



DRONES: A GROWING CYBERSECURITY THREAT

GENEVA INTERNET L@W RESEARCH COLLOQUIUM 2019

JUNE 21, 2019

MOHAMED RASHID AL BALUSHI, LLB, LLM.

HISTORY OF MILITARY DRONES

- It all started in the early 1900s'
- No. of drones increases = cyberattacks increase
- 18 million drones by 2023 (globally)
- \$91 Billion market over the next decade
- The advent of AI

QUESTIONS & POINTS

- The manipulation of AI robots through the application of adversarial machine learning
- A systematic process in evaluating the potential risks of such attacks
- The regulatory scene & whether Codes of Ethics, Executive Orders and Recommendations are sufficient in addressing AI robustness?
- Formulating a proper regulatory framework

THE MANIPULATION OF AI ROBOTS

- The Theory behind AI
- Machine Learning & Deep Learning
- The Application of Adversarial Machine Learning

IS THERE A SYSTEMATIC PROCESS IN EVALUATING THE POTENTIAL RISKS OF SUCH ATTACKS?

- On-Board Sensors
- Predictive Analytics
- Tracking Devices
- Encryption
- Adversarial Training & Defensive Distillation

REGULATORY SCENE

- United States of America

- “ Executive Order on Maintaining American Leadership in Artificial Intelligence ”

- European Commission

- “ Ethics Guidelines for trustworthy Artificial Intelligence ”

- OECD

- “OECD Council Recommendation on Artificial Intelligence”

“ EXECUTIVE ORDER ON MAINTAINING AMERICAN LEADERSHIP IN ARTIFICIAL INTELLIGENCE ”

- The extent to which the 2019 White House E.O. on AI addresses technical robustness and safety of AI systems
- What is the exact role of the US. National Institute of Standards and Technology in creating a plan for the development of technical and legal standards to support secure & robust AI?

“ ETHICS GUIDELINES FOR TRUSTWORTHY AI ”

- Ethical, Lawful, & Robust AI
- What sets the EU’s approach apart from the US approach in addressing cybersecurity of AI systems?

“ OECD COUNCIL RECOMMENDATION ON ARTIFICIAL INTELLIGENCE ”

- Principles for the implementation of AI systems
- What sets the OECD’s approach apart from the US & EU approaches in addressing cybersecurity of AI systems?

The background is a dark teal gradient. In the corners, there are decorative white line-art elements resembling circuit traces or neural network connections, with small circles at the end of the lines.

ARE CODES OF ETHICS, EXECUTIVE ORDERS, &
RECOMMENDATIONS SUFFICIENT IN ADDRESSING AI
ROBUSTNESS?

FORMULATING A PROPER REGULATORY FRAMEWORK

- Purpose of government regulation
- Update existing regulations?
- Designating accountability and liability?

The image features a dark blue gradient background with white, stylized circuit board traces in the corners. These traces consist of straight lines and small circles, resembling electronic components or data paths. The traces are located in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

FINAL WORD: PARTNERSHIP

...

THANK YOU

...

Mohamed Rashid Al Balushi (LinkedIn)

Legal Researcher

Email: mrabalushi94@gmail.com