Predictive Analytics, Watson, and Cybersecurity: Beyond *Jeopardy!*

MARK GREAVES

PACIFIC NORTHWEST NATIONAL LABORATORY

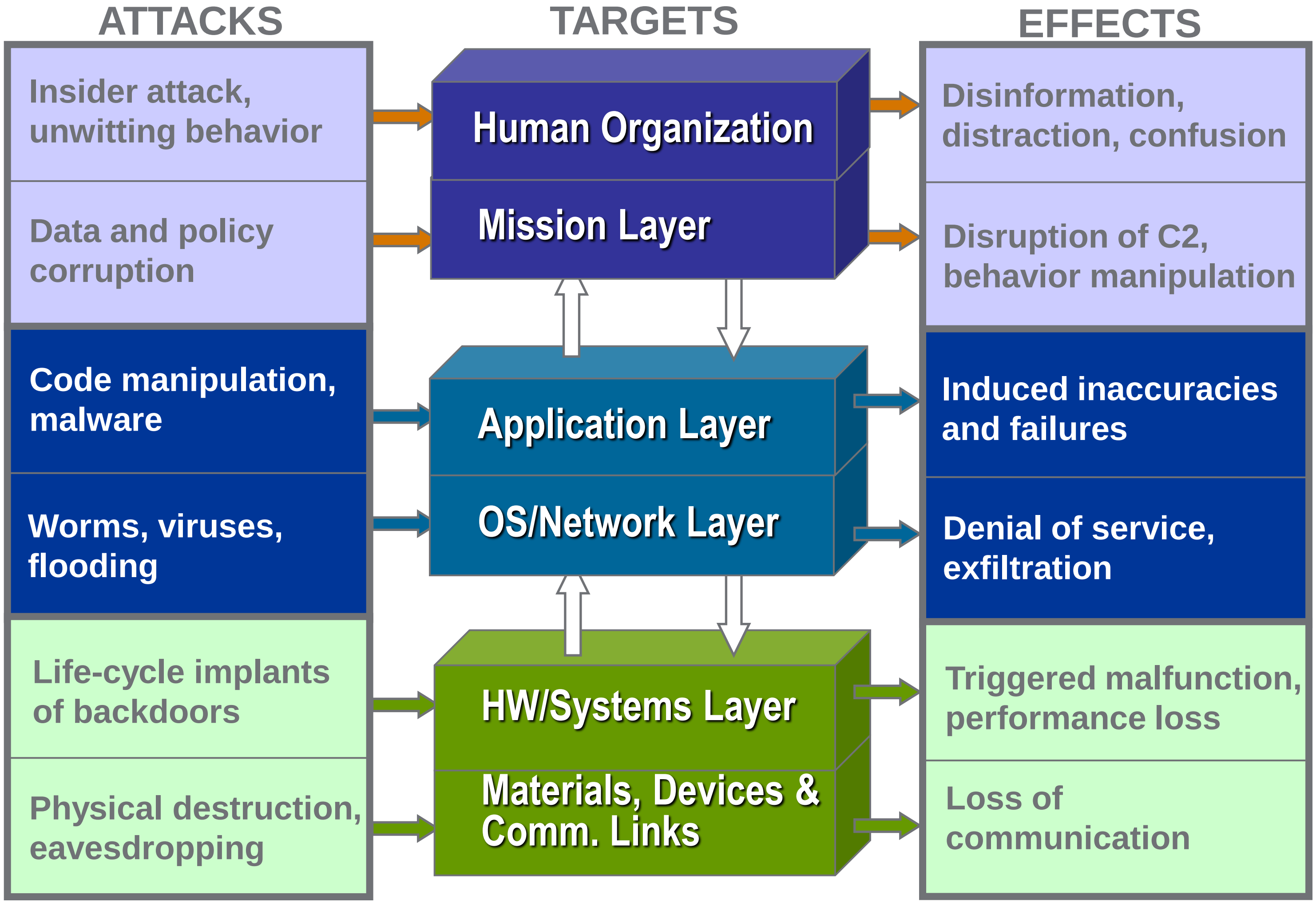
Cybersecurity Ideal: A Strong Deterrence

- **Ultimate prevention depends upon an ability to deter the attacker**

Deterrence: The attempt to prevent or forestall undesired activity through influencing an attacker's or potential attacker's perception of the gain-loss balance

- **Relies upon prevention, detection, response, and recovery**
- **Both policy and technology based**
  - Willingness to respond in a meaningful, targeted way
  - Must have a range of responses built and ready to use
  - Must be able to deploy with pinpoint accuracy
- **Goals**
  - Reduce likelihood of success
  - Increase the attacker's "cost"

Elements of a Contested Cyber Environment[1]

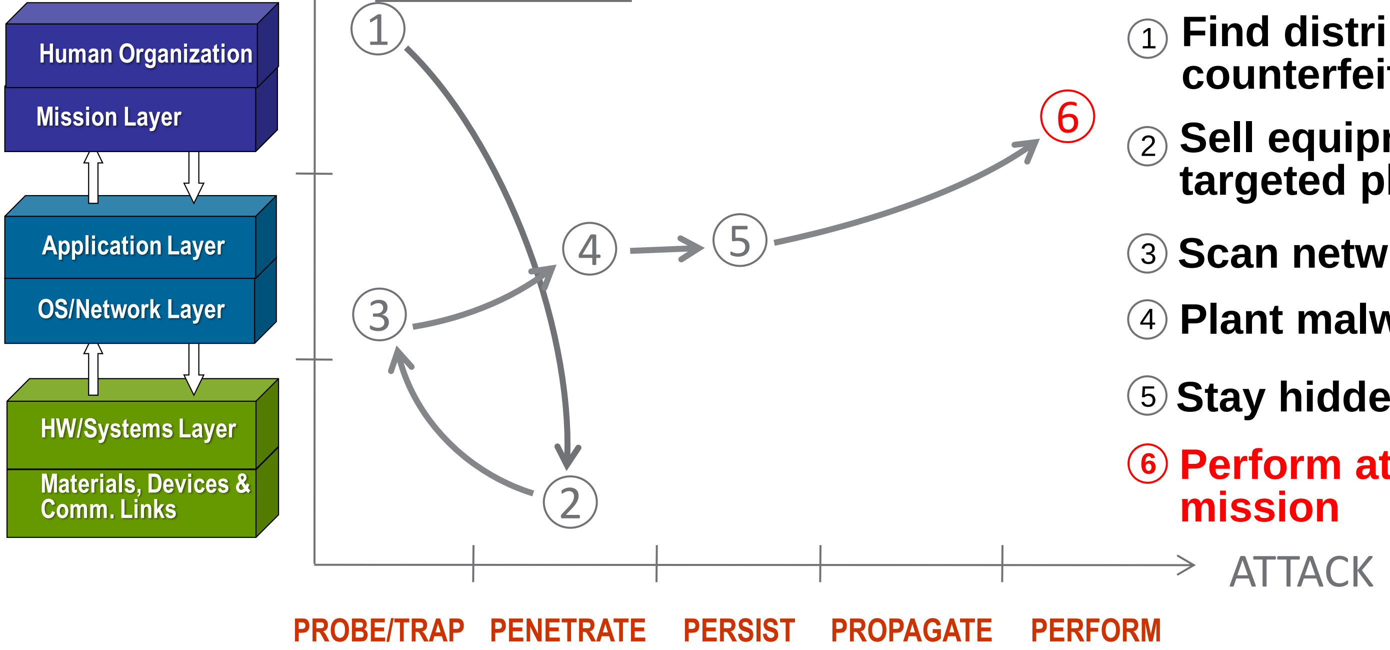


ATTACKS
TARGETS
EFFECTS
Insider attack, unwitting behavior
Data and policy corruption
Code manipulation, malware
Worms, viruses, flooding
Life-cycle implants of backdoors
Physical destruction, eavesdropping
Human Organization
Mission Layer
Application Layer
OS/Network Layer
HW/Systems Layer
Materials, Devices & Comm. Links
Disinformation, distraction, confusion
Disruption of C2, behavior manipulation
Induced inaccuracies and failures
Denial of service, exfiltration
Triggered malfunction, performance loss
Loss of communication

[1] 2008 AFSAB report “Defending and Operating in a Contested Cyber Domain”

Example of Attack Trajectories[2]

Counterfeit CISCO 1721 Router
1/5 of cost of original
2002-2007
FBI Report, January 2008



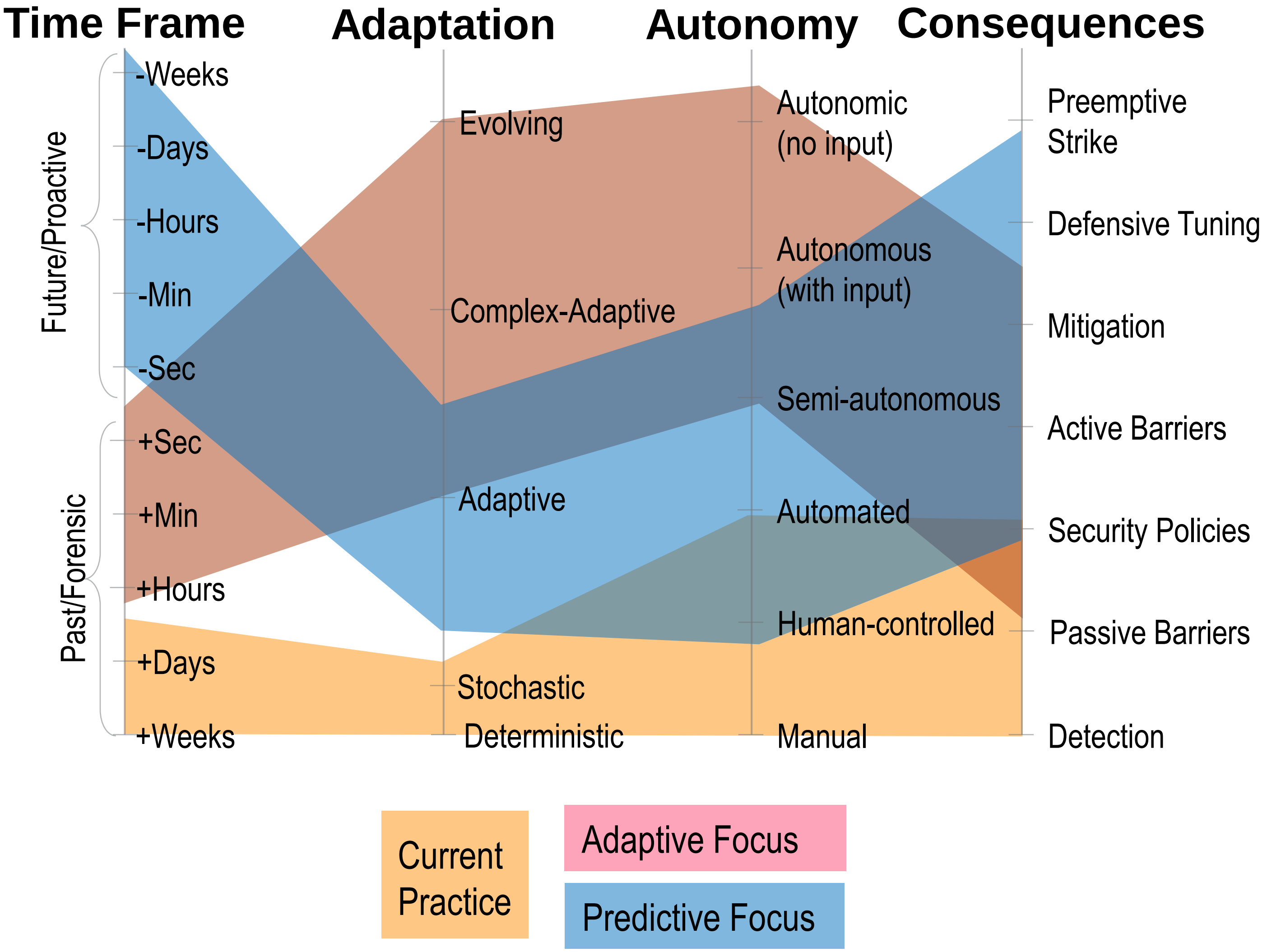
1. Find distributors for counterfeit equipment
2. Sell equipment to targeted place
3. Scan network
4. Plant malware
5. Stay hidden
6. Perform attack on mission

Attack trajectories are dynamic:

- Depend on target and choose the least resistance
- May leave out layers (such as network layer)
- May change dynamically by reacting to defensive actions

[2] 2008 AFSAB report “Defending and Operating in a Contested Cyber Domain”

Defining Terms: Adaptive and Predictive



Predictive Analytics in Cybersecurity

- **Role of Predictive Analytics**
  - Set and modify defensive configurations based on a threat model or simulation
  - Guide system owners on preemption and deterrence posture
  - Quantify the impact of different system tradeoffs

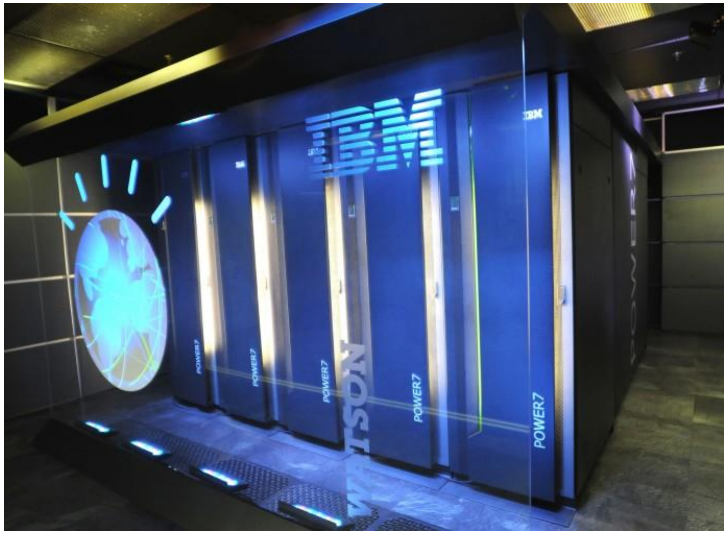
- **Issues in building Models and Classifiers**
  - Target system modeling
    - Massive data scale, heterogeneity, and streaming issues
    - Knowledge acquisition in dynamic environments
    - Situation awareness barriers (sensor placement, encryption, noise/deception)
    - Abstraction to appropriate system metrics
  - Human organization modeling
    - Attacker’s camouflage, C2/OODA loop
    - Target organization’s vulnerabilities
  - Modeling of hardware, materials, devices, communication links
  - Acquiring training data
    - Modeling normalcy vs. modeling attack behavior

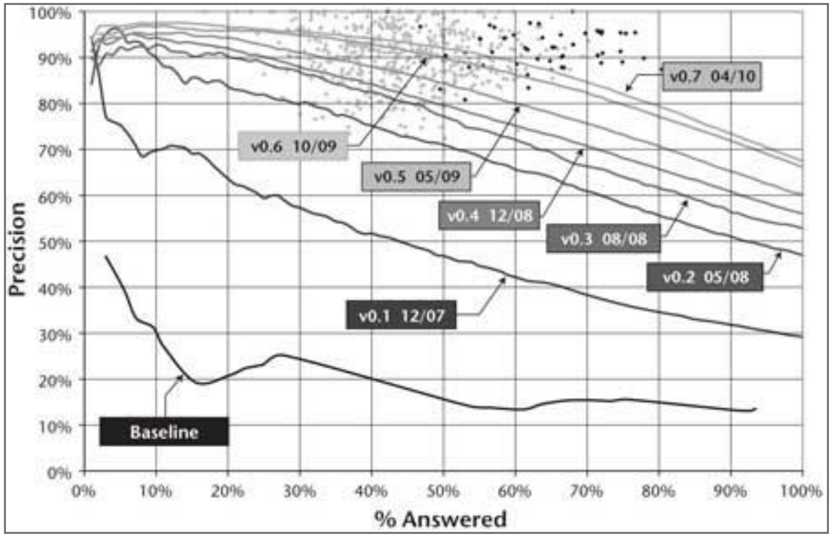
Resilient Cyber Systems

- **Today's Cybersecurity Reality**
  - Software complexity guarantees vulnerabilities
  - Unknown network, system, and human-system configurations
  - Attacker advantages in time, location, and target
  - Low cost of entry and limited ability to identify the perpetrator
- **Given sufficient time and resources, any perimeter and system can be breached**
- **Resilient Systems for Cyber Defense:** PNNL's ARC initiative
  - Modeling problem is hard, but not as hard as pure prediction
  - Still require many of the same kinds of models
    - System models: configurations, connections, normal/abnormal use
    - Attack models: attack vectors, vulnerabilities, targets, attack goals
    - Resilience models: resilience resources, task importance, possible workflows
  - Not a solution for privacy and data exfiltration

We still need effective predictive models and classifiers

Watson for *Jeopardy*: Key Features





- **IBM Jeopardy Power7 cluster**
  - 2880 POWER7 cores at 3.5 GHz
  - 16 Terabytes of memory
  - 80 Teraflops, #94 on Top500
  - ~$3 million
  - Run DeepQA in <3 sec
- ***IBM Journal of R&D*, May 2012**
- ***Jeopardy's* central graph**
  - Metric: be in the winner's cloud
  - Multiple DeepQA systems at different levels of performance
  - Constant testing
    - ~40K official *Jeopardy* QA pairs
    - New QA pairs easy to create
    - Decomposable metric
    - Factoid answers

Lessons From Watson

IBM WATSON

- **Recognition that *Jeopardy* could be modeled**
  - An empirically-grounded model of 100s candidate Q-A pair types
  - A learned model of the ability of each solver to accurately answer a question type
  - A complete model of the Jeopardy rules, objectives, and buzzer management
  - An large but incomplete model of needed domain knowledge
  - Needed knowledge is static and mostly available

- **Key Watson Innovations**
  - Software Engineering : high-speed iteration and competition through a complex parameter space vs. “the BOGSAT design method”
  - Question-Answering Architecture: Build a haystack, then find the needle vs. “1-5 carefully designed algorithms to rule them all”
    - Not classical forward-chaining or backward-chaining
  - Embrace Data Heterogeneity: Language-based interlingua vs. fixed database schema or pre-built formal ontology

Responding to Watson in Cyber Analytics

- **Software Engineering**
  - Adequate system simulations to test/iterate on, including system/context dynamism
  - Tractable system metrics (parallel to the winner’s cloud)
  - Appropriate and redundant system sensors and attack/failure/degradation detectors

- **Security Analytics Architecture**
  - Overgenerate security hypotheses, filter, rank, and check
  - Decompose attack signatures into detectable atomic components, recompose detections into threats
  - Uncertainty management and ranking

- **Embrace Data Heterogeneity**
  - Base of models and data sources is “all of the above”
  - Can the language of cybersecurity work as a non-brittle KR in this application?

Beyond Jeopardy: Watson for Cyber?

- **Use Predictive Analytics to enhance resilience, rather than fight the attack as it happens**

- **Cybersecurity Analytics with a Watson Architecture**
  - Situation awareness and system metrics from streaming data
  - Decompose security analytics to independently-solvable components
    - Multiple independent solvers that can each contribute “factoid” system hypotheses
    - Standing task-based resilience queries that can combine solver outputs
  - Maintain multiple active threat/failure hypotheses and likelihoods
  - Parallelism for speed of response

- **Challenges**
  - Creating and maintain the necessary models using streaming data
  - Uncertainty management and scenario ranking
  - Creating and building 100s of “solvers” that together build the haystack
  - Tractable account of resiliency, system tasking, and degradation

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

Thank You