Artificial Intelligence and Law Enforcement: The Good, the Bad and the Unknown

Dr. Philipp Amann, MSc
Head of Strategy
European Cybercrime Centre
23 Sep 2019
Our Role
Europol’s Mandate

“Europol shall support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy”

(Europol Regulation)
Europol’s European Cybercrime Centre (EC3)

- Cyber Threats and Trends
- Capacity Building
- Prevention & Awareness
- Internet Governance
- Outreach

- Payment Fraud
- Hi-Tech Crimes
- Child Sexual Exploitation
- Dark Web Investigations

January 2013

Europol Unclassified – Basic Protection Level

✓ Digital Forensics
✓ Document Forensics
Europol Unclassified – Basic Protection Level

Tools and Services

- Training and Capacity Building
- Decryption Platform
- Awareness Raising and Sharing of Best Practices
- On-the-spot Operational and Technical Support
- J-CAT & Attachment Scheme
Artificial Intelligence: friend or foe?
Artificial Intelligence refers to a system, machine or algorithm that is capable of observing its environment, learning, and based on the insights and experience gained, take actions or propose decisions. These actions include a certain degree of autonomy, while retaining a human-centric approach to ensure trustworthiness and respect for fundamental rights.
AI Opportunities

- Reduce human error
- Faster, better & more proactive exploration of data → identify high-value targets, relevant connections & leads from large data sets
- Automate steps within the data/intelligence management cycle
- Improve efficiency through AI techniques (e.g. machine learning)
AI Risks and Challenges

- The “black box” problem
- AI governance including data governance (training data)
- Need for an ethical, legal, privacy and data protection framework
- Need for human involvement and supervision
- Need to adapt the law enforcement ecosystem
Adversarial AI

Facilitate cybercrime

- Improve social engineering attacks (e.g. phishing)
- Find new attack vectors & vulnerabilities
- Automate attacks against the Internet of Things
- Improved protection of criminal infrastructure

Disinformation or data poisoning

- Manipulate AI systems into working erratically
- Disable AI-based defence measures
- Create false flags
Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies.

By Catherine Stupp

Updated Aug. 30, 2019 12:52 pm ET

Criminals used artificial intelligence-based software to impersonate a chief executive’s voice and demand a fraudulent transfer of €220,000 ($243,000) in March in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking.

The CEO of a U.K.-based energy firm thought he was speaking on the phone with his boss, the chief executive of the firm’s German parent company, who asked him to send the funds to a Hungarian supplier. The caller said the request was urgent, directing the executive...
Looking ahead
It takes a network to unlock the potential of AI