A Scientific Approach to Financial Supernetworks

Anna Nagurney

John F. Smith Memorial Professor
Director of the Virtual Center for Supernetworks
Isenberg School of Management
University of Massachusetts
Amherst, Massachusetts 01003

International Expert Panel
Washington DC, March 2, 2017

We Are in a New Era of Decision-Making Characterized by:

- *complex interactions* among decision-makers in organizations;
- *alternative and, at times, conflicting criteria* used in decision-making;
- *constraints on resources*: human, financial, natural, time, etc.;
- *global reach* of many decisions;
- *high impact* of many decisions;
- *increasing risk and uncertainty*;
- the *importance of dynamics* and realizing a timely response to evolving events.

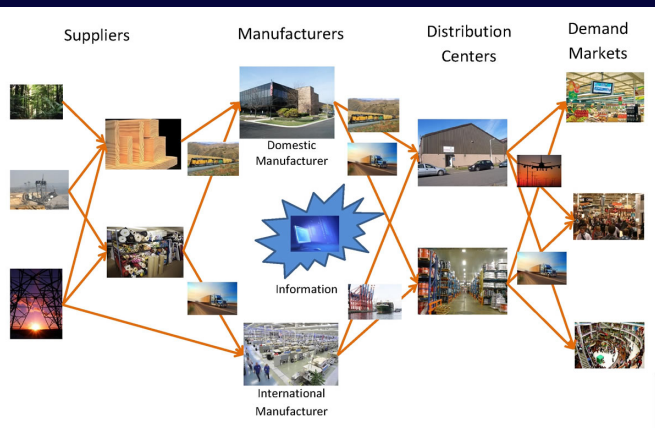
The Era of Supernetworks

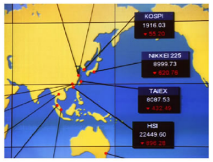
Supernetworks are *Networks of Networks*, and their prevalence in the world around us is illustrated by:

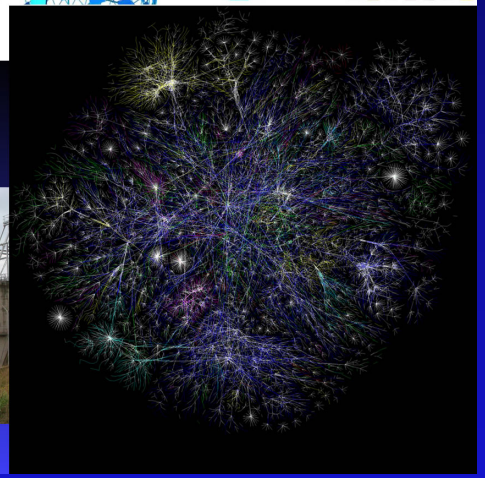
- *multimodal transportation networks*;
- *complex supply chain networks consisting of manufacturers, shippers and carriers, distributors, and retailers*;
- *electric power generation and distribution networks*,
- *multitiered financial networks*, and
- *social network platforms such as Facebook and Twitter*, along with the Internet itself,

as well as interactions among these network systems.

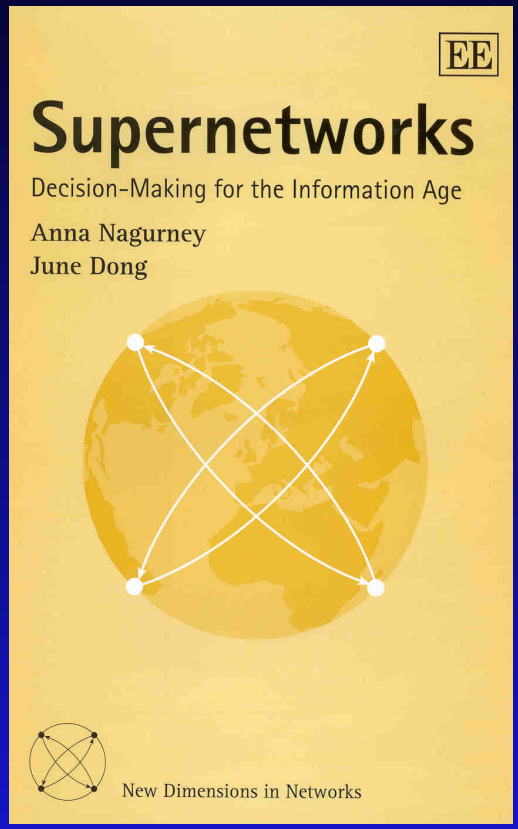
Supernetworks

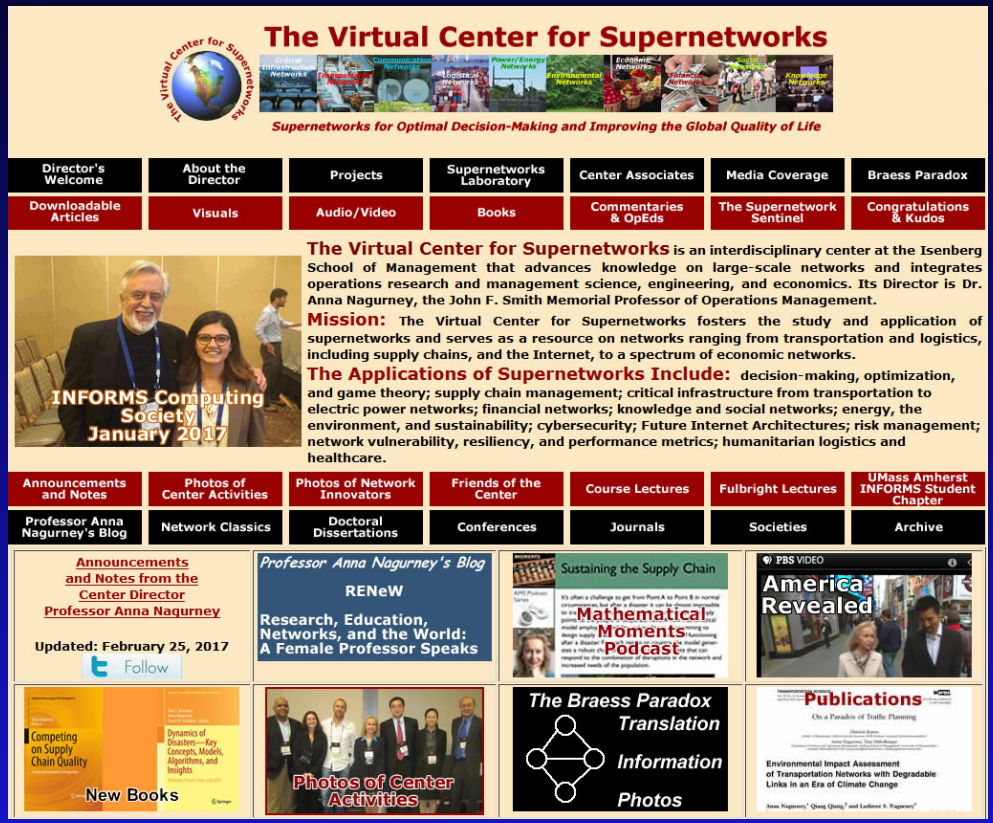






Virtual Center for Supernetworks at UMass Amherst





For more information see: https://supernet.isenberg.umass.edu/

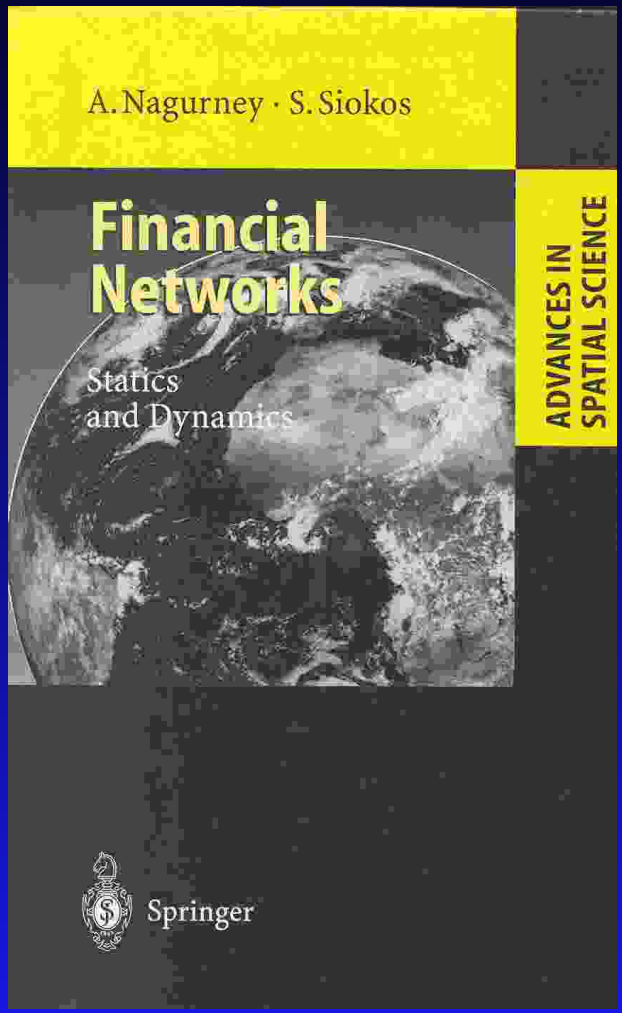
Characteristics of Networks Today

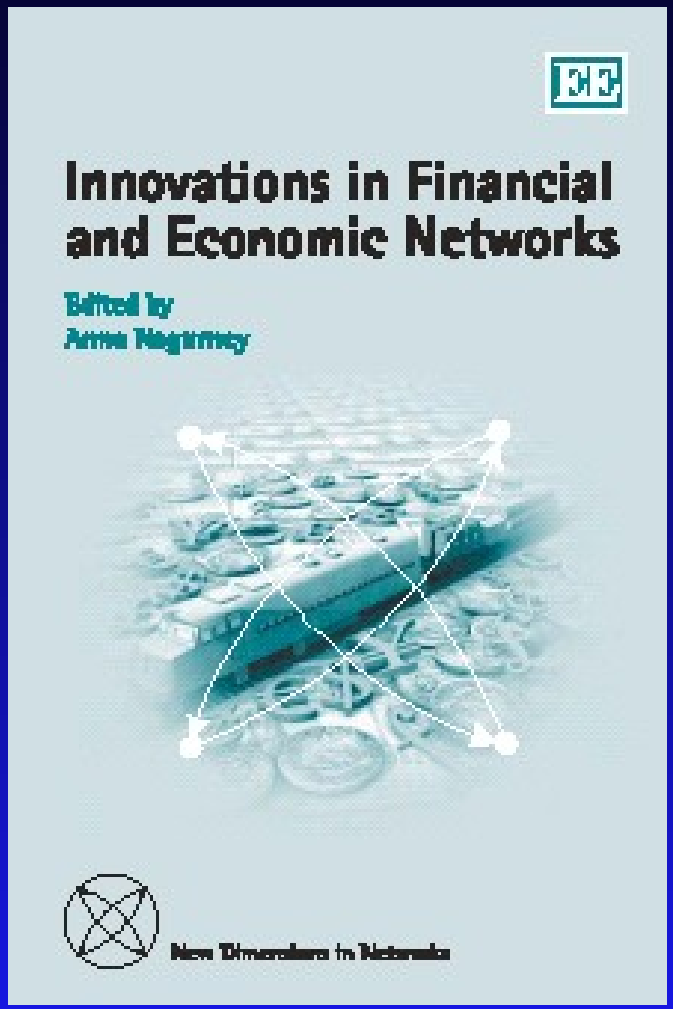
- *large-scale nature* and complexity of network topology;
- *congestion*, which leads to nonlinearities;
- *alternative behavior of users of the networks*, which may lead to paradoxical phenomena;
- *possibly conflicting criteria associated with optimization*;
- *interactions among the underlying networks themselves*, such as the Internet with electric power, financial, and transportation and logistical networks;
- recognition of *their fragility and vulnerability*;
- policies surrounding networks today may have major impacts not only economically, but also *socially, politically, and security-wise*.

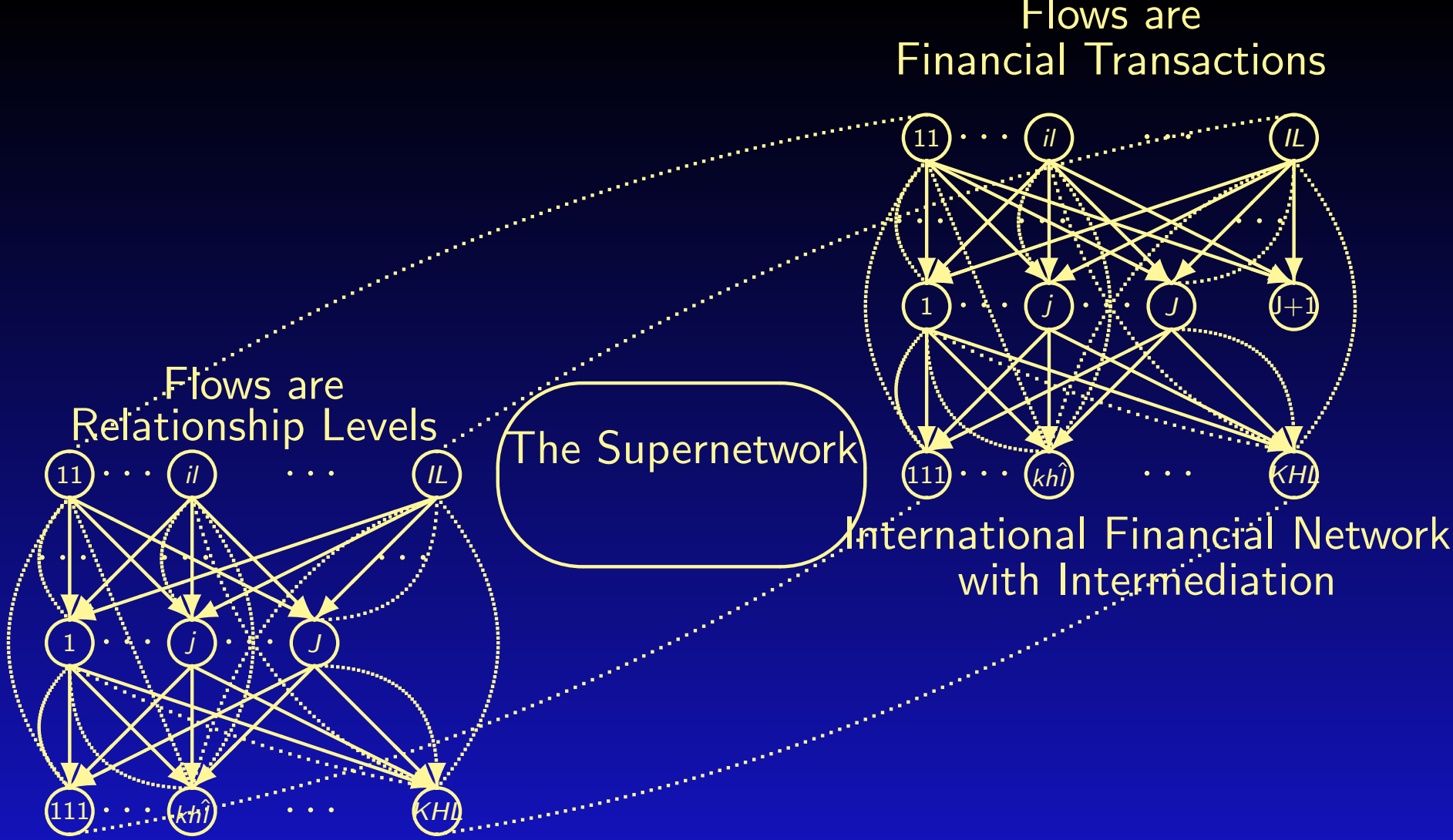
Networks consist of nodes, links, and flows and one must capture the underlying behavior and interactions of decision-makers and the induced costs, the relevant risks, and prices.

Network methodologies provide a spectrum of tools for problem formulation, analysis, and solution of both licit and illicit problems.

Financial Networks

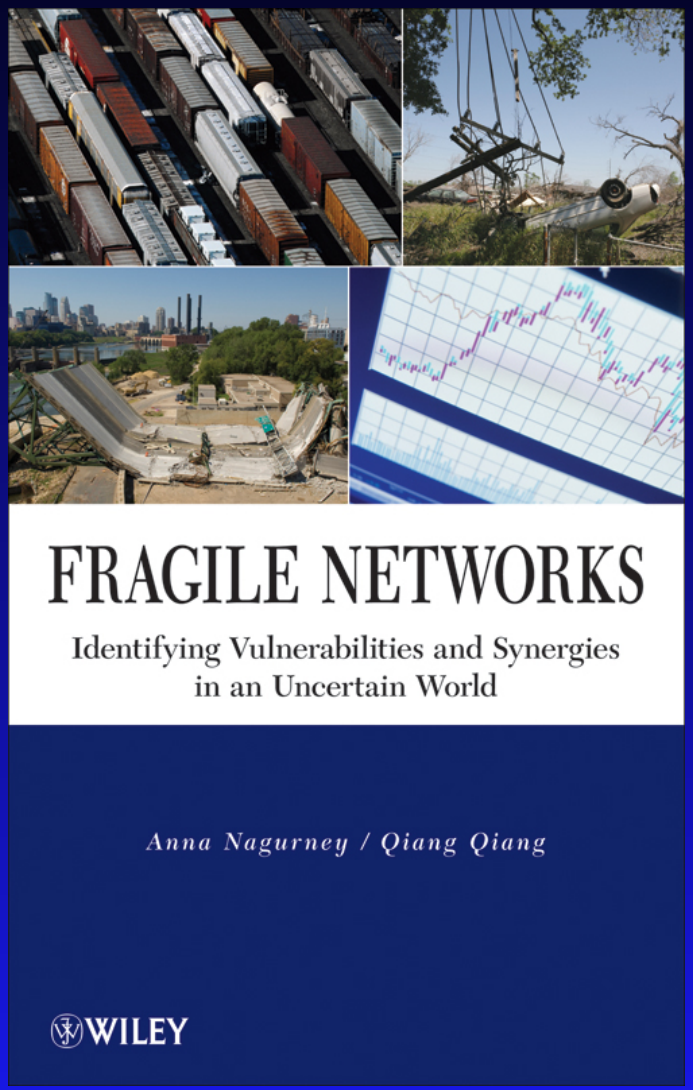






Multilevel Supernetwork Structure of the Integrated International Financial Network / Social Network System (Nagurney, Cruz, and Wakolbinger (2007))

We are Living in a World of Fragile Networks!



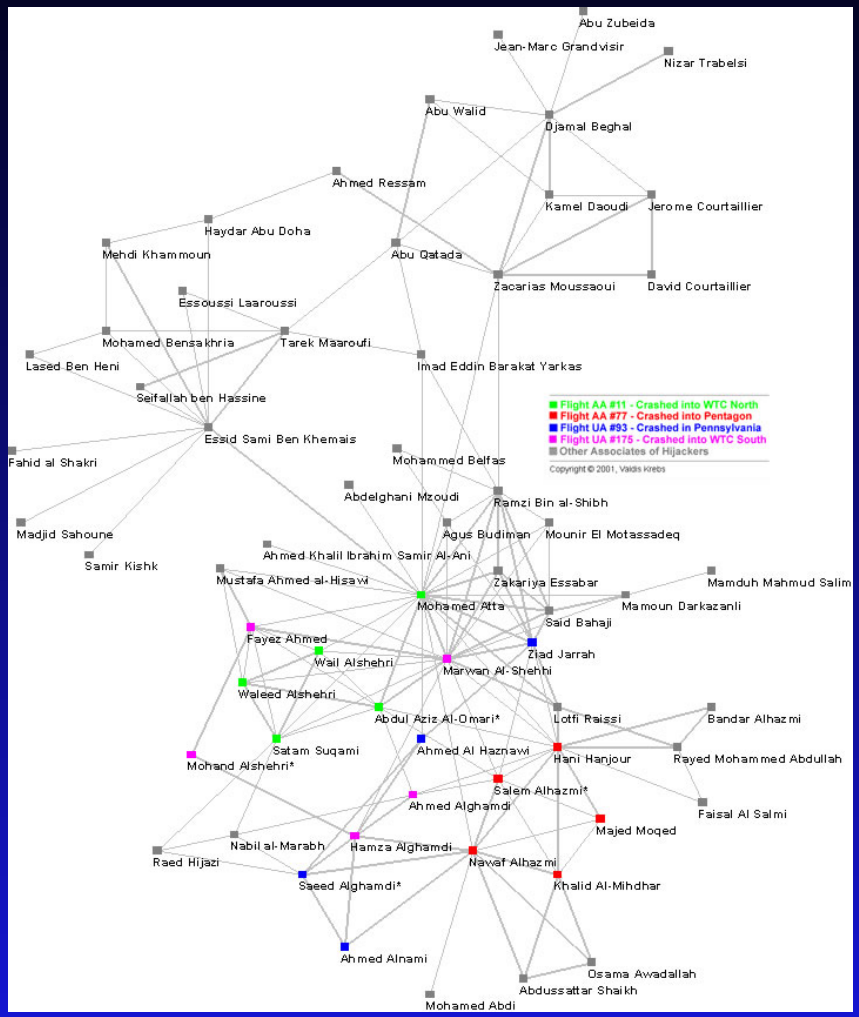
Because today's financial networks may be *highly interconnected and interdependent*, any disruptions that occur in one part of the network may produce consequences in other parts of the network, which may not only be in the same region but miles away in other countries.

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.

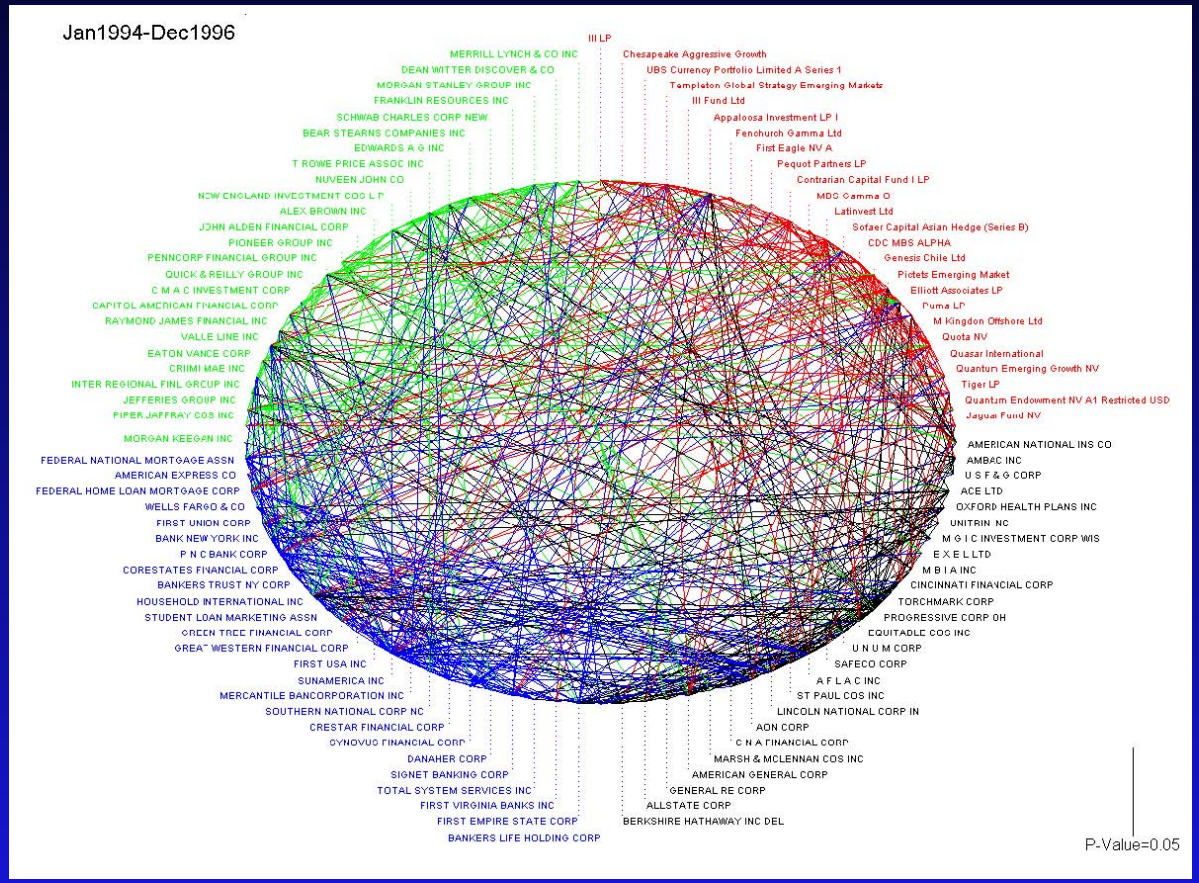
Which Nodes and Links Really Matter?

Terrorist Network



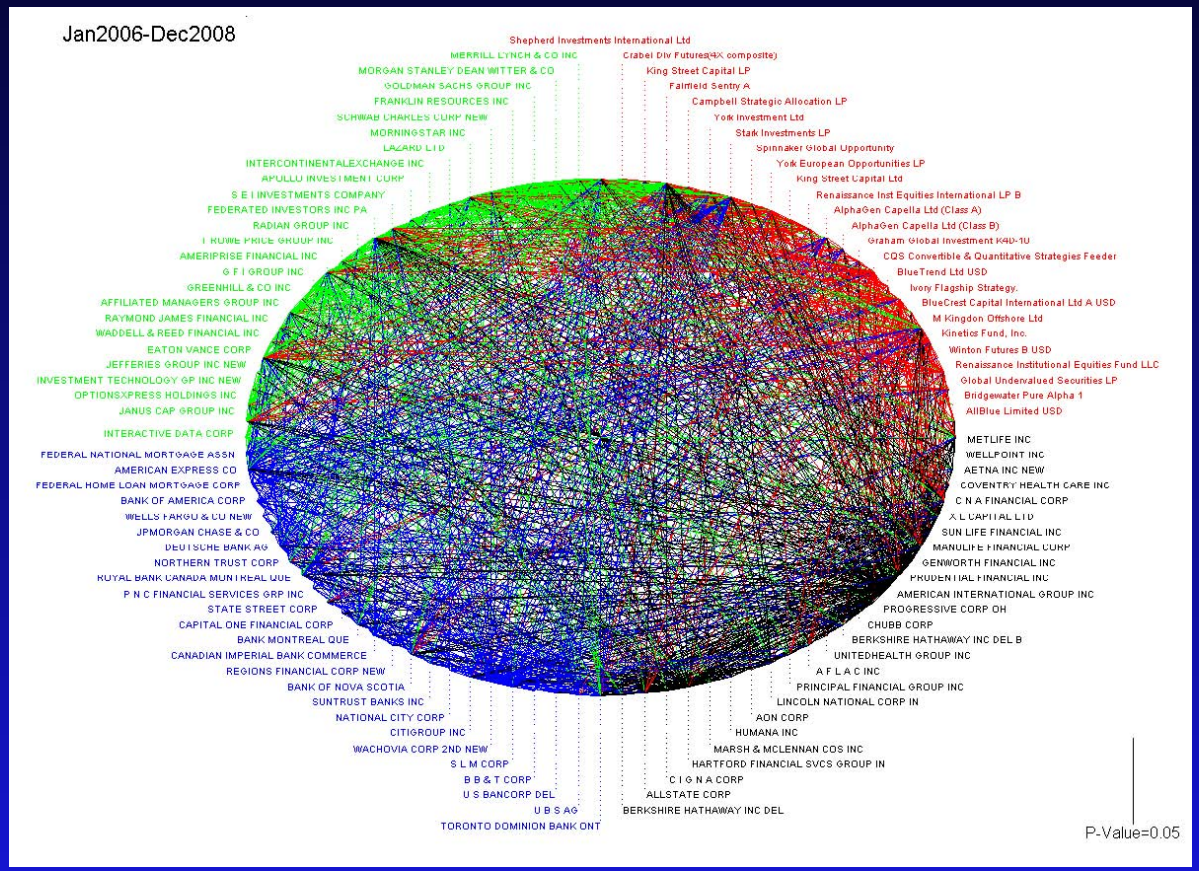
Valis Krebs (2001): Mohamed Atta scores the highest on all network centrality metrics - Degrees, Closeness, and Betweenness.

Financial Network Empirical Evidence: Jan. 1994 - Dec. 1996 - Connectivity, Vulnerability



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

Financial Network Empirical Evidence: Jan. 2006 - Dec. 2008 - Connectivity, Vulnerability

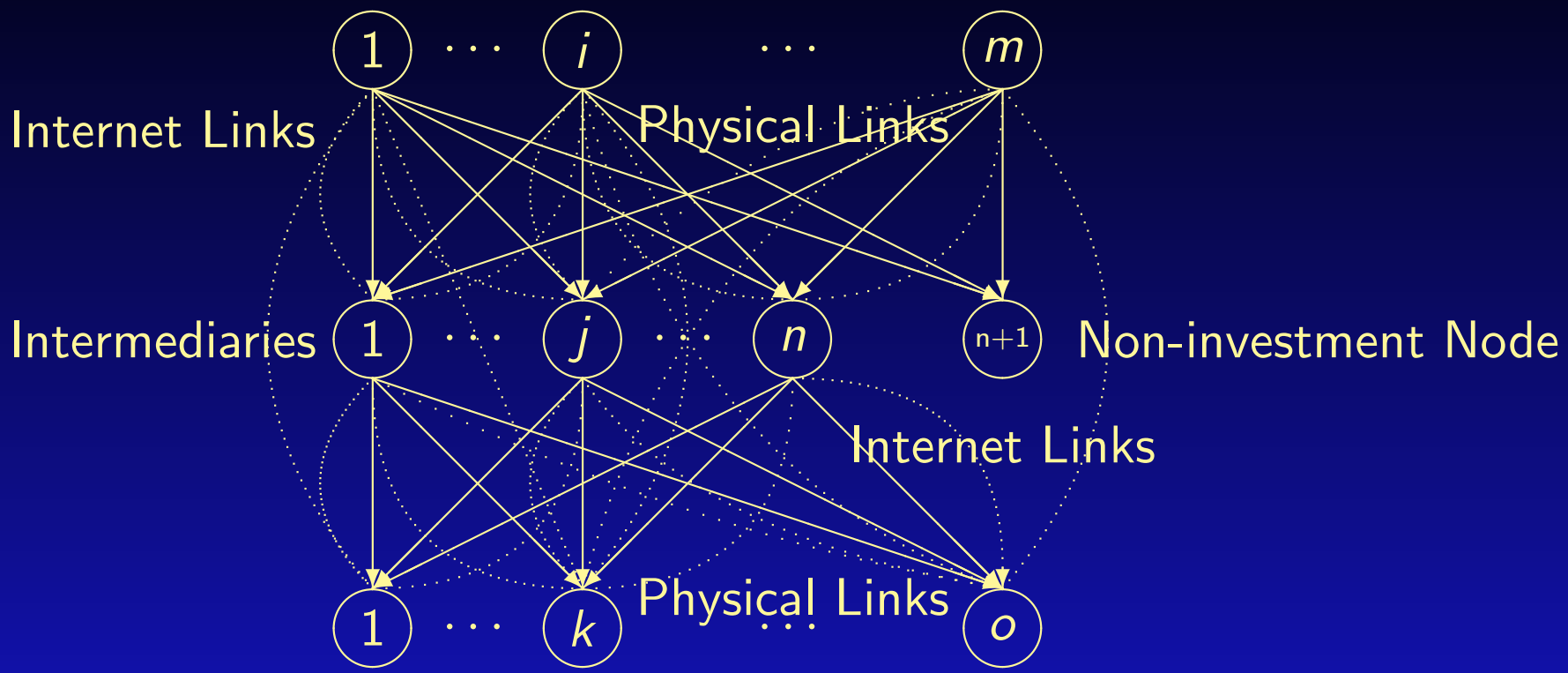


Granger Causality Results: Green Broker, Red Hedge Fund, Black Insurer, Blue Bank Source: Billio, Getmansky, Lo, and Pelizzon (2011)

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.

Our financial network performance measure (Nagurney and Qiang (2008)) and component importance indicator was published in the edited volume *Computational Methods in Financial Engineering*.

Sources of Financial Funds



Demand Markets - Uses of Funds

The Structure of the Financial Network with Intermediation and with Electronic Transactions

Definition: The Financial Network Performance Measure

The financial network performance measure, $\mathcal{E}$, for a given network topology G, and demand price functions $\rho_{3k}(d)$ $(k = 1, 2, \ldots, o)$, and available funds held by source agents S, is defined as follows:

$$\mathcal{E} = \frac{\sum_{k=1}^{o} \frac{d_k^*}{\rho_{3k}(d^*)}}{o},$$

where o is the number of demand markets in the financial network, and d_k^* and $\rho_{3k}(d^*)$ denote the equilibrium demand and the equilibrium price for demand market k, respectively.

The financial network performance measure $\mathcal{E}$ defined above is actually the average demand to price ratio. It measures the overall (economic) functionality of the financial network.

When the network topology G, the demand price functions, and the available funds held by source agents are given, a financial network is considered performing better if it can satisfy higher demands at lower prices.

Definition: Importance of a Financial Network Component

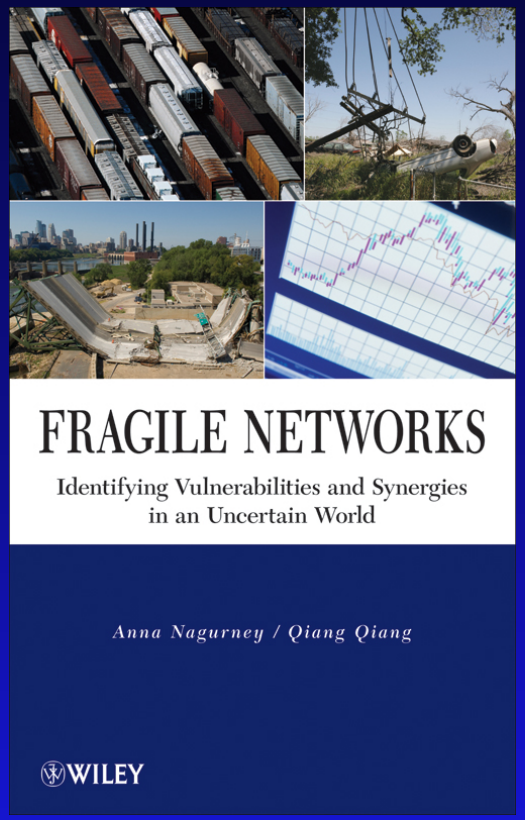
The importance of a financial network component $g \in G$, $I(g)$, is measured by the relative financial network performance drop after g is removed from the network:

$$I(g) = \frac{\triangle \mathcal{E}}{\mathcal{E}} = \frac{\mathcal{E}(G) - \mathcal{E}(G - g)}{\mathcal{E}(G)}$$

where $G - g$ is the resulting financial network after component g is removed from network G.

How I Became Interested in Criminal Networks

My *Fragile Networks* book was hacked and digital copies of it posted on websites around the globe.



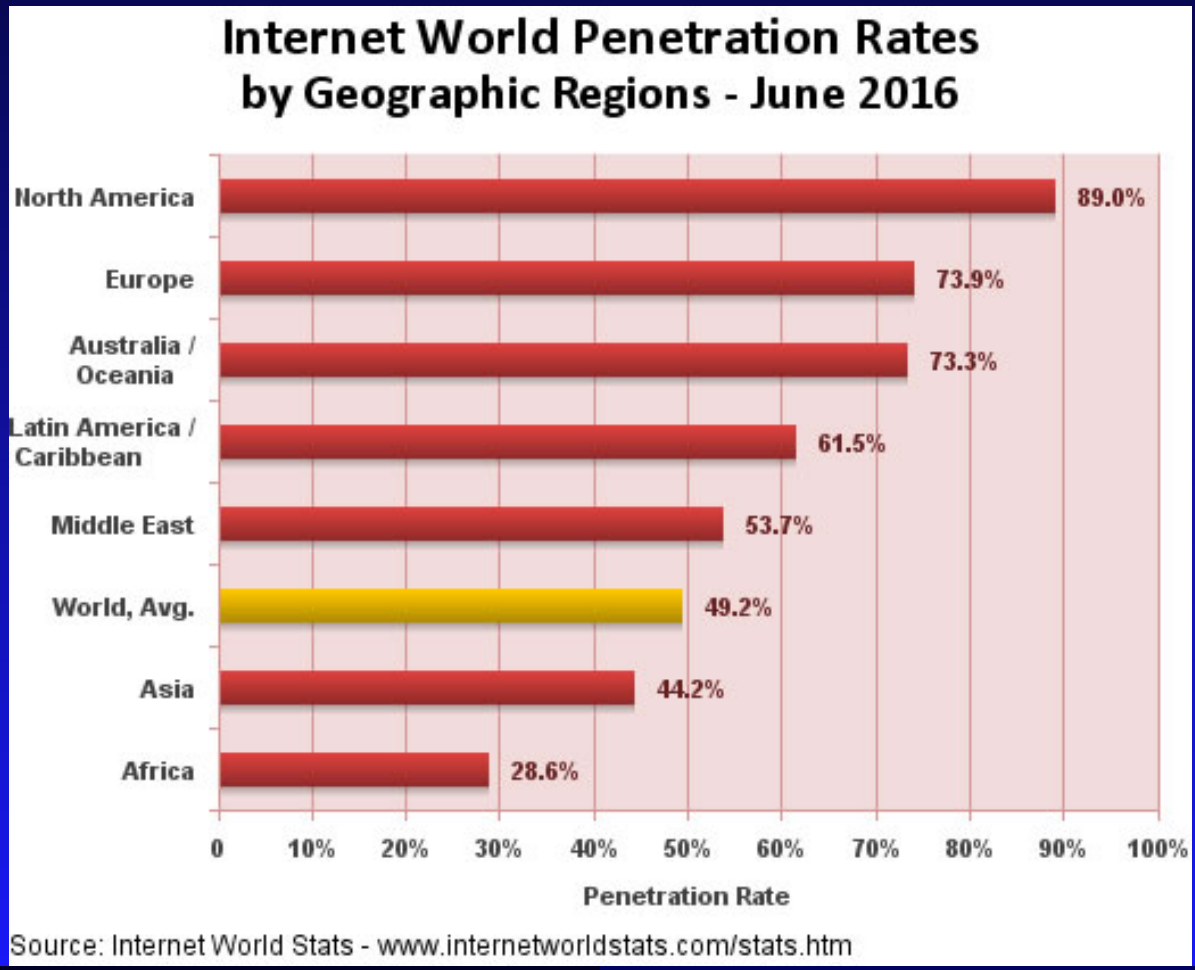
In a sense, this may be viewed as a compliment since clearly someone had determined that it has some sort of *value*.

The publisher John Wiley & Sons was notified and lawyers got involved but how do you contact and then influence those responsible for postings on rather anonymous websites?

About the same time news about cyberattacks was getting prominent attention in the media and there were those interested in working with us on related research on cybersecurity.

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

In 2012, there were over 2.4 billion users. In 2016, there are 3.5 billion users, almost half of the world population



The Cost of Cybercrime

According to the Center for Strategic and International Studies (2014), the world economy sustained $445 billion in losses from cyberattacks in 2014.

- The United States suffered a loss of $100 billion.
- Germany lost $60 billion.
- China lost $45 billion, and
- The United Kingdom reported a loss of $11.4 billion due to cybersecurity lapses.

Cybercrime

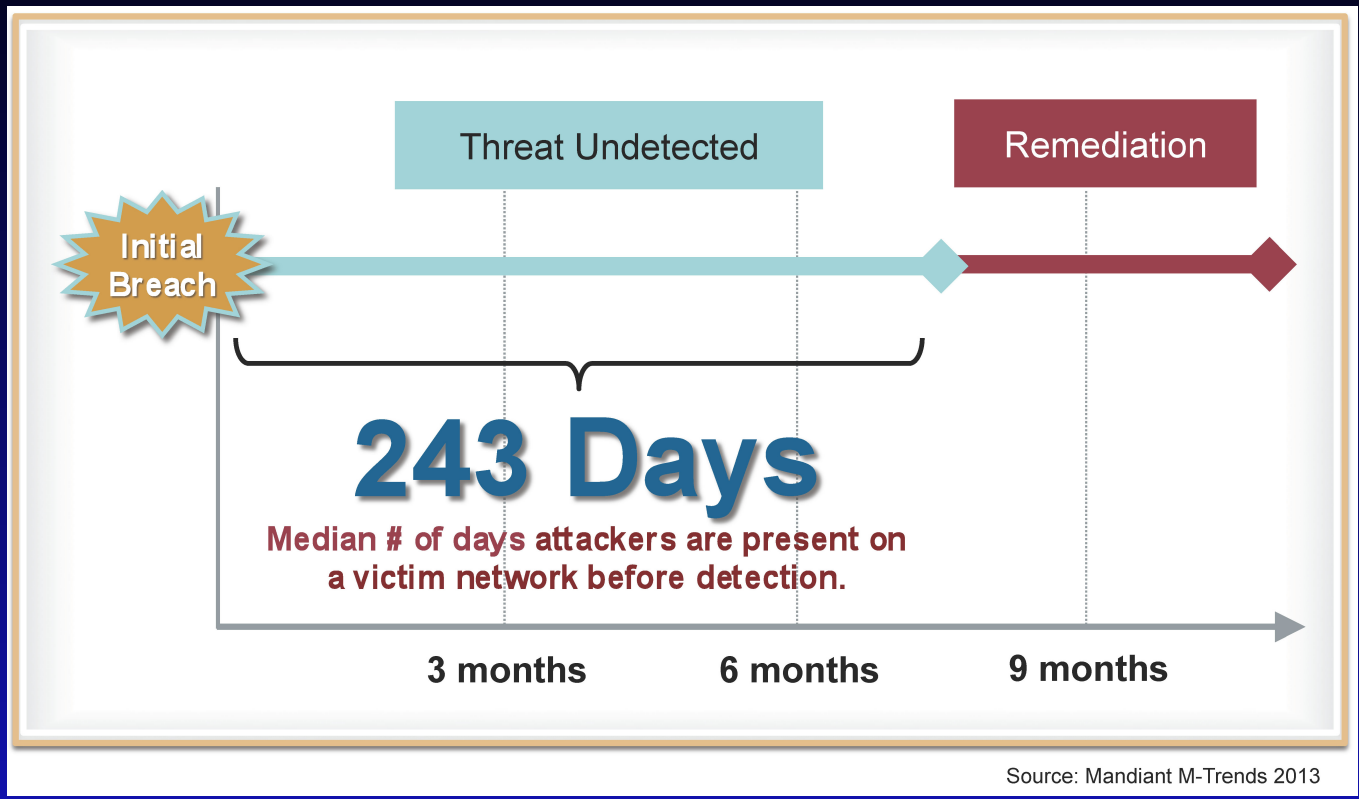
Clearly, hackers go where there is money.

Putting Cybercrime in Context

Putting Malicious Cyber Activity in Context			
CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashes	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US- cyber activity	$24 billion to $120 billion	0.2% to 0.8%	Various

Source: The Economic Impact of Cybercrime and Cyber Espionage, Center for Strategic and International Studies, July 2013, sponsored by McAfee.

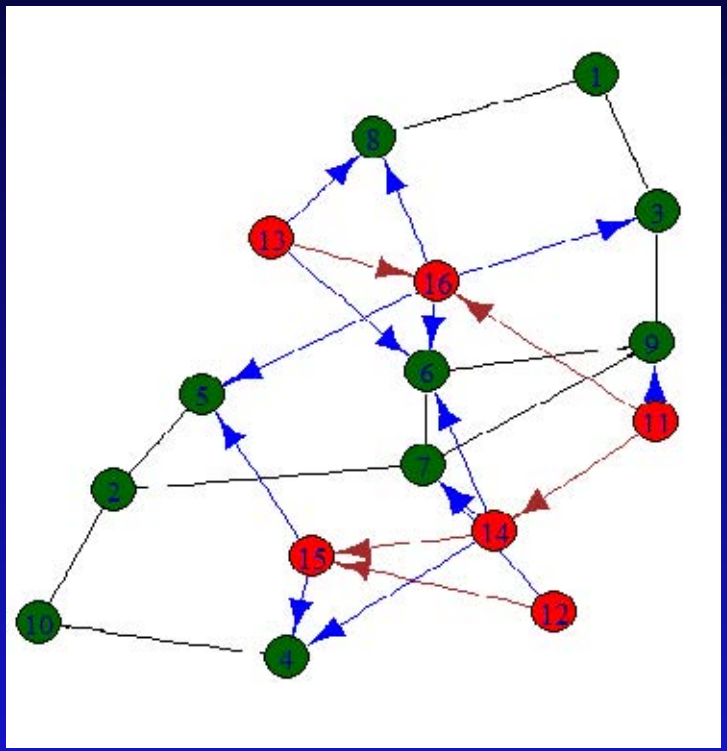
Cyberattacks



The median number of days that attackers were present on a victim's network before being discovered dropped to 146 days in 2015 from 205 days in 2014 – a trend that shows positive improvement since measuring 416 days back in 2012. However, breaches still often go undetected for years, according to Mandiant.

Network Economics of Cybercrime

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 Cybercrime

Financial firms produce/possess commodities (or products) that hackers (criminals) seek to obtain.

Financial services firms as well as hackers are economic agents.

Financial service firms may also be interpreted as prey and the hackers as predators.

There is a *supply price* at which the hackers acquire the financial commodity from a financial institution and a *demand price* at which they sell the hacked product in the demand markets.

Network Economics of Cybercrime

If the cyber criminals do not find demand markets for their acquired financial commodities then there is no economic incentive for them to acquire the financial commodities.

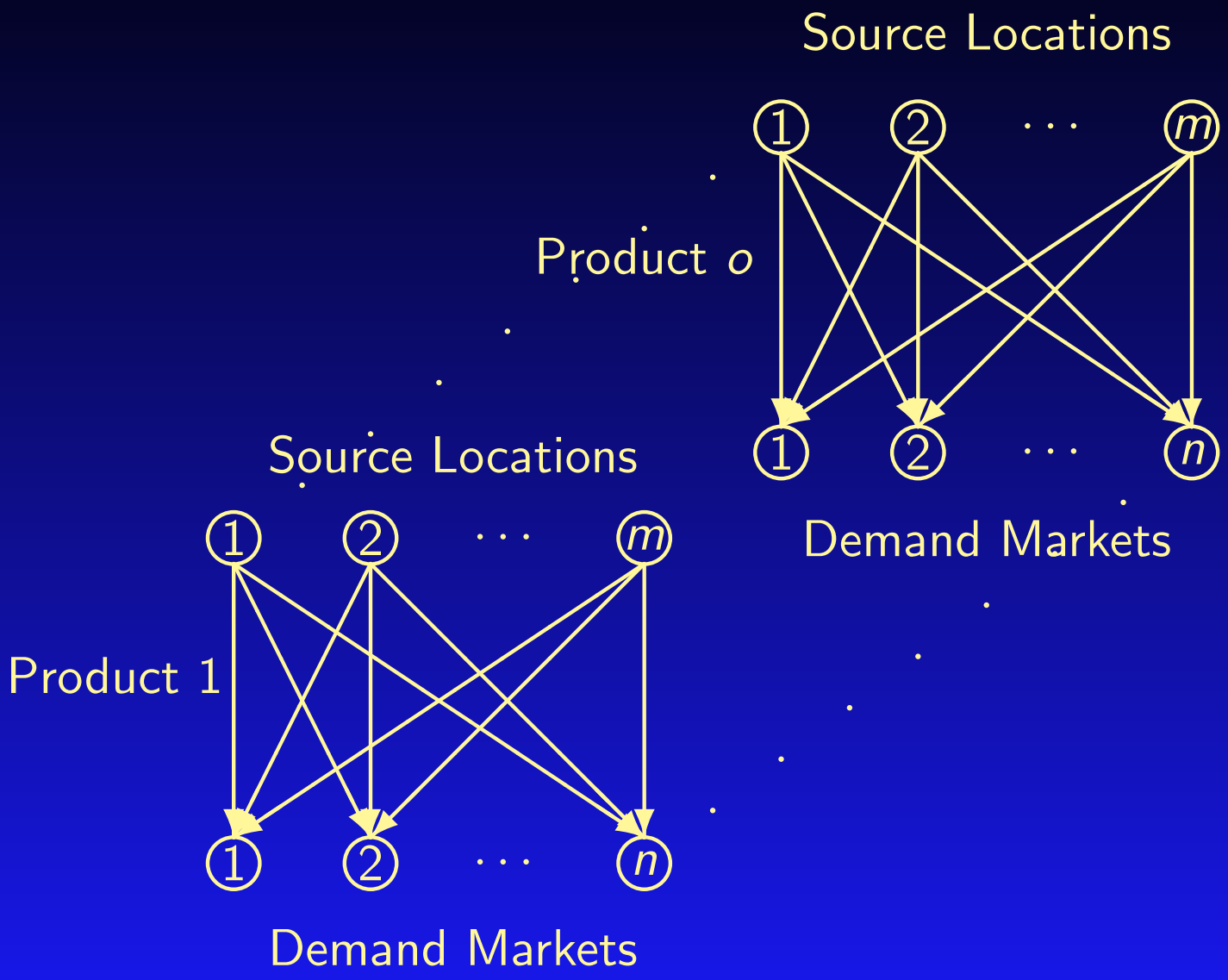
Consider the market for illegal drugs in the US. If there is no demand for the drugs then the suppliers of illegal drugs cannot recover their costs of production and transaction and the flows of illegal drugs will drop.

Perishability and Cybercrime in Financial Products

There is a short time window during which the value of an illicit financial product (such as a hacked credit card) is positive but it decreases during the time window. Thus, illicit financial products can be treated as perishable products such as fruits and vegetables.

See: A Multiproduct Network Economic Model of Cybercrime in Financial Services, Anna Nagurney, *Service Science* 7(1) (2015) pp 70-81.

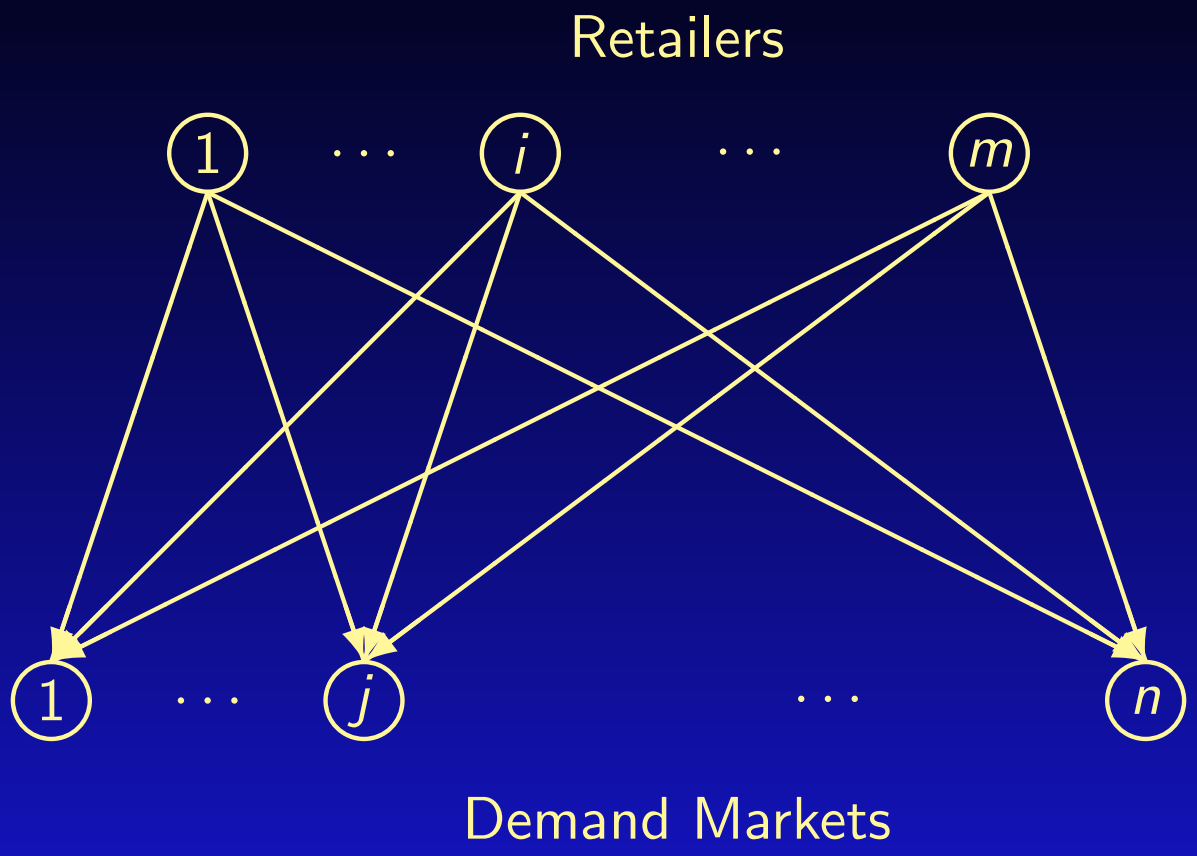
Perishability and Cybercrime in Financial Products



Cybersecurity and Supply Chains

Supply chains are also vulnerable to cyber attacks and can serve as entre points.

Cybersecurity, Supply Chains, and Game Theory



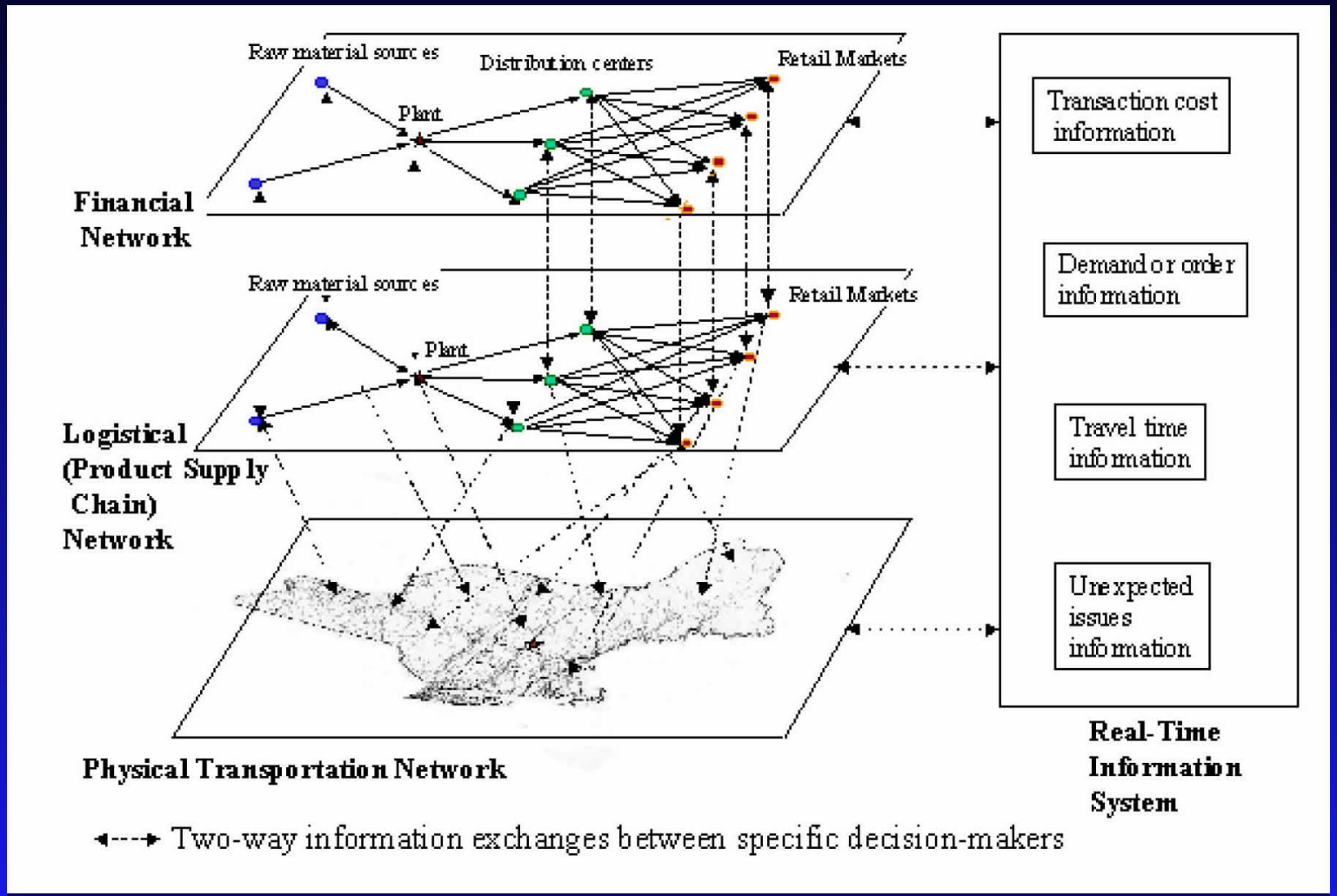
The structure of the Supply Chain Network Game Theory Model.

We also have developed an applied cooperative game theory to assess cybersecurity investments and network vulnerability.

Disrupting Illicit Financial Networks at the Source - Through Supply Chains (Licit)

Disrupting Illicit Financial Networks at the Source - Through Supply Chains (Illicit)

Disrupting Illicit Financial Networks at the Source - Through Supply Chains



Nagurney, Ke, Cruz, Hancock, Southworth, *Environment and Planning B* (2002).

Some More of Our Recent Work

A Supply Chain Network Game Theory Model of Cybersecurity Investments with Nonlinear Budget Constraints, A. Nagurney, P. Daniele, and S. Shukla (2017), *Annals of Operations Research* 248(1), pp 405-427.

Multifirm Models of Cybersecurity Investment Competition vs. Cooperation and Network Vulnerability, A. Nagurney and Shivani Shukla (2017), *European Journal of Operational Research*, in press.

A Supply Chain Game Theory Framework for Cybersecurity Investments Under Network Vulnerability, A. Nagurney, L.S. Nagurney, and S. Shukla (2015), in: *Computation, Cryptography, and Network Security*, N.J.Daras and M.Th. Rassias (Eds.), Springer, pp 381-398.

A Game Theory Model of Cybersecurity Investments with Information Asymmetry, A. Nagurney and L.S. Nagurney (2015), *Netnomics* 16(1-2), pp 127-148.

THANK YOU!