

# Synthetic Teammates and the Future of Cybersecurity

**Dr. Fernando Maymí**

Lead Scientist, Cyberspace Operations

Soar Technology, Inc.

[fernando.maymi@soartech.com](mailto:fernando.maymi@soartech.com)



**SOARTECH**

Modeling human reasoning.  
Enhancing human performance.

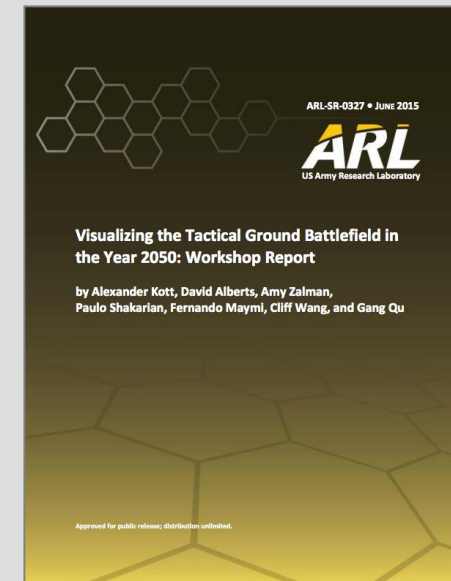
8 August 2017

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

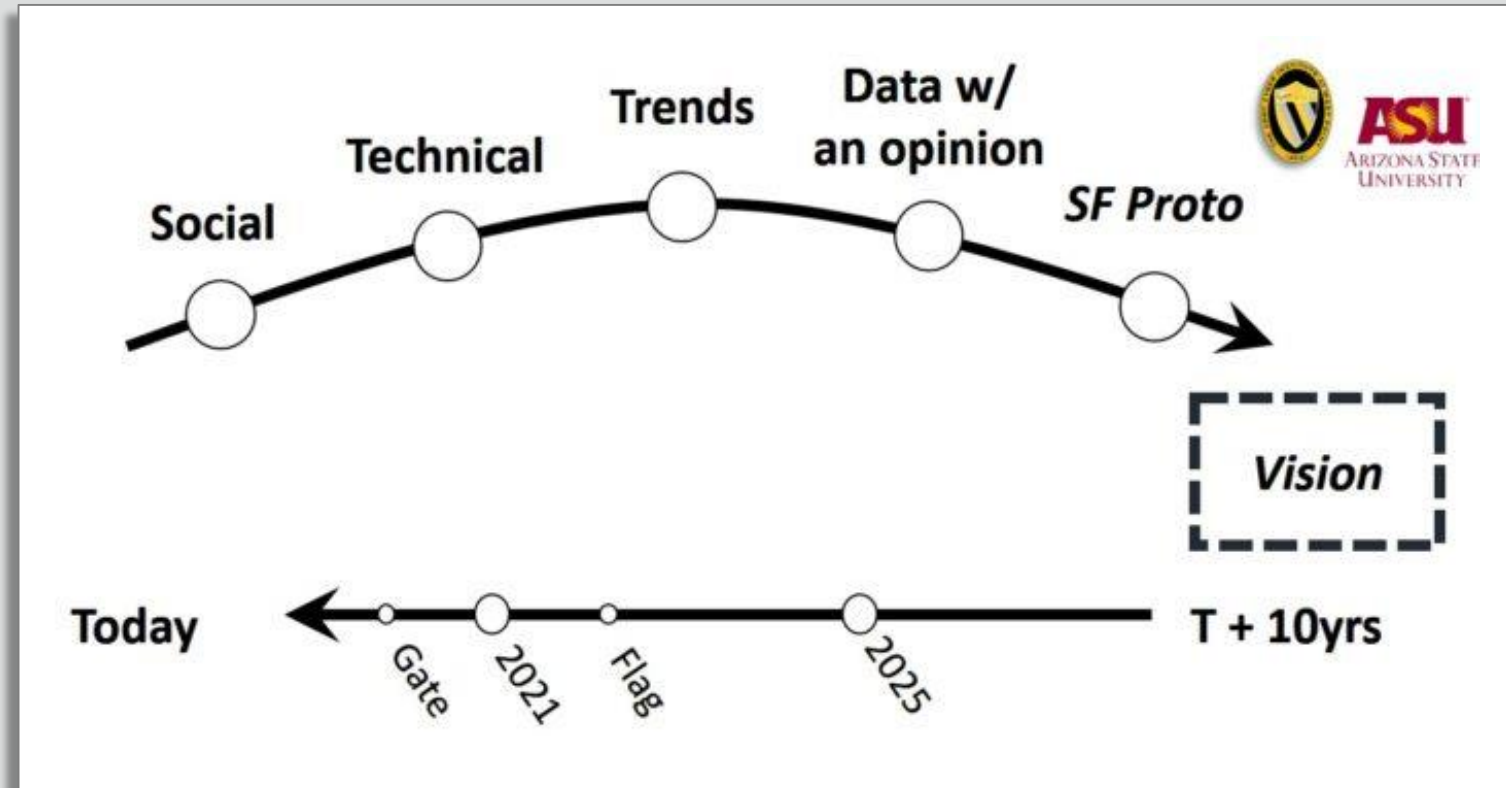
- **THE FUTURE THREAT LANDSCAPE**
- SYNTHETIC TEAMMATES
- WORKFORCE DEVELOPMENT

# 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**

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...





**PART ONE: BEFORE TUESDAY****WEAVER & SONS SUPPLY CO.**

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.

**FAST SHIPPING & MOVING**  
TAOCOR SYSTEM TECHNOLOGIES

**877-555-08**

• **SHIPPING & MOVING  
SUPPLIES**

• **MONEY TRANSFER**

**FROM:** FUNDS@UUSBANK.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**

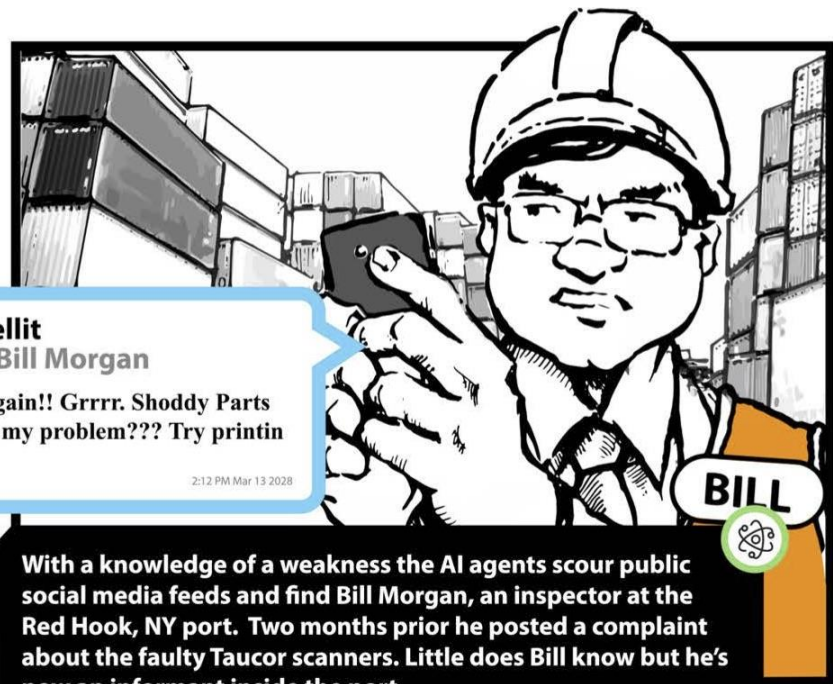
Now with access to internal supply chain networks and using artificial intelligence (AI) agents to crawl message boards, the terror group discovers the Taucor Detectr 400, a gaseous ionization detector used to inspect cargo. The scanners are prone to malfunction and critical repair parts come from limited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



**Tellit**  
@Bill Morgan

Taucor Again!! Grrrr. Shoddy Parts somehow my problem??? Try printin local!?!

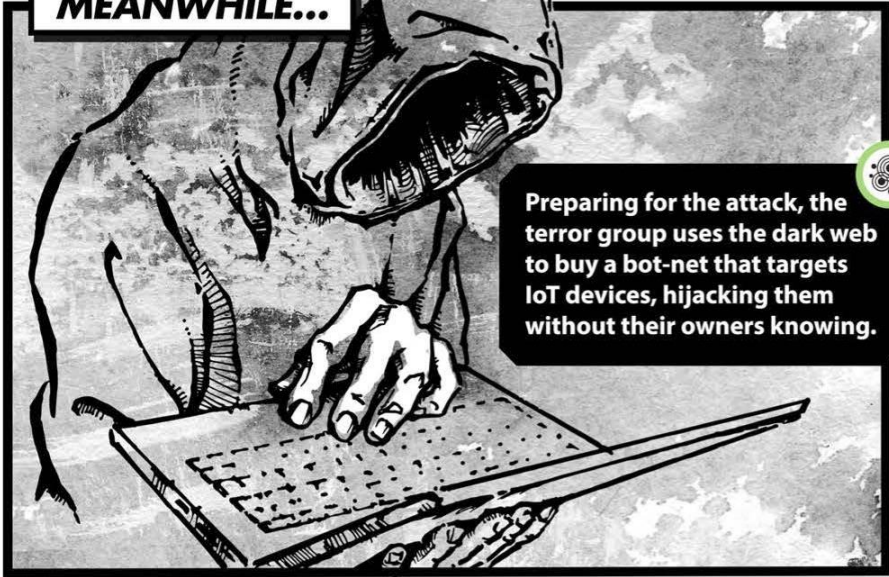
2:12 PM Mar 13 2028



**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

Taucor Again!!! Stupid scanners. Long night for me.

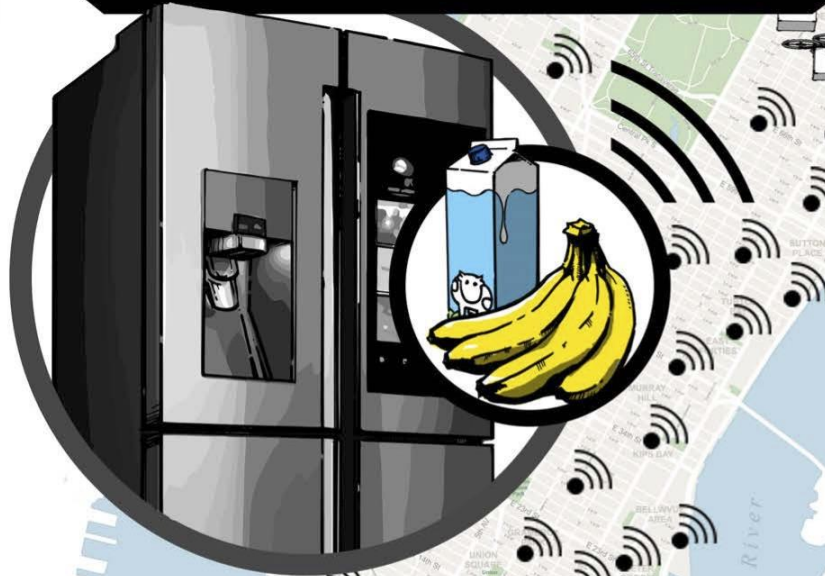
5:33 PM July 26 2028

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

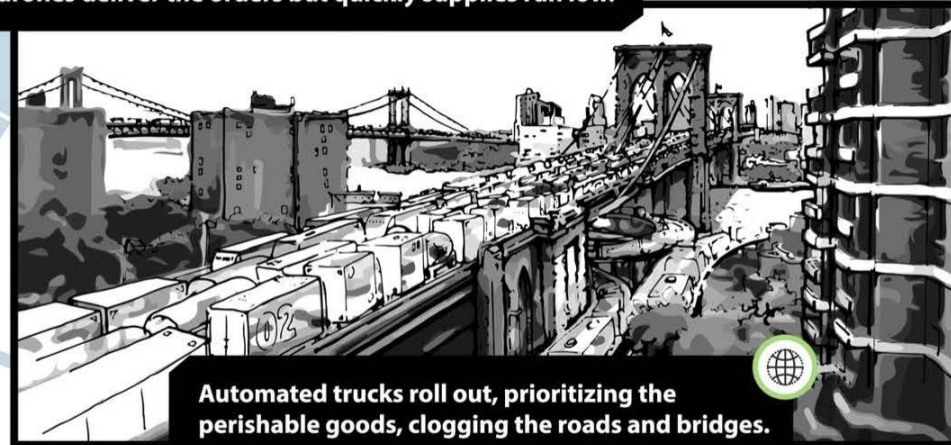


## PART TWO: TUESDAY

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.



A single container slips through uninspected...

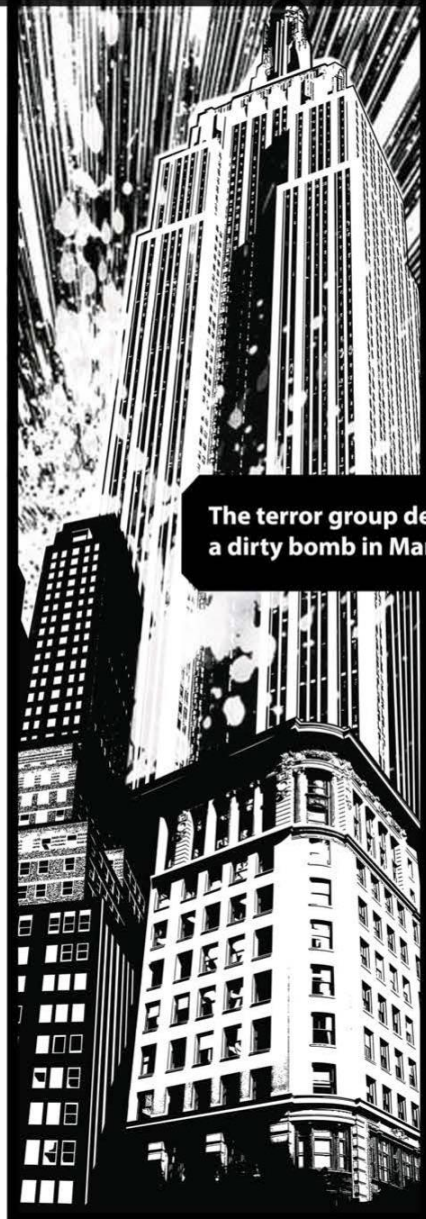


# PART THREE: TWO DAYS AFTER TUESDAY

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

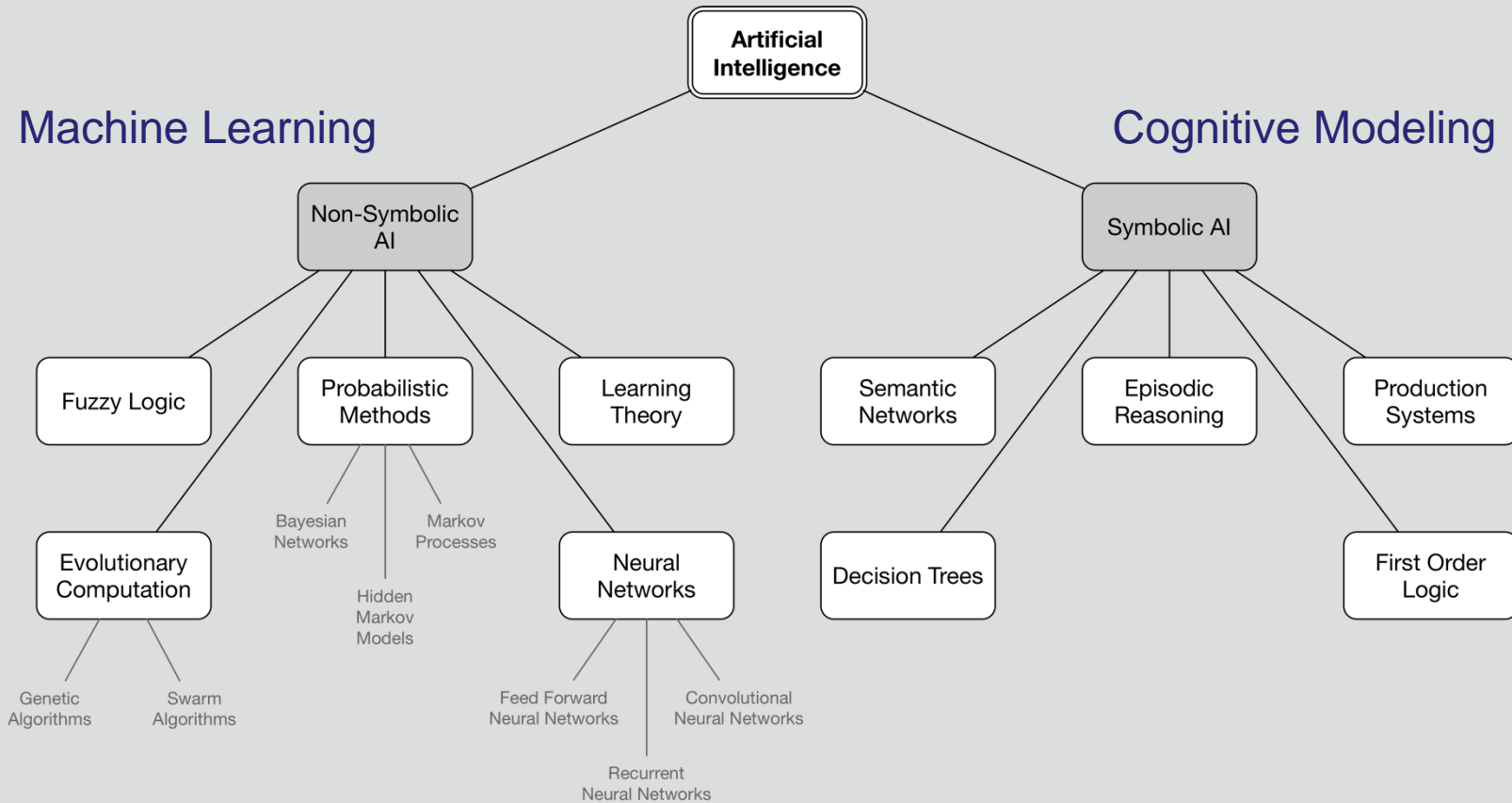
### *Understanding the context is essential*

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

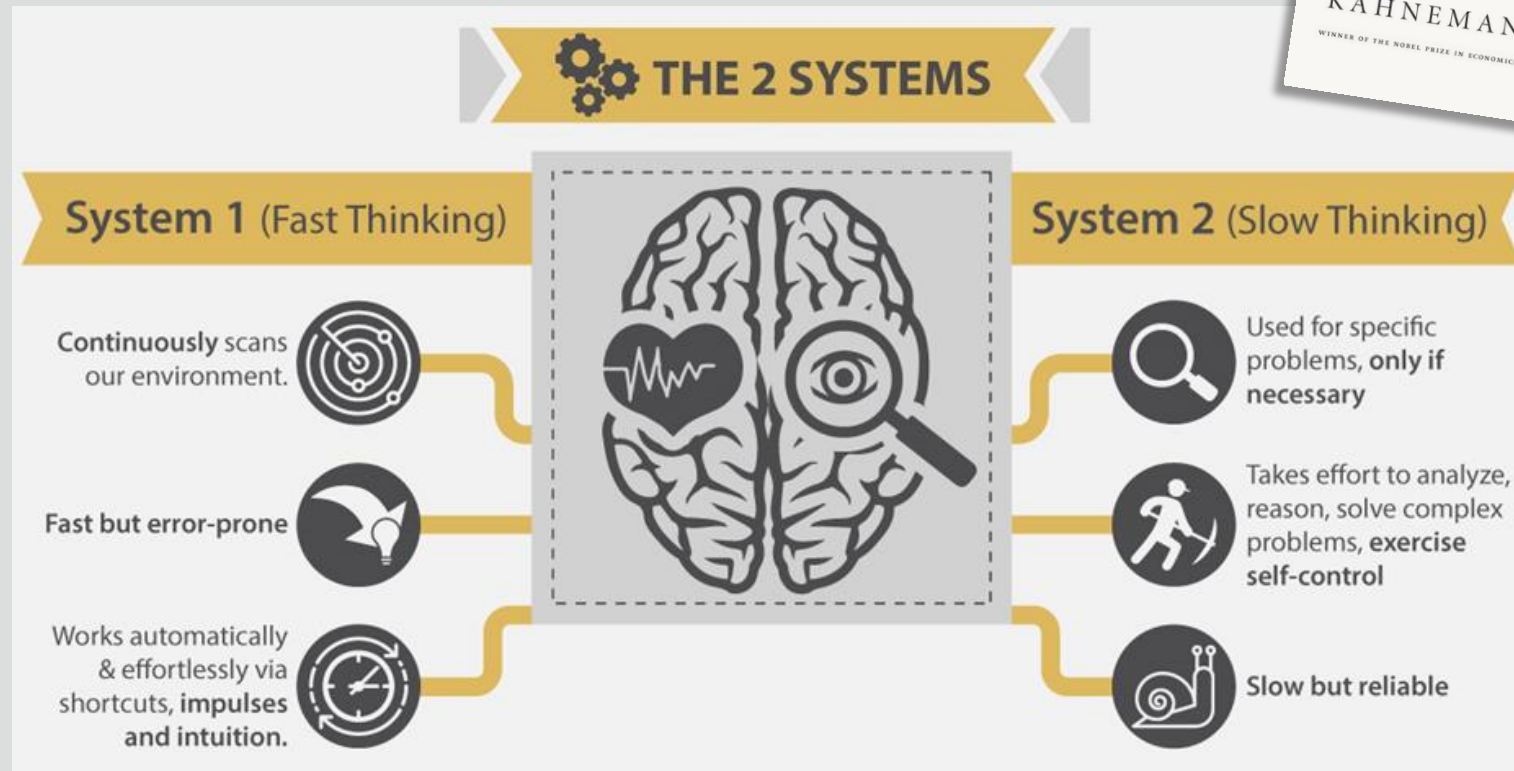
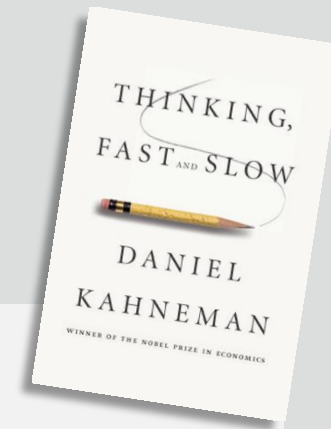


- THE FUTURE THREAT LANDSCAPE
- **SYNTHETIC TEAMMATES**
- WORKFORCE DEVELOPMENT

# Partial Artificial Intelligence Taxonomy



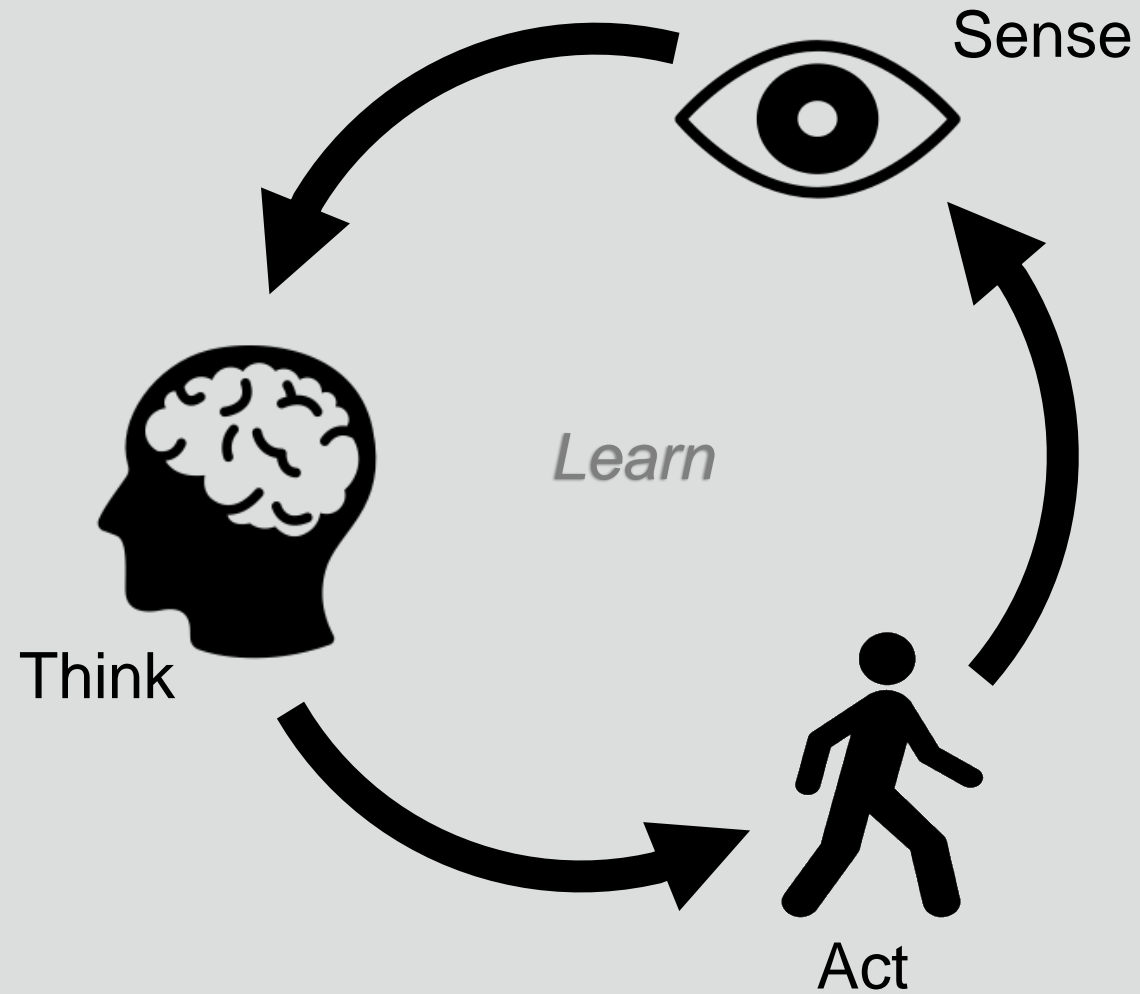
# (Oversimplifying) Artificial Intelligence



Analogous to  
Machine Learning

Analogous to  
Cognitive Modeling

# Autonomous Agents

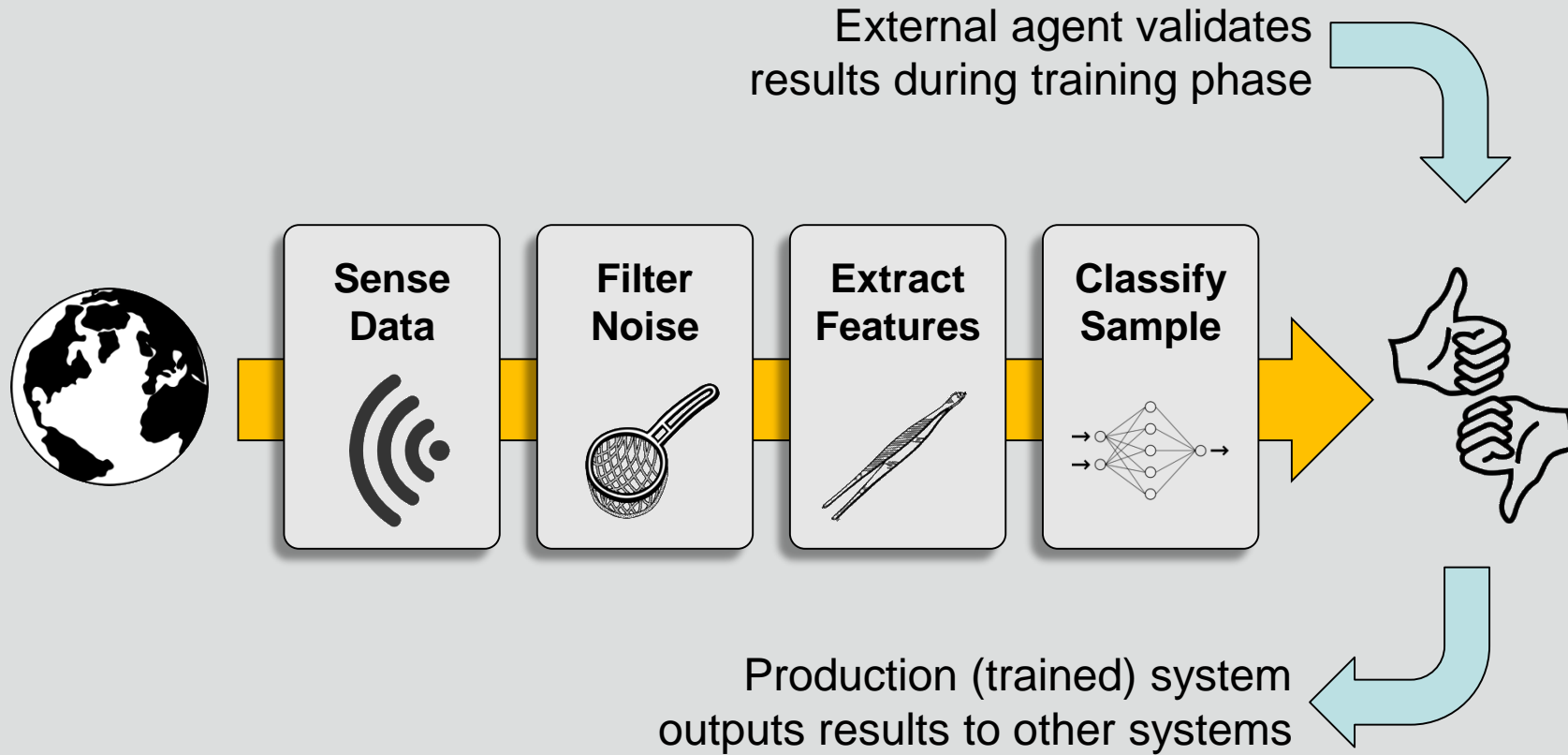




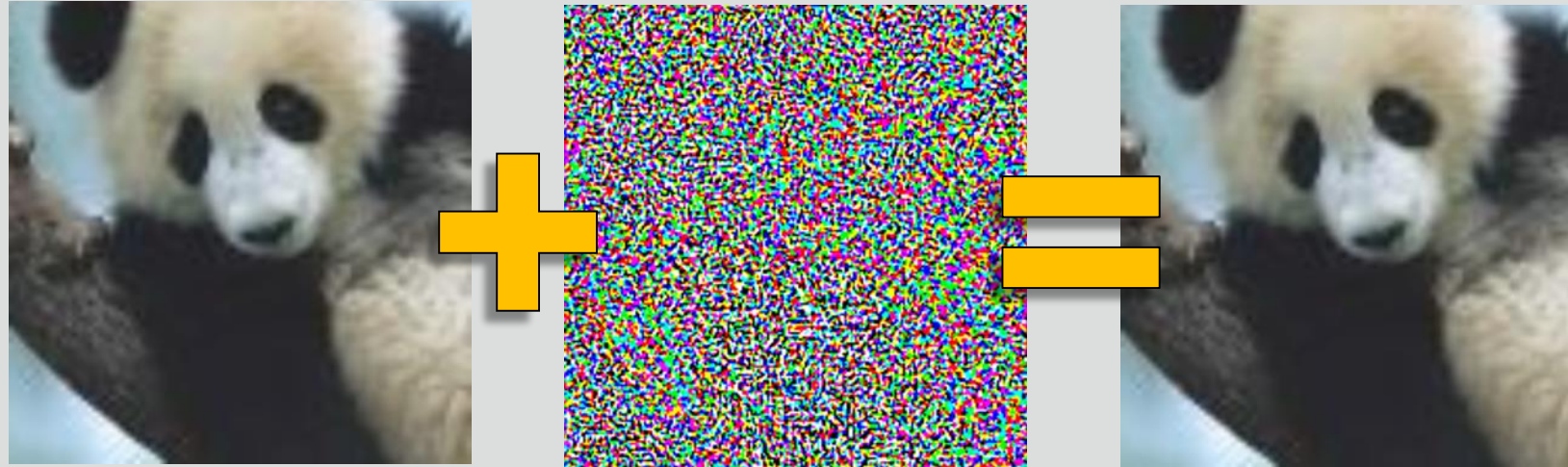
System 1

# MACHINE LEARNING

# Machine Learning



# Adversarial Machine Learning



Original image  
classified as a panda  
with 60% confidence

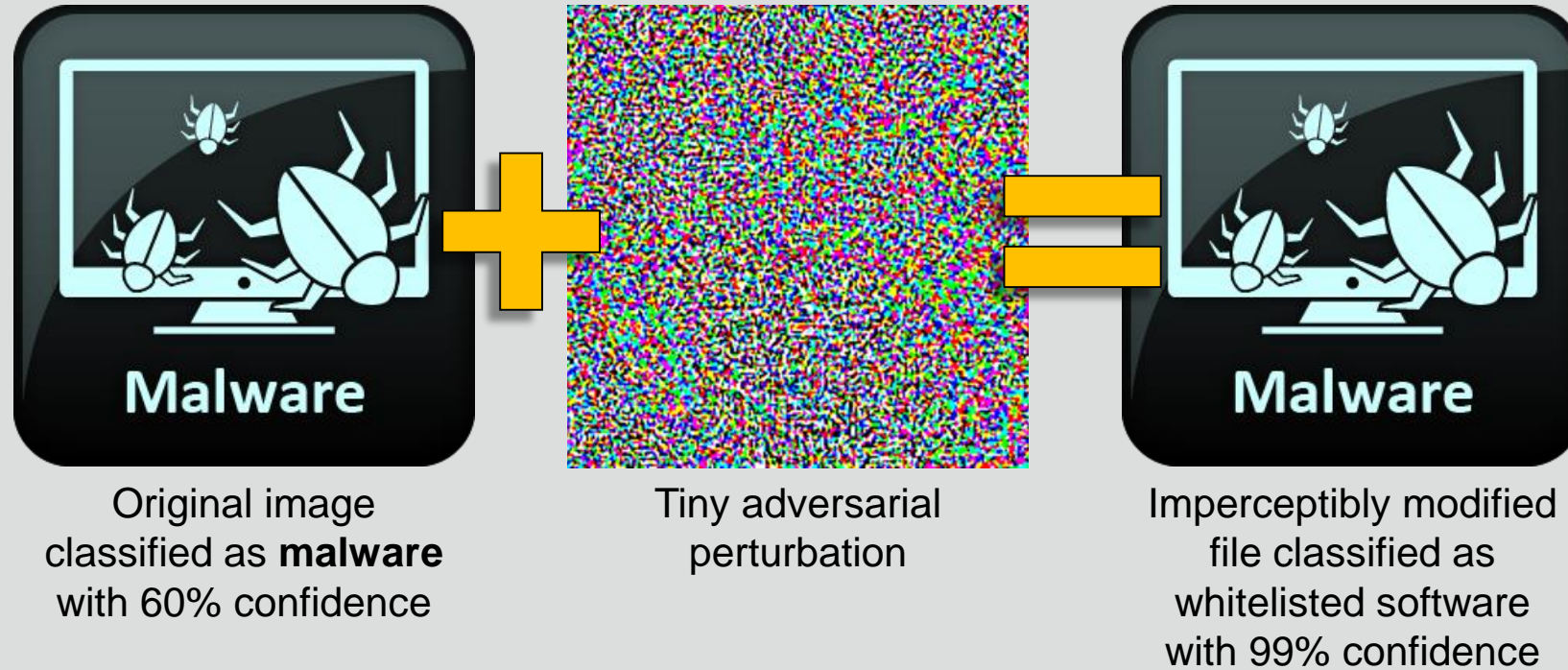
Tiny adversarial  
perturbation

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



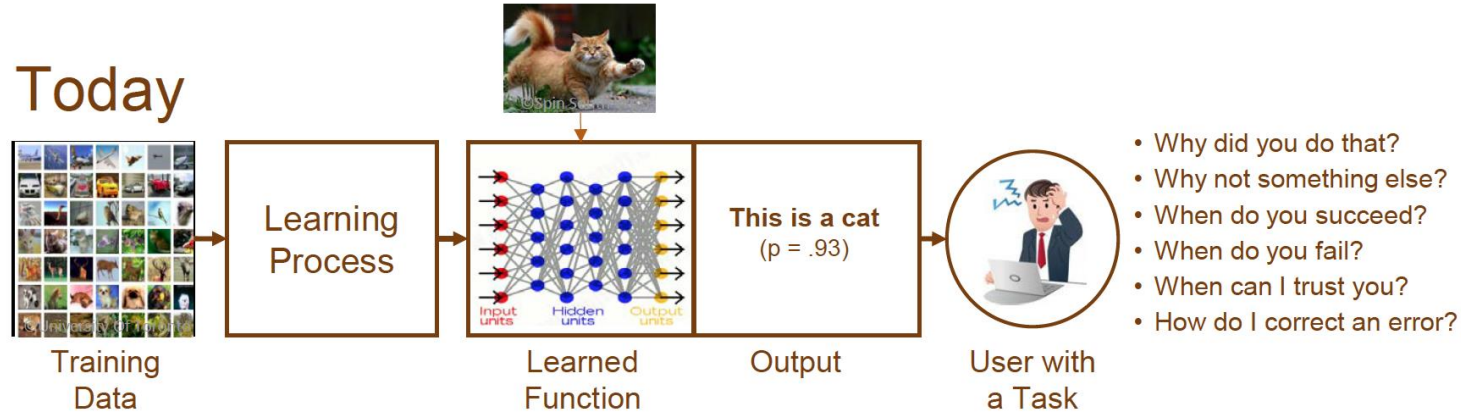


# Towards a Solution

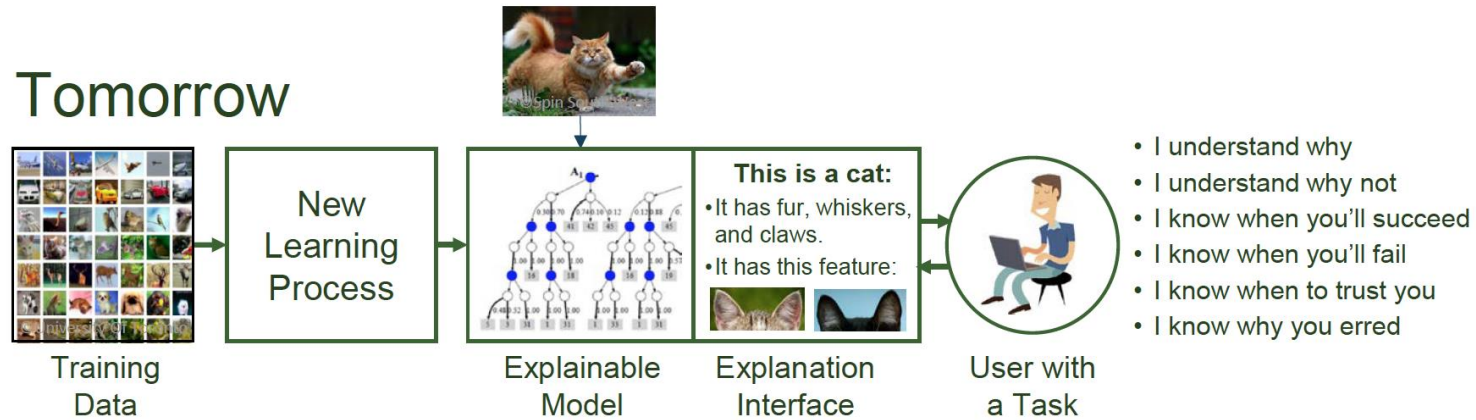


## Explainable AI – What Are We Trying To Do?

### Today



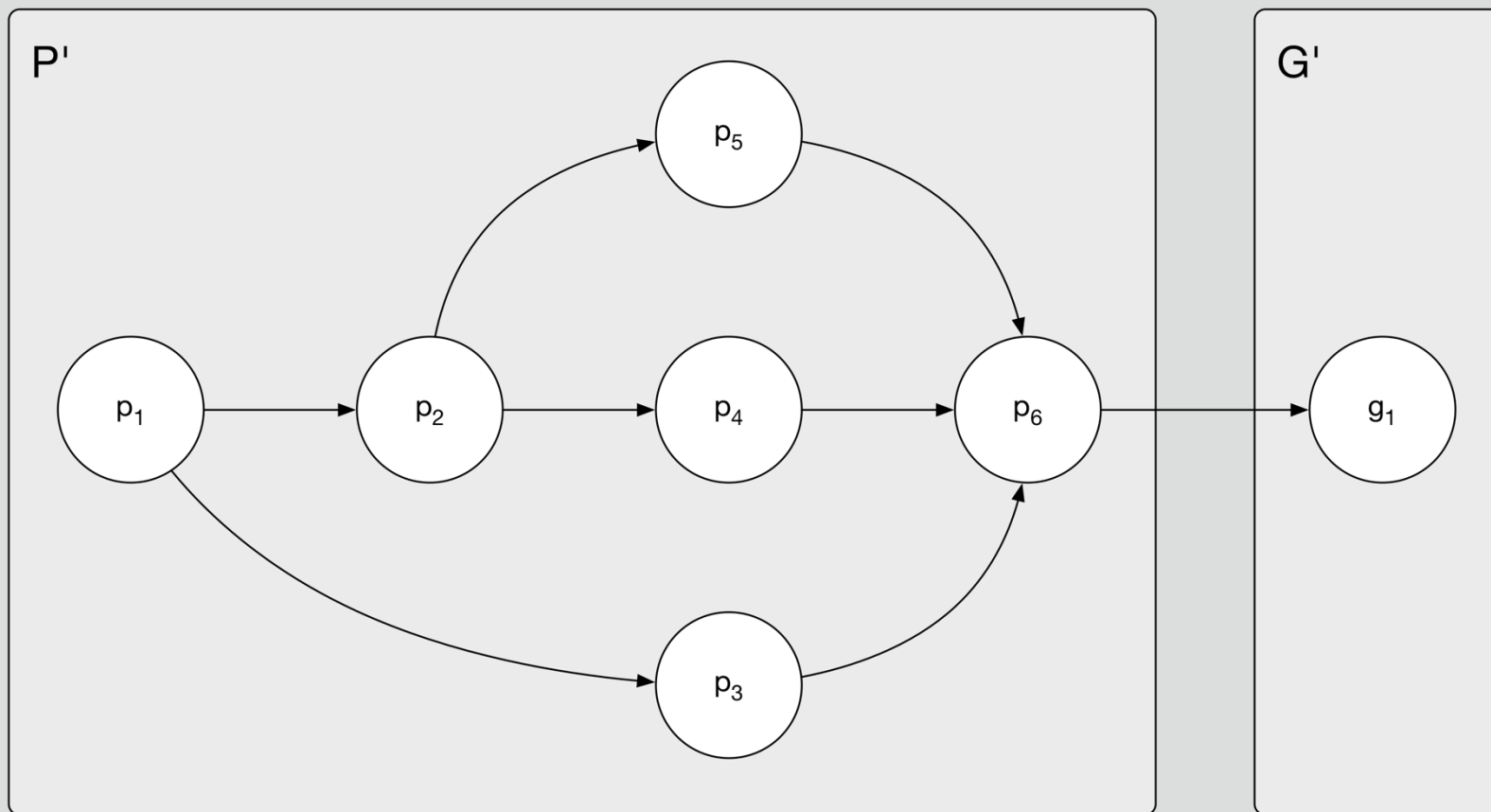
### Tomorrow



System 2

# COGNITIVE MODELING

## Towards a Common Model of TTPs

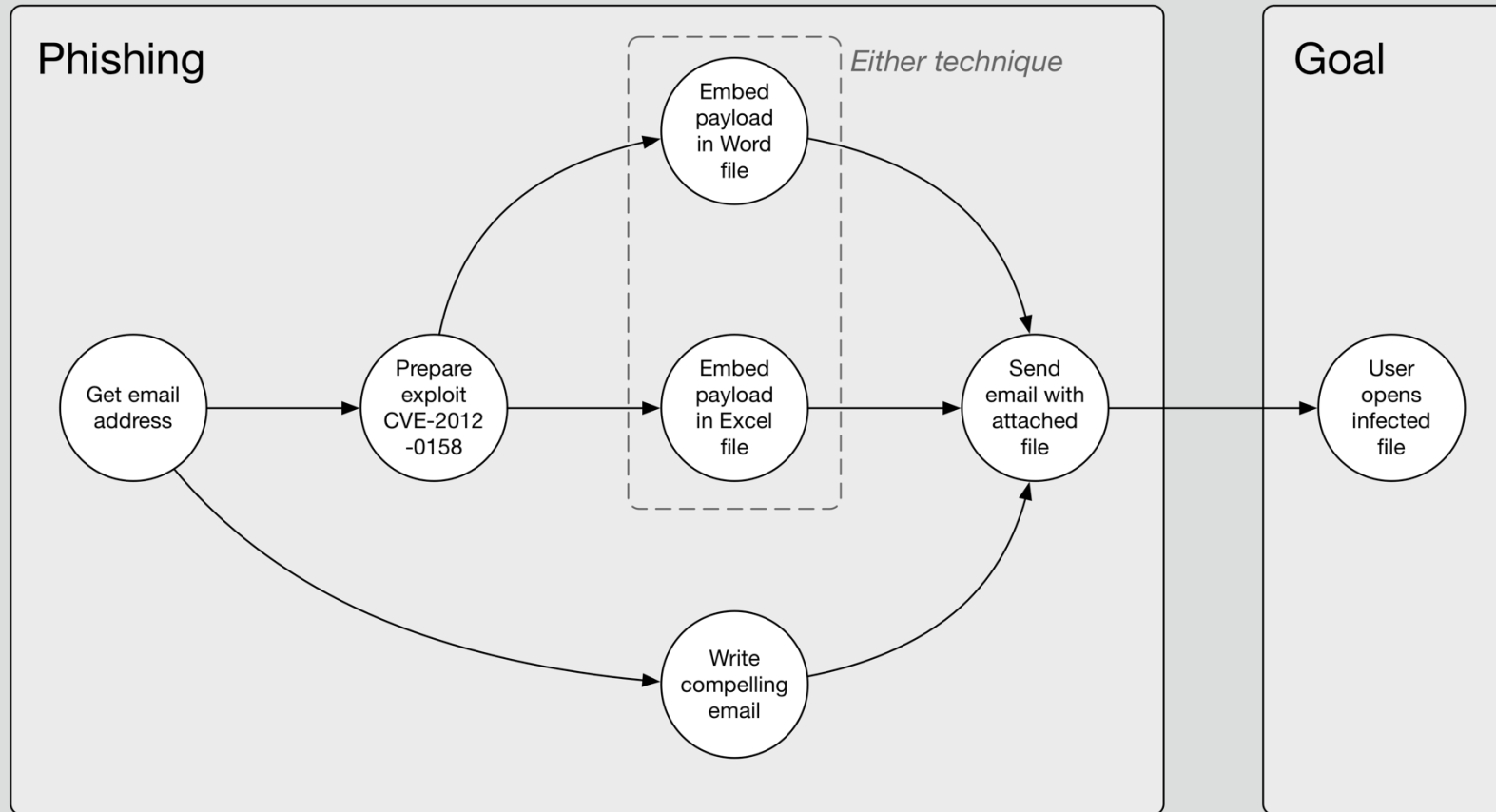


**Procedures:** the algorithmic, atomic unit of cyberspace operations

**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



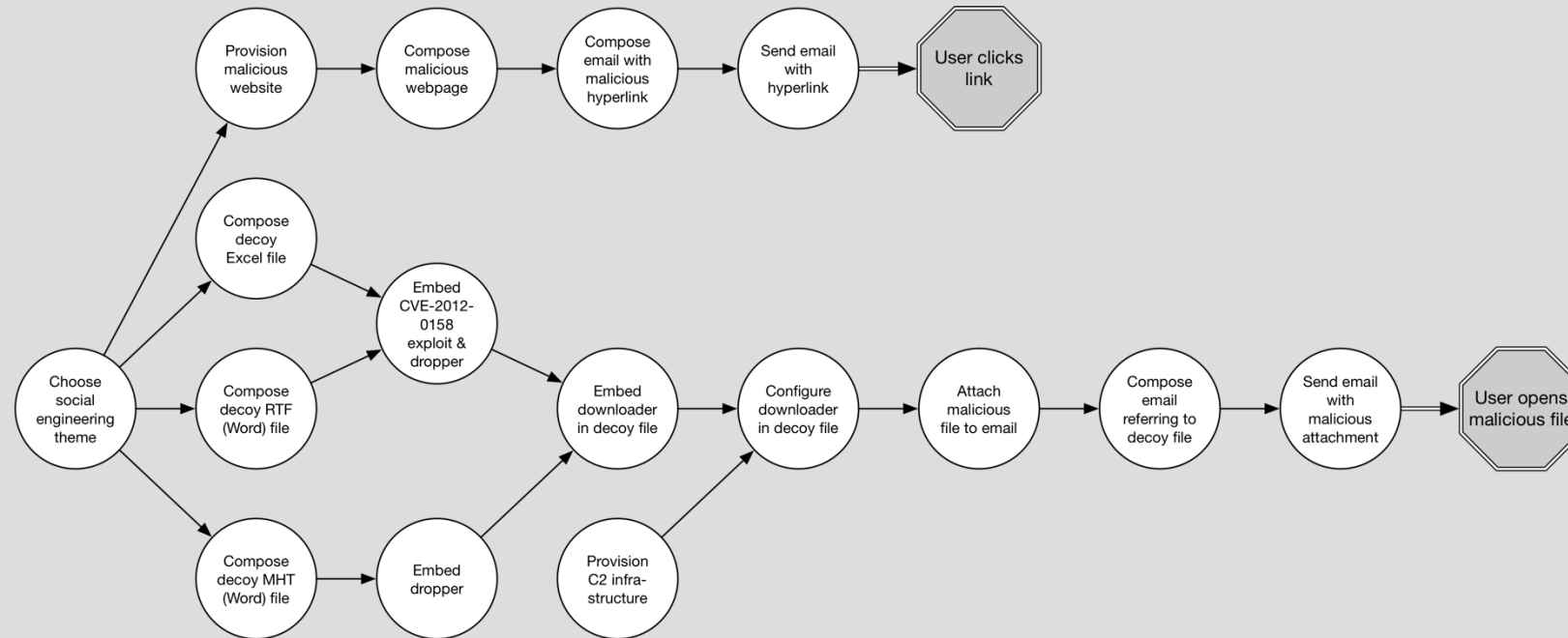
**Procedures:** the algorithmic, atomic unit of cyberspace operations

**Techniques:** unique ways to perform procedures

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

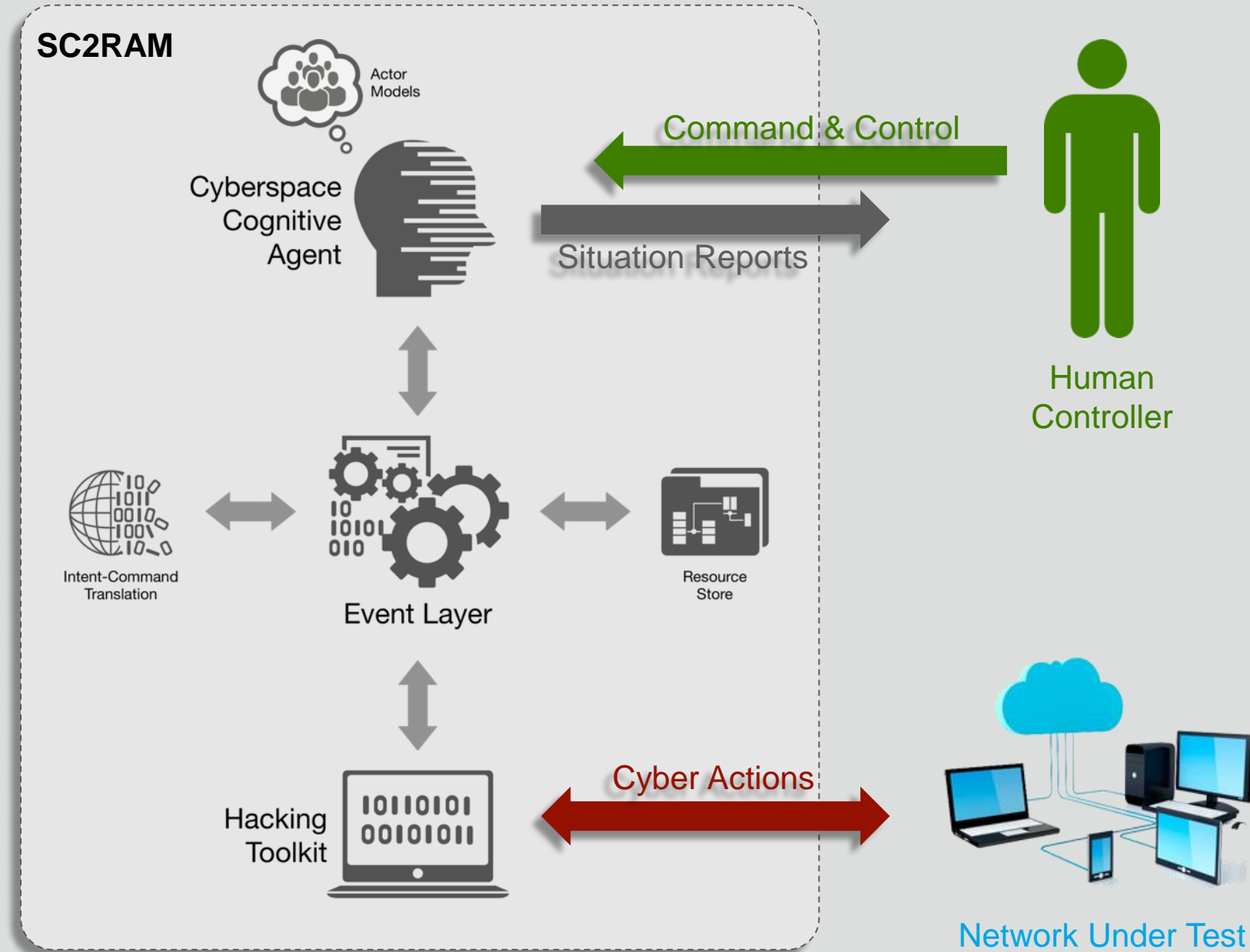
# Towards Common Models of Threat Actors

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





# Simulated Cognitive Cyber Red-team Attack Model



# SC2RAM Graphical User Interface

SC2RAM
Agent no longer connected: Agent was "attacker-agent", MissionId was "attacker-agent".

Plan

Execute

Review

Config

```

graph TD
    A[Possess Information] --> B[Possess Information on System]
    A --> C[Maintain Access to System]
    B --> D[Possess Information Using System Access]
    B --> E[Possess Information Using Filesystem Access]
    C --> F[Select System Access Method]
    C --> G[Maintain Access to System]
    G --> H[Possess File Contents on Host]
    G --> I[Inject Malware Client]
    I --> J[Use Malware Access Method]
    J --> K[Use Phishing Injection Method]
    K --> L[Select Phishing Delivery Method]
    L --> M[Create Malicious Content]
    M --> N[Select Phishing Content]
    N --> O[Select Phishing Content]
    N --> P[Select Phishing Content]
    C --> Q[Use Malware Access Method]
    Q --> R[Inject Malware Client]
    R --> S[Enable Malware]
    S --> T[Select Phishing Delivery Method]
    T --> U[Create Malicious Content]
    U --> V[Select Phishing Content]
    V --> W[Select Phishing Content]
    V --> X[Select Phishing Content]
    C --> Y[Use Malware Propagation Method]
    Y --> Z[Start System with Malware]
    Z --> AA[run-botnet-single-scan]
    C --> AB[Manage Access]
    C --> AC[Propagate System]
    C --> AD[Recon System]
    
```

**Goal Display Name** *Inject Malware Client*

**Goal Name** *inject-malware-client*

**Description** *Description goes here...*

**Type** *achieve*

**Status** *complete*

- client:attacker-agent pause
- IRC:attacker-agent unpause
- IRC:attacker-agent stop

HexChat: alex @ scam / #scram

HexChat View Server Settings Window Help

MYNet

#scram 0 ops, 2 total

[14:19:59] (Read error) c4server has joined

[14:21:40] c4server attacker-agent pause

[14:22:10] alex attacker-agent unpause

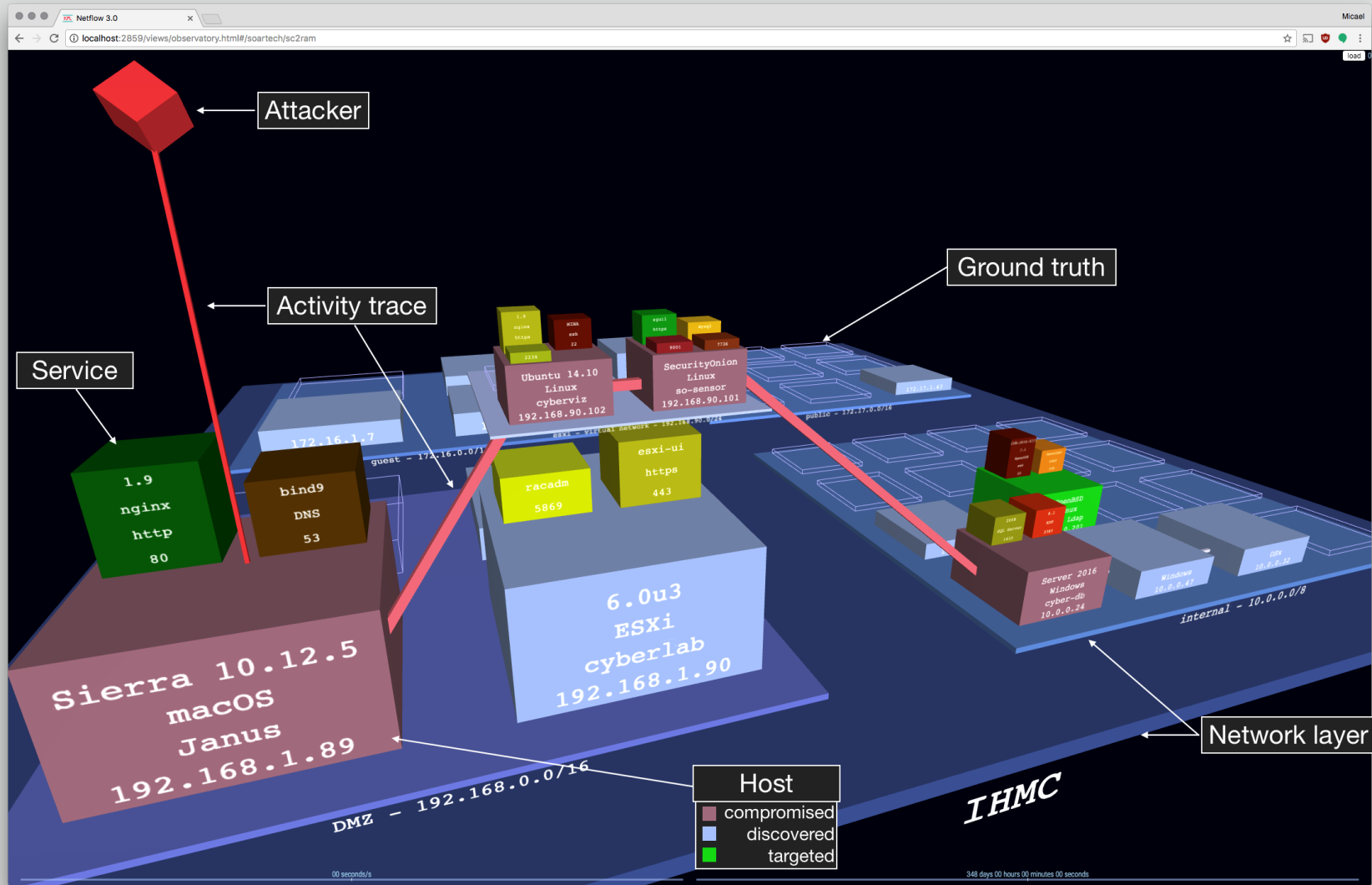
[14:22:10] c4server attacker-agent unpause

[14:22:30] alex attacker-agent stop

[14:22:30] c4server attacker-agent stop

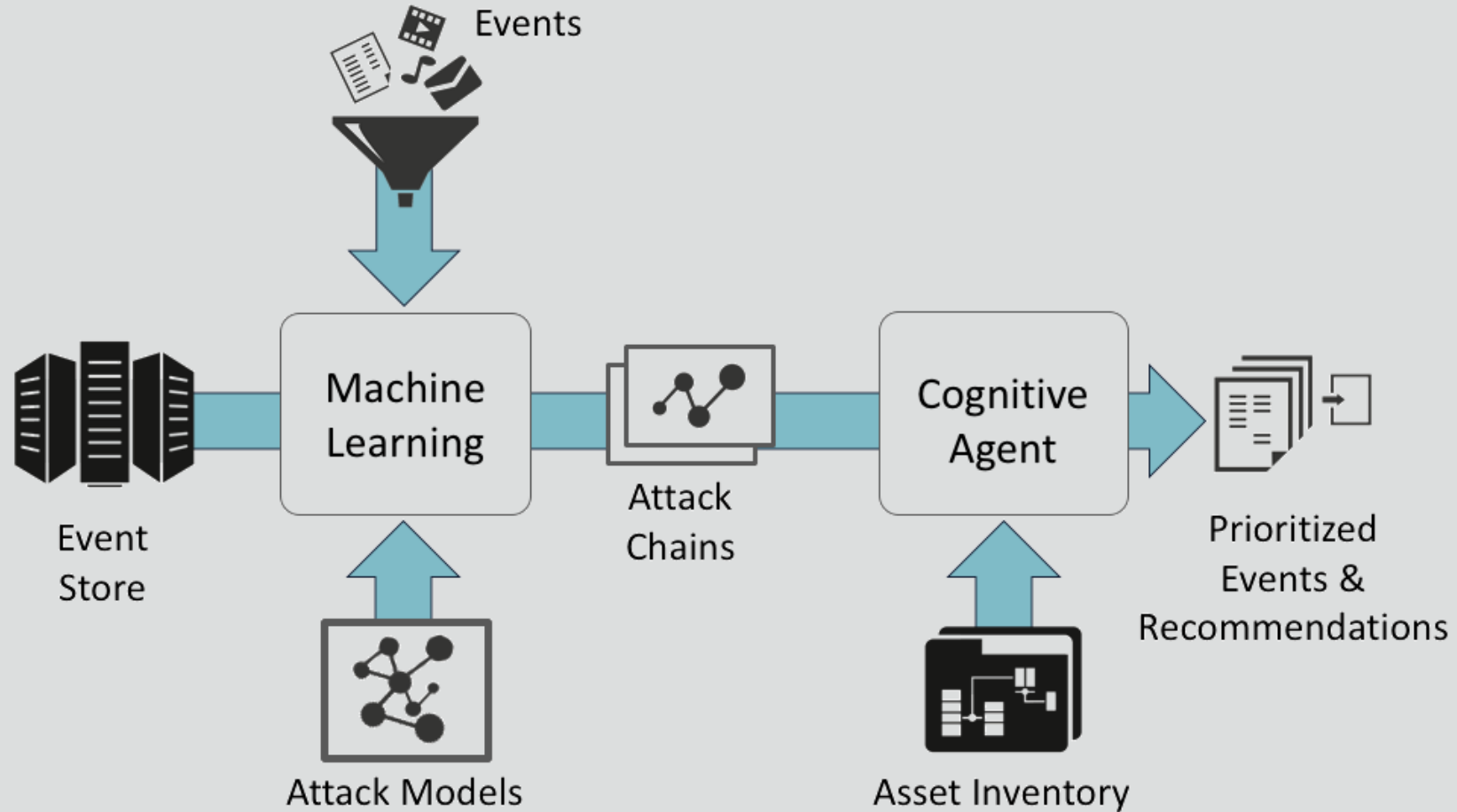
alex |

# Network Attack Visualization

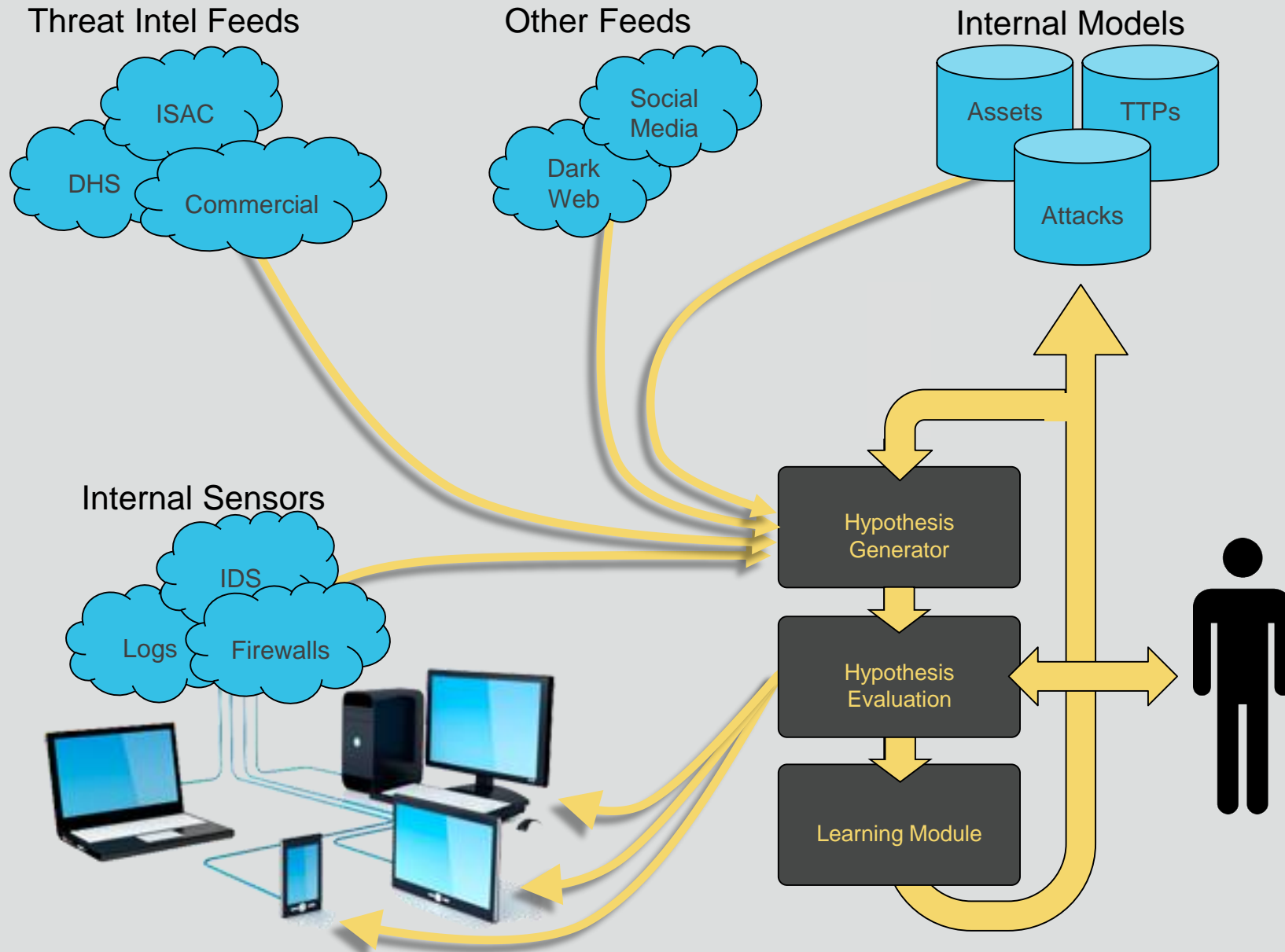


Developed by IHMC for SC2RAM

# Using Synthetic Attackers for Cybersecurity



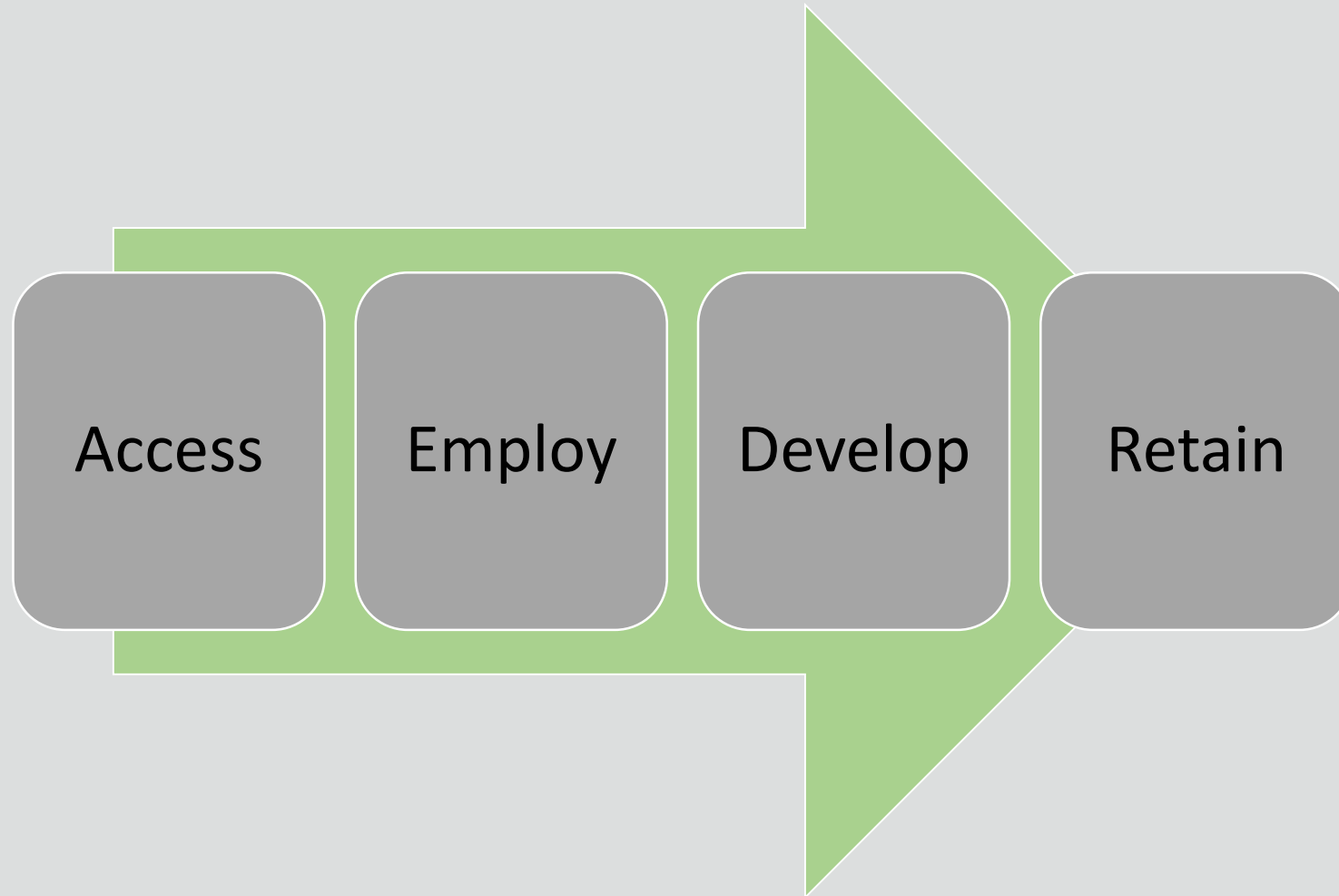
# Autonomous Hunt Teammate





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

# Workforce Pipeline



# What Are We Looking For?



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





# Why?

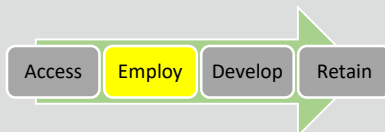


Source, fair use: <http://dailymail.co.uk>



# 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



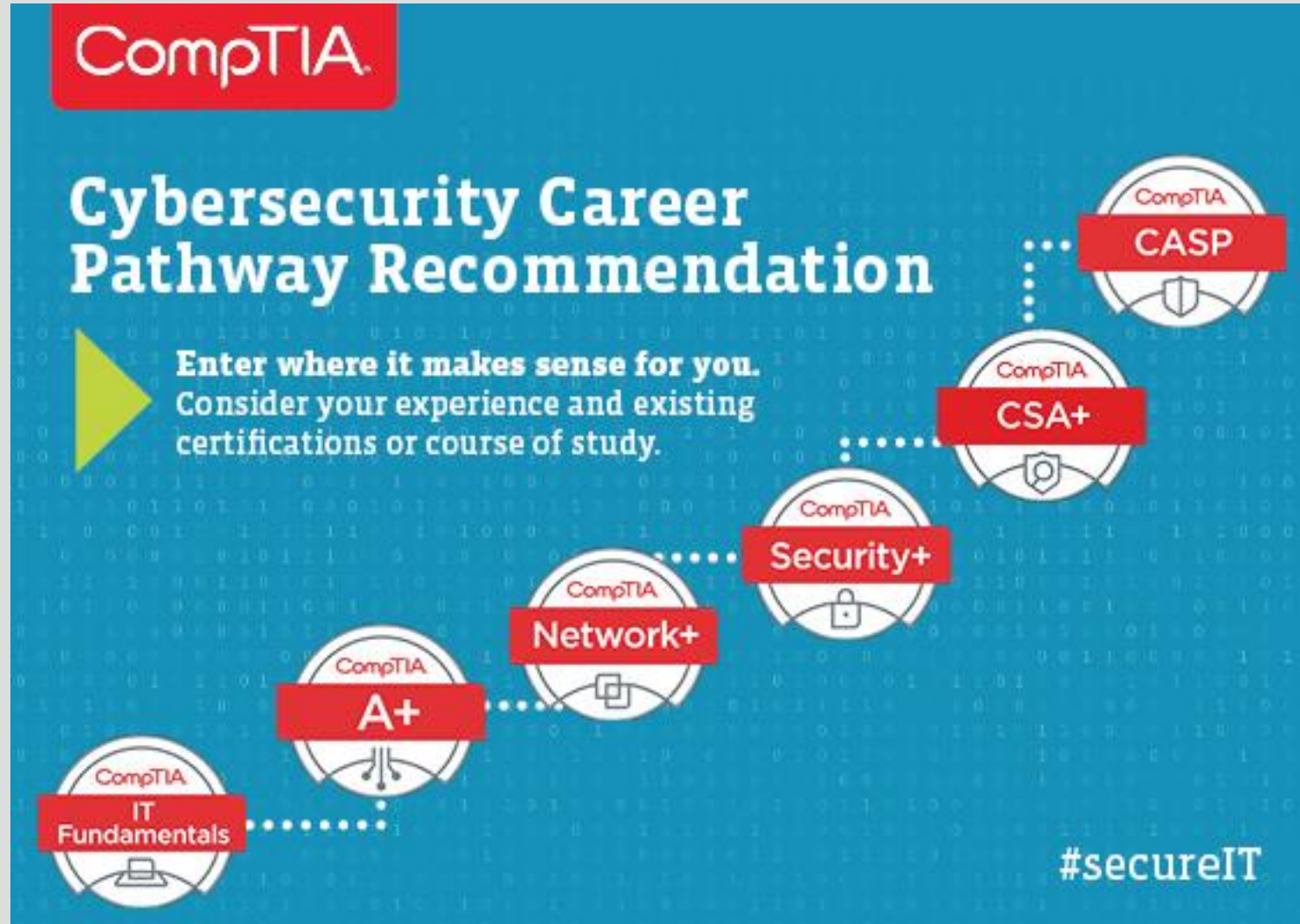
# Developing the Cybersecurity Workforce



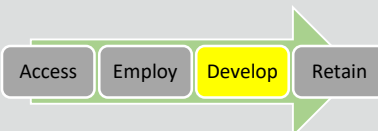
Source, fair use: <http://www.naturethruphotos.com>



# Developing the Cybersecurity Workforce

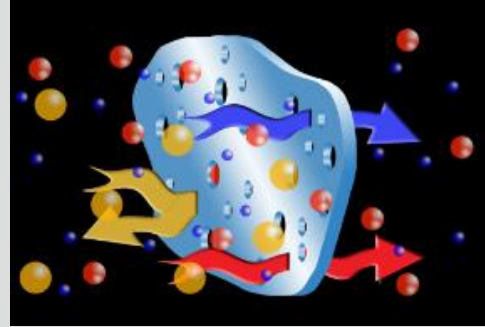


Source, fair use: <https://certification.comptia.org>





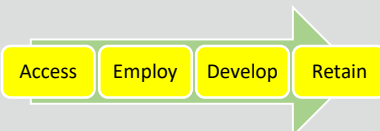
# Retention



# Most Importantly...



Source: [https://www.123rf.com/profile\\_garagestock](https://www.123rf.com/profile_garagestock)





# SOARTECH

Modeling human reasoning.  
Enhancing human performance.

[fernando.maymi@soartech.com](mailto:fernando.maymi@soartech.com)