

Botnet and Flashcrash: AI and the Future of Cyber Crime

Prof. dr. Andrej Zwitter

Overview

- Governance: Traditional vs. Cyber
- Taxonomy of AI Enhanced Crime
- Effect on Governance And LEAs

Governance

Traditional - Governance

1

Entities:

- States
- Companies
- IOs
- NGOs & Civil Society

2

Resource:

- Raw Materials
- Money
- Territory
- Extraction:
Productivity

3

Regulation:

- Law
- Contracts
- Enforcement

Underlying Assumptions:

- Individual Agency and Law
- Territorial Principle and Enforcement

Cyber - Governance

1

Cyber Entities:

- States
- Tech-Companies
- Online: Interest Groups
- Hackers, Hacktivists
- Cyber-Criminals
- **Digital Entities**

2

Cyber Resource:

- Data (Oil)
- Attention Space (Territory)
- Extraction Method: AI

3

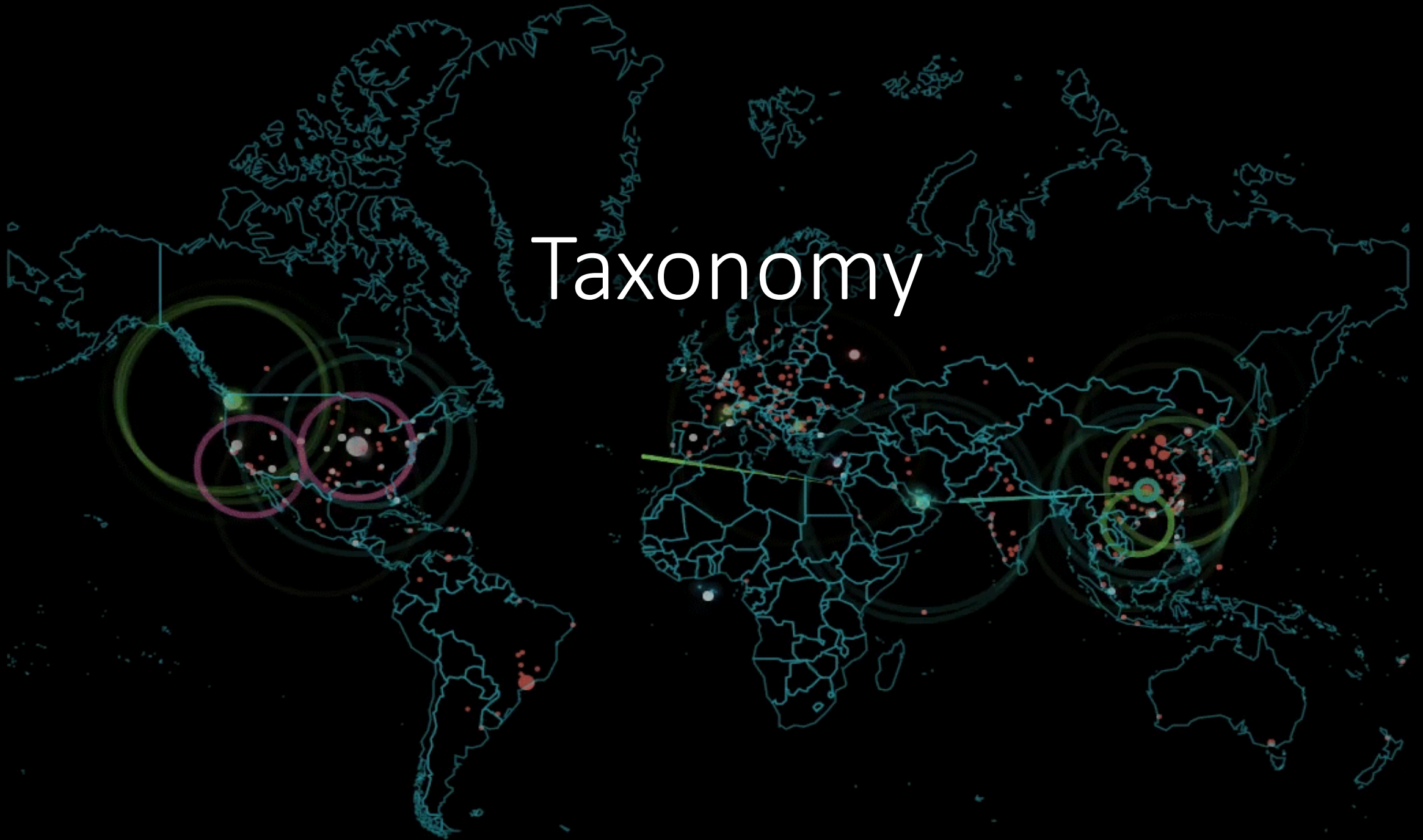
Cyber Regulation:

- Law
- Terms of Use
- Code
- Blockchain
- **Bots**

Underlying Assumptions:

- ??? Individual Agency and Law
- ??? Territorial Principle and Enforcement

Taxonomy



Taxonomy of AI enhanced crime (AIC)

- Bots:
 - Hacker-bots, Chat-Bots, Impersonators, Bot-Nets, Scrapers
- Intelligent Viruses and Evasive Malware (StuxNet / DeepLocker)
- Deep-fakes (video / audio / pictures)
- Market manipulation (e.g. Flash-Crash)
- Reverse-engineered PredPol

Taxonomy of AI enhanced crime (AIC)

- Hacking with AI enhanced tools:
 - Image classification (Captchas) / Cryptography / automated vulnerability discovery
- Phishing (impersonation / reverse phishing detection)
- ML enhanced profiling and manipulation (Social Engineering)
- ML poisoning
- Robotics and unmanned vehicles as tools (smuggling drones / drone attacks / swarm attacks)

Taxonomy of AI enhanced crime (AIC)

- Exploits:
 - Technical Vulnerability
 - Human Vulnerability
 - Automatization of Tasks
- Gains:
 - Financial (direct – theft / indirect – market manipulation)
 - Digital assets and IP
 - Data
 - Physical Threats
 - Political Manipulation
- Actors:
 - Human agent
 - Artificial agent

Effects



Effects on Governance and LEAs

- Threat expansion / Change of Character / New Threats / New Threat Areas (Assets, e.g. Data)
- Criminal liability
- Digitalization / Community Policing / HumInt / CrowdSourcing
- Collaboration with AI Development Community

Thank you for your
attention!

Prof. dr. Andrej Zwitter
Chair of Governance and
Innovation
Dean / Campus Fryslân



andrej.zwitter



a.zwitter@rug.nl



university of
groningen
campus fryslân