



Using AI in domain name registries: threats and opportunities

Thijs van den Hout (SIDN Labs, .nl)

CENTR Jamboree L&R | Belgrade

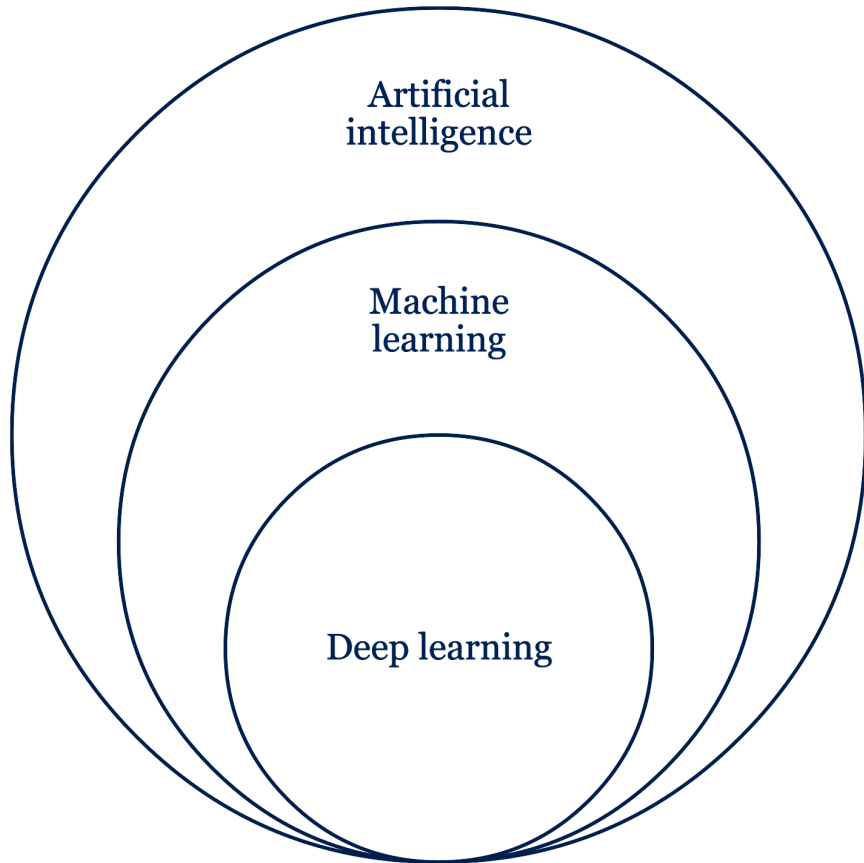
June 1, 2023

Agenda



1. What's AI / Machine Learning (ML)?
2. Use of ML in registry-developed projects
3. Use of existing AI tools internally in registries
4. Threats & opportunities

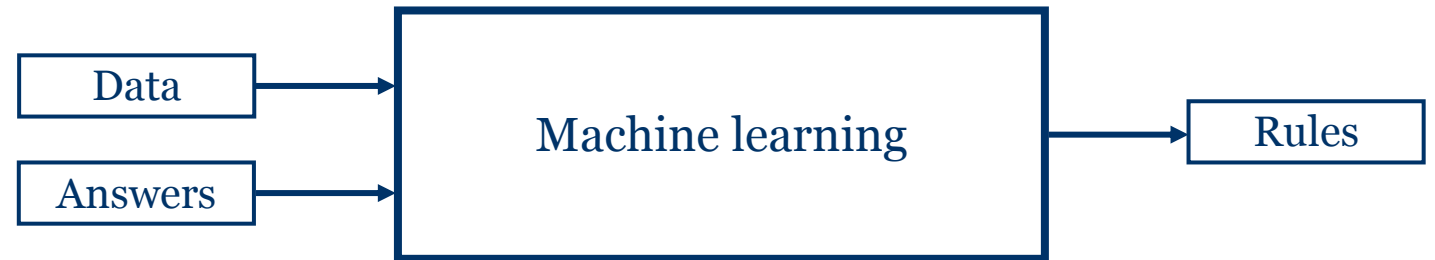
What is AI/ML (not)?



Knowledge-driven programming



Data-driven programming



Different AI tasks

Descriptive AI



Predictive AI



Generative AI

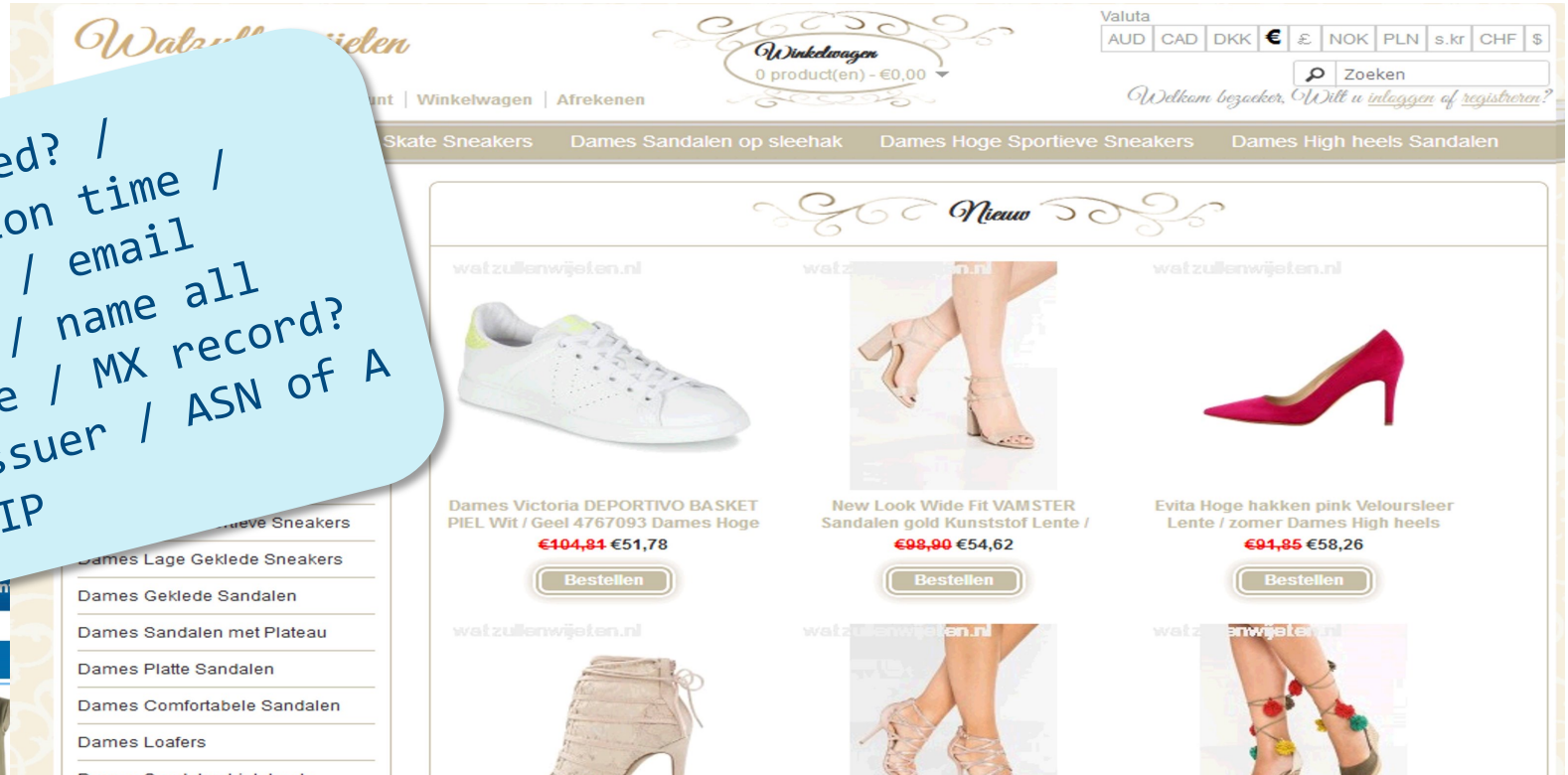
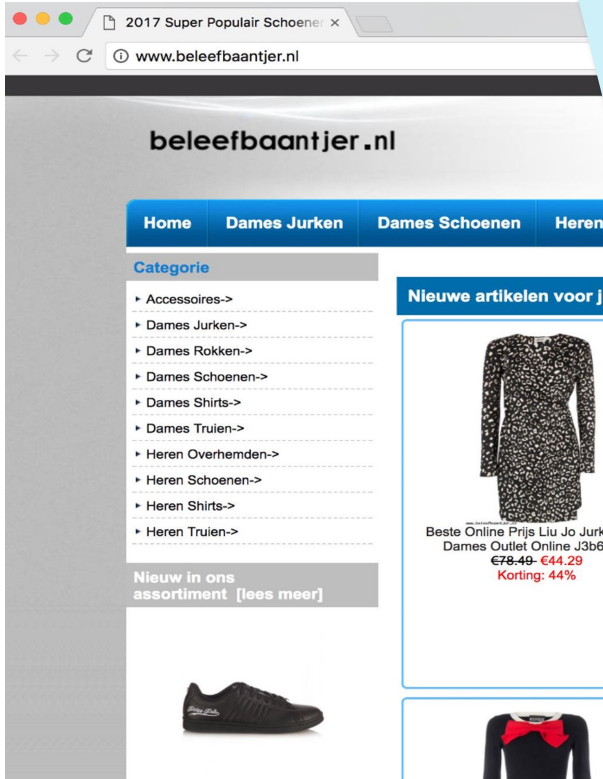


Use of Machine Learning in R&D-born projects



Detecting fake webshops (FaDE)

Reregistered? /
registration time /
registrar / email
provider / name all
lowercase / MX record?
/ TLS issuer / ASN of A
record IP



Detecting logos to find abuse (*Logomotive*)

Pagina's

- Home
- Problemen
- Vragen
- Nieuws
- Video's
- Quizen
- Over ons

Volg ons

- Facebook
- Twitter
- Instagram
- YouTube
- Vimeo

Privacyverklaring Cookieverklaring Responsible disclosure Disclaimer DigiD

Website screenshots /
known logo positions /
logo type

Een initiatief van:

rijksoverheid 0.9 **rijksoverheid 0.98**

Ministerie van Economische Zaken en Klimaat Nationaal Cyber Security Centrum Ministerie van Justitie en Veiligheid ECP Platform voor de InformatieSamenleving

Mede mogelijk gemaakt door:

kpn vodafone Ziggo Betaalvereniging Nederland sidn 0.97 SIDN T-Mobile Google

Microsoft **POLITIE** thuiswinkel 0.95 thuiswinke .org SENIORWEB mediateam SIC

NLdigital FRAUDEHELPDESK.nl ACM ConsuWijzer Co-financed by the European Union Connecting Europe Facility

veilig internetten.nl

EN | **NL**

rijksoverheid 0.98

Inloggen bij DigiD GGD Online

Hoe wilt u inloggen?

- Met de DigiD app
De makkelijkste manier om veilig in te loggen
- Met een sms-controle
- Met mijn identiteitskaart

Annuleren

Kunt u niet verder? Download dan de DigiD app [opent in een nieuw venster] of activeer de sms-controle [opent in een nieuw venster]

Nog geen DigiD? Vraag uw DigiD aan

Vraag en antwoord

- Ik ben mijn gebruikersnaam vergeten
- Hoe kan ik de sms-controle activeren?
- Waar download ik de DigiD app?

Geen antwoord op uw vraag?
Bekijk de DigiD website [opent in een nieuw venster] of **neem contact op** [opent in een nieuw venster]

Assign economic activity to domain names (*WebCola*)

- Statistical classification of economic activities in the European Community (NACE)
- The Domain Industry Taxonomy (DIT)

Page title / HTML content
/ meta tags / description
/ domain name / resolver
preference / known
categories



Identifying suspicious domain registrations (*RegCheck*)

securepaymentportal.nl WHOIS DRS Historie Website KASM

Risk score 90%

Name Stichting Internet Domeinregistratie Nederland

Address ▲ fake address, 12345AB Randomsterdam, NL

Email

Phone

Registrar

Reseller

Registration date

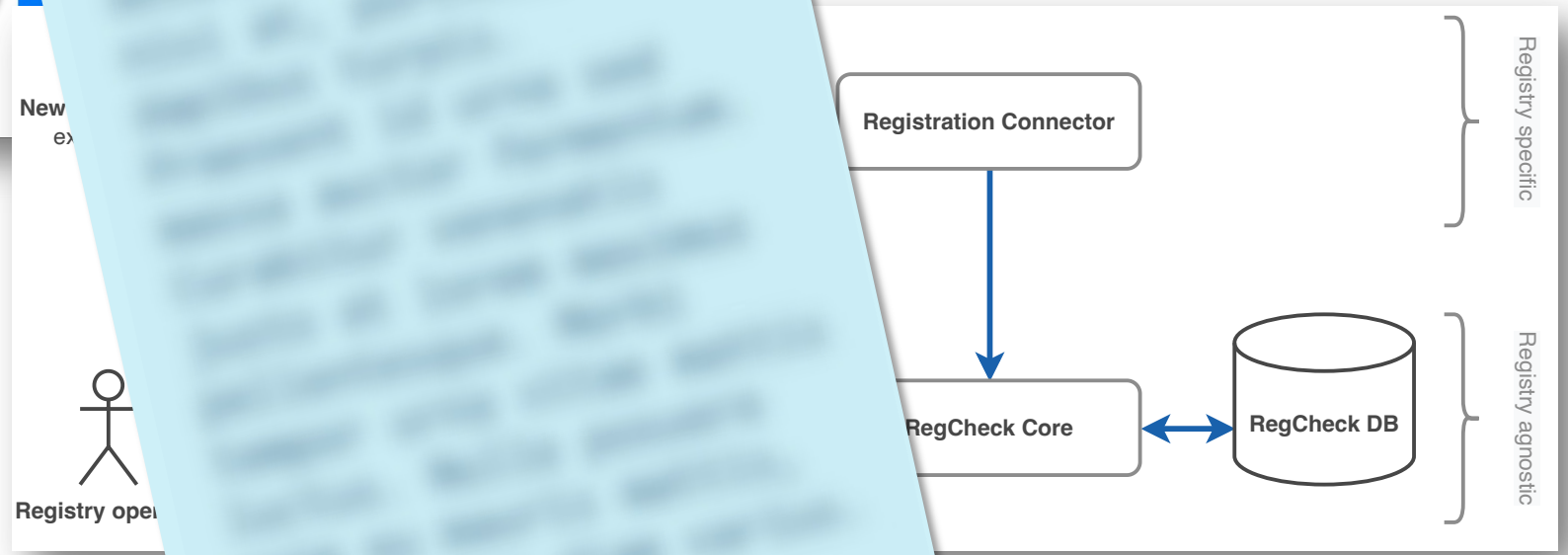
Name servers

Comment
Could be a scam, given the word 'pay' and invalid address. I will verify registrant's identity.

High-risk registration Done
 Registration invalid

Number of suspicious key words in domain / registered at night / more than 1 hyphen / bad reputation country

Domain name characters / inconsistencies in registrant data /







Future work: Domain name suggestion tools

centr.nl is already taken

[Show me details.](#)

Choose an alternative domain name

NB: registering a domain name can be unlawful or indecent, or infringe someone else's rights (e.g. trademark rights).
[See what your responsibilities are](#)

- uwcentr.nl
- onlinecentr.nl
- onzecentr.nl 
- centr2023.nl 
- dollarcent.nl 
- centrshop.nl 

● ● ●

Show more domain names >

Pre-trained language model / descriptions of websites / domain names



Use of AI tools internally

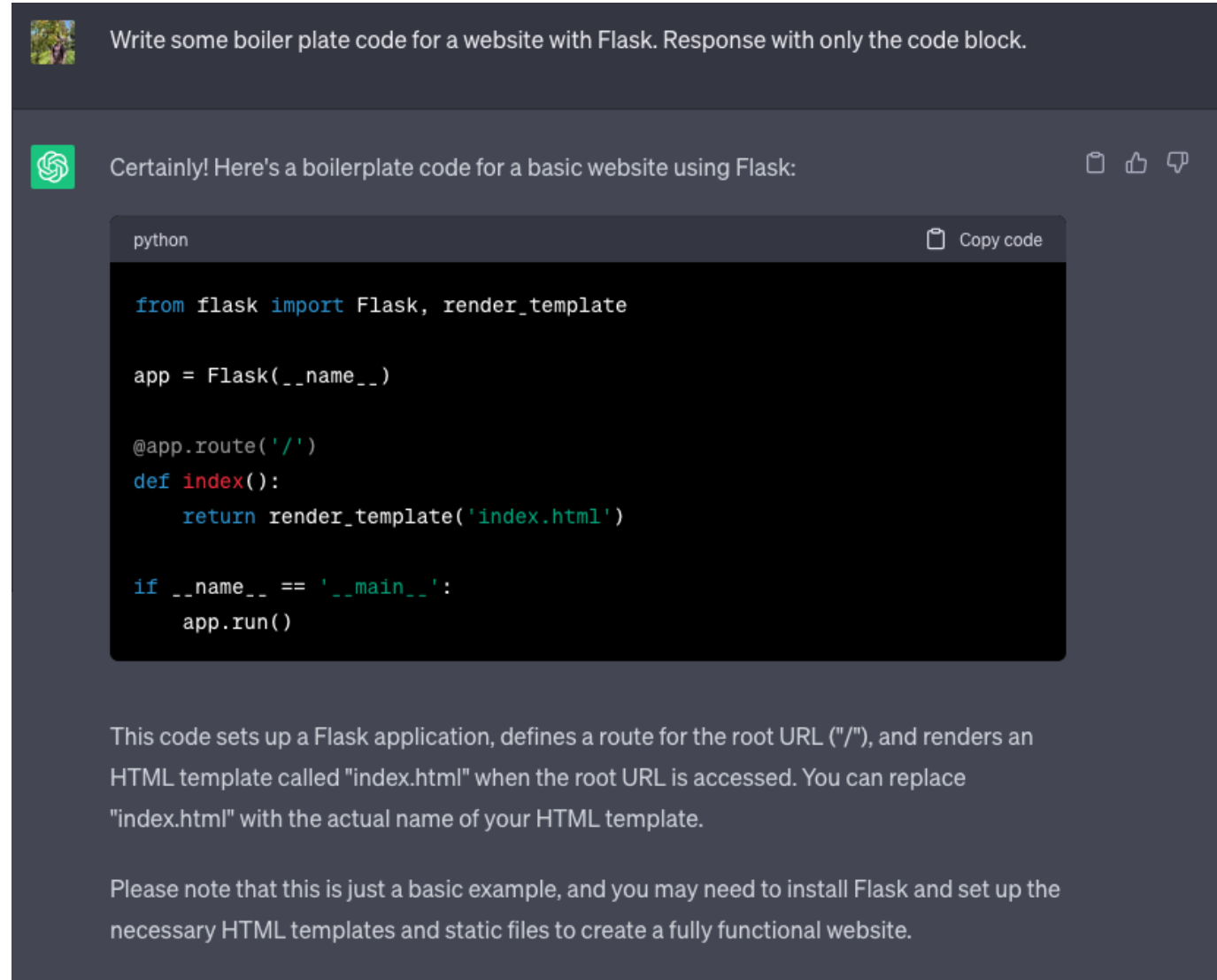
- Email spam filters
- Anti-virus software
- Search engines
- Calendar scheduling assistant
- Network intrusion detection

- ChatGPT and other LLMs
 - Blogs / news articles
 - Marketing material
 - Code*



Opportunities of generative AI

- Domain name market increase:
 - Lower bar for website creation
 - Lower bar for content creation
 - Better domain name suggestions
- Increased employee productivity
 - (Re)writing
 - Translation
 - Coding
 - Other content generation



Write some boiler plate code for a website with Flask. Response with only the code block.

Certainly! Here's a boilerplate code for a basic website using Flask:

```
python Copy code

from flask import Flask, render_template

app = Flask(__name__)

@app.route('/')
def index():
    return render_template('index.html')

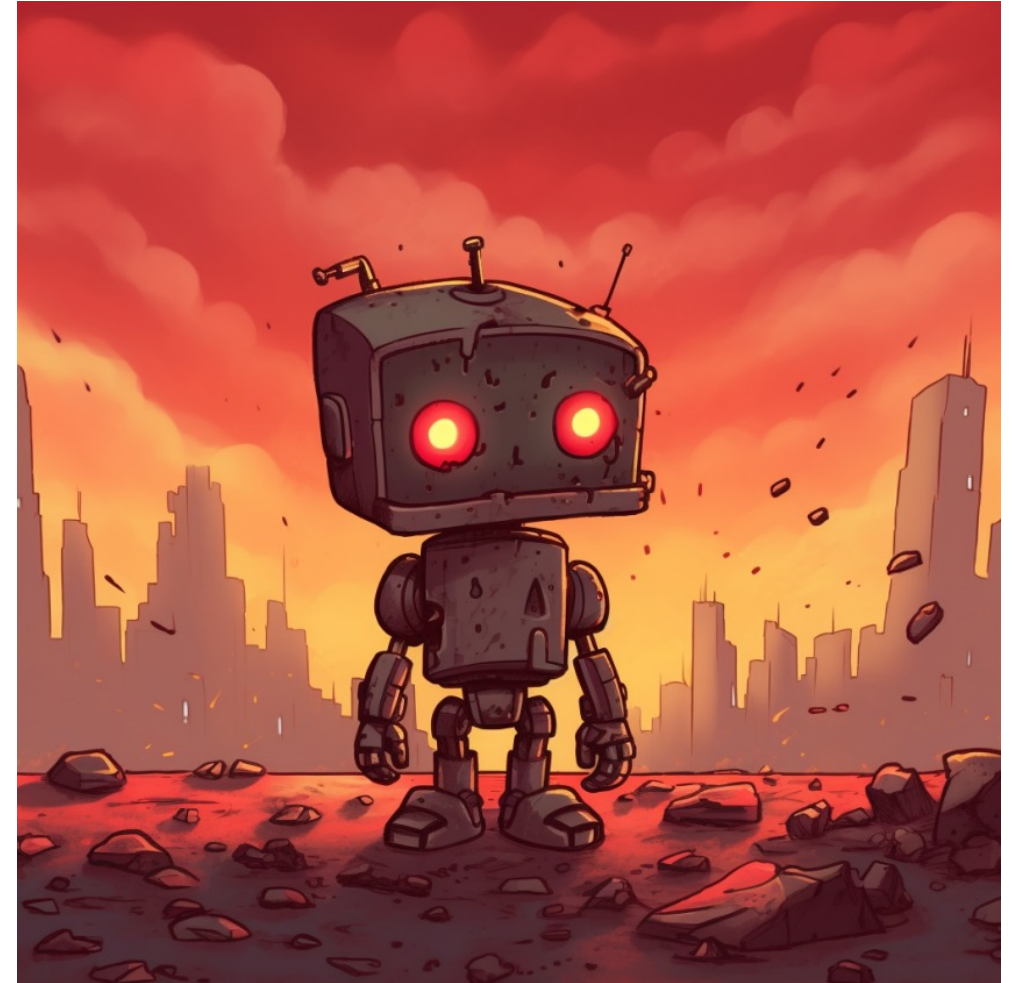
if __name__ == '__main__':
    app.run()
```

This code sets up a Flask application, defines a route for the root URL ("/"), and renders an HTML template called "index.html" when the root URL is accessed. You can replace "index.html" with the actual name of your HTML template.

Please note that this is just a basic example, and you may need to install Flask and set up the necessary HTML templates and static files to create a fully functional website.

Threats

- Domain name relevance decrease
- Increase in abuse
- Centralization of the Internet
- Leaking of sensitive information
- Many more (unknown) societal implications



Questions and remarks?



“realistic photograph of an audience looking up with puzzled and confused expressions”