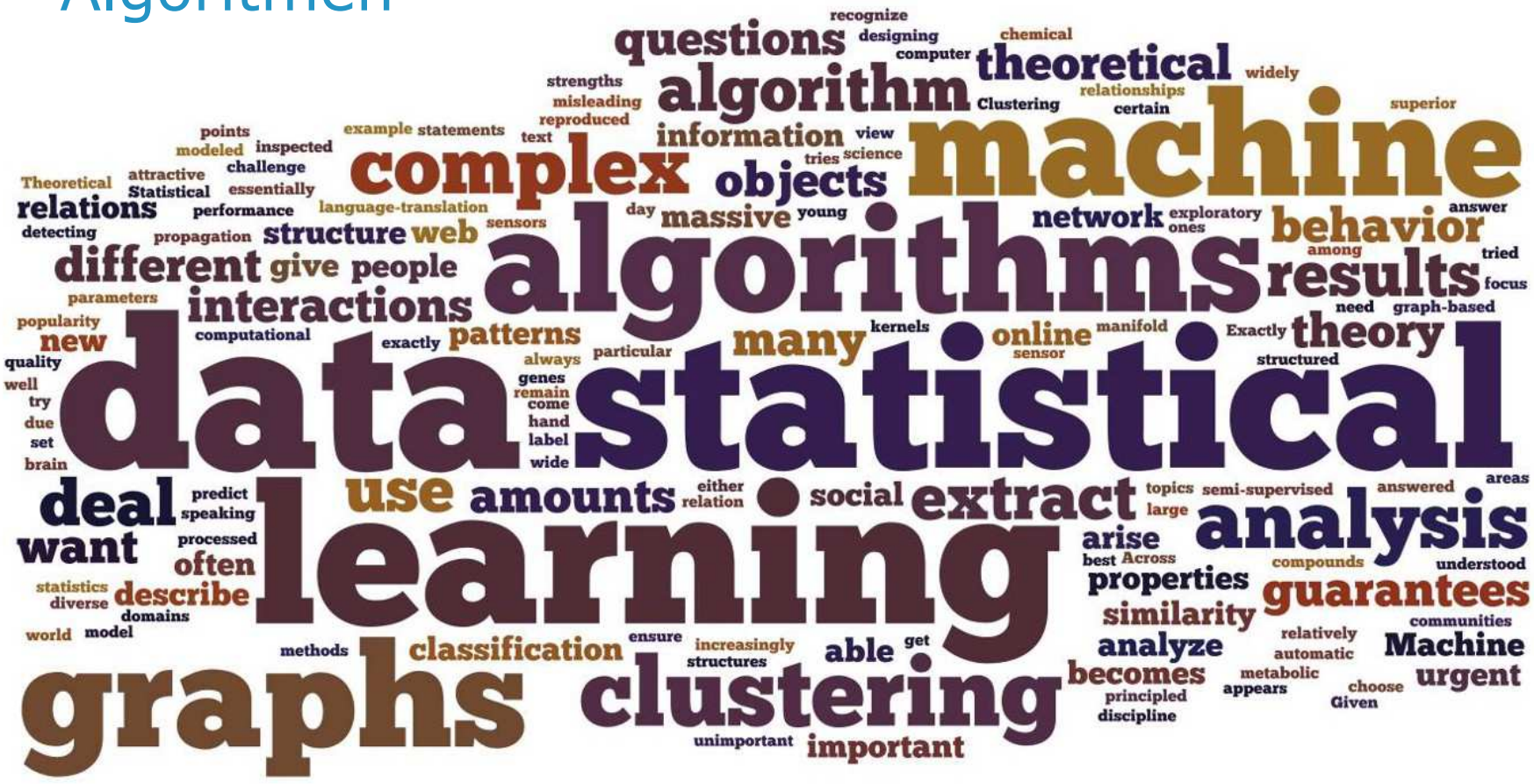
Uitdagingen

- Verwerken grote volumes en variëteit van ‘noisy’ gegevens
- Ontwikkelen en valideren van nieuwe (onconventionele?) methoden & technieken
- De mens (analist) moet complementair zijn aan het mechanisme (algoritme)
- Rekening houden met veroudering van gegevens en informatie
- Rekening houden met socio-culturele en linguïstische factoren

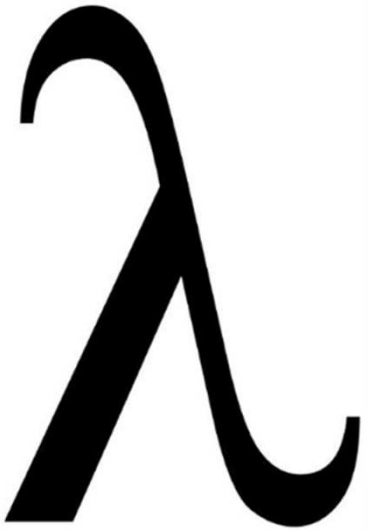
Uitdagingen 2

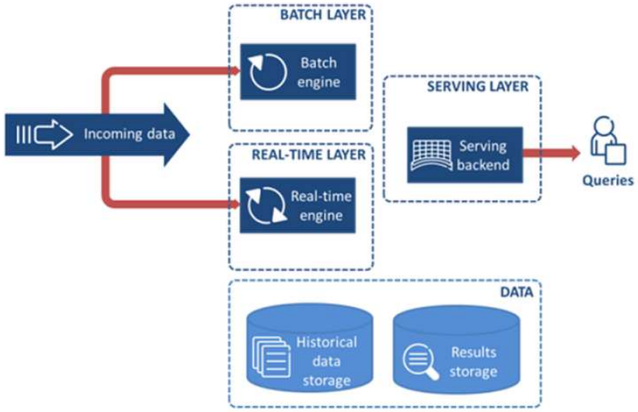
- Hoe gaat Big Data om met de consequenties van toegenomen encryptie?
- Hoe kan zeker gesteld worden dat we structureel meer dingen in kortere tijd kunnen aanpakken: dus géén éénmalige oplossing
- Sizing, focusing, ‘waar’ wegblijven
- Oplossing is een AANPAK, niet zozeer 1 ALGORITME

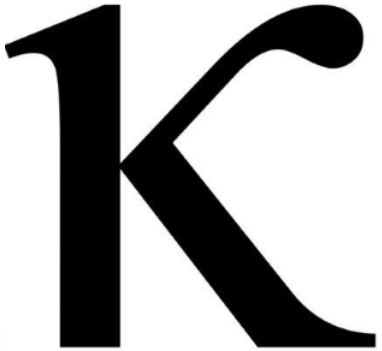
Algoritmen

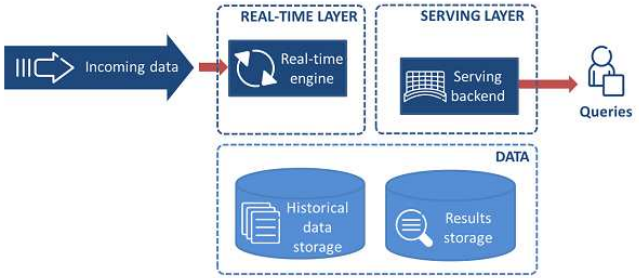

recognize
questions
designing
chemical
computer
theoretical
widely
strengths
misleading
reproduced
algorithm
Clustering
relationships
certain
superior
machine
points
modeled
inspected
example
statements
text
information
view
tries
science
challenge
Theoretical
attractive
Statistical
essentially
complex
objects
relations
performance
language-translation
day
massive
young
network
exploratory
ones
behavior
answer
among
detecting
propagation
structure
web
sensors
different
give
people
algorithms
results
tried
focus
parameters
interactions
need
graph-based
popularity
new
computational
exactly
patterns
kernels
online
manifold
Exactly
theory
quality
always
particular
many
sensor
structured
well
genes
data
statistical
try
remain
come
due
hand
set
label
brain
wide
areas
deal
predict
speaking
use
amounts
either
relation
social
extract
topics
semi-supervised
answered
large
want
processed
often
learning
arise
analysis
best
Across
compounds
understood
statistics
diverse
describe
properties
guarantees
domains
similarity
communities
world
model
relatively
analyze
automatic
Machine
methods
classification
ensure
increasingly
structures
able
get
becomes
metabolic
urgent
graphs
clustering
principled
appears
choose
discipline
Given
unimportant
important

Architecturen

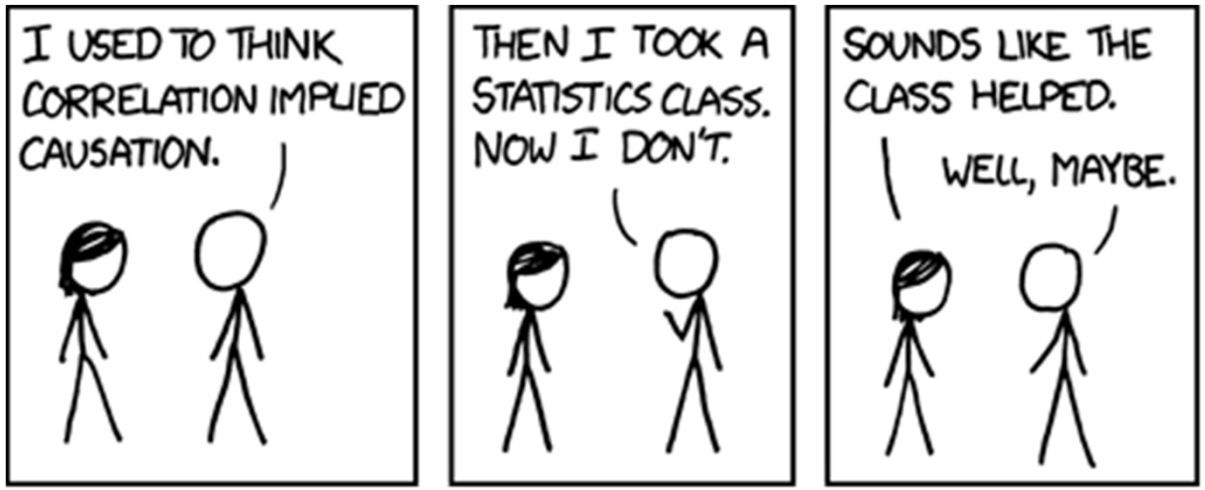








Causaliteit en correlatie



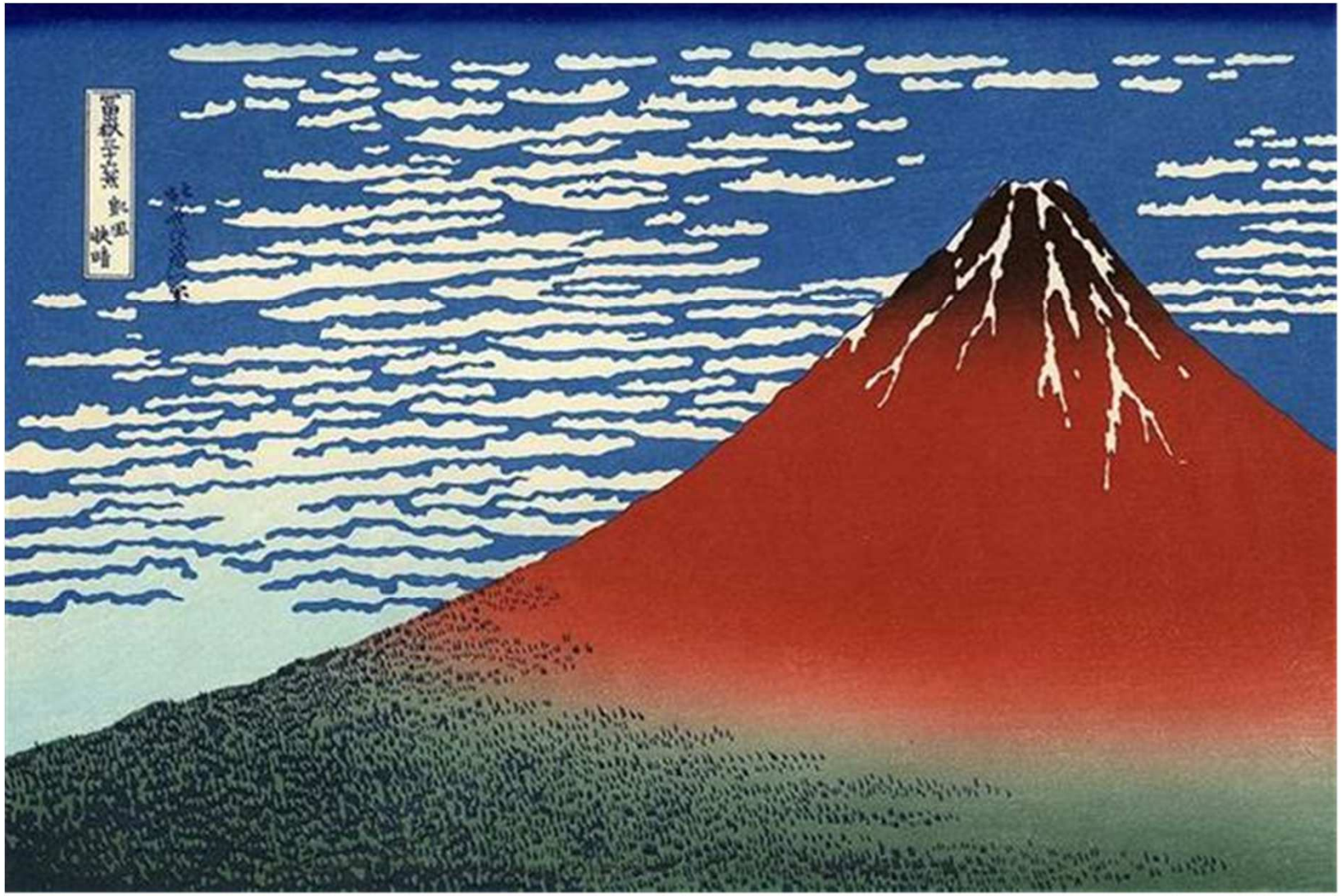
Toekomstbeeld

- Detecteren dreigingsindicatoren en voorspellen cyberaanvallen (aanvulling op bestaande IDS'en)
- Sneller zicht op dreigingsindicatoren (uren tot dagen sneller!)
- Efficiënte en effectieve algoritmen voor de verwerking van grote hoeveelheden gegevens
- Fuseren van gegevens uit verschillende bronnen
- Samenwerking tussen mens (analist) en machine (algoritme)
- Test en evaluatie van de gebruikte algoritmen

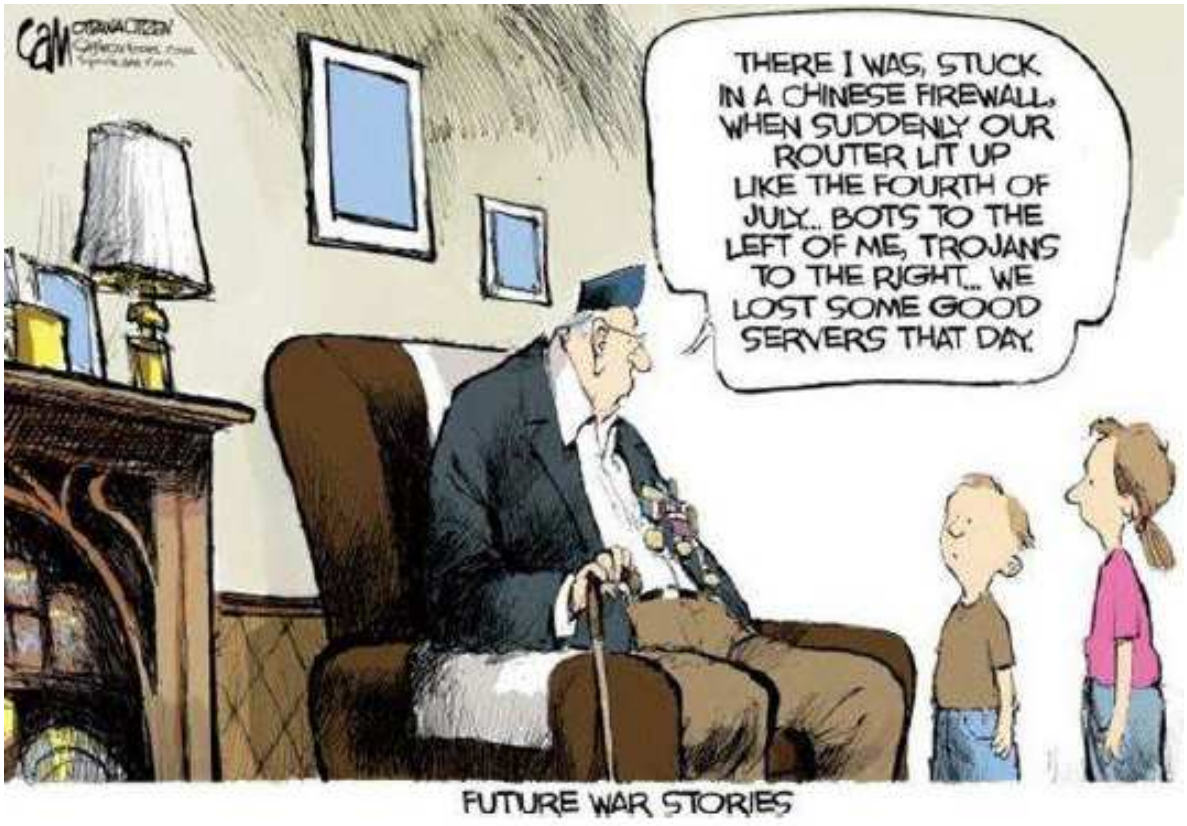
Toekomstbeeld 2

- Help ons met zo min mogelijk sensoren een zo zinvol mogelijke analyse uit te voeren!
- Exploratie: perception, comprehension, projection
- Hoe kunnen we het zelf-lerend vermogen versterken?
- ‘Honderd perspectieven op cyber data analytics’


竹林の不二
富嶽百景二編



Vragen?


THERE I WAS, STUCK IN A CHINESE FIREWALL, WHEN SUDDENLY OUR ROUTER LIT UP LIKE THE FOURTH OF JULY... BOTS TO THE LEFT OF ME, TROJANS TO THE RIGHT... WE LOST SOME GOOD SERVERS THAT DAY.
FUTURE WAR STORIES