Synthetic Teammates and the Future of Cybersecurity

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

SOARTECH

Modeling human reasoning.
Enhancing human performance.

8 August 2017

SOARTECH

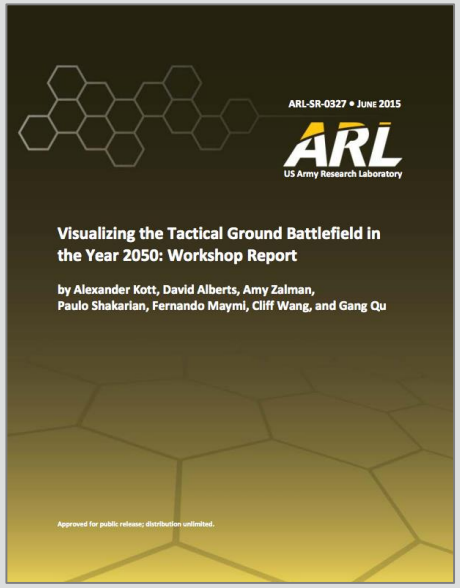
- THE FUTURE THREAT LANDSCAPE
- SYNTHETIC TEAMMATES
- WORKFORCE DEVELOPMENT

SOARTECH

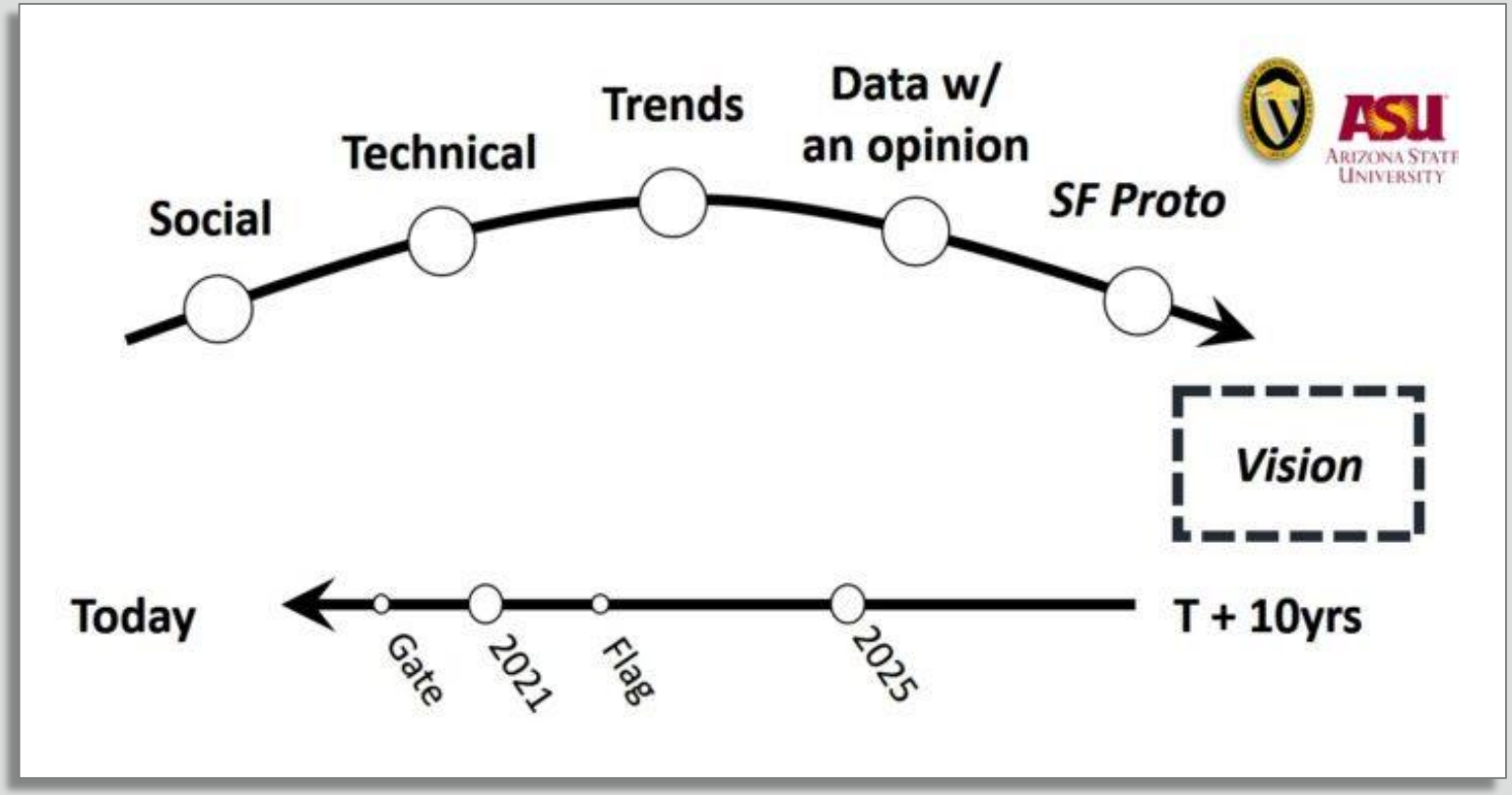
- THE FUTURE THREAT LANDSCAPE
- SYNTHETIC TEAMMATES
- WORKFORCE DEVELOPMENT

The Tactical Battlefield of 2050

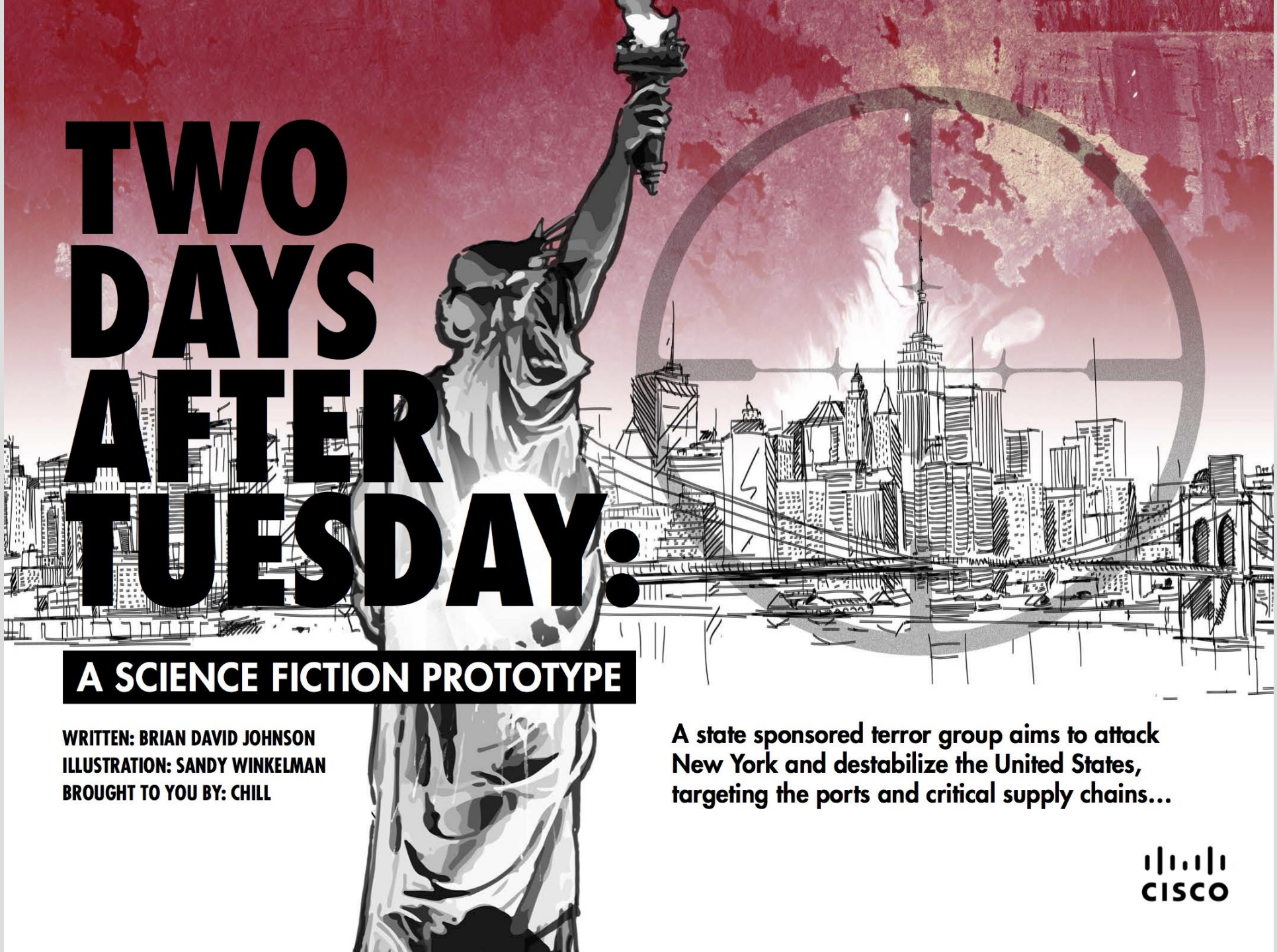
- Augmented humans
- Automated decision making and autonomous processes
- Misinformation as a weapon
- Micro-targeting
- Large-scale self-organization and collective decision making
- Cognitive modeling of the opponent
- Ability to understand and cope in a contested, imperfect, information environment



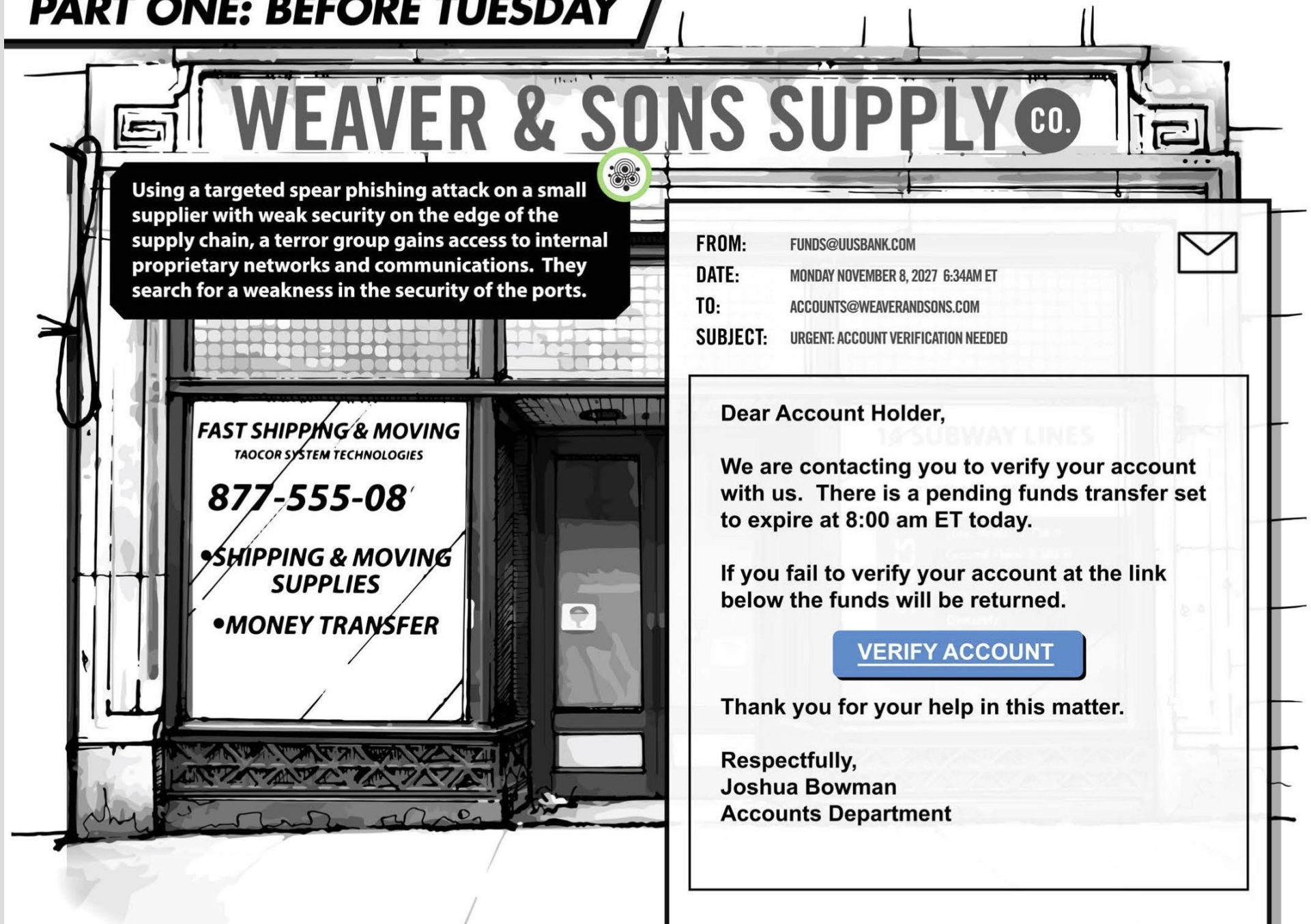
Threatcasting

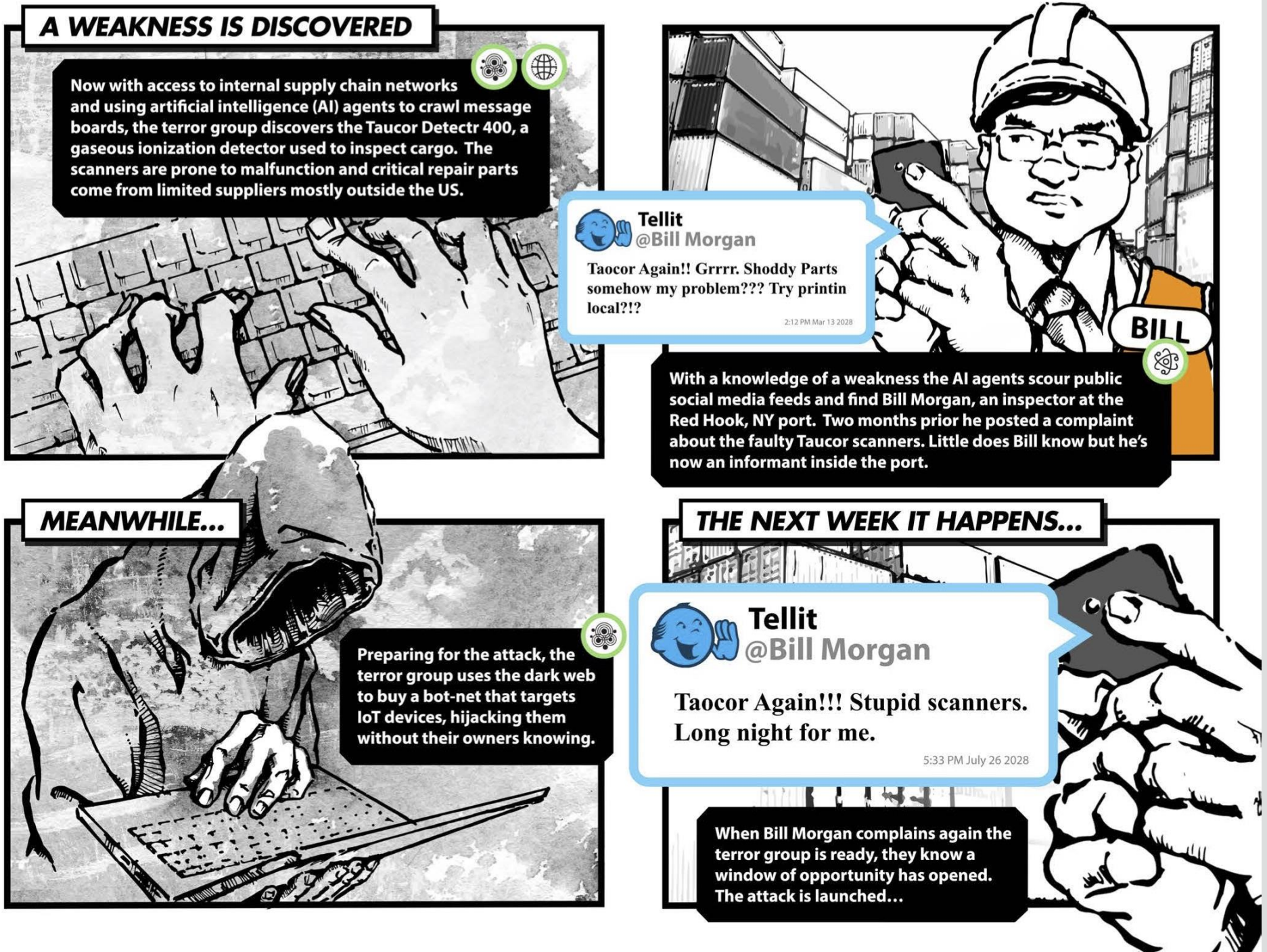


http://threatcasting.com


TWO DAYS AFTER TUESDAY:
A SCIENCE FICTION PROTOTYPE
WRITTEN: BRIAN DAVID JOHNSON
ILLUSTRATION: SANDY WINKELMAN
BROUGHT TO YOU BY: CHILL
A state sponsored terror group aims to attack New York and destabilize the United States, targeting the ports and critical supply chains...
cisco

PART ONE: BEFORE TUESDAY




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

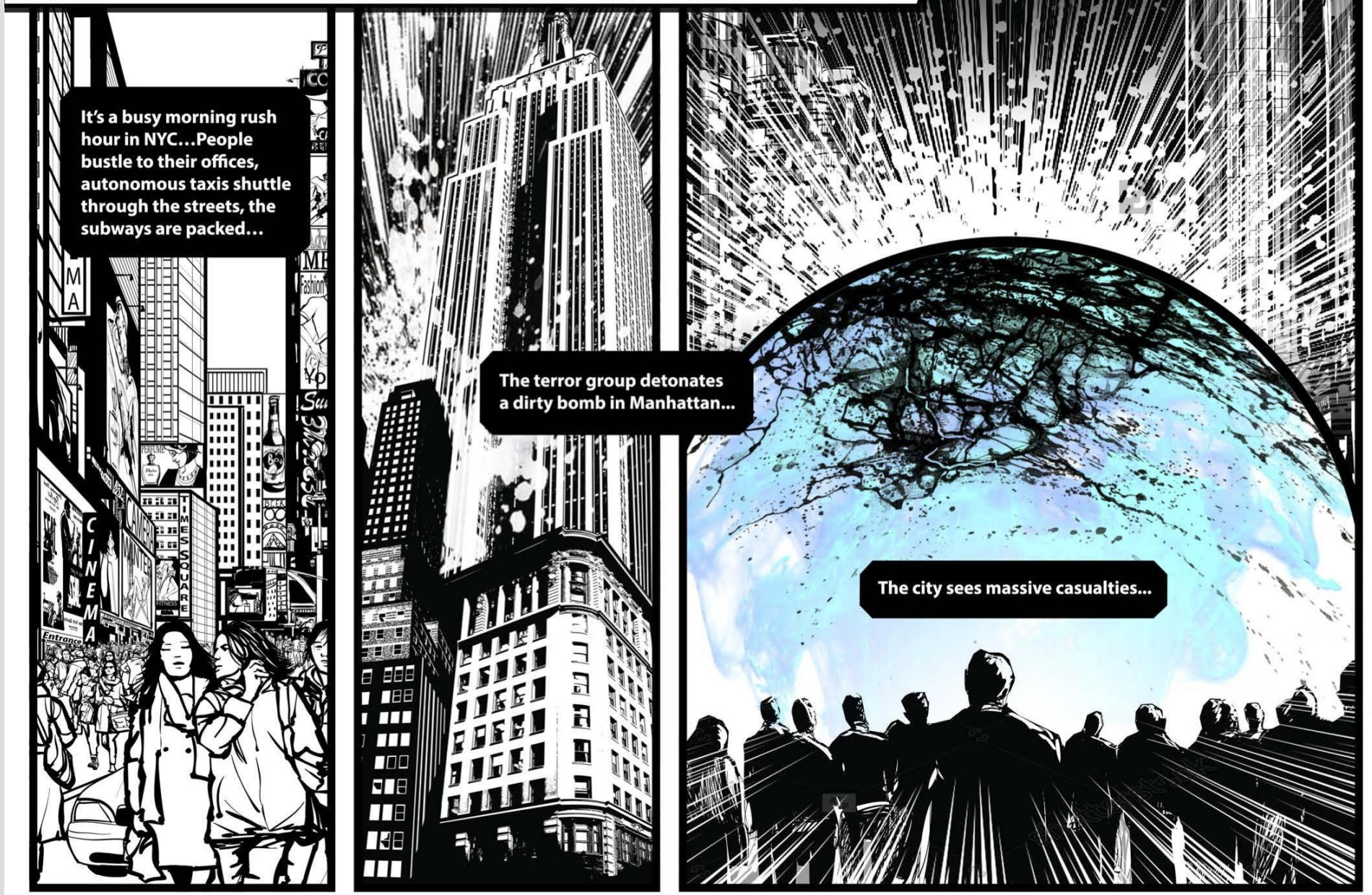
Automated trucks roll out, prioritizing the perishable goods, clogging the roads and bridges.

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.
BILL
RADIATION
A single container slips through uninspected…

SOARTECH

PART THREE: TWO DAYS AFTER TUESDAY



Concerns

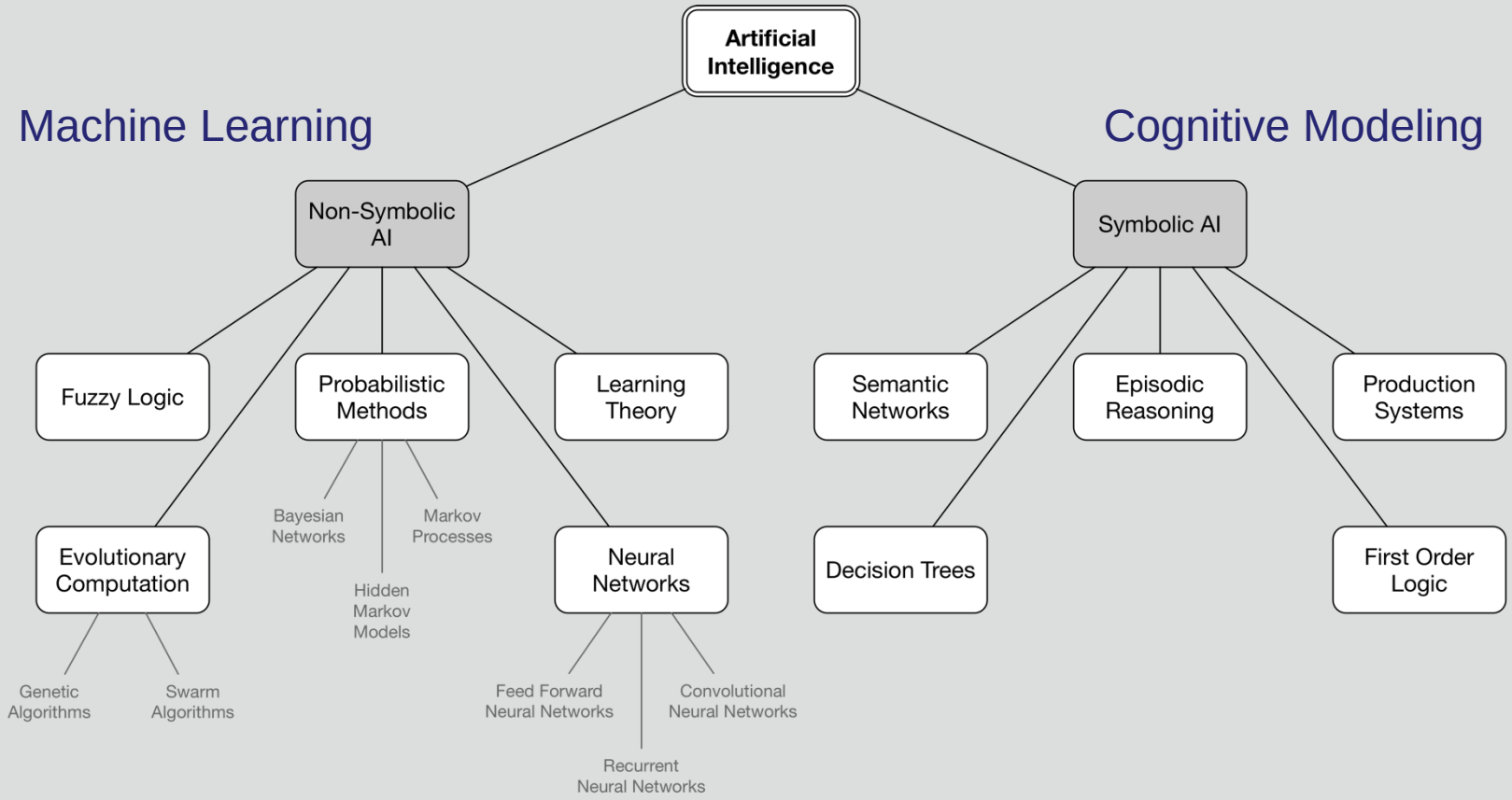
Understanding the context is essential

- War on reality: the weaponization of data
- Blended attacks
- Micro-targeting
- Efficiency is easy to hack
- Complex autonomous systems

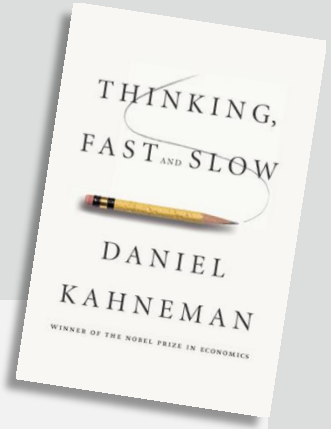
SOARTECH

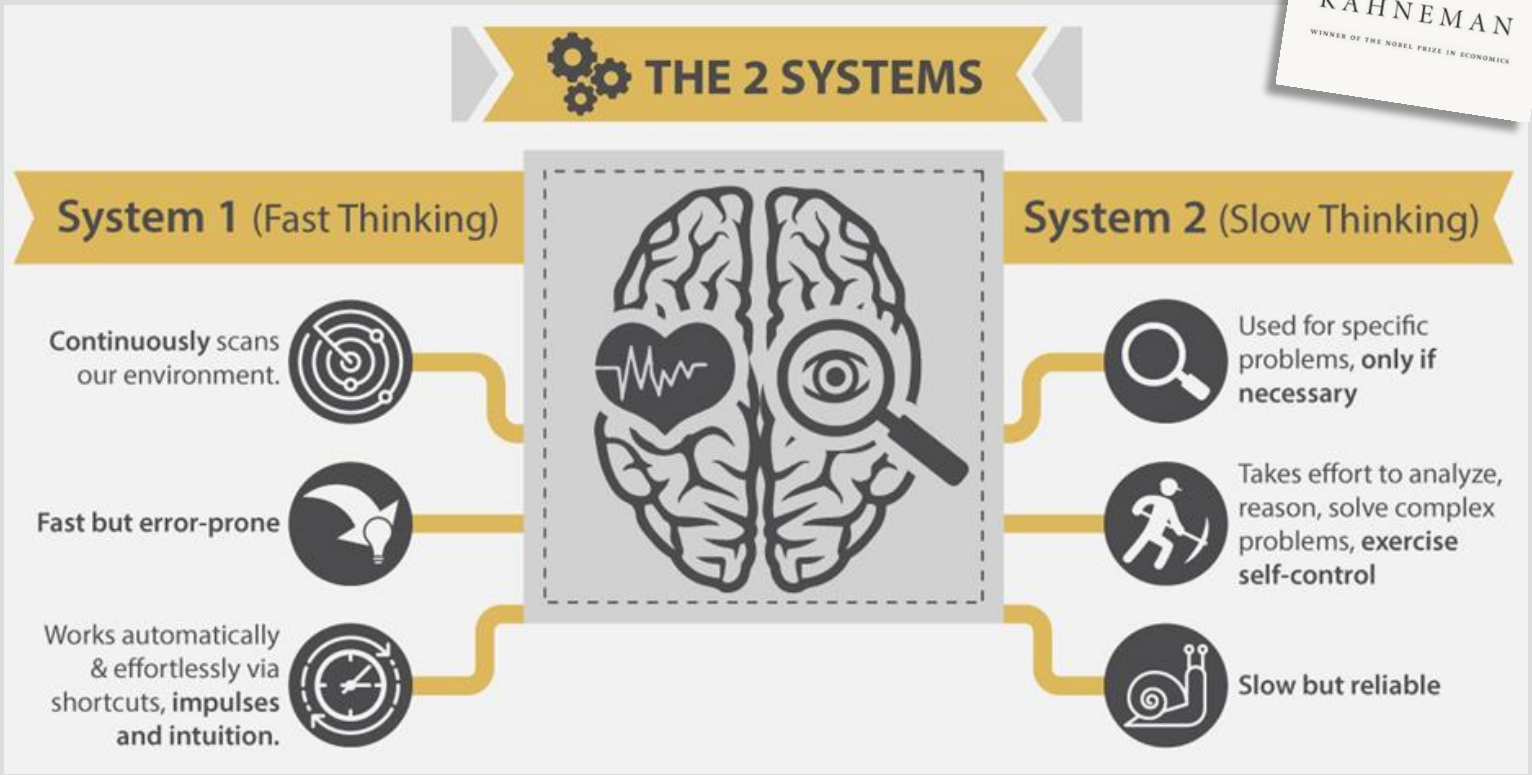
- THE FUTURE THREAT LANDSCAPE
- **SYNTHETIC TEAMMATES**
- WORKFORCE DEVELOPMENT

Partial Artificial Intelligence Taxonomy



(Oversimplifying) Artificial Intelligence



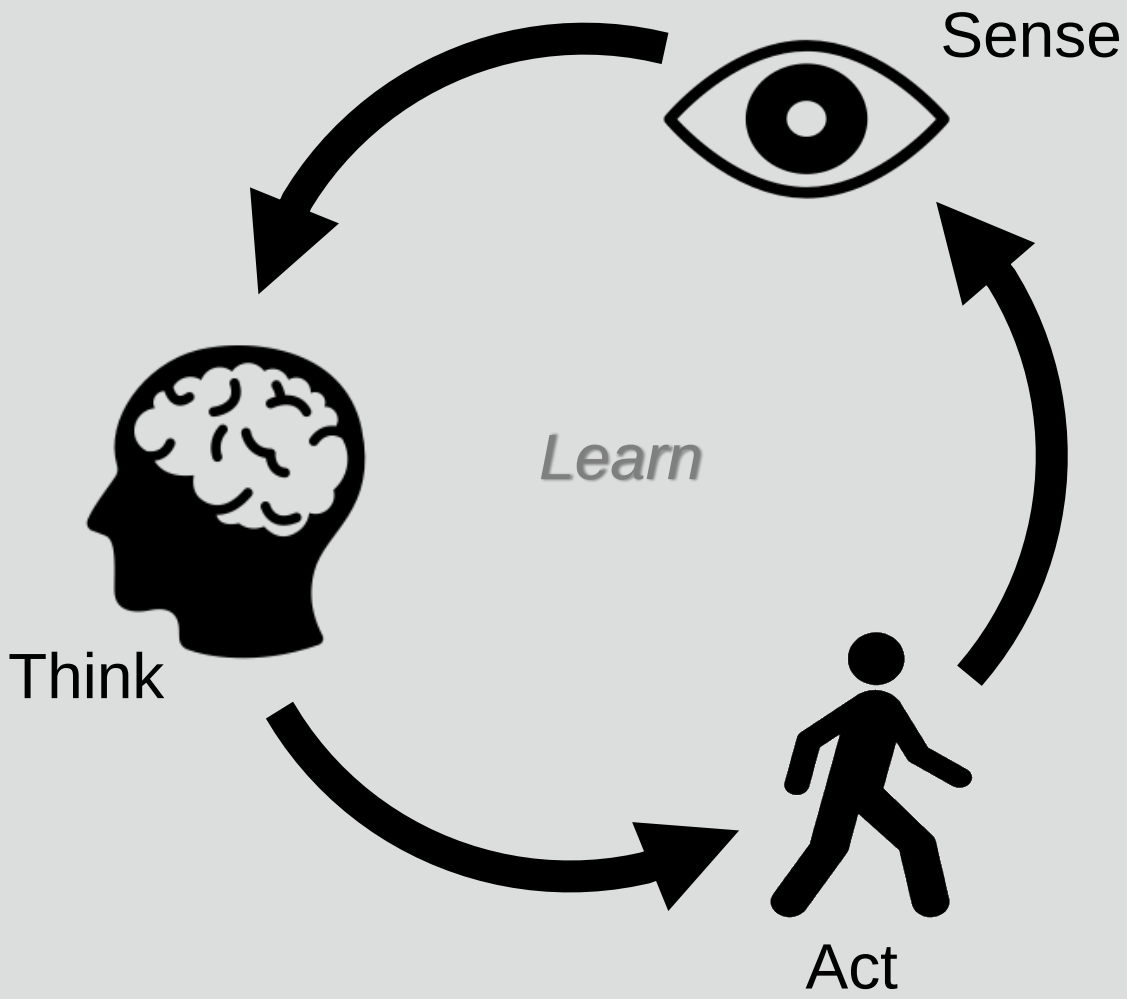


Analogous to Machine Learning

Analogous to Cognitive Modeling

Source, Fair use, https://en.wikipedia.org/w/index.php?curid=36632393, https://readingraphics.com/book-summary-thinking-fast-and-slow/

Autonomous Agents

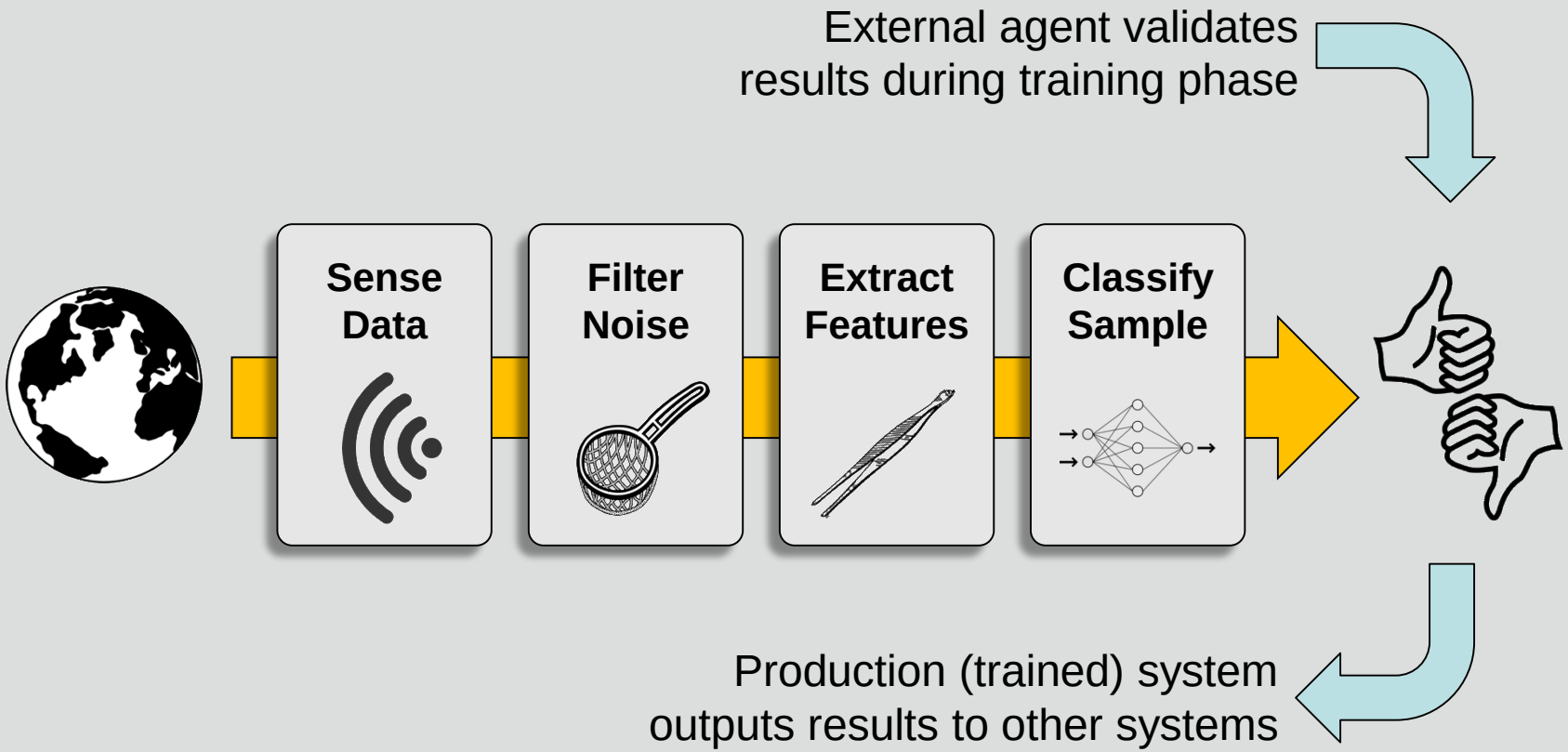


System 1

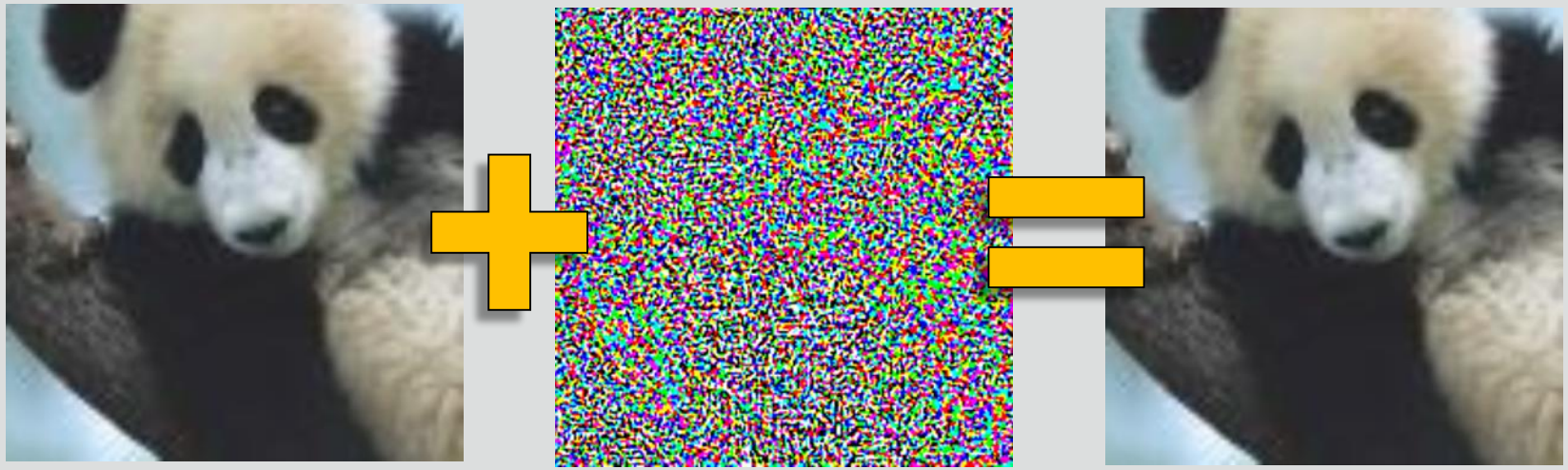
MACHINE LEARNING

17

Machine Learning



Adversarial Machine Learning



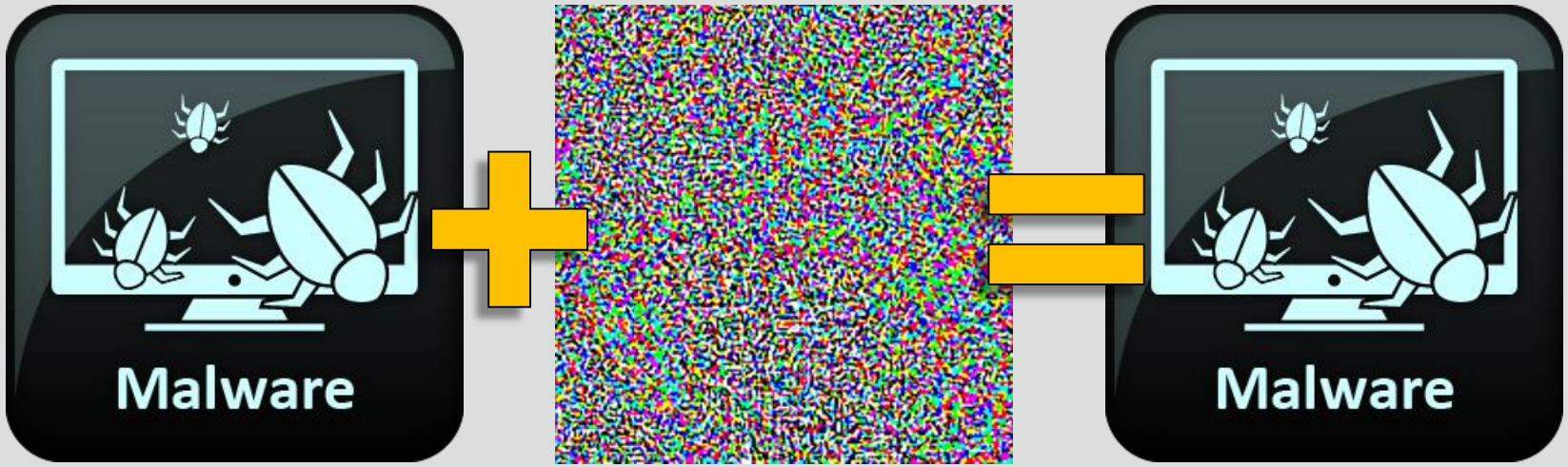
Original image classified as a panda with 60% confidence

Tiny adversarial perturbation

Imperceptibly modified image classified as a gibbon with 99% confidence

Source, Fair use, http://www.kdnuggets.com/2015/07/deep-learning-adversarial-examples-misconceptions.html, https://www.ippl.org/gibbon/wp-content/uploads/2010/09/peppyaction-269x300.jpg

Adversarial Machine Learning



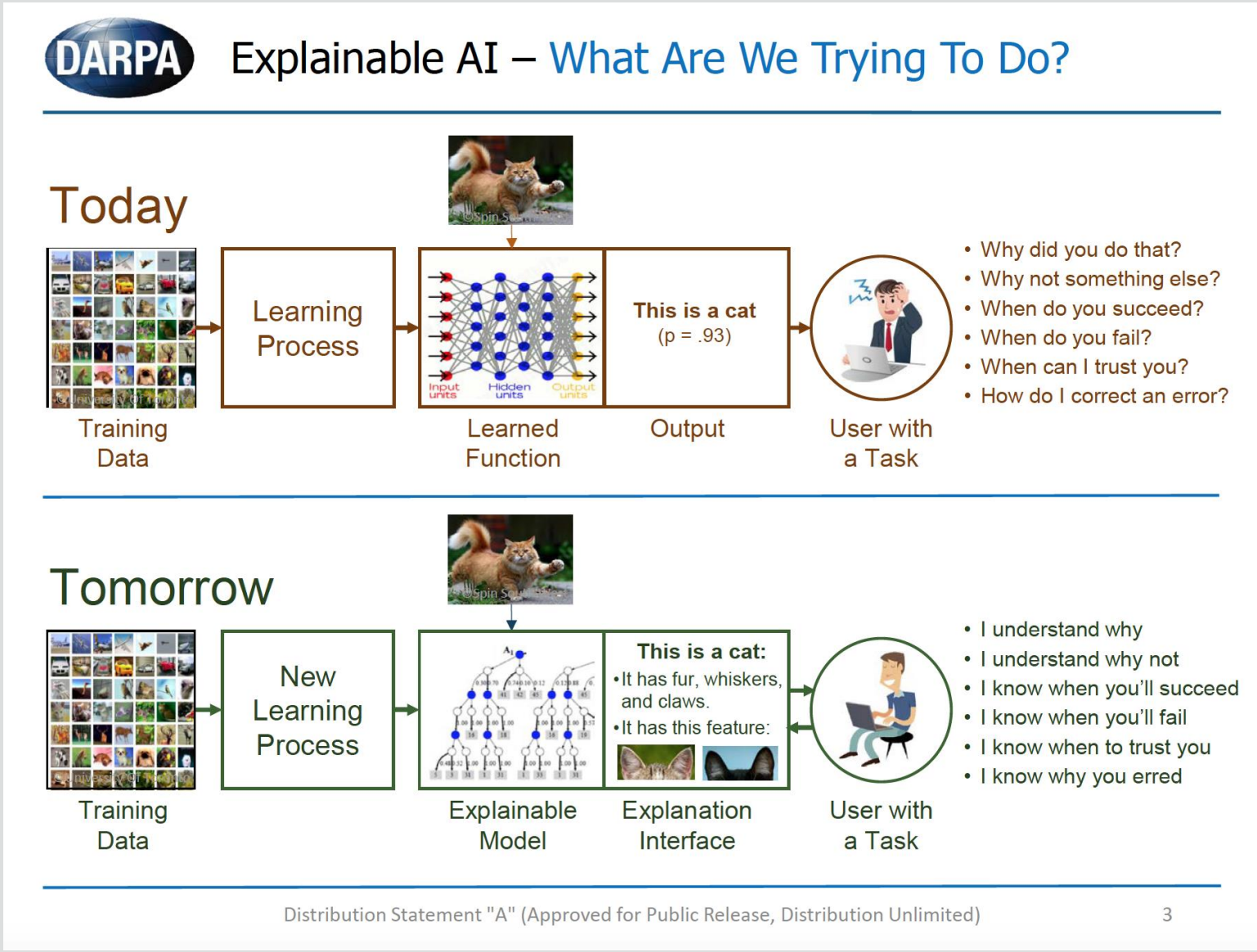
Original image classified as **malware** with 60% confidence

Tiny adversarial perturbation

Imperceptibly modified file classified as whitelisted software with 99% confidence

Source, Fair use, http://www.kdnuggets.com/2015/07/deep-learning-adversarial-examples-misconceptions.html, https://stixproject.github.io/documentation/idioms/maec-malware/

Towards a Solution

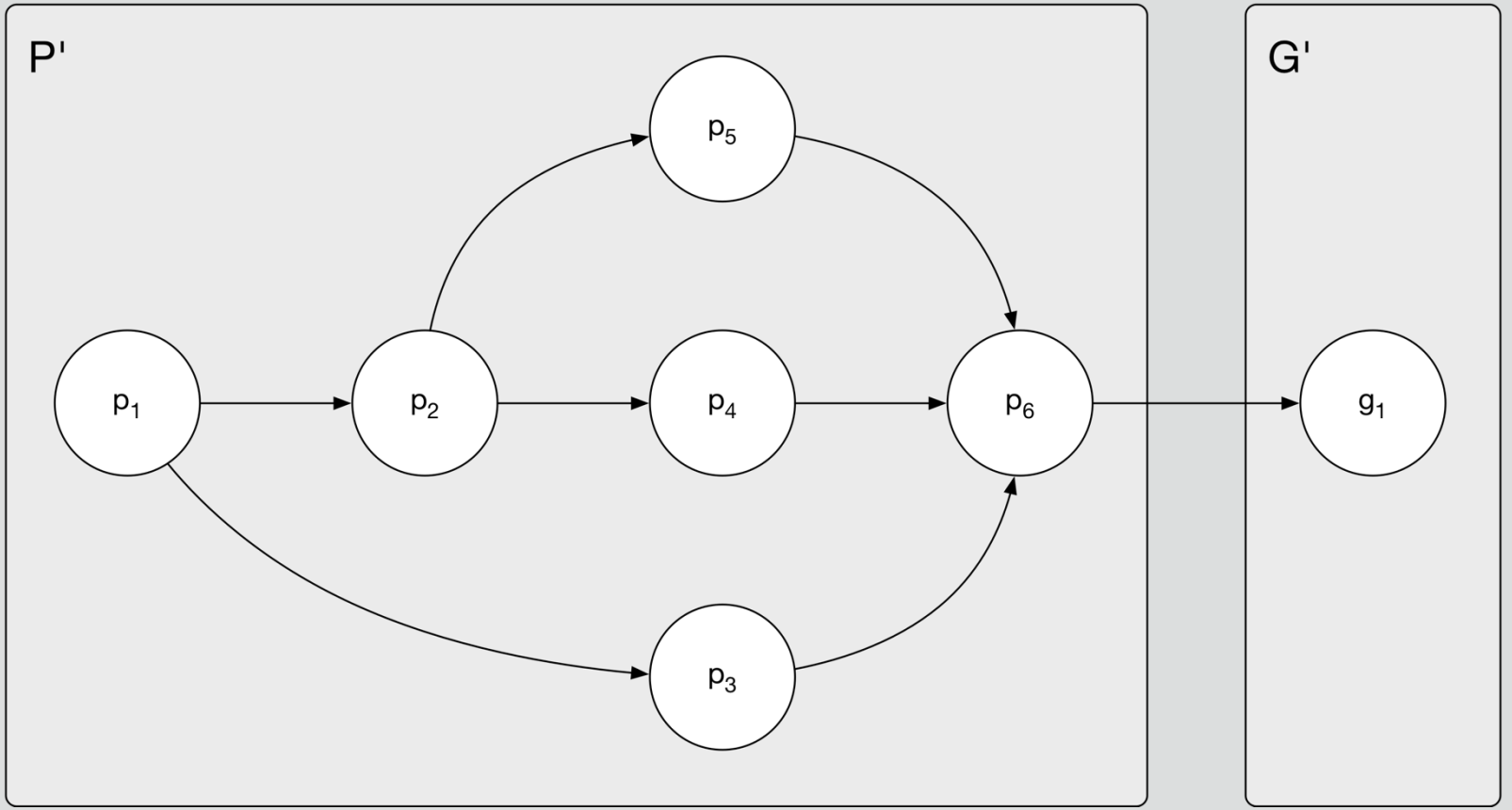


System 2

COGNITIVE MODELING

22

Towards a Common Model of TTPs

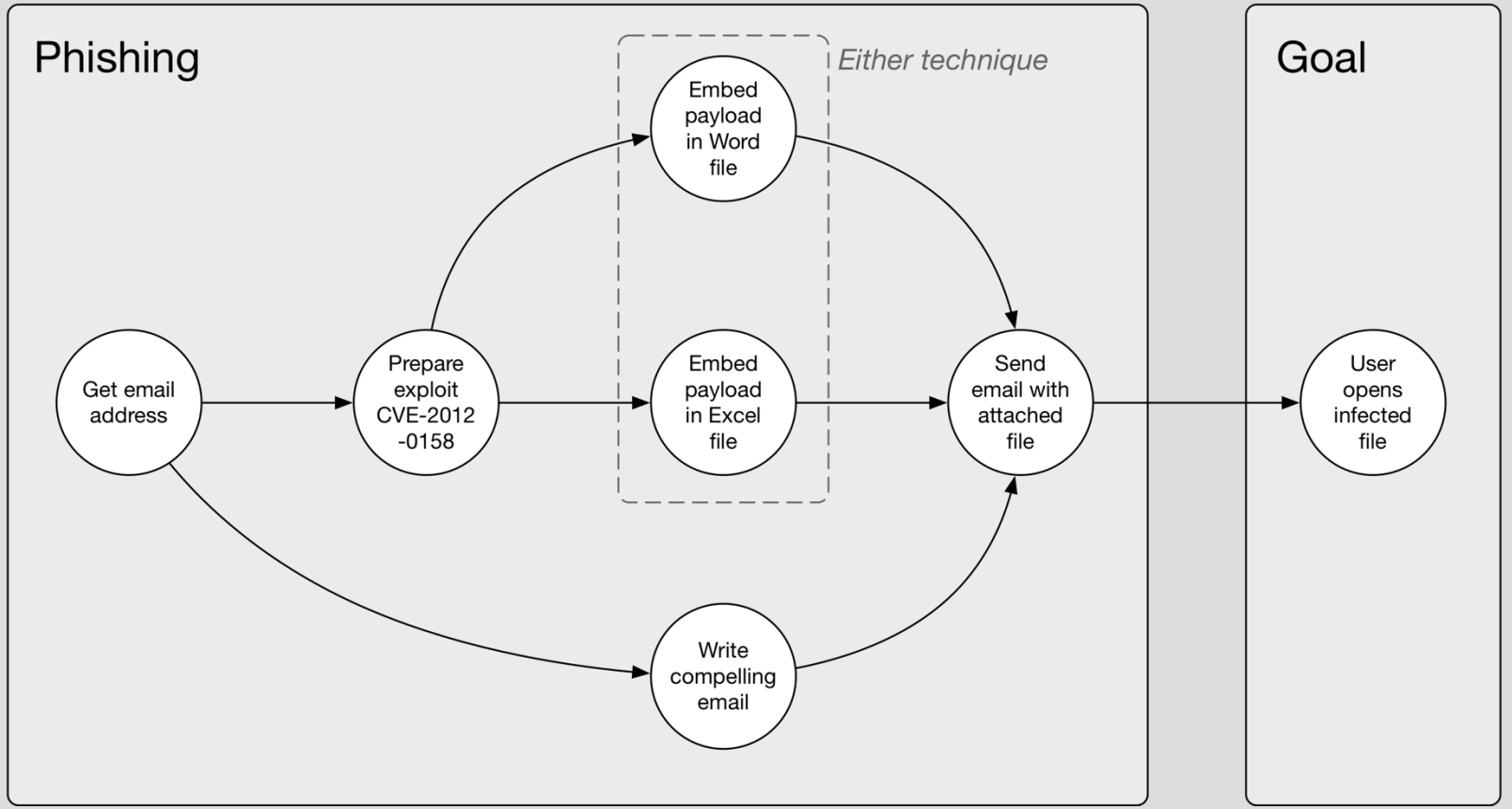


Procedures: the algorithmic, atomic unit of cyberspace operations

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



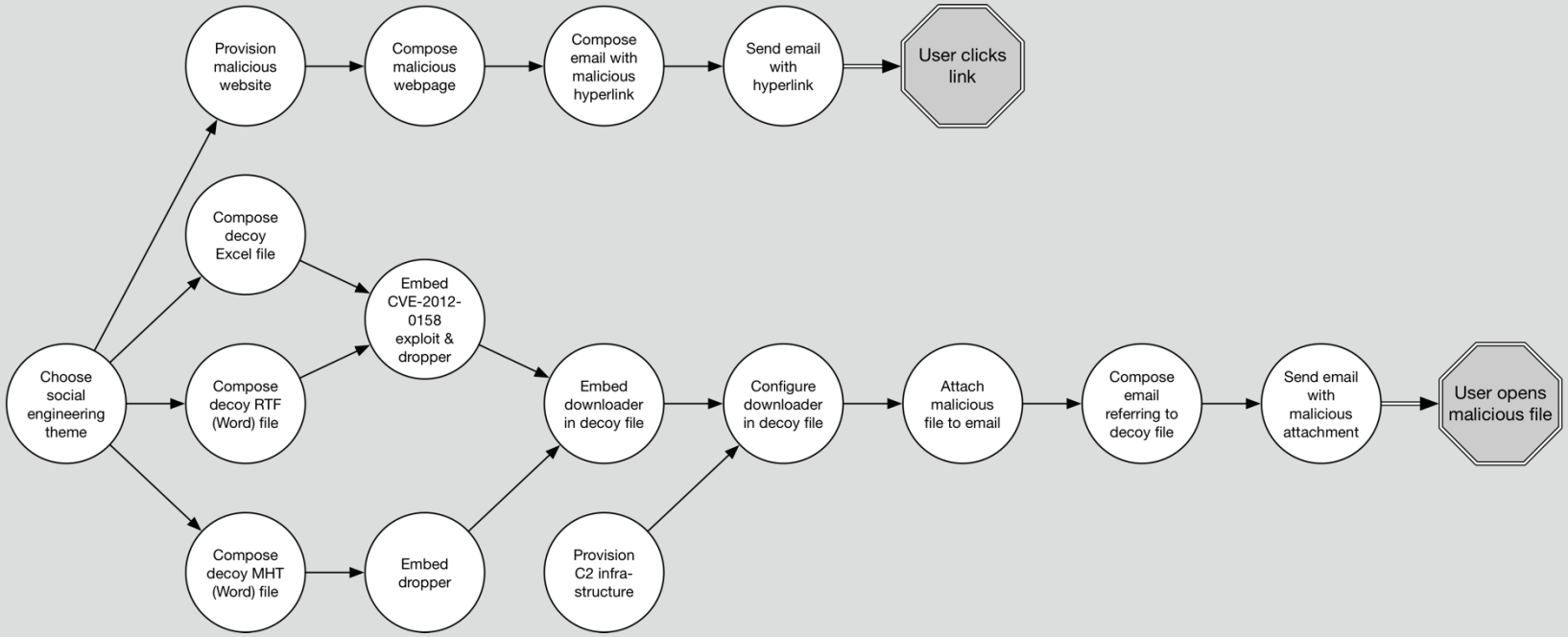
Procedures: the algorithmic, atomic unit of cyberspace operations

Techniques: unique ways to perform procedures

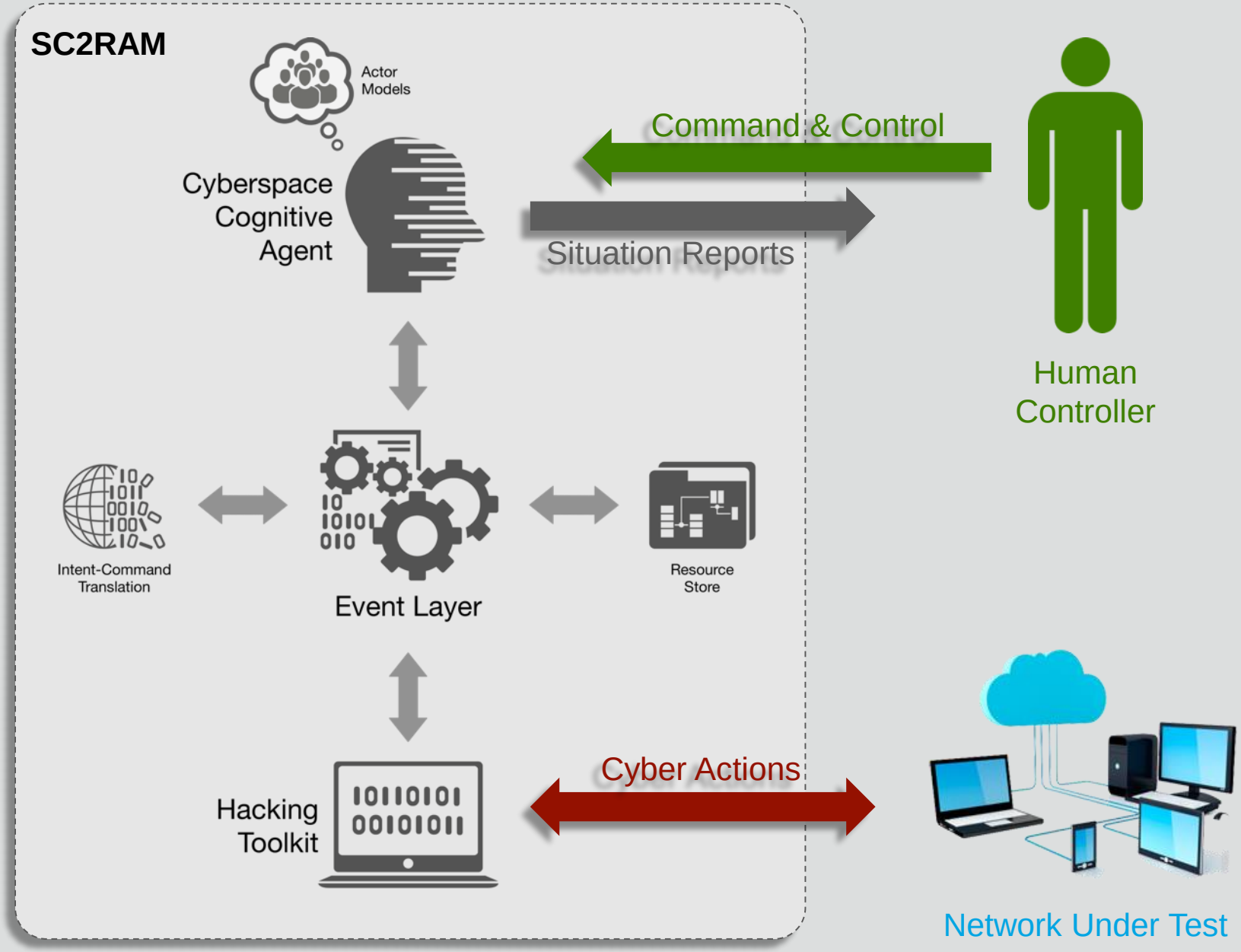
Tactics: directed subgraphs of procedures with one or more goals as their terminal nodes

Towards Common Models of Threat Actors

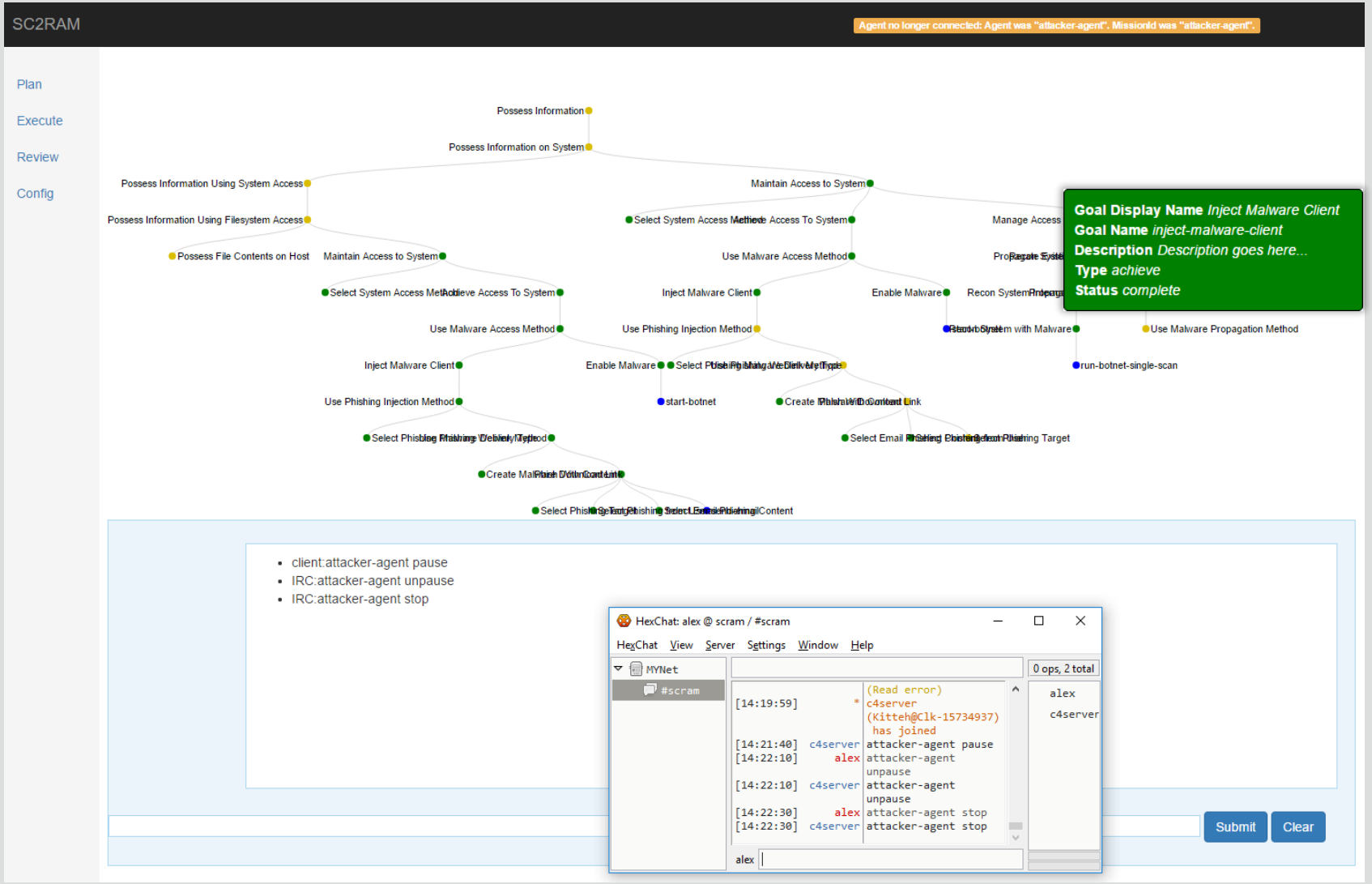
Partial model of APT28 (Fancy Bear) during Operation Pawn Storm



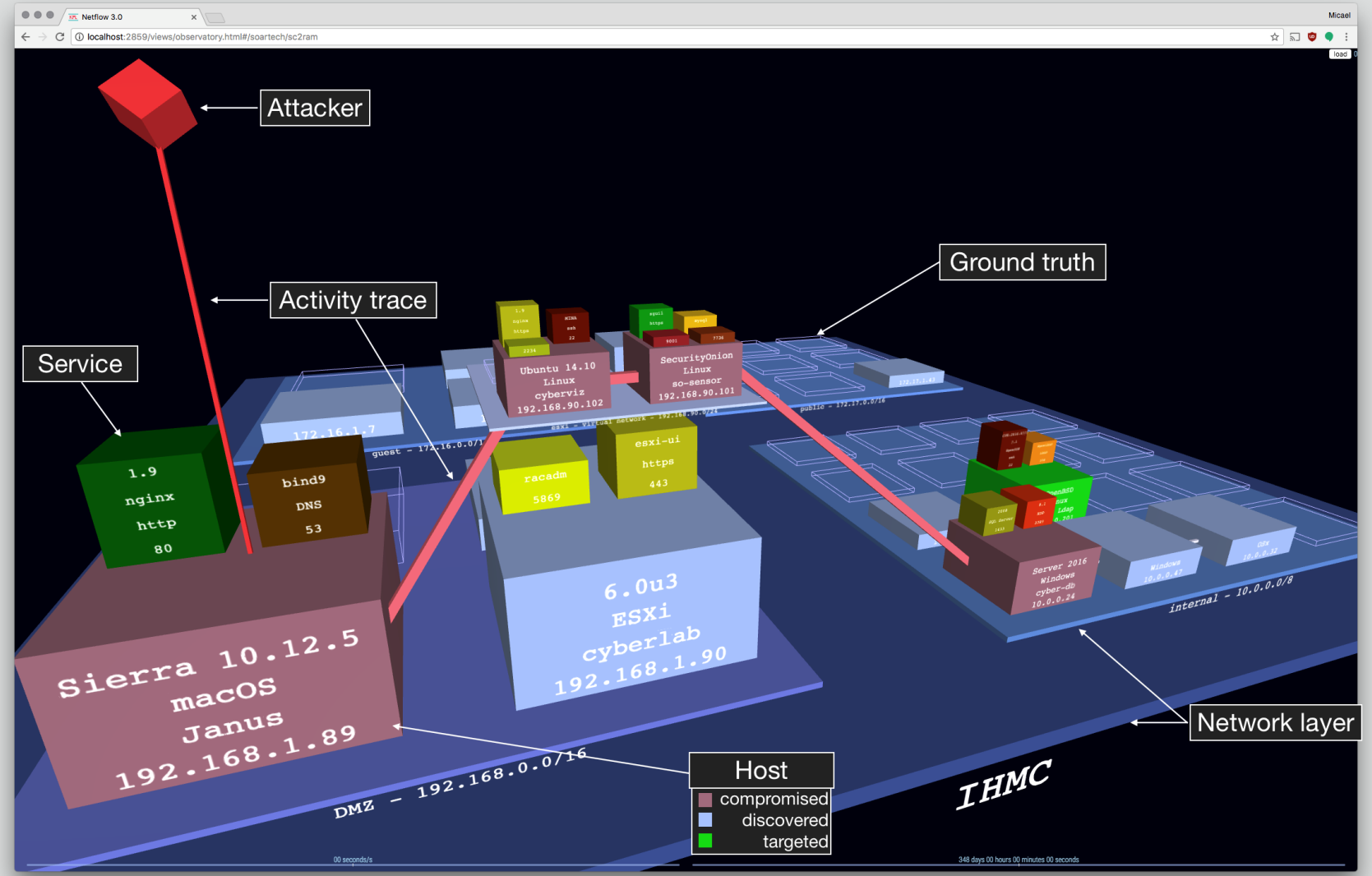
Simulated Cognitive Cyber Red-team Attack Model



SC2RAM Graphical User Interface

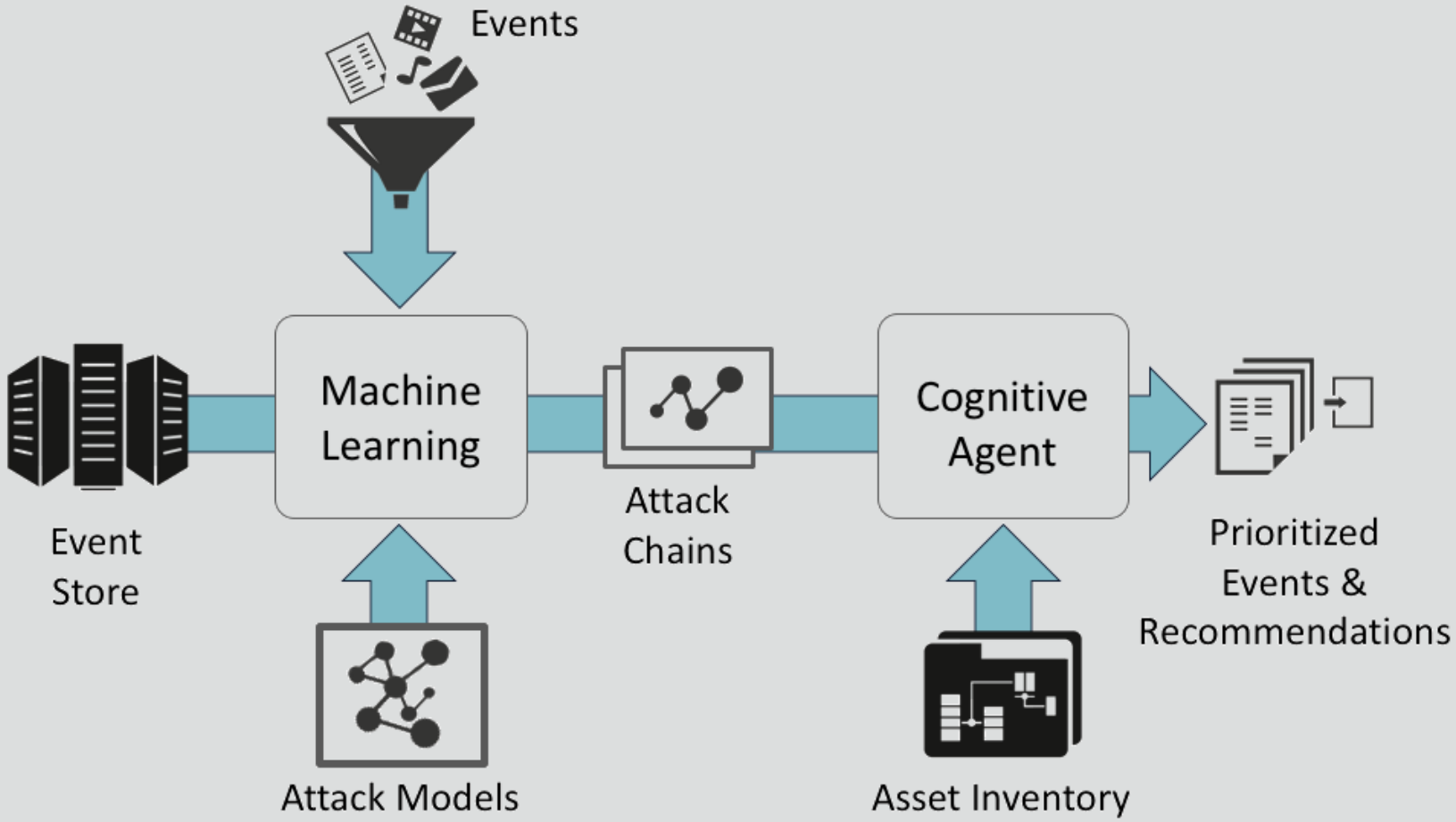


Network Attack Visualization

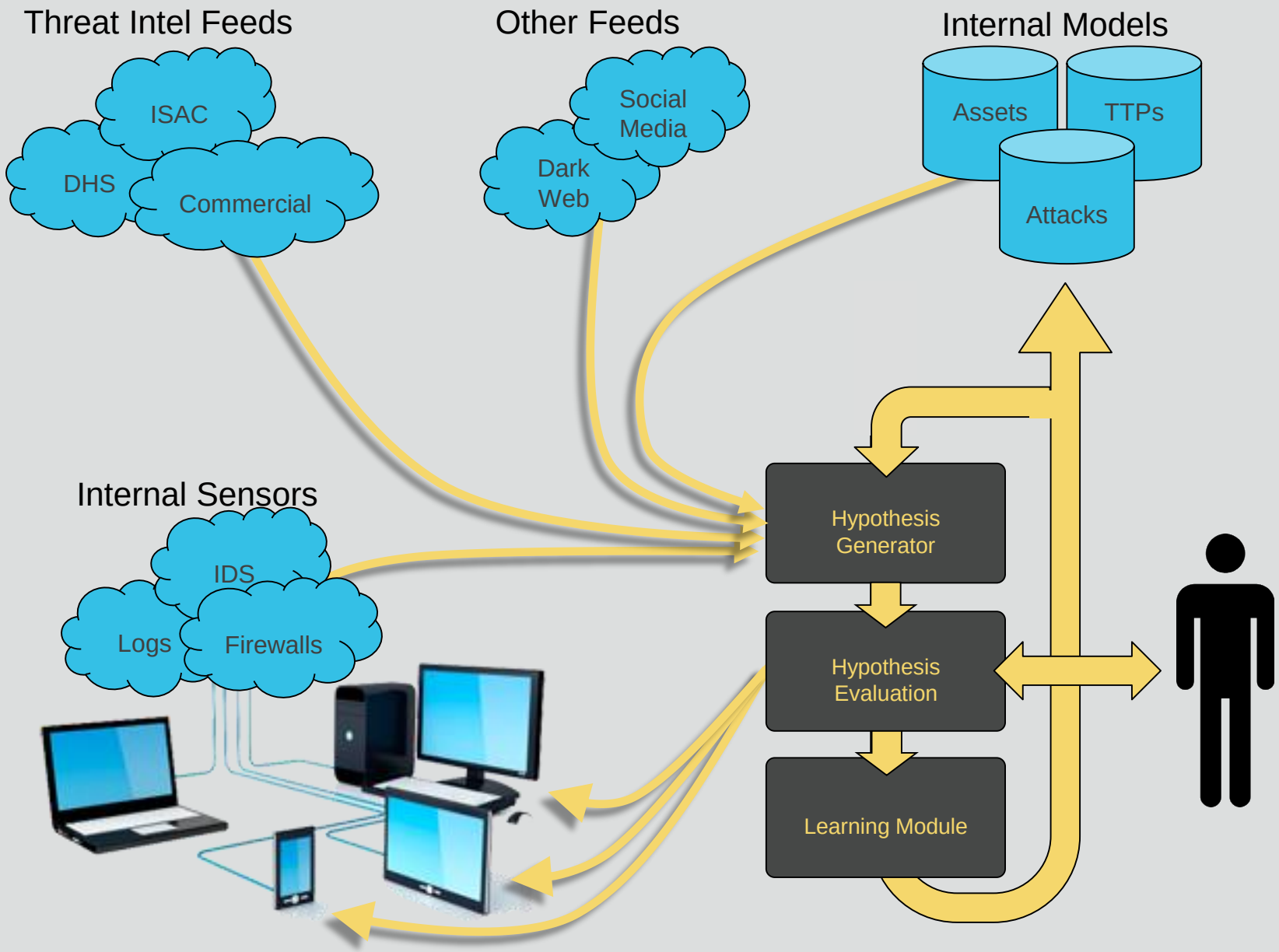


Developed by IHMC for SC2RAM

Using Synthetic Attackers for Cybersecurity



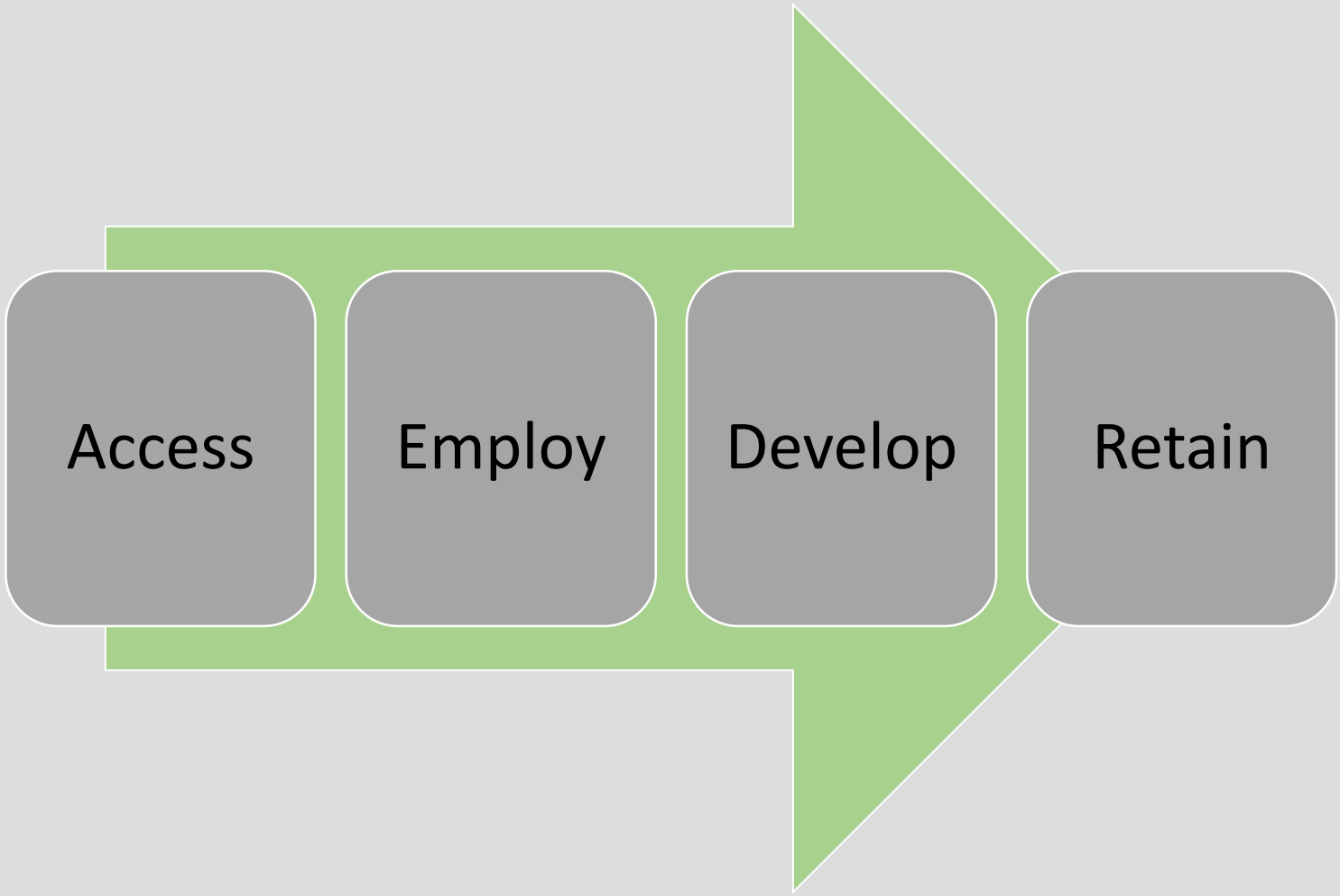
Autonomous Hunt Teammate



SOARTECH

- THE FUTURE THREAT LANDSCAPE
- SYNTHETIC TEAMMATES
- **WORKFORCE DEVELOPMENT**

Workforce Pipeline



What Are We Looking For?

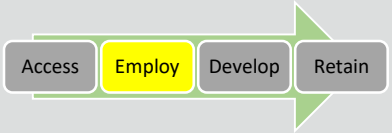
Source, fair use: http://host.madison.com/ct

Why?

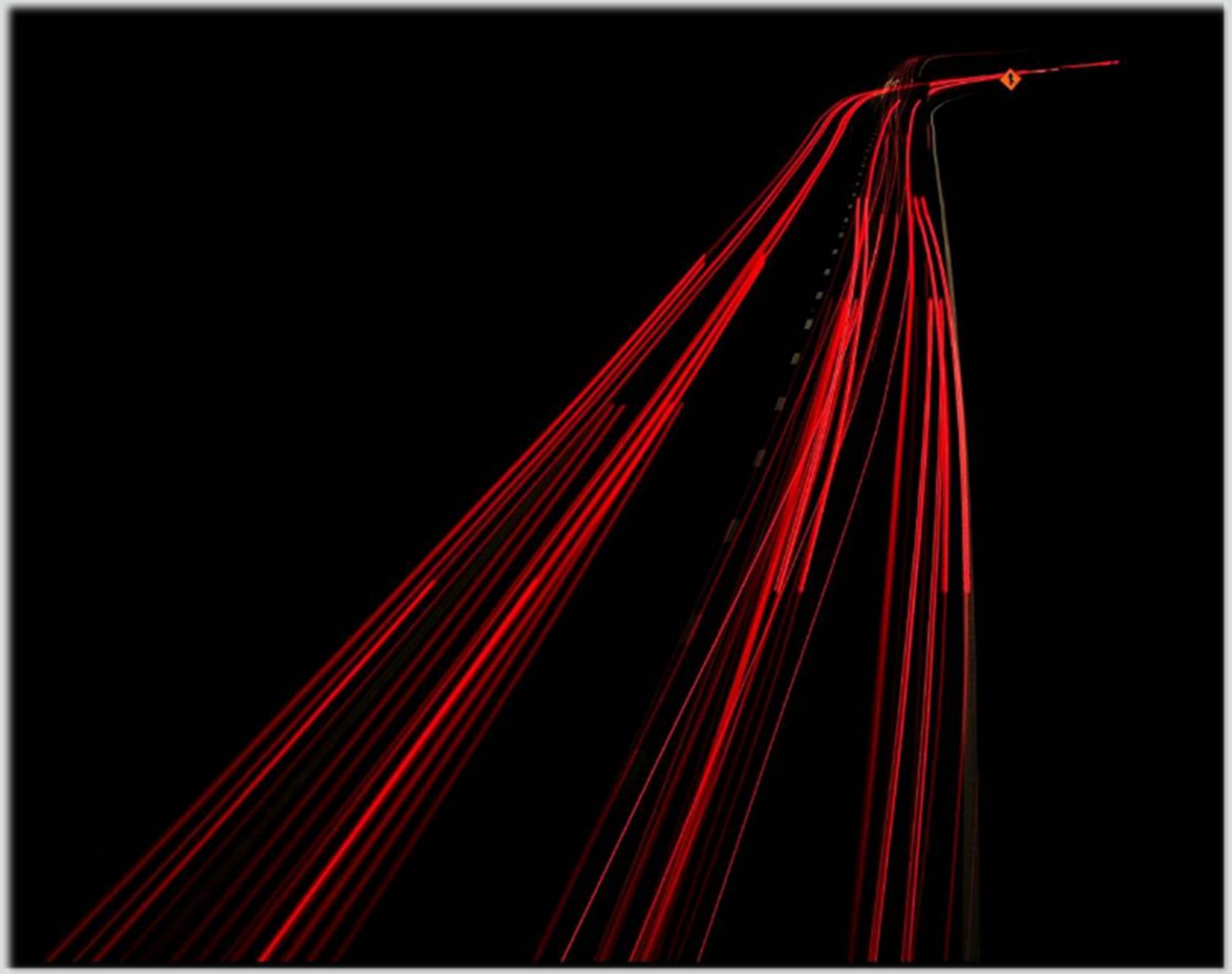
Source, fair use: http://dailymail.co.uk

Key Hiring Trends in Cybersecurity

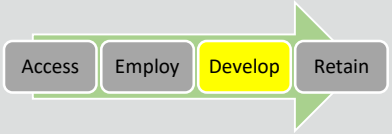
- Companies are seeking ***certified*** candidates
  - 35% of positions required a certification
- Companies are seeking ***educated*** candidates
  - 80% of positions require a Bachelor's degree
- Hands-on skills are more valuable than managerial ones
  - Lead Software Developer average salary: $ 233,333
  - 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

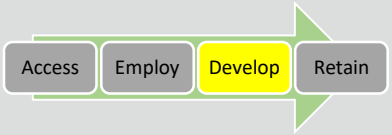


Source, fair use: http://www.naturethruphotos.com

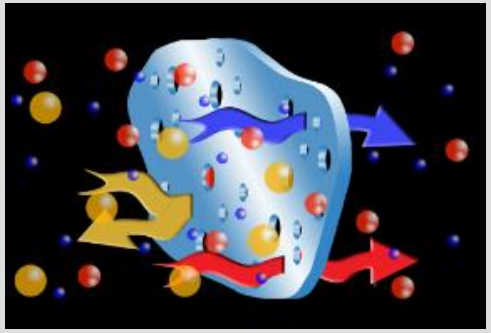


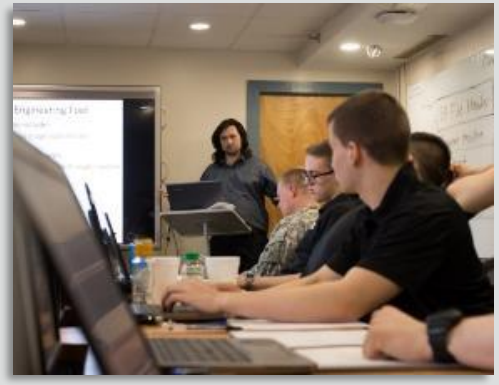
Developing the Cybersecurity Workforce

Source, fair use: https://certification.comptia.org



Retention





Most Importantly…

Source: https://www.123rf.com/profile_garagestock

Access | Employ | Develop | Retain

SOARTECH

Modeling human reasoning.
Enhancing human performance.

fernando.maymi@soartech.com