RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: MBS-T07

Evolution of AI-Bot Swarming Intelligence with Robots

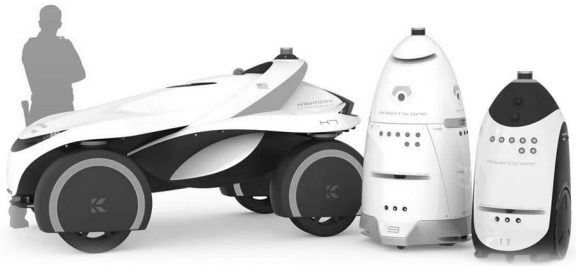
Thomas Caldwell

Founder/President/CTO
League of AI
@cybersdtom

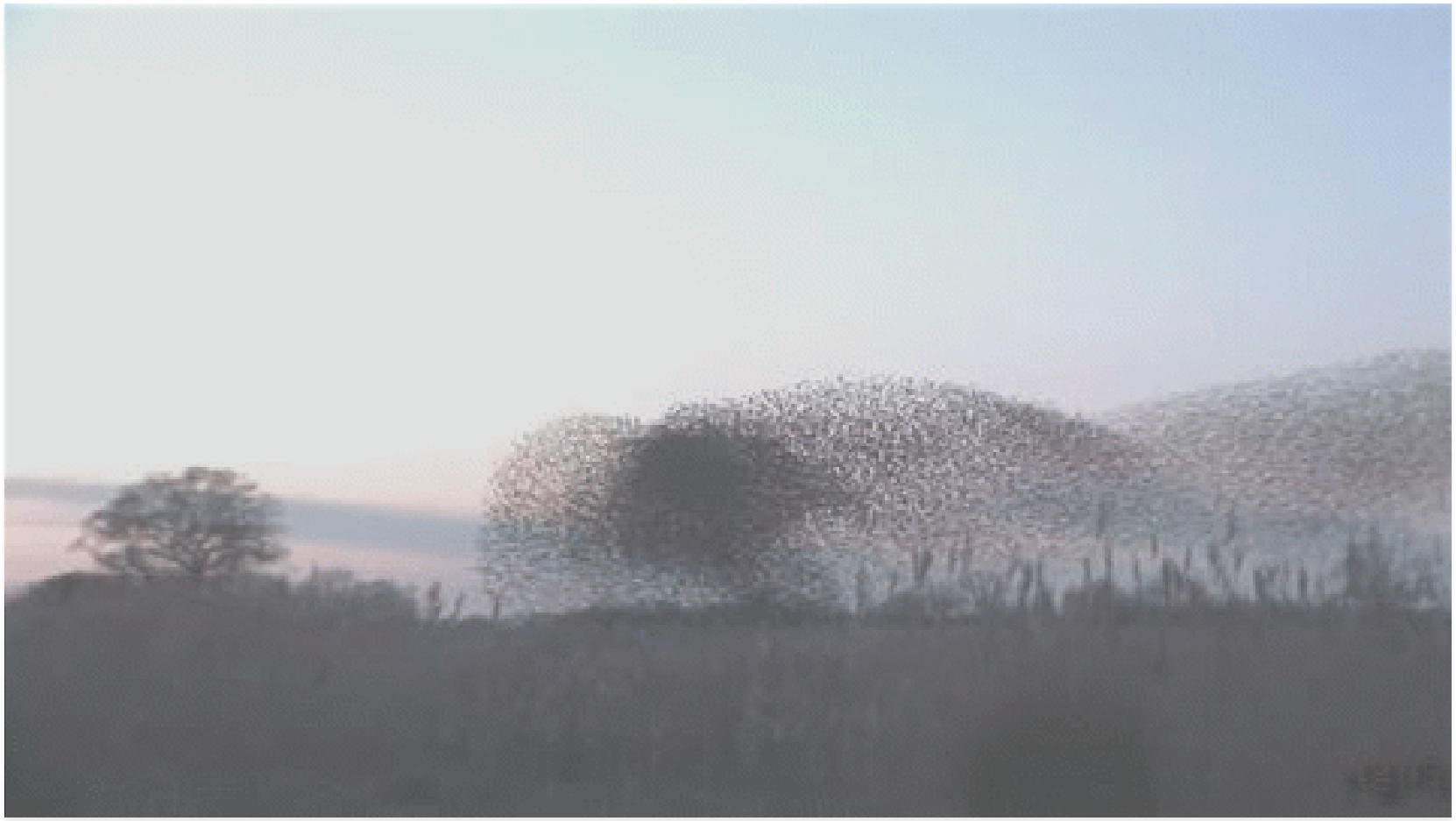
#RSAC

Will Robots be Top of Mind for Parents?

- 20 years ago: Physical Security in Schools was not a concern of parents and students
- Present Day: Security Officers (humans) are being added to Schools
- Future: Robots will work with Officers:
  - Higher Quality of Safety
  - More Rapid Detection of Danger
  - A safer Team-oriented Resolution
  - Lower costs of School Safety
  - Machine-Human “swarming”



Swarms



Swarm-as-a-Service

threatpost

A new methodology was announced by scientists in Hong Kong that uses natural swarm behaviors to control clusters of nano-robots. These micro-swarms can be directed to perform precise structural changes with a high degree of reconfigurability, such as extending, shrinking, splitting and merging.

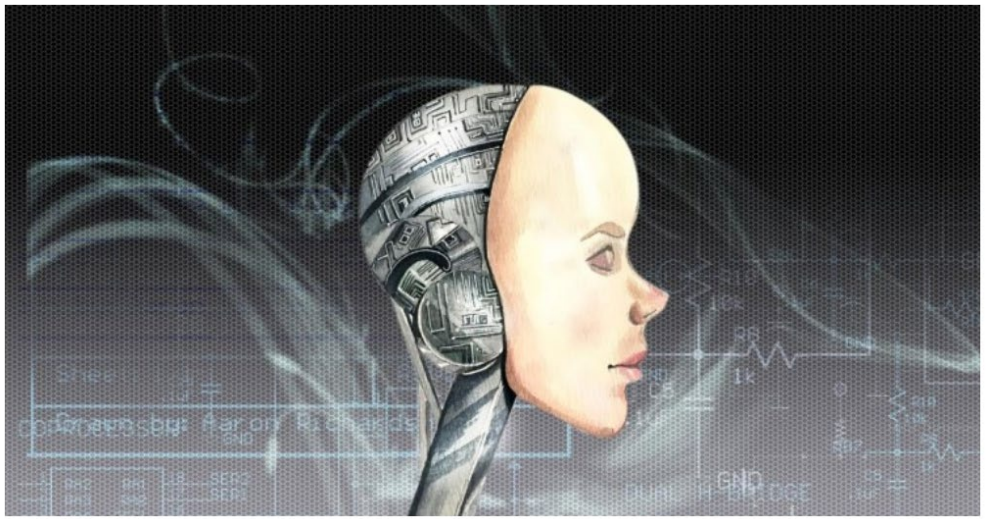
https://threatpost.com/prepare-to-defend-your-network-against-swarm-as-a-service/141381/

Swarm Intelligence

INNOVATION / AI

This Start-Up Uses Human Swarm Intelligence to Develop AI That Can Predict the Future

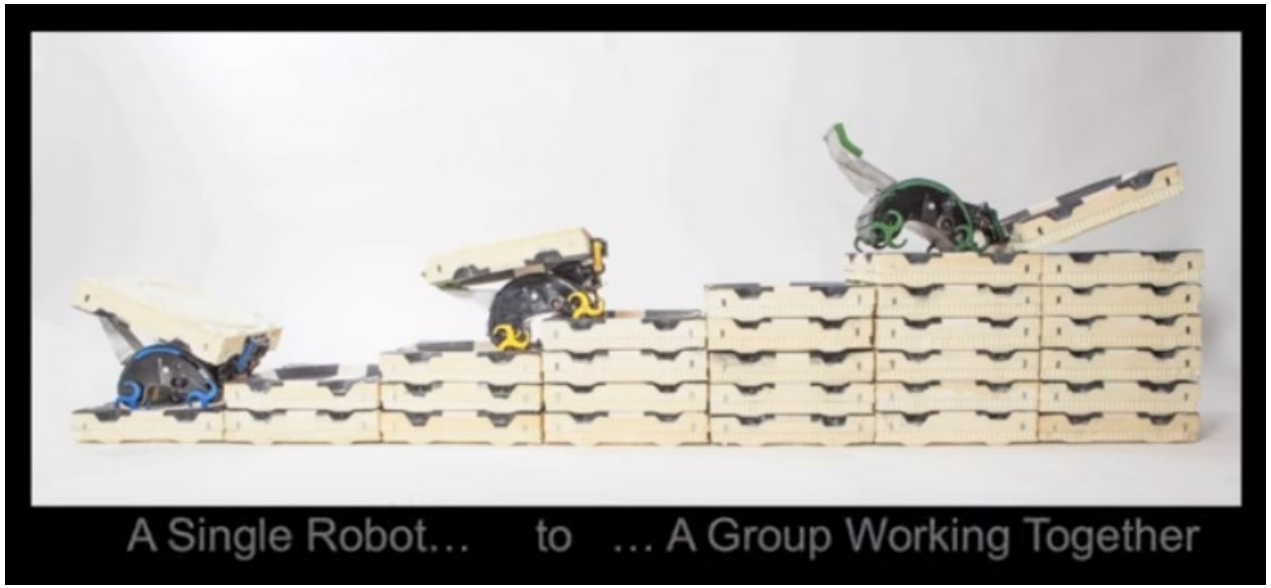
Unanimous A.I. is using human swarm intelligence to help its AI algorithms predict with better accuracy.

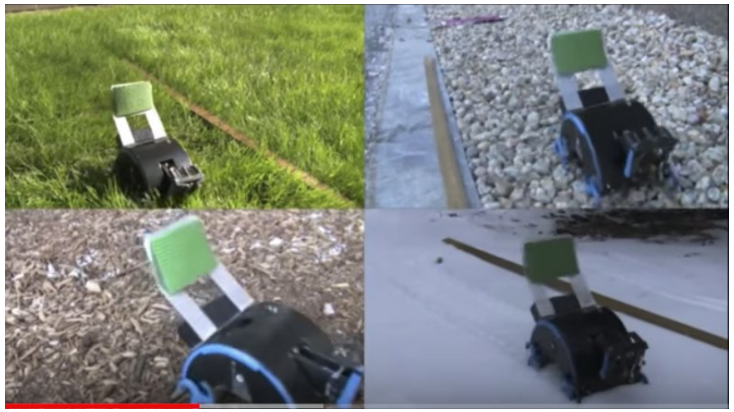


https://interestingengineering.com/this-start-up-uses-human-swarm-intelligence-to-develop-ai-that-can-predict-the-future

Swarming Robots

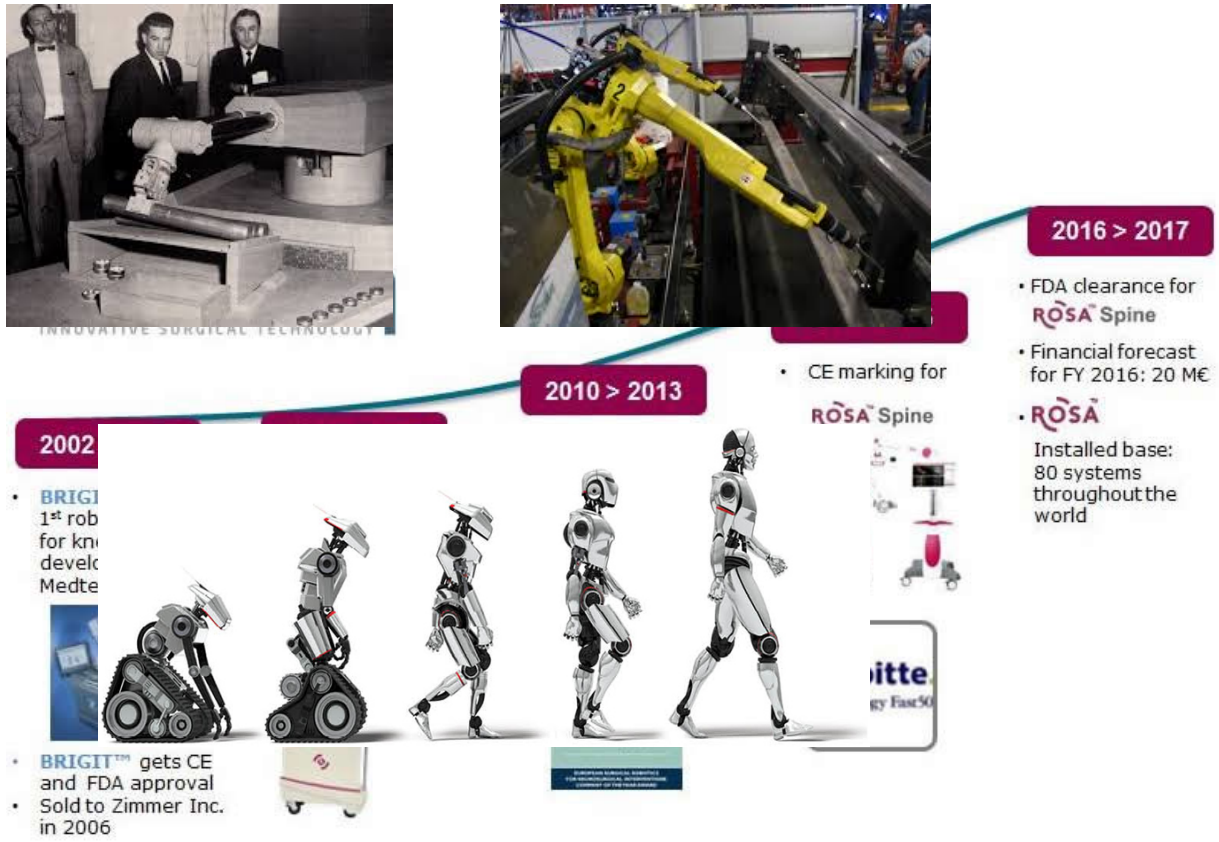
- Radhika Nagpal is an American computer scientist and researcher in the fields of self-organising computer systems, biologically-inspired robotics, and biological multi-agent systems. She is a Professor of Computer Science at Harvard University and the Harvard School of Engineering and Applied Sciences.



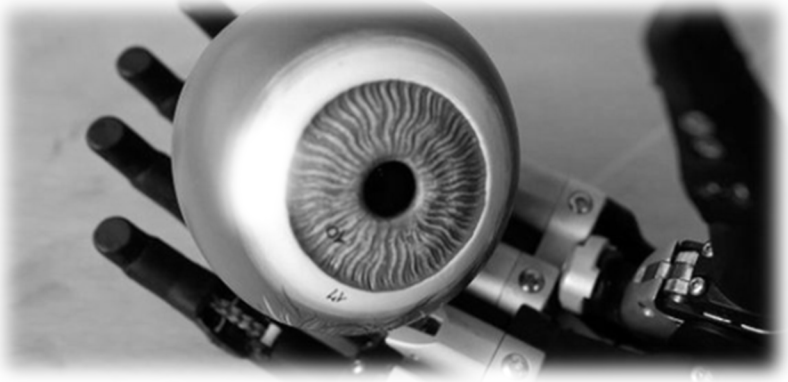


The Evolution of Robotics

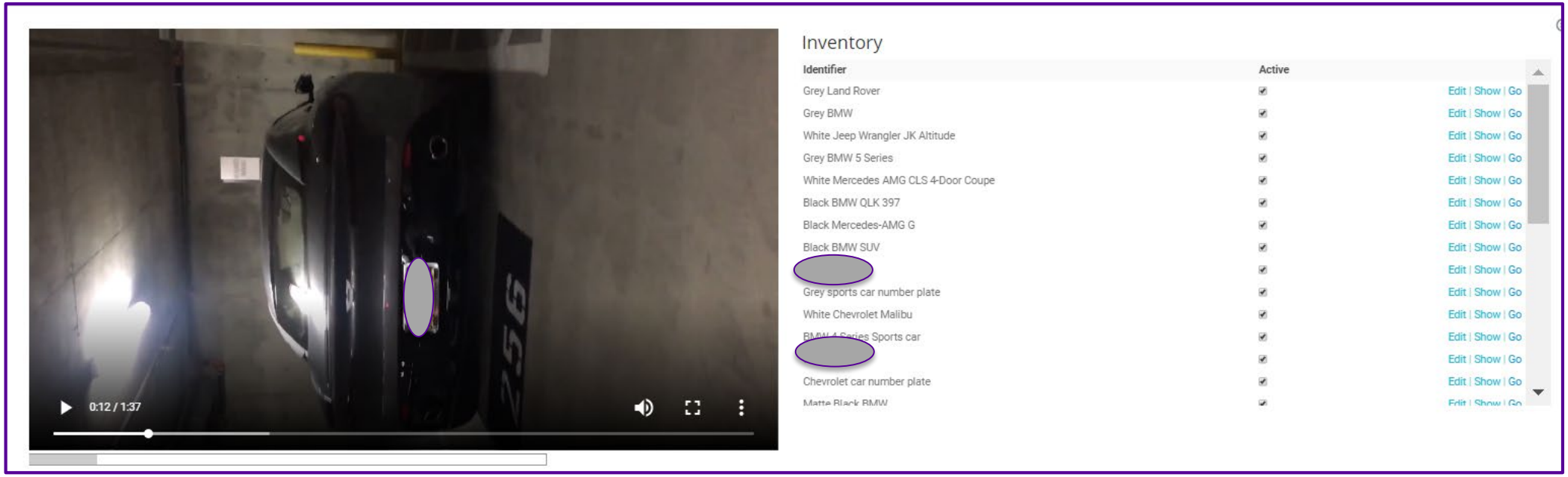
- 1962-1979: Robots emerged in Manufacturing
- 1908-Present: Modern Industrial Robots
- Robots now assist with Brain Surgery
- Robotic Swarming Intelligence is an emerging Technology



Robotic Vision/NLP with Deep Learning Algorithms

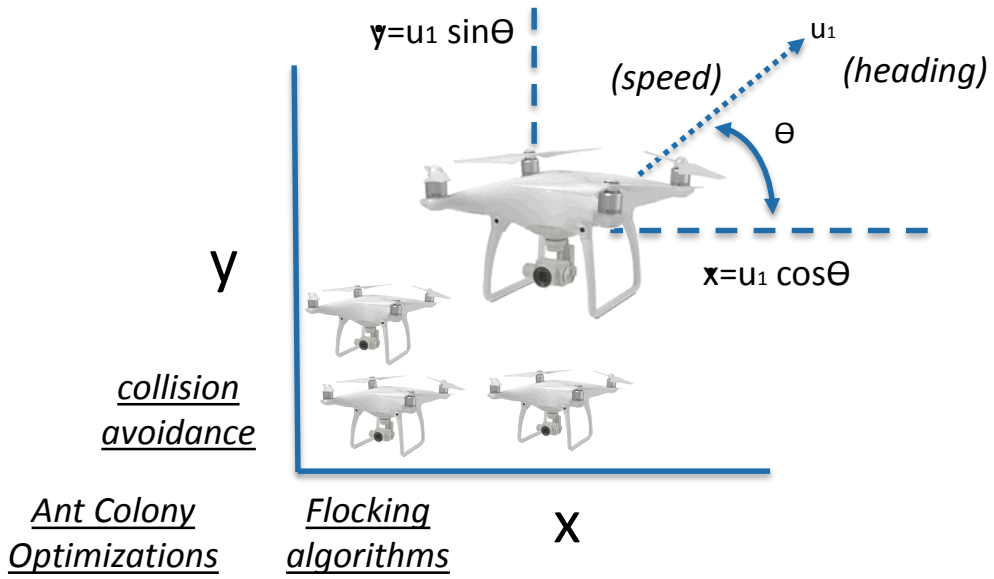


- TensorFlow and other Open Source Deep Learning algorithms are available for computer vision and NLP
- Example: WowYow (startup) and video object recognition through lens of a robot camera



Swarming Algorithms

- Vector = spatial heading and velocity of robots and drones
- Swarms: Collective, Collaborative, Cooperative… execute missions
- Can Vectors represent cognitive behaviors and discovered opinions?
- Could Blockchain be used for de-centralized sharing and voting in swarms?



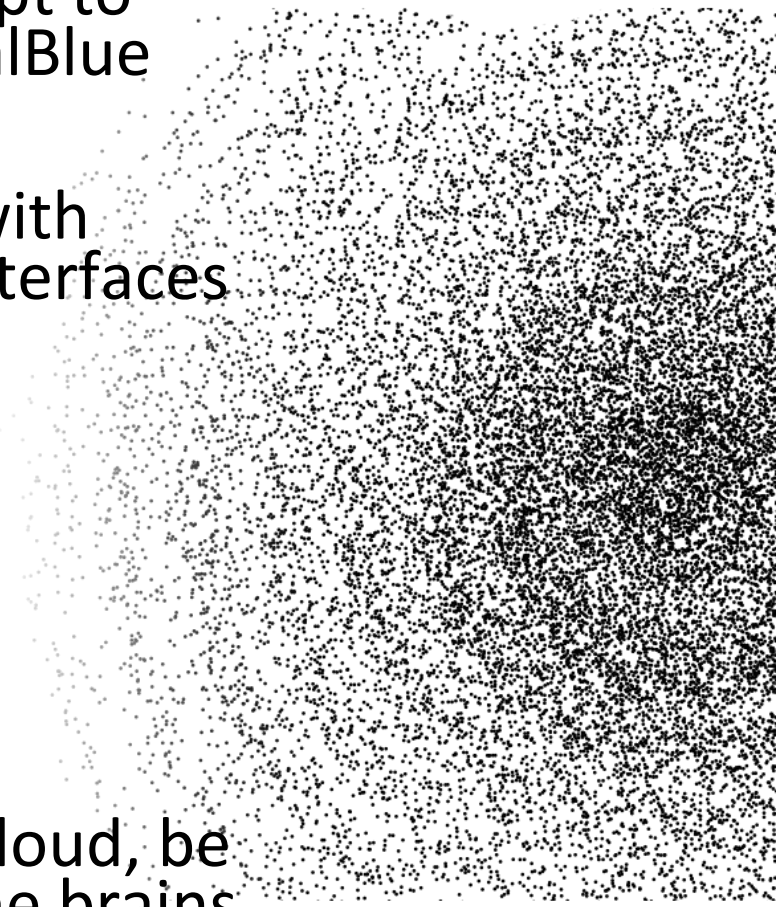
Today's robot Swarming Algorithms are focused on physical spatial aspects of swarming Drones and Robots

Swarming Algorithm Examples

- 2018 Winter Olympics, record-setting 1,218 drones
- Intel's Shooting Star drones are a foot-long, weigh eight ounces, and can fly in formation up to 20 minutes
- “A Sea of Robots”: Institute of Telecommunications at University Institute of Lisbon and from University of Lisbon in Portugal
- Learned “Behaviors” to Communicate, Collaborate and reach Consensus

Back to Cyber Security and AI-Bots

- Cyber-Criminals build systems that can ‘learn’ and adapt to defenses: Nachi Worm, Mirai, Reaper Botnets… EternalBlue exploit has now merged with the Mirai botnet!
- Bots are becoming one of the fastest growing trends with intelligent reasoning, messaging and conversational interfaces (e.g. Chatbots)
- AI-Bot Capabilities:
  - Machine Learning and Cyber Intelligence
  - Behavioral Analysis and Ontology
  - Understands Entity State (Posture)
  - Orchestration and Deception Tactics
- AI-Bots can live inside a Robot, Drone, be virtual in a Cloud, be resident on an Edge (Raspberry Pi, NVIDIA TXT2), be the brains of a new-age SIEM (AI Cognitive Security Tool)



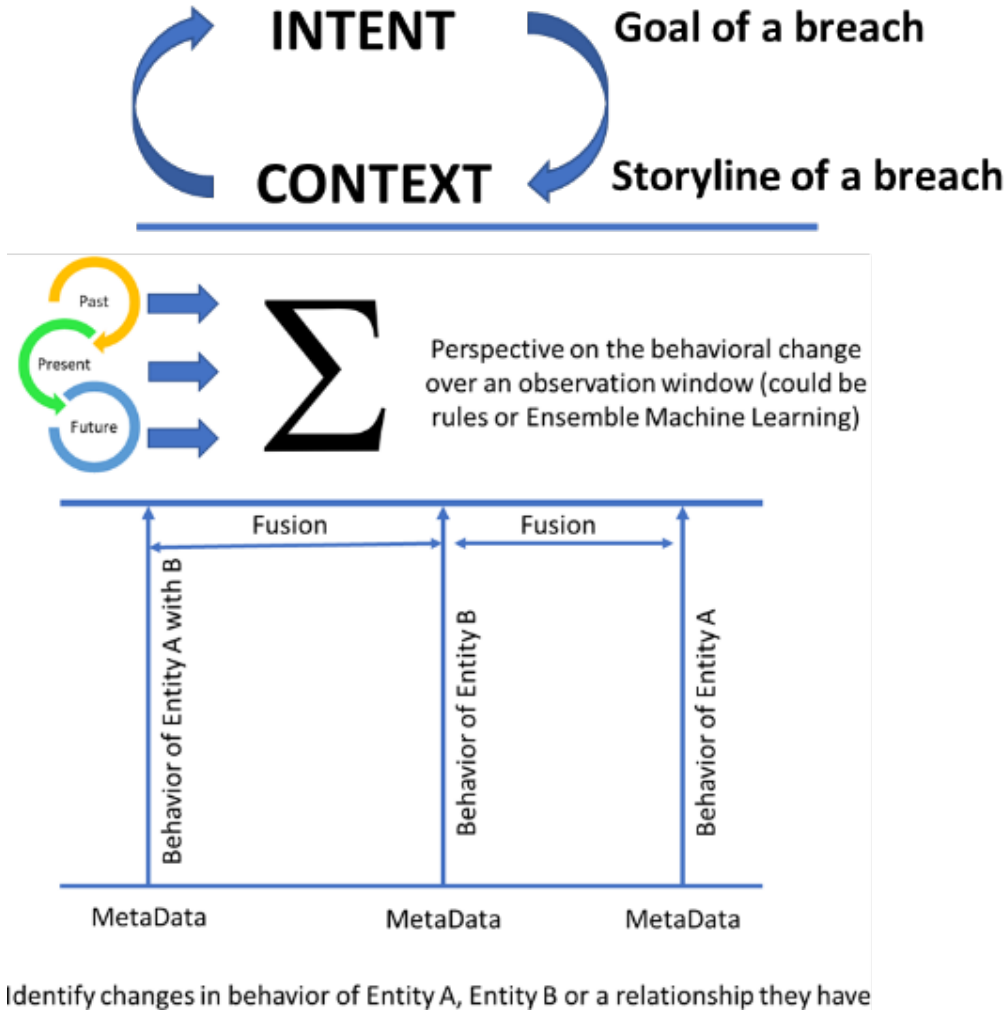
AI-Bots and Cognitive Machine Learning Value-add?

Security Operations Centers (SOC) require a new paradigm to be effective, especially when the attackers may now be using AI/Machine-Learning technology (Attack Bots) in their attack vectors:

- Automation where it hurts the most
- Visualization Tools which “Connect the Dots” on a potential breach
- Combine the strengths of Humans and Machines
- Create unified Workflow and a seamless investigation Workspace
- Use machines to Model how attackers operate and Automate the way analysts Investigate

Cognitive AI-Bots have Contextual Cyber Insight

- Many new Security Tools are focused on time-series data flows (Why?)
- Metadata-rich Security Events should:
  - Answer a “Question”
  - Reveal an “Intent”
  - Represent a “Behavior” that can be classified
- A Semantic Chain of Events can represent the “Incident” (related events)
- AI-Bots collaborate with humans to “team” and create the “Storyline” of behavioral changes and “Entity” changes in state (posture)



Physical and Cyber Security Convergence

- IT is an Event, Alert, Ticket oriented workforce
- Cognitive Engines will automate event workflow analysis between humans/machines/robots
  - Exposure: Virtual and Physical
  - Risk Profiles: Probability and Analytics
  - Threat Actors and Threat Methods
  - Human Understanding: “Controls”, Business Model

What { **Resources** **Vendors** **Business** **Technology** } **does the organization rely on that can be exploited by others?**

Summary: Cyber and Robotic Security Swarming

Cognitive AI-Bots are here today:

- can live inside a cloud, a robot, drone, a Raspberry Pi, TXT2 Edge…
- can chat with humans using Slack, Alexa, Mobile Apps…
- will have Cognitive Engines (brains) to understand an event stream of the Past, Present and AI/ML Predictive Future
- have vision through cameras for Objects of High Risk Interest (AI)
- can listen through microphones for gun shots or screams
- Can Swarm with other AI-Bots to Collaborate, Communicate and reach Consensus

Applying the Cyber and Physical Dimensions of Security

- Think about your Data Ingest points for “Cyber Intelligence” that are both Virtual (e.g. logs) and Physical (e.g. IoT cameras)
- Identify Use Cases where having physical intelligence would make your security framework “smarter” and more effective
  - For example, a Botnet attack on your IoT devices that cause them to change virtual and physical behaviors
- Get with your Facilities team to partner on making IoT devices not only protected, but part of the Security Framework.
  - For example, if a certain object of interest is seen, generate alert and also orchestrate an automated action to be taken
- Identify and track future Robot capabilities that can help integrate (swarm) with your security AI tools and staff for a safer, smarter security posture
  - Example: Promote and Support robots that can help secure your child’s schools

Robots are Now part of our Society

Example Use Cases in our Security Domain:

Tying AI/ML to Biometrics

Outdoor Surveillance

Home Security

Police Action

Work Safety

School Safety

Swarming Ant Robots

Crowd Control

Terrorist Threats

Immigration

RSAConference2019

Questions?

Tom Caldwell, Founder/President/CTO of League of AI

tomc@leagueofai.com

Twitter: @cybersdtom

LinkedIn: https://www.linkedin.com/in/tcaldwell/

Special thanks to Nir Daliot of League of AI for his collaboration and expertise