Teaming with the AI Cyber Warrior

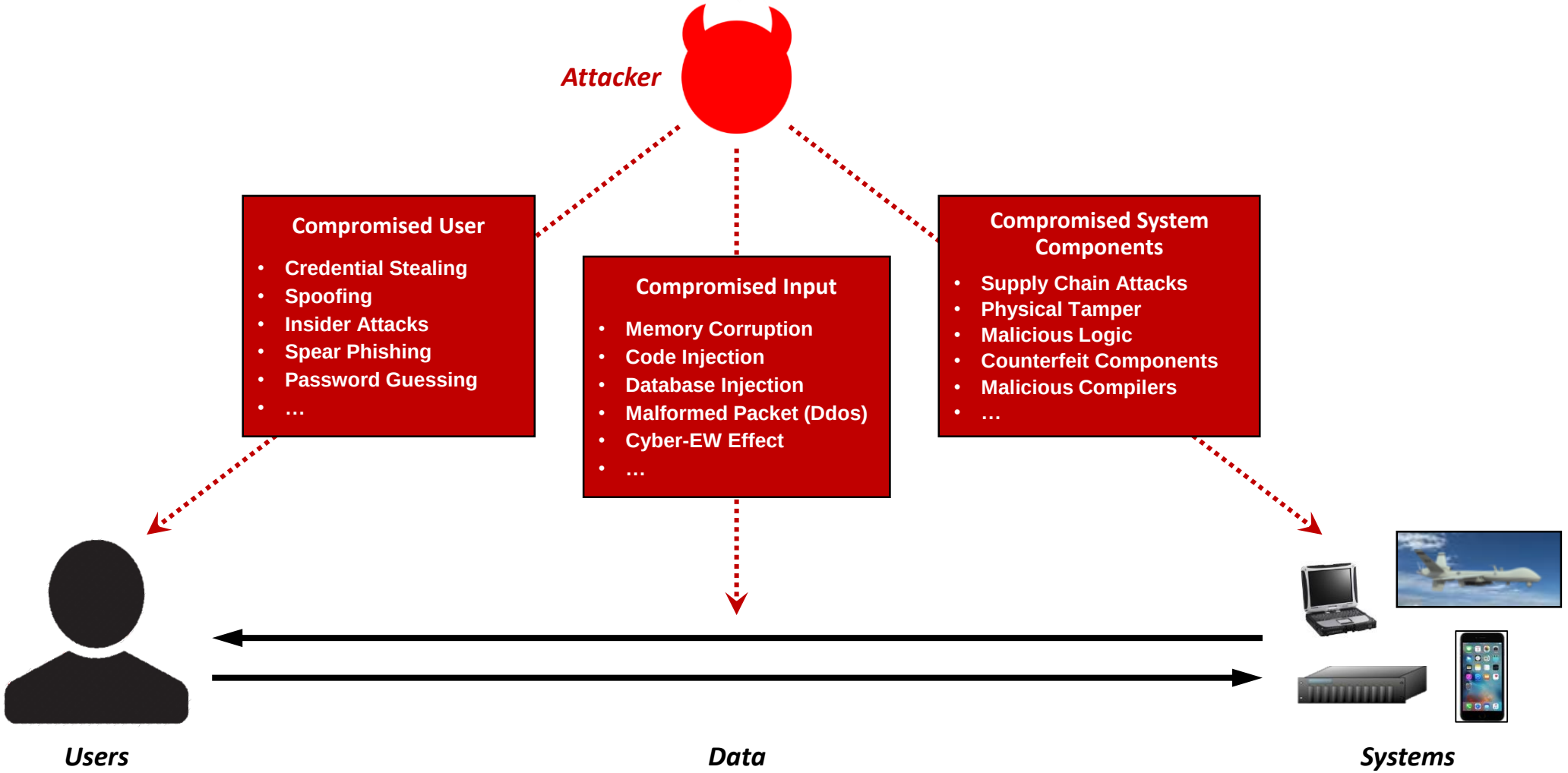
This material is based upon work supported by the Assistant Secretary of Defense for Research and Engineering under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Assistant Secretary of Defense for Research and Engineering.

Dr. William Streilein

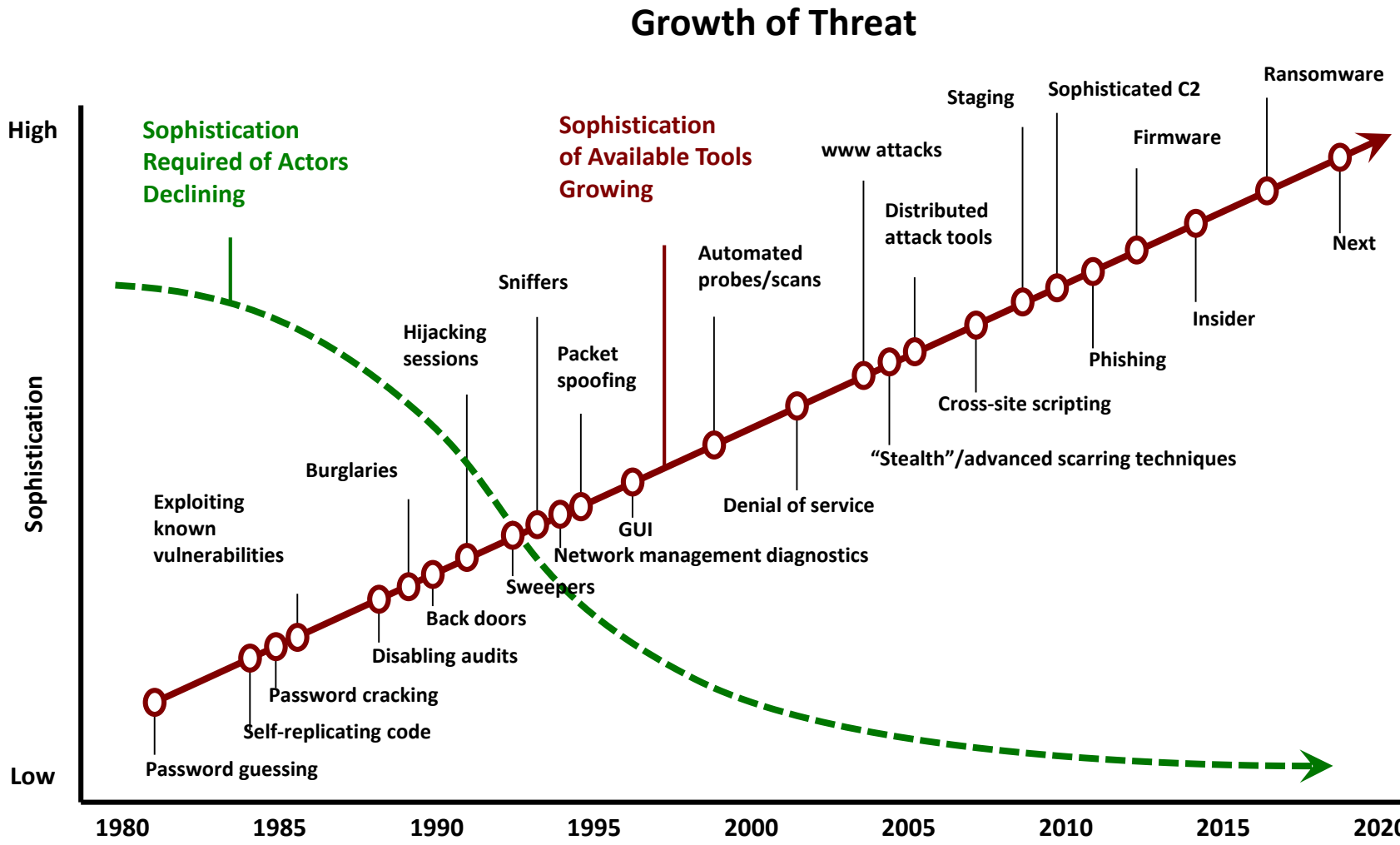
MIT Lincoln Laboratory

5 March 2018

Cyber Security: Critical Threat Surfaces



Sophisticated Attacks More Easily Accomplished with Automation



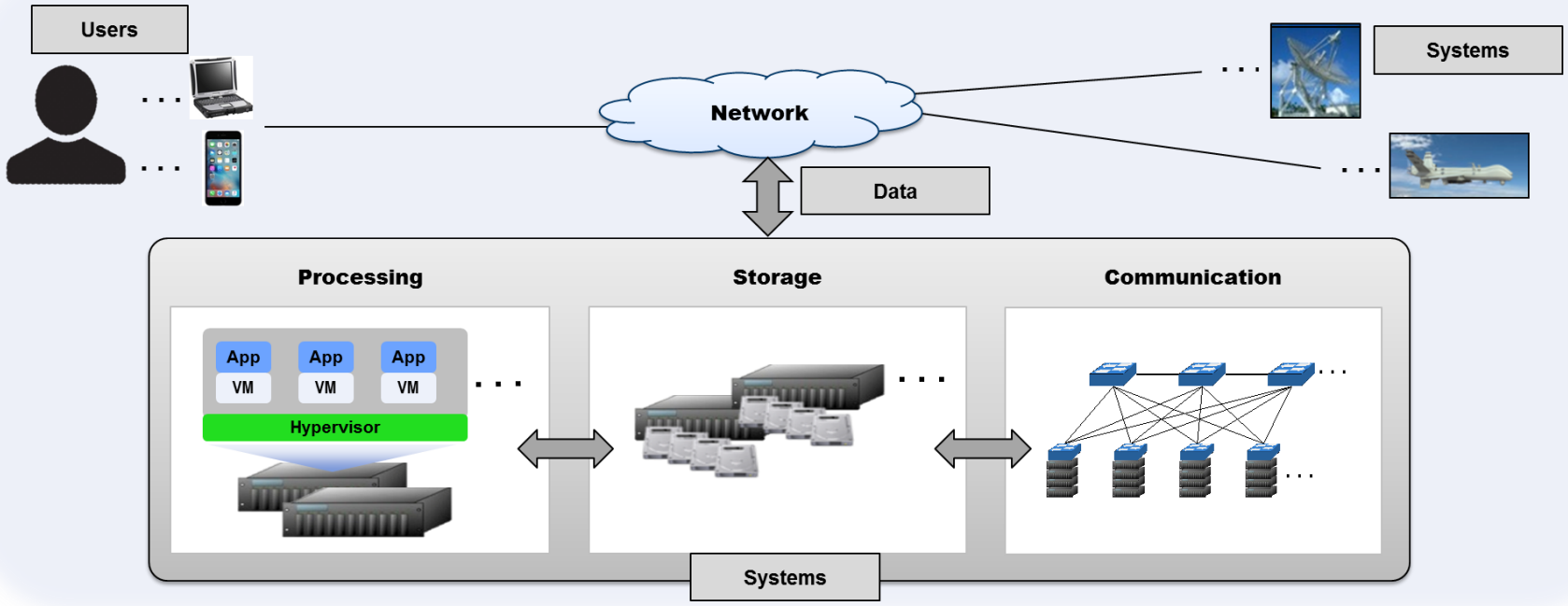
NOTEWORTHY FACTS

- 250K new malware programs are registered each day
- There were 357M new email malware variants in 2016 – 36% more new variants than in 2014.
- There were 463M new variants of ransomware in 2016 – 36% more new variants than in 2015.
- 99 days to detect compromise – adversary gains access in 3
- Internet of Things and Cloud are hot targets (e.g., Mirai botnet) – 2 min to compromise
- Projected cyber-attack costs in 2019: $2.1T

Sources: https://www.symantec.com/security-center/threat-report
http://expandedramblings.com/index.php/cybersecurity-statistics/
http://www.nato.int/docu/Review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/index.htm
https://www.fireeye.com/blog/threat-research/2017/03/m-trends-2017.htm
https://www.ag-test.org/en/statistics/malware

The Cyber Battleground

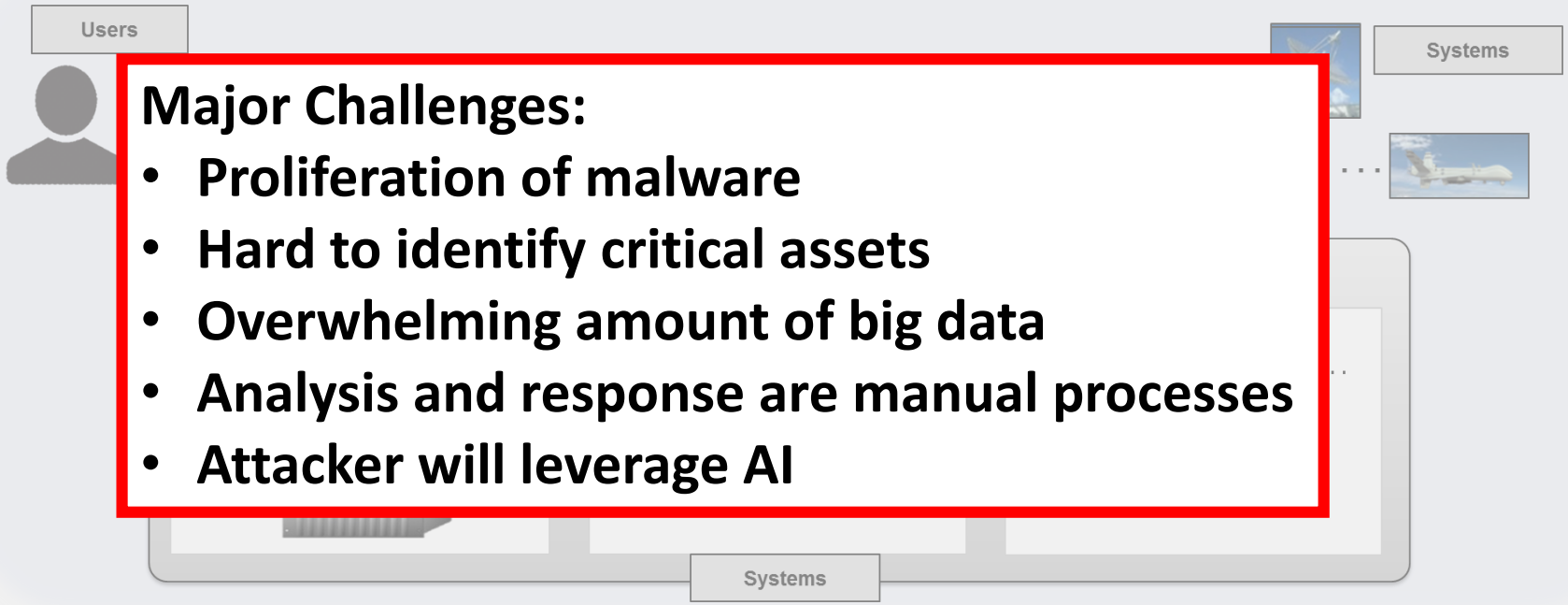
Offense Stages	Prepare (Recon)	Engage	Maintain Presence	Achieve Effect and Assess Damage
Impact	Know the target	Enable attack process	Support persistence	Attack effectiveness



Defense Stages	Identify (Recon)	Protect	Detect	Respond	Recover
Impact	Focused defense	Deflect attacks	ID new attacks	Stop attacks	"Mission" fight through

The Cyber Battleground

Offense Stages	Prepare (Recon)	Engage	Maintain Presence	Achieve Effect & Assess Damage
Impact	Know the target	Enable attack process	Support persistence	Attack effectiveness



Major Challenges:

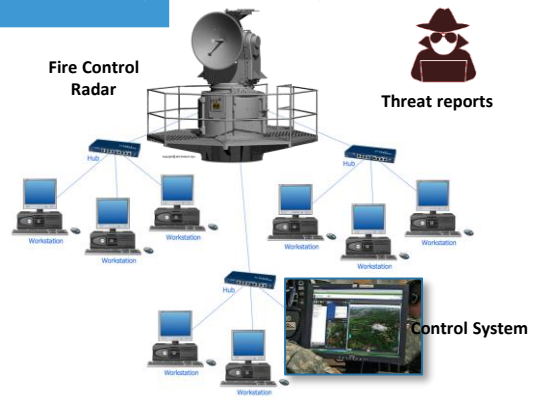
- **Proliferation of malware**
- **Hard to identify critical assets**
- **Overwhelming amount of big data**
- **Analysis and response are manual processes**
- **Attacker will leverage AI**

Defense Stages	Identify (Recon)	Protect	Detect	Respond	Recover
Impact	Focused defense	Deflect attacks	ID new attacks	Stop attacks	"Mission" fight through

Cyber Machine Intelligent Assistant (CyMIA)

How should I protect my mission-critical networks?

Natural language-based interaction interprets user queries

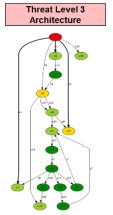


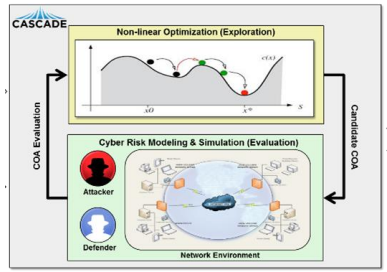
Automatically extract mission, network, and threat information

Fuse information into knowledge base, infer relationships

CyMIA Response

You should segment and isolate your C2 network coupled with the fire-control radar



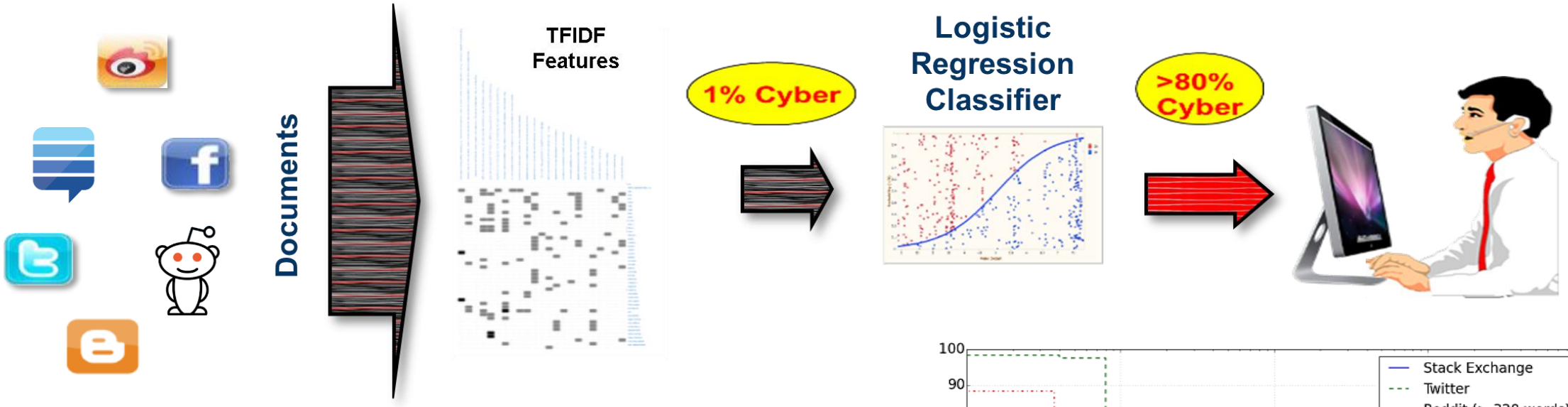


Choose CoA based on threat, knowledge base, and scenario

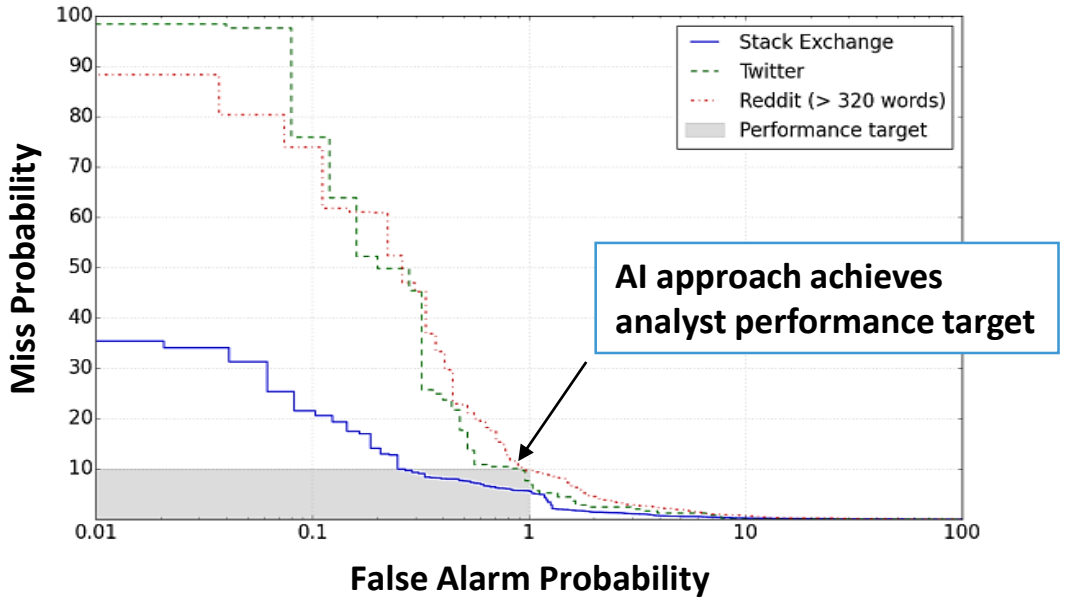
CyMIA processes natural language input in the context of cyber threats and network knowledge to respond with appropriate CoAs (Courses of Action)

Note: CASCADE is an existing Line funded effort

CHARIOT: Leverage HLT to Improve SNR for Cyber Analysts

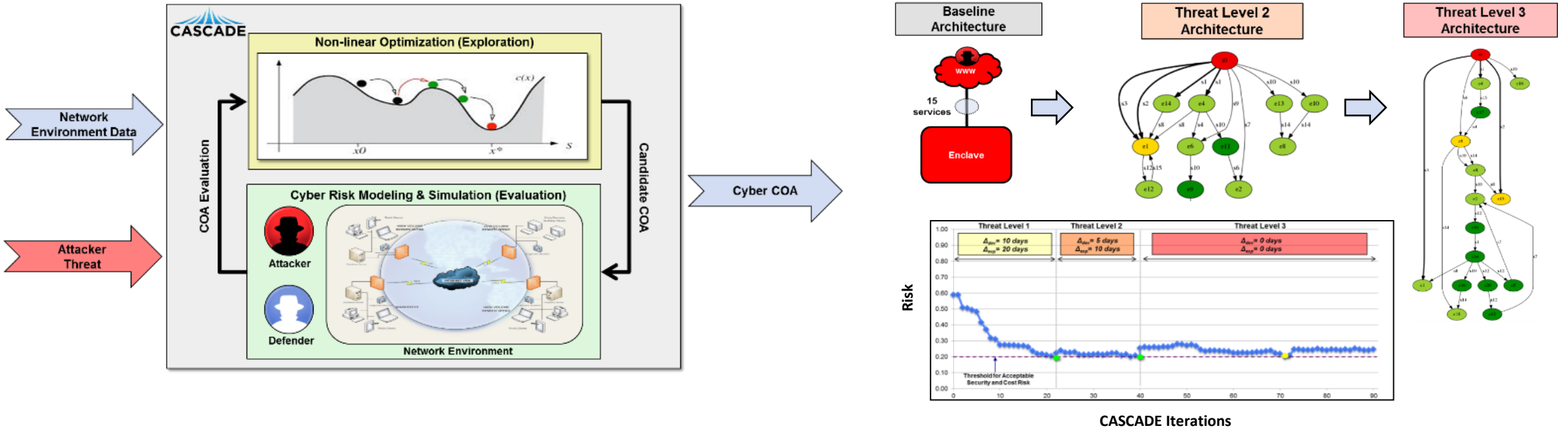


- **Source-dependent extraction/processing**
- **Feature generation**
  - **Word stemming (hack, hacker, hacks, hacking)**
  - **Term Frequency Inverse Document Frequency (TFIDF)**
- **Logistic regression classifier**



Automated Cyber Decision Making via Mod/Sim and Game Theory

- **CASCADE – Cyber Adversarial SCenario modeling and Automated Decision Engine**
  - **Dynamically quantifies risk in the face of an adaptive adversary**
  - **Considers mission context to selection optimal course of action (COA)**
  - **Prototype applied to configuration of network segmentation defense**



Cyber AI-Related Workshops and Symposiums

Artificial Intelligence for Cyber Security Workshop

- **Forum for AI researchers and practitioners to share research and experiences in applying AI to Cyber Security**

Chairs

Bill Streilein

Dave Martinez

Neal Wagner

New Orleans, Louisiana • February 2, 2018

Theme: Applications of AI to Internet of Things

Keynotes

Sal Stolfo
Professor of Computer Science
Dept. of Computer Science,
Columbia University

Trung Tran
Laboratory of Physical Sciences,
University of Maryland,
Baltimore County

Graph Exploitation Symposium

- **Brings together leading experts from universities, industry, and government to explore the state of the art and define a future roadmap in network science**

Dedham, Massachusetts • April 23–25, 2018

Technical Co-Chairs

Rajmonda Caceres

Ben Miller

Chairs

Bill Streilein

Sanjeev Mohindra

POC: Ben Miller, bamiller@ll.mit.edu

Areas of Continued and Future Research

- Robust detection capabilities to discover plans for new attacks in structured and unstructured data sources
- Automated methods to discover dependence of mission function on cyber systems (e.g., “mission mapping”)
- Graphical analysis methods to infer relationships and relevance to mission network
- Automated methods to develop simulation models from unstructured and structured data
- Techniques to quantify security risk from newly discovered cyber threats