Interational Computer Science Institute & University of California, Berkeley

Modeling Cyber-Insurance

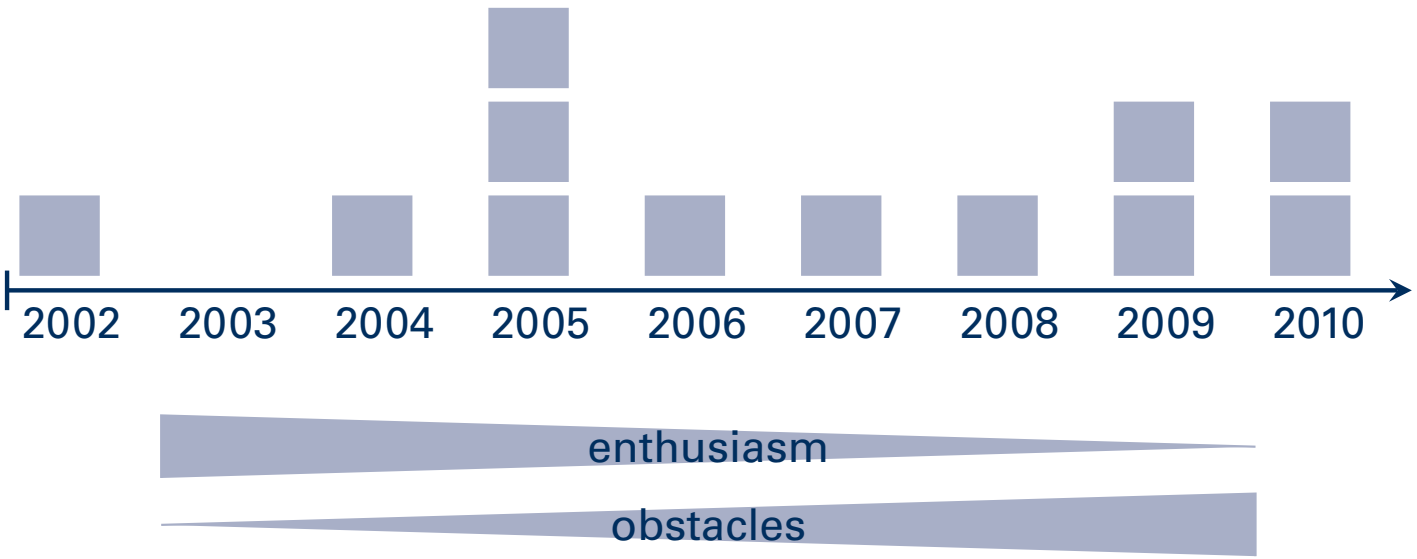
Towards a Unifying Framework

Rainer Böhme[*] **, Galina Schwartz**[†]

[*] **Networking Group, ICSI Berkeley** [†] **EECS, UC Berkeley**

Workshop on the Economics of Information Security, Harvard, 8 June 2010

Talks on Cyber-Insurance at WEIS



Outline

1. Characteristics of Cyber-Risk
2. Framework Overview
3. Selected Features
   - Network topology
   - Unified approach to interdependent security and correlated risk
4. “Results” and Conclusion

1

Characteristics of Cyber-Risk

What Is Specific to Cyber-Risk ?

success factors of ICT		**risk properties**
distribution & interconnection	→	interdependent security own risk depends on other parties' actions
universality & reuse	→	risk propagation & correlation incidents cause further incidents
+		
= complexity	→	imperfect information

Examples

Conventional risks in the economic insurance literature

neither interdependence nor correlation

Airline baggage security

interdependence, but no correlation

Kunreuther & Heal, 2003

Natural disasters in the actuarial literature

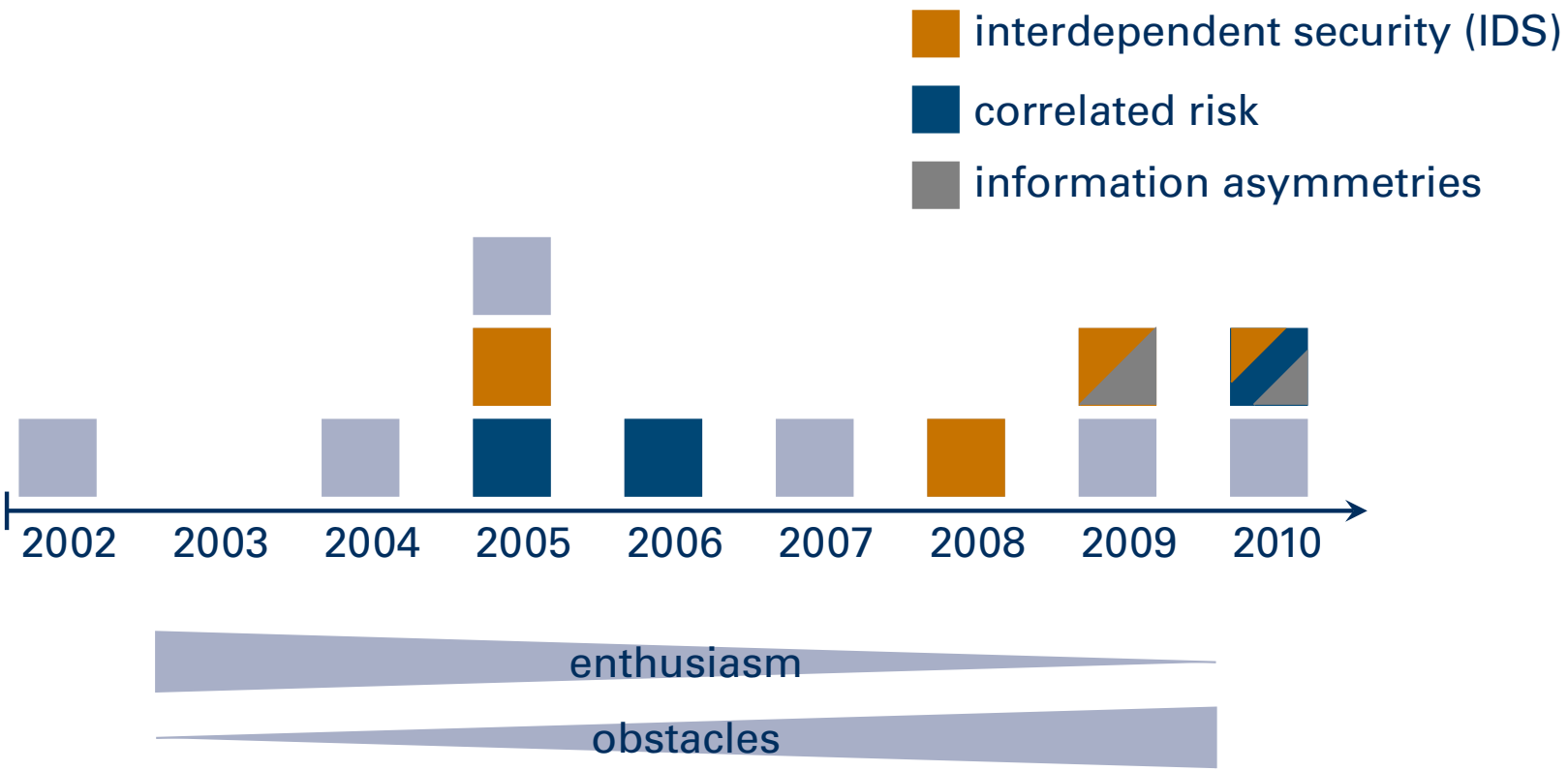
spatial correlation, but no interdependence

Embrechts et al., 1999

Cyber-insurance

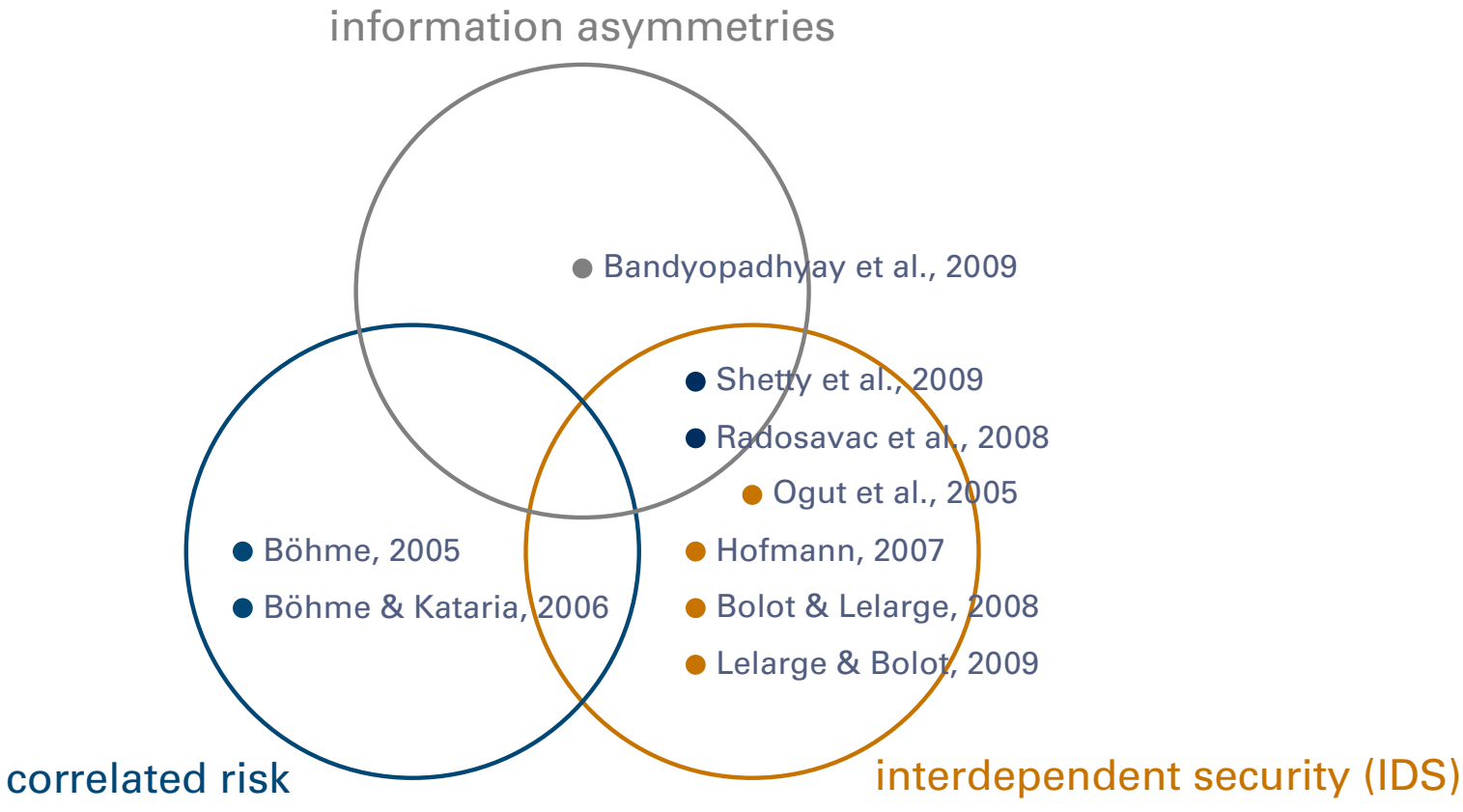
both interdependence and correlation, but never modeled together

Talks on Cyber-Insurance at WEIS



Risk Properties

in the Cyber-Insurance Literature



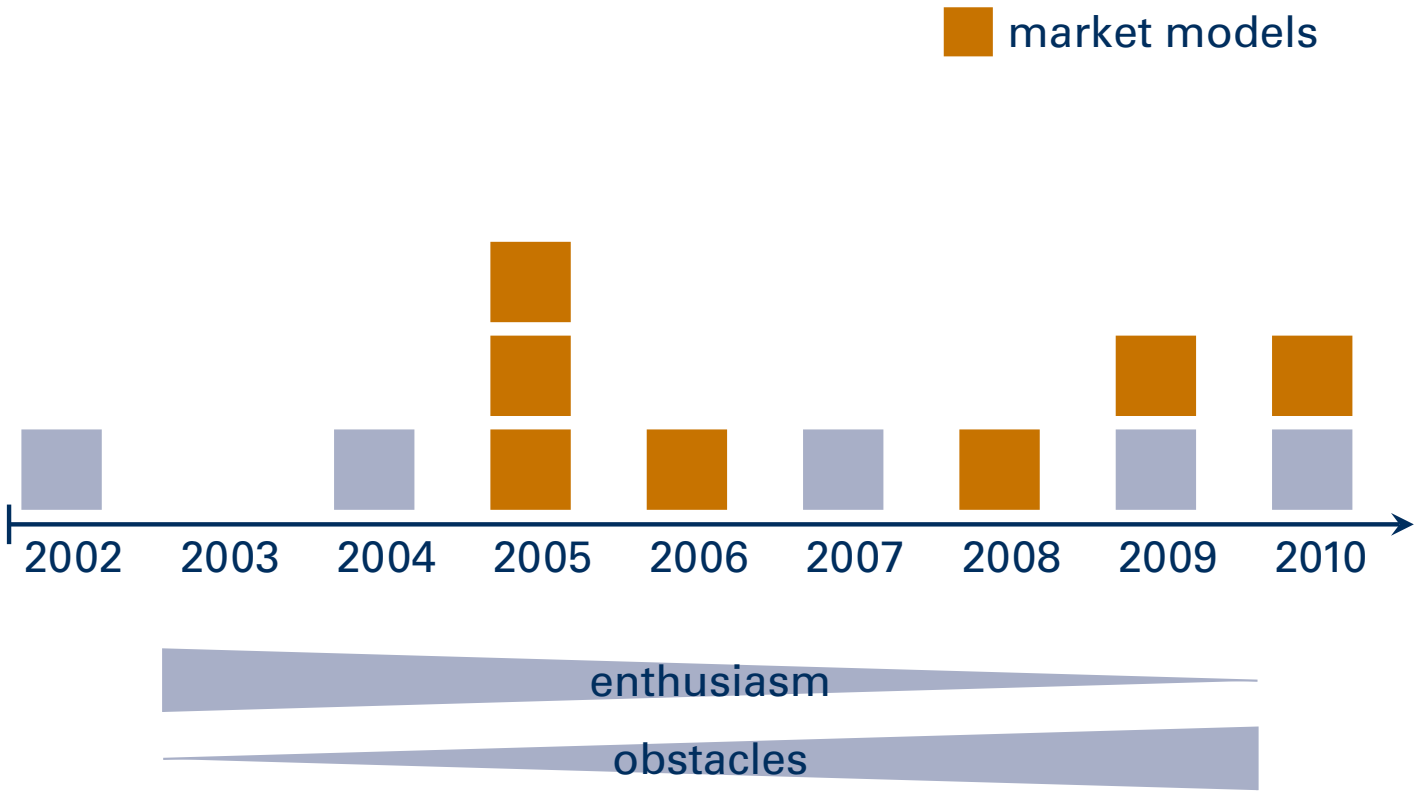
2

Framework Overview

Framework


1.
network
environment
(nodes)
design
utility
risk
2.
demand side
(agents)
risk
3.
supply side
(insurers)

Talks on Cyber-Insurance at WEIS



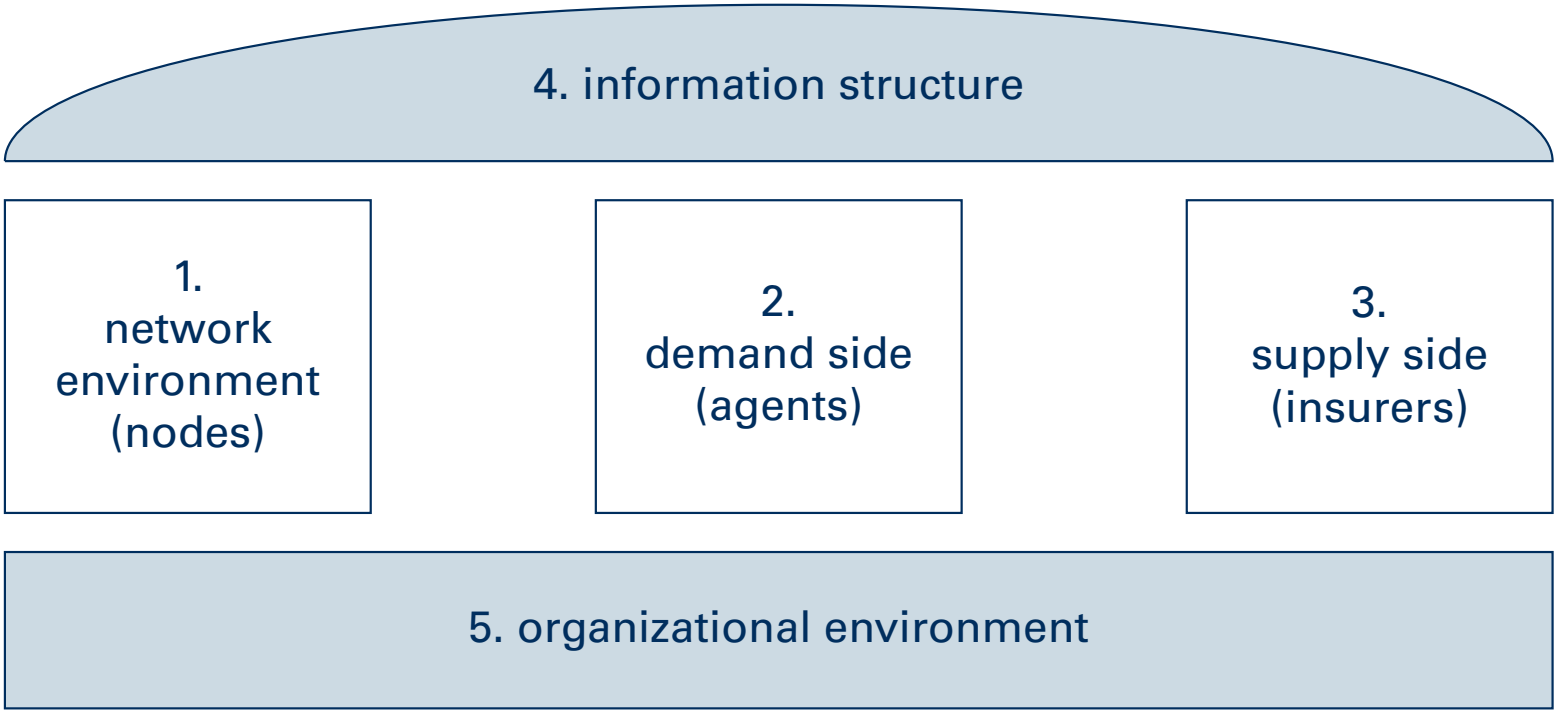
Framework


1.
network
environment
(nodes)
design
utility
risk
2.
demand side
(agents)
risk
3.
supply side
(insurers)

Framework


nature
players
1.
network
environment
(nodes)
2.
demand side
(agents)
3.
supply side
(insurers)

Framework


4. information structure
1.
network
environment
(nodes)
2.
demand side
(agents)
3.
supply side
(insurers)
5. organizational environment

Overview of Model Attributes

1. network environment

defense function
network topology
risk arrival
attacker model

2. demand side

node control
heterogeneity
agents' risk aversion
action space
time

3. supply side

market structure
insurers' risk aversion
markup
contract design
higher-order risk transfer

4. information structure

IA in conventional insurance
IA specific to cyber-insurance
timing

5. organizational environment

regulator
ICT manufacturers
network intermediaries
security service providers

Variables of Interest

Breadth of market

Under which conditions will a market for cyber-insurance thrive?

Network security

Can we expect fewer attacks if cyber-insurance is broadly adopted?

Social welfare

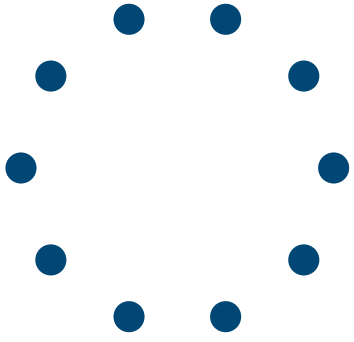
Will the world be a better place with cyber-risk reallocation?

3

Selected Features

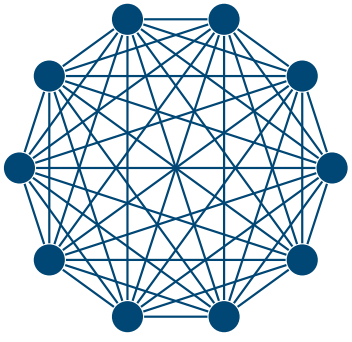
Network Topology

Examples



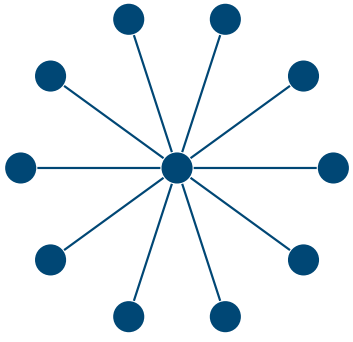
ideosyncratic

hardware failure



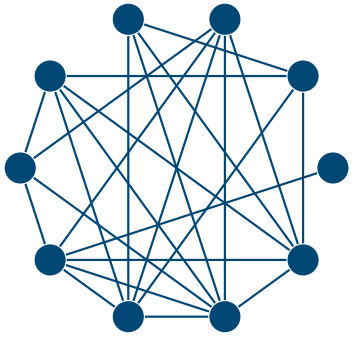
fully connected

email spam



single-factor model

OS vulnerability



Erdös-Rényi graph

inter-organizational dependence

⟶ Comprehensive insurance policies represent **bundles of contracts.**

Unified Approach to IDS and Correlation

Defense function for node i:

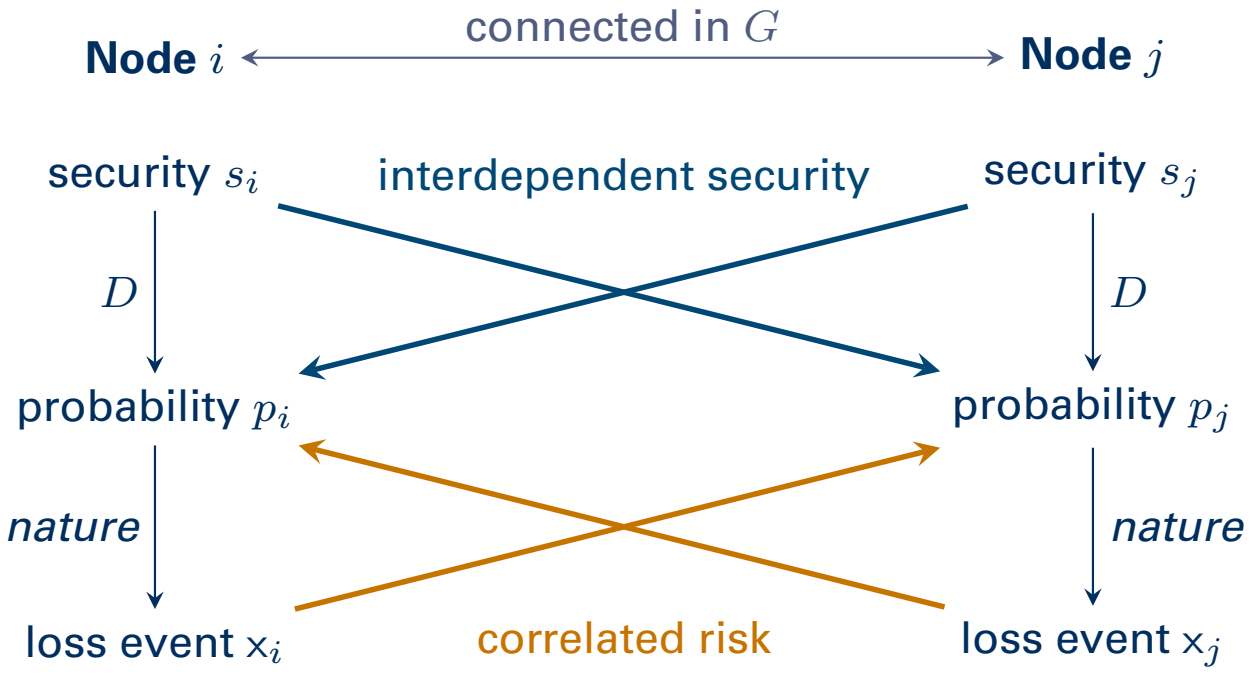
$$P(\mathsf{L}_i = l) = D(l, w_i, \boldsymbol{s}, G, \mathbf{x})$$

l	size of loss (random variable L_i)
w_i	initial wealth
$\boldsymbol{s}$	vector of security investments: $\boldsymbol{s} = s_i \cup \boldsymbol{s}_{j \neq i}$
G	network topology as model of interconnectedness

Simplification: fix w and normalize $l = 1$, then let p_i be the probability of a loss at node i and $\mathbf{X} \in \{0, 1\}^n$ be a random vector of realized losses per node.

Proposition: interdependent security and correlated risk can be modeled jointly by making $\boldsymbol{s}$ and realizations $\mathbf{x}$ of $\mathbf{X}$ parameters of D.

Illustration



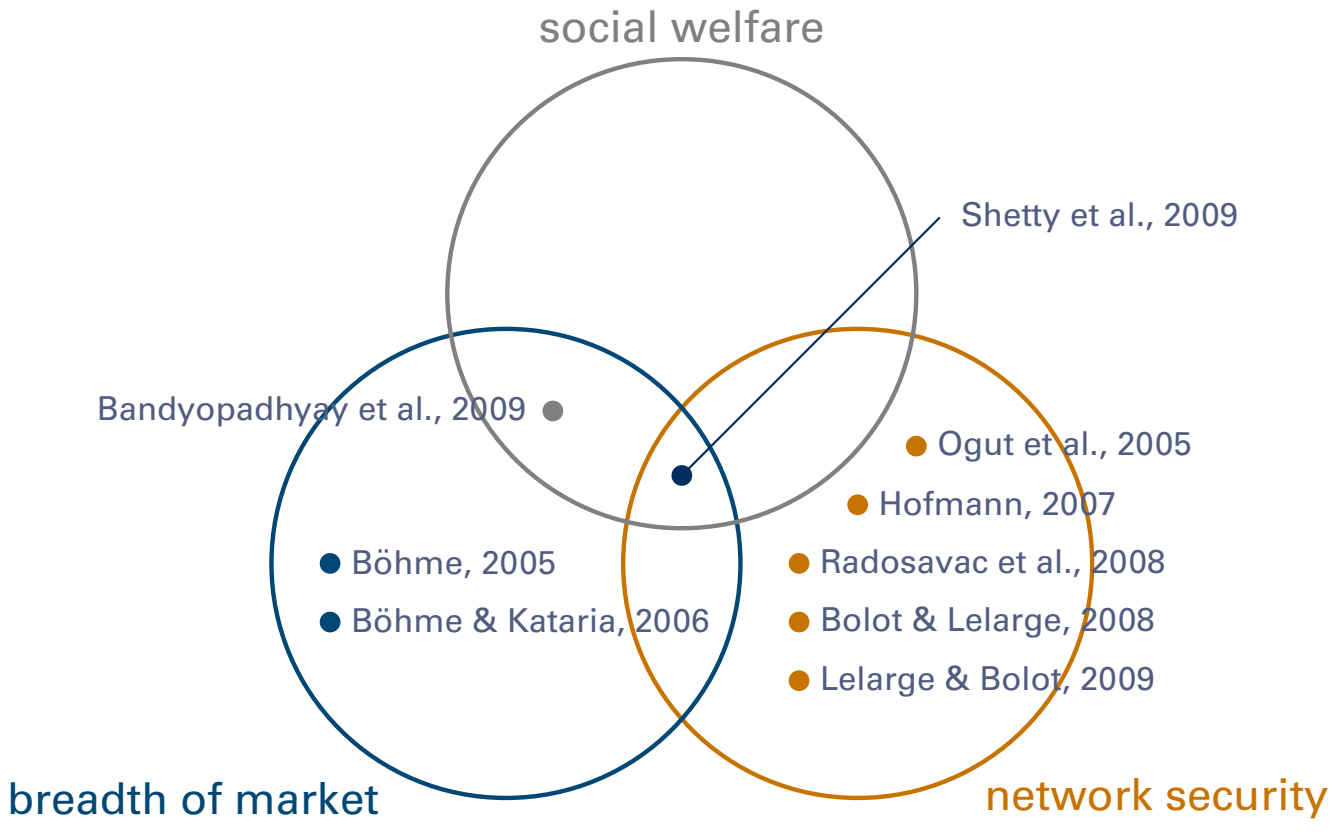
Risk propagation is hard to tract: the modeling requires recursive methods or approximations and it may lead to dynamic equilibria.

4

"Results" and Conclusion

Dependent Variables

in the Cyber-Insurance Literature



Discrepancy

between Statements and Models

Cyber-insurers will improve information about security levels;

. . . but relevant parameters not included in the model.

Cyber-insurers will positively affect agents' decisions in shaping the network environment;

. . . but existing models of contracts do not reflect these choices.

Broad adoption of cyber-insurerance will change the market structure and behavior of ICT manufacturers;

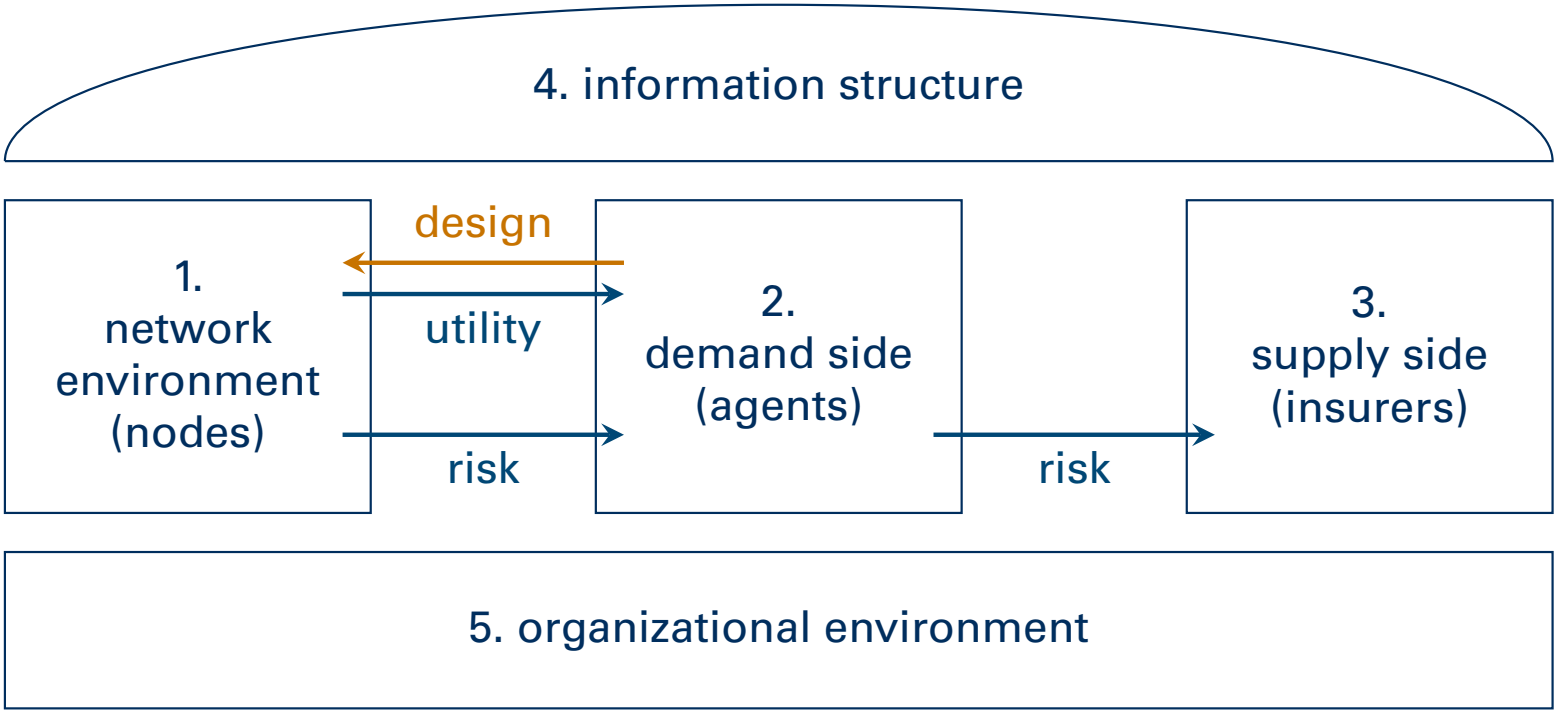
. . . but never modeled parametrically.

Endogenize!

Future modeling approaches should endogenize key parameters of the network environment, information structure, and organizational environment.

Example:
endogenous network formation to model platform switching dynamics

Framework


4. information structure
1.
network
environment
(nodes)
design
utility
risk
2.
demand side
(agents)
risk
3.
supply side
(insurers)
5. organizational environment

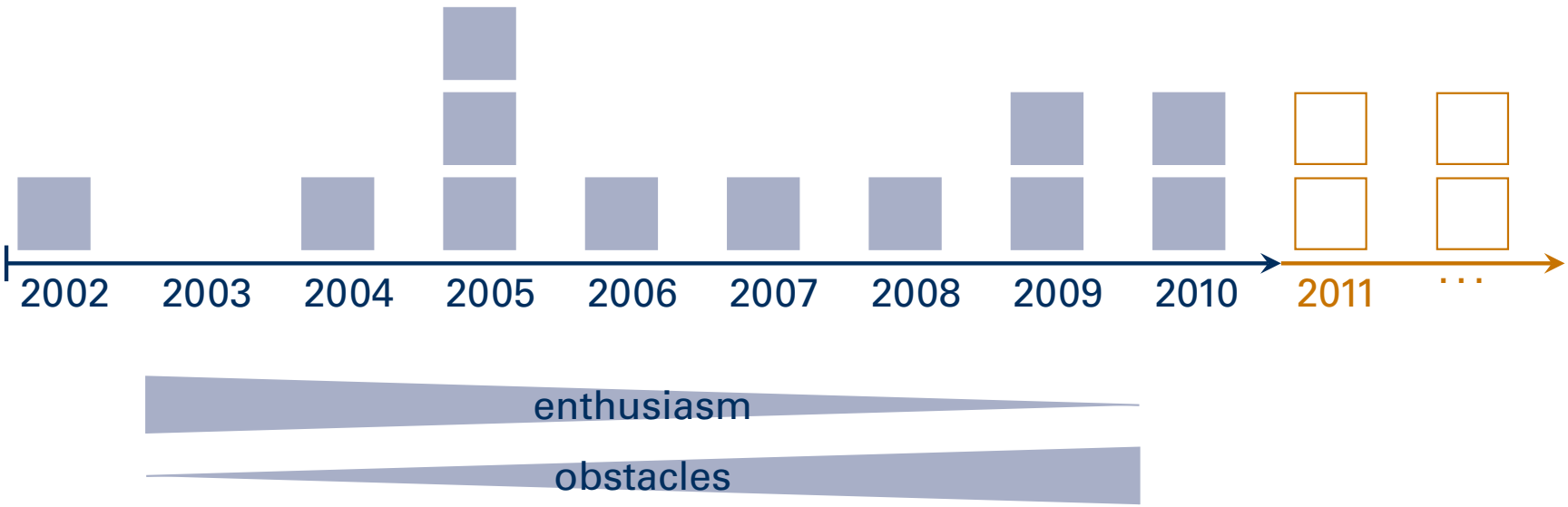
Endogenize!

Future modeling approaches should endogenize key parameters of the network environment, information structure, and organizational environment.

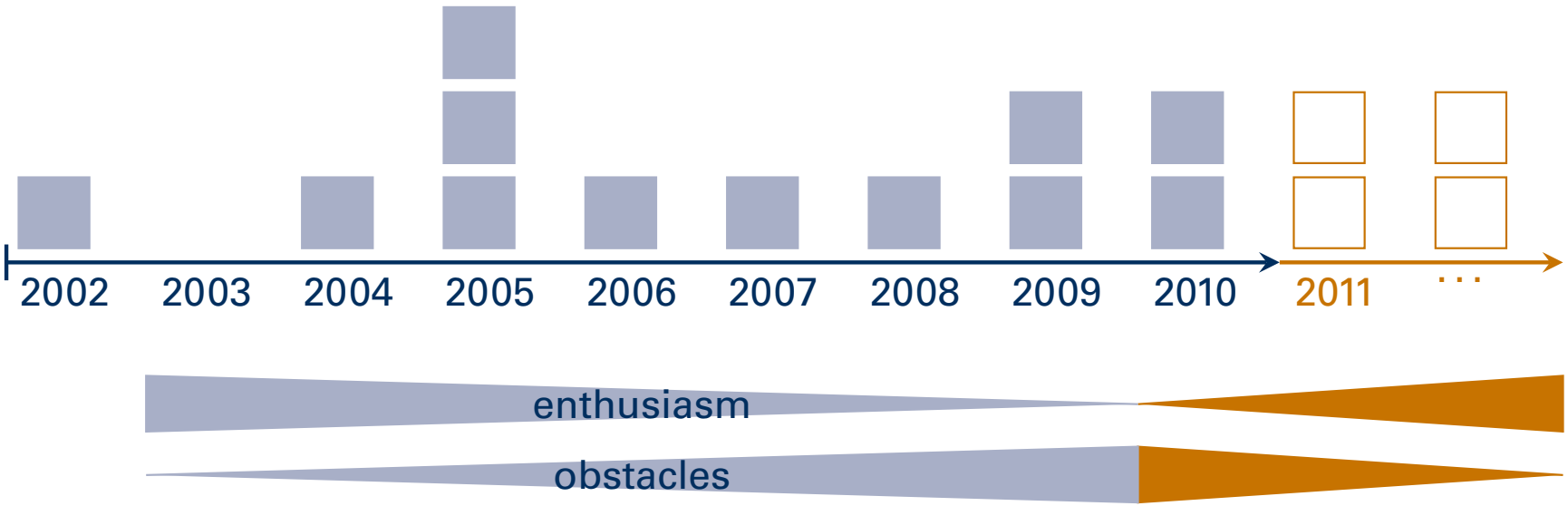
Example:
endogenous network formation to model platform switching dynamics

Policy recommendations need better foundations in analytical models.

Talks on Cyber-Insurance at WEIS



Talks on Cyber-Insurance at WEIS



Q & A

Thank you for your attention.

Rainer Böhme[*] **, Galina Schwartz**[†]

[*] **Networking Group, ICSI Berkeley** [†] **EECS, UC Berkeley**

Workshop on the Economics of Information Security, Harvard, 8 June 2010