HotSoS’14

Cybersecurity Dynamics:

A Foundation for the Science of Cybersecurity

Shouhuai Xu
Department of Computer Science, University of Texas at San Antonio

Introduction

Just like how concepts such as confidentiality, integrity and availability have been driving the study of security for decades, the concept of Cybersecurity Dynamics can serve as a foundation for driving the study of Cybersecurity for the many years to come.

The Concept

Cybersecurity Dynamics describes the evolution of global cybersecurity state as caused by cyber attack-defense interactions. Figure 1 illustrates the evolution of cybersecurity state of a toy cyber system that has six nodes, which can represent computers (but other resolutions are both possible and relevant). In this example, a node may be in one of two states, **secure** or **compromised**; a secure node may become compromised and a compromised node may become secure again, and so on. A red-colored node u pointing to a red-colored node v means u successfully attacked v. Even if node 5 is not attacked by any other node at time t_4, it still can become compromised because of (e.g.) an insider attack launched by an authorized user. An important abstraction in Cybersecurity Dynamics is ***attack-defense structure***, namely Complex Networks that capture the relation which computer can directly attack against and/or defend for which computers in a cyber system of interest.

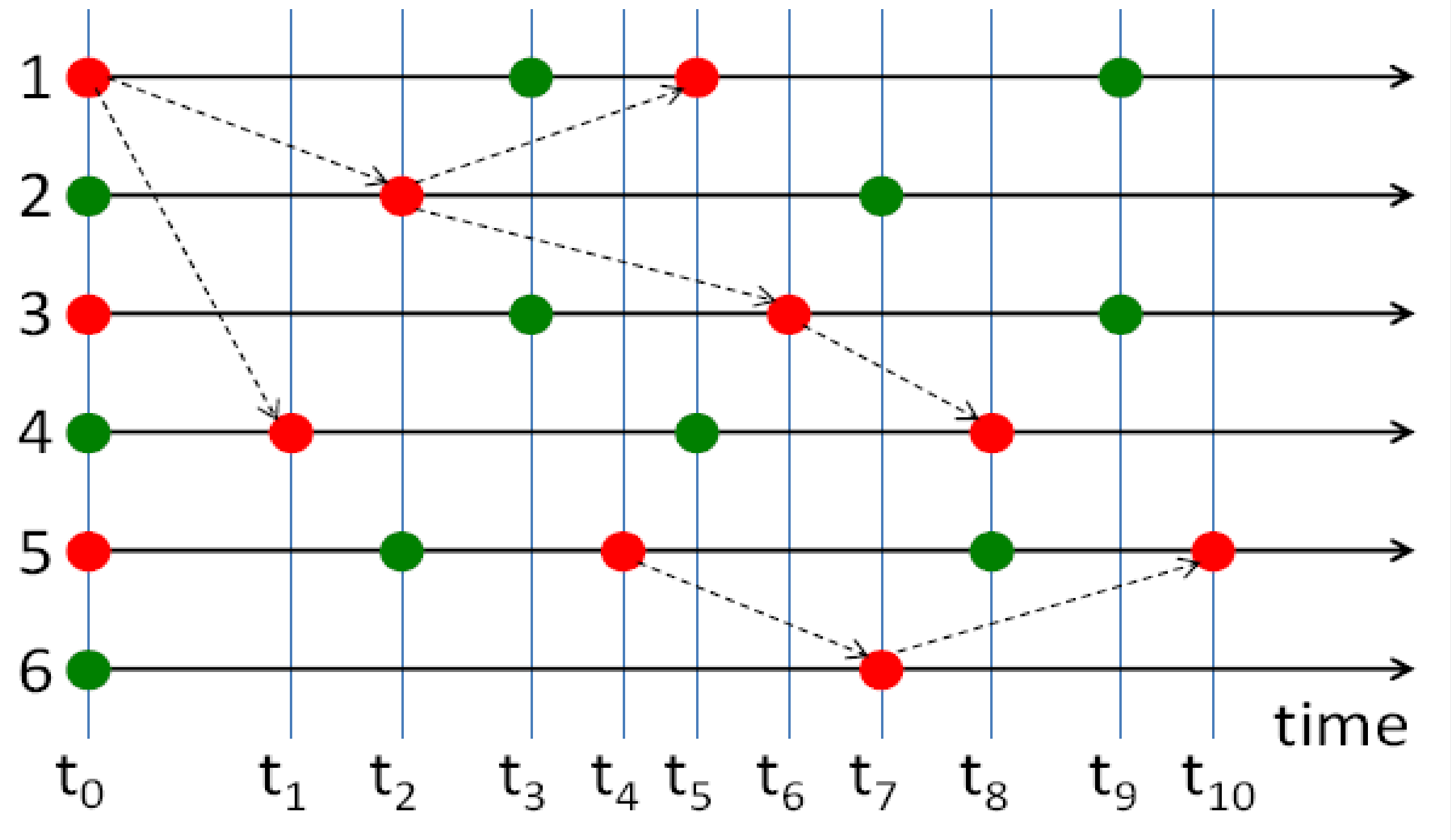


Figure 1. Illustration of Cybersecurity Dynamics in a toy cybersystem, which has six nodes (denoted by 1, …, 6) whose states evolve over time as caused by cyber attack-defense interactions. A node has two states: **secure** and **compromised**. Dashed arrows represent successful attacks.

Root Cause: Attack-Defense Interaction

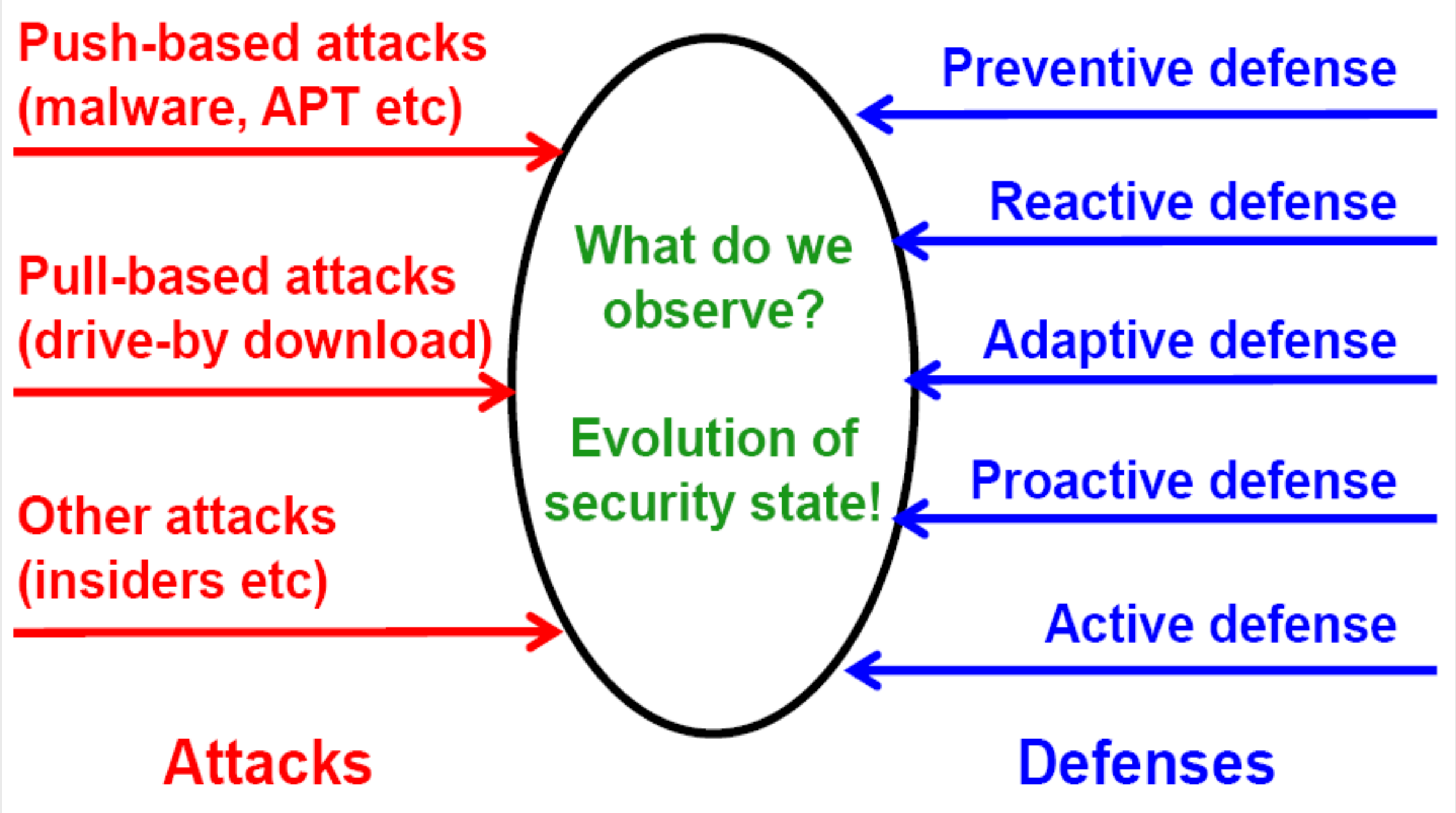

Push-based attacks (malware, APT etc)
Pull-based attacks (drive-by download)
Other attacks (insiders etc)
Attacks
What do we observe?
Evolution of security state!
Preventive defense
Reactive defense
Adaptive defense
Proactive defense
Active defense
Defenses

Figure 2. Root cause of Cybersecurity Dynamics: The attack-defense interaction, which offers a way to make connection between global state and local states.

Why Cybersecurity Dynamics?

First, cyber attacks are inevitable and defenders need to know the dynamic cybersecurity states so as to manage the risk (e.g., using appropriate threshold cryptosystems or Byzantine fault-tolerance schemes). Cybersecurity Dynamics offers natural security metrics such as: What is the probability that a node is compromised at time t? What is the (expected) number of nodes that are compromised at time t? Such basic metrics can be used to define more advanced security/risk metrics for decision-making purposes. Together they can be used to characterize the ***global*** effect of deploying new defense tools or mechanisms or security architectures.

Second, Cybersecurity Dynamics naturally leads to the notion of ***macroscopic*** cybersecurity, where the model parameters abstract (e.g.) the power of ***microscopic*** attack/defense mechanisms and security policies.

Third, Cybersecurity Dynamics offers an overarching framework that can accommodate ***descriptive***, ***prescriptive***, and ***predictive*** cybersecurity models, which can be systematically studied by using various mathematical techniques (broadly defined). For example, we can characterize the cybersecurity phenomena exhibited by the dynamics and pin down the factors/laws that govern the evolutions.

The Framework

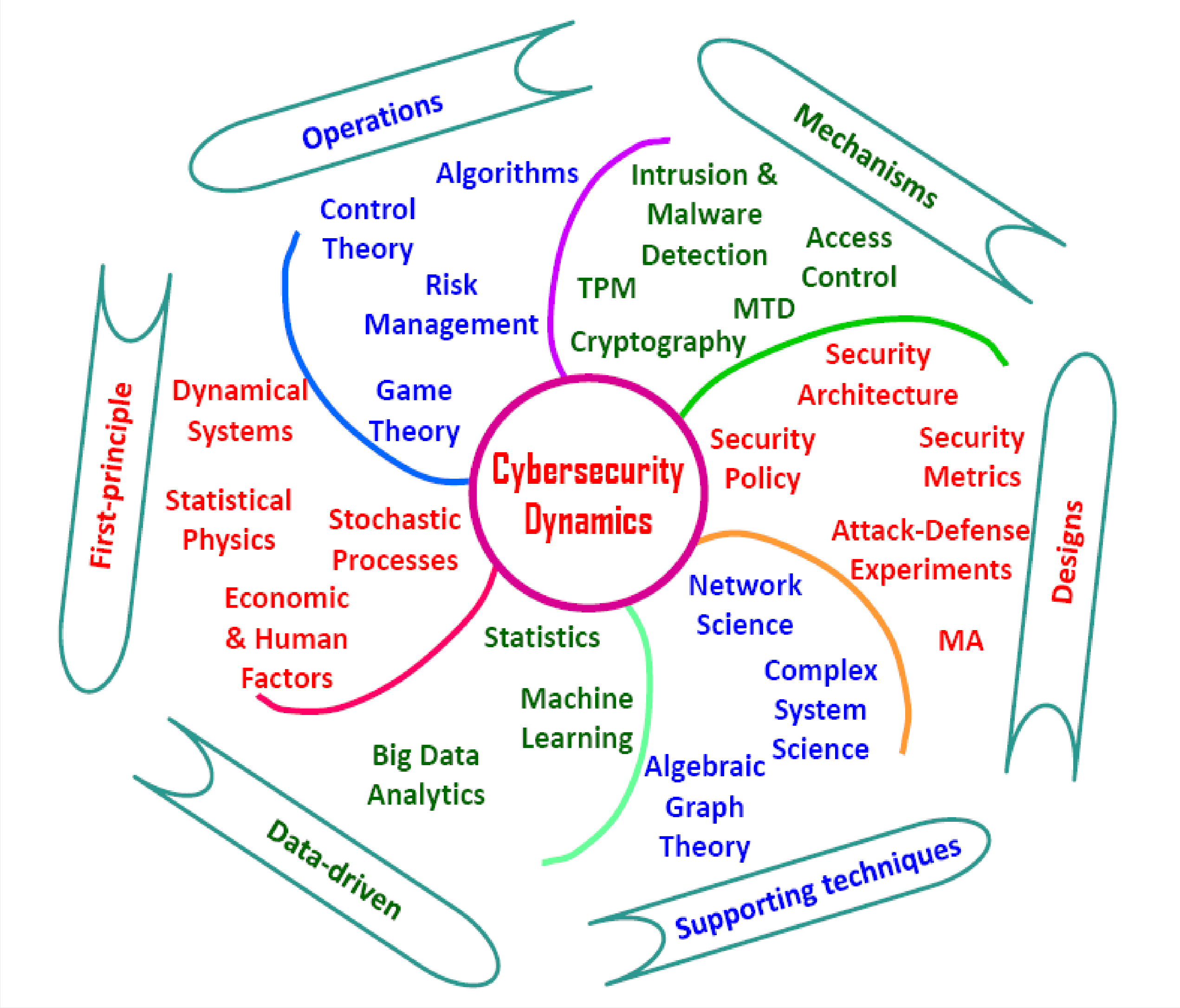
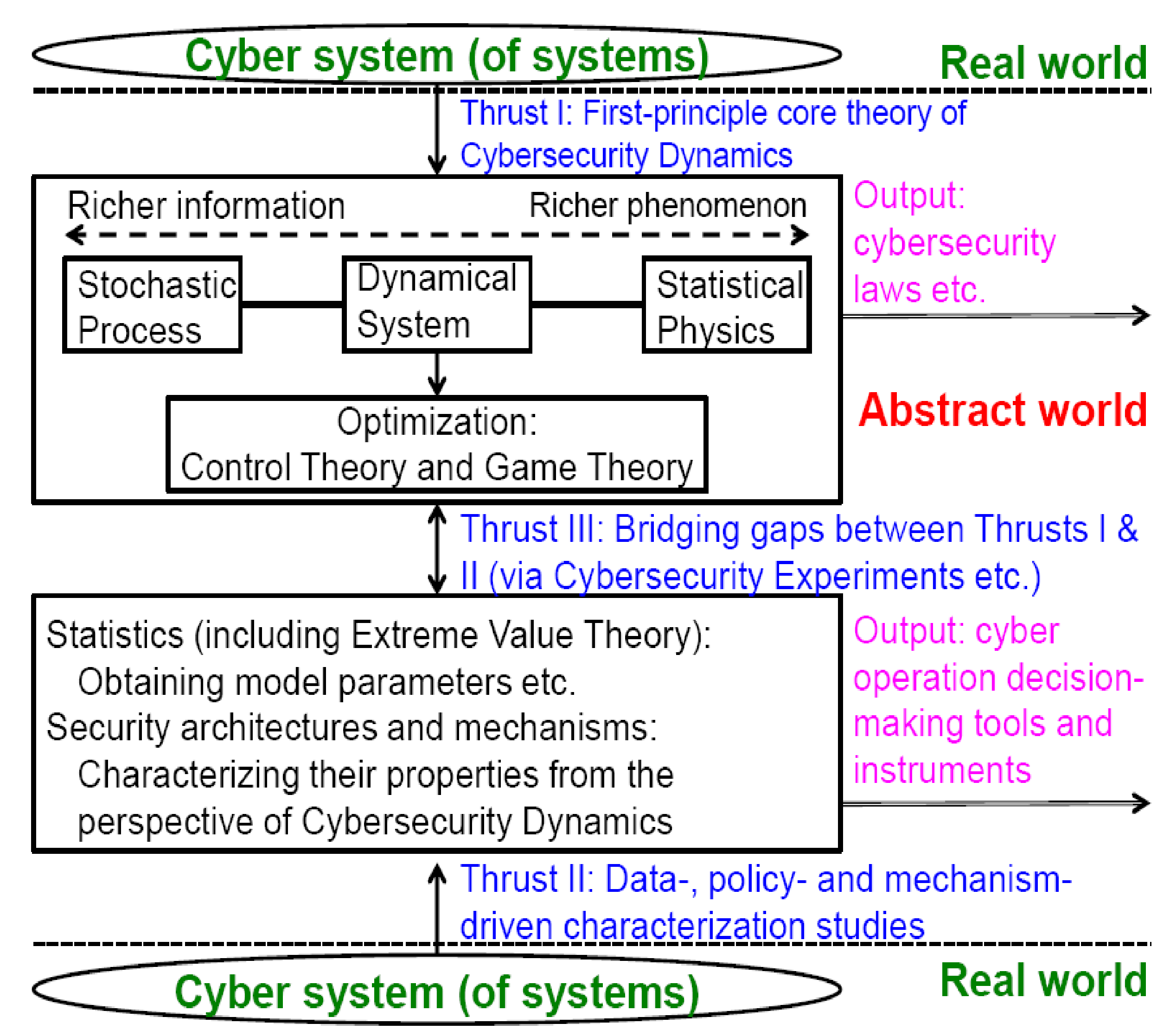


Figure 3. The Cybersecurity Dynamics overarching framework.

Research Roadmap


Cyber system (of systems)
Real world
Thrust I: First-principle core theory of Cybersecurity Dynamics
Richer information
Richer phenomenon
Stochastic Process
Dynamical System
Statistical Physics
Optimization: Control Theory and Game Theory
Output: cybersecurity laws etc.
Abstract world
Thrust III: Bridging gaps between Thrusts I & II (via Cybersecurity Experiments etc.)
Statistics (including Extreme Value Theory): Obtaining model parameters etc.
Security architectures and mechanisms: Characterizing their properties from the perspective of Cybersecurity Dynamics
Output: cyber operation decision-making tools and instruments
Thrust II: Data-, policy- and mechanism-driven characterization studies
Cyber system (of systems)
Real world

The Three Research Thrusts

Thrust I: Building a systematic theory of Cybersecurity Dynamics, via ***first-principle*** modeling, to derive macroscopic phenomena or properties from microscopic cyber attack-defense interactions. These studies can lead to cybersecurity laws of the following kind: What is the outcome of the interaction between a certain class of cyber defenses (including policies) and a certain class of cyber attacks?

Thrust II: Data-, policy-, architecture- and mechanism-driven characterization studies. These studies allow us to extract model parameters for practical use of the cybersecurity insights/laws discovered by Thrust I, and would lead to the development of cybersecurity instruments.

Thrust III: Bridging gaps between Thrusts I & II, by informing Thrust II what parameters used in the models of Thrust I are necessary to obtain (no matter how costly to obtain them), and informing Thrust I that certain other parameters may be easier to obtain in practice (i.e., alternate models may be sought instead).

Inherent Technical Barriers

Example inherent barriers (cannot be bypassed) include:

Scalability barrier: This state-space explosion problem.

Nonlinearity barrier: Highly nonlinear models.

Dependence barrier: Modeling dependent/adaptive attacks.

Structural dynamics barrier: Dynamic attack-defense structures.

Non-equilibrium/transient behavior barrier: Harder than equilibrium.

Preliminary Results

http://www.cs.utsa.edu/~shxu/socs/

Acknowledgement

ARO Grant # W911NF-13-1-0370 and AFOSR Grant # FA9550-09-1-0165.