

Network Economics of Cyber Crime with Applications to Financial Service Organizations

Anna Nagurney, Wayne Burleson, Mila Sherman, Senay Solak,
and Chris Misra

University of Massachusetts
Amherst, Massachusetts 01003

INFORMS Annual Meeting,
Minneapolis, Minnesota, October 6-9, 2013



We acknowledge support from the Advanced Cyber Security Center (ACSC) for funding our project, *Cybersecurity Risk Analysis and Investment Optimization*.



The Project Synopsis:

The vision of this project was to develop:

- rigorous models for cybersecurity risk,
- models for costs and benefits of various cybersecurity technologies,
- techniques for integrating these models into higher level models that account for other risks and risk management expenditures.

Our team is interdisciplinary and comprised of UMass Amherst faculty and an IT security operations professional.

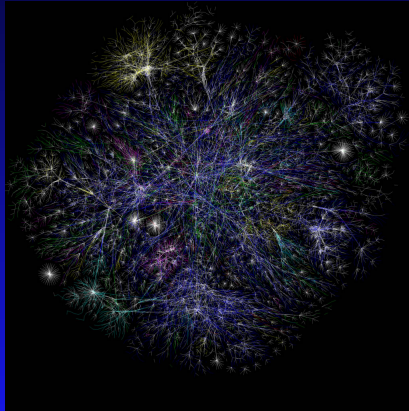
Outline of Presentation

- ▶ Background and Motivation
 - ● Internet
 - ● Financial Networks
- ▶ Cyber Crime and Network Economics
- ▶ The Model
- ▶ Summary and Conclusions

Background and Motivation

The Internet

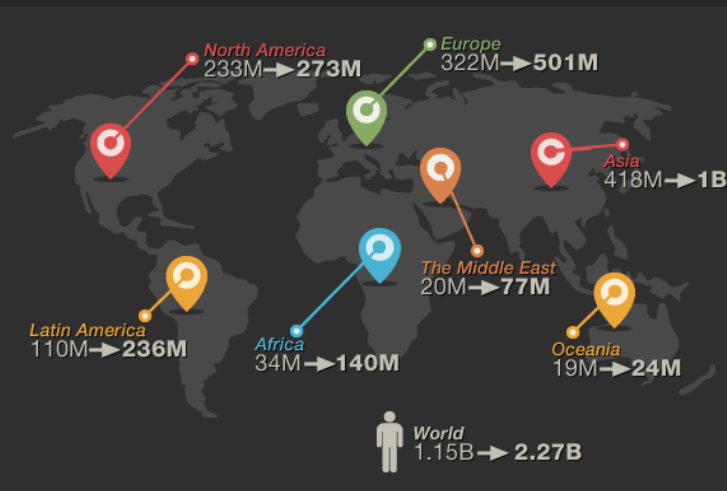
- The Internet has transformed the ways in which individuals, groups, and organizations communicate, obtain information, access entertainment, and conduct their economic and social activities.



The Internet

In 2012, there were over *2.4 billion users*

Internet population **2007 vs 2012**, a 2x increase in 5 years



Data source: Internet World Stats

www.pingdom.com

Financial Networks

The advances in information technology and globalization have further shaped today's financial world into a **complex network**, which is characterized by distinct sectors, the proliferation of new financial instruments, and with increasing international diversification of portfolios.

Financial Networks

As pointed out by Sheffi (2005) in his book, *The Resilient Enterprise*, one of the main characteristics of disruptions in networks is **“the seemingly unrelated consequences and vulnerabilities stemming from global connectivity.”**

Financial service firms were heavily impacted by **the recession** and are also dealing with **increasing numbers of cyber attacks**.

Financial Networks

In 2008 and 2009, the world reeled from the effects of the financial credit crisis; leading financial services and banks closed (including the investment bank Lehman Brothers), others merged, and the financial landscape was changed for forever.

Financial Networks

In 2008 and 2009, the world reeled from the effects of the financial credit crisis; leading financial services and banks closed (including the investment bank Lehman Brothers), others merged, and the financial landscape was changed for forever.

The domino effect of the U.S. economic troubles rippled through overseas markets and pushed countries such as Iceland to the verge of bankruptcy.

Financial Networks

It is crucial for the decision-makers in financial systems (managers, executives, and regulators) to be able **to identify a financial network's vulnerable components** to protect the functionality of the network.

Financial networks, as extremely important infrastructure networks, have a great impact on the global economy, and their study has recently also attracted attention from researchers in the area of complex networks.

Financial Networks

V. Boginski, S. Butenko, and P. M. Pardalos, 2005. Statistical Analysis of Financial Networks. *Computational Statistics and Data Analysis* 48(2), 431-443.

V. Boginski, S. Butenko, and P. M. Pardalos, 2003. On Structural Properties of the Market Graph. In *Innovations in Financial and Economic Networks*, A. Nagurney (ed.), Edward Elgar Publishers, pp. 28-45.

G. A. Bautin, V. A. Kalyagin, A. P. Koldanov, P. A. Koldanov, P. M. Pardalos, 2013. Simple measure of similarity for the market graph construction, special issue of *Computational Management Science* on Financial Networks.

Computational Management Science

10027

Computational Management Science • Volume 10 • Numbers 2–3 • 2013 • pp. 77–276

Editors

Beno Baudry
Hans Amman
Patrick Pardollé

Editorial Board

M.C. Bartholomew-Stiggs
Aharon Ben-Tal
Eduard Bojor
Mark Broadie
Sergio Bruni
Marco Campi
Nicola Chiaradonna
Thomas Coleman
Louis-Edouard
Schweickert
Robert Fourer
Marek Fukuda
Evel Gleditsch
Mehmet Güneş
Hiroshi Harashina
Brian Korte
Daniel Kuhn
Sven Leyffer
Leo Liberti
István Maros
János Mészáros
Hans-Martin
Anna Nagurny
Pascal Parys
Louis F. Pau
Georg Pfaff
Stefan Pöhl
Leonidas Pitsoulis
Andreas Pohl
Andreas Römisch
Wolfgang Römisch
Rüdiger Schütz
Alexander Shapiro
Attila Székely
Theodore Tsalikis
Lutz Vösch
Stefan Walz
Peter Winker
Georgios Zaccour

Special Issue: Financial Networks

Guest Editor: Anna Nagurny

EDITORIAL

Financial networks
A. Nagurny 77

ORIGINAL PAPERS

- Computational study of the US stock market evolution: a rank correlation-based network model
O. Narukhina, V. Bogdanov, S. Bruni 85
- A simple measure of similarity for the modular graph construction
G.A. Bounie, V.A. Bounie, A.P. Bounie, P.A. Bounie, D.M. Bounie 103
- Financial contagion: understanding the exposure network of the Mexican financial system
J.P. Sotomayor-Margam, J. Martínez-Fernández, F. López-Gallo 121
- Assessing interbank contagion using simulated networks
G. Babai, C. Böh 137
- Network analysis of the eMIP overnight money market: the informational value of different aggregation levels for systemic dynamic processes
F. Pösch, D. Brückner, T. Lutz 151
- Bolton network endogenous network dynamics
T. Pösch, F. Pösch 167
- Financial networks with socially responsible investing
Q. Guo, X. He, T. Hu 181
- The coordination of integrated corporate financial networks and supply chain networks with stochastic risk
Z. Liu 197

EDITORIAL BOARD

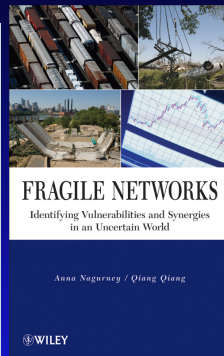
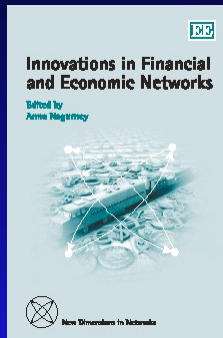
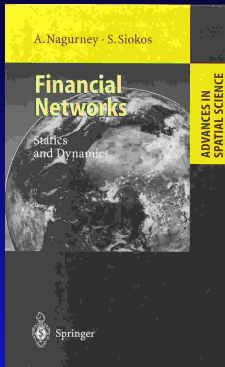
ISSN 1539-3062 (print) / ISSN 1539-3070 (online) / ISSN 1539-3062 (print) / ISSN 1539-3070 (online)
Abstracts of the Journal are available in English, French, German, Italian, Japanese, Korean, Spanish, and Chinese.
Reprints of the Journal are available in English, French, German, Italian, Japanese, Korean, Spanish, and Chinese.

10 (2–3) 77–276 (June 2013)

Printed on acid-free paper



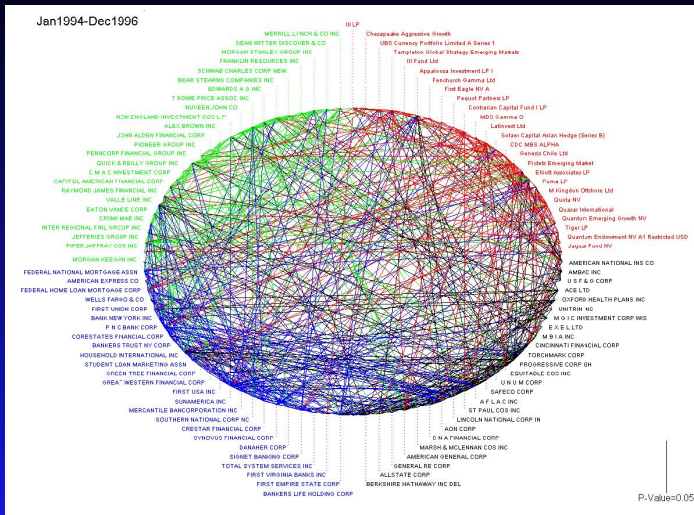
Financial Networks



Connectivity and Vulnerability

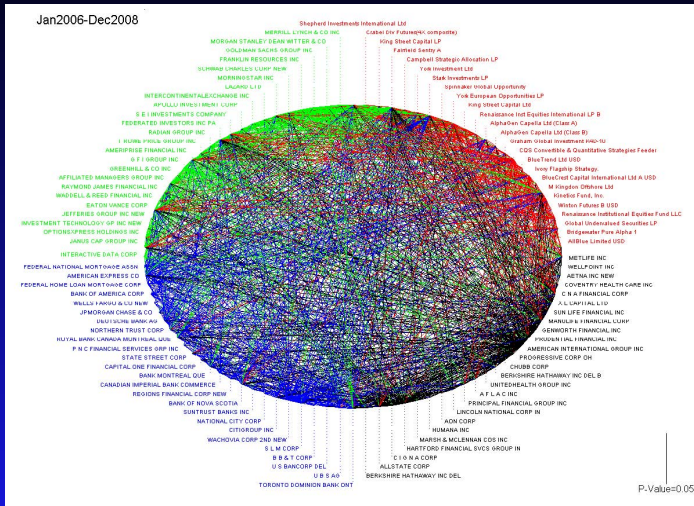
Recent empirical research has shown that connections increase before and during financial crises.

Empirical Evidence – January 1994 – December 1996



Granger Causality Results: **Green Broker**, **Red Hedge Fund**, **Black Insurer**, **Blue Bank** Source: Billio, Getmansky, Lo, and Pelizzon (2011)

Empirical Evidence – January 2006 – December 2008



Granger Causality Results: **Green Broker**, **Red Hedge Fund**, Black Insurer, Blue Bank Source: Billio, Getmansky, Lo, and Pelizzon (2011)

Financial Networks

Nevertheless, there is very little literature that addresses the vulnerability of financial networks.

Our network performance measure for financial networks captures both economic behavior as well as the underlying network/graph structure and the dynamic reallocation after disruptions.

The results are contained in the paper, "Identification of Critical Nodes and Links in Financial Networks with Intermediation and Electronic Transactions," A. Nagurney and Q. Qiang, in *Computational Methods in Financial Engineering*, E. J. Kontoghiorghes, B. Rustem, and P. Winker, Editors, Springer, Berlin, Germany (2008), pp 273-297.

Cyber Crime and Network Economics

Cyber Crime

- Cyber crimes continue to be quite costly for organizations. The Ponemon Institute (2012) determined that the average annualized cost for 56 benchmarked organizations is \$8.9 million per year, with a range from \$1.4 million to \$46 million each year per company. Last year's average cost per benchmarked organization was \$8.4 million.

Cyber Crime

- **Cyber crimes continue to be quite costly for organizations.** The Ponemon Institute (2012) determined that the average annualized cost for 56 benchmarked organizations is \$8.9 million per year, with a range from \$1.4 million to \$46 million each year per company. Last year's average cost per benchmarked organization was \$8.4 million.
- **Cyber crime cost varies by organizational size.** Results reveal a positive relationship between organizational size (as measured by enterprise seats) and annualized cost. However, based on enterprise seats, the Ponemon Institute (2012) determined that small organizations incur a significantly higher per capita cost than larger organizations (\$1,324 versus \$305).

Cyber Crime

- **Cyber crimes continue to be quite costly for organizations.** The Ponemon Institute (2012) determined that the average annualized cost for 56 benchmarked organizations is \$8.9 million per year, with a range from \$1.4 million to \$46 million each year per company. Last year's average cost per benchmarked organization was \$8.4 million.
- **Cyber crime cost varies by organizational size.** Results reveal a positive relationship between organizational size (as measured by enterprise seats) and annualized cost. However, based on enterprise seats, the Ponemon Institute (2012) determined that small organizations incur a significantly higher per capita cost than larger organizations (\$1,324 versus \$305).
- **All industries fall victim to cyber crime, but to different degrees with defense, utilities and energy, and financial service companies** experiencing higher costs than organizations in retail, hospitality, and consumer products.

Cyber Crime and Financial Institutions

According to a recent survey cyber crime is placing heavy strains on the global financial sector, with cyber crime now the second most commonly reported economic crime affecting financial services firms.

Cyber Crime and Financial Institutions

According to a recent survey cyber crime is placing heavy strains on the global financial sector, with cyber crime now the second most commonly reported economic crime affecting financial services firms.

Cyber crime accounted for 38% of all economic crimes in the financial sector, as compared to an average of 16% across all other industries.

Cyber Crime and Financial Institutions

According to a recent survey cyber crime is placing heavy strains on the global financial sector, with cyber crime now the second most commonly reported economic crime affecting financial services firms.

Cyber crime accounted for 38% of all economic crimes in the financial sector, as compared to an average of 16% across all other industries.

Cyber attacks are intrusive and economically costly. In addition, they may adversely affect a companys most valuable asset its reputation.

Cyber Attacks

The most costly cyber crimes are those caused by denial of service, malicious insider and web-based attacks. These account for more than 58 percent of all cyber crime costs per organization on an annual basis. Mitigation of such attacks may require enabling technologies, intrusion prevention systems, applications security testing solutions and enterprise solutions.

Network Economics of Cyber Crime

As noted by Sarnikar and Johnson (2009), **a secure financial market system is critical to our national economy**, with statistics on incident reports collected and disseminated by the Computer Emergency Response Team (CERT) demonstrating that a disproportionate number of security incidents occur in the financial industry.

With financial service firms providing one of the critical infrastructure networks on which our economy and society depends, it is imperative to be able to identify their vulnerabilities to cyber attacks in a rigorous, quantifiable manner as well as to identify possible synergies associated with information sharing.

Network Economics of Cyber Crime

Only by capturing the complexities and the underlying behavior can one then mitigate the risk as well as identify where to invest in order to secure the financial networks on which so many of the financial transactions now depend.

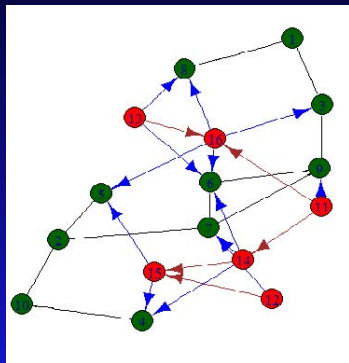
Network Economics of Cyber Crime

Green Nodes represent
Institutions

Red Nodes the Attackers
Red Edges between Attackers
can represent collusion or
transactions of stolen goods.

Black Edges between
Institutions can show sharing
of information and mutual
dependence.

Blue Edges between the
Attacker and Institution can
represent threats and attacks.



Network Economics of Cyber Crime

We lay the foundation for the development of network economics based models for cyber crime in financial services.

We use, as the framework, spatial network economic models, presenting here a single commodity model.

Our view is that financial firms produce/possess commodities (or products) that hackers (criminals) seek to obtain.

Both financial services firms as well as hackers are economic agents.

We assume that the firms (as well as the hackers) can be located in different regions of a country or in different countries. Financial service firms may also be interpreted as prey and the hackers as predators.

Network Economics of Cyber Crime

Commodities or products that the hackers seek to acquire may include: credit card numbers, password information, specific documents, etc.

The financial firms are the producers of these commodities whereas the hackers act as agents and “sell” these products, if they acquire them, at the “going” market prices. There is a “price” at which the hackers acquire the financial commodity from a financial institution and a price at which they sell the hacked product in the demand markets. The former we refer to as the supply price and the latter is the demand price.

Network Economics of Cyber Crime

In addition, we assume that there is a transaction cost associated between each pair of financial and demand markets for each commodity. These transaction costs can be generalized costs that also capture risk.

Network Economics of Cyber Crime

In the financial network cyber crime problem, we seek to determine the commodity supply prices, the demand prices, and the hacked product trade flows satisfying the equilibrium condition that, for each financial commodity, the demand price is equal to the supply price plus the transaction cost, if there is “trade” between the pair of financial and demand markets; if the demand price is less than the supply price plus the transaction cost, then there will be no (illicit) trade.

Network Economics of Cyber Crime

Indeed, if the cyber criminals do not find demand markets for their acquired financial commodities (since there are no consumers willing to pay the price) then there is no economic incentive for them to acquire the financial commodities.

To present another criminal network analogue – consider the market for illegal drugs, with the U.S. market being one of the largest, if not the largest one. If there is no demand for the drugs then the suppliers of illegal drugs cannot recover their costs of production and transaction and the flows of drugs will go to zero.

Network Economics of Cyber Crime

The framework that we utilize as the foundation for our modeling, analysis, and, ultimately, policy-making recommendations is that of spatial economics and network equilibrium. Background can be found in the books by Nagurney (1999, 2003) with analogues to financial networks made in the book by Nagurney and Siokos (1997)

The Model

The Model



Figure 1: A bipartite network of the model with financial institutions and demand markets for hacked products

Denote a typical financial institution by i and a typical demand market by j . Let s_i denote the supply of the commodity associated with i and let π_i denote the supply price of the commodity associated with i . Let d_j denote the demand associated with demand market j and let ρ_j denote the demand price associated with demand market j .

The Model

Let Q_{ij} denote the possible illicit nonnegative commodity trade flow between the firm and demand market pair (i, j) and let c_{ij} denote the nonnegative unit transaction cost associated with obtaining the product between (i, j) .

The market equilibrium conditions, assuming perfect competition, take the following form: For all pairs of firms and demand markets $(i, j) : i = 1, \dots, m; j = 1, \dots, n$:

$$\pi_i + c_{ij} \begin{cases} = \rho_j, & \text{if } Q_{ij}^* > 0 \\ \geq \rho_j, & \text{if } Q_{ij}^* = 0. \end{cases} \quad (1)$$

The condition (1) states that if there is illicit trade between a market pair (i, j) , then the supply price at i plus the transaction cost between the firm and demand market pair must be equal to the demand price at demand market j in equilibrium; if the supply price plus the transaction cost exceeds the demand price, then there will be no illicit trade between the market pair.

The Model

The feasibility conditions must hold for every i and j :

$$s_i = \sum_{j=1}^n Q_{ij} \quad (2)$$

and

$$d_j = \sum_{i=1}^m Q_{ij}. \quad (3)$$

(2) and (3) state that the markets clear and that the supply at each supply market is equal to the sum of the financial commodity flows to all the demand markets. Also, the demand at a demand market must be satisfied by the sum of the commodity shipments from all the supply markets. Let K denote the closed convex set where $K \equiv \{(s, Q, d) | (2) \text{ and } (3) \text{ hold}\}$.

The Model

The supply price, demand price, and transaction cost structure is now discussed. Assume that the commodity price associated with a firm may depend upon the supply of the commodity at every firm, that is,

$$\pi = \pi(s) \quad (4)$$

where π is a known smooth function.

Similarly, the demand price associated with a demand market may depend upon, in general, the demand of the commodity at every demand market, that is,

$$\rho = \rho(d) \quad (5)$$

where ρ is a known smooth function.

The transaction cost between a pair of supply and demand markets may, in general, depend upon the shipments of the commodity between every pair of markets, that is,

$$c = c(Q) \quad (6)$$

The Variational Inequality Formulation

We now present the variational inequality formulation of the equilibrium conditions (1).

Theorem 1. A commodity production, shipment, and consumption pattern $(s^*, Q^*, d^*) \in K$ is in equilibrium if and only if it satisfies the variational inequality problem:

$$\pi(s^*) \cdot (s - s^*) + c(Q^*) \cdot (Q - Q^*) - \rho(d^*) \cdot (d - d^*) \geq 0, \quad \forall (s, Q, d) \in K. \quad (7)$$

Qualitative Properties

Variational inequality (7) may be put into the standard form (1) by defining the vector $x \equiv (s, Q, d) \in R^{m+mn+n}$ and the vector $F(x)^T \equiv (\pi(s), c(Q), -\rho(d))$ which maps R^{m+mn+n} into R^{m+mn+n} .

In order to simplify the qualitative analysis, a simple calculation yields that $F(x)$ is a partitionable function of order 3 (cf. Nagurney (1999)). Hence, immediately one can state the following result.

Theorem 2. $F(x)$ as defined above is monotone, strictly monotone, or strongly monotone if and only if $\pi(s)$, $c(Q)$, and $\rho(d)$ are each monotone, strictly monotone, or strongly monotone in s , Q , d , respectively.

Qualitative Properties

Since the feasible set K is not compact, existence of an equilibrium pattern (s^*, Q^*, d^*) does not immediately follow. Nevertheless, it follows from the standard theory of variational inequalities that if π , c , and ρ are strongly monotone, then existence and uniqueness of the equilibrium production, flow, and consumption pattern are guaranteed.

Numerical Example

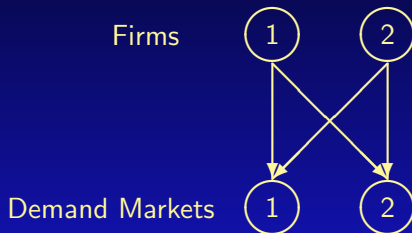


Figure 2: Example Network Topology

Numerical Example

The supply price functions are:

$$\pi_1(s) = 5s_1 + s_2 + 2, \quad \pi_2(s) = 2s_2 + s_1 + 3.$$

The transaction cost functions are:

$$\begin{aligned} c_{11}(Q) &= Q_{11} + .5Q_{12} + 1, & c_{12}(Q) &= 2Q_{12} + Q_{22} + 1.5, \\ c_{21}(Q) &= 3Q_{21} + 2Q_{11} + 15, & c_{22}(Q) &= 2Q_{22} + Q_{12} + 10. \end{aligned}$$

The demand price functions are:

$$\rho_1(d) = -2d_1 - d_2 + 28.75, \quad \rho_2(d) = -4d_2 - d_1 + 41.$$

The equilibrium supply, shipment, and consumption pattern is then given by:

$$\begin{aligned} s_1^* &= 3, & s_2^* &= 2, \\ Q_{11}^* &= 1.5, & Q_{12}^* &= 1.5, & Q_{21}^* &= 0, & Q_{22}^* &= 2, \\ d_1^* &= 1.5 & d_2^* &= 3.5. \end{aligned}$$

Numerical Example

The incurred equilibrium supply prices, costs, and demand prices are:

$$\begin{aligned}\pi_1 &= 19, & \pi_2 &= 10, \\ c_{11} &= 3.25, & c_{12} &= 6.5, & c_{21} &= 18, & c_{22} &= 15.5, \\ \rho_1 &= 22.25, & \rho_2 &= 25.5.\end{aligned}$$

Numerical Example

Firm 2 does not “trade” with Demand Market 1. This is due, in part, to the high fixed cost associated with trading between this market pair. Hence, one can interpret this as corresponding to a sufficiently high transaction cost (which can also capture in a generalized setting, the risk of being caught).

The above single commodity model we have generalized to multiple financial commodities.

In addition, we have included a variety of policy interventions.

We have solved problems of this type using variational inequality algorithms with more than 250,000 variables.

Summary and Conclusions

- In this talk, we have provided an overarching perspective of our ACSC research project with a focus on the network economic model of cyber crime.

Summary and Conclusions

- In this talk, we have provided an overarching perspective of our ACSC research project with a focus on the network economic model of cyber crime.
- Other issues that members of our team have also researched is systemic risk in this context and also portfolio optimization of countermeasures.

Summary and Conclusions

- In this talk, we have provided an **overarching perspective of our ACSC research project** with a focus on the network economic model of cyber crime.
- Other issues that members of our team have also researched is **systemic risk** in this context and also portfolio optimization of countermeasures.
- Our “clients” were financial service firms, who, besides dealing with **the recession**, have also encountered a **growing number of cyber attacks**.


Summary and Conclusions

- In this talk, we have provided an **overarching perspective of our ACSC research project** with a focus on the network economic model of cyber crime.
- Other issues that members of our team have also researched is **systemic risk** in this context and also portfolio optimization of countermeasures.
- Our “clients” were financial service firms, who, besides dealing with **the recession**, have also encountered a **growing number of cyber attacks**.
- The model that we developed was a **spatial price equilibrium model** in which producers are the financial service firms and consumers are the hackers/attackers.


Summary and Conclusions

- In this talk, we have provided an **overarching perspective of our ACSC research project** with a focus on the network economic model of cyber crime.
- Other issues that members of our team have also researched is **systemic risk** in this context and also portfolio optimization of countermeasures.
- Our “clients” were financial service firms, who, besides dealing with **the recession**, have also encountered a **growing number of cyber attacks**.
- The model that we developed was a **spatial price equilibrium model** in which producers are the financial service firms and consumers are the hackers/attackers.
- We have also **developed extensions of the model** to include multiple commodities (financial products) as well as policy interventions in the form of price supports to make, for example, the supply price “high” and hence less attractive for the attackers

THANK YOU!




The Virtual Center for Supernetworks



Supernetworks for Optimal Decision-Making and Improving the Global Quality of Life

Director's Welcome	About the Director	Projects	Supernetworks Laboratory	Center Associates	Media Coverage	What's New
Downloadable Articles	Visuals	Audio/Video	Books	Commentaries & OpEds	The Supernetwork Sentinel	Congratulations & Kudos



Network Models in Economics and Finance
Athens, Greece, June 2013

The Virtual Center for Supernetworks is an interdisciplinary center at the Isenberg School of Management that advances knowledge on large-scale networks and integrates operations research and management science, engineering, and economics. Its Director is Dr. Anna Nagurney, the John F. Smith Memorial Professor of Operations Management.


Mission: The Virtual Center for Supernetworks fosters the study and application of supernetworks and serves as a resource on networks ranging from transportation and logistics, including supply chains, and the Internet, to a spectrum of economic networks.

The Applications of Supernetworks Include: decision-making, optimization, and game theory; supply chain management; critical infrastructure from transportation to electric power networks; financial networks; knowledge and social networks; energy, the environment, and sustainability; risk management; network vulnerability, resiliency, and performance metrics; humanitarian logistics and healthcare.

Announcements and Notes	Photos of Center Activities	Photos of Network Innovators	Friends of the Center	Course Lectures	Fulbright Lectures	Umass Amherst INFORMS Student Chapter
Professor Anna Nagurney's Blog	Network Classics	Doctoral Dissertations	Conferences	Journals	Societies	Archive

Announcements and Notes from the Center Director
Professor Anna Nagurney


Updated: July 24, 2013

 Follow

Professor Anna Nagurney's Blog


RENw

Research, Education, Networks, and the World: A Female Professor Speaks




Sustaining the Supply Chain Mathematical Moments Podcast

FBS VIDEO




America Revealed

New Book




Networks Against Time



Photos of Center Activities

The Braess Paradox Translation



Information Photos

Publications

On a Paradox of Traffic Flowing

Environmental Impact Assessment of Transportation Networks with Degradable Links in an Era of Climate Change

Anna Nagurney, Qing Qiang, and Lubert K. Yeung

For more information, see: <http://supernet.isenberg.umass.edu>