Synthetic Teammates and the Future of Cybersecurity

Dr. Fernando Maymí
Lead Scientist, Cyberspace Operations
Soar Technology, Inc.
ferando.maymi@soartech.com

8 August 2017
- THE FUTURE THREAT LANDSCAPE
- SYNTHETIC TEAMMATES
- WORKFORCE DEVELOPMENT
- **THE FUTURE THREAT LANDSCAPE**
- **SYNTHETIC TEAMMATES**
- **WORKFORCE DEVELOPMENT**
The Tactical Battlefield of 2050

- Augmented humans
- Automated decision making and autonomous processes
- Misinformation as a weapon
- Micro-targeting
- Large-scale self-organization and collective decision making
- Cognitive modeling of the opponent
- Ability to understand and cope in a contested, imperfect, information environment
Threatcasting

http://threatcasting.com
TWO DAYS AFTER TUESDAY:
A SCIENCE FICTION PROTOTYPE

A state sponsored terror group aims to attack New York and destabilize the United States, targeting the ports and critical supply chains...

WRITTEN: BRIAN DAVID JOHNSON
ILLUSTRATION: SANDY WINKELMAN
BROUGHT TO YOU BY: CHILL
PART ONE: BEFORE TUESDAY

Using a targeted spear phishing attack on a small supplier with weak security on the edge of the supply chain, a terror group gains access to internal proprietary networks and communications. They search for a weakness in the security of the ports.

FROM: FUND5@USIBANK.COM
DATE: MONDAY NOVEMBER 8, 2027 6:34AM ET
TO: ACCOUNTS@WEAVERANDSONS.COM
SUBJECT: URGENT: ACCOUNT VERIFICATION NEEDED

Dear Account Holder,

We are contacting you to verify your account with us. There is a pending funds transfer set to expire at 8:00 am ET today.

If you fail to verify your account at the link below the funds will be returned.

VERIFY ACCOUNT

Thank you for your help in this matter.

Respectfully,
Joshua Bowman
Accounts Department
A WEAKNESS IS DISCOVERED

Now with access to internal supply chain networks and using artificial intelligence (AI) agents to crawl message boards, the terror group discovers the Taucor Detectr 400, a gaseous ionization detector used to inspect cargo. The scanners are prone to malfunction and critical repair parts come from limited suppliers mostly outside the US.

MEANWHILE...

Preparing for the attack, the terror group uses the dark web to buy a bot-net that targets IoT devices, hijacking them without their owners knowing.

THE NEXT WEEK IT HAPPENS...

With a knowledge of a weakness the AI agents scour public social media feeds and find Bill Morgan, an inspector at the Red Hook, NY port. Two months prior he posted a complaint about the faulty Taucor scanners. Little does Bill know but he's now an informant inside the port.

Tellit @Bill Morgan
Taucor Again!! Grrrr. Shoddy Parts somehow my problem?? Try printin local!!!
2:12 PM May 13 2028

Tellit @Bill Morgan
Taucor Again!!! Stupid scanners. Long night for me.
5:33 PM July 26 2028

When Bill Morgan complains again the terror group is ready, they know a window of opportunity has opened. The attack is launched...
PART TWO: TUESDAY

Across the greater New York City area, the bot-net takes over home IoT devices, placing orders for milk and fresh fruit before they are needed. Their owners never suspect.

The automated supply chain snaps into action. Local drones deliver the orders but quickly supplies run low.

Automated trucks roll out, prioritizing the perishable goods, clogging the roads and bridges.

The Red Hook port is at a stand still, clogged with produce shipments from fast-moving autonomous ships.
The supply chain is clogged and the Taucor Detects replacement parts are delayed. With the scanners down, Bill Morgan and the inspectors have no choice but to switch to random manual inspections of incoming containers.
PART THREE: TWO DAYS AFTER TUESDAY

It's a busy morning rush hour in NYC... People bustle to their offices, autonomous taxis shuttle through the streets, the subways are packed...

The terror group detonates a dirty bomb in Manhattan...

The city sees massive casualties...
Concerns

Understanding the context is essential

- War on reality: the weaponization of data
- Blended attacks
- Micro-targeting
- Efficiency is easy to hack
- Complex autonomous systems
- The Future Threat Landscape
- Synthetic Teammates
- Workforce Development
Partial Artificial Intelligence Taxonomy

Artificial Intelligence

Non-Symbolic AI
- Fuzzy Logic
- Probabilistic Methods
  - Bayesian Networks
  - Hidden Markov Models
- Evolutionary Computation
  - Genetic Algorithms
  - Swarm Algorithms
- Neural Networks
  - Feed Forward Neural Networks
  - Convolutional Neural Networks
  - Recurrent Neural Networks

Learning Theory
- Markov Processes

Symbolic AI
- Semantic Networks
- Episodic Reasoning
- Production Systems
- First Order Logic

Machine Learning

Cognitive Modeling
(Oversimplifying) Artificial Intelligence

Analogous to Machine Learning

Analogous to Cognitive Modeling

Autonomous Agents

Think → Learn → Sense → Act
System 1

MACHINE LEARNING
Machine Learning

External agent validates results during training phase.

Production (trained) system outputs results to other systems.

- Sense Data
- Filter Noise
- Extract Features
- Classify Sample
Adversarial Machine Learning

Original image classified as a panda with 60% confidence

Tiny adversarial perturbation

Imperceptibly modified image classified as a gibbon with 99% confidence

This is a gibbon

Adversarial Machine Learning

Original image classified as malware with 60% confidence

Tiny adversarial perturbation

Imperceptibly modified file classified as whitelisted software with 99% confidence

Towards a Solution

DARPA

Explainable AI – What Are We Trying To Do?

Today

Training Data → Learning Process → Learned Function → Output → User with a Task

- Why did you do that?
- Why not something else?
- When do you succeed?
- When do you fail?
- When can I trust you?
- How do I correct an error?

Tomorrow

Training Data → New Learning Process → Explainable Model → Explanation Interface → User with a Task

- I understand why
- I understand why not
- I know when you’ll succeed
- I know when you’ll fail
- I know when to trust you
- I know why you erred

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)
System 2

COGNITIVE MODELING
Towards a Common Model of TTPs

**Procedures**: the algorithmic, atomic unit of cyberspace operations

**Techniques**: unique ways to perform procedures

**Tactics**: directed subgraphs of procedures with one or more goals as their terminal nodes
Towards a Common Model of TTPs

**Procedures**: the algorithmic, atomic unit of cyberspace operations

**Techniques**: unique ways to perform procedures

**Tactics**: directed subgraphs of procedures with one or more goals as their terminal nodes
Towards Common Models of Threat Actors

Partial model of APT28 (Fancy Bear) during Operation Pawn Storm
Simulated Cognitive Cyber Red-team Attack Model

SC2RAM

Cyberspace Cognitive Agent

Command & Control

Situation Reports

Human Controller

Event Layer

Intent-Command Translation

Resource Store

Hacking Toolkit

Cyber Actions

Network Under Test
SC2RAM Graphical User Interface
Network Attack Visualization

Developed by IHMC for SC2RAM
Using Synthetic Attackers for Cybersecurity
Autonomous Hunt Teammate

**Threat Intel Feeds**
- ISAC
- DHS
- Commercial

**Other Feeds**
- Social Media
- Dark Web

**Internal Sensors**
- IDS
- Logs
- Firewalls

**Internal Models**
- Assets
- TTPs
- Attacks

**Components**
- Hypothesis Generator
- Hypothesis Evaluation
- Learning Module
- THE FUTURE THREAT LANDSCAPE
- SYNTHETIC TEAMMATES
- WORKFORCE DEVELOPMENT
Workforce Pipeline

Access  Employ  Develop  Retain
What Are We Looking For?

Source, fair use: http://host.madison.com/ct
Why?

Source, fair use: http://dailymail.co.uk
Key Hiring Trends in Cybersecurity

• Companies are seeking **certified** candidates
  - 35% of positions required a certification

• Companies are seeking **educated** candidates
  - 80% of positions require a Bachelor’s degree

• Hands-on skills are more valuable than managerial ones
  - Lead Software Developer average salary: $233,333
  - Chief Security Officer average salary: $225,000

• Openings are harder to fill
  - Cybersecurity openings remain open 8% longer than IT ones
  - Security clearances or financial sector experience is even harder to fill

• Next-generation gap
  - Younger generation is not as interested in cybersecurity, particularly women
Developing the Cybersecurity Workforce

Source, fair use: http://www.naturethruphotos.com
Developing the Cybersecurity Workforce

Source, fair use: https://certification.comptia.org
Retention
Most Importantly...
SOARTECH

Modeling human reasoning.
Enhancing human performance.

fernando.maymi@soartech.com