DRONES: A GROWING CYBERSECURITY THREAT

GENEVA INTERNET LAW 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?
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?
FINAL WORD: PARTNERSHIP
THANK YOU

Mohamed Rashid Al Balushi (LinkedIn)
Legal Researcher
Email: mralbalushi94@gmail.com