BBN Systems: Adversary Modeling to Develop Forensic Observables

By

John Lowry, Rico Valdez, Brad Wood

Presented At

The Digital Forensic Research Conference

DFRWS 2004 USA Baltimore, MD (Aug 11th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Adversary Modeling to Develop Forensic Observables

John Lowry
jlowry@bbn.com

Digital Forensic Research Workshop
August 2004

BBN TECHNOLOGIES

BBN TECHNOLOGIES

Background

- Let me introduce myself …
  - I am not a forensics practitioner - or expert !
  - 30 years in CNA/CNE/CND
- The current set of CND TTPs are not sufficient to defend the United States or its interests
- My current research focus is on I&W, AS&W, and adaptation of the laws of war to the asymmetries of cyber conflict.

BBN TECHNOLOGIES

Motivation

- Adversaries may not be what you think
  - They are not omnipotent
  - They live in constrained spaces too …
  - They are "sneaky and lazy" - well, they're sneaky anyway …
  - Being an adversary is *extremely hard work !*
- It would be nice for US defenders to *win* once in a while
- We need new ways of identifying and classifying adversaries, adversary missions
- My goal is to provide some thoughts from outside the field of forensics in the hope that something might be helpful.

BBN TECHNOLOGIES

A Theory of Observables

- This is a *general* theory applicable to many domains, not just CNA/CNE/CND
- *There* are two primary components
  - *A posteriori* development
    - Characterized by *event* ⇢ *analysis* ⇢ *observable*
  - *A priori* development
    - Characterized by *threat* ⇢ *analysis* ⇢ *observable*
- *A priori* development is frequently the missing component – and the only one capable of addressing *novel* or *novel variations* of attack.

BBN TECHNOLOGIES

What is an adversary ?

- Named Actor Schema
  - Naïve Novice (hacker)
  - Advanced Novice (hacker)
  - Professional or Dedicated Hacker
  - Disgruntled Employee (insider)
  - Corporate Espionage (Professional Hacker)
  - Organized Crime
  - Hacker Coalition
  - Zealot Organization
  - Cyber Terrorist
  - Nation State actor
  - Foreign Intelligence
- Resource Class Schema
- Class I to IV
  - Motivation – the level of intensity and degree of focus
  - Objectives - boasting rights, disruption, destruction, learn secrets, make money
  - Timeliness - how quickly they work (years, months, days, hours)
  - Resources - well funded to unfunded
  - Risk Tolerance – high (don't care) to low (never want to be caught)
  - Skills and Methods - how sophisticated are the exploits (scripting to hardware lifecycle attacks)
  - Actions - well rehearsed, ad hoc, random, controlled v. uncontrolled
  - Attack Origination Points – outside, inside, single point, diverse points
  - Numbers Involved in Attack - solo, small group, big group
  - Knowledge Source - chat groups, web, oral, insider knowledge, espionage

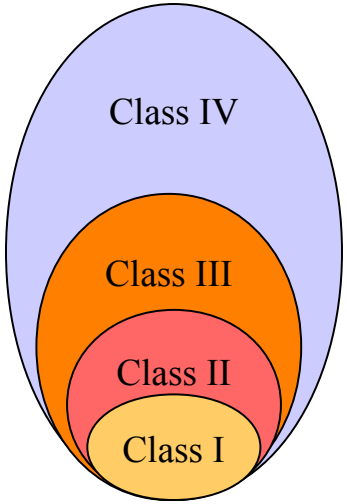
BBN TECHNOLOGIES

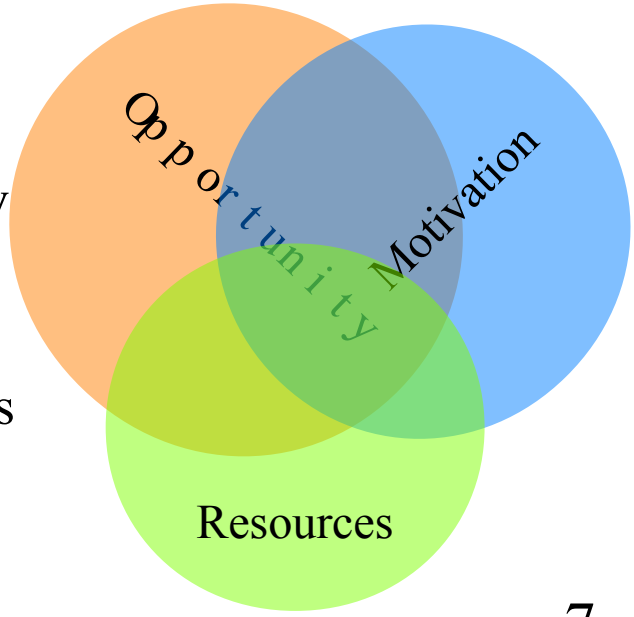
Adversary Modeling

- Adversary modeling is a critical element in *a priori* development of observables
  - *Hypothesize* potential adversaries or malicious acts
  - Identify *threats* and adversarial *missions*
  - Identify the *means* that would *have to be used* or have a *high probability* of being used
  - Develop *observables* for those *means*
- This will give coverage of *novel* attacks or *novel variations* of attacks
  - Degree of coverage remains a significant issue as does metrics for success
- Novel attacks are only those you haven't seen yet
  - You may already be under attack or being exploited
  - This technique will identify attacks not yet launched and those already underway

Adversary Characterization

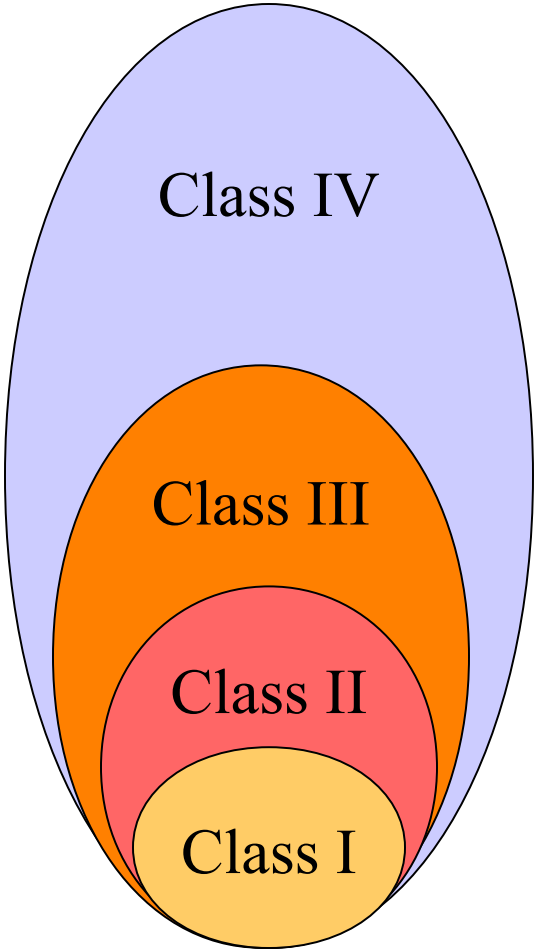
- Named schema
  - Useful for "political" purposes, shorthand.
  - We resonate with "nation state", "terrorist", etc.
  - We do a mapping to known actors:
    - "nation state" = Russia, not Botswana
    - "terrorist" = al Qaeda, not Greenpeace
    - Therefore, we miss potential adversaries
- Class schema
  - Useful for analytical and technical purposes
  - Focuses attention on resources, opportunity, and motivation - capability and intent.
    - Capabilities model
    - Threat model
  - Actors can be "fit" in to class categories as necessary and as circumstances change.





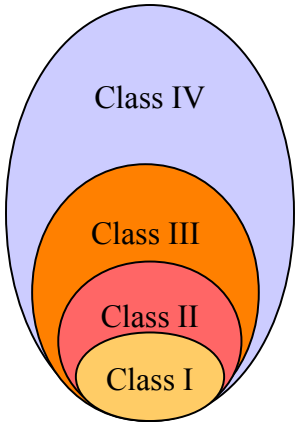
Capabilities Model

- More dangerous adversaries are full supersets of less dangerous adversaries
  - Everything available to a Class III adversary is available to a Class IV adversary - including using the Class III adversary as a proxy.
- The model captures both the breadth of capabilities and the sophistication
  - Area is the breadth
  - Height of the sophistication

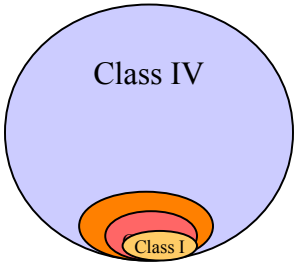


Capabilities Model Applied

- The Capability Model when applied to a particular adversary has abstract value, but
- It has additional value when applied against a potential target
- We're still developing the variables and metrics for these concepts.



Adversary X against the Internet has capabilities of greater breadth and sophistication than …



Adversary X against a system-high protected enclave who not only possess fewer and less sophisticated capabilities in the Class IV space, but has fewer capabilities within the Class I, II, and III space

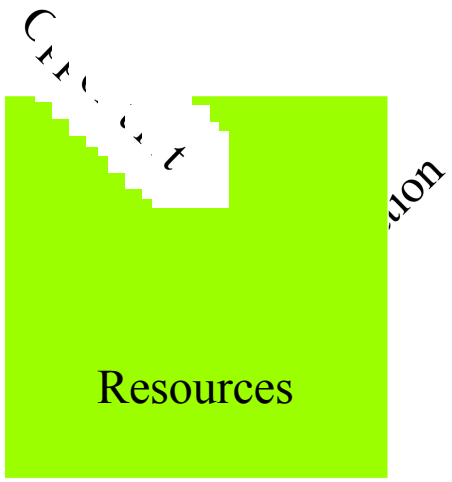
Threat Model

- Threat is composed of three primary components
  (despite the model developed by the IATF, etc.)
  - Resources
    - A relatively slow changing component
    - Money, technology, human capital, infrastructure, organization, etc.
  - Opportunity
    - Must be measured against the vulnerabilities
    - Can change radically within any time window as a step function
    - Consists of varying kinds of potential and current access
    - Can be both created or developed and discovered
  - Motivation
    - Can change dramatically within any time window but at different rates depending on adversary type, context, and outside events.
    - Mission, strategic and tactical interests, political, economic, personal, emotional, etc.
- Work is on-going to identify variables and metrics

Threat Model

- Mapping or estimating resources, motivation, and opportunity is important overall, but
- A critical space for focused effort is the intersections.
- Next step is to move beyond these conceptual models into concrete definitions and categorizations.

Class I adversary against Internet



Class III military "coalition partner" against SIPRNET

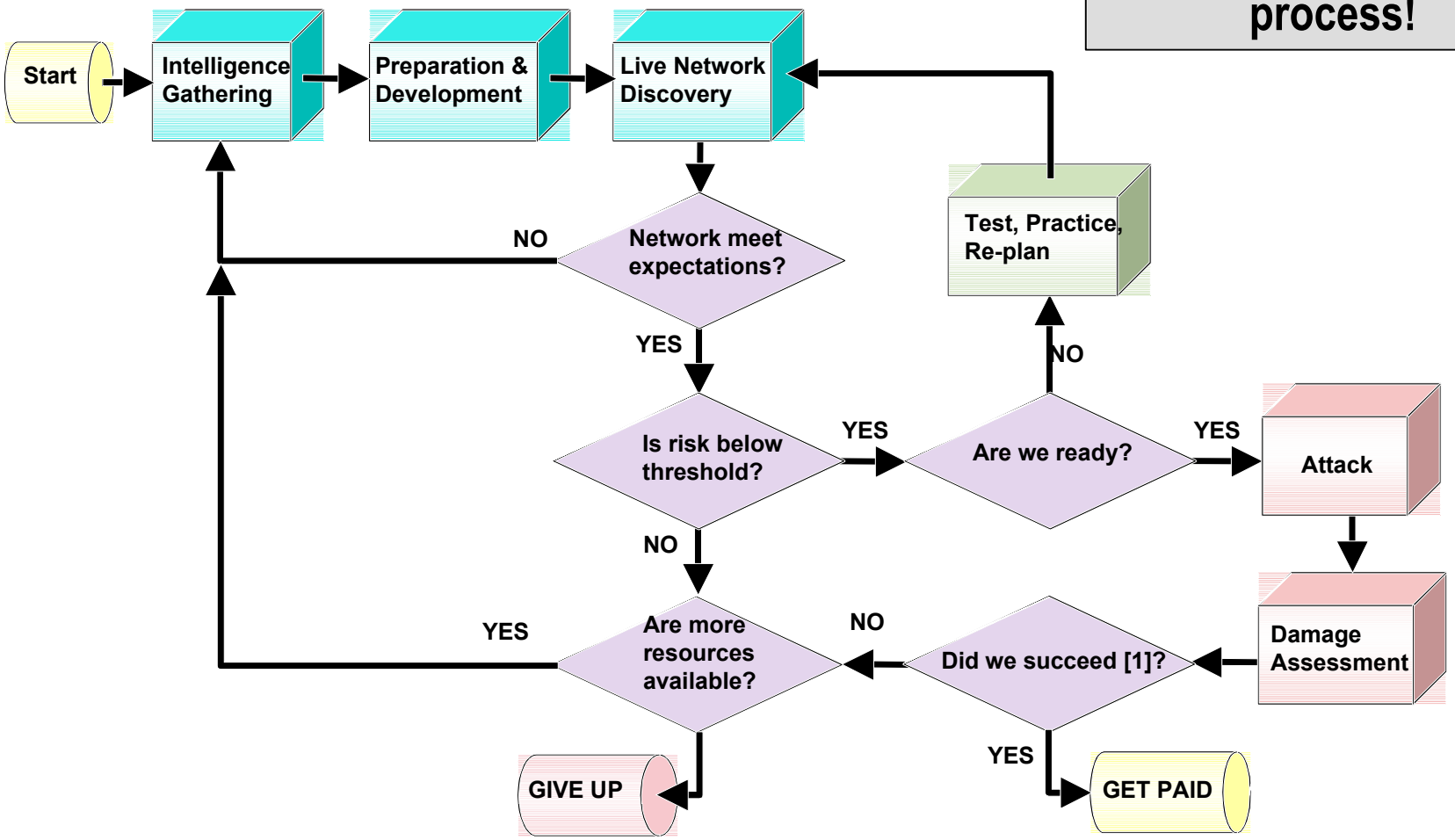
BBN TECHNOLOGIES

Some definitions

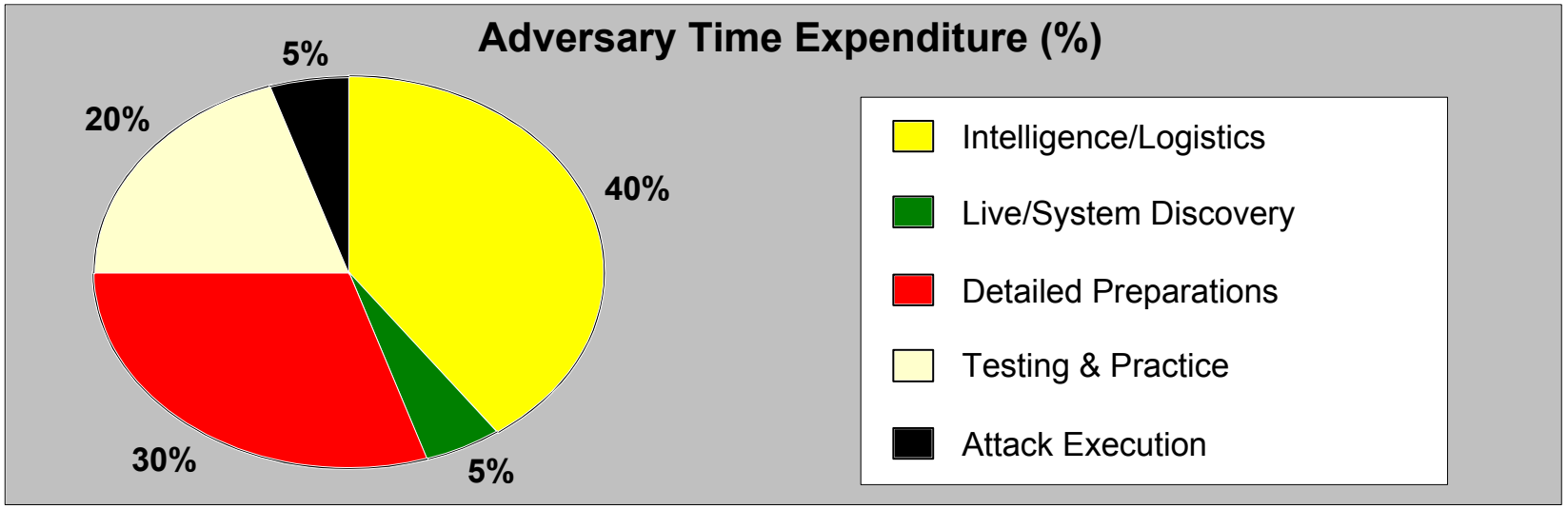
- Cyber Adversary - a person or group who intends to or attempts to use *your* systems to achieve his/her goals.
  - This is a little different from other kinds of adversary, e.g., kinetic, economic, etc.
- Exploit - one or more technical means designed to defeat confidentiality, integrity, availability, access controls, etc., at an *atomic* level.
- Attack - a sequence of one or more exploits used to achieve a tactical advantage or mission element.
- Campaign - a sequence of one or more attacks used to achieve a strategic objective

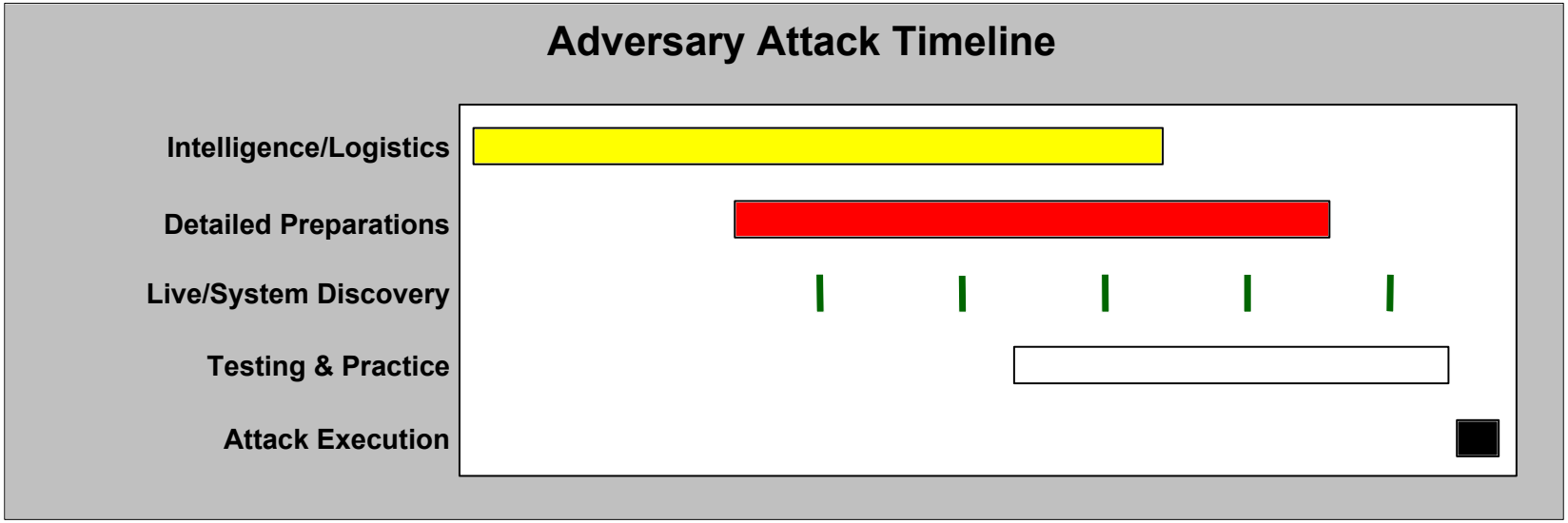
Example adversary process model

Adversaries follow a process!

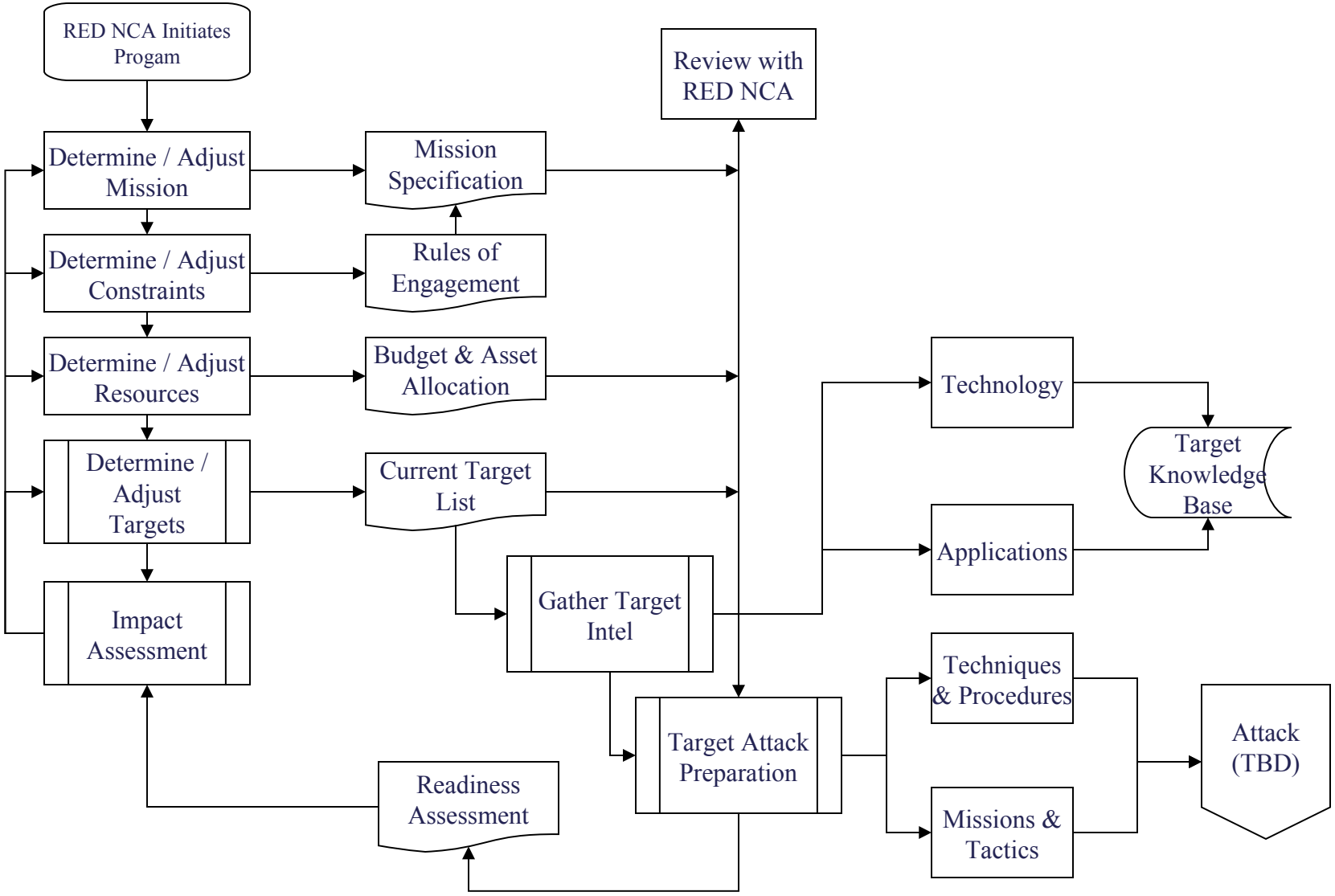


Example adversary resource expenditures



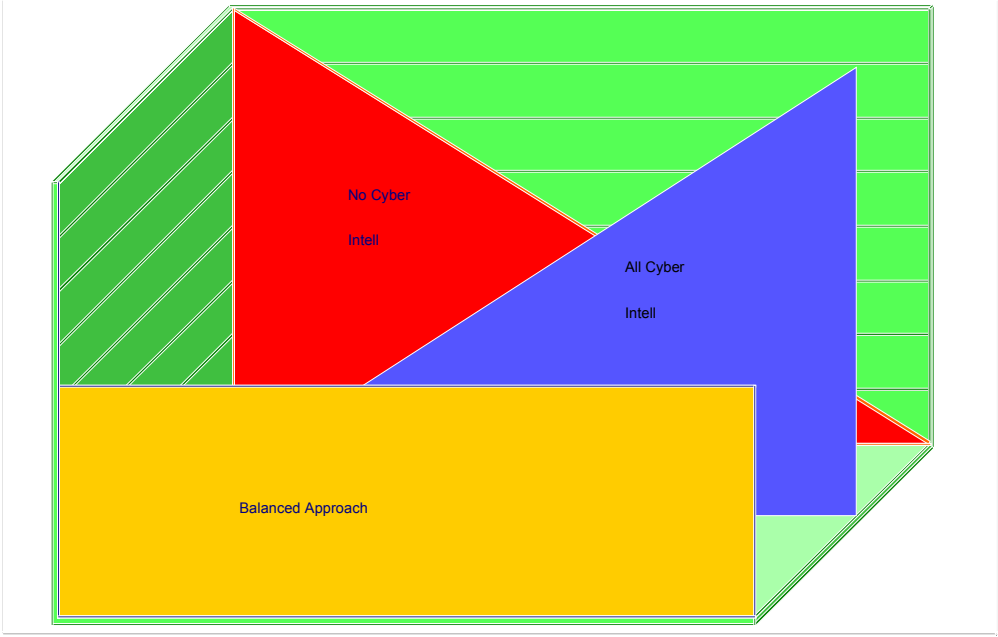


Class IV Adversary Process Model



"Law" of Conservation of Observables

- We are just beginning to examine the mix of just what observables are necessary or likely during IPB.
  - Good news / Bad news
    - We believe that most, if not all, adversaries will have to use a mix of cyber and non-cyber intelligence techniques for IPB.
    - However, a very sophisticated, resourced, motivated (and lucky ?) adversary *might* be able to use no cyber intelligence gathering techniques to do IPB.



BBN TECHNOLOGIES

PACCERT Example

- Challenge: Improve detection of probes and scans
  - Why ? "So we can see who poses an increased threat."
  - Problem: Detecting probes and scans addresses the issue obliquely and insufficiently
- Approach: Examine the challenge directly
  - Under what conditions does an increased threat exist ?
- Answer: When an adversary has sufficient information to attack some or all of your computer networks.
- New challenge: Identify and classify who has gained sufficient information to pose a threat to some or all of your computer networks.

PACCERT Example (cont.)

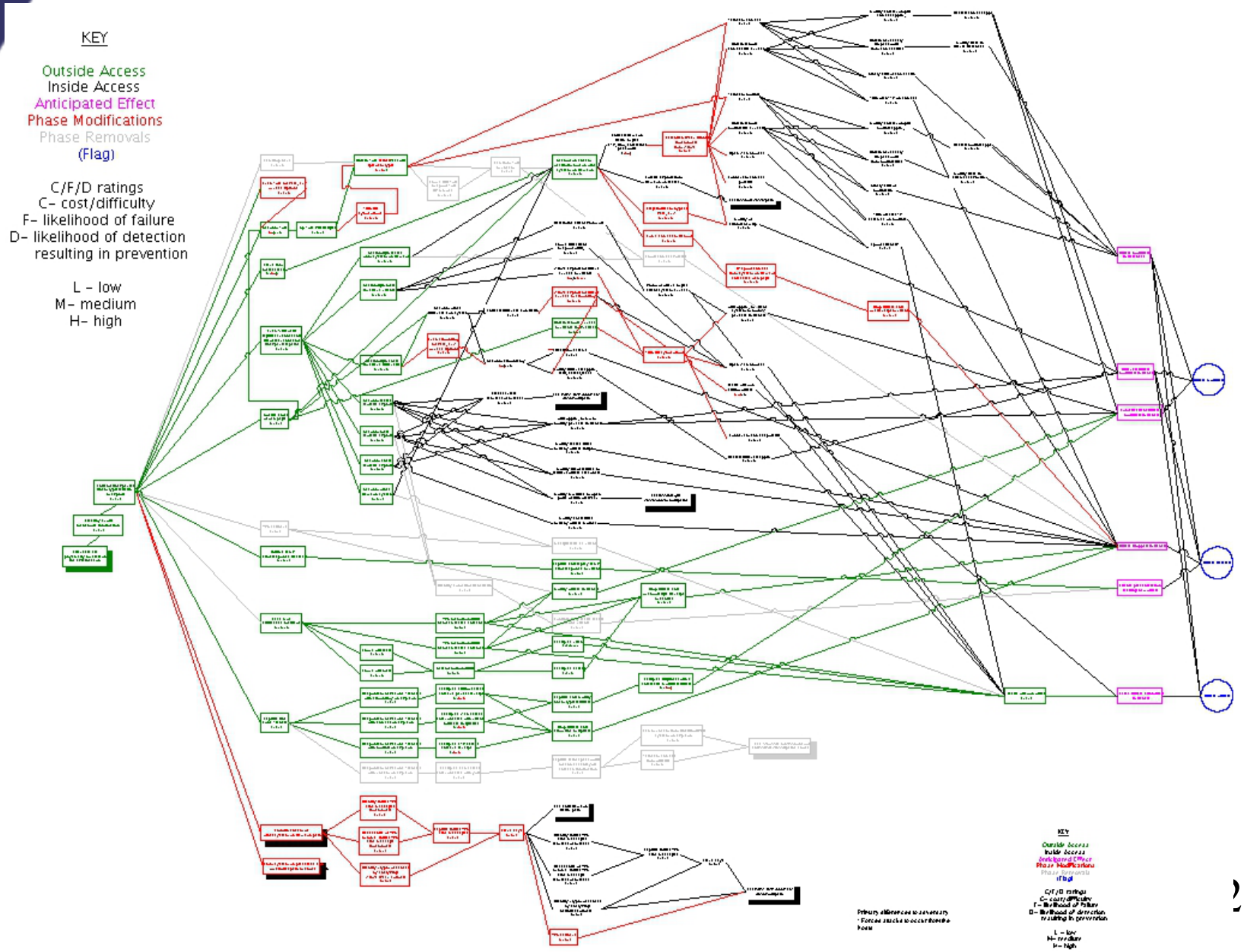
- Who has information about my network ?
  - Everyone using it, BUT, unevenly distributed.
- Hypothesis
  - Information gathering is different from normal usage of the network. Normal users do gain information but not as their primary purpose.
- Analysis
  - Normal usage exhibits low information gain and unpredictable behavior
  - Information gathering exhibits high information gain and predictable behavior
- Observables
  - *Distance from uniformity:* how predictable is the behavior of a source entity no matter where it goes ?
  - *Independence:* how predictable is the destination of any source entity ?

PACCERT Example (cont.)

- Results
  - An ordered list of source entities by *distance from uniformity* and *independence.*
    - Those at the top were deemed "most worthy of investigation"
  - Identification of a *novel variation of attack*
    - The fifth "most worthy of investigation" was an instance of the Lion worm.
    - Investigation of CERT alerts showed that the Lion worm alert was first issued *two weeks after* the dataset used was recorded.
  - Identification of other instances of Lion using basic clustering techniques
    - As a deterministic automaton, the Lion worm exhibits close to identical behavior for the observables
- Feature: No intrusive inspection of network traffic (i.e., payload)
  - Use of source IP, destination IP, and destination port numbers was sufficient.

BBN TECHNOLOGIES

Attack Graph



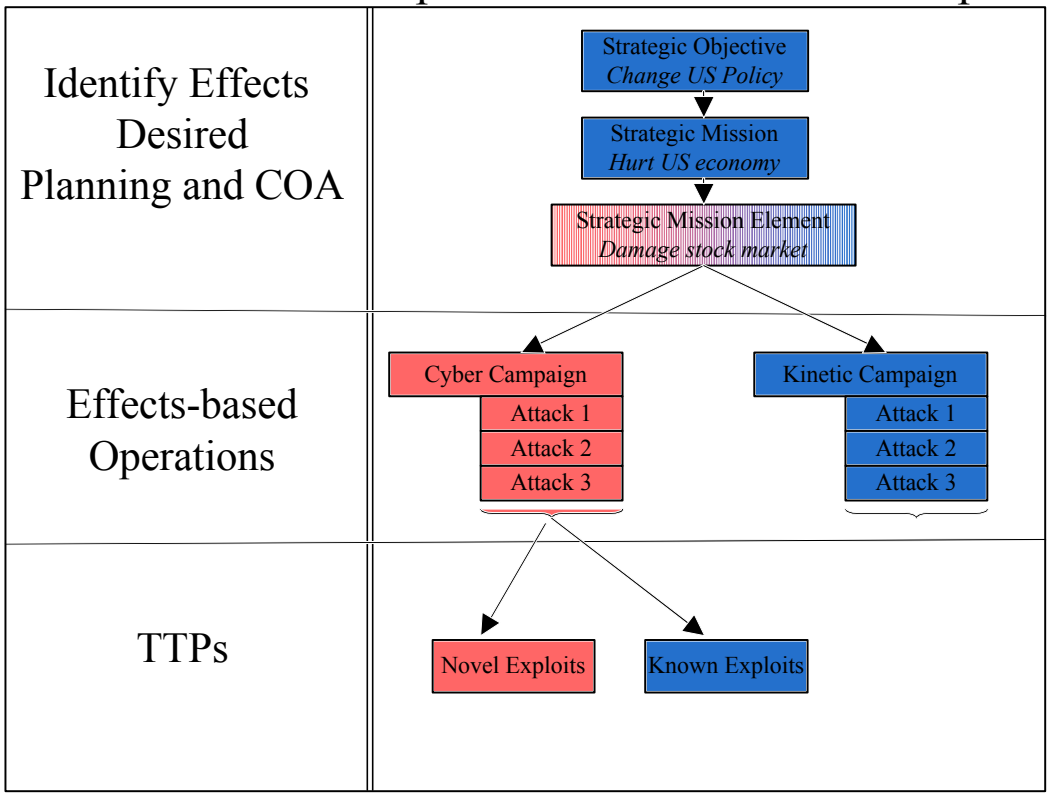
BBN TECHNOLOGIES

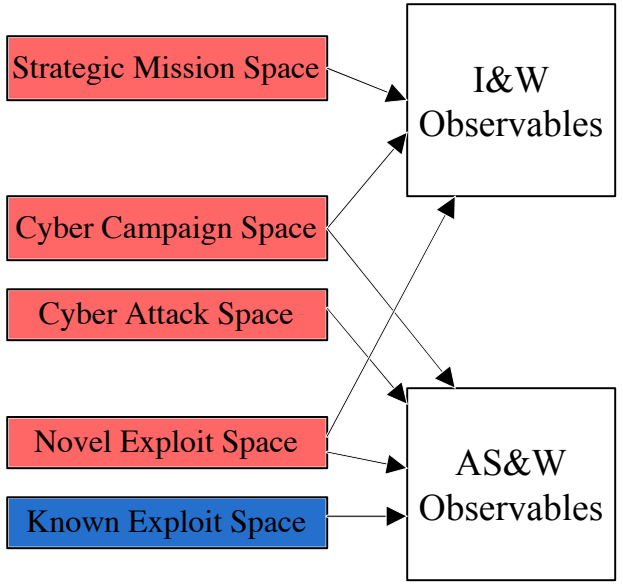
Challenge to Research Community

- All previous attempts at detecting malicious behavior fail to include *a priori* development of observables
  - *A posteriori* methods not only fail to detect novel attacks but generate observables that rely on *over specification*.
    - *Over specification* generally guarantees intrusiveness, complexity, and cost
      - For computers and networks this requires wide deployment, consistent configuration and management, and significant resources
  - *A priori* methods will detect novel attacks and rely on high value or overlapping observables
    - An important hypothetical attack may generate single observables but those observables cannot be ignored due to the risk and cost should the attack occur
    - Many lesser important hypothetical attacks will generate independent observables, but many are likely to be in common – e.g., overlap.
- The research community must address *a priori methods* whether applied to CNA/CNE or terrorism else:
  - Defensive resources will become exhausted or ineffective
  - Defenders will become unacceptably intrusive
  - *Novel attacks will still not be detected or prevented*

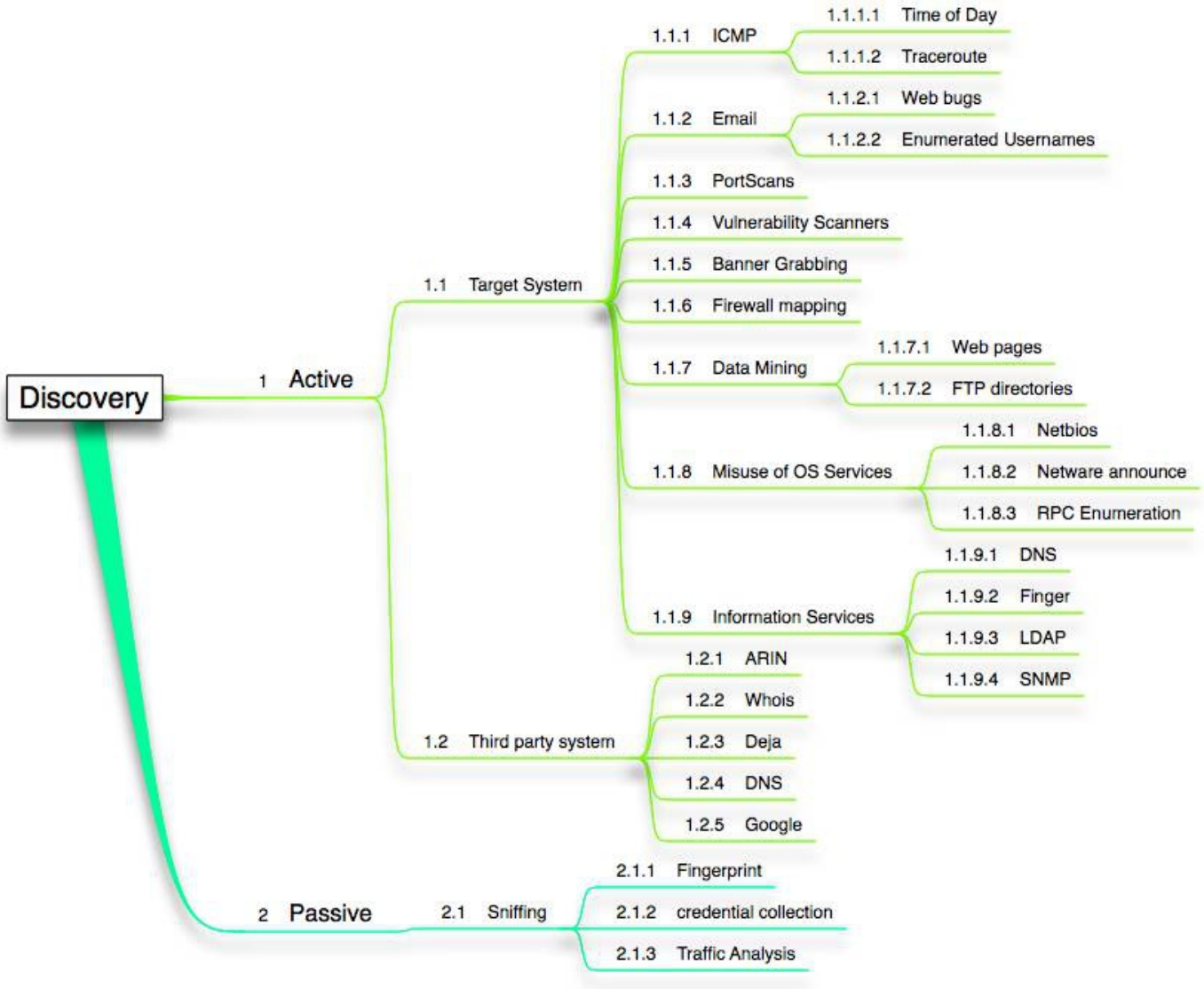
Process Model Development

- Two parallel paths
  - Top-down leading to observables spaces
  - Bottom-up leading observables spaces
  - Keep the focus on developing a-priori observables
    - Use a-posteriori observables to help validation





Attack Phase Categorization Development



Attacker Action Categorization Development