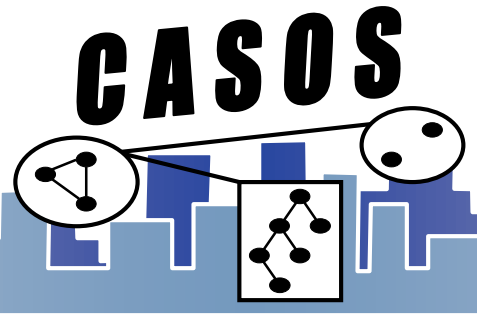


Social Network Analysis for Science of Security

Prof. Kathleen M. Carley

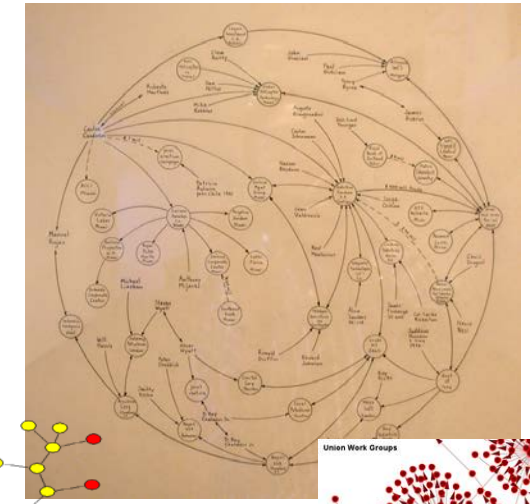
412-267-6016

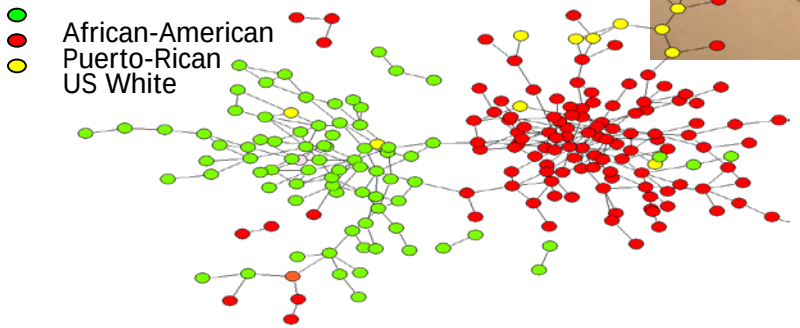
kathleen.carley@cs.cmu.edu

Networks!

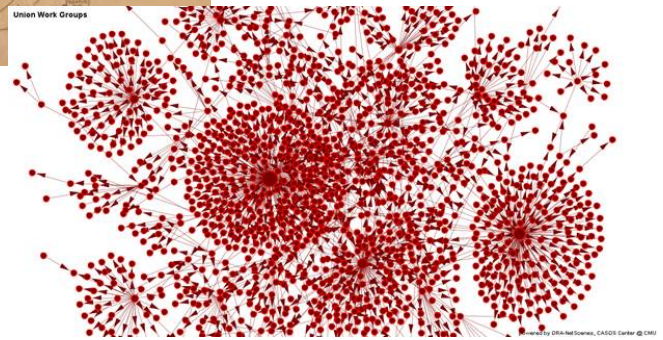
Fotosearch 2009

Network Art
Marc Lombardi





Drug using relations in
Hartford, CT
Steve Borgatti 2004

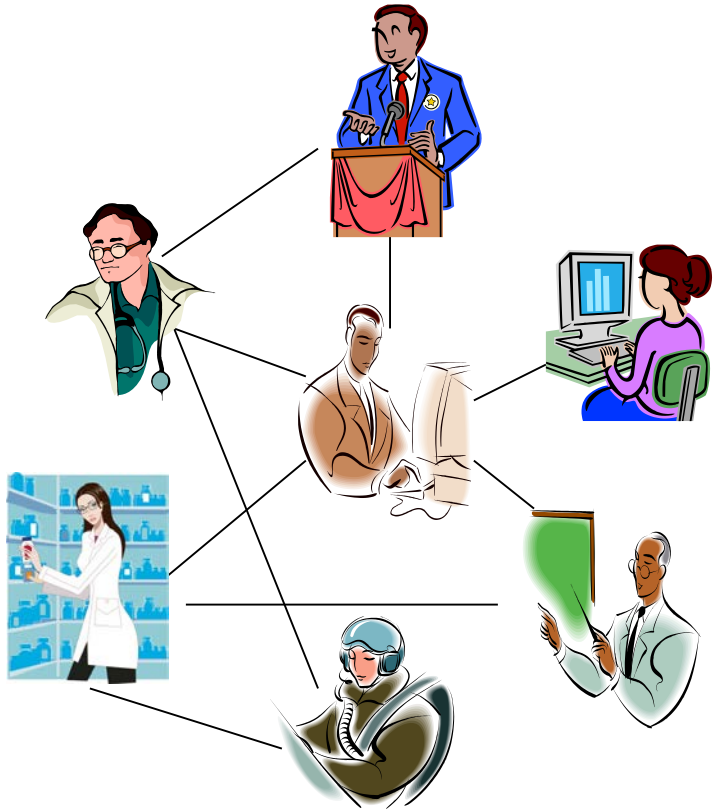


Benghazi Consulate
Twitter Network
Kathleen M. Carley, 2013

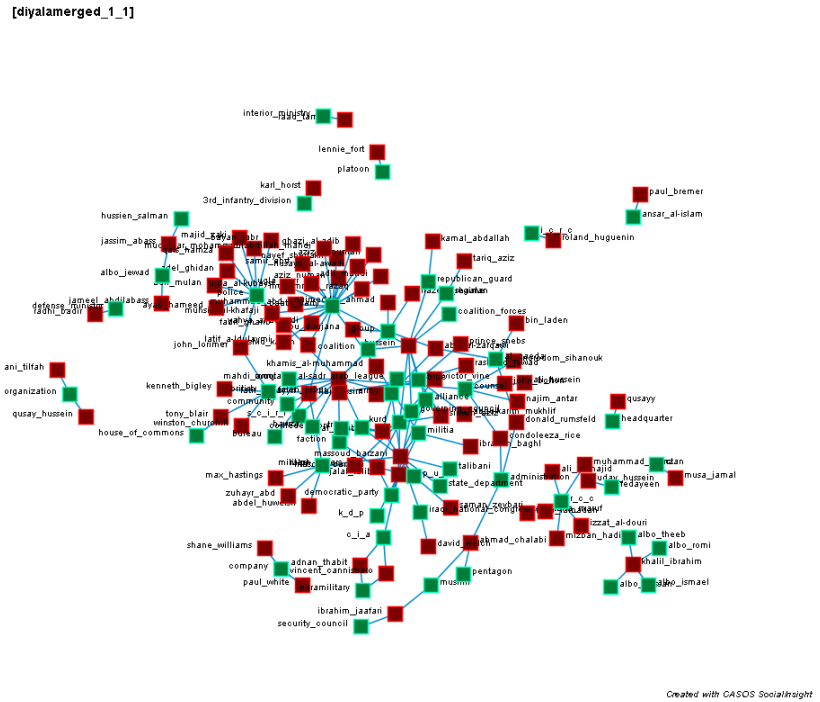
Social Networks

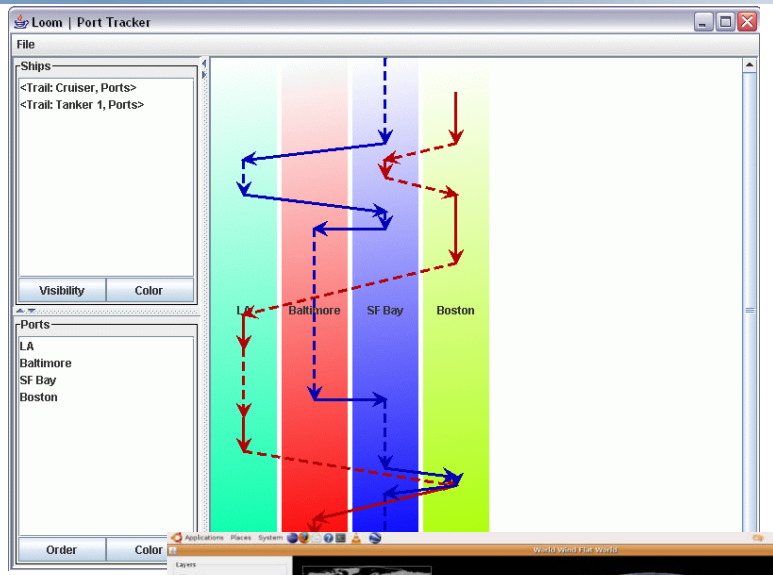
A **social network** is a description of the social structure at a particular point in time in terms of the actors, mostly individuals or organizations and the links among them.

A social network indicates the ways in which the actors are connected through various social familiarities ranging from casual acquaintance to close familiar bonds.



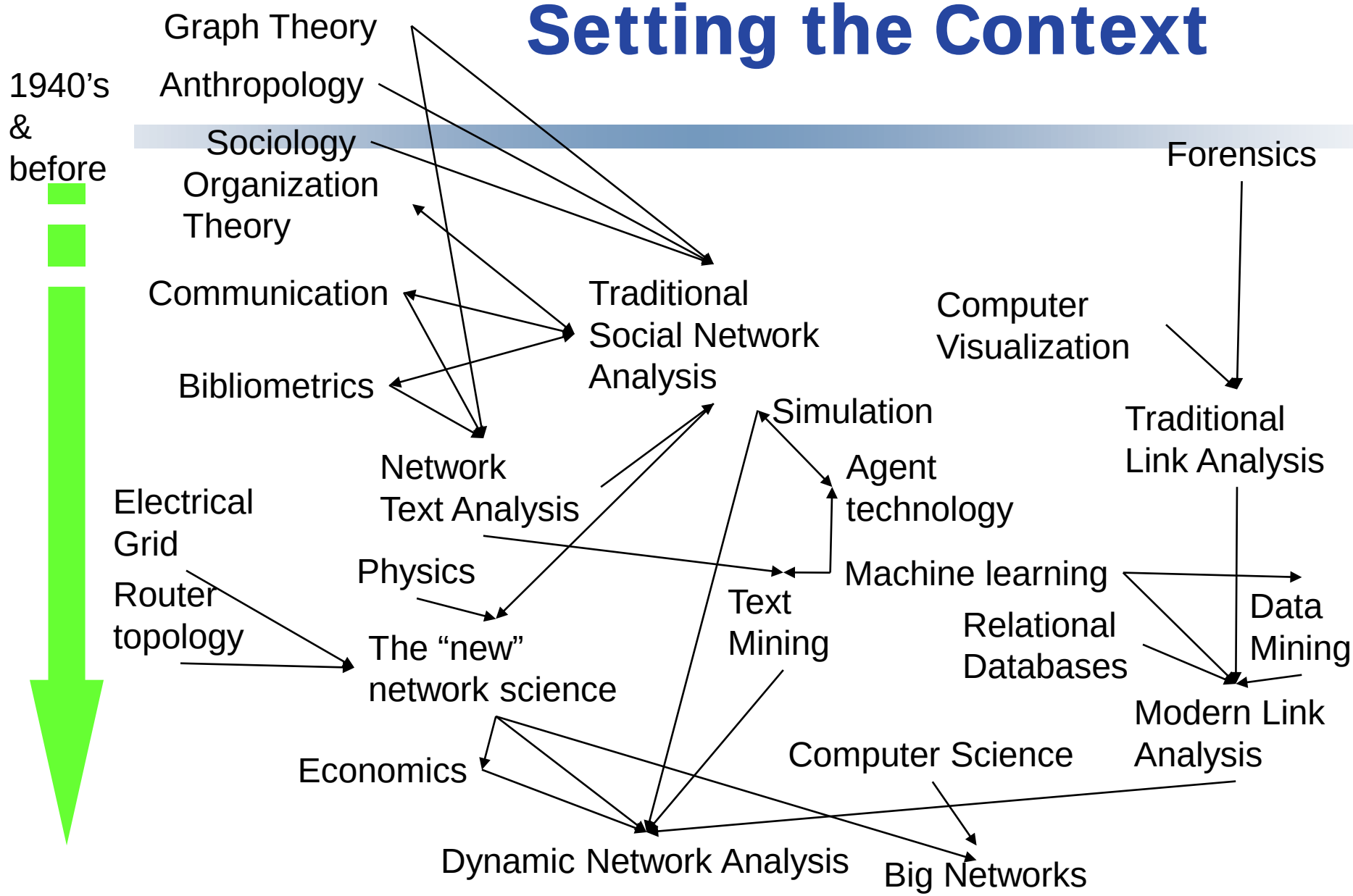
Connecting the Dots and Trails to Predict and Explain Behavior





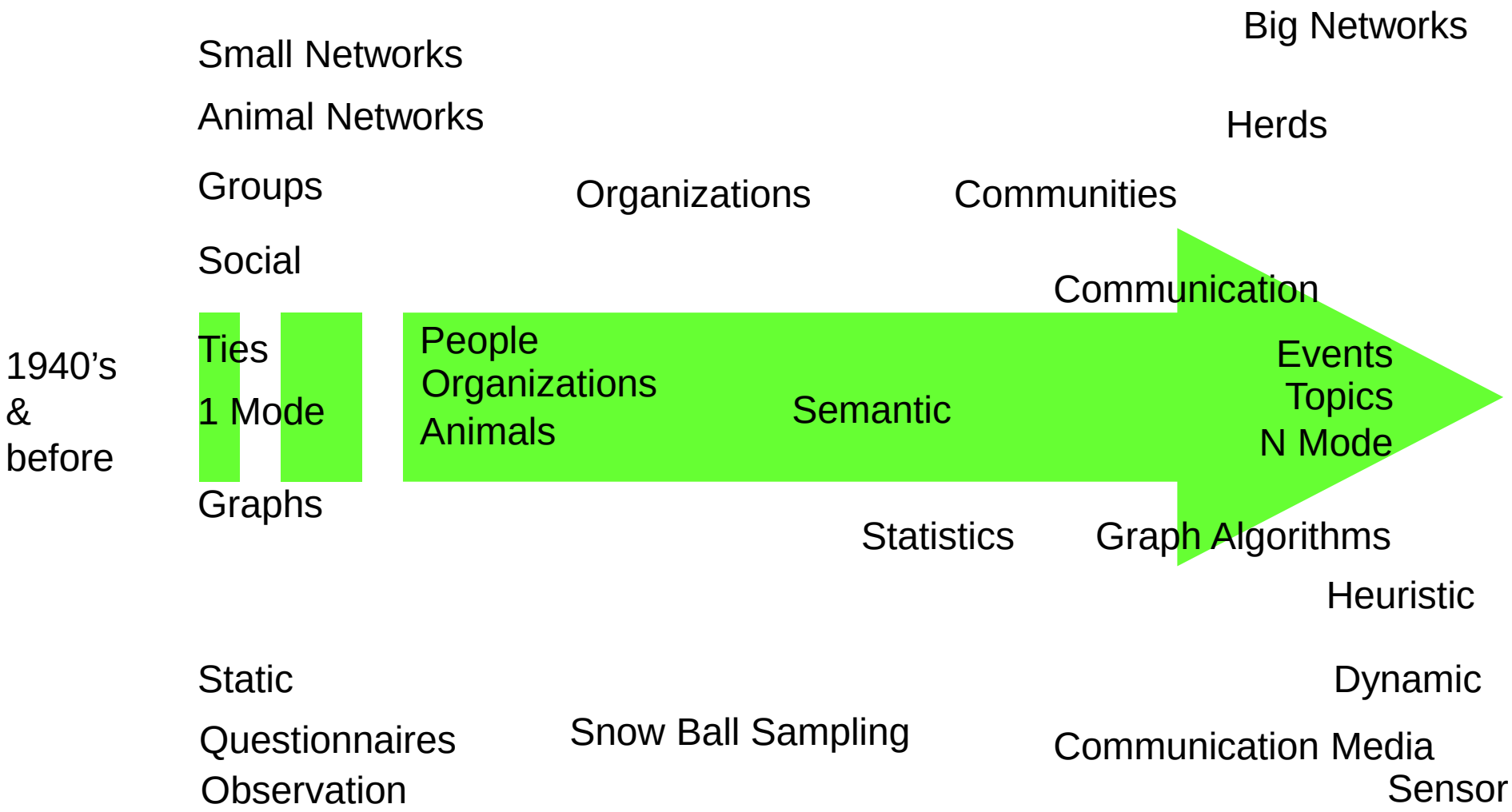
- Social Network Analysis
- Dynamic Network Analysis
- Network Science
- Link Analysis

Setting the Context



Carnegie Mellon
institute for SOFTWARE RESEARCH

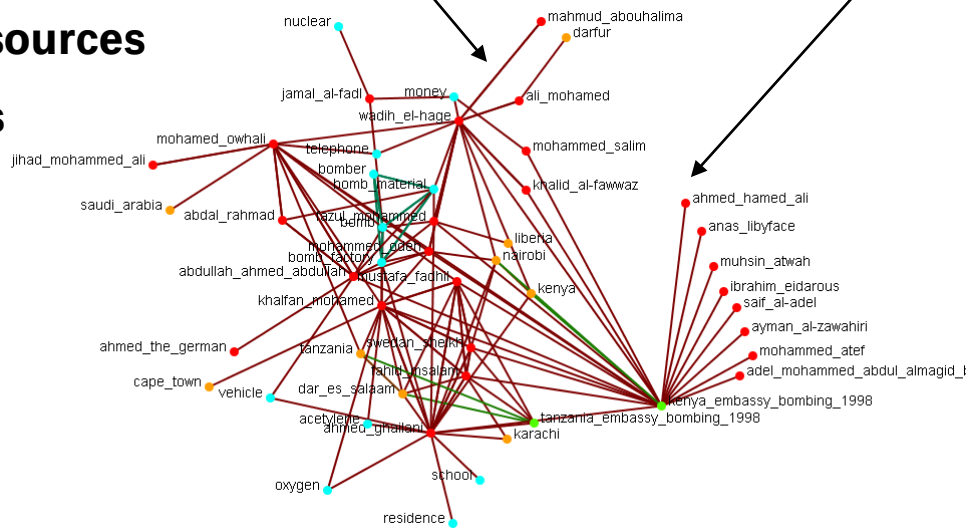
Evolutionary Themes



What is a network?

Ties Between Nodes (links)

- Who do you like or respect?
- Association or affiliation
- Transfer of resources
- Authority lines
- Alliance
- Substitution
- Precedence
- Proximity

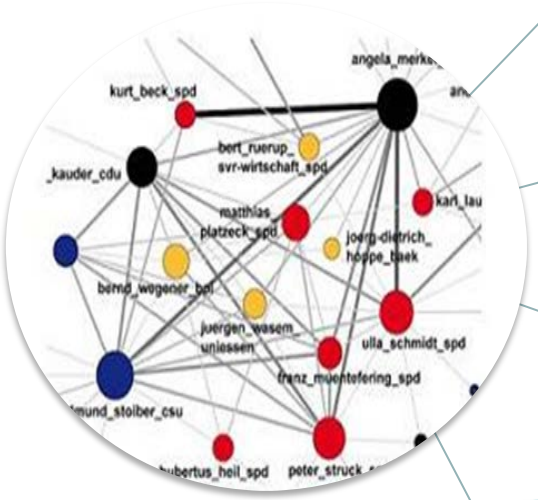


Networks are ubiquitous

Nodes

- People
- Units of action
- Coalition partners
- Departments
- Resources
- Ideas or Skills
- Events
- Nation-states

Areas of Application



Resiliency
- Organizational
- Design to mitigate cyber attacks

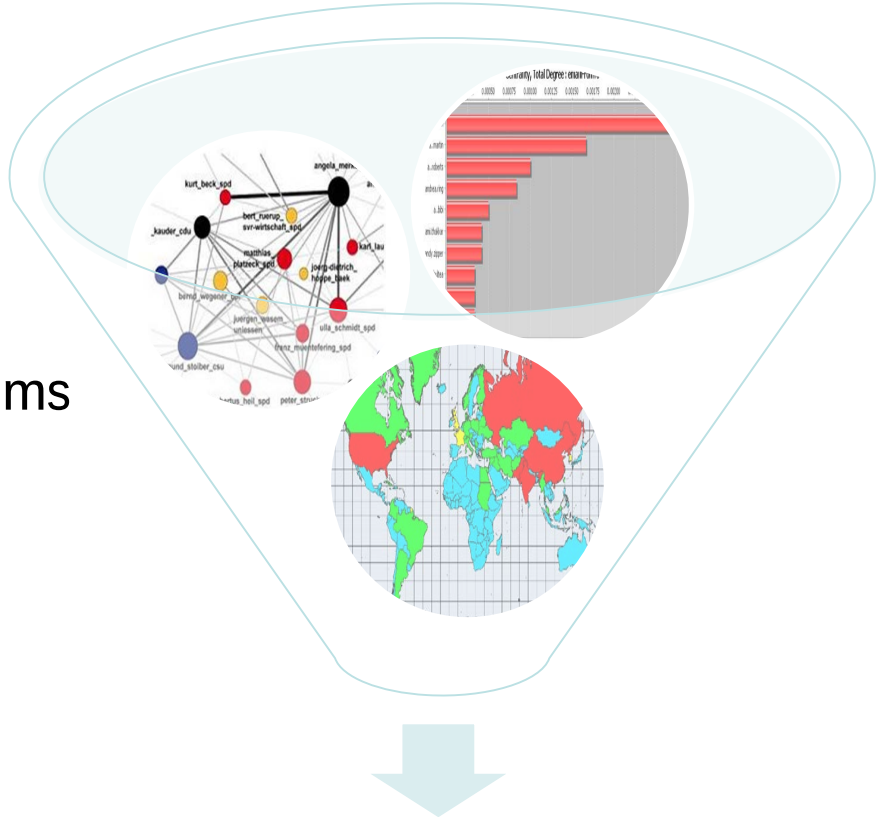
Global Map
- Cyber Warfare

Insider Threat
- Case Studies
- Sensor/email analysis

Social Media
- Sensitivity to Cyber issues

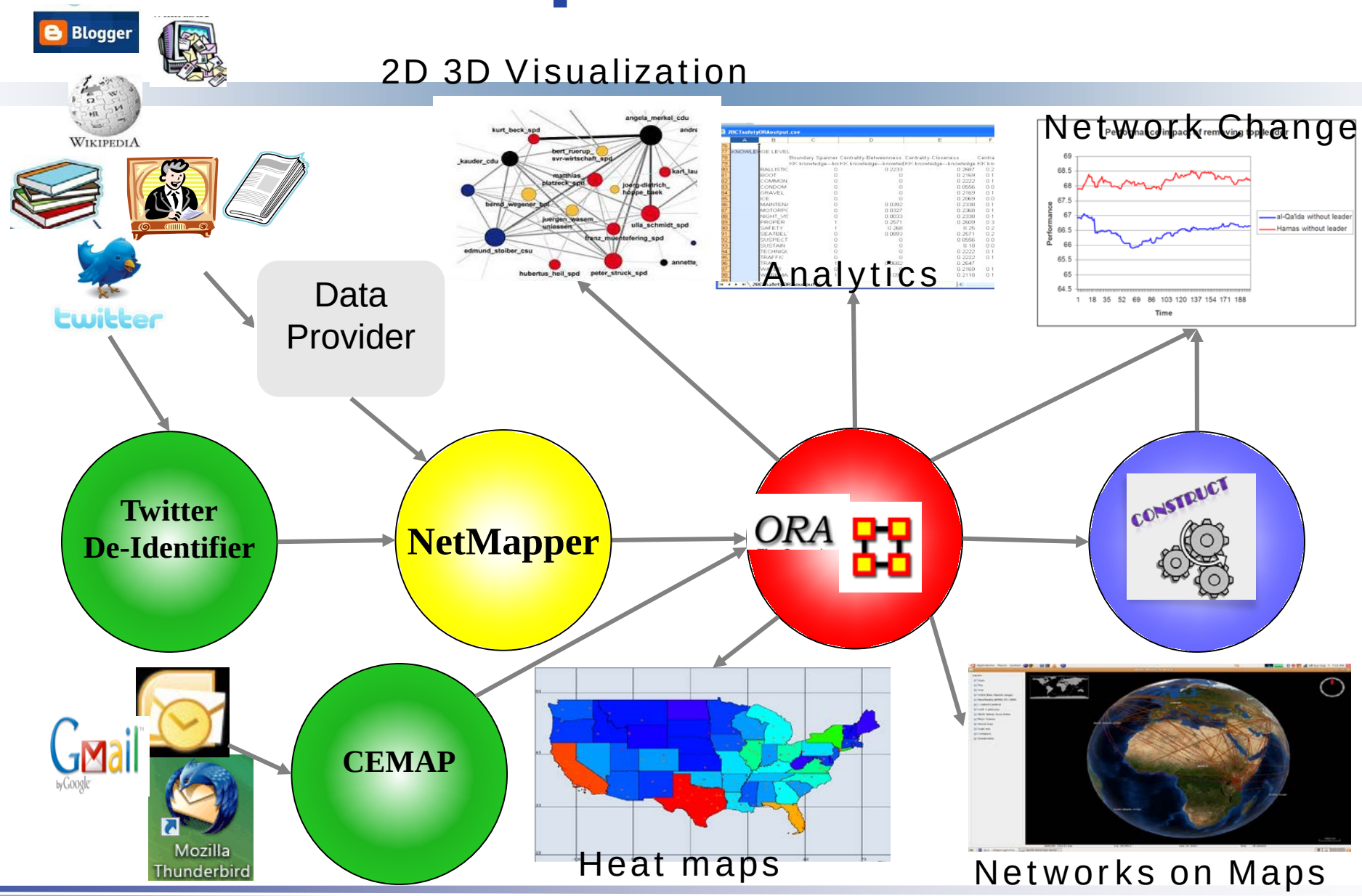
Supporting Technologies

- Network Analytics
  - Graph metrics & algorithms
  - Statistical metrics & algorithms
  - Simulation
- Visual Analytics
- Text Analytics
- Machine Learning



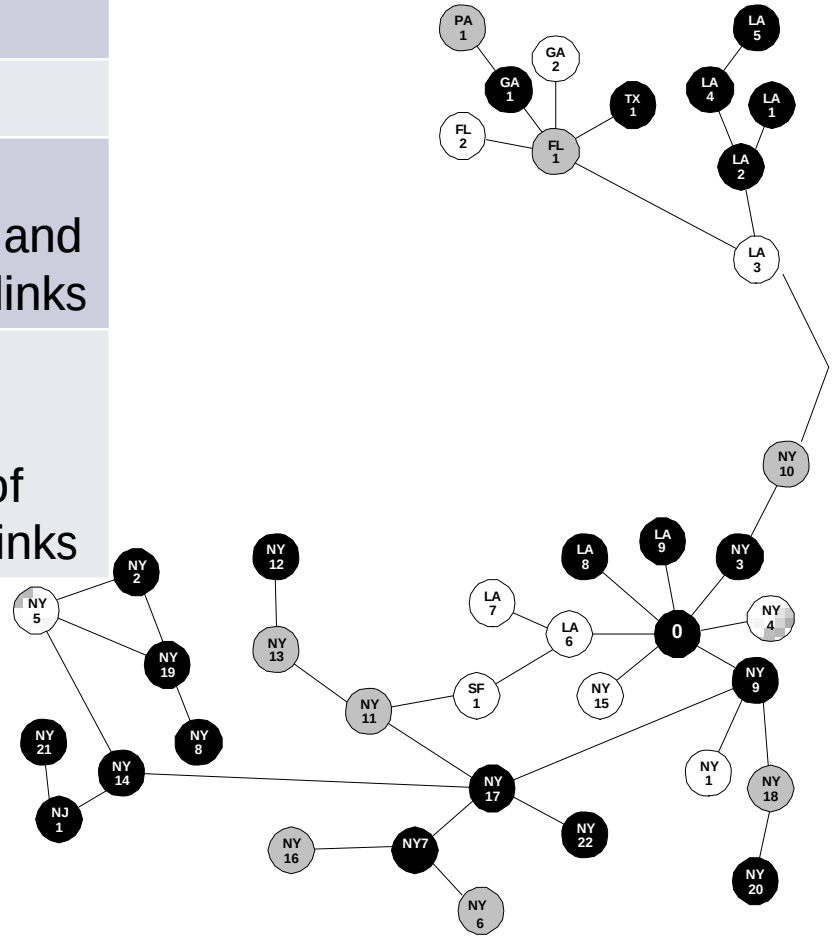
Analysis of who communicates, influences or did / will do what to whom - when, how, and why

Capabilities



The Network Perspective

Standard Statistics	Social Network Analysis	Dynamic Network Analysis
Attributes	Relations	Relations + Attributes
Atomistic	Interdependence	
Actors as independent	Actors constrained and enabled by links	Actors constrained and enabled by links
Actor state matters	Actor state irrelevant	Actor state impacts perception of and use of links



Discovery of HIV: Sexual contacts among gay men w/ unusual cancers, traced by Bill Darrow of the CDC

Definitions

- Node
  - The entity of interest (point, entity,dot, <person>)
  - Mode aka Node type
- Link
  - relation, link, edge, connection, <friendship>
  - vary in strength (weight), direction, type, confidence (another weight)
  - Link type
- Ego-Network
  - The set of nodes directly connected to ego and the relations among them
- Social Network
  - A one-mode, one-link network from a single time
  - Nodes are generally people
- High-dimensional aka Meta-network
  - Multi-mode, multi-link network
  - Often geo-temporal
- Path
  - A path in a network between two nodes, such that no link or node is crossed twice

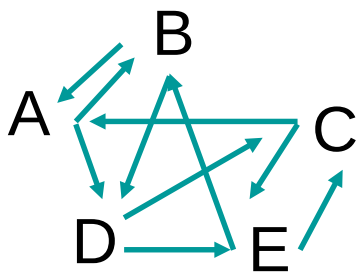
Simple SNA Measures

Measure	Definition	Meaning	Usage
Degree Centrality	Node with the most connections	In the know	Identifying sources for intel; Reducing information flow
Betweenness	Node in the most best paths Needs symmetric data	Connects groups	Typically has political influence, but may be too constrained to act
Eigenvector Centrality	Node most connected to other highly connected nodes	Strong social capital	Identifying those who can mobilize others
Closeness	Node that is closest to all other nodes	Rapid access to all information	Identifying sources to acquire/transmit information
Betweenness - Centrality	High in betweenness but not degree centrality	Connects disconnected groups	Go-between; Reduction in activity by disconnecting groups

Degree Centrality

- Degree – total number of edges/ nodes ego is connected to
- In Degree – total number of nodes that send edge to ego
- Out Degree – total number of nodes that receive edge from ego
- Sink – 0 in degree; Source – 0 out degree

0 1 0 1 0
1 0 0 1 0
1 0 0 0 1
0 0 1 0 1
0 1 1 0 0



N	In	Out	Total
A	2	2	4
B	2	2	4
C	2	2	4
D	2	2	4
E	2	2	4

Betweenness Centrality

- How often a node lies along the shortest path between two other nodes
- Computed as: $$b_k = \sum_{i,j} \frac{g_{ikj}}{g_{ij}}$$

where gij is the number of geodesic paths from i to j and gikj is number of those paths that pass through k

- Index of potential for
  - gate-keeping, brokering, controlling the flow, and liaising between disparate parts of network – “connects groups”
- Indicates power, access to diversity of flows, potential for synthesizing
- Very “expensive” to compute

Closeness Centrality

- Measured as:
  - Sum of distances to all other nodes
  - Computed as marginals of symmetric geodesic distance matrix

- Closeness is an inverse measure of centrality
- Index of expected time until arrival for given node of whatever is flowing through the network
  - –Gossip network: central player hears things first

Eigenvector Centrality

- Node has high score if connected to many nodes that are themselves well connected
- Computed as:

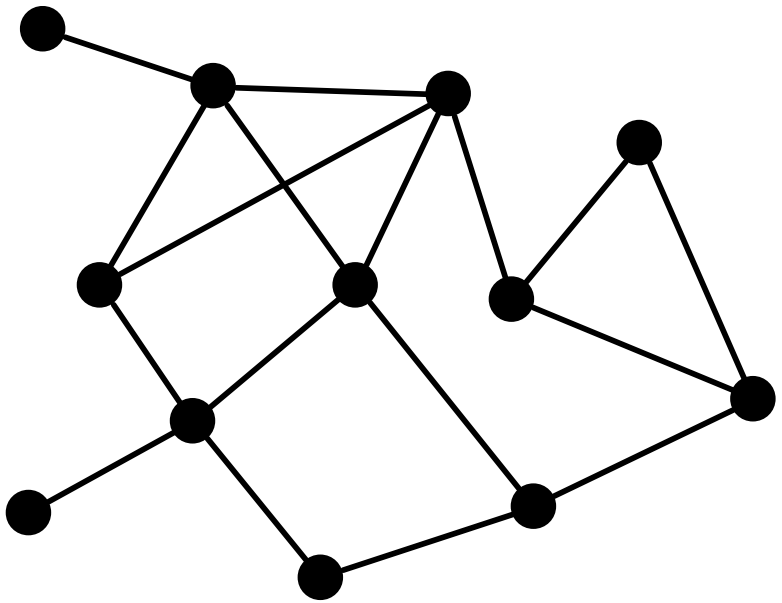
$$\lambda v = Av$$

where A is adjacency network and V is eigenvector centrality. V is the principal eigenvector of A

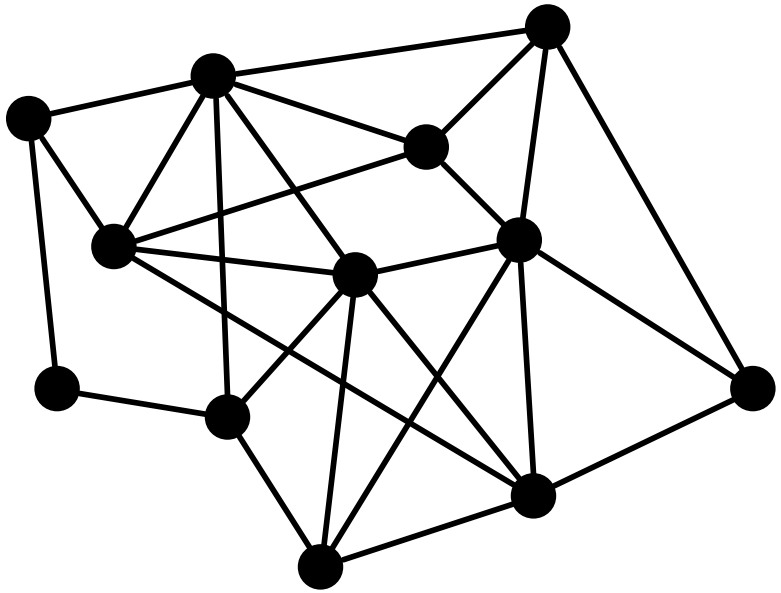
- Indicator of popularity, “in the know”
- Index of exposure, risk
- Tends to identify centers of large cliques
  - Often identified as leader of self-contained group
  - Leader of Leaders

Density

- Number of ties, expressed as percentage of the number of ordered/unordered pairs
- Number of ties / Number of possible ties
- If number of nodes = N and number of ties is M, then M/(N*(N-1)) if directed and M/((N*(N-1))/2) if undirected

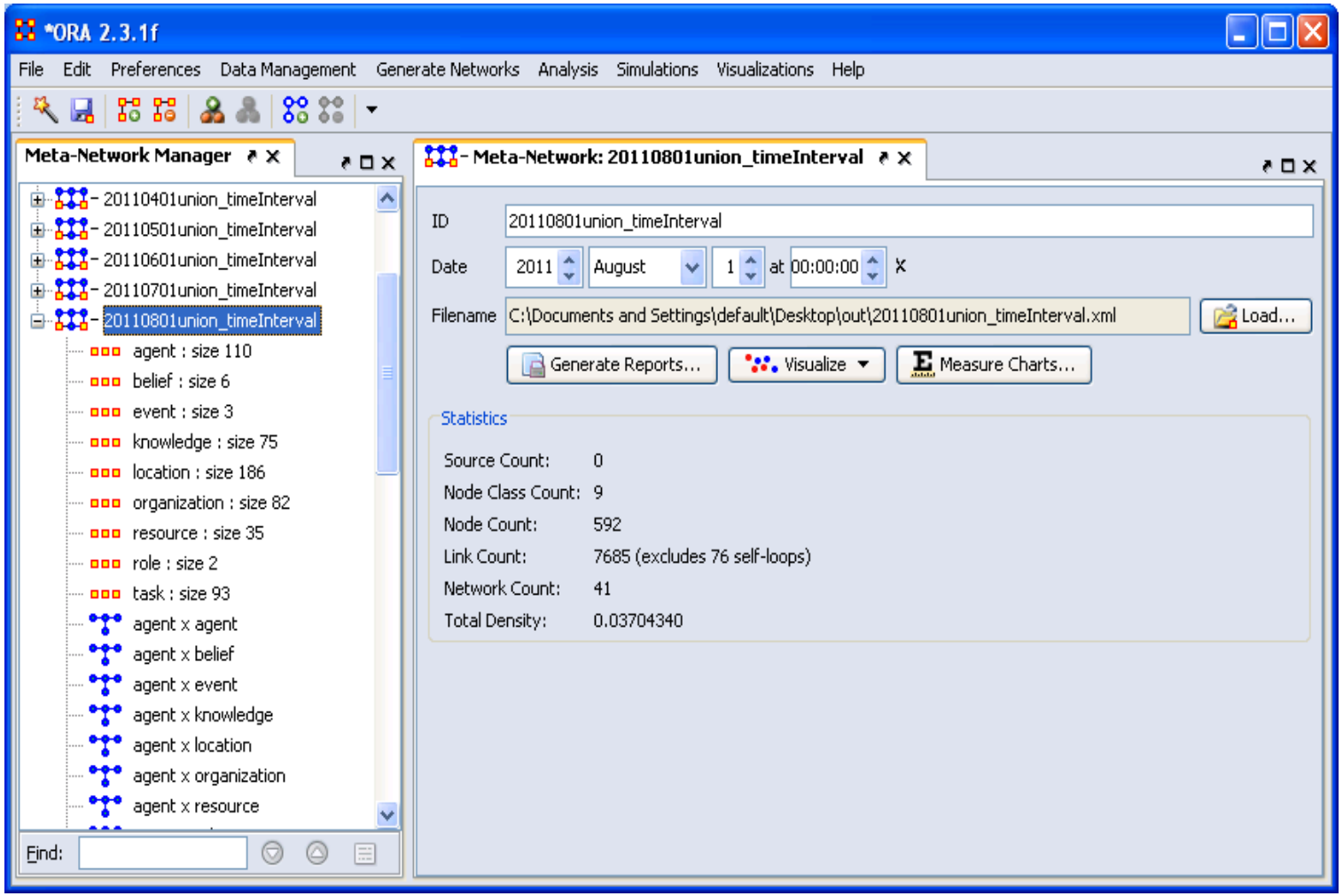


Low Density (25%)
Avg. Dist. = 2.27



High Density (39%)
Avg. Dist. = 1.76

Network Analytic Toolkits



Identify: Who are the Key Players? Or Locations, Resources …

Agents 286, 652, 97 repeatedly rank in top three in the measures.

In-the-Know
(total degree centrality)

Rank	Value	Unscaled	Agent
1	0.181	181	652
2	0.176	176	286
3	0.175	175	97
4	0.165	165	412
5	0.158	158	502
6	0.154	154	273
7	0.139	139	246
8	0.115	115	615
9	0.111	111	829
10	0.109	109	8

Potentially Influential
(betweenness centrality)

Rank	Value	Unscaled	Agent
1	0.0988664	24667.2	286
2	0.0705427	17600.4	97
3	0.0625256	15600.1	502
4	0.0609523	15207.6	829
5	0.0548627	13688.2	652
6	0.0542421	13533.4	615
7	0.0524498	13086.2	412
8	0.0410645	10245.6	501
9	0.0306578	7649.12	273
10	0.0305522	7622.78	552

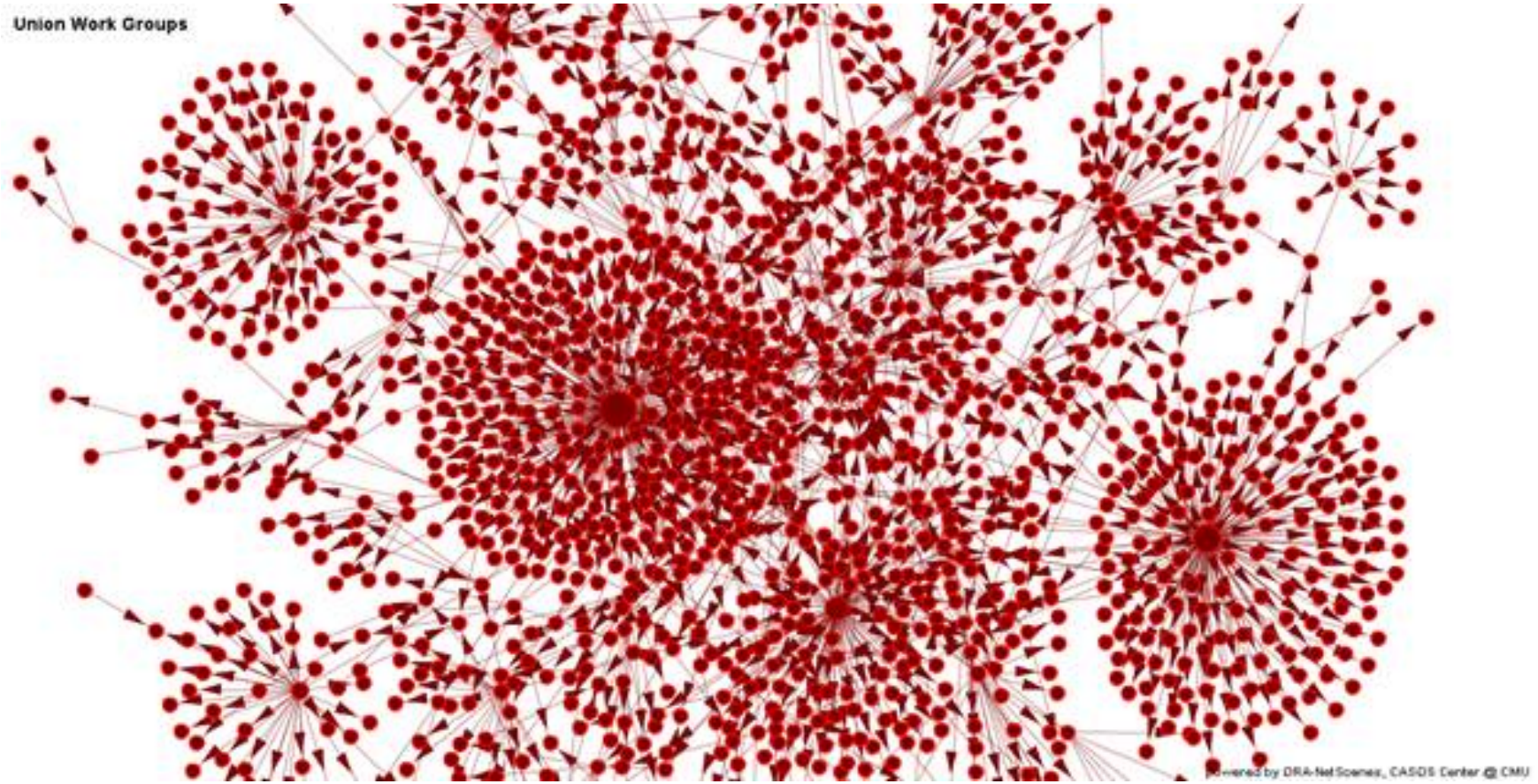
Drilling down…

*ORA's **Key Entity Report** shows 3 agents critical to operations.

Narrow our focus from set of interstitial members to small group of leaders.

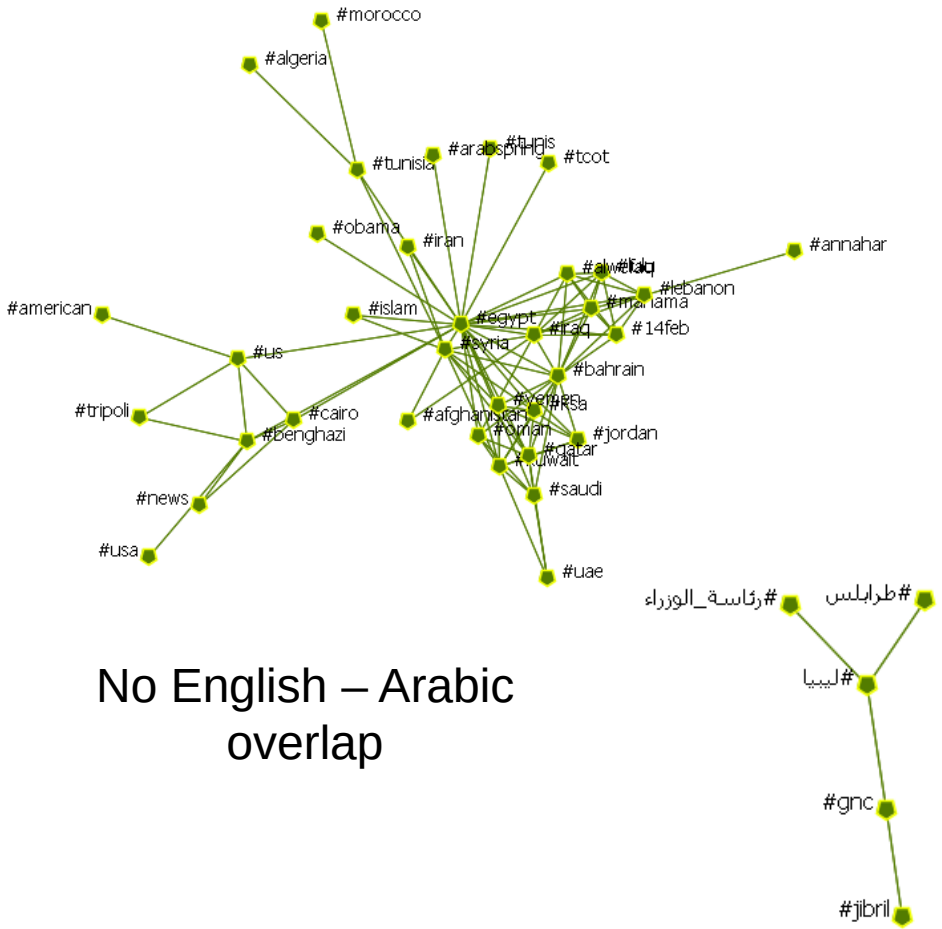
Overall Tweet Network

Note there are a few sources that are picked up



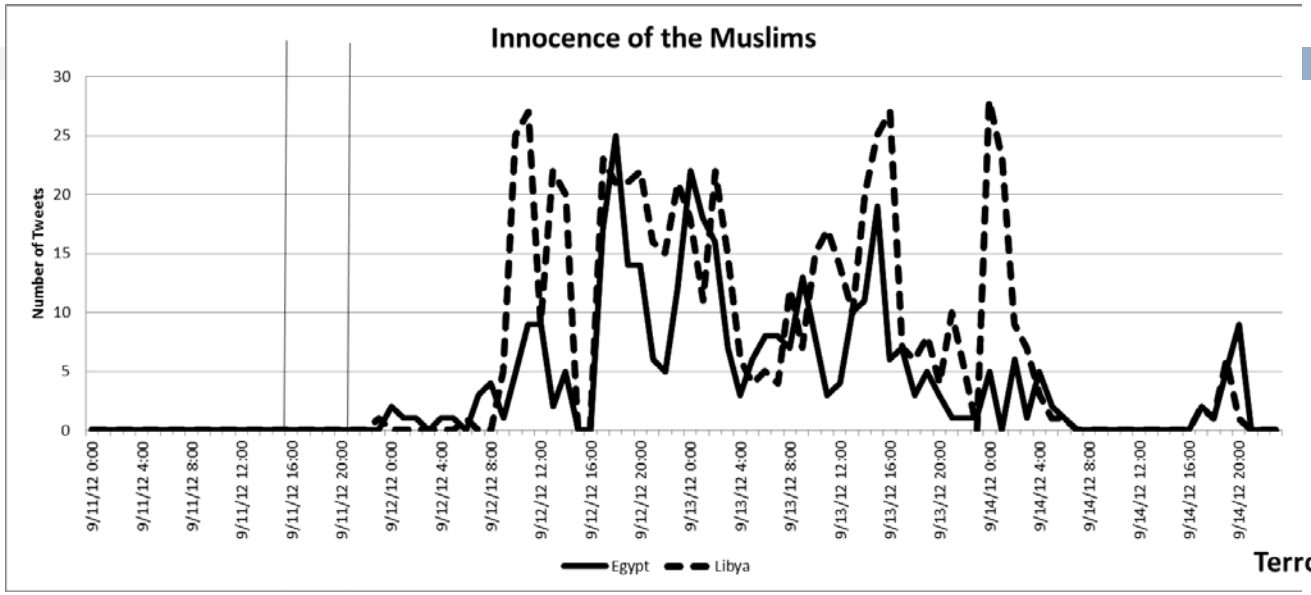
Retweeted Actors & Hashtags

Most are newspapers

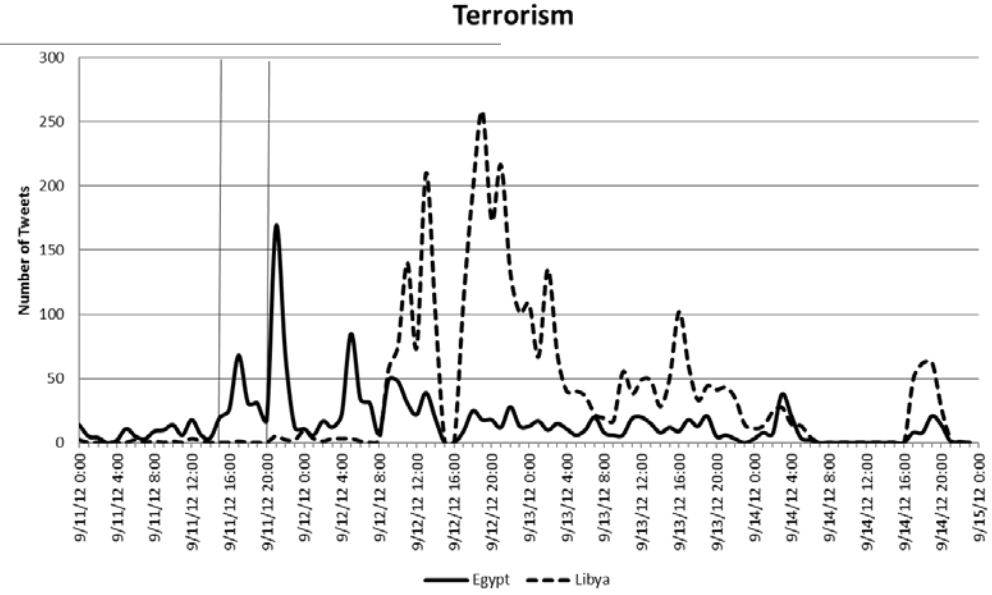


No English – Arabic overlap

Benghazi Consulate

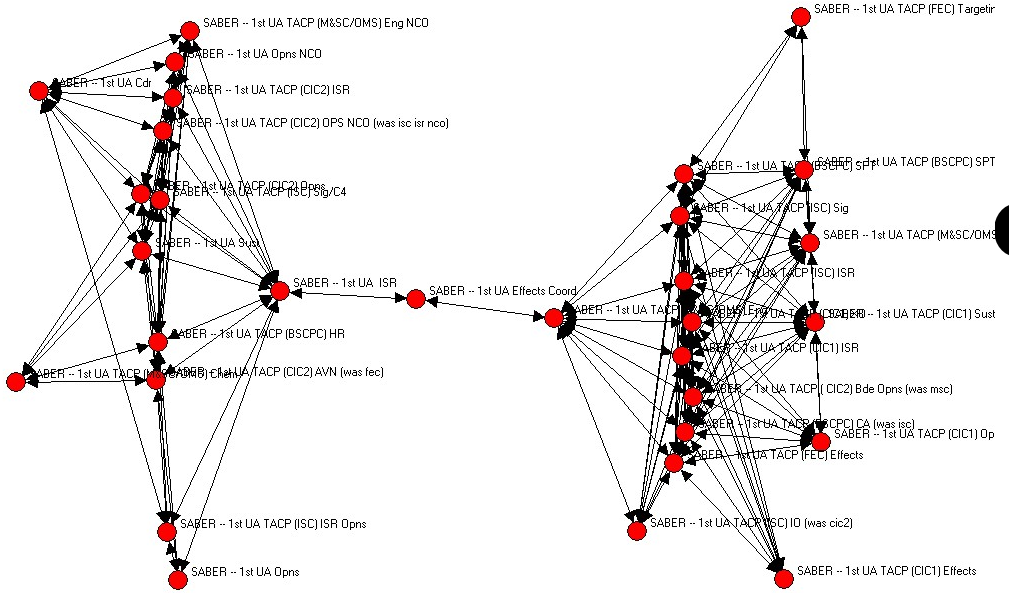


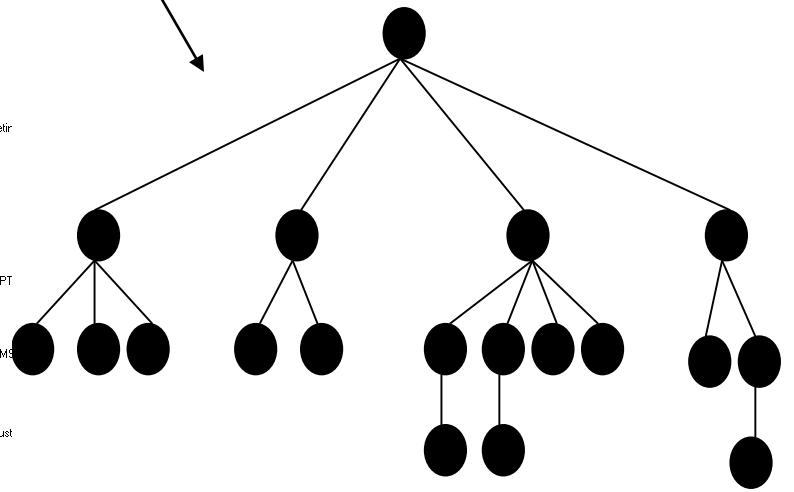
Movie not a precipitating event



Each person is embedded in many networks

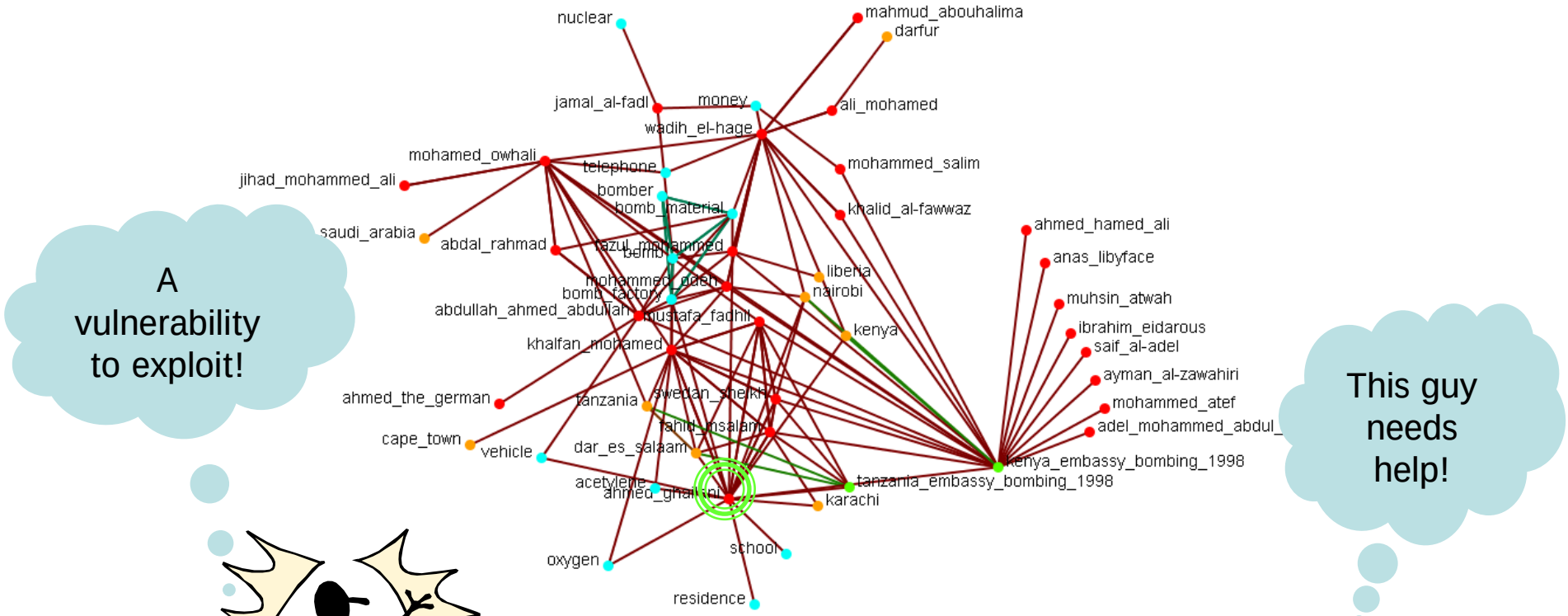
Informal and Formal Structure





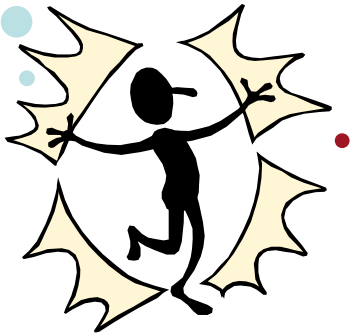
- Security Relevance
  - Formal controls access
  - Informal controls social pressure

Network Analysis Enables Management and Disruption



A vulnerability to exploit!

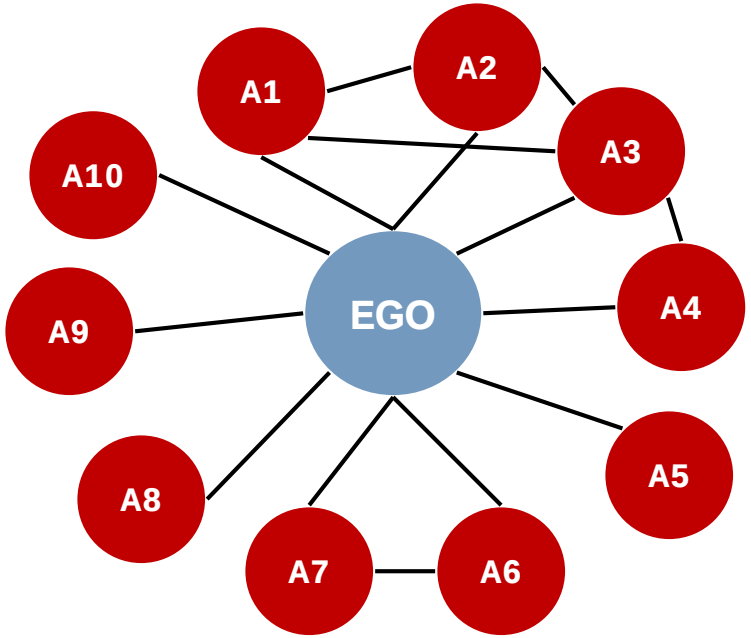
This guy needs help!



- Security Relevance
  - Prevention of potential threats
  - Identification of potential exploits

Ego Networks

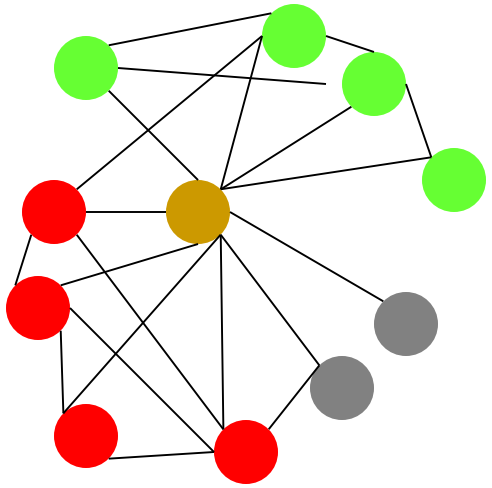
A node's (ego's) set of alters, the connections of ego to alters, and the connections among the alters



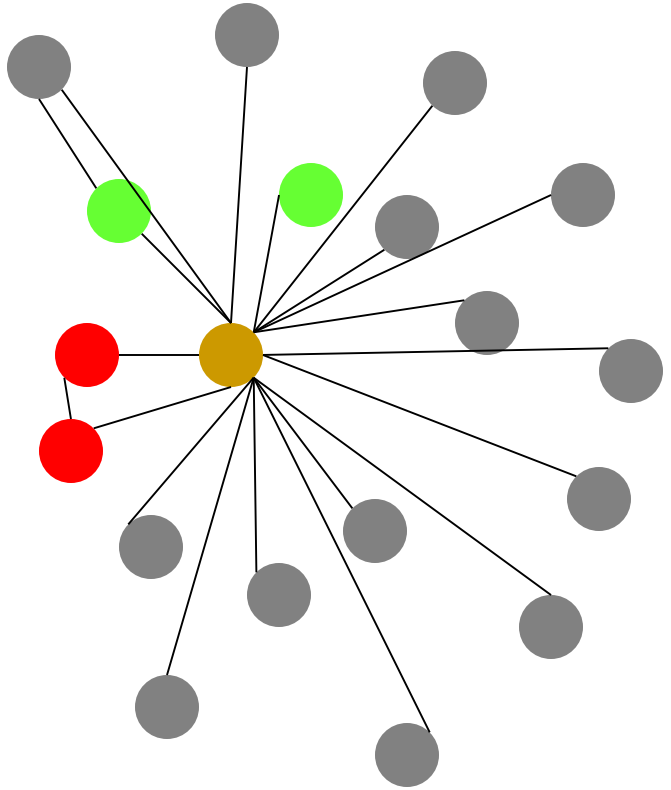
Differences in Ego Networks for Drug Users

Family
Work
Friend

Normal Person



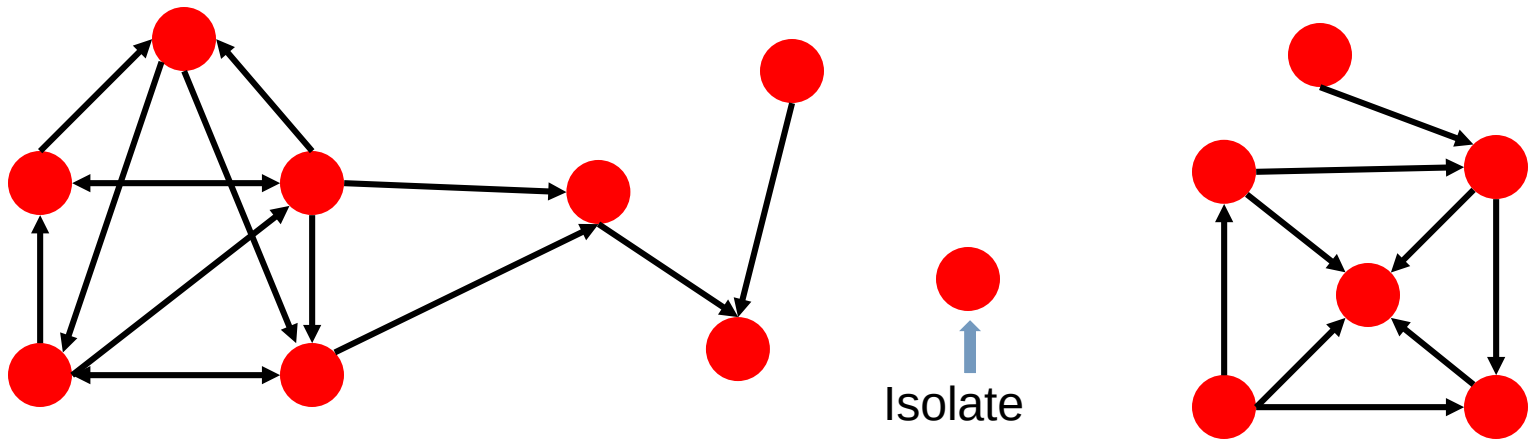
Cocaine User



People with Different Roles have Different Networks

Terminology: Components

- A subgraph S of a graph G is a component if S is maximal and connected
- If G is a digraph, then
  - S is a weak component if it is a component of the underlying (undirected) graph
  - S is a strong component if for all dyads u,v in S, there is a path from u to v
- Finding components is the first step in analysis of large graphs
  - Analyze each component separately, or discard very small components



Grouping Algorithms

- Aka community detection
- All good at finding cliques
- All good at ignoring isolates
- Some notion of “cohesion”

	CONCOR	FOG	NEWMAN-GIRVIN	LOUVAIN	Johnson Hierarchical
Exclusive	yes	no	yes	yes	no
Overlappd	no	yes	no	no	yes
Bottom-up	no	yes	yes	yes	yes
Top-Down	yes	no	no	yes	no

Critical Actors are Interstitial

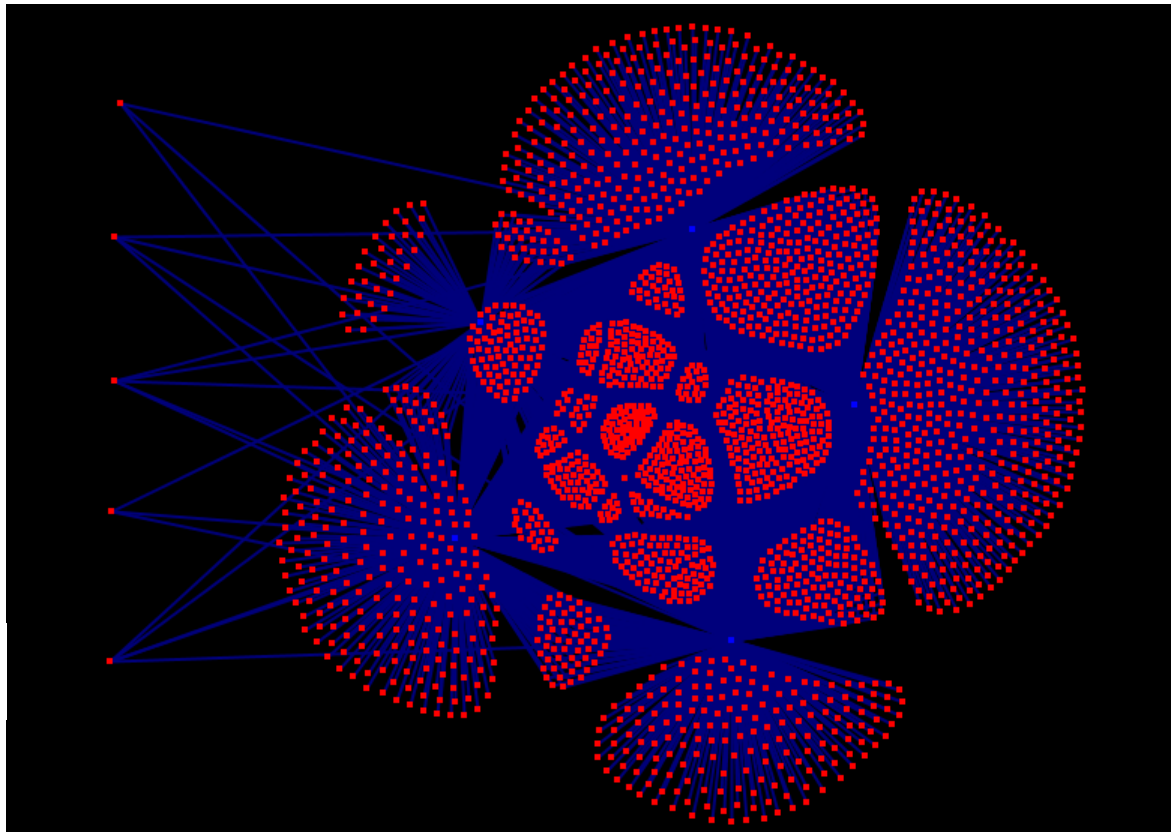
Jeff Skilling

Kenneth Lay

Tanya Jones

Veronica Espinoza

Jeff Dasovich

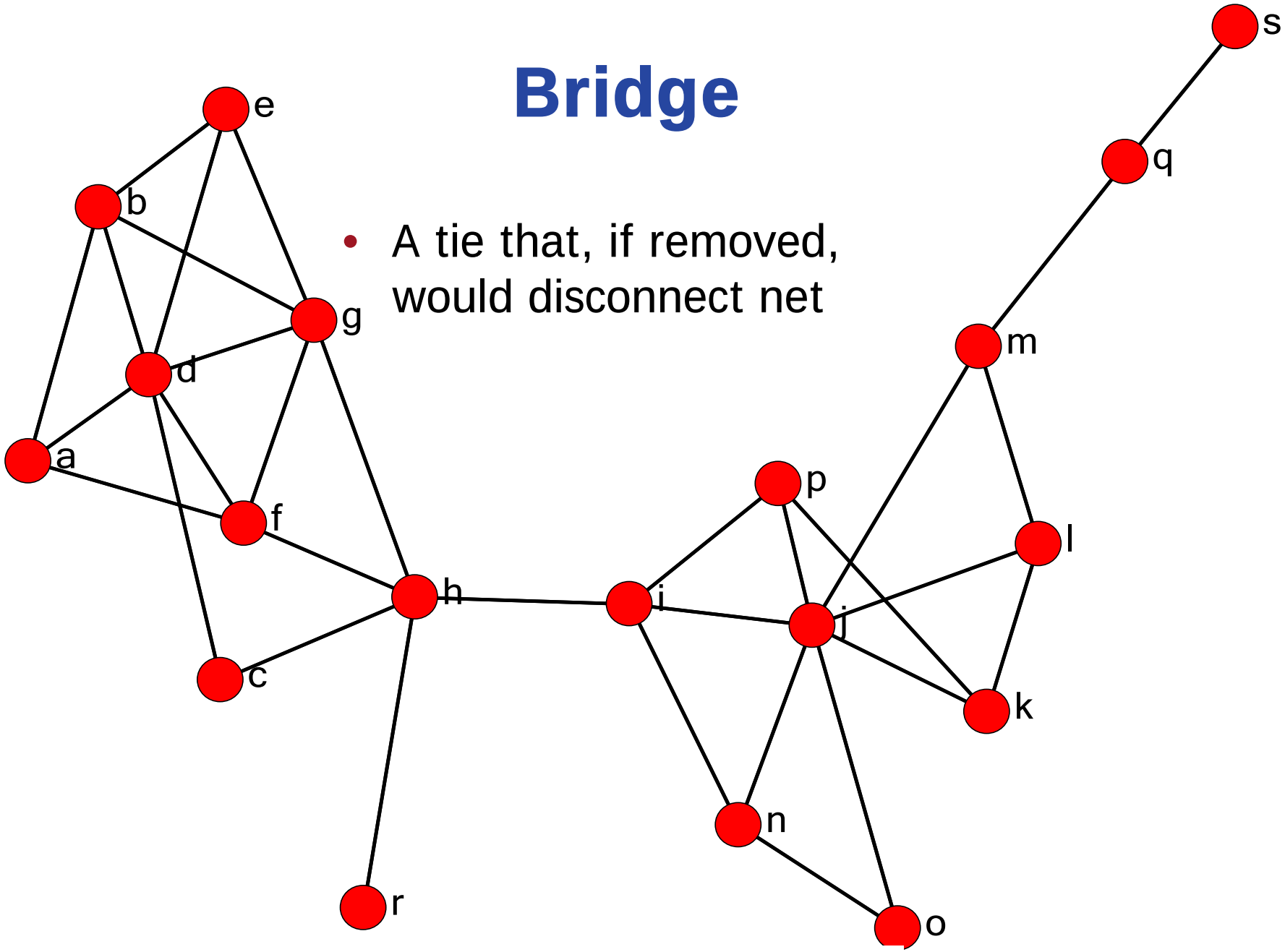


Insider Threat Example

- Extracted meta-networks from texts
- Semi-automated
- Data organized by year
- Coding is from perspective of “spy”
- Roles of actors coded
- Attributes of “spy” coded

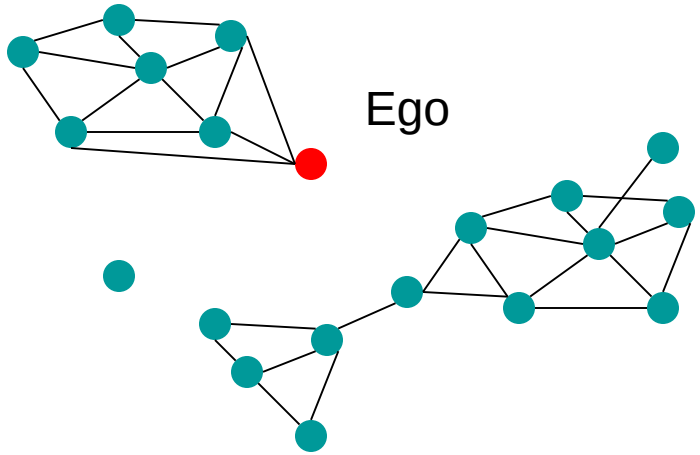
Bridge

- A tie that, if removed, would disconnect net

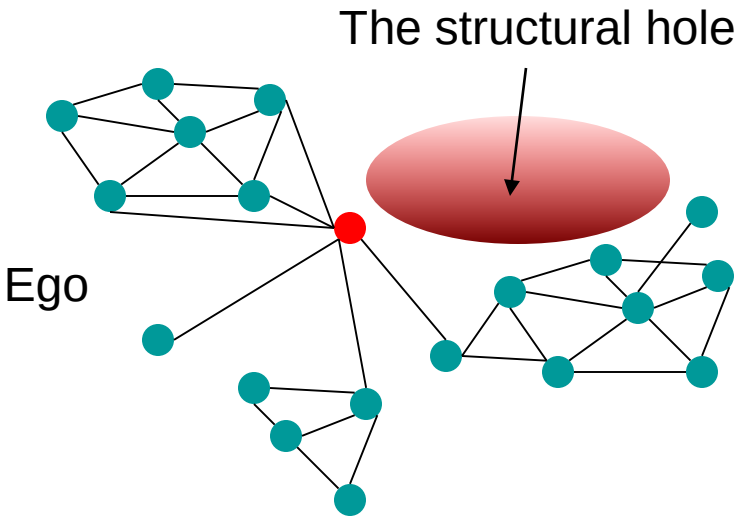


Structural Holes

Local Betweenness



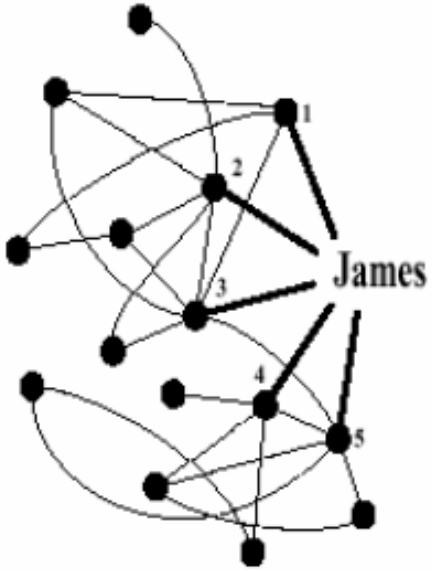
Few structural holes



Many structural hole

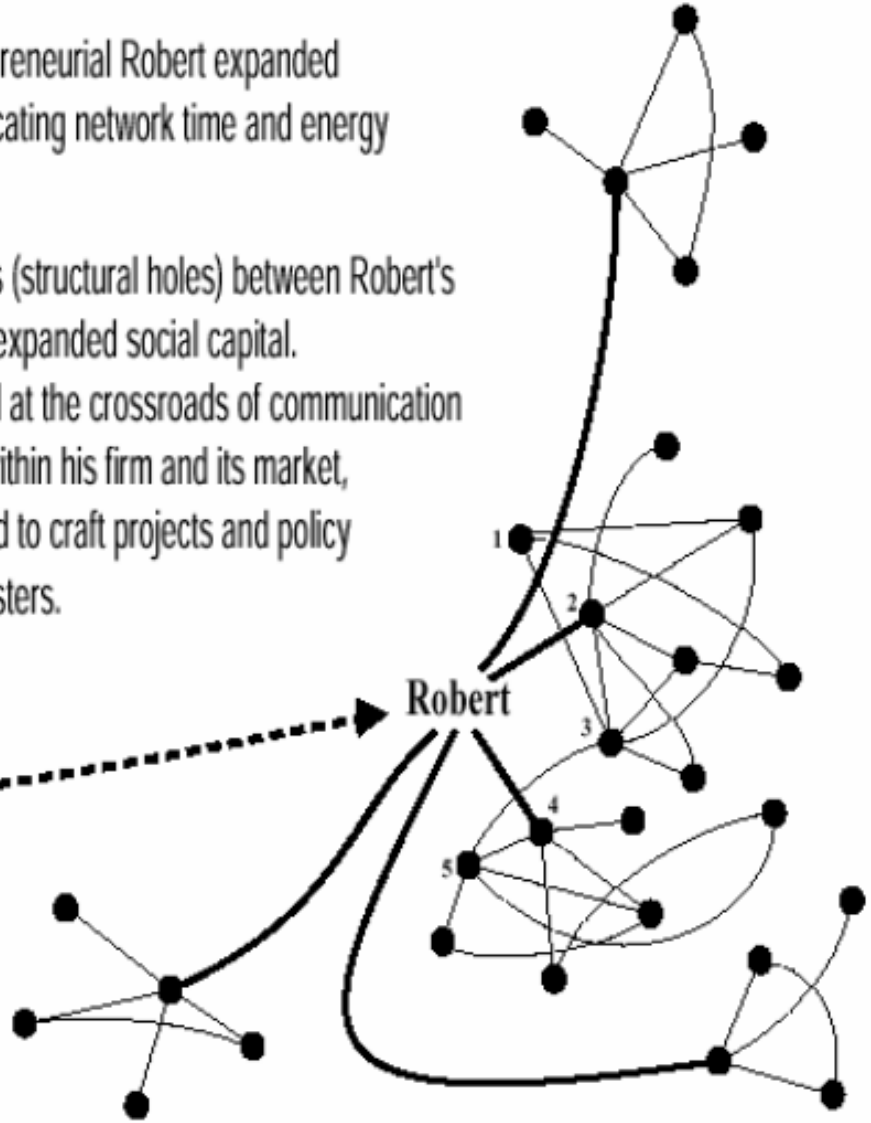
Measured by:
Burt's effective size
Burt's constraint
Everett & Borgatti's ego betweenness - This last is recommended

Structural Holes



Robert took over James' job. Entrepreneurial Robert expanded the social capital of the job by reallocating network time and energy to more diverse contacts.

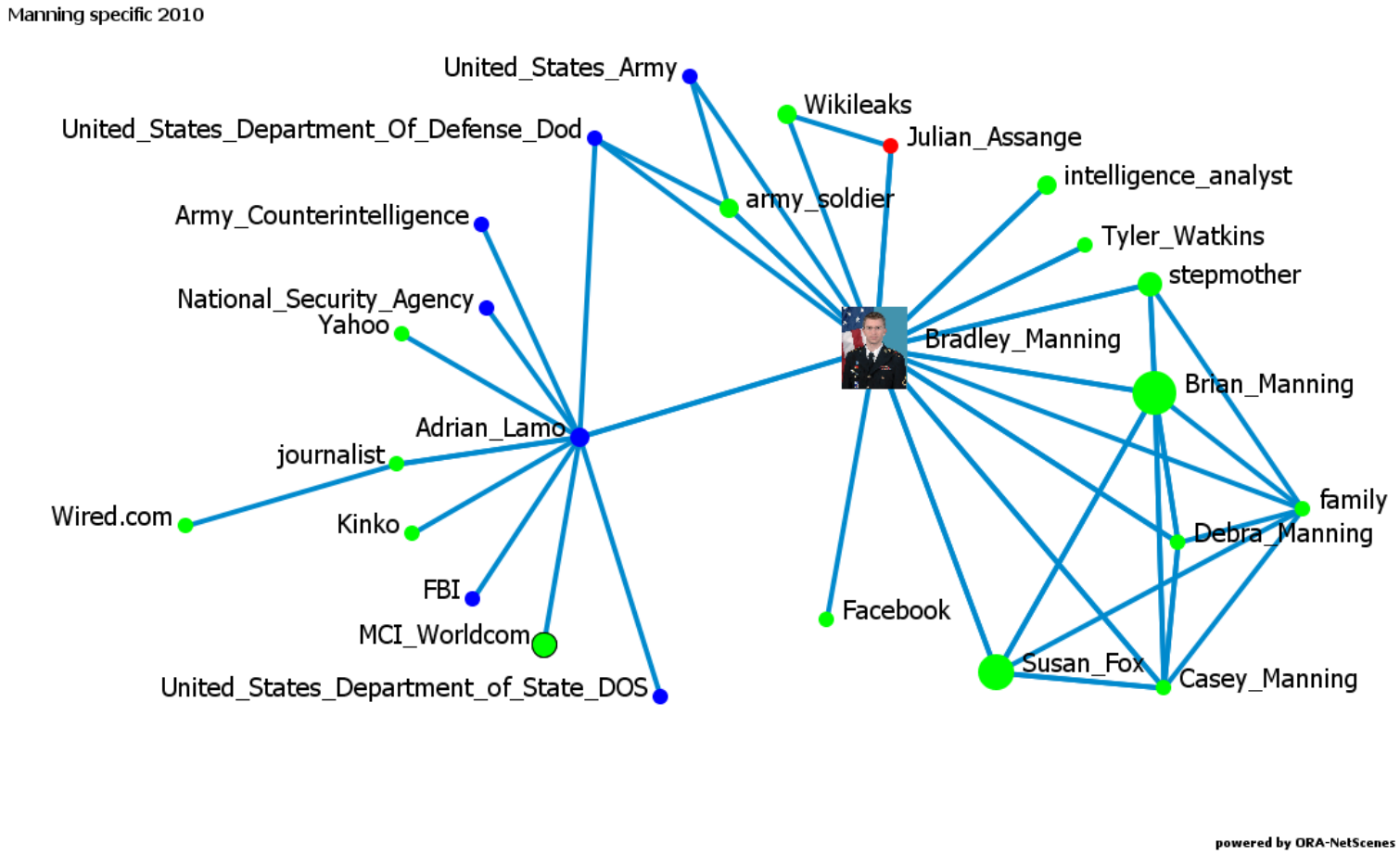
It is the weak connections (structural holes) between Robert's contacts that provide his expanded social capital. Robert is more positioned at the crossroads of communication between social clusters within his firm and its market, and so is better positioned to craft projects and policy that add value across clusters.



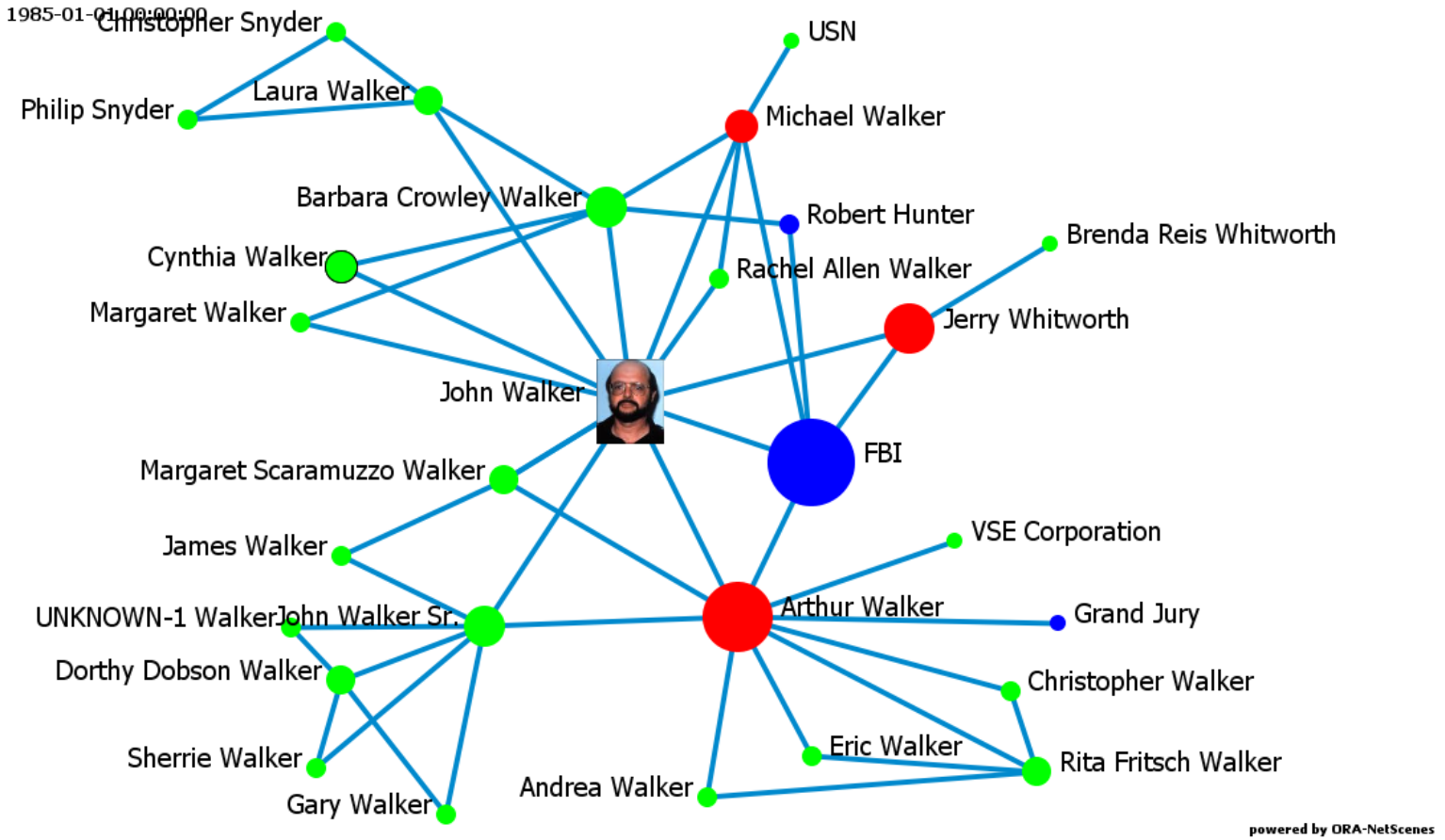
Research shows that people like Robert, better positioned for entrepreneurial opportunity, are the key to integrating across functions and across the people of increasingly diverse backgrounds in today's flatter organizations. In research comparisons between managers like James and Robert, it is the people like Robert who get promoted faster, earn higher compensation, receive better performance evaluations, and perform more successfully on teams.

Slide from Ron Burt

Manning – Lone Wolf example open-source

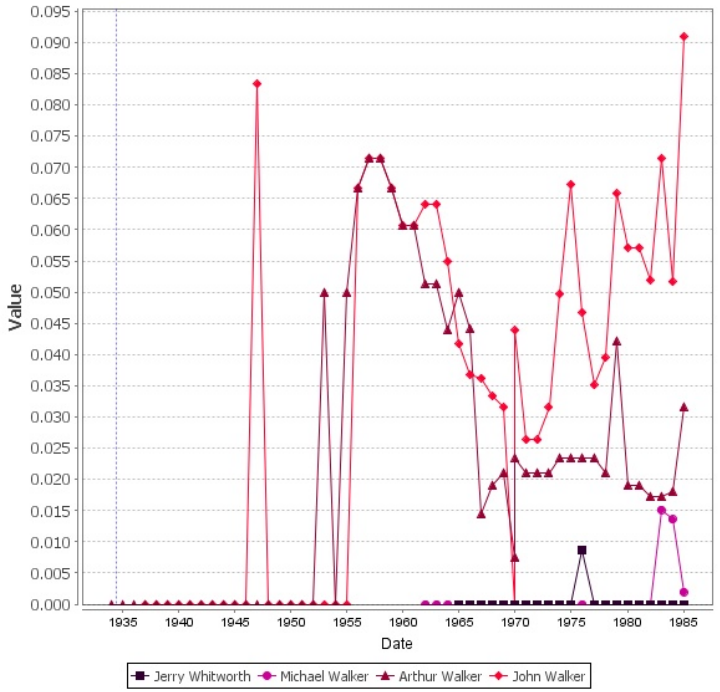


Walker – Gang example Case records/searches (open-source)

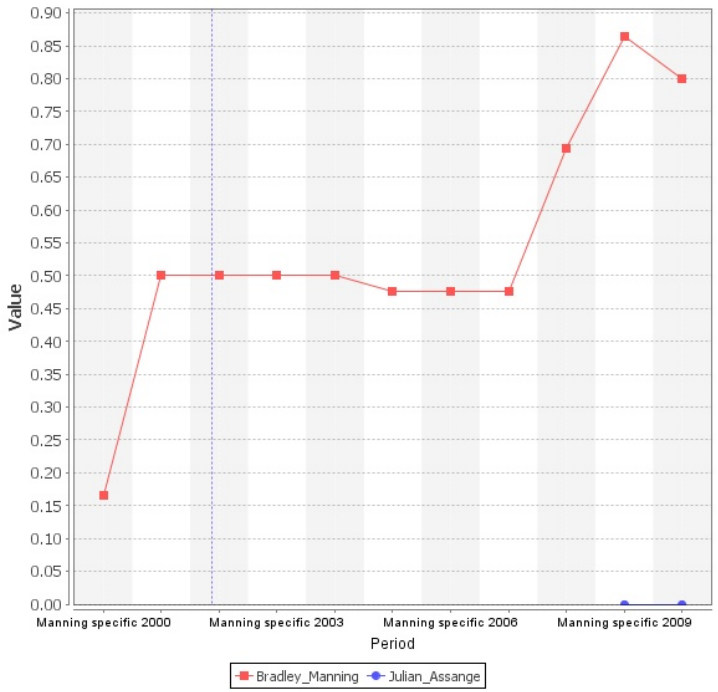


Increasing betweenness during spy activities – insider starts connecting more individuals

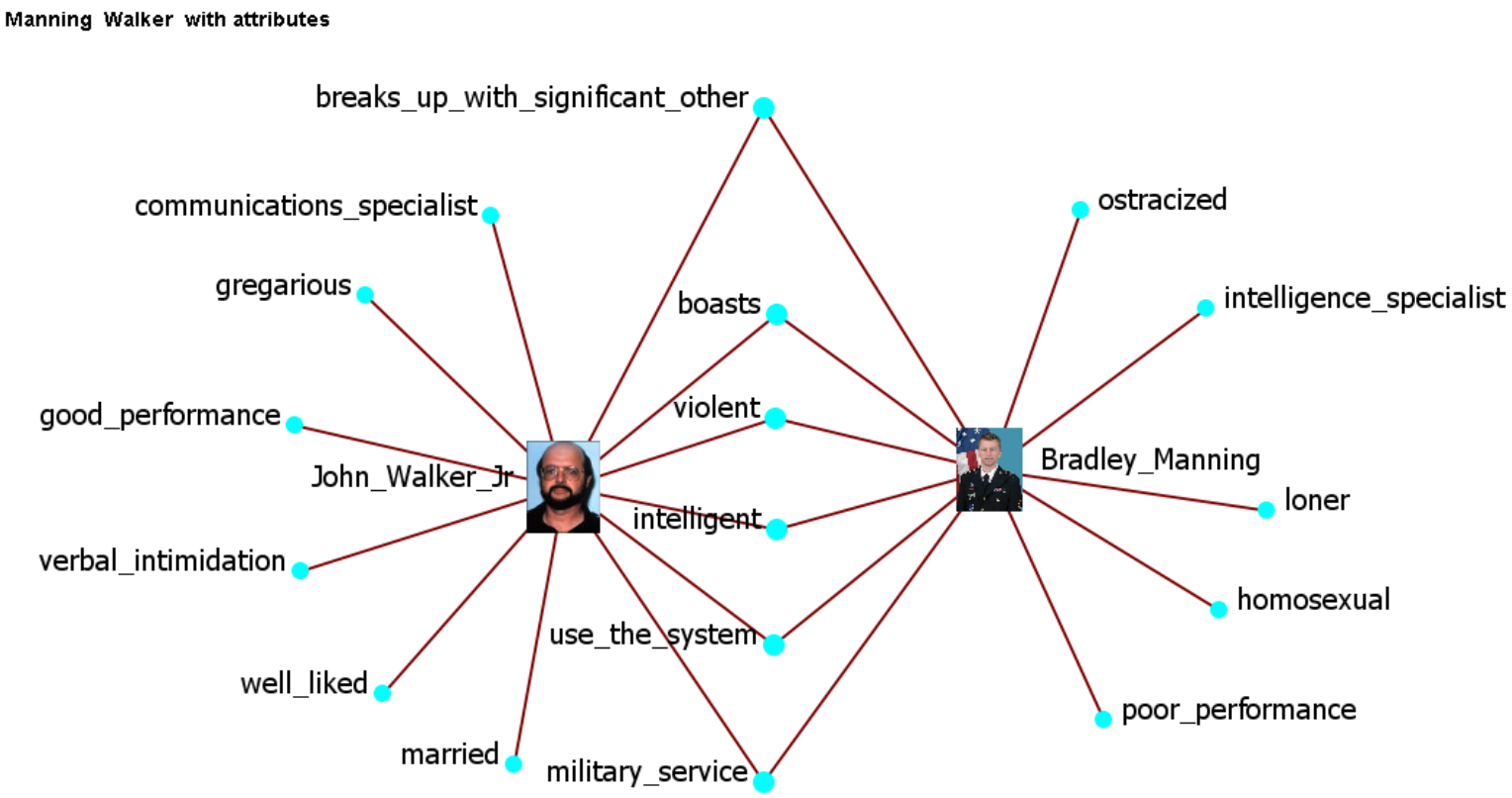
Walker Case



Manning Case



Characteristics shared and not shared by Walker and Manning



Insiders examined have these characteristics

- Special characteristics
  - Boastful
  - Abusive or violent when provoked
  - Intelligent
  - Had or was in military service
  - Had broken up with significant other
  - Wanted to “use-the-system” for own gain
  - Wanted change (money/psych change)

- Access to classified material
- Increasing betweenness over time
- Increasing structural holes
- Disrupted family network – tie strength with family decreased
- Irrelevant characteristics
  - Gender
  - Age
  - Loner/outgoing

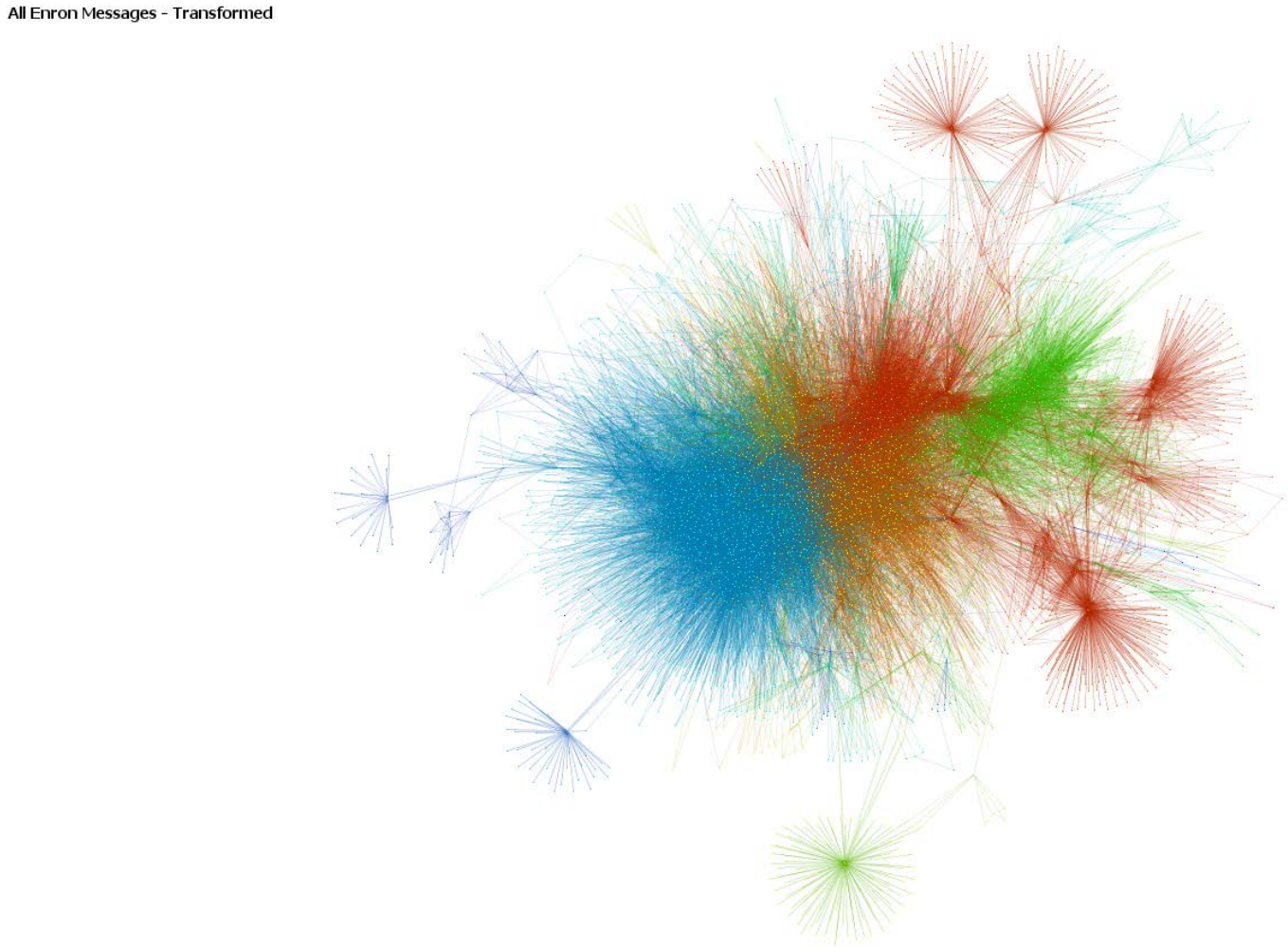
Demos

- NetMapper
- ORA

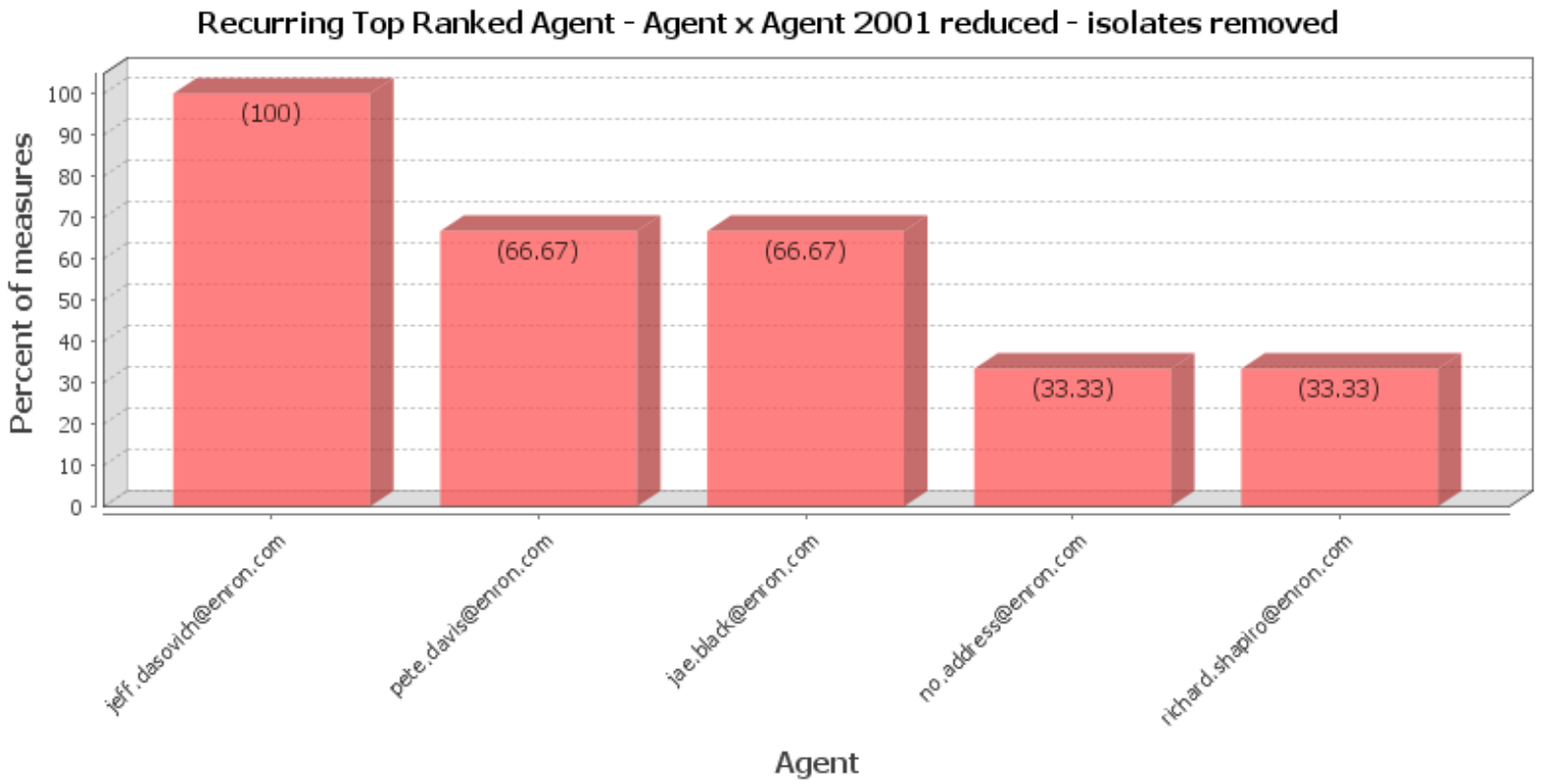
Enron – Network Anomaly Detection

- Anomaly assessment
  - Can we identify insiders in an organization based on their recorded email habits?
  - Are different network features more useful for identification?
- Identify features of Enron “insider-threats” and compare with other Enron employees
  - Insiders Threats will show
    - greater connections outside than inside firm and that change may grow over time
    - Increasing betweenness prior to events
    - Structural holes prior to events
- Extracted meta-networks from email headers
  - Automated
- Data organized by year
- Segmented out the Enron insiders
- Data cleaning
  - Collapsed all email ids of same Enron insider into single person
- Machine learning algorithm to identify insiders

Enron 2001



Enron Insiders are not top actors



Critical Actors are Interstitial

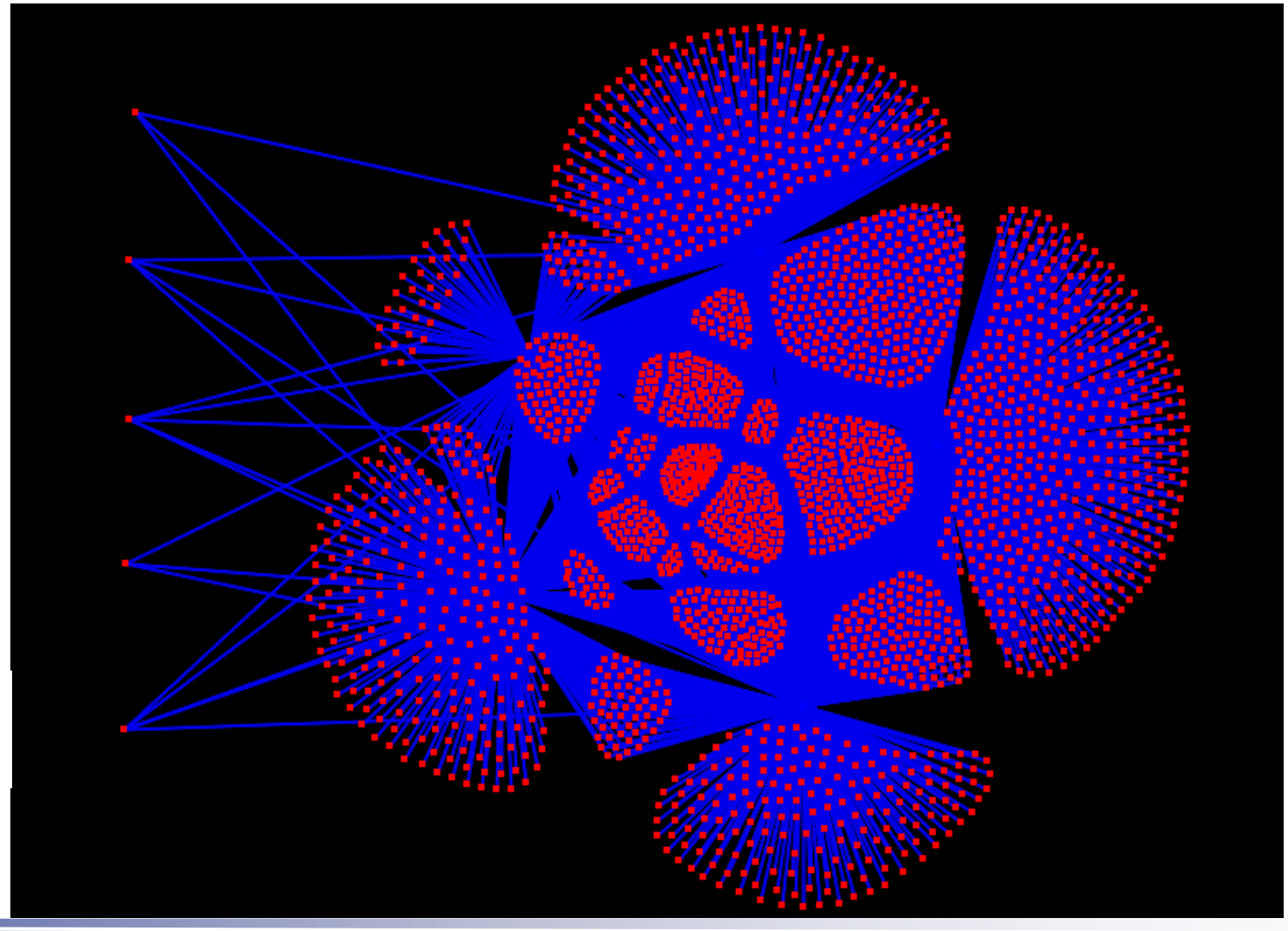
Jeff Skilling

Kenneth Lay

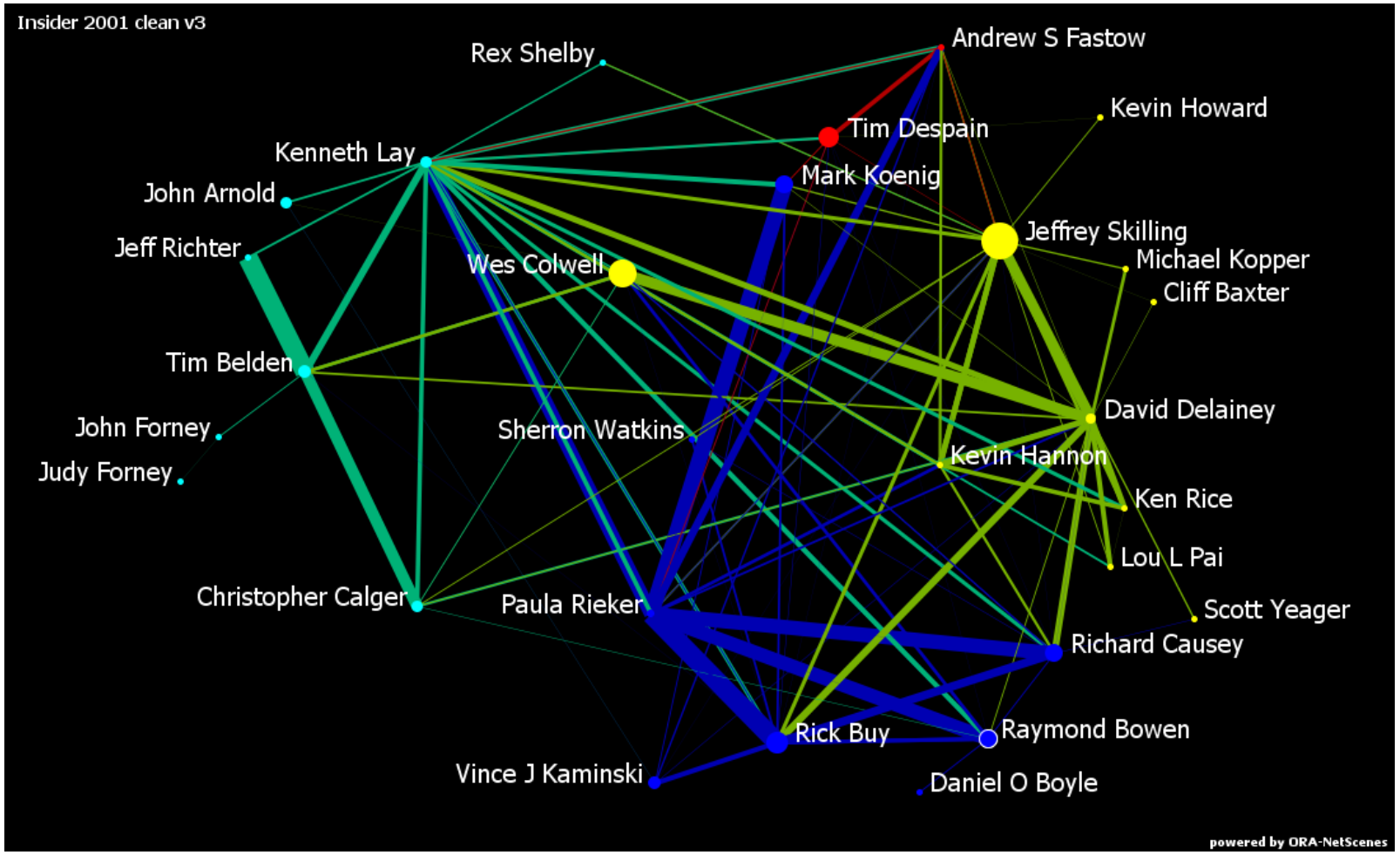
Tanya Jones

Veronica Espinoza

Jeff Dasovich

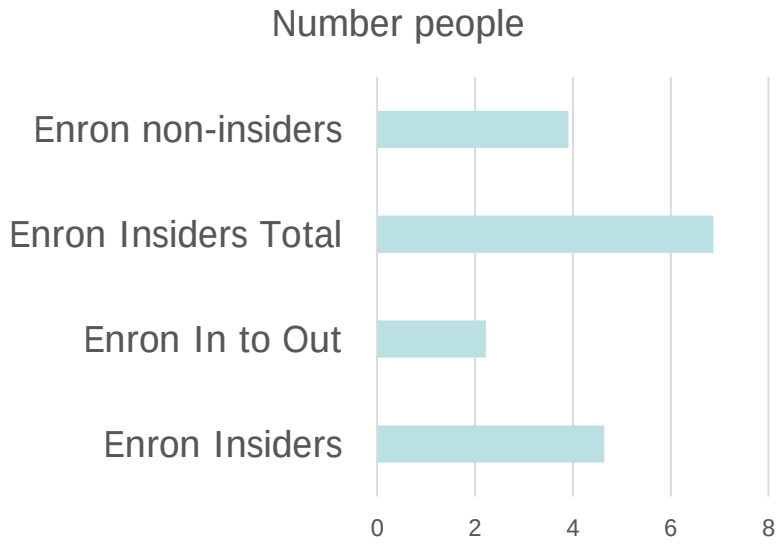


Enron "Insiders" – those accused – A densely connected sub-group

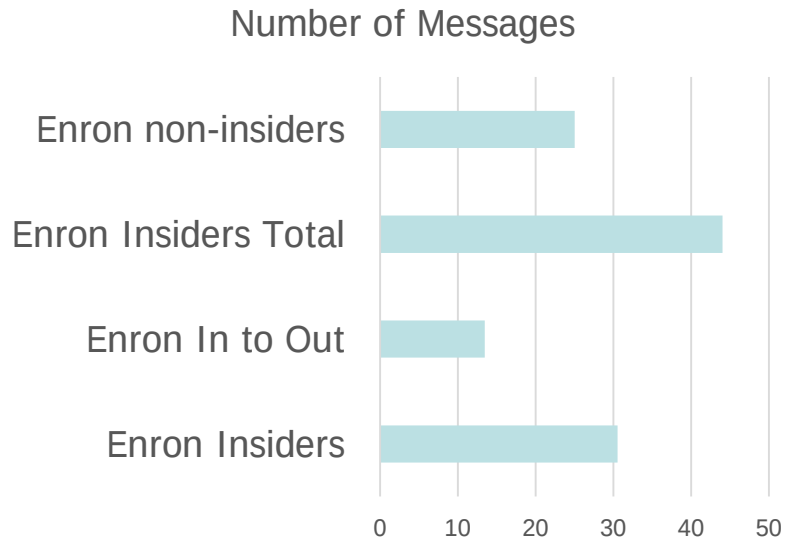


Enron Comparison of Insiders and non Insiders

Number of People Communicated with on Average



Number of Messages sent on Average



Details on Machine Learning Setup

- Algorithm: JRIP, which is based on RIPPER (Cohen 1995)
  - Supervised Learning Algorithm
  - Scales linearly with training instances
  - Goal was to handle hundreds of thousands of examples quickly
  - Roughly a thousand instances a second with our data
- Data-Cleaning:
  - Nodes with multiple email addresses had been consolidated
  - Distribution Lists had been removed
- We use five-fold cross-validation to evaluate performance (and generate the ROC curve, later).
  - 20% used to build classifier, 80% tested, flipping through what each 20% is used to build the classifier.

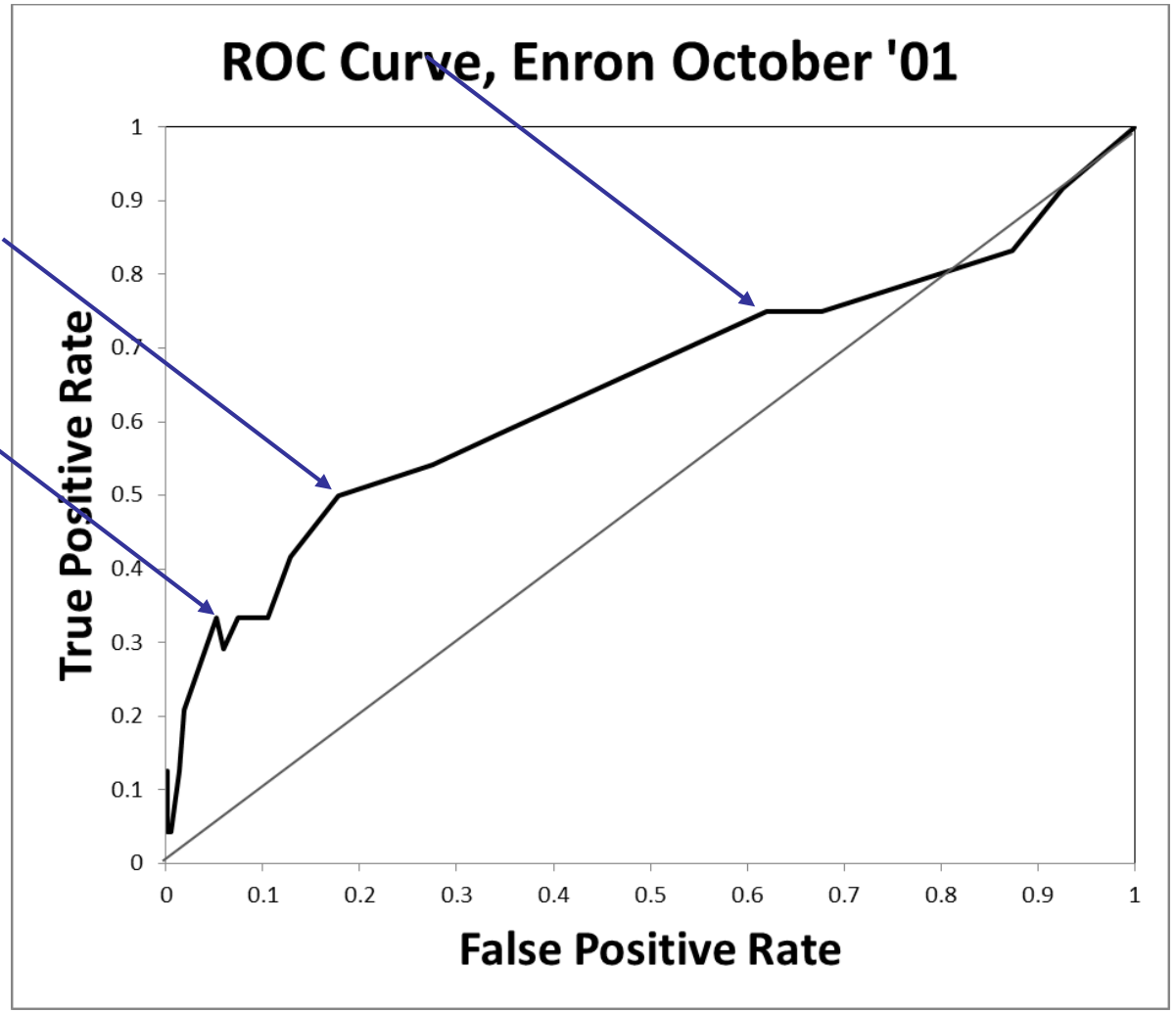
Definitions of Machine Learning Feature Groups

- Structural Features – Node-level network measures describing the position of the node in the entire network
  - Snapshot: These node-level network measures for a single meta-network representing a period of time
  - Summaries: Numerical summaries of these node-level network features over multiple points in time. Count, Min, Max, Sum, Average, Median, StDev
- Message Ratios – In-Degree and Out-Degree based on messages to employees and outsiders
  - Snapshot: These in-degree and out-degree for a single collection period
  - Multiple Snapshots: In-Degree and Out-Degree for multiple collection periods represented separately (May01, Oct01, etc)
  - Summaries: Numerical summaries of these ratios for multiple points in time for these nodes. Count, Min, Max, Sum, Average, Median, StDev

Feature Creation Summary

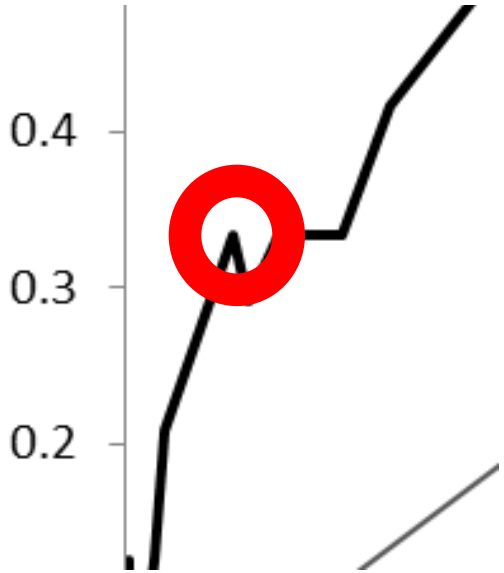
- Method:
  - All nodes
  - Structural Features: Snapshot + Message Ratio: Multiple Snapshots
- Filtering down to only organizational members is not useful
  - Insiders look like other employees
  - Insiders do not look like external actors
- Internal vs External Ratio very useful!
- Summaries (e.g. cumulative sums or averages) add noise features
  - Network collection not regular in Enron corpus
  - Executives trained to delete emails

ROC Curve for October 2001



JRIP Features on the ROC Curve (Alphabetical Order)

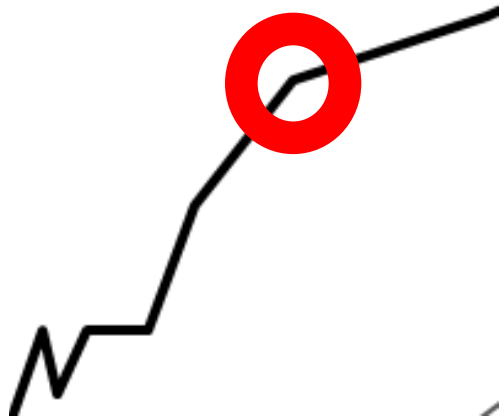
- AuthorityCentrality_TO
- CliqueCount_TO
- ClusteringCoefficient_TO
- CognitiveSimilarity_TO
- ColumnGiniMeansDifference_TO
- Constraint_TO
- CorrelationResemblance_TO
- InverseClosenessCentrality_BCC
- InverseClosenessCentrality_TO
- Oct2001_InDegree_TO_Internal
- May2001_InDegree_TO_ALL
- May2001_InDegree_TO_Internal
- WeakComponentMembers_BCC



33% True
.05% False

JRIP Features on the ROC Curve (Alphabetical Order)

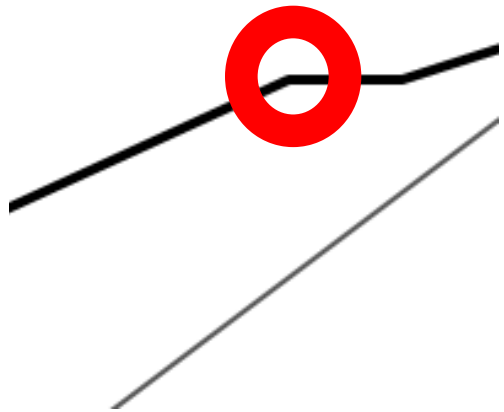
- ColumnGiniMeansDifference_TO
- InverseClosenessCentrality_BCC
- InverseClosenessCentrality_TO
- Oct2001_InDegree_TO_Internal
- May2001_InDegree_TO_ALL
- May2001_InDegree_TO_Internal
- WeakComponentMembers_BCC



50% True
18% False

JRIP Features on the ROC Curve (Alphabetical Order)

- ColumnGiniMeansDifference_TO
- May2001_InDegree_TO_ALL
- WeakComponentMembers_BCC



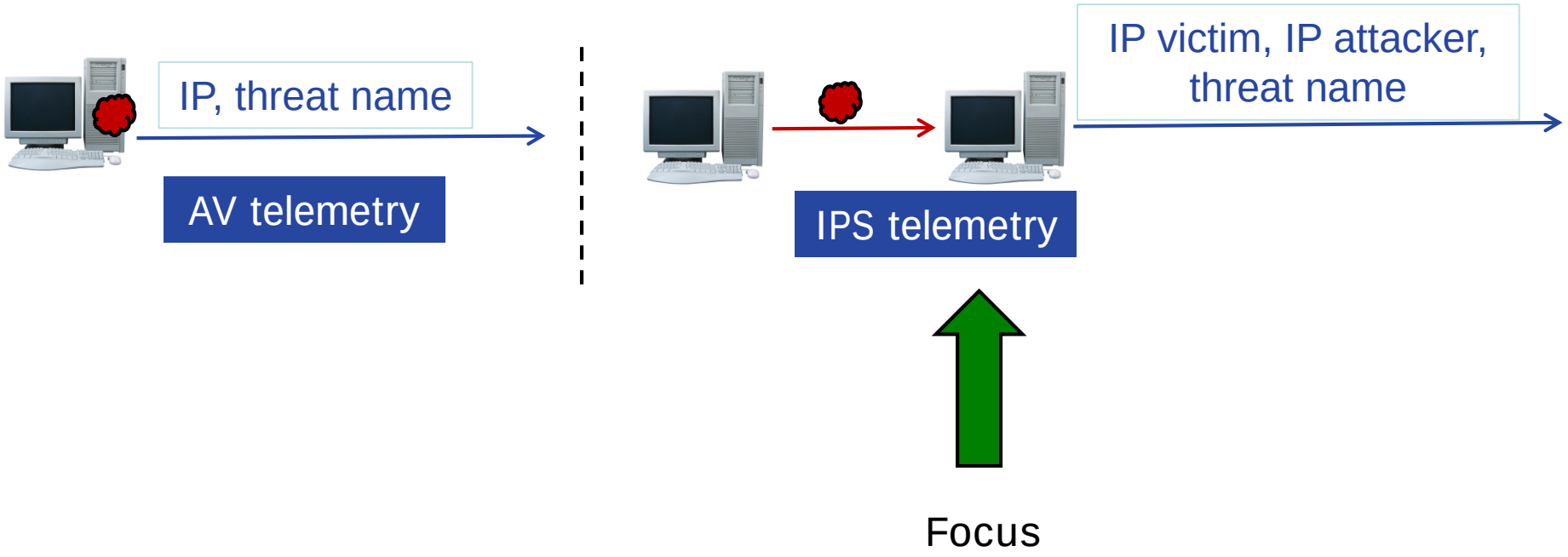
78% True
60% False

Findings on Insiders – those accused

- Are not “top” network actors
- Form a densely connected sub-group
- High level of in-group communication
- Low out-group communication
- Overall have many structural holes
- Part of a hidden network (BCC Weak component)
- Have long reach – inside and out – inverse closeness

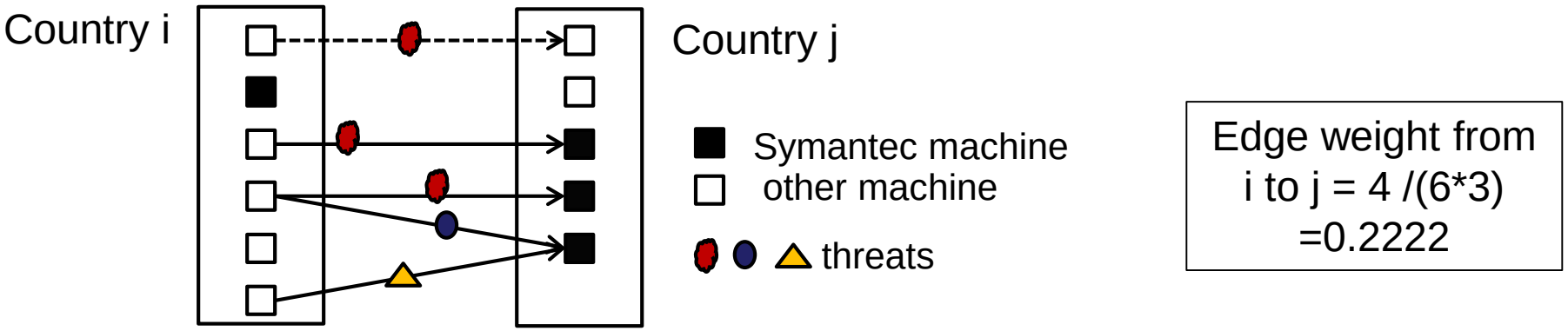
Symantec's WINE telemetry data

- From ~10 million customer machines worldwide
- Use thesaurus for threat attributes
  - AV: type, IPS: type, infrastructure



Attack Network

- Cyber attack network
  - Avg # of attacks by a computer in country i on a computer in country j
  - (# of attacks by computers in country i on computers in country j)/ (# of computers in i * # Symantec computers in j)
  - Total, infrastructure * type, (IPS)

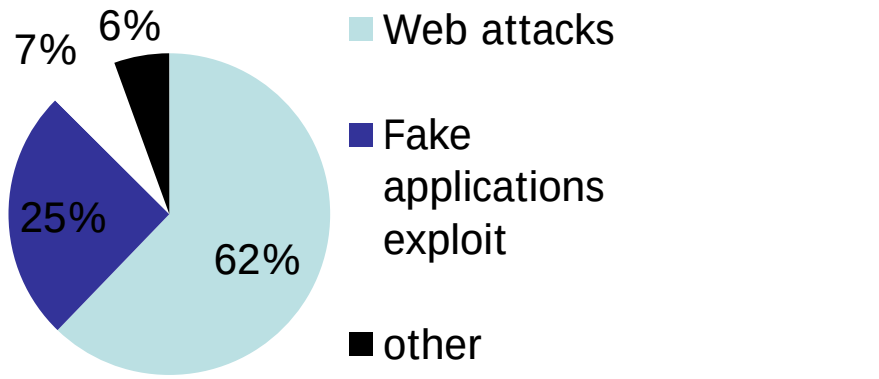


Edge weight from i to j = 4 /(6*3) =0.2222

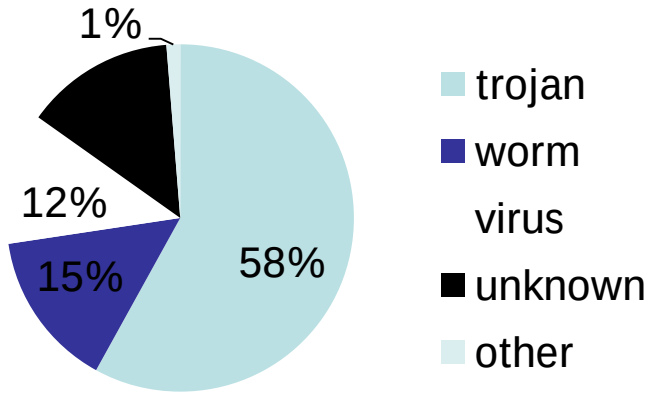
Non-Attack Data

- ICT development index
  - ICT development index [ITU 2010] that combines 11 indicators (fixed telephone lines per 100 inhabitants, mobile cellular telephone subscriptions per 100 inhabitants, international Internet bandwidth per Internet user(bits/s), % of households with a computer, % of households with Internet access, % of individuals using Internet, fixed broadband Internet subscriptions per 100 inhabitants, active mobile broadband subscriptions per 100 inhabitants, adult literacy rate, secondary gross enrolment ratio, tertiary gross enrolment ratio)
- Cyber Research
  - # cyber security papers during 2002-2011[SCOPUS]
- Region
  - Africa, Asia, Eastern European, Western European and others (includes US, Canada, N. Zealand), Latin America
- Corruption [transparency international]
  - Index of corruption in the public sector
  - High index value: low corruption
- Software piracy rate [Business software alliance]
  - Number of units of pirated software installed divided by total number of units of installed software
- GDP per capita [world bank]
- Alliance Network [correlates of war]
- Hostility Network network [Center for International Development & Conflict Management, Department of Peace and Conflict Research]

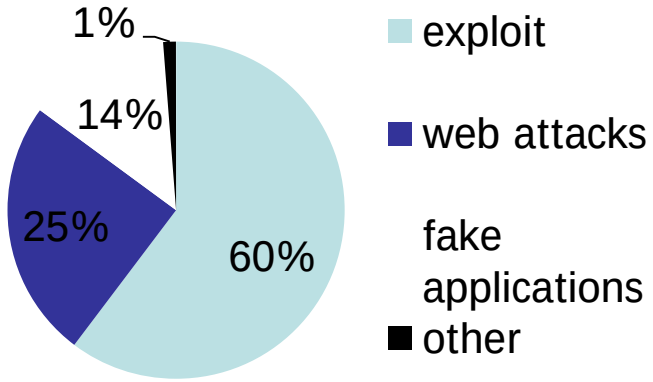
Relative Prevalence



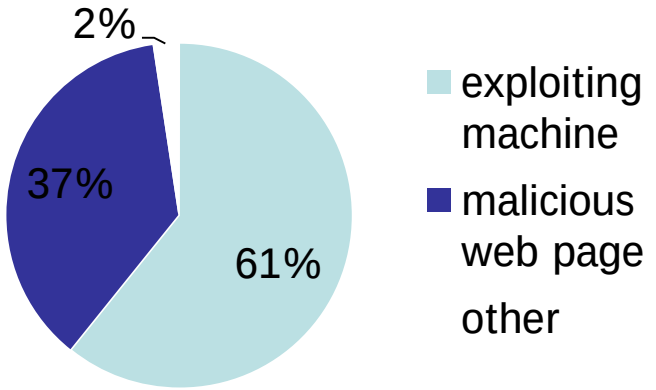
Threats encountered . Total = 24.52 M



Threats encountered (AV). Total = 9.75 M

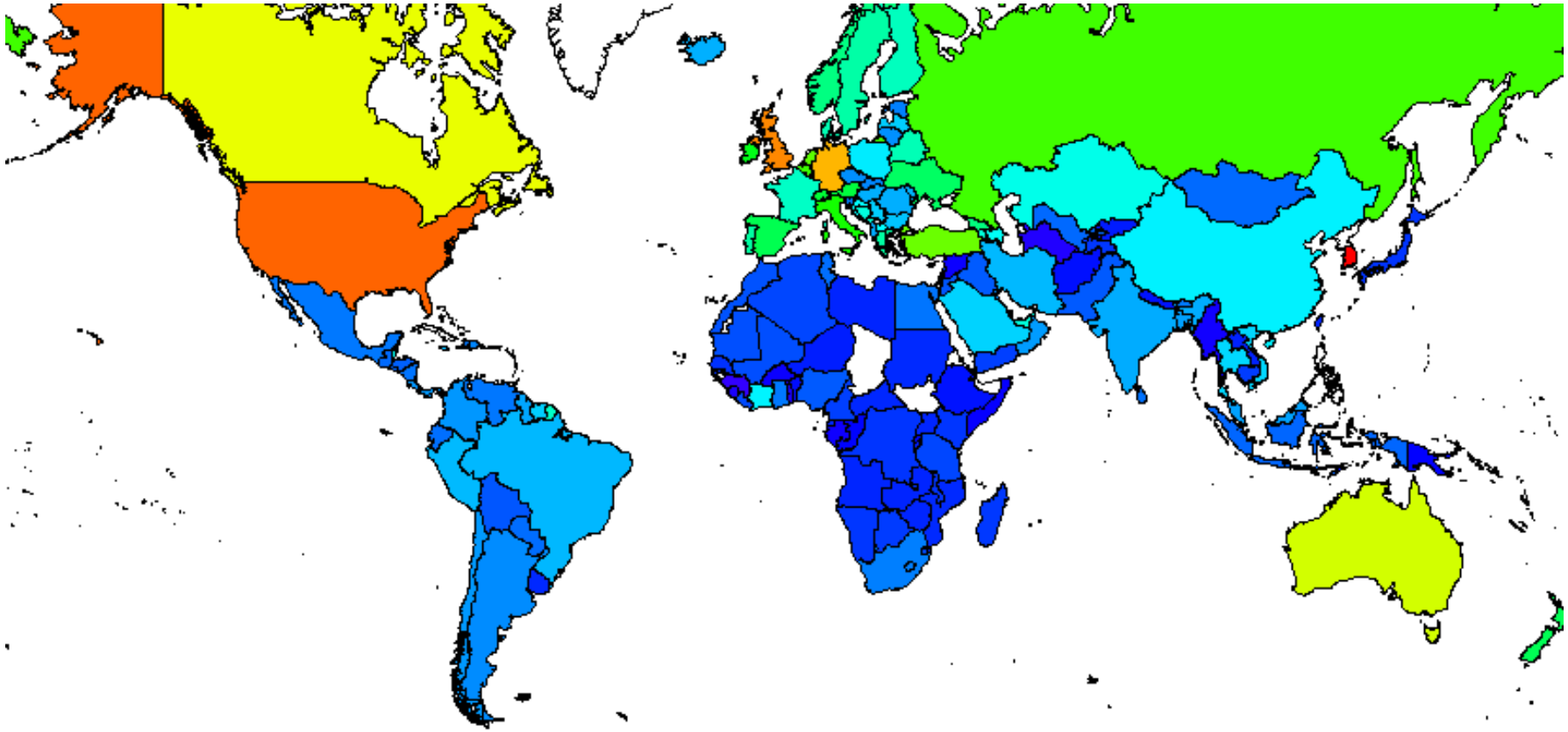


Attacks encountered.
Total ~ 35.9 M



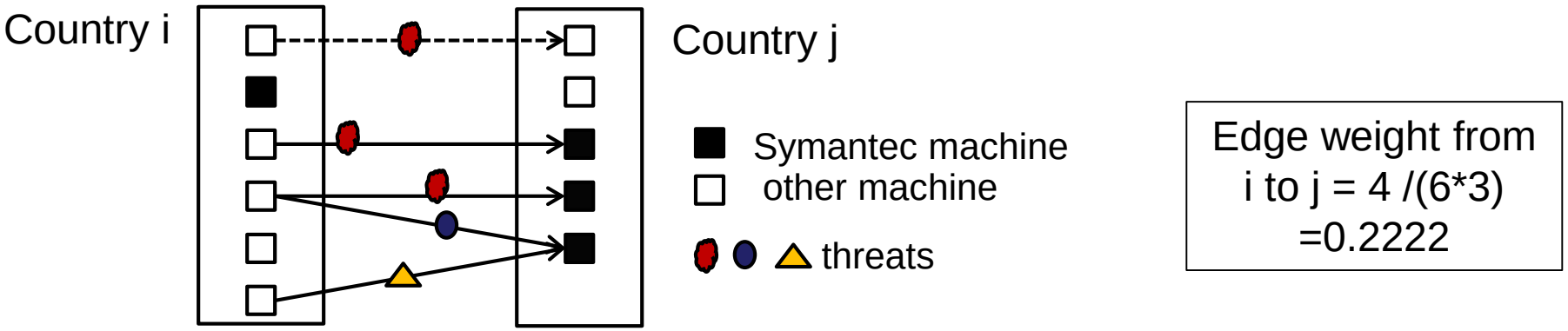
Attacks transmitted.
Total ~ 35.9 M

Web Site Threats Encountered



Attack Network

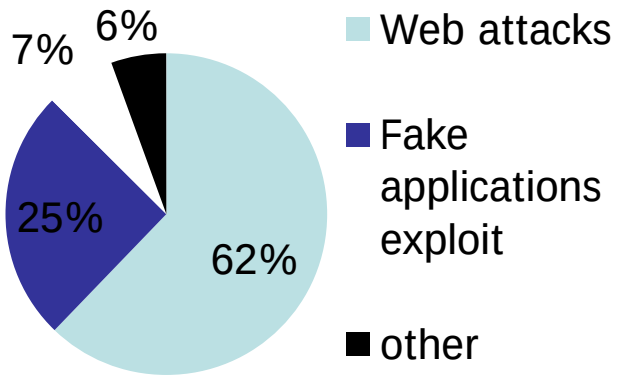
- Cyber attack network
  - Avg # of attacks by a computer in country i on a computer in country j
  - (# of attacks by computers in country i on computers in country j)/ (# of computers in i * # Symantec computers in j)
  - Total, infrastructure * type, (IPS)



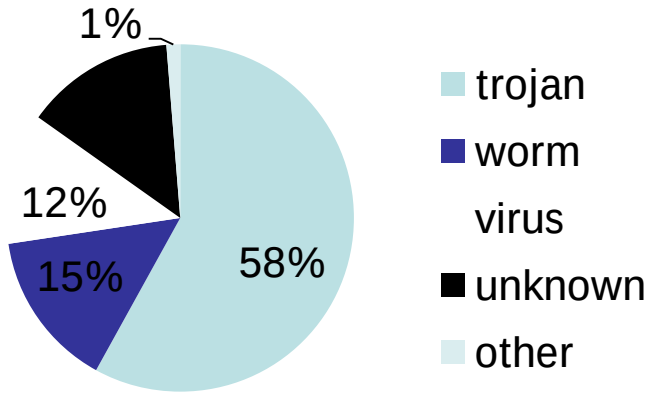
Non-Attack Data

- ICT development index
  - ICT development index [ITU 2010] that combines 11 indicators (fixed telephone lines per 100 inhabitants, mobile cellular telephone subscriptions per 100 inhabitants, international Internet bandwidth per Internet user(bits/s), % of households with a computer, % of households with Internet access, % of individuals using Internet, fixed broadband Internet subscriptions per 100 inhabitants, active mobile broadband subscriptions per 100 inhabitants, adult literacy rate, secondary gross enrolment ratio, tertiary gross enrolment ratio)
- Cyber Research
  - # cyber security papers during 2002-2011[SCOPUS]
- Region
  - Africa, Asia, Eastern European, Western European and others (includes US, Canada, N. Zealand), Latin America
- Corruption [transparency international]
  - Index of corruption in the public sector
  - High index value: low corruption
- Software piracy rate [Business software alliance]
  - Number of units of pirated software installed divided by total number of units of installed software
- GDP per capita [world bank]
- Alliance Network [correlates of war]
- Hostility Network network [Center for International Development & Conflict Management, Department of Peace and Conflict Research]

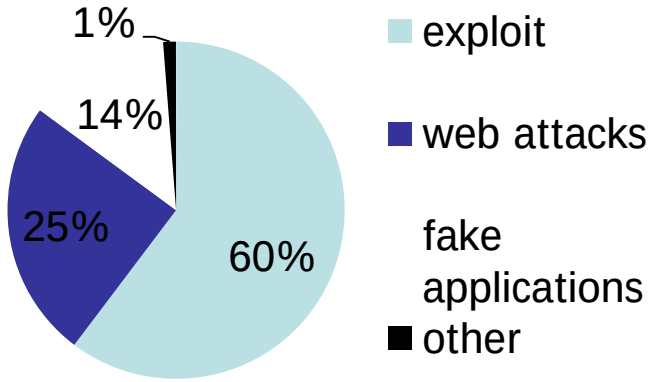
Relative Prevalence



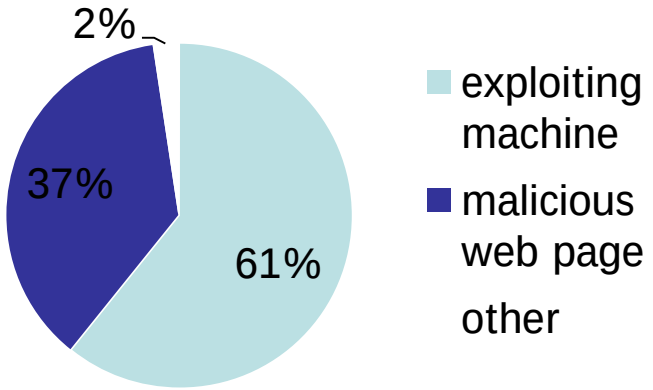
Threats encountered . Total = 24.52 M



Threats encountered (AV). Total = 9.75 M

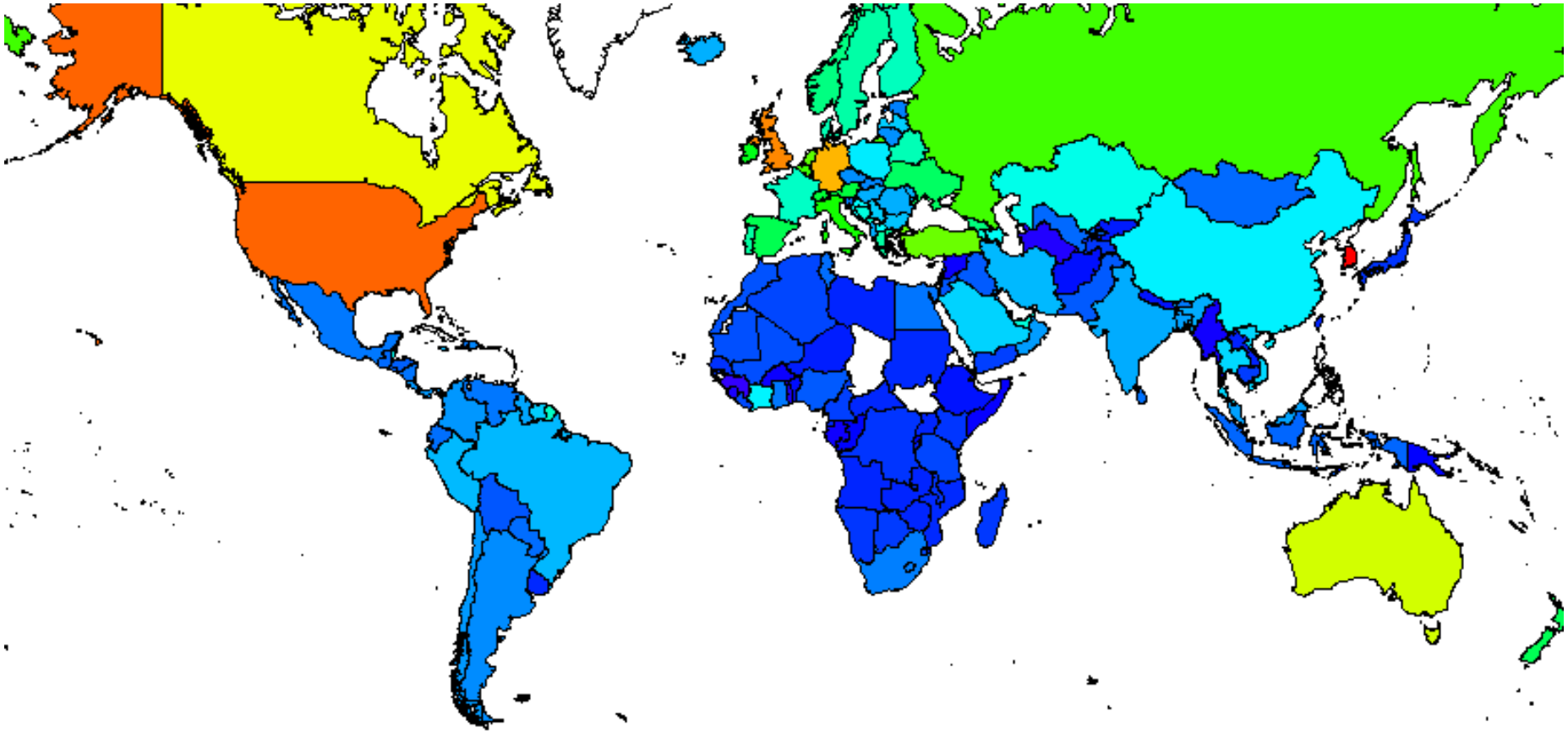


Attacks encountered.
Total ~ 35.9 M

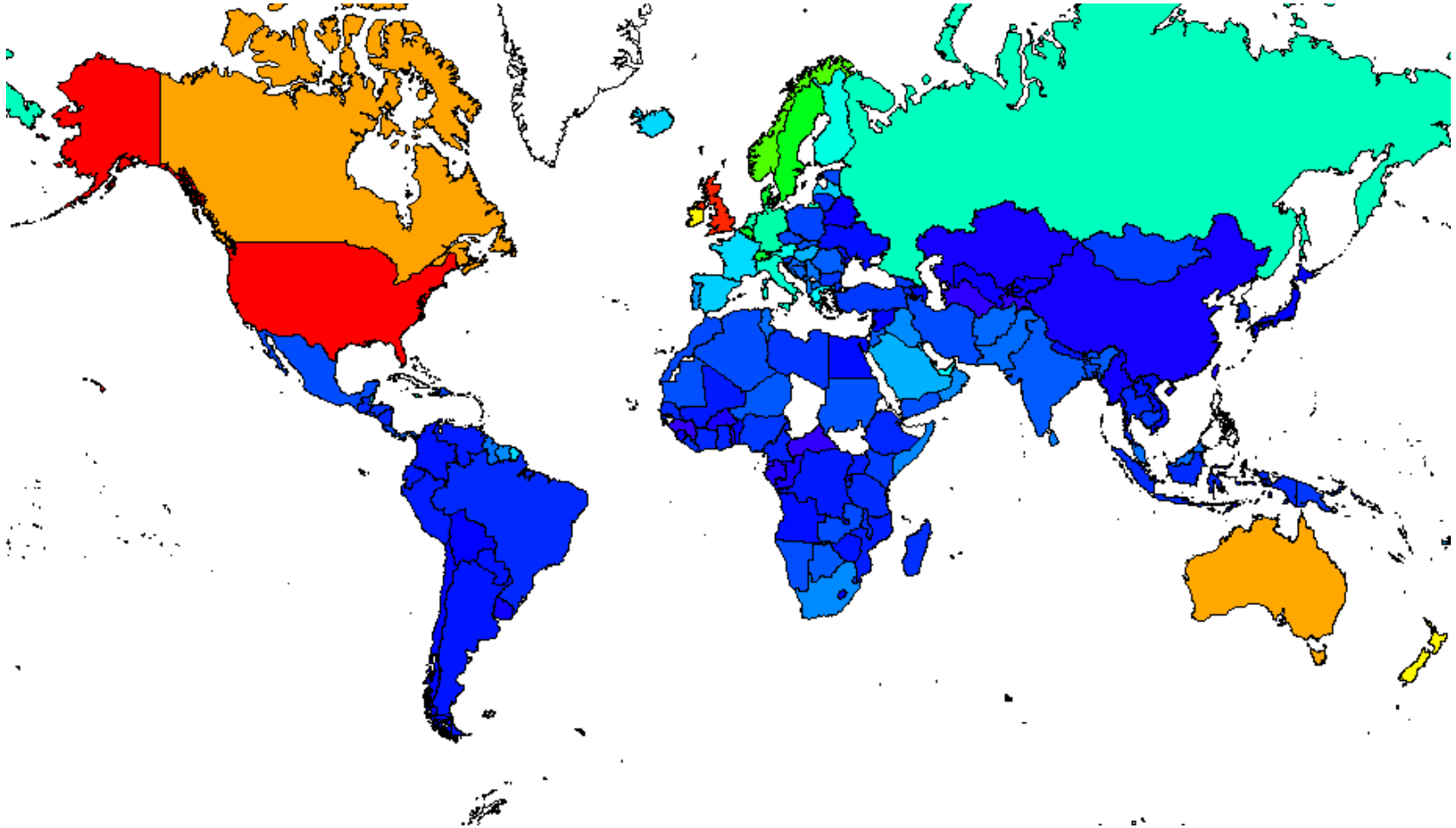


Attacks transmitted.
Total ~ 35.9 M

Web Site Threats Encountered



Fake Application Threats Encountered



Top Countries – Threats Encountered (IPS)

- Top countries for web attacks & fake applications
  - High ICT development
- Top countries for exploits
  - Middle ICT development

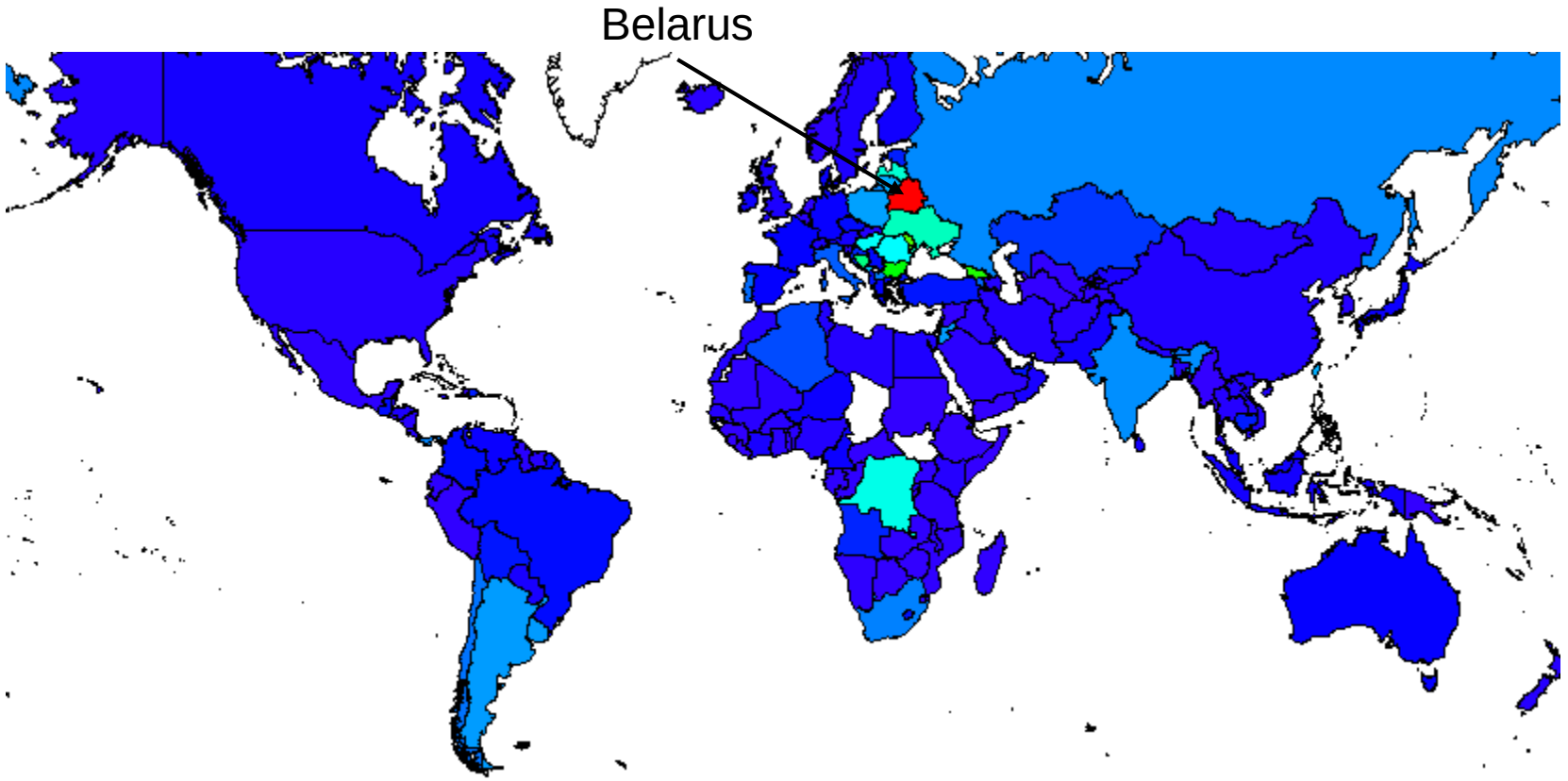
	All		Web attack		Fake application		Exploit	
Rank	country	value	country	value	country	value	country	value
1	United States	1.412	S. Korea	0.957	United States	0.424	Moldova	0.553
2	United Kingdom	1.34	United States	0.874	United Kingdom	0.409	India	0.369
3	Canada	1.199	United Kingdom	0.844	Canada	0.361	Latvia	0.309
4	Australia	1.164	Germany	0.805	Australia	0.359	Uruguay	0.284
5	S. Korea	1.058	Canada	0.727	Ireland	0.328	Ukraine	0.259
6	Germany	1.042	Australia	0.706	New Zealand	0.327	Taiwan	0.257
7	Ireland	0.97	Turkey	0.619	Norway	0.256	Bangladesh	0.24
8	Russia	0.942	Netherlands	0.608	Vatican	0.239	Mali	0.232
9	Italy	0.937	Russia	0.585	Sweden	0.217	Belarus	0.226
10	Moldova	0.869	Belgium	0.581	Belgium	0.212	Kazakhstan	0.223

Top Countries – Attacks Encountered (IPS)

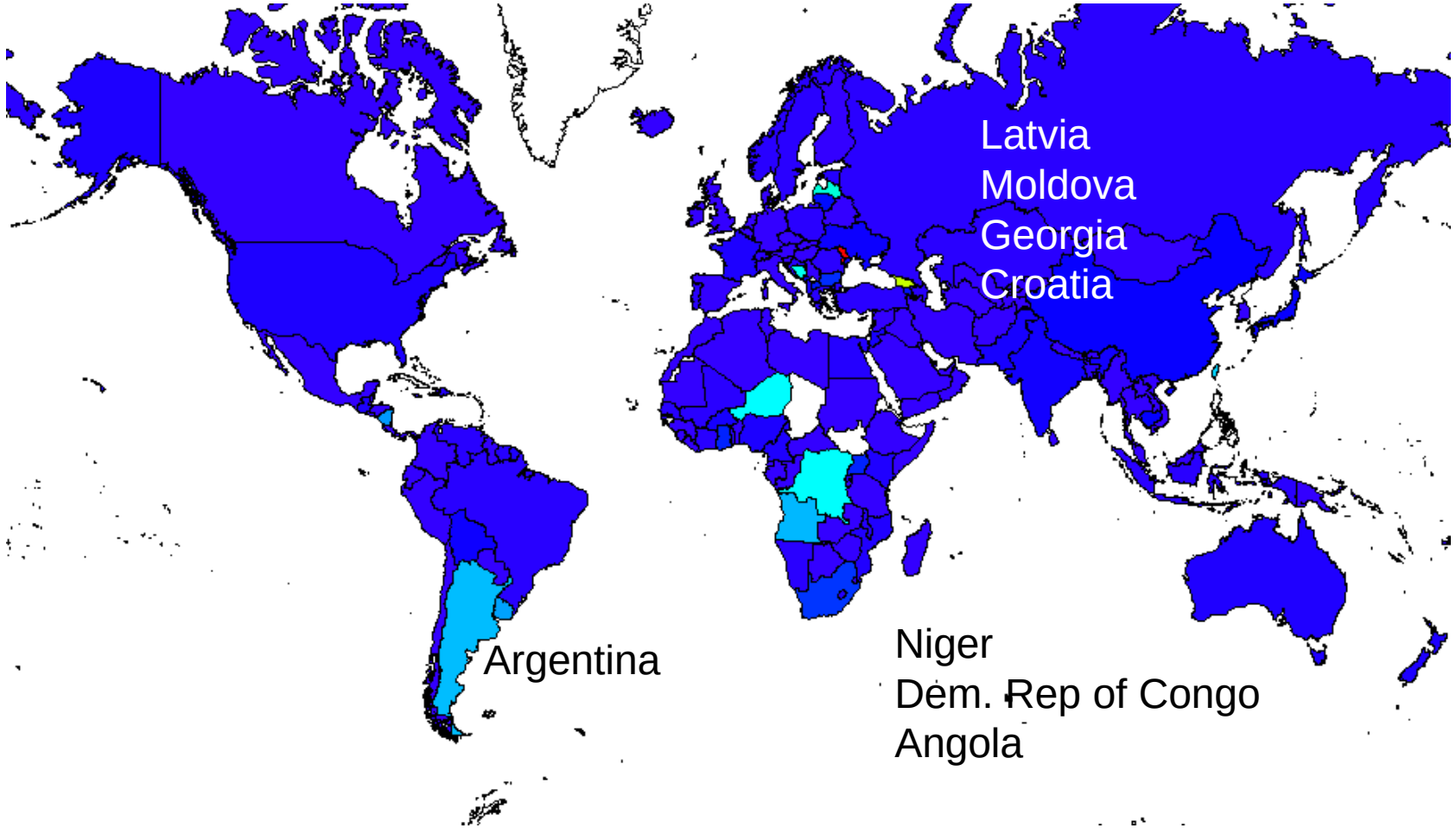
- Top countries for web attacks & fake applications
  - High ICT development
- Top countries for exploits
  - Middle ICT development

	All		Exploit		Web attacks		Fake application	
Rank	country	value	country	value	country	value	country	value
1	Moldova	28.77	Moldova	28.42	Germany	1.64	United States	0.92
2	India	16.56	India	16.22	S. Korea	1.64	United Kingdom	0.83
3	Taiwan	15.91	Taiwan	15.75	United States	1.29	Canada	0.76
4	Nicaragua	13.3	Nicaragua	13.02	United Kingdom	1.25	Australia	0.68
5	Latvia	13.05	Latvia	12.58	Netherlands	1.06	Ireland	0.59
6	Italy	11.13	Italy	10.09	Canada	0.99	New Zealand	0.56
7	Israel	10.1	Israel	9.54	Australia	0.99	Norway	0.46
8	Uruguay	8.41	Uruguay	8.23	Russia	0.83	Switzerland	0.4
9	Bosnia & Herzegovina	7.45	Bosnia & Herzegovina	6.86	Belgium	0.81	Belgium	0.38
10	Georgia	7.07	Georgia	6.54	Italy	0.79	Sweden	0.36

Exploits Transmitted – "Purportedly"



Exploits: Countries that act as wayports



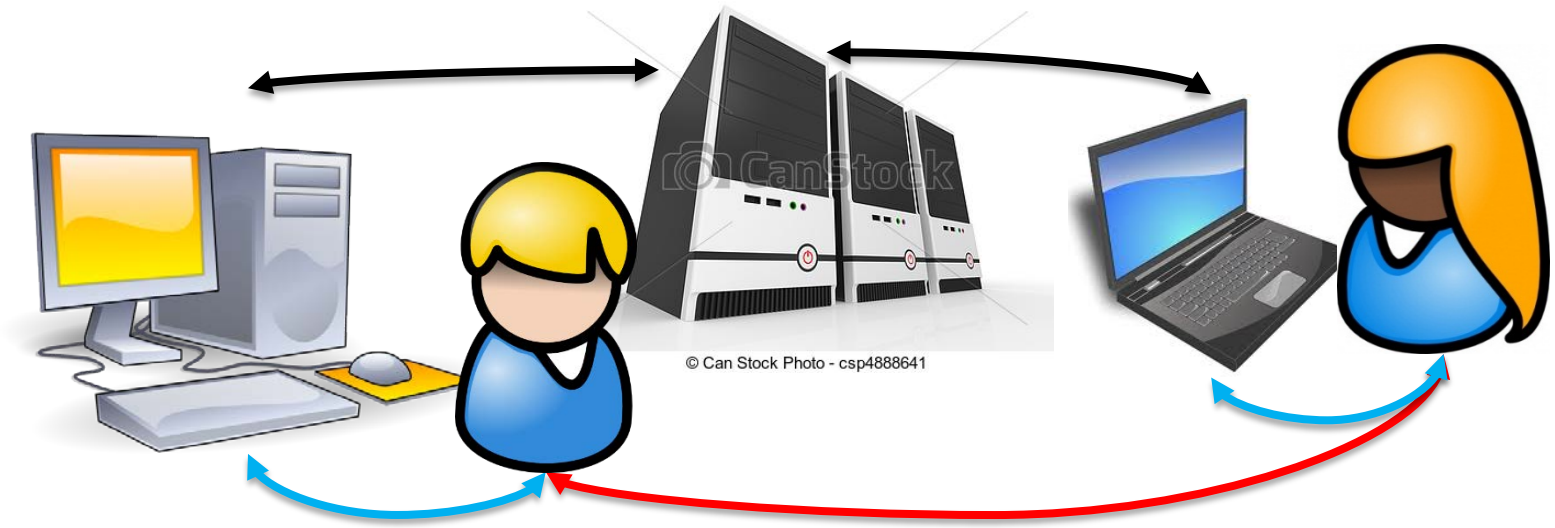
Findings on Global Mapping

- Web Attacks Increasing
- Wayport countries
  - High corruption
  - Unsophisticated IT infrastructure
  - Include some in Russia sphere of influence
- Third world countries may be more susceptible to wide range of attacks

Resiliency

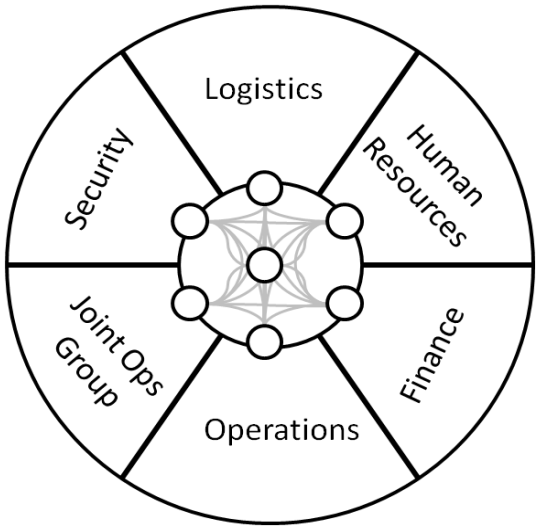
How should organizations be structured to mitigate the impact of cyber attacks?

- Approach:
  - Empirically Grounded Computer Simulation
- Why are we unique:
  - Model both the human side and the information technology side

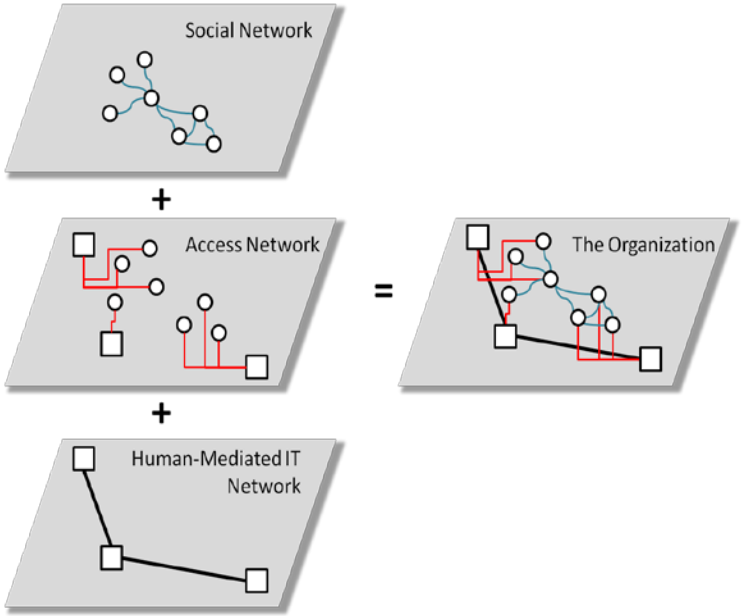


Modeling the Organization

- Organizations have multiple functions each necessary for operation

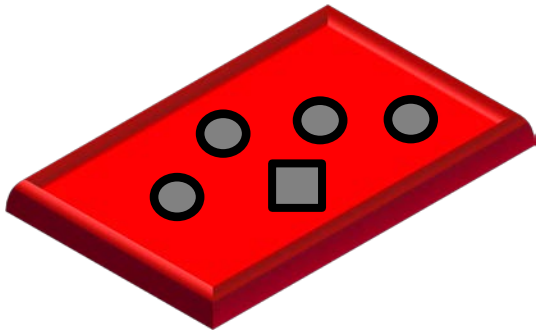


- Interactions occur across multiple modalities

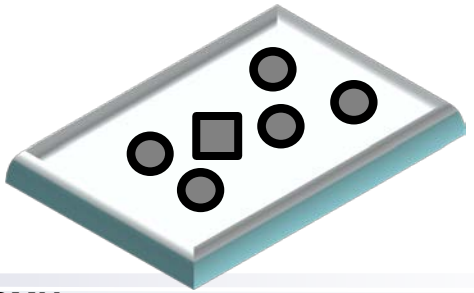


- Organizations with sensitive information have clearance or control systems for protected information

Has Clearance:



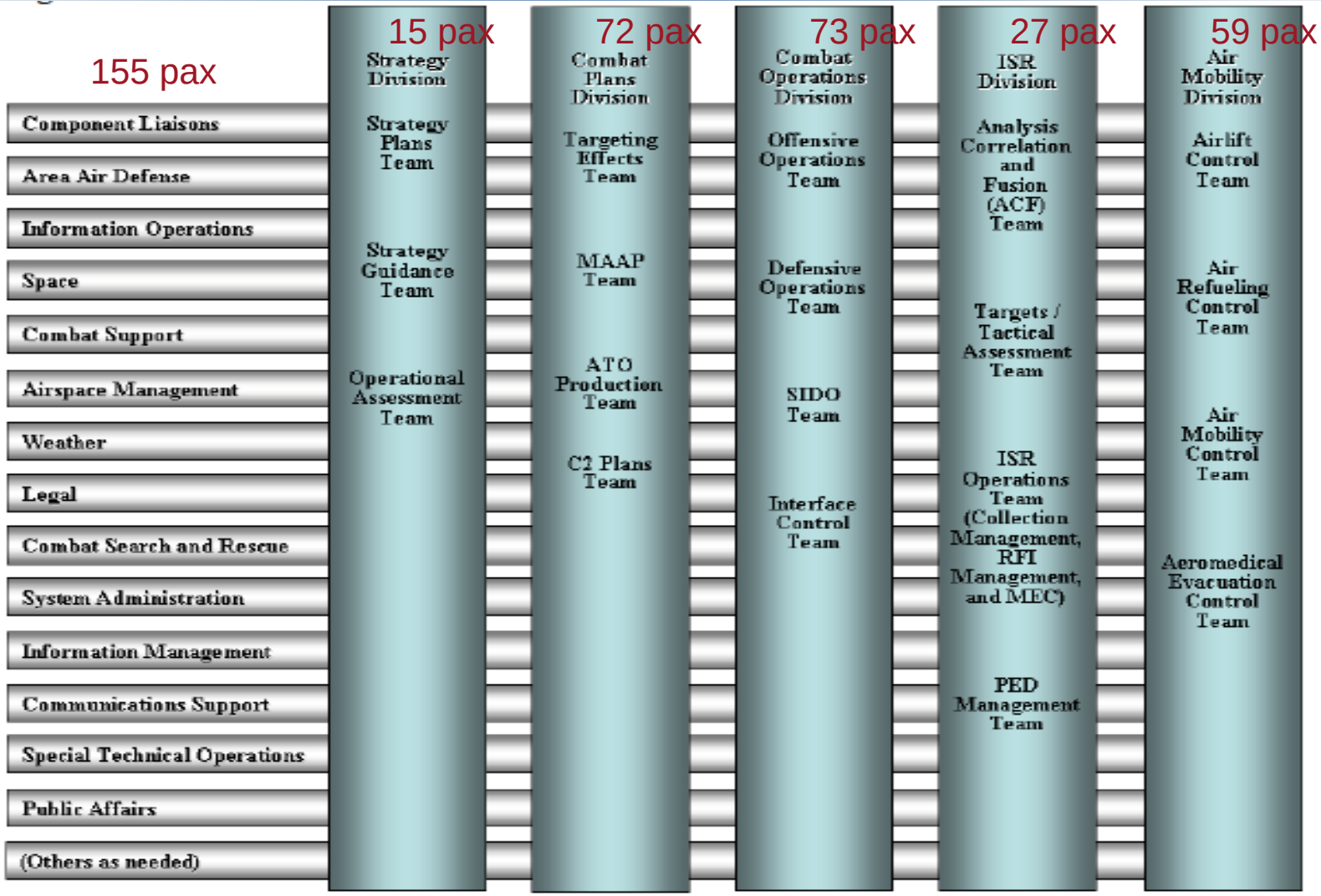
No Clearance:



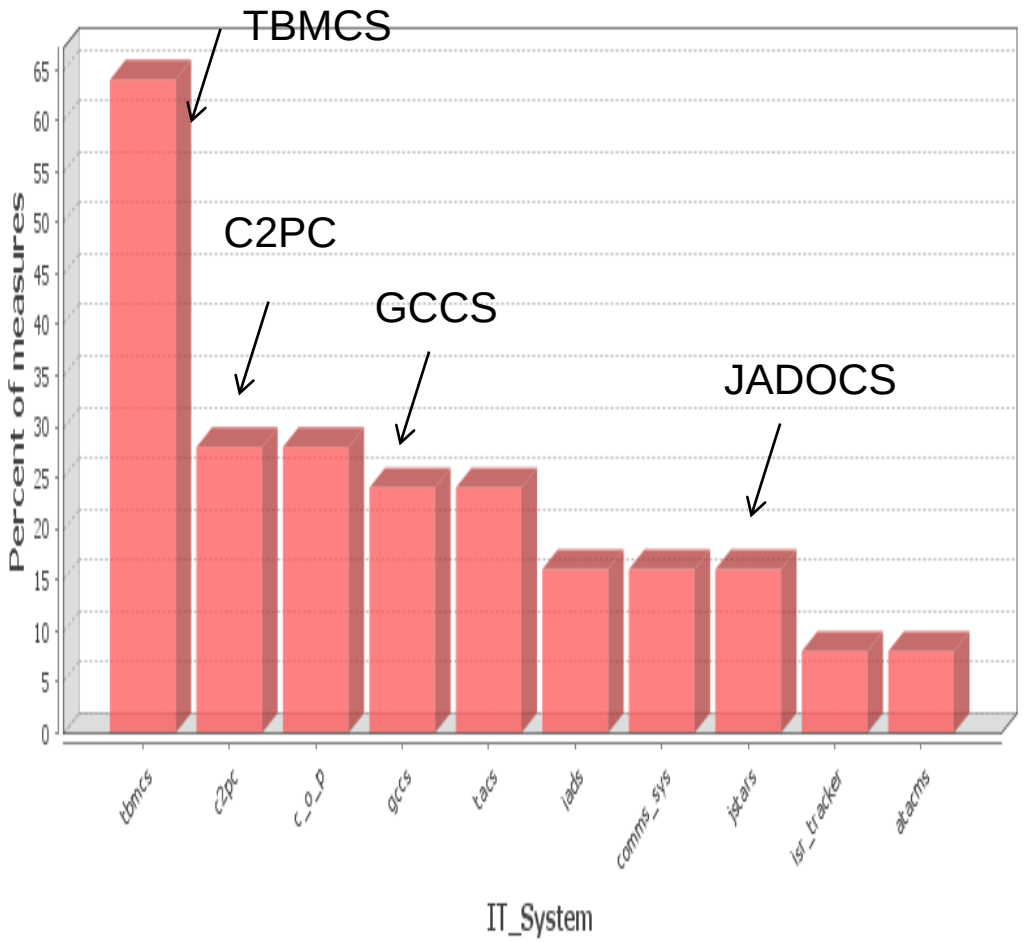
USAF AOC – a cross between Divisions and Functional Areas

Overall number of people in AOC:401

Extrapolated from Automap generated model from doctrinal references (AFI 13-1 AOC v3, AFTTP 3-3.2 AOC Nov '07, AFD 2-1.17 May '01)



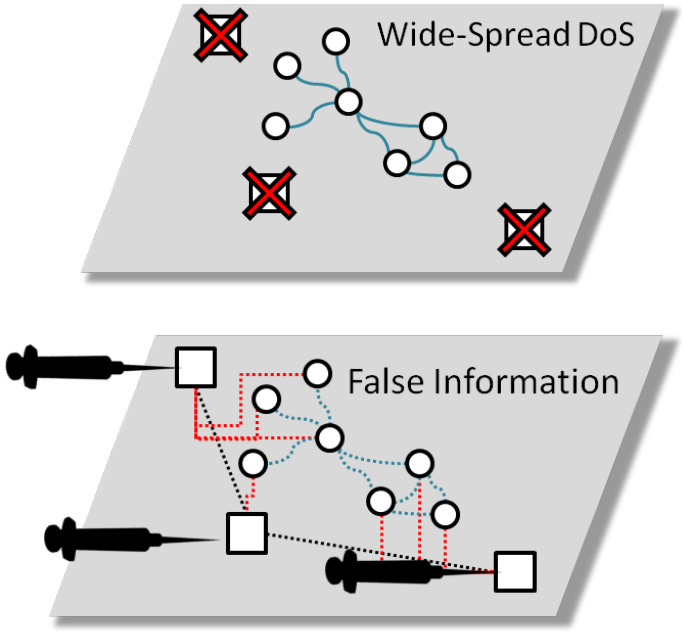
Key Entities in USAF AOC



- For USAF Regional AOC
  - TBMCS, is in top 10 list ~60% of the agent-relevant measures (13 of 22) (Lanham et al, 2011b)
  - E.g., Betweeness Centrality (across all node pairs that have a shortest path containing *v*, the percentage that pass through *v*) (Freeman, 1979)

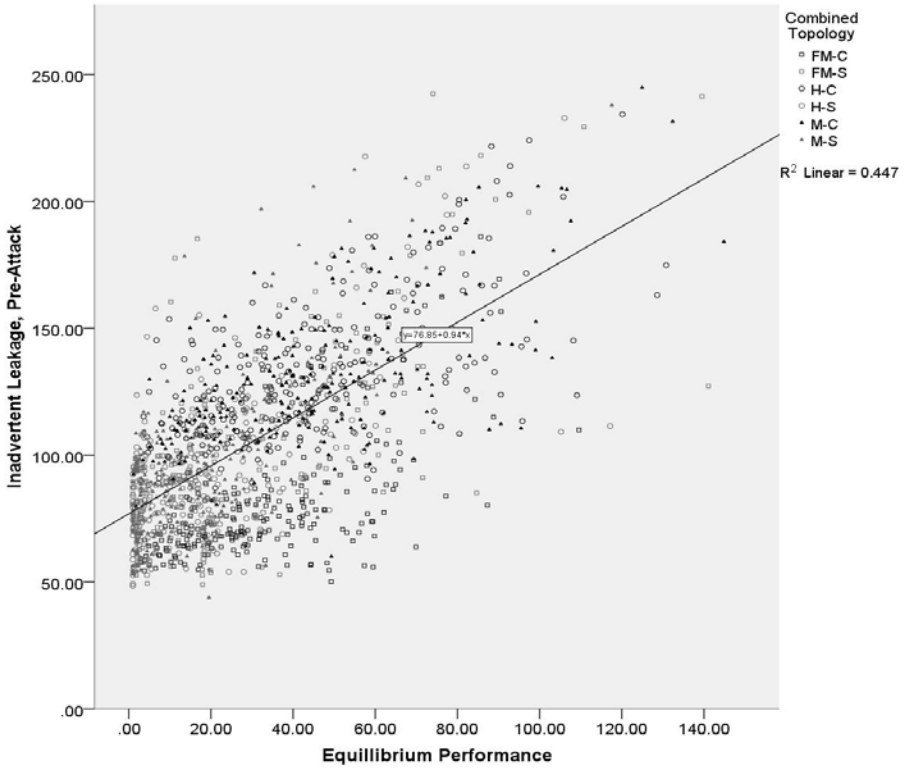
Most Attacks are Minimally Disruptive

- Our models have shown that most attacks cause minimal disruption to the organization's processes
- Supported by the empirical literature.
- We now focus on **severe** attacks and on attack combinations.



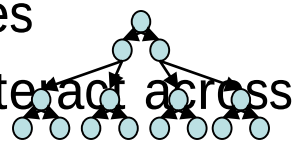
Inadvertent Leaks

- Inadvertent leaks occur when proprietary or classified information is transferred to those who should not have access, s.t. the transfer may have occurred without explicit intent
- Inadvertent leaks are:
  - Inevitable
  - More likely in higher performing organizations
  - More likely in certain network topologies
  - Prevention requires heedful interaction and acting as a high reliability organization

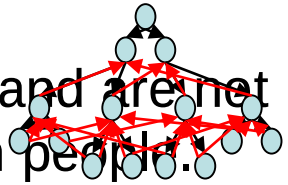


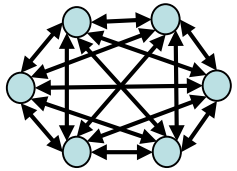
Topologies

- Social network – people to people
  - Functional Mesh: members of each functional area may interact with each other
  - Hierarchy: 3-4 levels with each manager having 3-7 subordinates
  - Matrix: Hierarchy + cross-functional teams where members interact across functional areas



- IT Networks – system to system
  - Stove-pipe: All Decision Support IT Systems are autonomous, and are not intended to be cross-linked with each other except through interaction with people.
  - Cloud: All Decision Support IT Systems are allowed to create cross-linkages as desired.



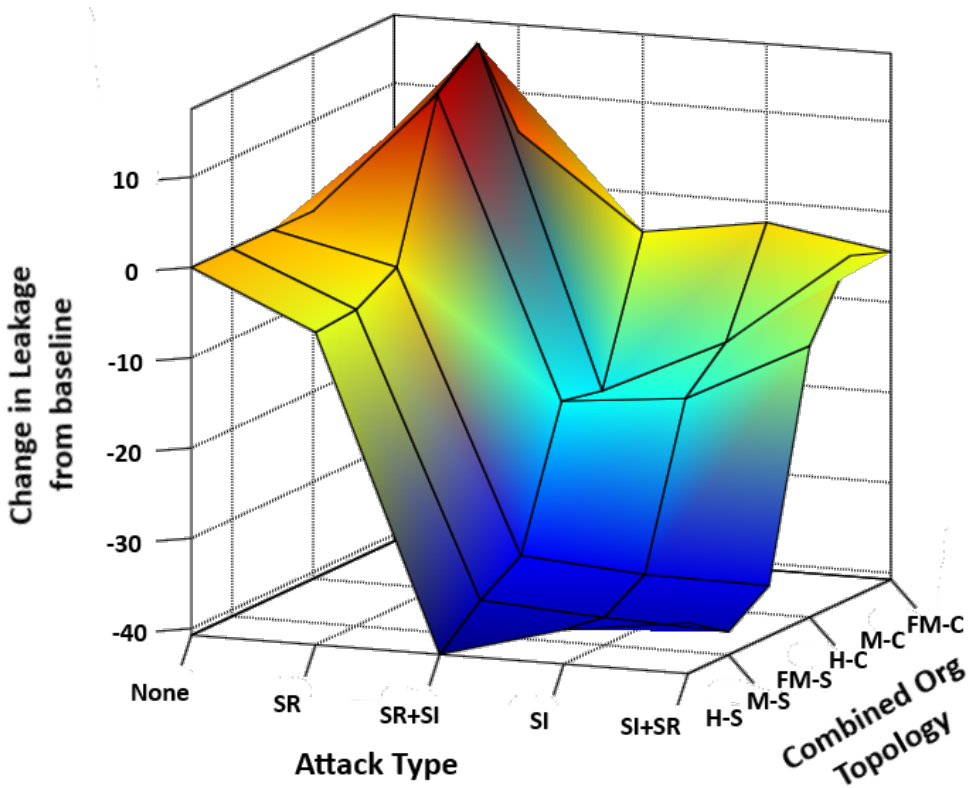


Attacks

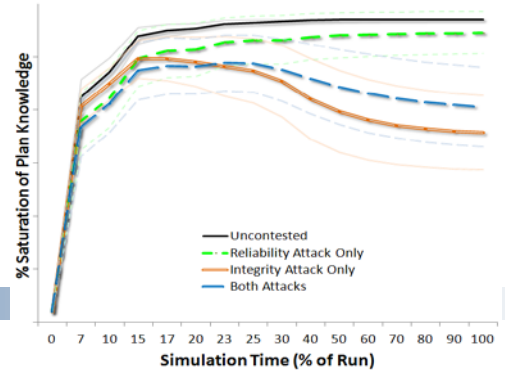
- No Attacks
- Reliability
  - Non-Severe – IT support system is unavailable
  - Severe – all IT support systems are unavailable
- Integrity
  - Non-Severe – compromised IT system has ingested new non-relevant data
  - Severe - introduce new non-relevant but interesting information to the organization through all IT systems
- Reliability & Integrity

Impact of Attacks and Topology

- Hierarchical Siloed organizations least prone to inadvertent leaks and performance will be least degraded by attacks
- Combined attacks most harmful
- Cloud is more conducive to inadvertent leaks



Illustrative Results



- Most organizations resilient to small and medium attacks
- Integrity attacks more devastating than DOS attacks
  - shown Air Operations Command (AOC).
- Resiliency is enhanced by redundancy
- Resiliency is increased by coordination
- When only a few systems face an integrity attack, key decision makers are less impacted than others
  - Possibly leading to feeling attack is not serious
  - Contributes to resiliency as key personnel are able to operate
- When many systems are attacked key decision makers are more impacted

Network Analytics

- Useful for insider threat
- Supports analysis of high dimensional networks
- Supports analysis of big data
- Supports social media analytics
- Valuable methodology for Science of Security