REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)
21-08-2014

2. REPORT TYPE
Final Report

3. DATES COVERED (From - To)
1-Sep-2013 - 31-May-2014

4. TITLE AND SUBTITLE
Final Report: Cybersecurity Dynamics

5a. CONTRACT NUMBER
W911NF-13-1-0370

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
Shouhuai Xu

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of Texas at San Antonio
One UTSA Circle

San Antonio, TX 78249 -0603

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
64623-CS-II.3

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

In the course of seeking fundamental concepts that can drive the study of cybersecurity for the many years to come --- just like how concepts such as confidentiality, integrity and availability have been driving the study of information security for decades --- the idea of Cybersecurity Dynamics emerged. Intuitively, Cybersecurity Dynamics describes the evolution of cybersecurity state as caused by cyber attack-defense interactions. By studying Cybersecurity
Dynamics, we can characterize the cybersecurity phenomena exhibited in the evolution of cybersecurity state and

15. SUBJECT TERMS
Foundation, Models, Cybersecurity Dynamics

16. SECURITY CLASSIFICATION OF:

a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
UU	UU	UU	UU		Shouhuai Xu
					19b. TELEPHONE NUMBER 210-458-5739

Report Title

Final Report: Cybersecurity Dynamics

ABSTRACT

In the course of seeking fundamental concepts that can drive the study of cybersecurity for the many years to come --- just like how concepts such as confidentiality, integrity and availability have been driving the study of information security for decades --- the idea of Cybersecurity Dynamics emerged. Intuitively, Cybersecurity Dynamics describes the evolution of cybersecurity state as caused by cyber attack-defense interactions. By studying Cybersecurity

Dynamics, we can characterize the cybersecurity phenomena exhibited in the evolution of cybersecurity state and pin down the factors and laws that govern the evolution. Cybersecurity Dynamics offers a new way of thinking in formulating the ultimately wanted foundation for the science of cybersecurity. One fundamental implication of Cybersecurity Dynamics is that emergent behavior is inherent to cybersecurity. This issue has not been understood, or even recognized, by many researchers.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received		Paper
08/21/2014	1.00	Shouhuai Xu. Cybersecurity Dynamics, HoTSoS'2014. 08-APR-14, . : ,
08/21/2014	2.00	Shouhuai Xu. Emergent Behavior in Cybersecurity, HotSoS'2014. 08-APR-14, . : ,
TOTAL:		**2**

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received	Paper

TOTAL:

Number of Manuscripts:

Books

Received	Book

TOTAL:

Received	Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Moustafa Saleh	0.45	
Weiliang Luo	0.10	
Li Xu	0.20	
Zhenxin Zhan	0.45	
Qingji Zheng	0.45	
FTE Equivalent:	**1.65**	
Total Number:	**5**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Shouhuai Xu	0.07	
FTE Equivalent:	**0.07**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:...... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):...... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:...... 0.00

Names of Personnel receiving masters degrees

NAME	
Weiliang Luo	
Total Number:	**1**

Names of personnel receiving PHDs

NAME	
Li Xu	
Zhenxin Zhan	
Qingji Zheng	
Total Number:	**3**

Names of other research staff

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

See Attachment

Technology Transfer

The results of the project have been briefed to:

-- Dr. Steven King, Deputy Director, Cyber Technology, ASD (R&E), and his staff
Dr. Thomas Moyer

-- Dr. Alexander Kott, Chief, Network Science Division, ARL

-- Edward Paul Ratazzi, Researcher, AFRL/RIG

ARO Project Final Report

Cybersecurity Dynamics

Grant number: W911NF-13-1-0370

PI: Prof. Shouhuai Xu
Department of Computer Science
University of Texas at San Antonio
email: shxu@cs.utsa.edu
web: www.cs.utsa.edu/~shxu
phone: 210-458-5739
fax: 210-458-4437

Program Manager: Dr. Cliff Wang

Report date: August 20, 2014
Project period: September 2013 — June 2014

Contents

1 Executive Summary

In the course of seeking fundamental concepts that can drive the study of cybersecurity for the many years to come — just like how concepts such as confidentiality, integrity and availability have been driving the study of security for decades — the idea of **Cybersecurity Dynamics** emerged. Intuitively, Cybersecurity Dynamics describes the evolution of cybersecurity state as caused by **cyber attack-defense interactions**. By studying Cybersecurity Dynamics, we can characterize the **cybersecurity phenomena** exhibited in the evolution of cybersecurity state and pin down the factors and laws that govern the evolution. As highlighted in Figure 1, Cybersecurity Dynamics offers a new way of thinking in formulating the ultimately wanted foundation for the science of cybersecurity. One fundamental implication of Cybersecurity Dynamics is that **emergent behavior** is inherent to cybersecurity. This issue has not been understood, or even recognized, by many researchers.

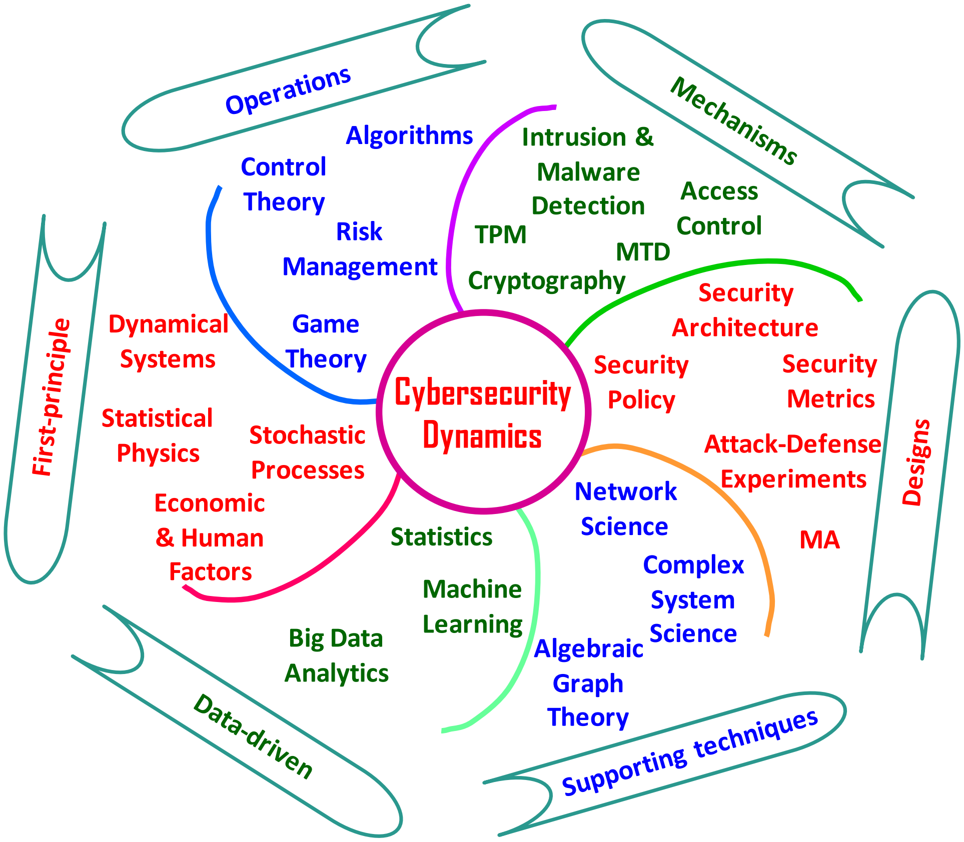


Figure 1: The vision of Cybersecurity Dynamics as the foundation of the science of cybersecurity; see Appendix A for a presentation. (The fields or sub-fields mentioned in each of the six perspectives are by no means exclusive.)

2 Cybersecurity Dynamics

In [1] (see Appendix B), we describe the fundamental ideas behind the novel concept of Cybersecurity Dynamics. At a high level, Cybersecurity Dynamics describes the evolution of global cybersecurity state as caused by **cyber attack-defense interactions**. It can serve as a foundation for the Science of Cybersecurity because of the following. 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 or Moving Target Defense). Cybersecurity Dynamics offers natural security metrics such as: What is the probability that a node/computer is compromised at time t? What is the (expected) number of nodes/computers 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 some defense tools or mechanisms. Second, 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.

Cybersecurity Dynamics was inspired by ideas underlying the epidemic models in Biology, ideas underlying the interacting particle systems in Physics, and ideas underlying the microfoundation in economics. However, Cybersecurity Dynamics goes beyond them because it imposes a distinguishing set of technical barriers, such as:

- The **nonlinearity** barrier: The probability that a computer is compromised would depend on the states of other computers in a (highly) nonlinear fashion. This can render many analysis techniques useless.

- The **dependence** barrier: The states of computers are dependent upon each other (e.g., they may have the same software vulnerability), and thus we need to accommodate such dependence between them.

- The **non-equilibrium** (or **transient behavior**) barrier: It is important to understand both the equilibrium states and the dynamics before it converges to the equilibrium distribution/state (if it does at all).

A profound implication of Cybersecurity Dynamics is that the concept of **emergent behavior** is inherent to cybersecurity, as we illustrate in [2] (see Appendix C). Emergent behavior highlights that there are cybersecurity properties of cybersystems that are not possessed/implied by the cybersecurity properties of the component cybersystems (i.e., the "$1+1>2$" effect). This has been acknowledged by our recent results [3, 4, 5, 7, 8, 9, 10, 11].

3 Future Research Directions

The novel concept of Cybersecurity Dynamics opens the door for a rich field of research, as demonstrated by our results [3, 4, 5, 7, 8, 9, 10, 11]. This concept is unique in that it can systematically and seamlessly incorporate many disciplines in order to formulate the foundation of cybersecurity. The research blueprint outlined in [1] includes three integral research thrusts:

- Thrust I: Building a systematic theory of cybersecurity dynamics.
- Thrust II: Data-, policy-, architecture- and mechanism-driven characterization studies.
- Thrust III: Bridging the gaps between Thrusts I & II (including the gaps between theory and practice).

We believe that a research community will be fostered to extensively explore this innovative approach for the many years to come.

References

[1] Shouhuai Xu. *Cybersecurity Dynamics*. Proceedings of 2014 Symposium and Bootcamp on the Science of Security (HotSoS'14), pages 14:1–14:2.

[2] Shouhuai Xu. *Emergent Behavior in Cybersecurity*. Proceedings of 2014 Symposium and Bootcamp on the Science of Security (HotSoS'14), pages 13:1–13:2.

[3] Shouhuai Xu, Wenlian Lu, and Hualun Li. *A Stochastic Model of Active Cyber Defense Dynamics*. Internet Mathematics, accepted for publication, 2014.

[4] Ren Zheng, Wenlian Lu, and Shouhuai Xu. *Active Cyber Defense Dynamics Exhibiting Rich Phenomena*. Manuscript in submission, 2014.

[5] Yujuan Han, Wenlian Lu and Shouhuai Xu. *Characterizing the Power of Moving Target Defense via Cyber Epidemic Dynamics*. Proceedings of 2014 Symposium and Bootcamp on the Science of Security (HotSoS'14), pages 10:1–10:12.

[6] Maochao Xu, Gaofeng Da, and Shouhuai Xu. *Cyber Epidemic Models with Dependencies*. Internet Mathematics (accepted for publication in 2014).

[7] Gaofeng Da, Maochao Xu and Shouhuai Xu. *A New Approach to Modeling and Analyzing Security of Networked Systems*. Proceedings of 2014 Symposium and Bootcamp on the Science of Security (HotSoS'14), pages 6:1–6:12.

[8] Gaofeng Da, Maochao Xu, and Shouhuai Xu. *On the Quasi-Stationary Distributions of Birth-Death Processes*. Manuscript in submission, 2014.

[9] Shouhuai Xu, Wenlian Lu, Li Xu, Zhenxin Zhan. *Adaptive Epidemic Dynamics in Networks: Thresholds and Control*. ACM Transactions on Autonomous and Adaptive Systems (ACM TAAS), 8(4): 19 (2014).

[10] Shouhuai Xu, Wenlian Lu, Li Xu. *Push- and pull-based epidemic spreading in networks: Thresholds and deeper insights*. ACM Transactions on Autonomous and Adaptive Systems (ACM TAAS), 7(3): 32 (2012).

[11] Maochao Xu and Shouhuai Xu. *An Extended Stochastic Model for Quantitative Security Analysis of Networked Systems*. Internet Mathematics 8(3): 288-320 (2012).

4 Appendix

The appendix contains the afore-mentioned presentation on Cybersecurity Dynamics and two extended abstracts [1, 2], namely:

- Appendix A: Shouhuai Xu. *Cybersecurity Dynamics* (presentation).
- Appendix B: Shouhuai Xu. *Cybersecurity Dynamics.* Proceedings of 2014 Symposium and Bootcamp on the Science of Security (HotSoS'14), pages 14:1–14:2.
- Appendix C: Shouhuai Xu. *Emergent Behavior in Cybersecurity.* Proceedings of 2014 Symposium and Bootcamp on the Science of Security (HotSoS'14), pages 13:1–13:2.

Appendix A

Cybersecurity Dynamics:

A Foundation for the Science of Cybersecurity

Shouhuai Xu

Department of Computer Science

University of Texas at San Antonio

www.cs.utsa.edu/~shxu

4/10/2014 @ UNC

One-Page Summary of the Talk

❑ Describing one approach to modeling cybersecurity from a holistic perspective, w/ example results.

❑ The approach is systematic and promising.

❑ To my knowledge, it is perhaps the only systematic approach that has been exposed to the public.

❑ And, of course, we are far away from where we can be.

The Situation … My Perspective

Q: There are many compromised computers in cyberspace. Is that because attackers are much smarter than "defenders + researchers"?

A: Perhaps not; it is caused by many "asymmetries".

Q: Why are there many "asymmetries"?

A: Cyberspace is *complex* (>>complicated), and pretty much everything we ("defenders + researchers") currently do is heuristic (or ad hoc) when considering whole-system (i.e., holistic; rather than building-blocks) properties.

Q: What can we do to fundamentally change the situation?

An Initial Observation

Cybersecurity is a (relatively) new subject.

❑ More about systems properties, than about building-blocks properties and data/information properties.

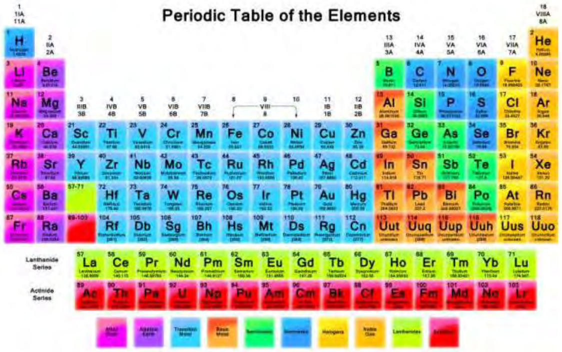
❑ Putting risk management etc. into context

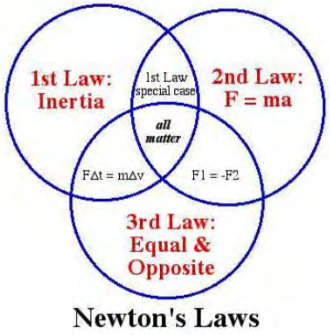
Understanding it would require a new way of thinking.

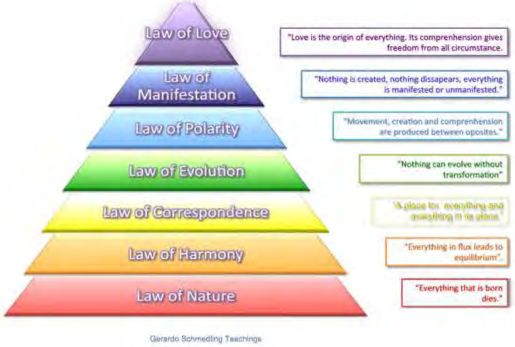
❑ What are the core concepts of cybersecurity (e.g., as fundamental as concepts such as confidentiality, integrity etc. that have driven research for decades)?

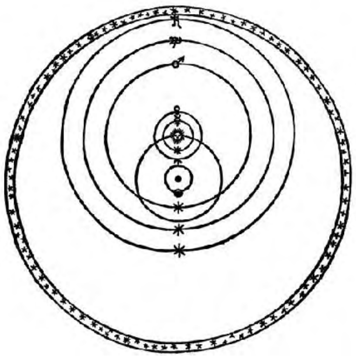
❑ What is the right abstraction for modeling and analyzing cybersecurity?

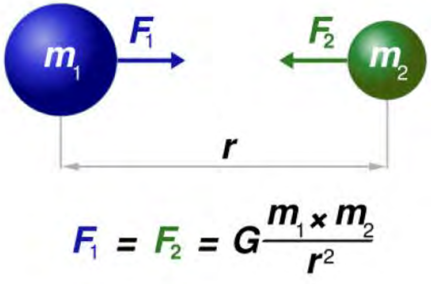
For example, what are the following kinds of things for the Science of Cybersecurity?


Periodic Table of the Elements




Law of Love
"Love is the origin of everything. Its comprehension gives freedom from all circumstance.
Law of Manifestation
"Nothing is created, nothing dissapears, everything is manifested or unmanifested."
Law of Polarity
"Movement, creation and comprehension are produced between oposites."
Law of Evolution
"Nothing can evolve without transformation"
Law of Correspondence
"A place for everything and everything in its place."
Law of Harmony
"Everything in flux leads to equilibrium".
Law of Nature
"Everything that is born dies."
Gerardo Schmedling Teachings

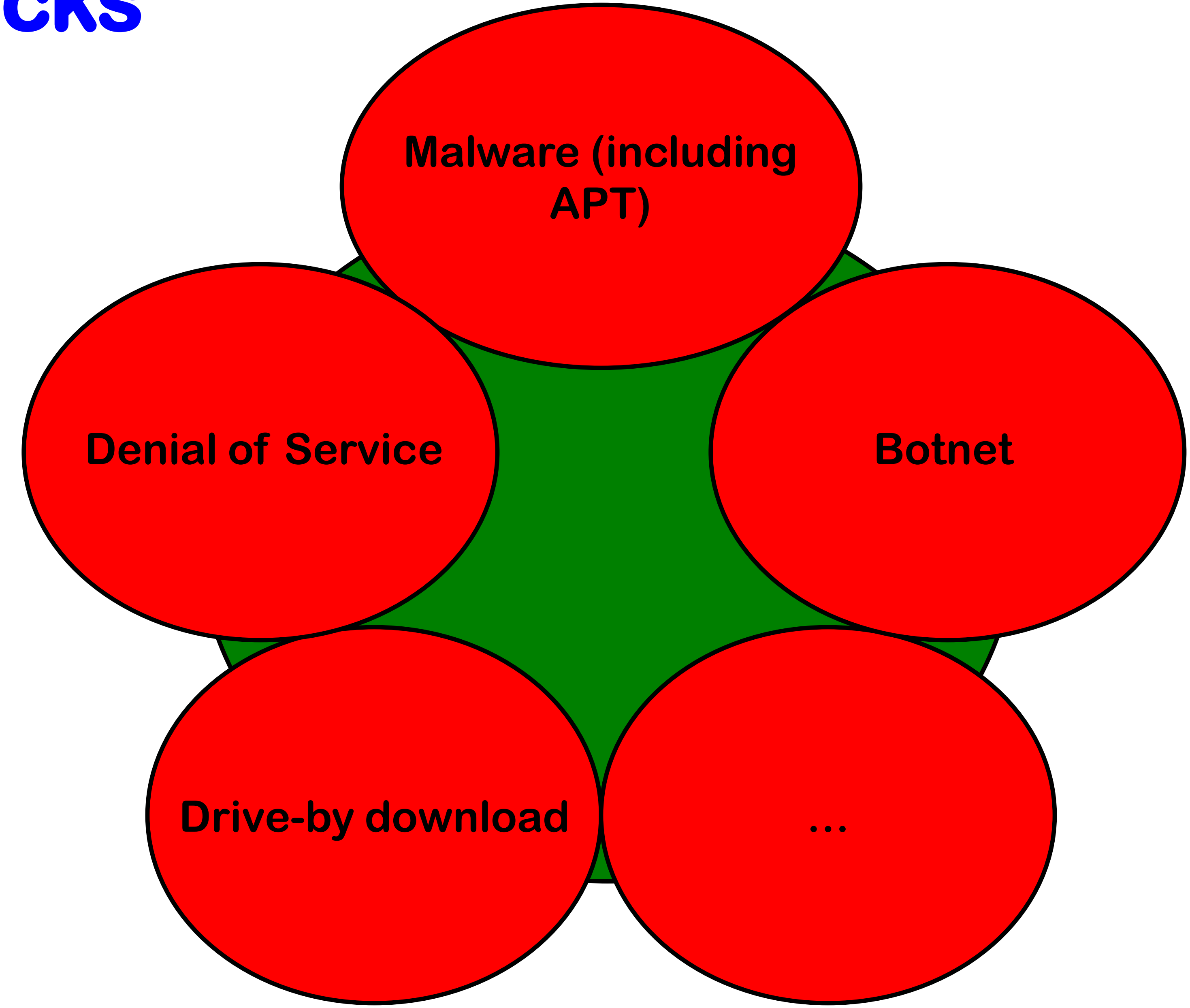




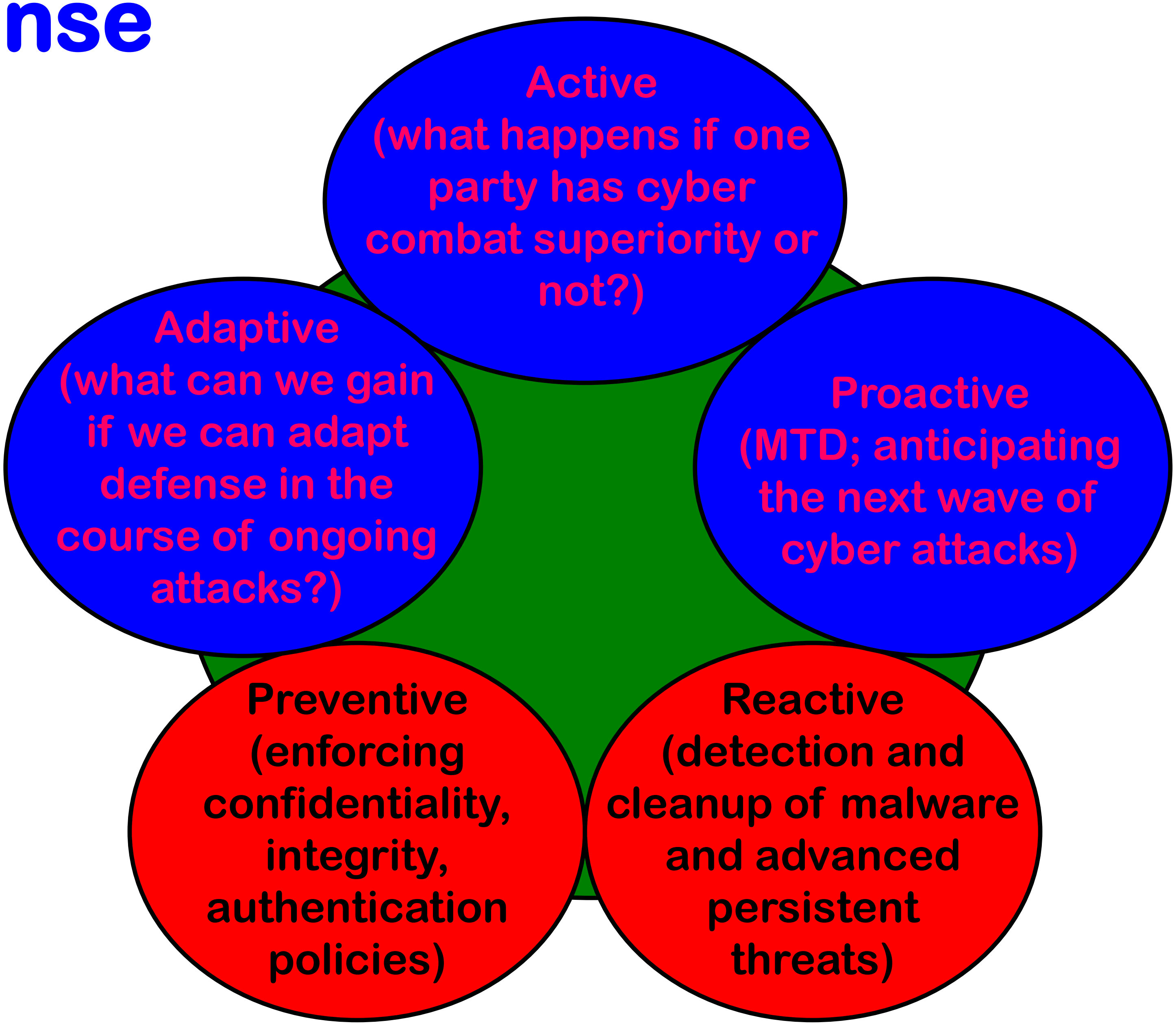
$$F_1 = F_2 = G\frac{m_1 \times m_2}{r^2}$$

Pictures borrowed from Internet.

Further Observation: Many Kinds of Attacks



Further Observation: Many Kinds of Defense



Active (what happens if one party has cyber combat superiority or not?)

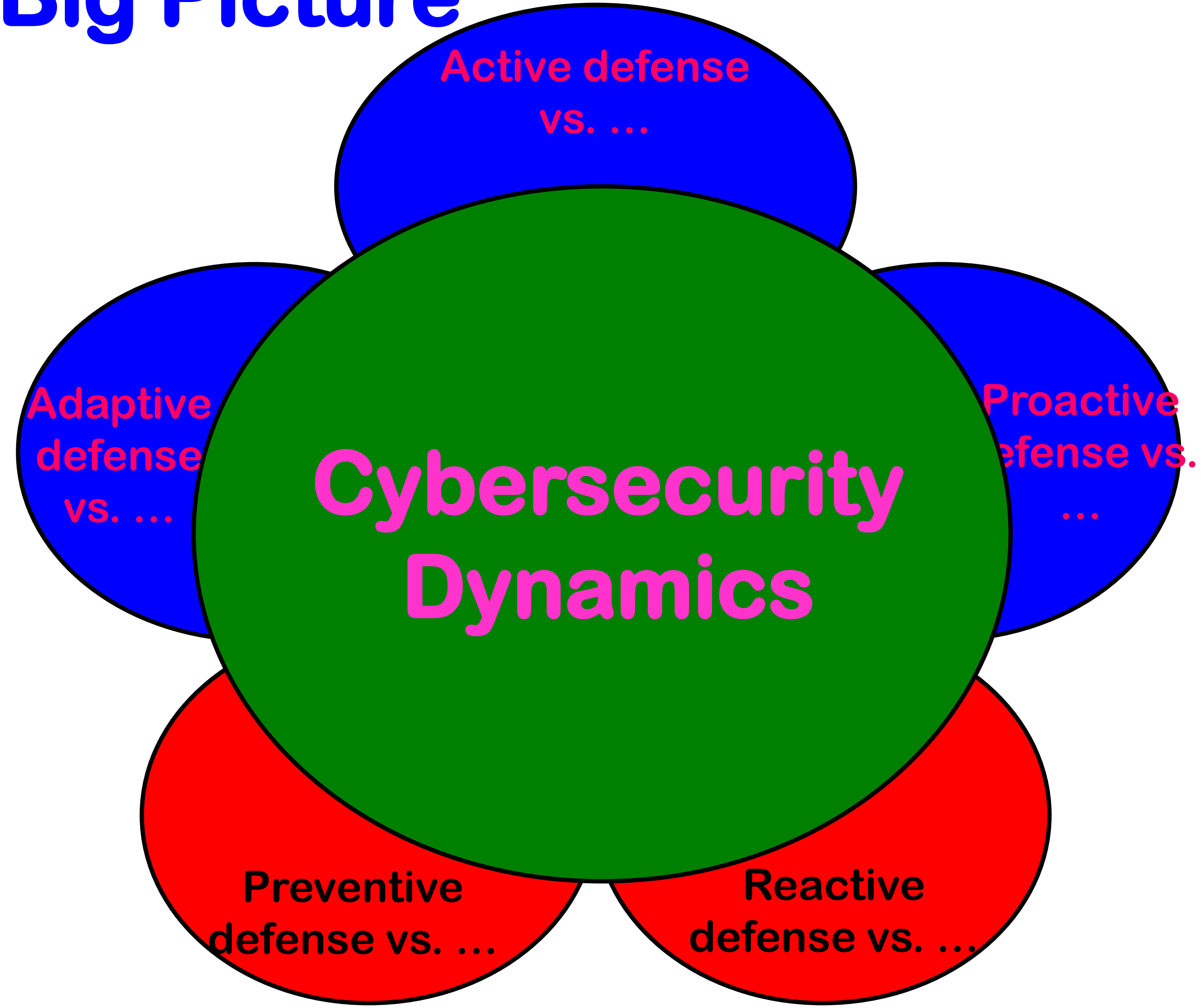
Adaptive (what can we gain if we can adapt defense in the course of ongoing attacks?)

Proactive (MTD; anticipating the next wave of cyber attacks)

Preventive (enforcing confidentiality, integrity, authentication policies)

Reactive (detection and cleanup of malware and advanced persistent threats)

Two Sides of the Same Coin: The Big Picture



Active defense vs. …

Adaptive defense vs. …

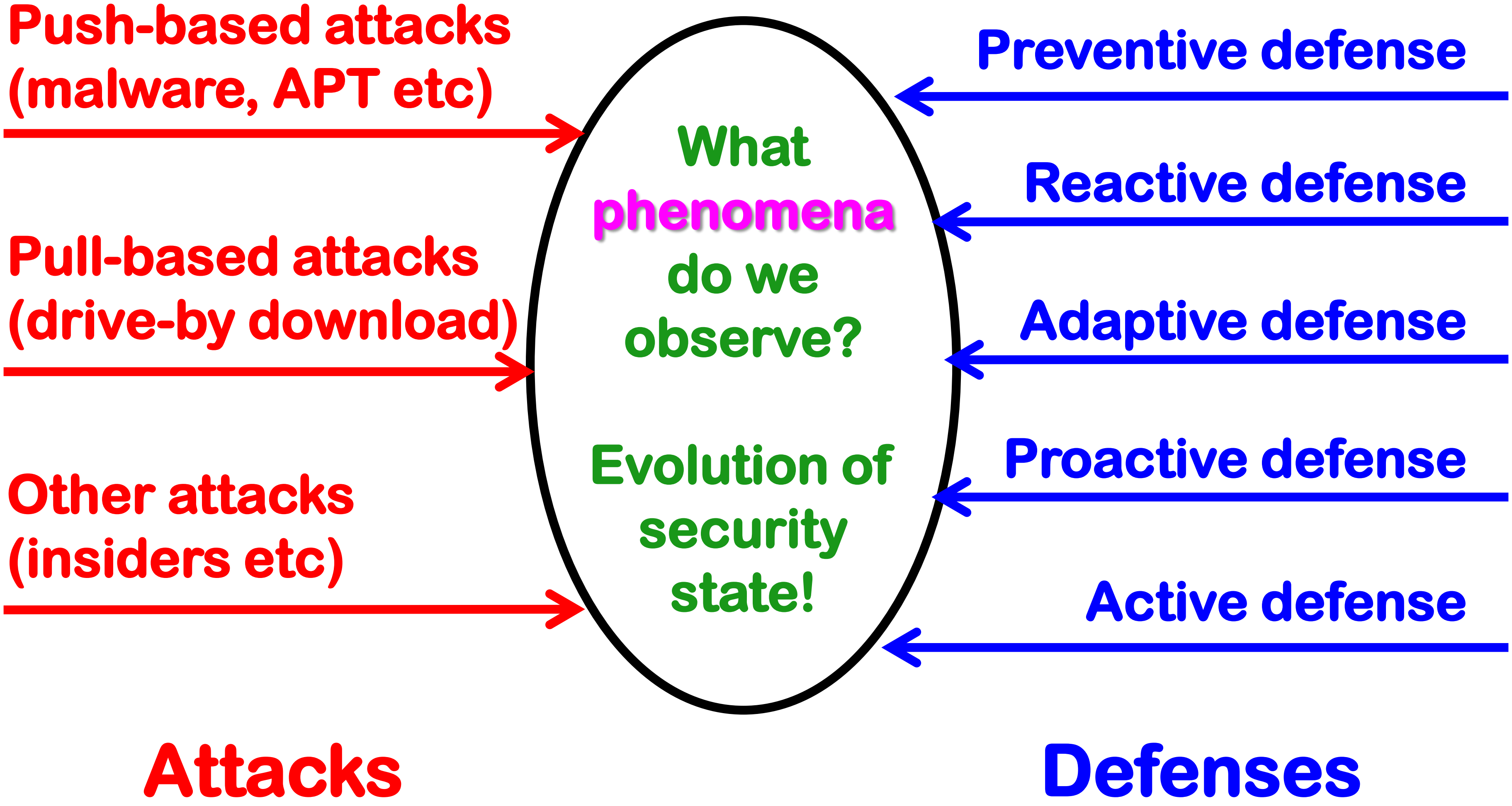
Proactive defense vs. …

Cybersecurity Dynamics

Preventive defense vs. …

Reactive defense vs. …

Cybersecurity Dynamics Caused by Cyber Attack-Defense Interactions



Push-based attacks (malware, APT etc)

Pull-based attacks (drive-by download)

Other attacks (insiders etc)

What phenomena do we observe?

Evolution of security state!

Preventive defense

Reactive defense

Adaptive defense

Proactive defense

Active defense

Attacks

Defenses

C.D. Reminiscent of …

The Art of War (Sun Tzu):

知彼知己，百戰不殆；不知彼而知己，一勝一負；不知彼，不知己，每戰必殆。

If you know your enemies and know yourself, you can win a hundred battles without a single loss.

- **Knowing the dynamics makes you always win!**

If you only know yourself, but not your opponent, you may win or may lose.

If you know neither yourself nor your enemy, you will always endanger yourself.

(English translation by http://en.wikipedia.org/wiki/The_Art_of_War)

Cybersecurity and Levels of Abstraction

Cybersecurity is NOT to replace existing body of security knowledge, but complementary. It offers an overarching abstraction from a holistic or global-system perspective.

Level of Abstraction	Models / objects for study

HIGHER-LEVEL

Connection between multiple levels of abstraction: Parameters in macroscopic cybersecurity models are derived from microscpoic cyber attack/defense tools (e.g., their power) , human factors, etc.

Reminiscent of Macroscopic Economics vs. Microscopic Economics?

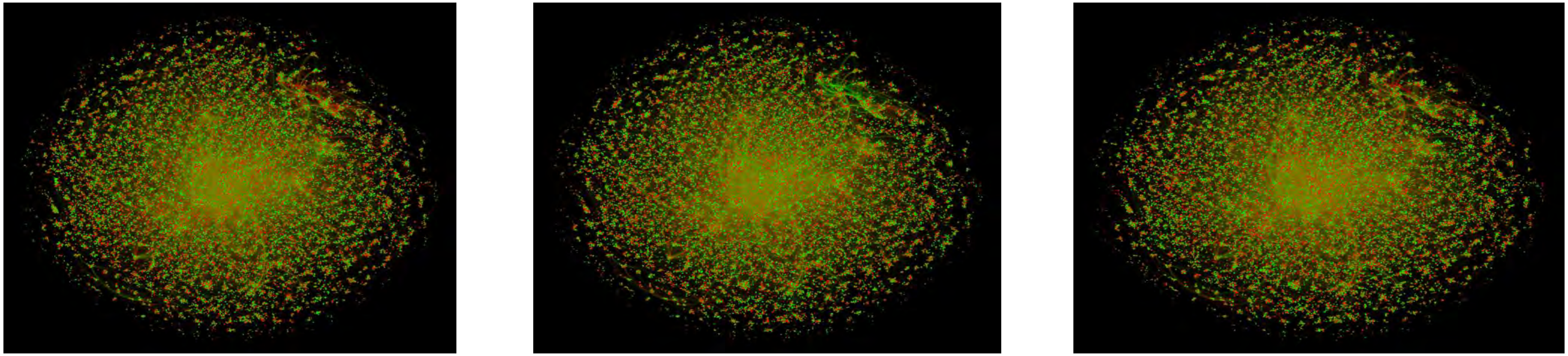
Evolution of Global Security State

Complex Network based abstraction:

❑ Nodes abstract entities (e.g., computer)

❖ Node state: green -- secure; red -- compromised

❑ Edges abstract the attack-defense interaction structure (system description/representation)

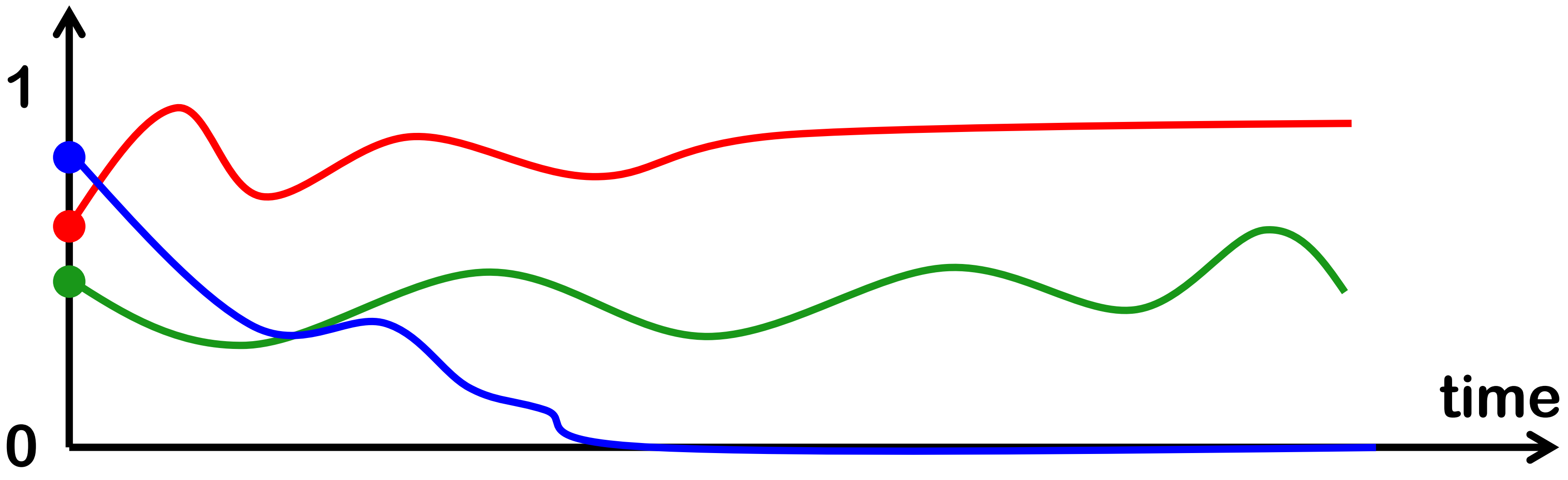


Three kinds of outcomes of evolution of global security state

Q: what are the governing/scaling laws?

Illustration: Evolution of Sec. State

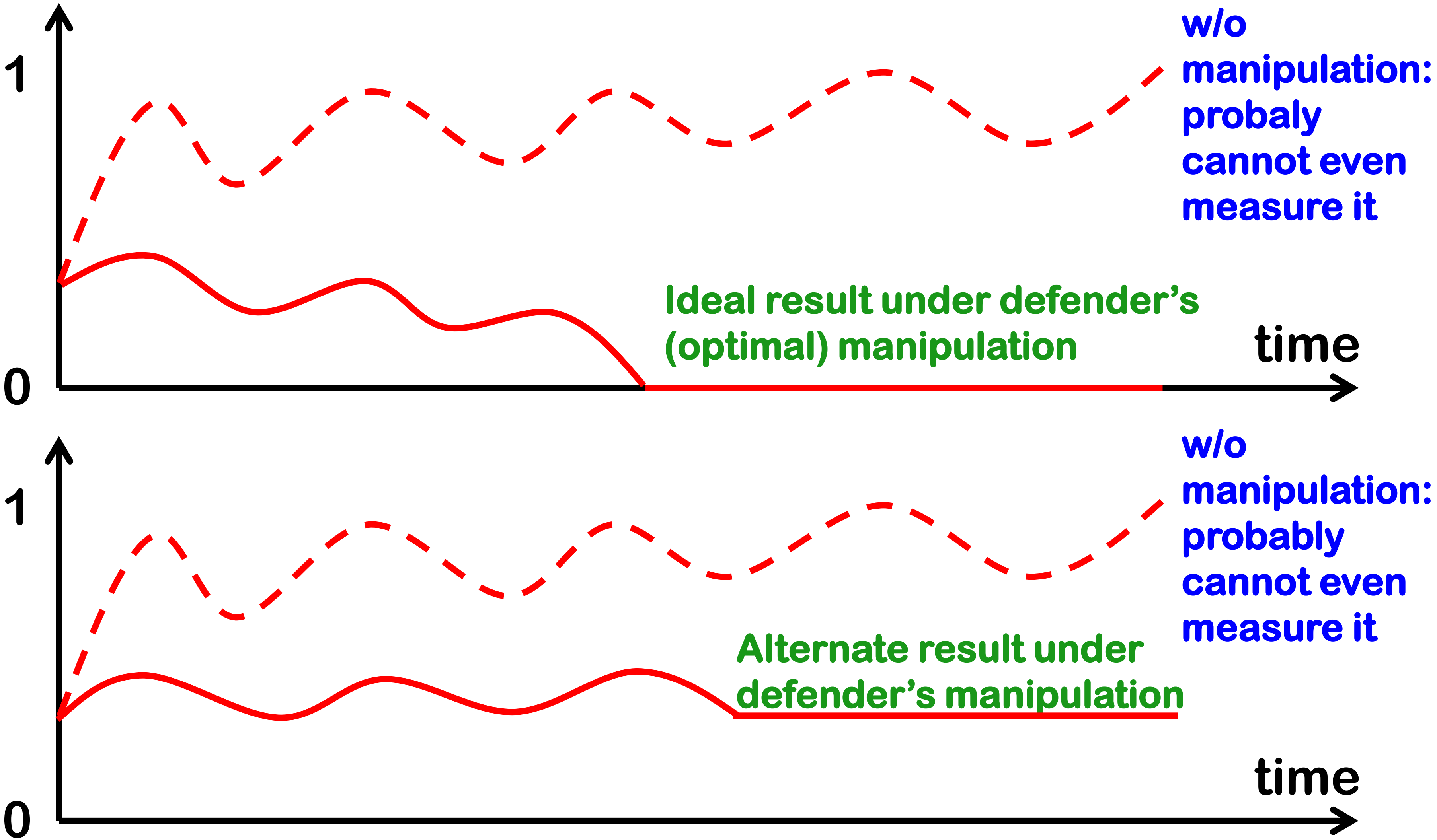
(Expected) portion of compromised nodes w.r.t. time



- ❑ This is perhaps the most natural ***cybersecurity metric.***
- ❑ With information about the probability that the nodes are compromised at time t, we can make better decisions. E.g., can a task be disrupted at time t (< mission lifetime) with probability at most p?

Illustration: Manipulating Evolution

(Expected) portion of compromised nodes w.r.t. time



w/o manipulation: probaly cannot even measure it

Ideal result under defender’s (optimal) manipulation

w/o manipulation: probably cannot even measure it

Alternate result under defender’s manipulation

Cybersecurity Dynamics

A phenomenon-centric new way of thinking:

❑ Cybersecurity Dynamics is an abstraction for understanding and managing (manipulating or even predicting) the evolution of security state.

❑ The evolution of security state is a “natural” phenomenon in cyber (and cyber-physical) systems, ranging from a small enterprise system to the entire cyberspace.

❑ The evolution of security state is caused by the attack-defense interactions.

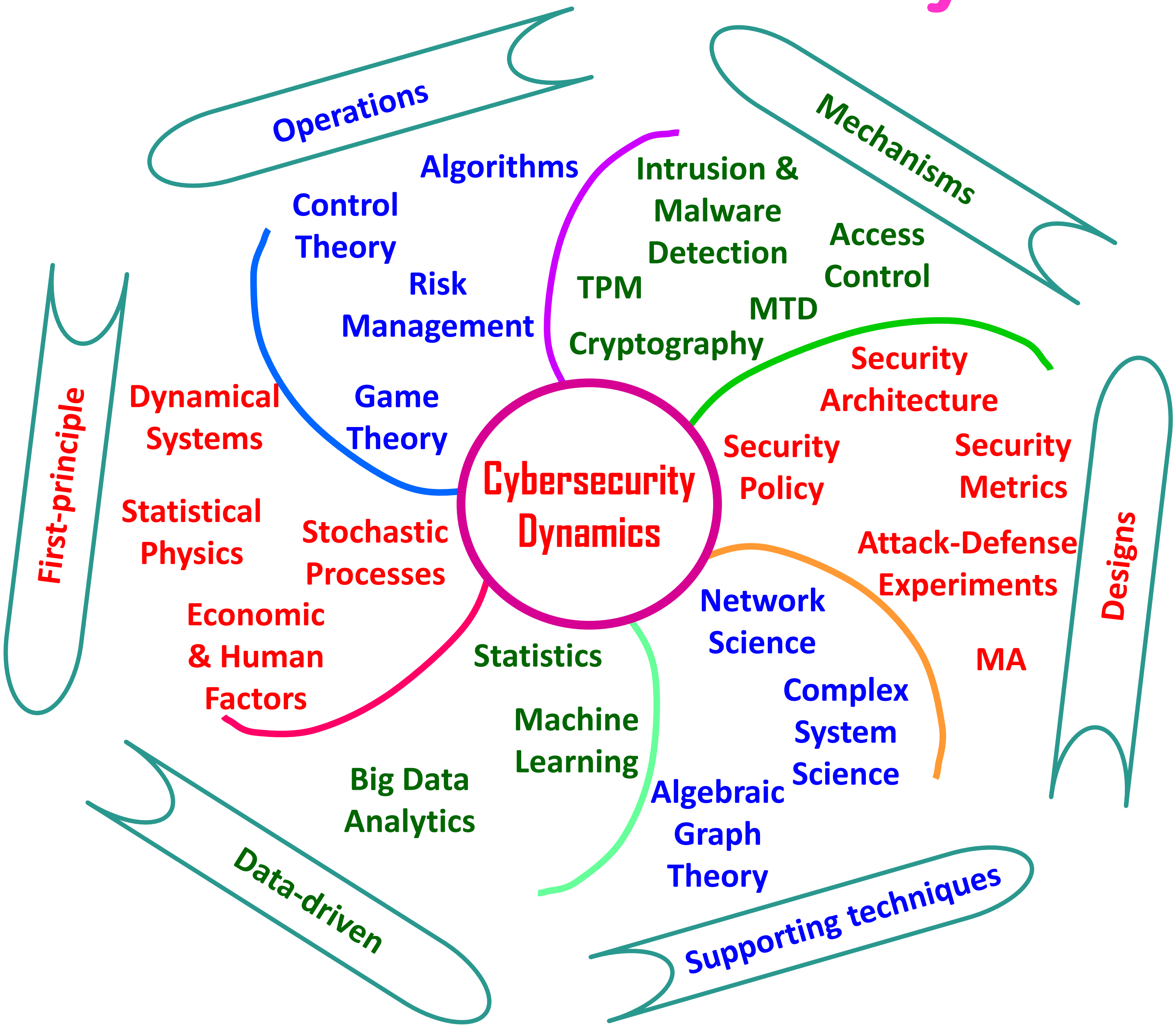
Roadmap

- ❑ Vision for Cybersecurity Dynamics Foundation
- ❑ Example Results Towards Fulfilling the Vision
  - ❖ Limitation of Preventive & Reactive Defense
  - ❖ Overcoming the Limitation w/ Active Defense
  - ❖ Optimizing Active Defense
- ❑ Challenges Ahead: Tackling Technical Barriers

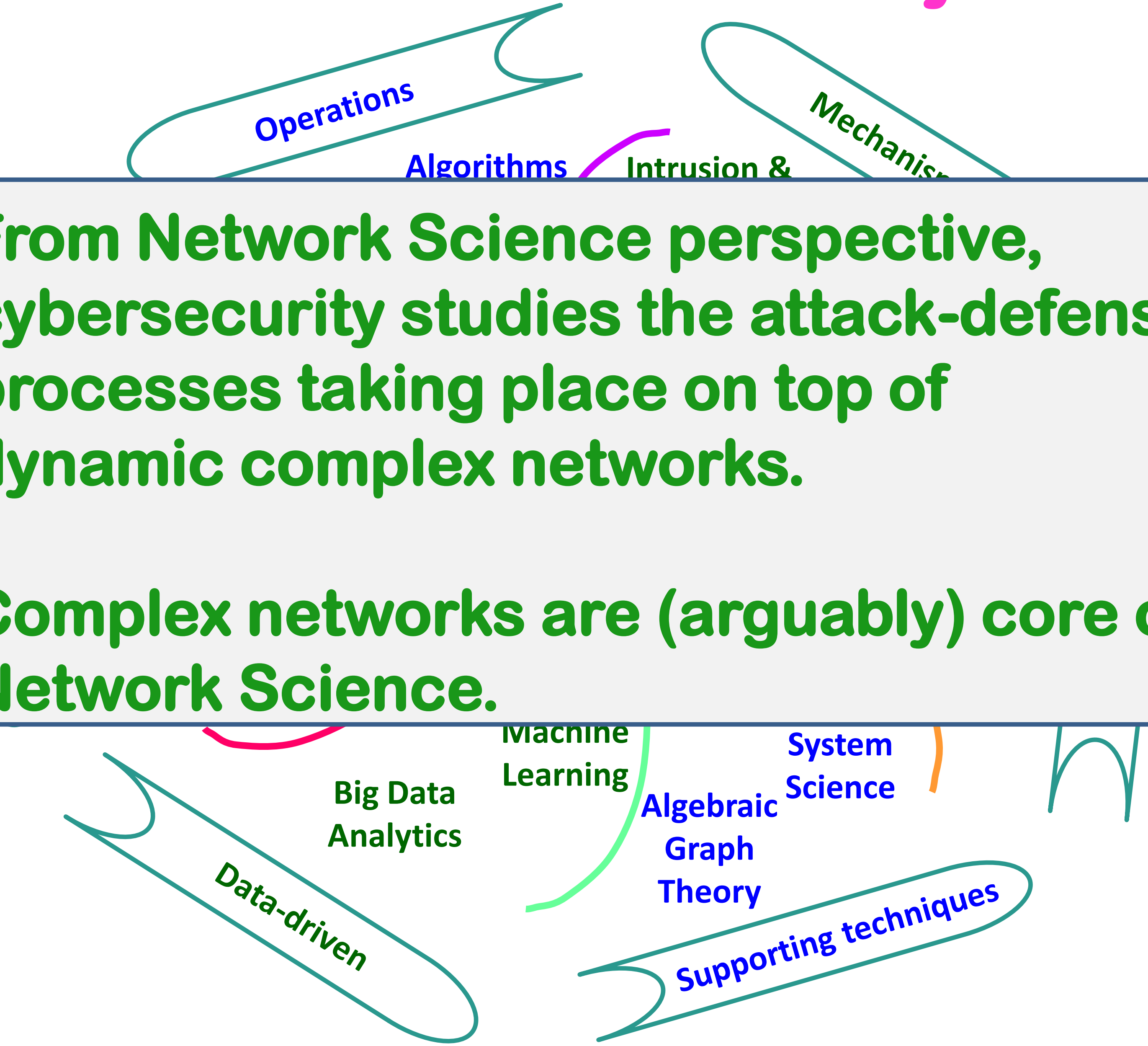
(Potential) Power of Cybersecurity Dynamics

- Descriptive power: Understanding the dynamics
  - What laws govern the evolution of security state?
  - Which security architecture is better?
- Prescriptive power: Manipulating the dynamics
  - How can we manipulate it to benefit the defender?
- Predictive power: Predicting and therefore proactively manipulating the dynamics
  - What can and cannot be predicted?
  - How can we quantify the effect of MTD?

The Vision: Cybersecurity Dynamics Foundation for the Science of Cybersecurity



The Vision: Cybersecurity Dynamics Foundation for the Science of Cybersecurity



From Network Science perspective, cybersecurity studies the attack-defense processes taking place on top of dynamic complex networks.

Complex networks are (arguably) core of Network Science.

The Vision: Cybersecurity Dynamics Foundation for the Science of Cybersecurity

From security perspective, by modeling cybersecurity through families of functions

$f(t, system\_description(t), a_1(t), \ldots, a_n(t), d_1(t), \ldots, d_m(t))$,

where $a_i(t)$'s and $d_i(t)$'s respectively abstract powers of cyber attack and defense deployments, we can (i) characterize ***the global effect of Δd_i*** (i.e., deploying a new defense mechanism) and (ii) compare ***security architectures***.

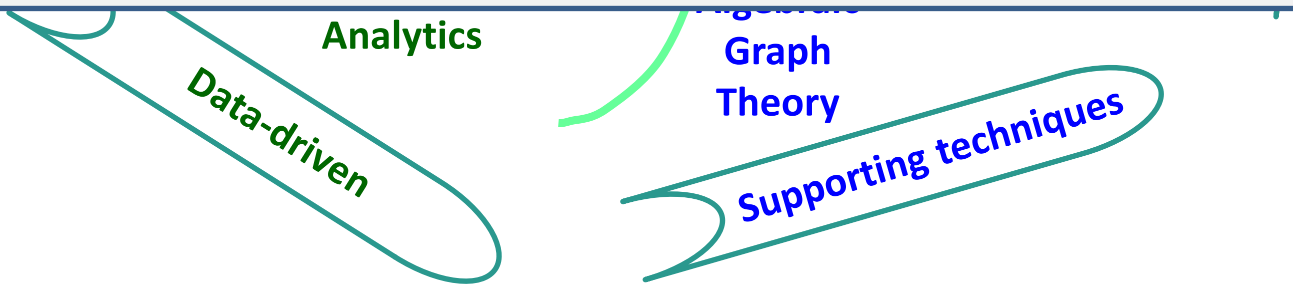
In principle, such f's exist.

The matter is how good/close we can approximate it.

(analogy: approximate solution to NP-hard problems?)

The Vision: Cybersecurity Dynamics Foundation for the Science of Cybersecurity

From defense operators' perspective, cybersecurity dynamics studies aim to offer **quantitative, real-time decision-making tools for optimal defense operations** (e.g., control the evolution of cybersecurity dynamics towards the desired destinations, at minimal cost).



The Vision: Cybersecurity Dynamics
Foundation for the Science of Cybersecurity

First-principle models aim to derive laws that govern the evolution of cyberscurity dynamics and to understand the phenomena that may or may not be beneficial to the defenders (e.g., Chaos).

Observation: Dynamical System is relevant to the very microscopic ciphers and the very macroscopic cybersecurity!

The Vision: Cybersecurity Dynamics Foundation for the Science of Cybersecurity

Data-driven studies aim to validate model assumptions, extract model parameters, characterize the statistical properties of cyber attack-defense processes as well we cyber attack processes, and understand the predictability of properties of these processes.

The Vision: Cybersecurity Dynamics Foundation for the Science of Cybersecurity

Disclamer: This is something being made, meaning that views/ideas can be subject to refinement (or even correction).

Note: We are not trying to attain any kind of very general science (e.g., the failed attempt at General System Science)

Rather, we want a science for the specific domain of cybersecurity, although it gets inspirations and supporting techniques from other kinds of sciences.

Not overly broad, not too narrow.

Complexity Science Comes to Rescue Again?

The (envisioned) Science of Cybersecurity:

- ❑ Soul: Security (concepts)
- ❑ Brain: Cybersecurity Dynamics (kind of Complexity Science)
- ❑ Muscle & Blood: Complex System/Network, Stochastic Process, Dynamical System, Statistical Physics, Control Theory, Game Theory, Statistics, Algebraic Graph Theory, Algorithms, Programming Language, etc.

The Science of Cryptography:

- ❑ Soul: Security (concepts)
- ❑ Brain: Comp. Complexity Theory (kind of Complexity Science)
- ❑ Muscle & Blood: Probability Theory, Number Theory, Abstract Algebra, etc.

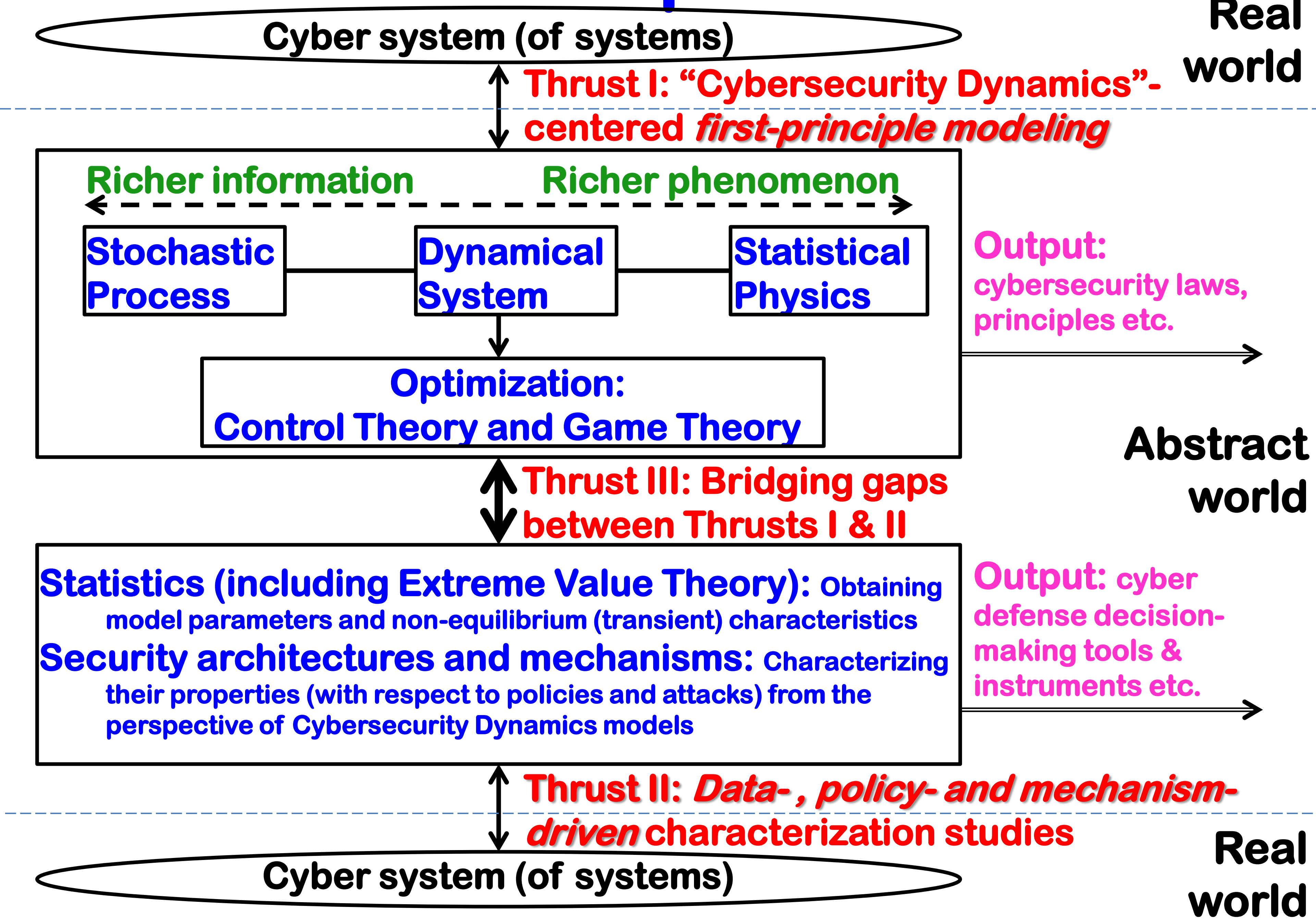
Research Roadmap: Three Thrusts Towards Fulfilling the Vision

- ❑ Thrust I: Building a systematic theory of Cybersecurity Dynamics

- ❑ Thrust II: Data-, policy- & mechanism-driven characterization studies, and developing (theory inspired/guided) tools for practice (e.g., managing mission assurance & risk)

- ❑ Thrust III: Bridging gaps between Thrusts I & II

Research Roadmap



Real world

Cyber system (of systems)

Thrust I: "Cybersecurity Dynamics"-centered *first-principle modeling*

Richer information

Richer phenomenon

Stochastic Process

Dynamical System

Statistical Physics

Optimization: Control Theory and Game Theory

Output: cybersecurity laws, principles etc.

Abstract world

Thrust III: Bridging gaps between Thrusts I & II

Statistics (including Extreme Value Theory): Obtaining model parameters and non-equilibrium (transient) characteristics

Security architectures and mechanisms: Characterizing their properties (with respect to policies and attacks) from the perspective of Cybersecurity Dynamics models

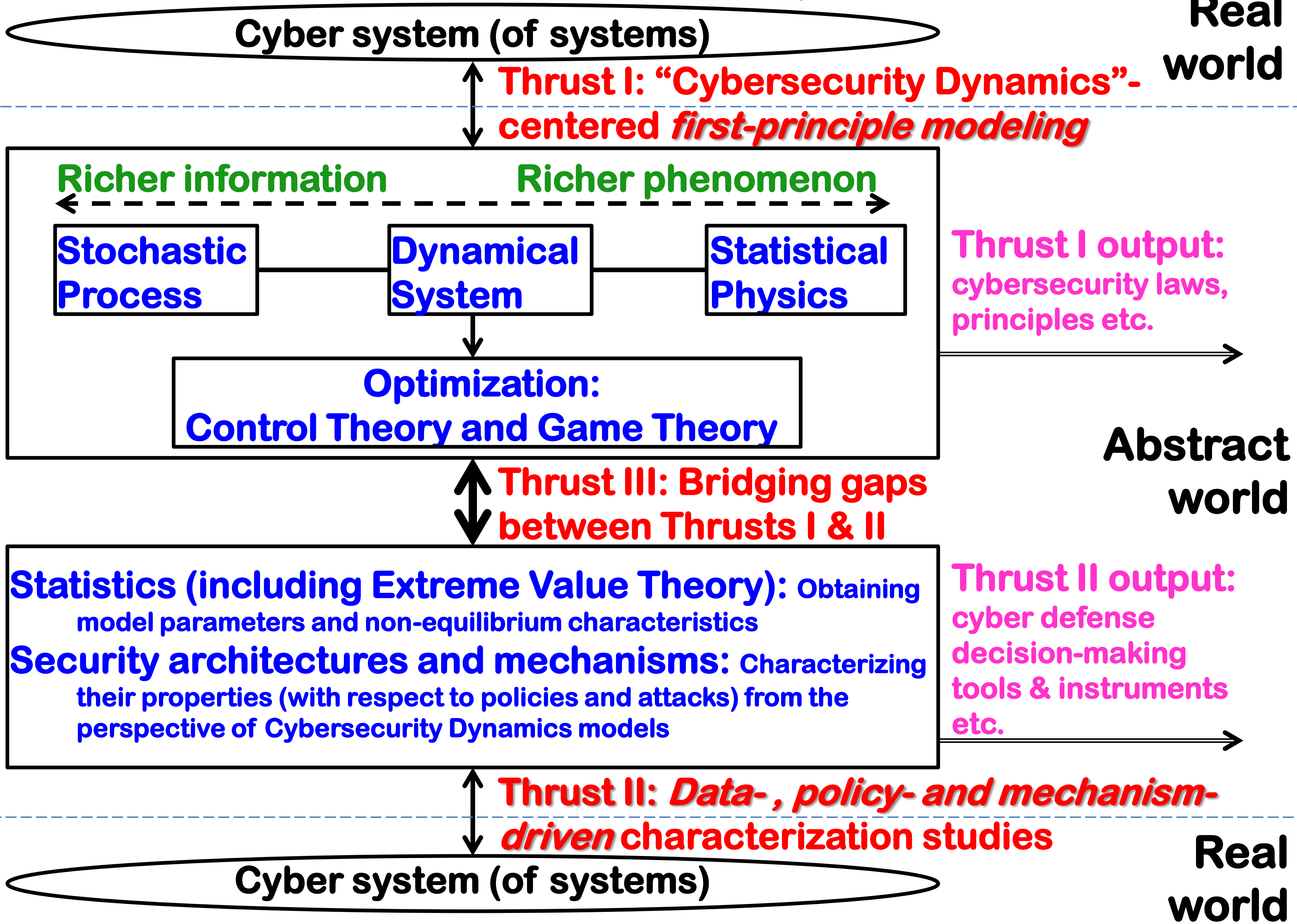
Output: cyber defense decision-making tools & instruments etc.

Thrust II: *Data-, policy- and mechanism-driven* characterization studies

Cyber system (of systems)

Real world

Rest of the Talk: Example Results



Real world

Cyber system (of systems)

Thrust I: “Cybersecurity Dynamics”-centered *first-principle modeling*

Richer information

Richer phenomenon

Stochastic Process

Dynamical System

Statistical Physics

Optimization: Control Theory and Game Theory

Thrust I output: cybersecurity laws, principles etc.

Abstract world

Thrust III: Bridging gaps between Thrusts I & II

Statistics (including Extreme Value Theory): Obtaining model parameters and non-equilibrium characteristics

Security architectures and mechanisms: Characterizing their properties (with respect to policies and attacks) from the perspective of Cybersecurity Dynamics models

Thrust II output: cyber defense decision-making tools & instruments etc.

Thrust II: *Data- , policy- and mechanism-driven* characterization studies

Cyber system (of systems)

Real world

Publications:

(see http://www.cs.utsa.edu/~shxu/socs/index.html for more recent ones)

Red color: used as examples today (rest of the talk)

- ❑ Push- and Pull-based Epidemic Spreading in Networks: Thresholds and Deeper Insights. ACM Transactions on Autonomous and Adaptive Systems (ACM TAAS), 7(3), 2012
- ❑ A Stochastic Model of Active Cyber Defense Dynamics, Internet Mathematics, accepted
- ❑ Optimizing Active Cyber Defense, GameSec'13
- ❑ Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study, IEEE Transactions on Information Forensics & Security (IEEE TIFS), 8(11): 1775-1789 (2013)
- ❑ An Extended Stochastic Model for Quantitative Security Analysis of Networked Systems. Internet Mathematics, 8(3): 288-320 (2012)
- ❑ L-hop percolation on networks with arbitrary degree distributions and its applications. Physical Review E 84, 031113 (2011)
- ❑ A Stochastic Model of Multi-Virus Dynamics. IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), 9(1): 30-45 (2012).
- ❑ Adaptive Epidemic Dynamics in Networks: Thresholds and Control. ACM Transactions on Autonomous and Adaptive Systems (ACM TAAS), 2014
- ❑ A Stochastic Model for Quantitative Security Analysis of Networked Systems. IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), 8(1): 28-43 (2011).

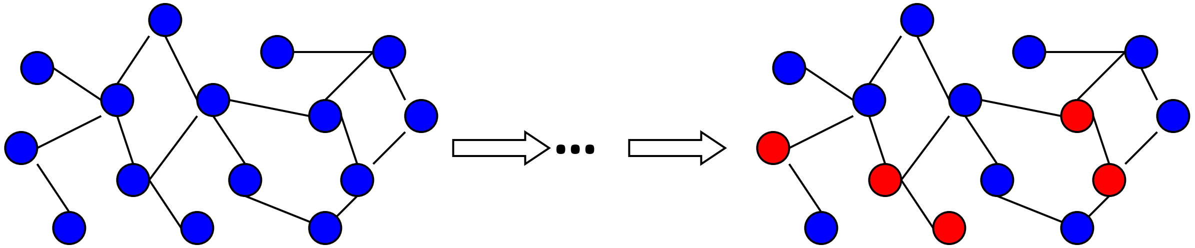
When the Vision Becomes Real …

- Cyber defense operators can make principled quantitative decisions (based on predicted threats).
- We cannot eliminate all attacks and guarantee zero compromises; but, as long as we can control the degree of compromise below to a threshold (e.g., <1/3), we can at least manage (i.e., tolerate) them.
- Two analogies:
  - We cannot prevent all crimes; but, as long as it is low enough …
  - We cannot prevent all people from being sick; but , as long as most people survive …

Roadmap

- ❑ Vision for Cybersecurity Dynamics Foundation
- ❑ Example Results Towards Fulfilling the Vision
  - ❖ Limitation of Preventive & Reactive Defense
  - ❖ Overcoming the Limitation w/ Active Defense
  - ❖ Optimizing Active Defense
- ❑ Challenges Ahead: Tackling Technical Barriers

Dynamics: Evolution of Sec. State



(● secure node ● compromised node)

- Can be instantiated at multiple resolutions: nodes represent (for example) computer, component, etc.

- Topology can be arbitrary in real-life: from complete graph to any structure

Dynamics: Push- and Pull-based Attacks against Preventive & Reactive Defense

[ACM Transactions on Autonomous and Adaptive Systems, 2012]

G is called attack-defense interaction structure, which is a complex network, capturing who (or which node) can attack whom (which other nodes).

G is often not the same as the underlying physical network structure.

G always exists, although obtaining G is an important problem that is assumed away for now.

This is sufficient for characterization studies as we do not make any restriction on G's topology.

Dynamics: Push- and Pull-based Attacks against Preventive & Reactive Defense

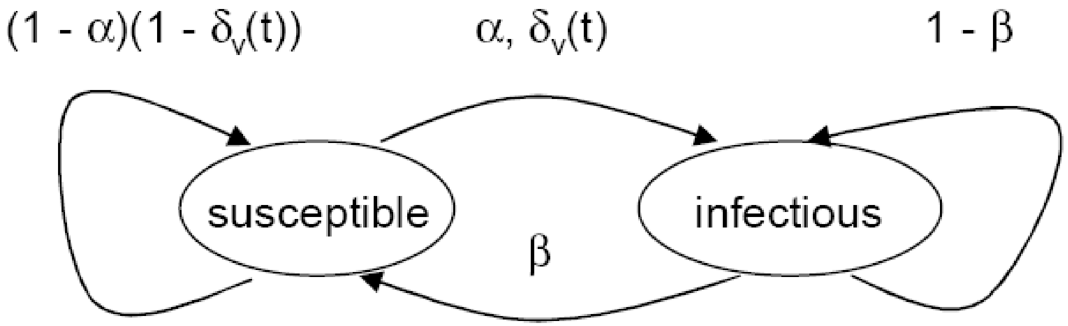
Model parameter:

- α: Pull-based infection capability, namely the probability a secure node becomes compromised at a discrete time step because of its own activity (e.g., connecting to a malicious website which may not belong to G).

- γ: The push-based infection capability, namely the probability an compromised node u successfully infects a secure node v, where $(u, v) \in E$.

- β: The cure capability, namely the probability an compromised node becomes secure at a single time step.

Dynamics: Push- and Pull-based Attacks against Preventive & Reactive Defense



State transition diagram for individual node v∈V

The master equation of the nonlinear dynamical system is

$$\begin{cases} s_v(t+1) &= [(1-\alpha)(1-\delta_v(t))]\, s_v(t) + \beta i_v(t) \\ \boxed{i_v(t+1) = [1-(1-\alpha)(1-\delta_v(t))]\, s_v(t) + (1-\beta) i_v(t).} \end{cases}$$

where

Need to analyze: How does the probability that node v is compromised at time t evolves?

Difficulty: There are ~10^6 or ~10^9 nodes!

Dynamics: Push- and Pull-based Attacks against Preventive & Reactive Defense

Stable equilibrium is perhaps necessary for cybersecurity measurement.

Theorem:

Caveat: Expected portion of compromised nodes converges to equilibrium does not necessarily mean every evolution instance behaves that way.

Fundamentally because of the mean-field analysis.

Higher-order moments are definitely important, but much harder to derive (work-in-progress).

Dynamics: Push- and Pull-based Attacks against Preventive & Reactive Defense

Stable equilibrium is perhaps necessary for cybersecurity measurement.

Theorem:

(a more succinct sufficient condition under which the dynamics will become stable) Let $m = \max_{v \in V} \deg(v)$.

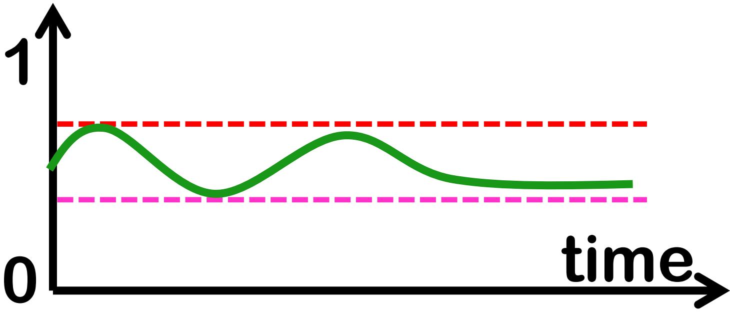
In the case $\beta < (1-\alpha)(1+(1-\gamma)^m)/2$, *if*

Insight: Largest eigenvalue of the adjacency matrix of the attack-defense interaction structure, which is a complex network, plays an important role in governing the evolution of security state.

This is how Algebraic Graph Theory comes to play

then the dynamic system is globally stable.

Bounding the Equilibrium State:



Tackling the Scalability Barrier Analytically

It is hard to compute the equilibrium state because of pull attacks. Can we bound it?

Theorem 3

Let $\overline{\lim}_{t\to\infty} i_v(t)$ *denote the upper bound of the limit of* $i_v(t)$*, and* $\underline{\lim}_{t\to\infty} i_v(t)$ *denote the lower bound of the limit of* $i_v(t)$*. Then, we have* $\overline{\lim}_{t\to\infty} i_v(t) \le \theta_v^+$ *and* $\underline{\lim}_{t\to\infty} i_v(t) \ge \theta_v^-$*, where*

$$\theta_v^+ = \frac{1-(1-\alpha)(1-\gamma)^{\deg(v)}}{\min\{1+\beta-(1-\alpha)(1-\gamma)^{\deg(v)}, 1\}},$$

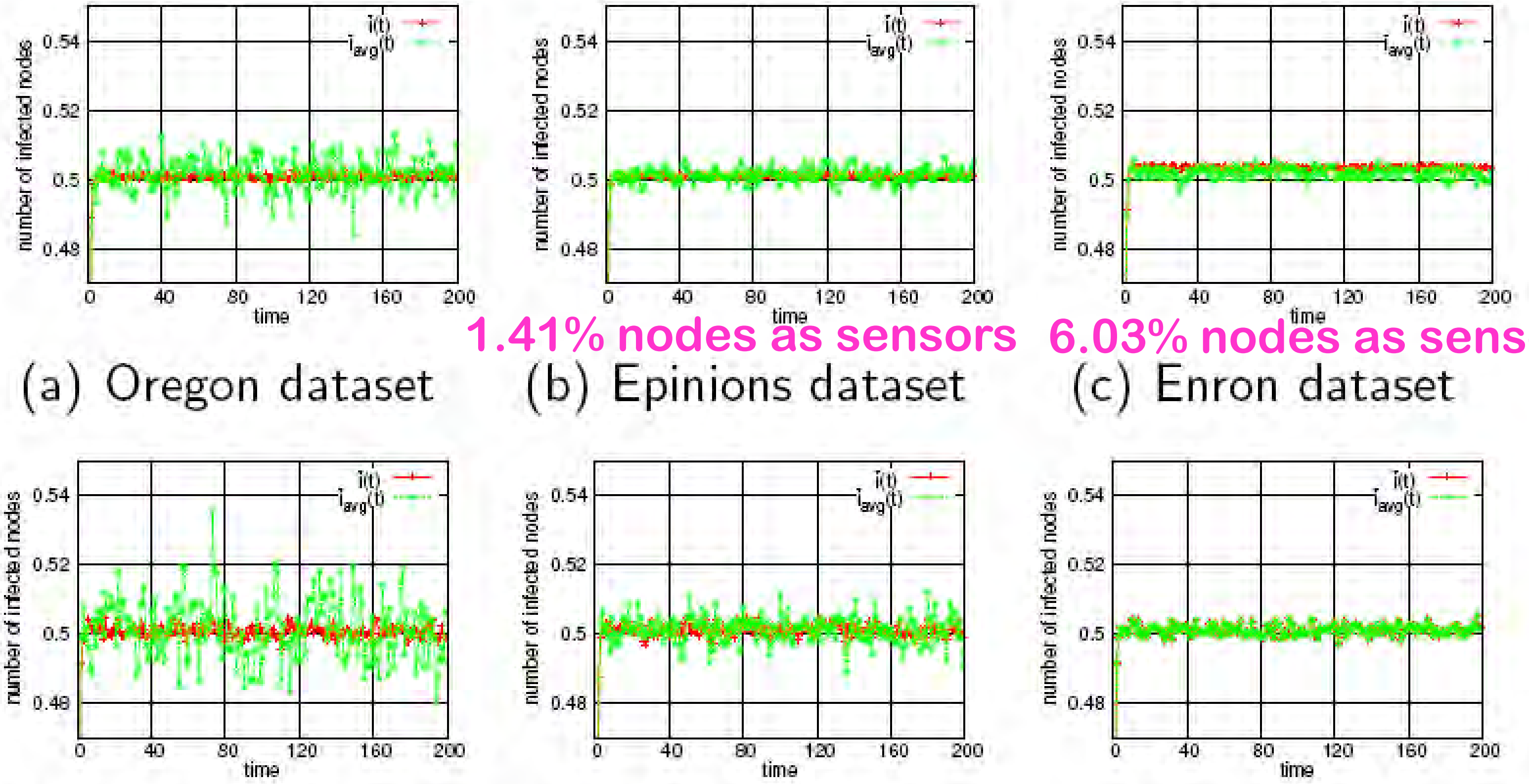
$$\theta_v^- = \begin{cases} \frac{1-(1-\alpha)(1-\gamma\nu)^{\deg(v)}}{1+\beta-(1-\alpha)(1-\gamma\nu)^{\deg(v)}} & (1-\alpha)(1-\gamma\nu)^{\deg(v)} \ge \beta \\ ((1-\alpha)(1-\gamma\nu)^{\deg(v)} - \beta)\theta_v^+ + 1 - (1-\alpha)(1-\gamma\nu)^{\deg(v)} & \textit{otherwise} \end{cases},$$

with $\nu = \min\{1-\beta, \alpha\}$.

Tackling the Scalability Barrier via Sampling:

How Theory May Guide Practice

Estimating global state from O(|V|) localized sensors/monitors.



1.41% nodes as sensors

6.03% nodes as sensors

(a) Oregon dataset

(b) Epinions dataset

(c) Enron dataset

(d) Power-law graph

(e) Random graph

(f) Regular graph

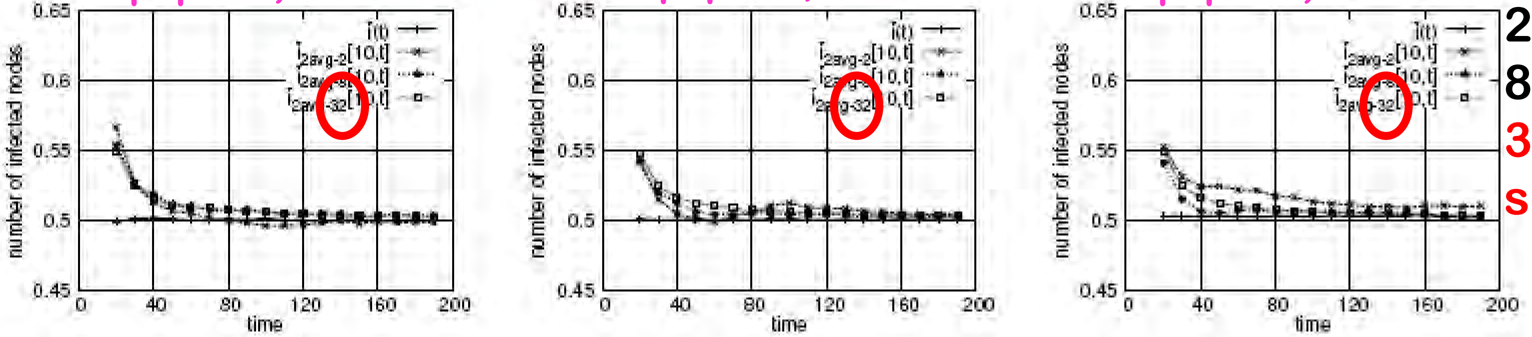
Figure 3 : $\bar{i}(t)$ vs. $\bar{i}_{avg}(t)$

Tackling the Scalability Barrier via Constant Sensors: How Theory May Guide Practice

|V|=11,461

|V|=75,879

|V|=36,692



2
8
32
sensors

(a) Oregon dataset

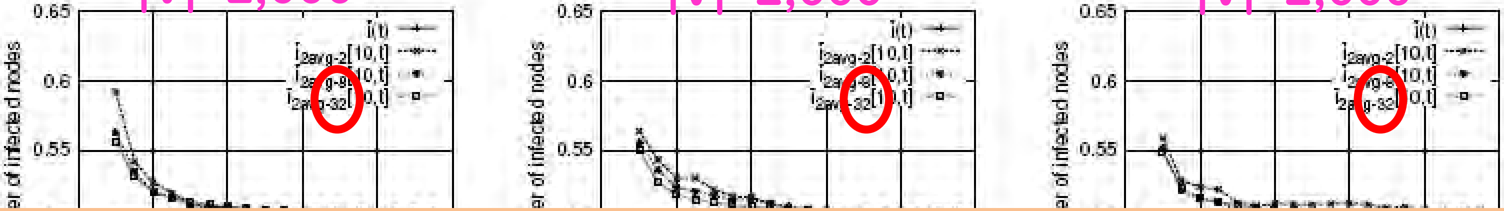
(b) Epinions dataset

(c) Enron dataset

|V|=2,000

|V|=2,000

|V|=2,000



2
8
32
sensors

Implication: It is possible to derive global cybersecurity state from o(|V|) or even constant number of sensors.

Limitation of Preventive & Reactive Defense

The Cyber Attack Amplification Phenomenon:

The preceding results say that the power of push and pull attack is amplified by a function of $\lambda_{1,A}$ of the adjacency matrix.

Insight: Cyber attack effect is automatically amplified by the network, which explains one kind of attack-defense asymmetry.

$\lambda_{1,A}$ is a sort of communicability or connectivity measure (needs to be precisely characterized).

Implication: There is possibly a fundamental trade-off between communicability and resilience under preventive & reactive defense against push- and pull-based attacks.

Limitation of Preventive & Reactive Defense

How can we deal with the limitation?

- ❑ The straightforward way is to reduce the network radius (e.g., communicability or network connectivity).
- ❑ An alternative: active cyber defense

Roadmap

- ❑ Vision for Cybersecurity Dynamics Foundation
- ❑ Example Results Towards Fulfilling the Vision
  - ❖ Limitation of Preventive & Reactive Defense
  - ❖ Overcoming the Limitation w/ Active Defense
  - ❖ Optimizing Active Defense
- ❑ Challenges Ahead: Tackling Technical Barriers

Active Cyber Defense Dynamics

[Paper: In Internet Mathematics, to appear]

Active defense: Using goodware (e.g., white worm) or its like to kill malware

- Also an automated tool for "clean up" networks

A cyber system is again abstracted as a finite (un)directed graph $G = (V, E)$,

- G can have any topology and always exists.

At any time t, $v \in V$ is in one of two states: blue (occupied by defender) or red (occupied by attacker).

The combat between attacker and defender takes place over G, where v's state changes because of u with $(u, v) \in E$.

The Native Markov Process Model

The state of v at time t is random variable $\xi_v(t) \in \{0, 1\}$:

$$\xi_v(t) = \begin{cases} 1 & v \in V \text{ is blue at time } t \\ 0 & v \in V \text{ is red at time } t. \end{cases}$$

Correspondingly, we define

$$B_v(t) = \mathrm{P}(\xi_v(t) = 1) \quad \text{and} \quad R_v(t) = \mathrm{P}(\xi_v(t) = 0).$$

Denote by $\tilde{\theta}_{v,BR}(t)$ the rate at which v changes from blue to red at time t, which is a random variable because it depends on the states of v's neighbors.

Denote by $\tilde{\theta}_{v,RB}(t)$ the random rate at which v changes from red to blue at time t.

The Native Markov Process Model (cont.)

The state evolution of $v \in V$ is naturally described by a Markov process with ransition probabilities:

$$\mathrm{P}(\xi_v(t + \Delta t) = 1 \big| \xi_v(t))$$

$$= \begin{cases} \Delta t \cdot \tilde{\theta}_{v,RB}(t) + o(\Delta t) & \xi_v(t) = 0 \\ 1 - \Delta t \cdot \tilde{\theta} \quad (t) + o(\Delta t) & \xi \ (t) = 1 \end{cases}$$

Analysis difficulty:

The scalability barrier: It has 2^n states and is nonlinear in general!

Approach:

Simply (i.e., approximate) it as a Dynamical System model

From Markov Model to Dynamic System Model

By letting $\Delta t \to 0$, we have

$$\begin{cases} \frac{dB_v(t)}{dt} = \tilde{\theta}_{v,RB}(t) \cdot R_v(t) - \tilde{\theta}_{v,BR}(t) \cdot B_v(t) \\ \frac{dR_v(t)}{dt} = \tilde{\theta}_{v,BR}(t) \cdot B_v(t) - \tilde{\theta}_{v,RB}(t) \cdot R_v(t). \end{cases} \quad (5)$$

Via mean-field approximation, we can replace the random rates $\tilde{\theta}_{v,BR}(t)$ and $\tilde{\theta}_{v,RB}(t)$ with their mean values $\theta_{v,BR}(t)$ and $\theta_{v,RB}(t)$, respectively. Eq. (5) becomes Dynamic System:

$$\begin{cases} \frac{d}{dt}B_v(t) = \theta_{v,RB}(t) \cdot R_v(t) - \theta_{v,BR}(t) \cdot B_v(t) \\ \frac{d}{dt}R_v(t) = \theta_{v,BR}(t) \cdot B_v(t) - \theta_{v,RB}(t) \cdot R_v(t). \end{cases} \quad (6)$$

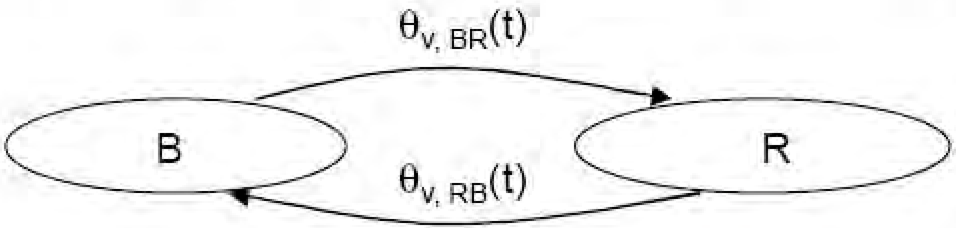


Figure 5 : State transition diagram of $v \in V$ (B: blue; R: red)

One Class of Active Cyber Defense Dynamics Models

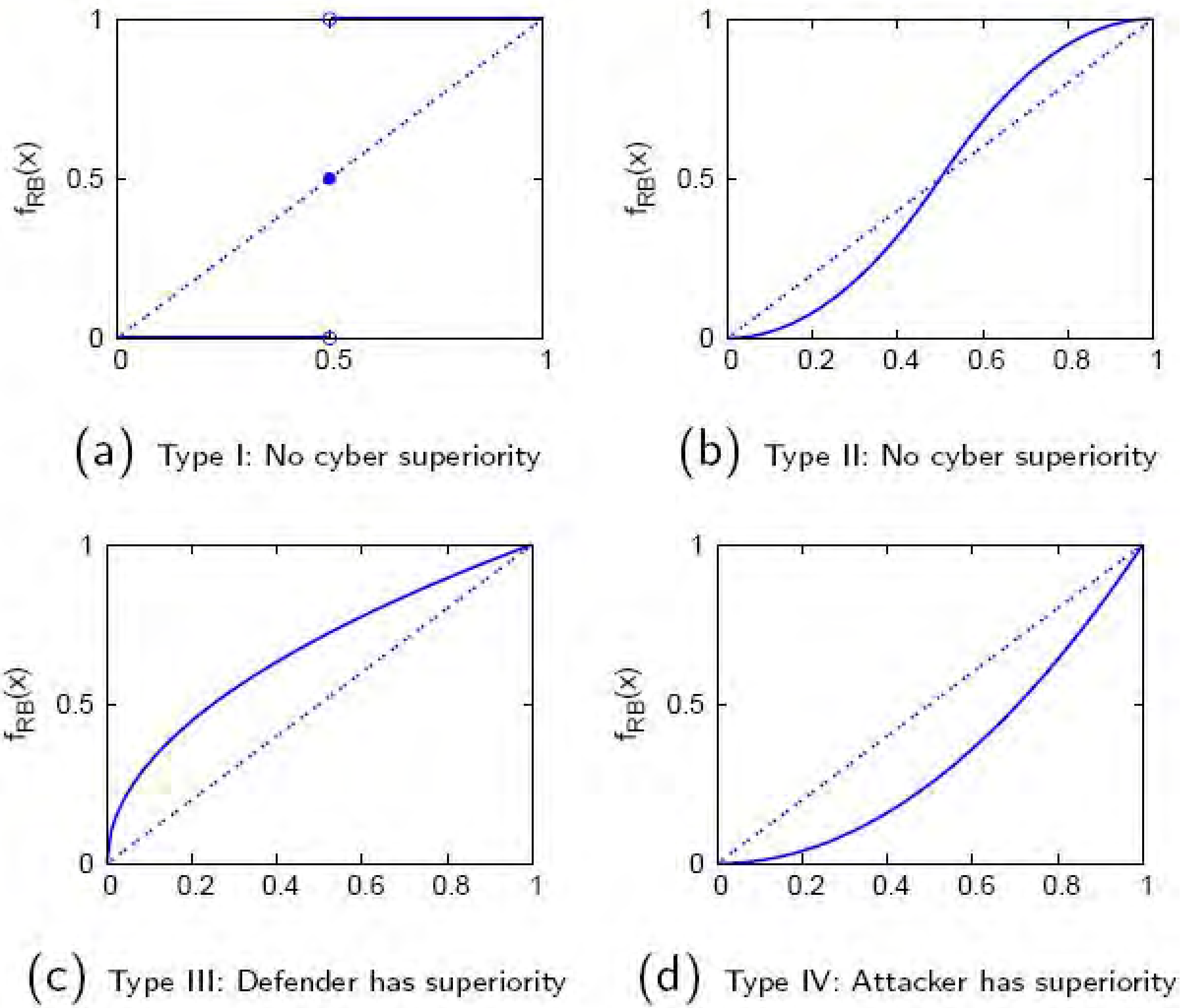
System (6) is very general because $\theta_{v,RB}(t)$ and $\theta_{v,BR}(t)$ can be defined via various combat-power functions, which abstract the defender's power/capability against the attacker.
One class of combat-power function $f_{RB}(\cdot) : \mathbb{R} \to [0,1]$ is:

$$\theta_{v,RB}(t) = f_{RB}\left(\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(t)\right),$$

where $f_{RB}(0) = 0$, $f_{RB}(1) = 1$, and $f_{RB}(\cdot)$ increases monotonically.

Intuition: The more blue nodes active-defending against a red node, the greater the chance the red node will be cleaned up.

Four Types of Combat-Power Functions



(a) Type I: No cyber superiority

(b) Type II: No cyber superiority

(c) Type III: Defender has superiority

(d) Type IV: Attacker has superiority

Figure 6 : Examples of combat-power function $f_{RB}(\cdot)$

Characterizing Type I Dynamics with Node-Independent Occupation Posture $B_v(0)$

Theorem 5

(a sufficient condition for one party to occupy the entire network) Consider Type I dynamics in **arbitrary** *network* $G = (V, E)$ *with parameter* σ. *If* $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(0) > \sigma$ *for all* $v \in V$, $\lim_{t \to \infty} B_v(t) = 1$; *if* $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(0) < \sigma$ *for all* $v \in V$, $\lim_{t \to \infty} B_v(t) = 0$.

Insight *1*

When is active cyber defense useful?

When the defender is not superior to the attacker in cyber combat, active defense can effectively "clean up" a compromised network only after the defender has occupied more than threshold σ *portion of the networks. In other words, the defender can first use an expensive procedure to manually "clean up" a threshold* σ *portion of the network, and then use active defense to automatically "clean up" the entire network.*

Characterizing Type I Dynamics with Node-Independent Occupation Posture $B_v(0)$

Theorem 6

(a sufficient condition under which no party can occupy the entire network) Consider Type I dynamics in clustered **arbitrary** *network $G = (V, E)$ with parameter σ. Let $B_v(0) = \alpha_k$ for every $v \in V_k$ and β_k be the minimum node expansion as defined in Eq. (11). If $\alpha_k \beta_k > \sigma$, all nodes in V_k will become* blue*; if $(1 - \alpha_k)\beta_k > 1 - \sigma$, all nodes in V_k will become* red*.*

When is active cyber defense useful?

Insight 2

In clustered networks, active defense may only be able to "clean up" some, but not all, clusters/portions of compromised networks.

Characterizing Type I Dynamics with Degree-dependent Occupation Posture $B_v(0)$

The proceeding analysis applies to node-independent initial occupation posture $B_v(0)$, where the defender does not play strategy (e.g., better defending the more important nodes).

This serves as baseline understanding.

What if the defender (or attacker) play strategically?

Hard to analyze in general (because of the dependence!).

Approach: Use the generalized random graph model

Advantage of Strategic Defender: $B_v(0) \propto \deg(v)$

Define

$$\alpha_{threshold} = \frac{\sigma}{n} \frac{[\sum_{u \in V(n)} \deg(u)]^2}{\sum_{v \in V(n)} \deg(v)^2}, \qquad (14)$$

where $\deg(v)$ is the (in-)degree of node $v \in V(n)$. Theorem 8 implies the following: if $\frac{|S|}{n} > \alpha_{threshold}$, then $\lim_{t \to \infty} B_v(t) = 1$ for $v \in V(n)$; if $\frac{|S|}{n} < \alpha_{threshold}$, then $\lim_{t \to \infty} B_v(t) = 0$ for $v \in V(n)$. Since $\frac{[\sum_{u \in V(n)} \deg(u)]^2}{\sum_{v \in V(n)} \deg(v)^2} \leq n$, we have $\alpha_{threshold} < \sigma$.

Insight 4

When is active cyber defense useful?

If (i) the large-degree nodes are appropriately better protected, namely that the probabilities that they are secure initially are proportional to their degrees, and (ii) the attacker has not compromised too many nodes (more than $1 - \alpha_{threshold} > 1 - \sigma$ portions of the network), the defender can still use active defense to automatically "clean up" the network.

Consequence of Strategic Attacker: $R_v(0) \propto \deg(v)$

The blue-node initial occupation threshold is

$$\beta_{threshold} = 1 - \frac{1-\sigma}{n} \frac{\left[\sum_{v \in V} \deg(v)\right]^2}{\sum_{v \in V} \deg(v)^2}. \qquad (15)$$

If $\frac{|S|}{n} > \beta_{threshold}$, then $\lim_{t \to \infty} B_v(t) = 1$; if $\frac{|S|}{n} < \beta_{threshold}$, then $\lim_{t \to \infty} B_v(t) = 0$.
We have $\beta_{threshold} > \sigma$.

Insight *5*

When is active cyber defense useful?

If large-degree nodes are compromised with probabilities proportional to their degrees, the defender can use active defense to "clean up" the network only after occupying $\beta_{threshold} > \sigma$ portions of the network.

Quantifying Advantage of Strategic Defender/Attacker

Now we know strategic player has some advantage:

- If the defender strategically occupies the large-degree nodes, active defense is still effective even if the defender occupied $\alpha_{threshold} < \sigma$ portions of the nodes.
- If the attacker strategically occupies the large-degree nodes, active defense is effective only after the defender occupied $\beta_{threshold} > \sigma$ portions of the nodes.

How significant are the benefits? Can we quantify it?

Yes, we can (see paper for details)!

Active Defense Dismisses the Attack Amplication Phenomenon

In any case, asymmetry disappears with active defense because the largest eigenvalue of the adjacency matrix (indeed, any other measures) does not play any significant role in governing the outcome of active cyber defense dynamics.

Insight *10*

Active cyber defense dismisses the attack amplification phenomenon that is exhibited by reactive defense.

A Further Result: Paper in Submission

- □ We show: active cyber defense dynamics exhibits rich phenomena: Bifurcation and Chaos

- □ Implication: There exists some fundamental limit on cybersecurity measurementability and predictability.

- □ Further Implication: We need to manipulate cybersecurity dynamics (if possible/feasible) to avoid such “unmanageable” situations.

- □ This is how Control Theory and Game Theory naturally come to play (under the umbrella of Optimization).

Roadmap

- ❑ Vision for Cybersecurity Dynamics Foundation
- ❑ Example Results Towards Fulfilling the Vision
  - ❖ Limitation of Preventive & Reactive Defense
  - ❖ Overcoming the Limitation w/ Active Defense
  - ❖ Optimizing Active Defense
- ❑ Challenges Ahead: Tackling Technical Barriers

Optimizing Active Defense

[Paper: GameSec’13]

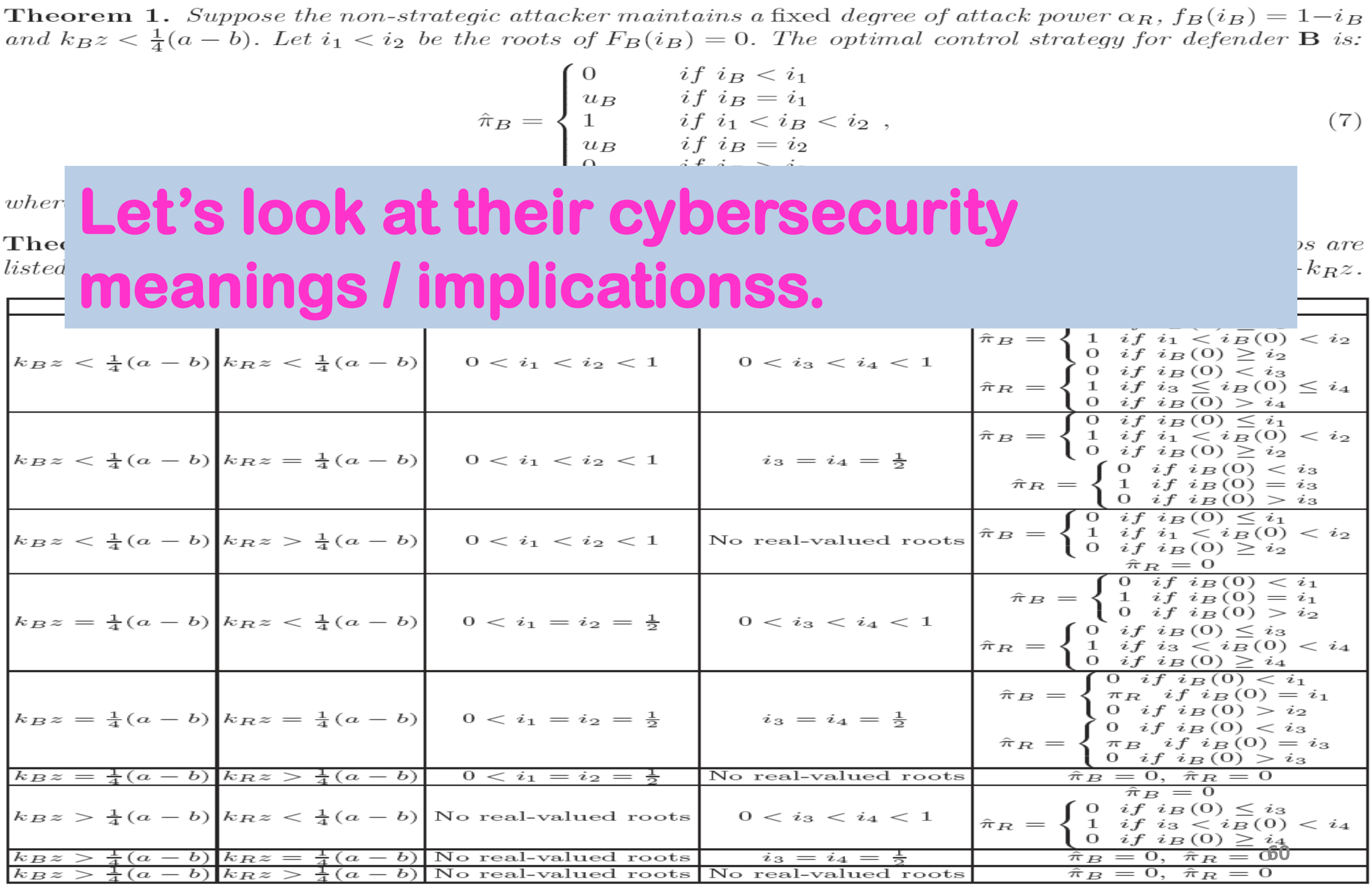
For now, we assume away the attack-defense interaction graph structure.

- ❑ Equivalent to “homogeneous mixing” assumption

Below is a highlight of some model-derived insights.

- ❑ Optimal Control and Game Theory models

Example Results



Theorem 1. *Suppose the non-strategic attacker maintains a* fixed *degree of attack power* α_R, $f_B(i_B) = 1 - i_B$ *and* $k_B z < \frac{1}{4}(a-b)$. *Let* $i_1 < i_2$ *be the roots of* $F_B(i_B) = 0$. *The optimal control strategy for defender* **B** *is:*

$$\hat{\pi}_B = \begin{cases} 0 & if\ i_B < i_1 \\ u_B & if\ i_B = i_1 \\ 1 & if\ i_1 < i_B < i_2 \\ u_B & if\ i_B = i_2 \\ 0 & if\ i_B > i_2 \end{cases}, \qquad (7)$$

wher

The *ps are*

listed $- k_R z$.

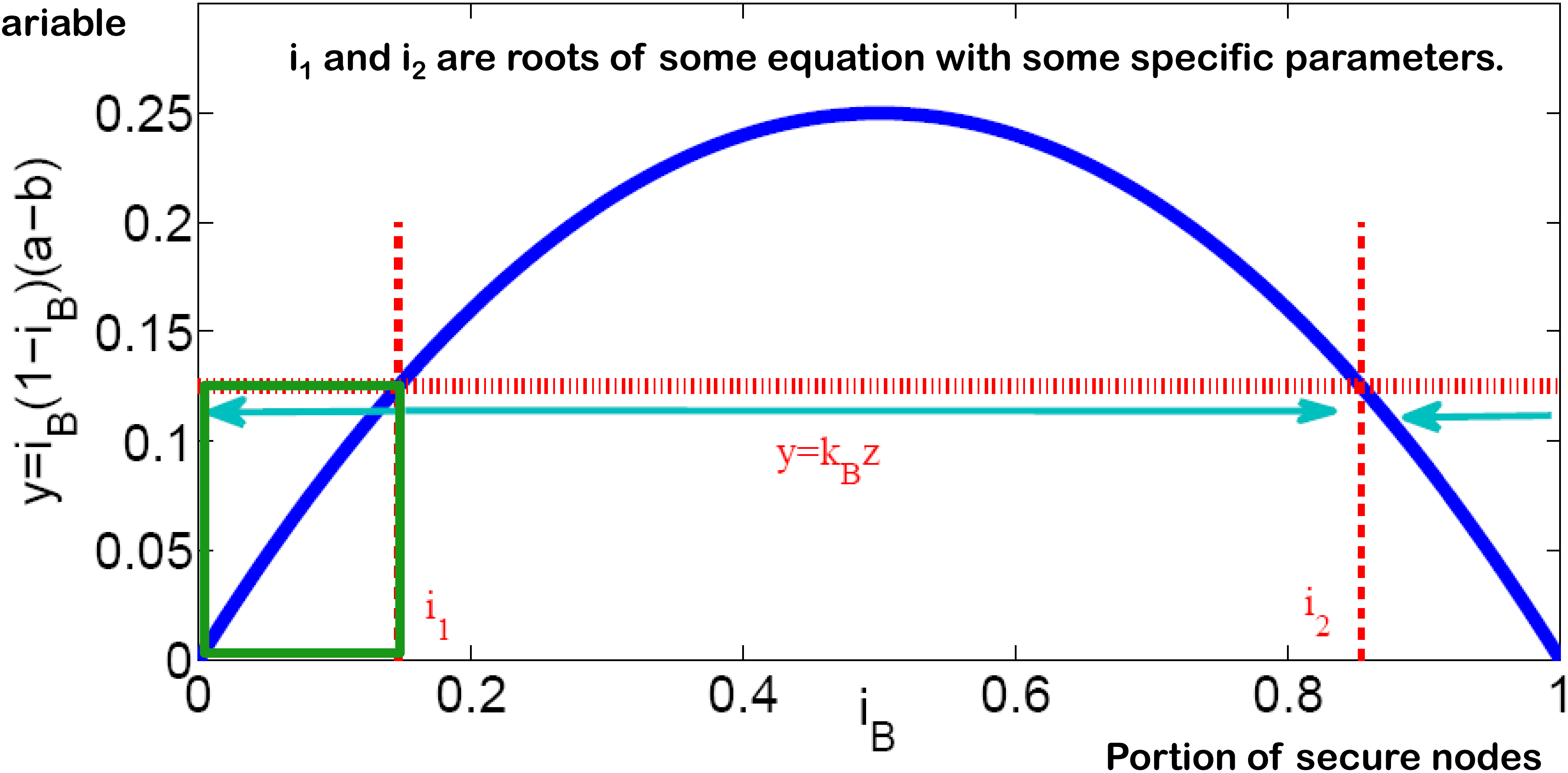
$k_B z < \frac{1}{4}(a-b)$	$k_R z < \frac{1}{4}(a-b)$	$0 < i_1 < i_2 < 1$	$0 < i_3 < i_4 < 1$	$\hat{\pi}_B = \begin{cases} 1 & if\ i_1 < i_B(0) < i_2 \\ 0 & if\ i_B(0) \geq i_2 \end{cases}$ $\hat{\pi}_R = \begin{cases} 0 & if\ i_B(0) < i_3 \\ 1 & if\ i_3 \leq i_B(0) \leq i_4 \\ 0 & if\ i_B(0) > i_4 \end{cases}$
$k_B z < \frac{1}{4}(a-b)$	$k_R z = \frac{1}{4}(a-b)$	$0 < i_1 < i_2 < 1$	$i_3 = i_4 = \frac{1}{2}$	$\hat{\pi}_B = \begin{cases} 0 & if\ i_B(0) \leq i_1 \\ 1 & if\ i_1 < i_B(0) < i_2 \\ 0 & if\ i_B(0) \geq i_2 \end{cases}$ $\hat{\pi}_R = \begin{cases} 0 & if\ i_B(0) < i_3 \\ 1 & if\ i_B(0) = i_3 \\ 0 & if\ i_B(0) > i_3 \end{cases}$
$k_B z < \frac{1}{4}(a-b)$	$k_R z > \frac{1}{4}(a-b)$	$0 < i_1 < i_2 < 1$	No real-valued roots	$\hat{\pi}_B = \begin{cases} 0 & if\ i_B(0) \leq i_1 \\ 1 & if\ i_1 < i_B(0) < i_2 \\ 0 & if\ i_B(0) \geq i_2 \end{cases}$ $\hat{\pi}_R = 0$
$k_B z = \frac{1}{4}(a-b)$	$k_R z < \frac{1}{4}(a-b)$	$0 < i_1 = i_2 = \frac{1}{2}$	$0 < i_3 < i_4 < 1$	$\hat{\pi}_B = \begin{cases} 0 & if\ i_B(0) < i_1 \\ 1 & if\ i_B(0) = i_1 \\ 0 & if\ i_B(0) > i_2 \end{cases}$ $\hat{\pi}_R = \begin{cases} 0 & if\ i_B(0) \leq i_3 \\ 1 & if\ i_3 < i_B(0) < i_4 \\ 0 & if\ i_B(0) \geq i_4 \end{cases}$
$k_B z = \frac{1}{4}(a-b)$	$k_R z = \frac{1}{4}(a-b)$	$0 < i_1 = i_2 = \frac{1}{2}$	$i_3 = i_4 = \frac{1}{2}$	$\hat{\pi}_B = \begin{cases} 0 & if\ i_B(0) < i_1 \\ \pi_R & if\ i_B(0) = i_1 \\ 0 & if\ i_B(0) > i_2 \end{cases}$ $\hat{\pi}_R = \begin{cases} 0 & if\ i_B(0) < i_3 \\ \pi_B & if\ i_B(0) = i_3 \\ 0 & if\ i_B(0) > i_3 \end{cases}$
$k_B z = \frac{1}{4}(a-b)$	$k_R z > \frac{1}{4}(a-b)$	$0 < i_1 = i_2 = \frac{1}{2}$	No real-valued roots	$\hat{\pi}_B = 0,\ \hat{\pi}_R = 0$
$k_B z > \frac{1}{4}(a-b)$	$k_R z < \frac{1}{4}(a-b)$	No real-valued roots	$0 < i_3 < i_4 < 1$	$\hat{\pi}_B = 0$ $\hat{\pi}_R = \begin{cases} 0 & if\ i_B(0) \leq i_3 \\ 1 & if\ i_3 < i_B(0) < i_4 \\ 0 & if\ i_B(0) \geq i_4 \end{cases}$
$k_B z > \frac{1}{4}(a-b)$	$k_R z = \frac{1}{4}(a-b)$	No real-valued roots	$i_3 = i_4 = \frac{1}{2}$	$\hat{\pi}_B = 0,\ \hat{\pi}_R = 0$
$k_B z > \frac{1}{4}(a-b)$	$k_R z > \frac{1}{4}(a-b)$	No real-valued roots	No real-valued roots	$\hat{\pi}_B = 0,\ \hat{\pi}_R = 0$

Let's look at their cybersecurity meanings / implicationss.

Optimal Control for Strategic Active Defense against Non-strategic (Fixed) Attack:

infinite-time horizon optimal control (defender can use advanced tools if needed)

an intermediate variable



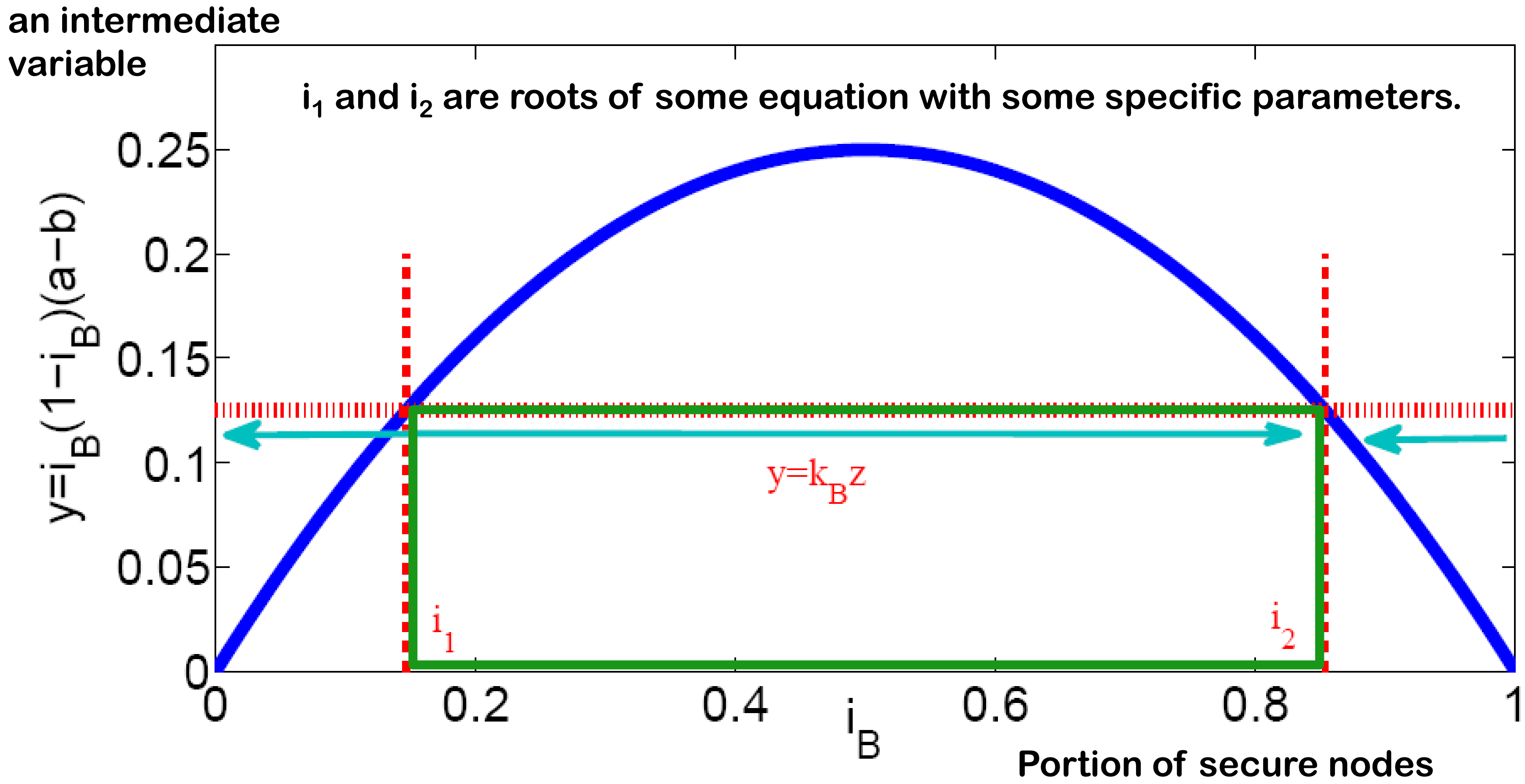
Portion of secure nodes

When the defender "occupies" less than i_1 portions of nodes, the defender should give up (active defense) and $\lim_{t\to\infty} i_B(t) = 0$

Cybersecurity meaning: incorporate other defenses!

Optimal Control for Strategic Active Defense against Non-strategic (Fixed) Attack:

infinite-time horizon optimal control (defender can use advanced tools if needed)

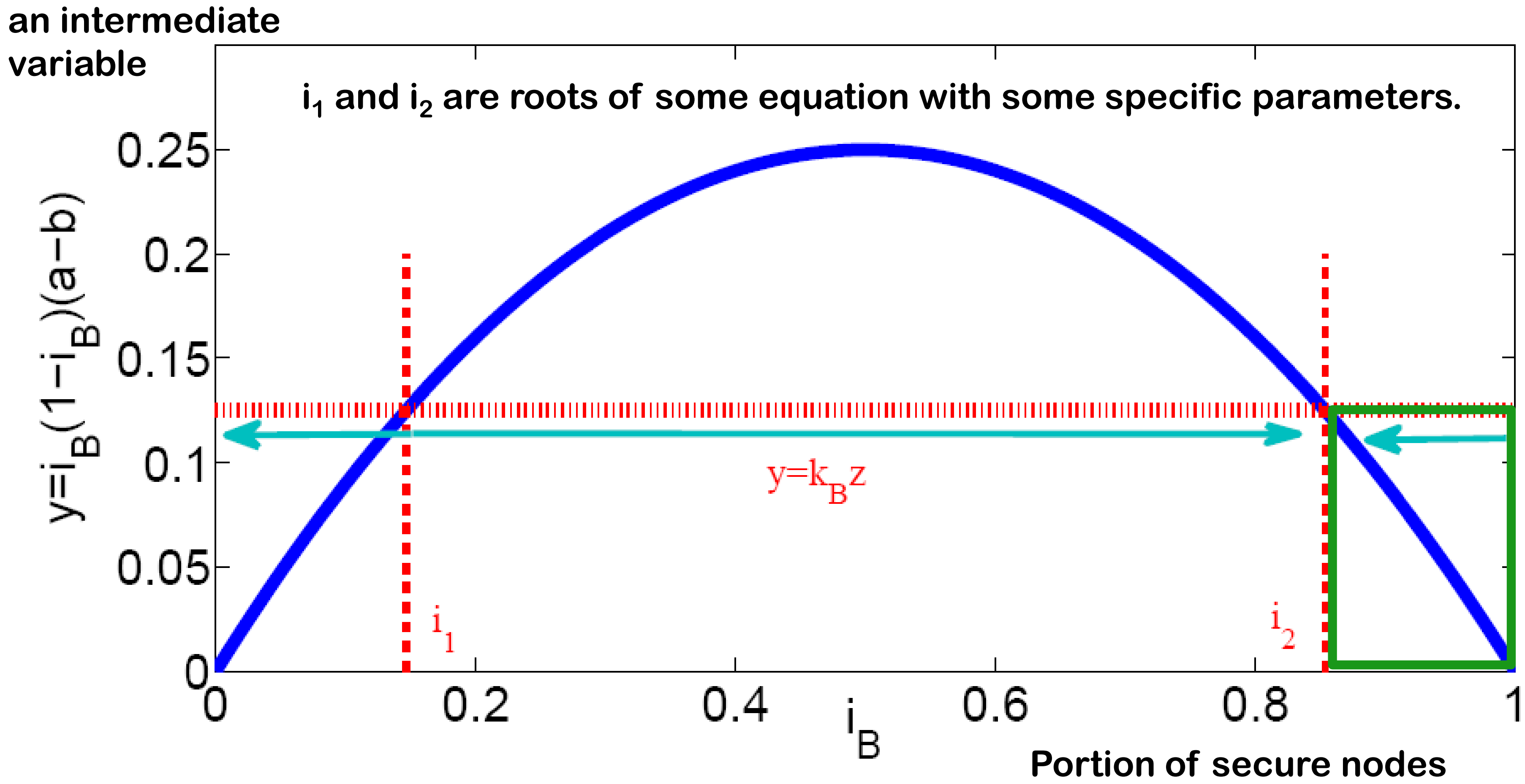


When the defender "occupies" more than i_1 but less than i_2 portions of nodes, the defender should users its best active defense tools and

$$\lim_{t\to\infty} i_B(t) = i_2$$

Optimal Control for Strategic Active Defense against Non-strategic (Fixed) Attack:

infinite-time horizon optimal control (defender can use advanced tools if needed)

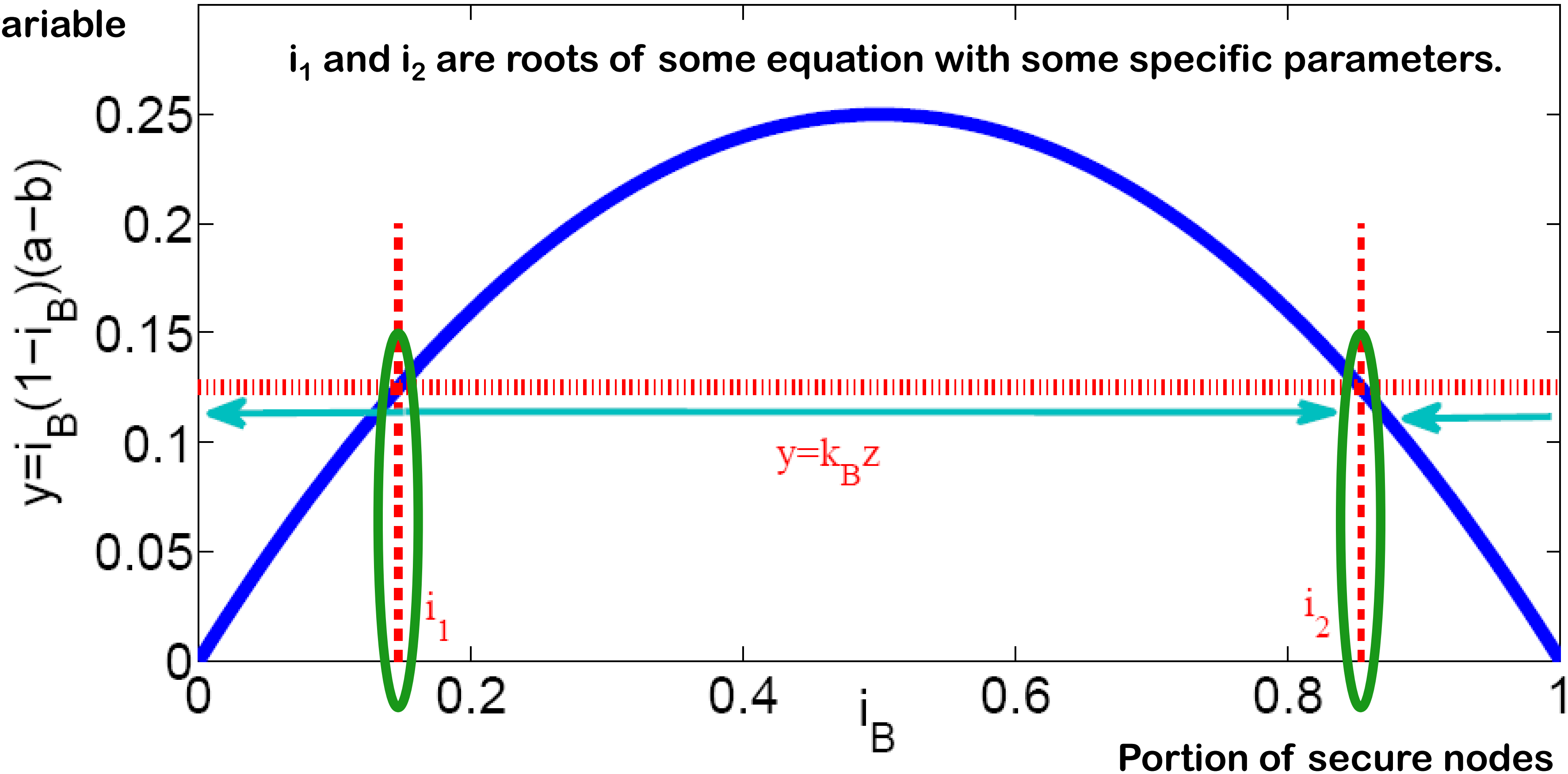


When the defender "occupies" more than i_2 portions of nodes, there is a sort of diminishing return in active defense (i.e., pursuing "good enough" security instead) and $\lim_{t\to\infty} i_B(t) = i_2$

Optimal Control for Strategic Active Defense against Non-strategic (Fixed) Attack:

infinite-time horizon optimal control (defender can use advanced tools if needed)

an intermediate variable

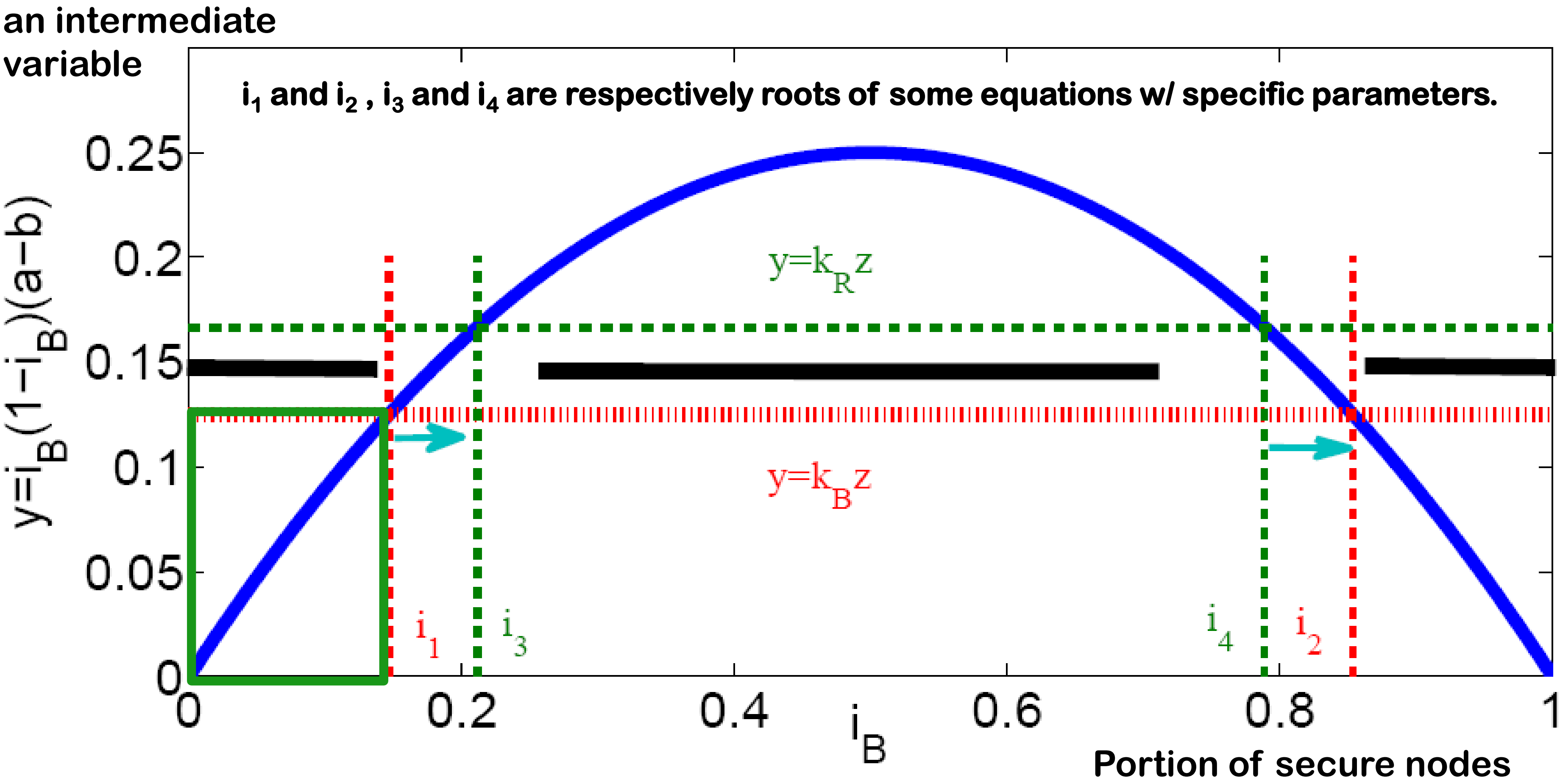


Portion of secure nodes

When the defender "occupies" exactly i_1 or i_2 portions of nodes, there is a specific way of launching active defense (based on parameters) and $i_B(t)=i_0(t)$ for any $t > 0$.

Nash Equilibrium for Strategic Active Defense against Strategic Attack:

attacker more unwilling to expose/use its 0-day (new) attack tools

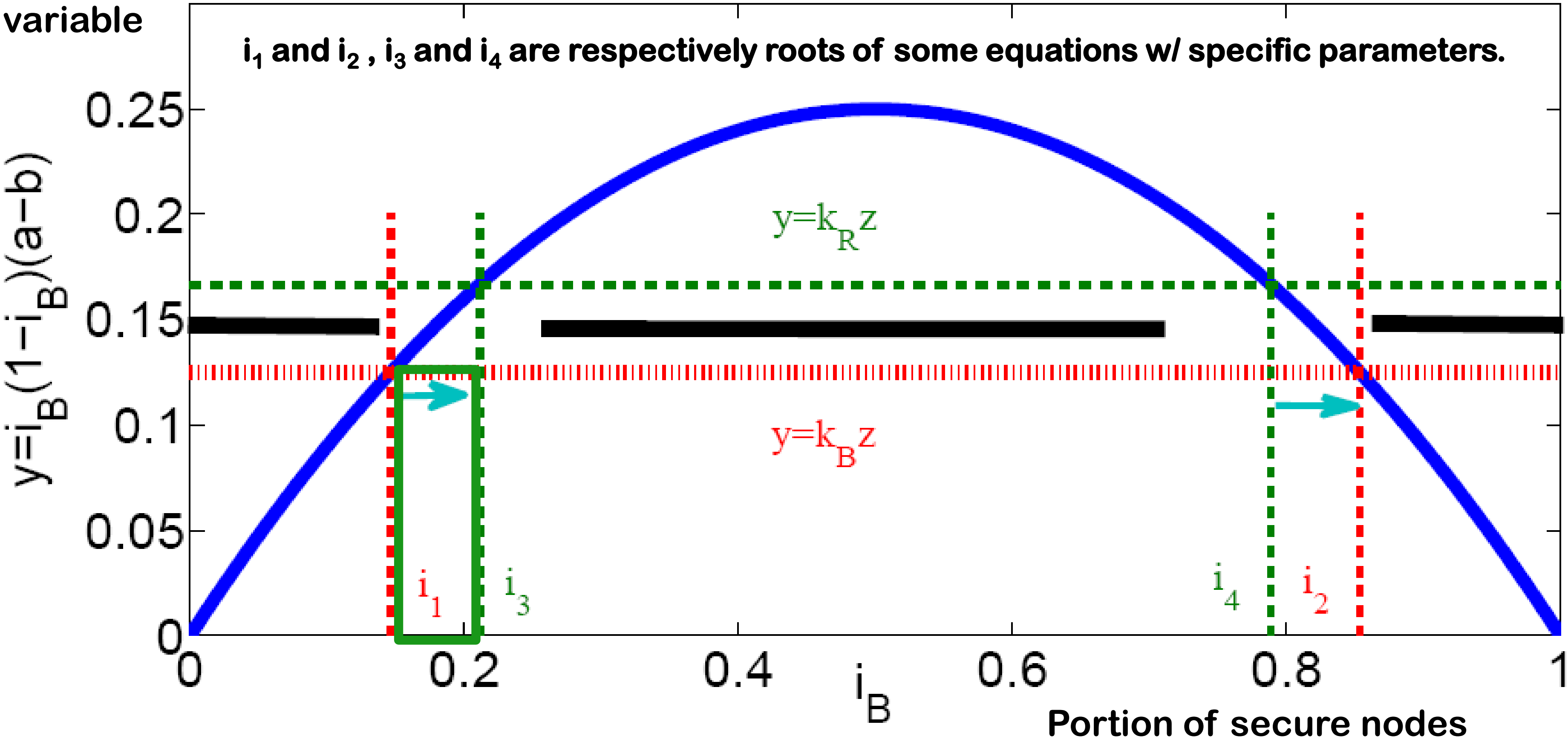


When the defender "occupies" less than i_1 portions of nodes, the NE strategy is that both attacker and defender use minimal attack/defense power. This leads to $i_B(t)=i_0(t)$ for any $t > 0$.

Nash Equilibrium for Strategic Active Defense against Strategic Attack:

attacker more unwilling to expose/use its 0-day (new) attack tools

an intermediate variable



i_1 and i_2 , i_3 and i_4 are respectively roots of some equations w/ specific parameters.

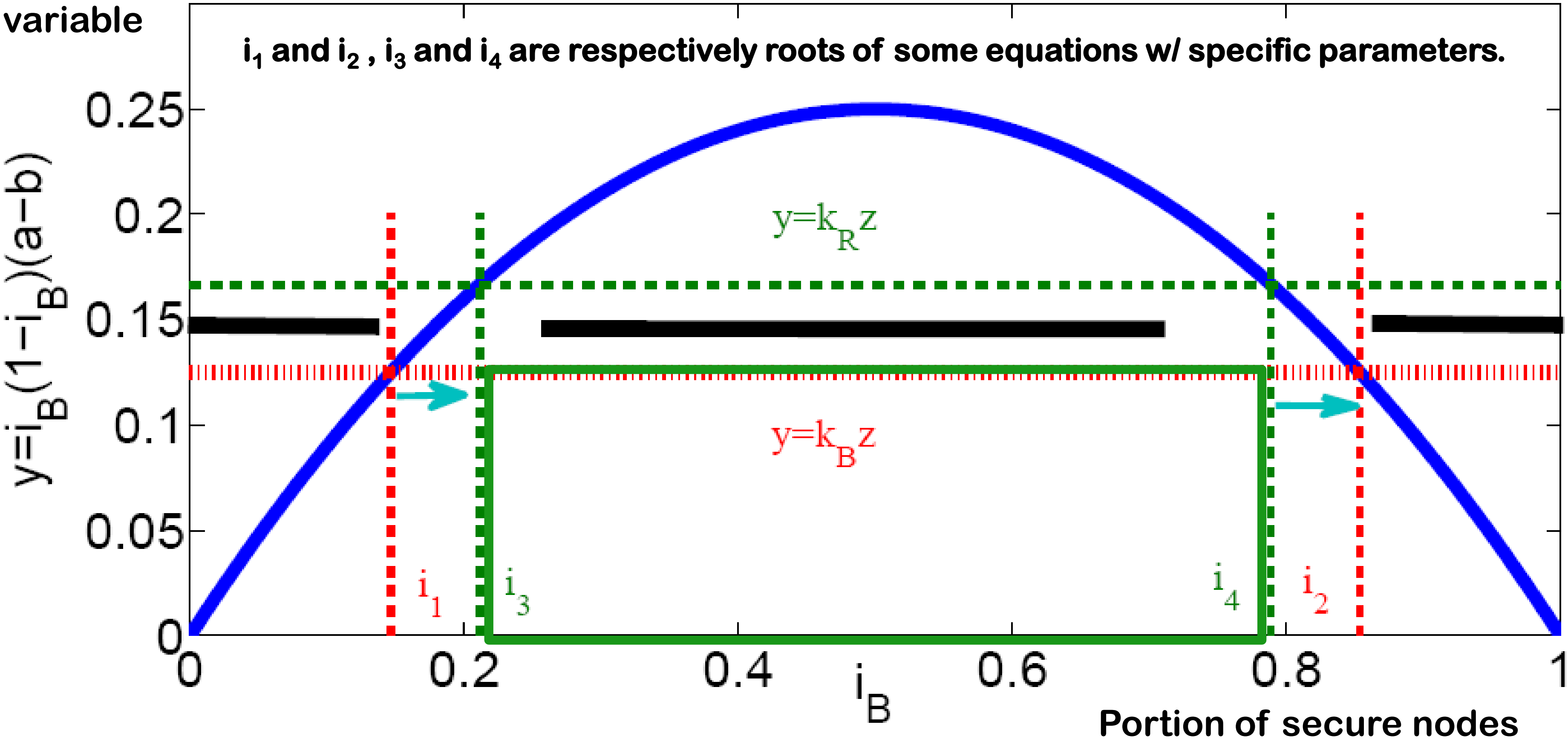
Portion of secure nodes

When defender "occupies" $>i_1$ but $< i_3$ portions of nodes, NE strategy is: defender and attacker use maximal active defense/attack until reaching $i_B(t)=i_3$. After reaching it, both maintain maximal attack/defense power.

Nash Equilibrium for Strategic Active Defense against Strategic Attack:

attacker more unwilling to expose/use its 0-day (new) attack tools

an intermediate variable

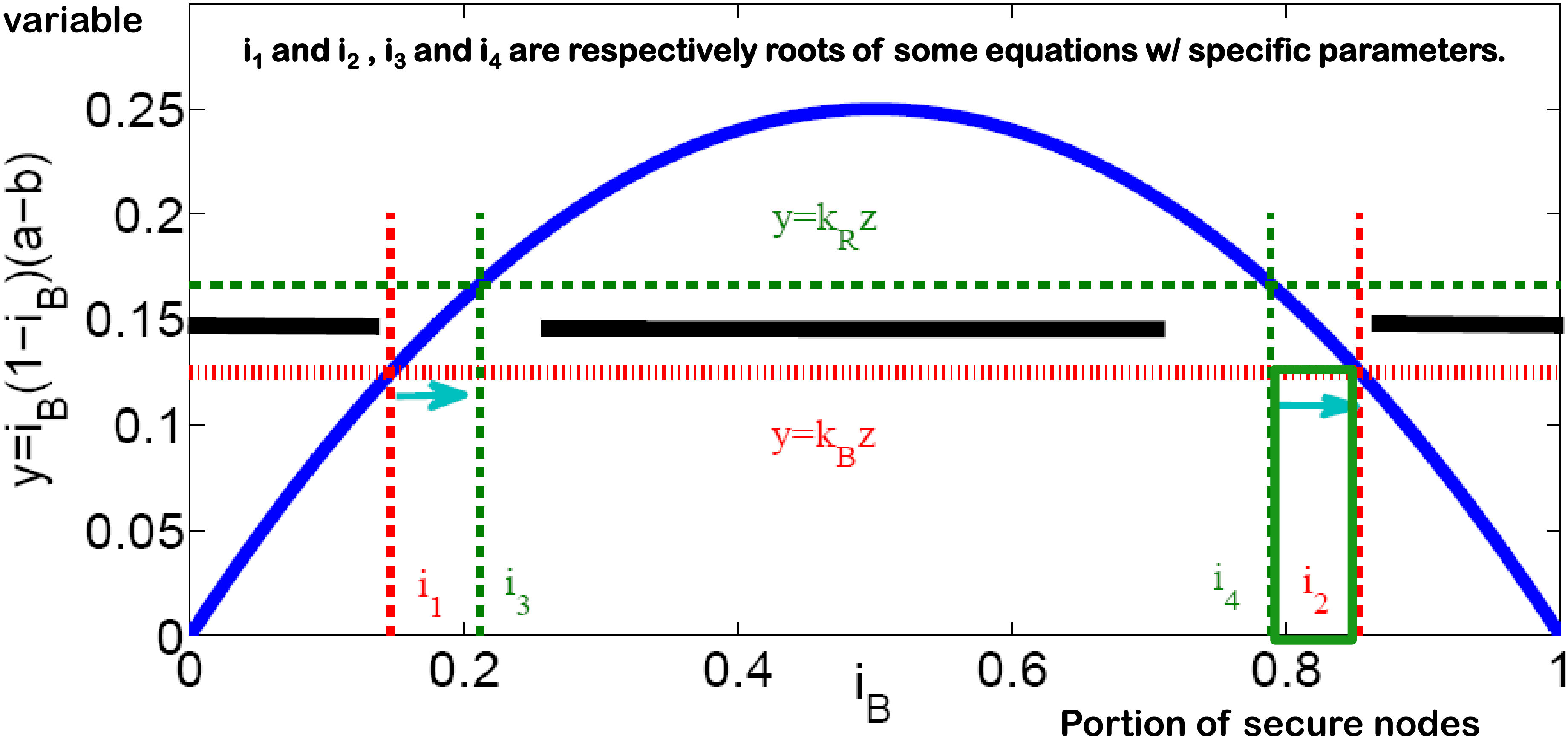


Portion of secure nodes

When defender “occupies” more than i_3 but less than i_4 portions of nodes, both defender and attacker launch their maximal attack/defense power. This results in $i_B(t)=i_0(t)$ for any t > 0.

Nash Equilibrium for Strategic Active Defense against Strategic Attack:

attacker more unwilling to expose/use its 0-day (new) attack tools



an intermediate variable

i_1 and i_2 , i_3 and i_4 are respectively roots of some equations w/ specific parameters.

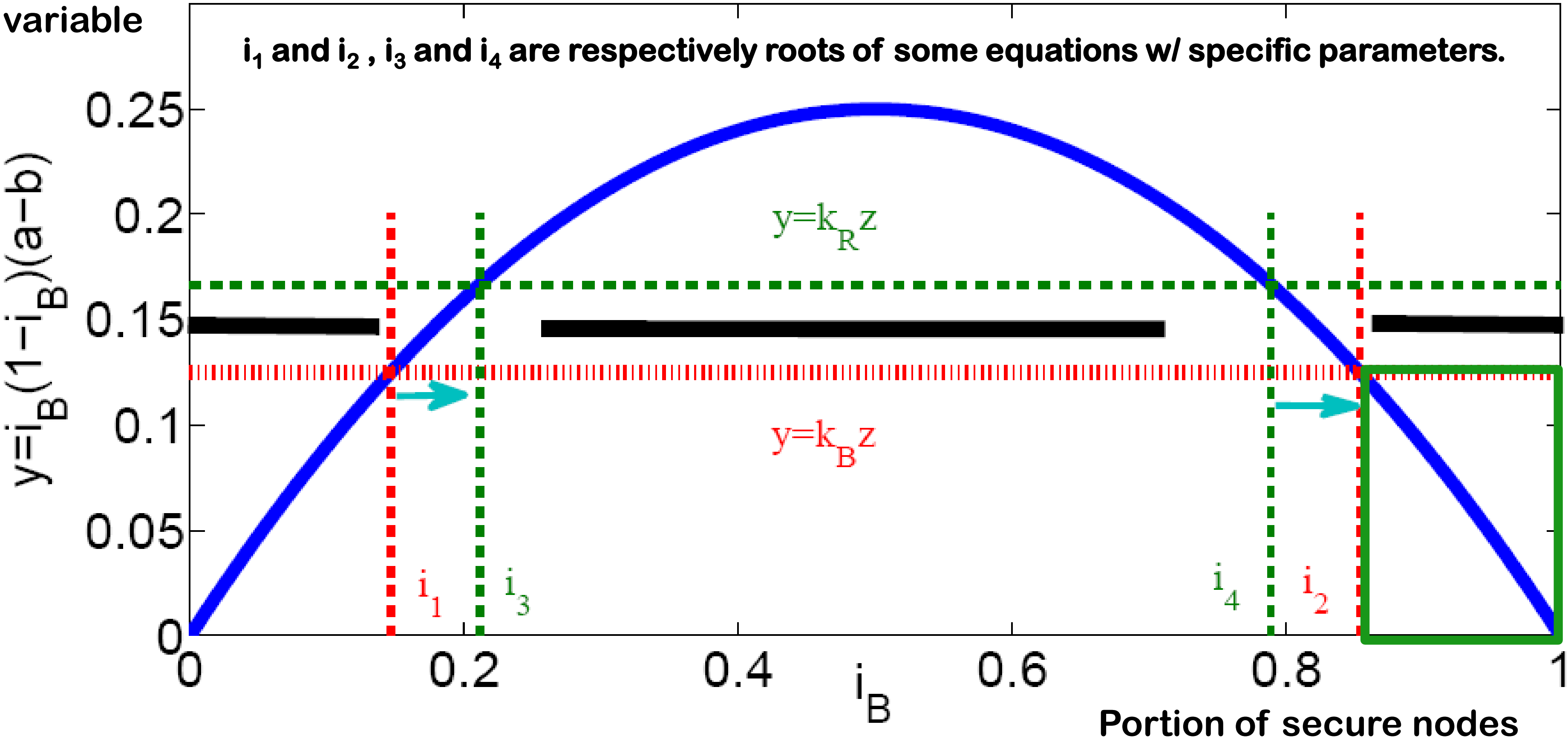
Portion of secure nodes

When defender "occupies" $>i_2$ but $< i_4$ portions of nodes, NE strategy is: defender should launch maximal active defense but attacker launches minimal attacks until reaching $i_B(t)=i_2$. After reaching it, both maintain maximal attack/defense power.

Nash Equilibrium for Strategic Active Defense against Strategic Attack:

attacker more unwilling to expose/use its 0-day (new) attack tools

an intermediate variable



i_1 and i_2 , i_3 and i_4 are respectively roots of some equations w/ specific parameters.

Portion of secure nodes

When the defender "occupies" more than i_2 portions of nodes, both attacker and defender use minimal attack/defense power. This leads to $i_B(t)=i_0(t)$ for any t > 0.

Roadmap

- ❑ Vision for Cybersecurity Dynamics Foundation
- ❑ Example Results Towards Fulfilling the Vision
  - ❖ Limitation of Preventive & Reactive Defense
  - ❖ Overcoming the Limitation w/ Active Defense
  - ❖ Optimizing Active Defense
- ❑ Challenges Ahead: Tackling Technical Barriers

Challenges Ahead for Thrust I

Systematic theory of cybersecurity dynamics (e.g., optimal allocation of preventive, reactive, active, proactive, adaptive defense), while overcoming inherent technical barriers

❑ Scalability barrier: exponentially many states

❑ Dependence barrier: dependent random variables

❑ Nonlinearity barrier: highly nonlinear systems

❑ Dynamics barrier: dynamic parameters and structures

❑ Nonequilibrium barrier: equilibrium behavior not suffici.

Challenges Ahead for Thrust II

This thrust deals with:

❑ Obtaining parameters in practice

❑ Validating assumptions

❑ Building tools for use in practice

❑ Bridging the theory-practice gap

Challenges Ahead for Thrust III

This thrust deals with:

❑ **Resolution barrier: Unified knowledge crossing macroscopic, mesoscopic and microscopic levels of abstraction**

❑ **Possibly others**

Key to Realizing the Vision

Need close collaborations:

- □ Cross multiple disciplines (kinds of math etc.)
- □ Cross multiple sub-disciplines within CS
- □ Cross the various security sub-fields

I myself am looking forward to such collaborations.

We also need to foster a research community ---

HotSoS is a good starting point!

Acknowledgement

Mentors (so far):

Moti Yung, Ravi Sandhu, Gene Tsudik, Elisa Bertino

Collaborators (so far):

Gaofeng Da, Xiaohu Li, Wenlian Lu, Yilun Shang,

Maochao Xu (mathematicians)

Students (so far): Li Xu, Zhenxin Zhan

Funding Acknowledgement

I greatly acknowledge funding support from:

- ARO (PM: Dr. Cliff Wang)
- AFOSR (PM: Dr. Bob Herklotz)

To students: Exciting time to do cybersecurity research (modeling and mechanism alike)!

Thanks!!

Questions / Comments?

Science of Cybersecurity Is NOT Applied X

The elementary entities of science X obey the laws of science Y, but science X is not "just applied Y."

X	Y
Solid state or many-body physics	Elementary particle physics
Chemistry	Many-body physics
Molecular biology	Chemistry
Cell biology	Molecular biology
…	…
Psychology	Physiology
Social science	Psychology

[P. Anderson. More is different. Science, Vol. 177, No. 4047, August 4, 1972, pp 393-6.]

Appendix B

Cybersecurity Dynamics[*]

Shouhuai Xu
Department of Computer Science
University of Texas at San Antonio
shxu@cs.utsa.edu

ABSTRACT

We explore the emerging field of *Cybersecurity Dynamics*, a candidate foundation for the Science of Cybersecurity.

Categories and Subject Descriptors

D.4.6 [**Security and Protection**]

General Terms

Security, Theory

Keywords

Cybersecurity dynamics, security model, security analysis

1. THE CONCEPT

In the course of seeking fundamental concepts that would drive the study of cybersecurity for the many years to come — just like how concepts such as confidentiality, integrity and availability have been driving the study of security for decades — the idea of *cybersecurity dynamics* emerged. Intuitively, 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* (green color) or *compromised* (red color); 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. A core concept in cybersecurity dynamics is *attack-defense structure*, namely complex network capturing the relation which computer can directly attack and/or defend for which other computer in a cyber system of interest. This means that another emerging field, called Network Science, would play a fundamental role in cybersecurity dynamics (as a supporting technology). From this perspective, a vision related to cybersecurity dynamics was recently independently explored by Kott [6].

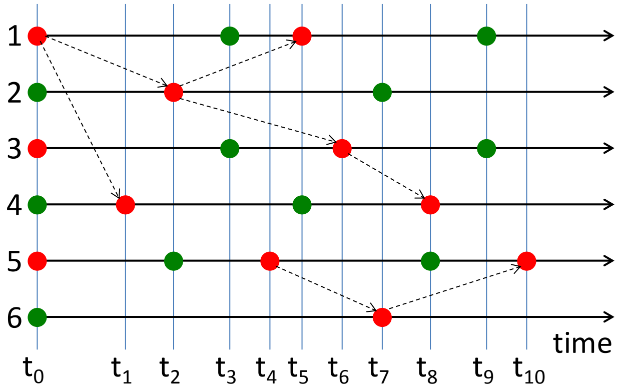


Figure 1: Illustration of cybersecurity dynamics in a toy cybersystem, which has six nodes (denoted by $1, \ldots, 6$) whose states evolve over time as caused by cyber attack-defense interactions. A node has two states: *secure* (green color) and *compromised* (red color). Dashed arrows represent successful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

Cybersecurity dynamics can serve as a foundation for the Science of Cybersecurity because of the following. 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 some defense tools or mechanisms. 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. The distinction between macroscopic security and microscopic security might help separate *security services* (i.e., management- or operation-oriented) from *security techniques* (i.e., design-oriented). 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

[*] A website dedicated to cybersecurity dynamics is available at `http://www.cs.utsa.edu/~shxu/socs/`

HotSoS '14, April 08 - 09 2014, Raleigh, NC, USA
ACM 978-1-4503-2907-1/14/04.
http://dx.doi.org/10.1145/2600176.2600190

the factors/laws that govern the evolutions.

Cybersecurity dynamics vs. biological epidemic dynamics. Researchers have been trying to design and build computer systems that can mimic the elegant properties of biological (especially human body) systems, through concepts such as Artificial Immune System [4]. Not surprisingly, the concept of cybersecurity dynamics is inspired by epidemic models of biological systems [9]. The concept is also inspired by models of interacting particle systems [7], and by the microfoundation in economics (i.e., macroeconomic parameters are ideally derived from, or the output of, some microeconomic models) [5]. Furthermore, the concept naturally generalizes the many models that are scattered in a large amount of literature in venues including both statistical physics (e.g., [10]) and computer science (e.g., [1, 13, 14]). However, as we will discuss in Section 3, fully understanding and managing cybersecurity dynamics requires us to overcome several technical barriers.

2. RESEARCH ROADMAP

In order to fulfill the envisioned cybersecurity dynamics foundation for the Science of Cybersecurity, we suggest a research roadmap that consists of three integral thrusts.

Thrust I: Building a systematic theory of cybersecurity dynamics. The goal is to understand cybersecurity dynamics via *first-principles* modeling, by using as-simple-as-possible models with as-few-as-possible parameters and making as-weak-as-possible assumptions. Such models aim 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? The models may assume away how model parameters can be obtained (obtaining the parameters is the focus of Thrust II), as long as they are consistent with cyber attack and defense activities. Such characterization studies might additionally address the following question: In order to obtain a certain kind of results, certain model parameters must be provided no matter how costly it is to obtain them. Early-stage investigations falling into this Thrust include [10, 1, 2, 3, 11, 12, 8, 13, 15, 14],

Thrust II: Data-, policy-, architecture- and mechanism-driven characterization studies. The goal is to characterize security policies, architectures and mechanisms from the perspective of cybersecurity dynamics. These studies allow us to extract model parameters for practical use of the cybersecurity insights/laws discovered by Thrust I, so as to guide real-life cyber operation decision-making. Data-driven cybersecurity analytics is relevant to all these studies. For example, by studying the notion of *stochastic cyber attack process*, it is possible to conduct “gray-box" (rather than “black-box") predictions [16], which can serve as earlywarning information and guide the provisioning of resources for cost-effective defense. This Thrust might lead to the development of cybersecurity instruments, which can measure useful attributes — like the various kinds of medical devices that can measure various health attributes/parameters of human body.

Thrust III: Bridging gaps between Thrusts I & II. The goal is to bridge the gaps between Thrust I and Thrust II. This Thrust can inform Thrust II what parameters used in the models of Thrust I are *necessary* to obtain, no matter how costly it is to obtain them. On the other hand, this Thrust can also inform Thrust I that certain other parameters may be easier to obtain in practice, and therefore alternate models may be sought instead. Research on *experimental cybersecurity*, in lieu of experimental physics, will be a main theme of this Thrust.

3. TECHNICAL BARRIERS

In order to fulfill the envisioned cybersecurity dynamics foundation for the Science of Cybersecurity, we need to overcome several technical barriers that are believed to be inherent to the problem of cybersecurity (i.e., they cannot be bypassed) and do not have counterparts (at least to a large extent) in the inspiring disciplines mentioned above. Representatives are: (a) The *scalability* barrier: Suppose there are n nodes, where each node has 2 states. Then, there are 2^n global states. This state-space explosion prevents simple treatment of stochastic processes. (b) The *nonlinearity* barrier: The probability that a computer is compromised would depend on the states of other computers in a (highly) nonlinear fashion. This can render many analysis techniques useless. (c) The *dependence* barrier: The states of computers are dependent upon each other (e.g., they may have the same software vulnerability), and thus we need to accommodate such dependence between them. (d) The *structural dynamics* barrier: The heterogeneous attack-defense complex network structures may be dynamic at a time scale that may or may not be the same as the time scale of the cybersecurity dynamics. (e) The *non-equilibrium* (or *transient behavior*) barrier: It is important to understand both the equilibrium states and the dynamics before it converges to the equilibrium distribution/state (if it does at all).

Acknowledgement. This work was supported in part by ARO Grant # W911NF-13-1-0370 and AFOSR Grant # FA9550-09-1-0165. The author also would like to thank his mentors for their encouragement, and his collaborators for deepening his understanding of the power and limitations of various mathematical techniques (broadly defined).

4. REFERENCES

[1] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos. Epidemic thresholds in real networks. *ACM Trans. Inf. Syst. Secur.*, 10(4):1–26, 2008.

[2] D. Gao, M. Xu, and S. Xu. A new approach to modeling and analyzing security of networked systems. In *HotSoS'14*.

[3] Y. Han, W. Lu, and S. Xu. Characterizing the power of moving target defense via cyber epidemic dynamics. In *HotSoS'14*.

[4] S. Hofmeyr and S. Forrest. Architecture for an artificial immune system. *Evolutionary Computation*, 8(4):443–473, 2000.

[5] K. Hoover. Idealizing reduction: The microfoundations of macroeconomics. *Erkenntnis*, 73:329–347, 2010.

[6] A. Kott. Towards fundamental science of cyber security. In *Network Science and Cybersecurity*, pp 1–13. 2014.

[7] T. Liggett. *Interacting Particle Systems*. Springer, 1985.

[8] W. Lu, S. Xu, and X. Yi. Optimizing Active Cyber Defense. *Proc. GameSec'13*, pp 206-225.

[9] A. McKendrick. Applications of mathematics to medical problems. *Proc. of Edin. Math. Soceity*, 14:98–130, 1926.

[10] R. Pastor-Satorras and A. Vespignani. Epidemic dynamics and endemic states in complex networks. *Physical Review E*, 63:066117, 2001.

[11] M. Xu and S. Xu. An extended stochastic model for quantitative security analysis of networked systems. *Internet Mathematics*, 8(3):288–320, 2012.

[12] S. Xu, W. Lu, and H. Li. A stochastic model of active cyber defense dynamics. *Internet Mathematics*, 2014 (to appear).

[13] S. Xu, W. Lu, and L. Xu. Push- and pull-based epidemic spreading in arbitrary networks: Thresholds and deeper insights. *ACM TAAS*, 7(3):32:1–32:26 (2012).

[14] S. Xu, W. Lu, L. Xu, and Z. Zhan. Adaptive Epidemic Dynamics in Networks: Thresholds and Control. *ACM TAAS*, 8(4):19 (2014)

[15] S. Xu, W. Lu, and Z. Zhan. A stochastic model of multivirus dynamics. *IEEE TDSC*, 9(1):30–45, 2012.

[16] Z. Zhan, M. Xu, and S. Xu. Characterizing honeypot-captured cyber attacks: Statistical framework and case study. *IEEE TIFS*, 8(11):1775–1789, 2013.

Appendix C

Emergent Behavior in Cybersecurity

Shouhuai Xu
Department of Computer Science
University of Texas at San Antonio
shxu@cs.utsa.edu

ABSTRACT

We argue that *emergent behavior* is inherent to cybersecurity.

Categories and Subject Descriptors

D.4.6 [**Security and Protection**]

General Terms

Security, Theory

Keywords

Emergent behavior, cybersecurity, security properties

1. INTRODUCTION

The human-created cyberspace is a very large-scale complex system of cybersystems. Its security properties are difficult to understand and characterize. We attribute this difficulty to its *complexity*, a manifestation of which is the so-called *emergent behavior* in Complexity Science [6]. Although there is no universally accepted definition of emergent behavior [11], the basic idea is intuitive. The simplest example of emergent behavior may be the well known “$1 + 1 > 2$" effect. For our purpose, it is sufficient to use the following informal definition of emergent behavior in cybersecurity domain.

DEFINITION 1. *A security property of a cybersystem exhibits emergent behavior if the property is* not *possessed by the underlying lower-level components of the cybersystem.*

A direct consequence of emergent behavior is that at least some security properties cannot be understood by solely considering the lower-level components; instead, we must explicitly consider the *interactions* between the lower-level components. Although emergent behavior of cybersystems has been discussed from a function or constructional perspective [10, 7], emergent behavior in cybersecurity is not systematically examined until now.

2. EMERGENT BEHAVIOR

We demonstrate emergent behavior in cybersecurity through three examples.

Example 1: Emergent behavior exhibited by cybersecurity dynamics. We refer to [15] for an exposition of the emerging field of cybersecurity dynamics. In order to explain how emergent behavior is exhibited by cybersecurity dynamics, we consider the perhaps simplest model [4]. For our purpose, it suffices to consider two cybersystems that respectively induce attack-defense structures (or graphs) $G_i = (V_i, E_i)$, where V_i is the node (vertex) set and E_i is the edge set for $i = 1, 2$. Let $\lambda_1(G)$ denote the largest eigenvalue of the adjacency matrix of a graph G, β denote the defense capability in detecting and cleaning compromised nodes (e.g., the probability that a compromised node gets cleaned at a time step), and γ denote the attack capability in compromising secure nodes (e.g., the probability that this event occurs over an edge at a time step). For simplicity, suppose G_i is a complete graph with n_i nodes for $i = 1, 2$. It is well known that $\lambda_1(G_1) = n_1 - 1$ and $\lambda_1(G_2) = n_2 - 1$. For $i = 1, 2$, if $\lambda_1(G_i) < \beta/\gamma$, the attacks will eventually be wiped out in the cybersystem that induces G_i; if $\lambda_1(G_i) > \beta/\gamma$, the attacks cannot be wiped out [4].

Now we consider a new cybersystem that is obtained by interconnecting the aforementioned two cybersystems that induced G_1 and G_2. Consider the simplest case that any node can attack any other node in the interconnected cybersystem, which effectively induces attack-defense structure, a complete graph, $G_{1,2}$ with n_1+n_2 nodes and $\lambda_1(G_{1,2}) = n_1 + n_2 - 1$. In many (if not all) cases, the defense capability β' and the attack capability γ' associated to $G_{1,2}$ are respectively the same as the defense capability β and the attack capability γ associated to G_1 and G_2. Since $\lambda_1(G_i) < \beta/\gamma$ for $i = 1, 2$ do not imply $\lambda_1(G_{1,2}) < \beta'/\gamma' = \beta/\gamma$, we conclude that the attacks can be wiped out in the two underlying component cybersystems, but cannot be wiped out in the interconnected cybersystem as long as $\lambda_1(G_{1,2}) > \beta/\gamma$. This phenomenon can be naturally extended to more sophisticated settings (e.g., [17, 16, 18, 19]). This implies that cybersecurity dynamics cannot be determined by looking at the component cybersystems alone. Rather, we need to look into how the component cybersystems interact with each other.

Example 2: Emergent behavior exhibited by security properties in the extended trace-property framework. In the field of program verification, it was known that specifications that are sufficient for *sequential* programs are not sufficient for *concurrent* programs. For dealing with concurrent programs, Lamport proposed the safety-liveness framework of trace properties [12]. Intuitively, a *trace* is a finite or infinite sequence of states corresponding to an execution of a program. A *trace property* is a set of traces such

HotSoS ’14, April 08 - 09 2014, Raleigh, NC, USA
ACM 978-1-4503-2907-1/14/04.
http://dx.doi.org/10.1145/2600176.2600189

that every trace, *in isolation*, satisfies the same predicate. A *safety* property says that no “bad thing" happens during the course of a program execution, while a *liveness* property says that “good thing" will eventually happen during the course of a program execution. Both safety and liveness are trace properties. A beautiful result is that every trace property is the intersection of a safety property and a liveness property [12, 1].

Given the above history, it is appealing to specify a cybersystem as a set of traces, and therefore as a subset of a security property that is also specified as *a set of traces*. Unfortunately, security properties are not trace properties as shown in [8, 5, 14] and refreshed below. First, *noninterference* is a security property that captures the intuition that system security is preserved as long as high-clearance (or high-privilege) processes cannot influence the behavior of low-clearance (low-privilege) processes. It is no trace property because it cannot be verified without examining the other traces. Second, *information-flow* captures some kind of correlation between the values of variables in multiple traces. It is no trace property because it cannot be verified by examining each trace alone. Third, *average service response time* is an availability property. It is no trace property because it depends on the response time in all traces.

In an effort to overcome the above limitation of the safety-liveness framework, Clarkson and Schenider extended the notion of *trace properties* to the notion of *trace hyperproperties* [5]. Basically, hyperproperties are *sets of trace properties*. In parallel to the safety-liveness framework, a hyperproperty is also the intersection of a safety hyperproperty and a liveness hyperproperty. It is now known that information-flow, integrity and availability can be hypersafety or hyperliveness [5]. Exactly because hyperproperties capture that the verification procedure *must* examine across *multiple* traces, which may accommodate interactions between the component systems, we say that hyperproperties exhibit the emergent behavior. This means that we need to study the emergent behavior in cybersecurity, which may explain why it took so long to realize the importance of hyperproperties.

Example 3: Emergent behavior exhibited by cryptographic security properties. Cryptographic secure multiparty computation allows multiple parties $P_1, \ldots, P_m$, each having a respective secret $x_1, \ldots, x_m$, to compute a function $f(x_1, \ldots, x_m)$ such that no information about the x_i's is leaked except for what is implied by the output of the function. This manifests a confidentiality property. A beautiful feasibility result is that any polynomial-time computable function $f(\cdot, \ldots, \cdot)$ can be securely computed [20, 9], as long as the protocol executes *in isolation* (the stand-alone setting) and trapdoor permutations exist. When such cryptographic protocols are used as building-blocks in larger applications/systems, they may execute concurrently (rather than in isolation). This leads to a natural question: Are the cryptographic protocols, which are provably secure when executed in isolation, still secure when they are concurrently called by larger applications/systems? Intuitively, concurrent executions offer the attacker the leverage (for example) to schedule the messages in a way that is to the attacker's advantage, which does not have a counterpart in the stand-alone setting.

Quite similar to what happened in the field of program verification, where specific properties (e.g., partial correctness and mutual exclusion) were investigated before the introduction of the unifying safety-liveness framework [12], the same kind of development was made in the field of cryptographic protocols. That is, specific cryptographic security properties were investigated before the introduction of the unifying notion called *universal composability* [2], or its equivalent (but perhaps more intuitive) version called *concurrent general composition* (arbitrarily many instances run possibly together with arbitrary other protocols) [13]. It is now known that there are cryptographic multiparty computation protocols, which are provably secure when executed in isolation, but are *not* secure when they are concurrently called by larger applications/systems. For example, there exist classes of functions that cannot be computed in the universally composably secure fashion [3]. In other words, these functions can be securely computed by running some cryptographic protocols in isolation, but cannot be securely computed when the protocols execute concurrently. In order to make cryptographic multiparty computation protocols secure when they are used as building-blocks for constructing larger cybersystems, we need to make extra assumptions, such as that majority of the parties $P_1, \ldots, P_m$ are not compromised [2]. This manifests emergent behavior. (It is interesting to note that whether or not it is reasonable to assume that majority of the parties are not compromised may be addressed by the cybersecurity dynamics framework [15].)

Acknowledgement. This work was supported in part by AFOSR Grant # FA9550-09-1-0165 and ARO Grant # W911NF-13-1-0370.

3. REFERENCES

[1] B. Alpern and F. Schneider. Defining liveness. *Inf. Process. Lett.*, 21(4):181–185, 1985.

[2] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proc. FOCS'01*, pp 136–145.

[3] R. Canetti, E. Kushilevitz, and Y. Lindell. On the limitations of universally composable two-party computation without set-up assumptions. In EUROCRYPT'03, pp 68–86.

[4] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos. Epidemic thresholds in real networks. *ACM Trans. Inf. Syst. Secur.*, 10(4):1–26, 2008.

[5] M. Clarkson and F. Schneider. Hyperproperties. *Journal of Computer Security*, 18(6):1157–1210, 2010.

[6] P. Erdi. *Complexity Explained*. Springer, 2008.

[7] V. Gligor. Security of emergent properties in ad-hoc networks. In *Proc. Security Protocols Workshop'04*, pp 256–266.

[8] J. Goguen and J. Meseguer. Security policies and security models. In *IEEE Symp. on Security & Privacy'82*, pp 11–20.

[9] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *Proc. ACM STOC'87*, pp 218–229.

[10] H. Hinton. Under-specification, composition and emergent properties. In *Proc. NSPW'97*, pp. 83–93.

[11] A. Kubík. Toward a formalization of emergence. *Artif. Life*, 9(1):41–65, 2002.

[12] L. Lamport. Proving the correctness of multiprocess programs. *IEEE Trans. Software Eng.*, 3(2):125–143, 1977.

[13] Y. Lindell. General composition and universal composability in secure multi-party computation. In *FOCS'03*, pp 394–403.

[14] F. Schneider. Beyond traces and independence. In *Dependable and Historic Computing*, pp 479–485, 2011.

[15] S. Xu. Cybersecurity dynamics. In *HotSOS'14 (poster)*.

[16] S. Xu, W. Lu, and H. Li. A stochastic model of active cyber defense dynamics. *Internet Mathematics*, 2014 (to appear).

[17] S. Xu, W. Lu, and L. Xu. Push- and pull-based epidemic spreading in arbitrary networks: Thresholds and deeper insights. *ACM TAAS*, 7(3):32:1–32:26, 2012.

[18] S. Xu, W. Lu, L. Xu, and Z. Zhan. Adaptive Epidemic Dynamics in Networks: Thresholds and Control. *ACM TAAS*, 8(4):19 (2014)

[19] S. Xu, W. Lu, and Z. Zhan. A stochastic model of multivirus dynamics. *IEEE TDSC*, 9(1):30–45, 2012.

[20] A. C. Yao. How to generate and exchange secrets. In *Proc. FOCS'86*, pp 162–167.