BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK

Cyberspace Security as an Emerging Area of International Collaborative Research

Dr. Victor A. Skormin
Distinguished Service Professor
Electrical/Computer Engineering
Watson School of Engineering
vskormin@binghamton.edu

- **The on-going "arms-race" is one of the realities of the cyberspace**

- **The ever-increasing resources invested in the development of computer defenses are often outweighed by low-cost efforts of the hacker community**

- **The term "asymmetric warfare" perhaps is best to describe the existing shaky balance between defensive and offensive forces in cyberspace**

- **Cyber attacks are very different from all traditional forms of warfare**
  - **Cyber attacks are inherently covert**
  - **It is difficult to identify the attackers**
  - **The cyberspace does not conform to geographical and geopolitical realities**

BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK

- **In response to economical loss and destabilization on the global scale caused by cyber attacks governments and professional communities must increase collaborative efforts to address this phenomenon**

- **International collaboration is a necessary condition for successful location of the origin of the attack, identification of the perpetrators, and attack mitigation**

- **International collaboration will lead to the development of mutual trust between specialists that eventually may result in the development of mutual trust between governments**

- **In many ways, international collaborative efforts in the area of cyber security should be modeled after the collaboration between those who predict hurricanes and spread of infectious diseases**

- **Such collaboration will be instrumental in dealing with many forms of cybercrime and cyber terrorism.**

Possible areas/forms of collaboration

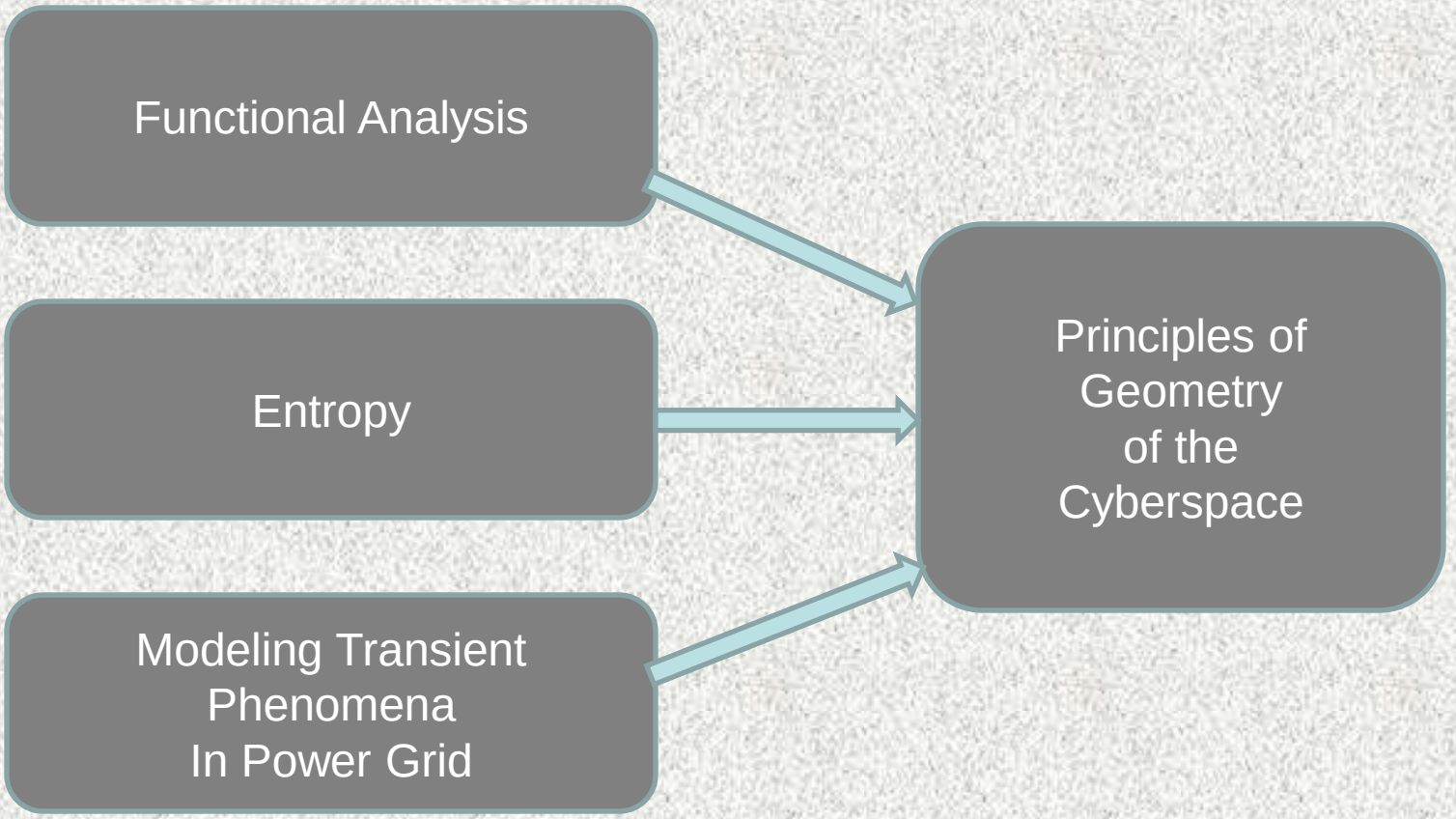
- Identifying attack targets
- Collaborative attack analysis
- Providing and exchanging complete incident reports
- Identifying vulnerabilities exploited by attackers
- Providing evidence of the perpetrated attack including captured code samples and malware binaries
- Identifying technologies used in the attack including botnets, malware hosting servers, etc.
- Working with digital forensics experts to extract evidence from captured hardware and data
- Exchanging malware samples and detection signatures

- Requesting governments to have their Internet service providers to disclose information about particular machines and users involved in the attack
- Requesting Internet service providers to provide connection activity logs. If logs are not being kept long enough, request ISP to hold logs for a longer period of time
- Establishing teams of multinational independent security experts to conduct attack analysis and investigation
- Requesting foreign governments to shut down malware hosting servers and tracing the origin of hosted malware code

and

Conducting Joint Research

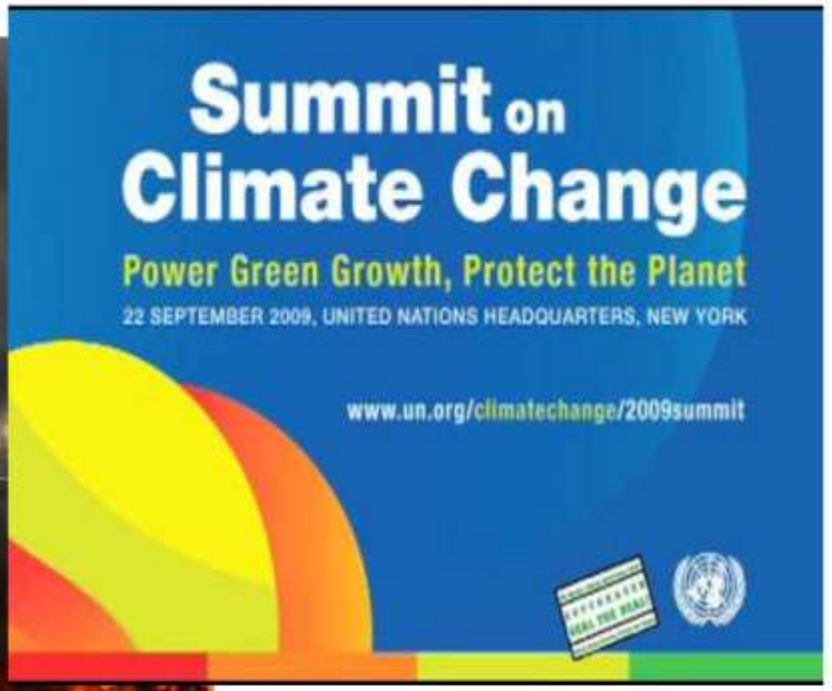
Specific Research Areas



CyCast- Cyberattack Forecasting

- Our Hypothesis:
  - Understanding the past and current relationships between Social, Political, Economic and Cultural events and cyber attacks can help us forecast impending cyber attacks
    - Working at the syntactic layer, intrusion-detection sensors observe the data packet headers and packet content
    - CyCast taps into the human-network looking for signs of motive for a cyber attack

What about the Human Network?



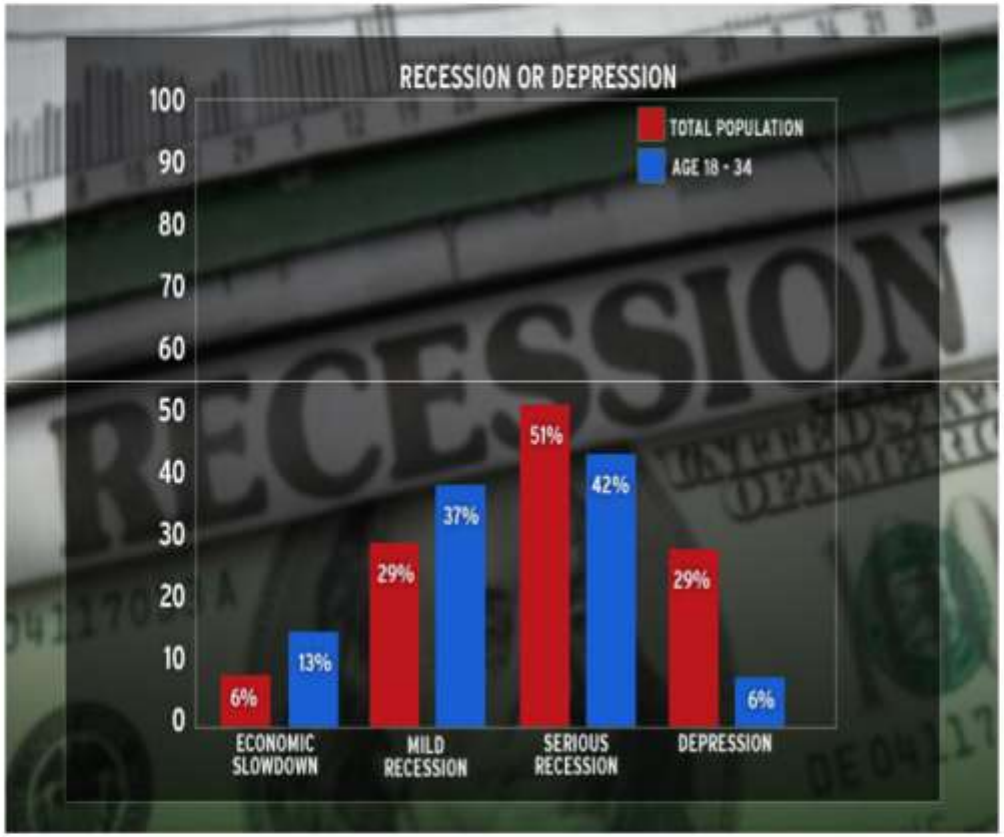
vancouver 2010

Social/cultural/environmental events

What about the Human Network?

Political events

What about the Human Network?



Economic events

Examples

- July 4, 2009 On Independence day
  - Federal Government websites came under DDoS attack

- October 13, 2009
  - On the 70th anniversary of the outbreak of World War II,
    - Unsuccessful cyber attack on Polish government systems
- November 6, 2009
  - Swedish Signals Intelligence Agency started new role of intercepting and monitoring Internet traffic passing through Sweden
    - Agency's website came under cyber attack

A Database of Cyber Attacks

http://kewi.unomaha.edu/cycast/

CyCast

Cyberattack Forecasting System

University of Nebraska Omaha

Main Menu

- Home
- Cyber Events Database
- Visual Representation
- Projects
- Publications
- Members
- About Us

Links

- KEWI
- NUCIA
- Computer Science
- College of Information Science and Technology
- University of Nebraska at Omaha

Recent Cyberattacks | Cyberattack Events | Advanced Search | Add New Events | Metrics Page

Recent events of Cyberattack

Koobface server pops up in China after HK takedown., Apr 23, 2010
Security experts in Hong Kong recently succeeded in taking down a key component of the Koobface botnet, only to witness the system popping up in China. The Koobface FTP grabber component uploaded stolen FTP user names and passwords to the remote server, which was under the control of cybercrooks. These stolen log-in credentials gave a pass into corporate networks and valuable data before the server was taken down last week, largely thanks to the efforts of the Hong Kong Computer Emergency Response Team Coordination Centre. In response, the Koobface gang moved their server to a hosting firm in China. Last month, the command and control servers associated with Koobface underwent a complete refresh. Koobface spread via messages on social networking sites like Facebook and Twitter. Cybercrooks behind the sophisticated malware make their money by distributing scareware packages onto compromised machines, and by other cyberscams, including information harvesting. The worm gets less press than the malware associated with the Google China attacks or the high-profile Conficker worm, though experts consider it both more sophisticated and a bigger security threat.
Reference: http://www.theregister.co.uk/2010/04/23/koobface_takedown/

Fake fast food survey with cash reward leads to phishing site, Apr 23, 2010
Scammers often use the familiarity of a brand as a means of lessening the victims' tendency to be cautious when perusing unsolicited e-mails. In this latest e-mail scam, this method is coupled with the offer of $80 to whomever takes a short survey. The e-mail supposedly comes from a globally well-known fast food chain, and claims that the company is planning major changes to the establishments in order to improve the quality of service. In order to do so, they are asking the customers to fill out a survey and they offer the cash as an incentive. Symantec reports that to access the survey, the victims are encouraged to follow the link in the e-mail, which will then take them to a bogus page ostensibly belonging to the company. After the survey is completed, the victims are redirected to a fake user-authentication page where they are asked to enter their name, e-mail address, credit card number, expiration date, verification number and personal identification number, in order to get the money. but the survey is fake, and the page is a phishing page.
Reference: http://www.net-security.org/secworld.php?id=9182

1.5 million stolen Facebook IDs up for sale, Apr 22, 2010
A hacker named Kirllos has a rare deal for anyone who wants to spam, steal or scam on Facebook: an unprecedented number of user accounts offered at rock-bottom prices. Researchers at VeriSign's iDefense group recently spotted Kirllos selling Facebook user names and passwords in an underground hacker forum, but what really caught their attention was the volume of credentials he had for sale: 1.5 million accounts. IDefense does not know if Kirllos' accounts are legitimate, and Facebook did not respond to messages April 22 seeking comment. If the accounts are legitimate, the hacker has data on about one in every 300 Facebook users. His asking price varies from $25 to $45 per 1,000 accounts, depending on the number of contacts each user has. To date, Kirllos seems to have sold close to 700,000 accounts, according to the VeriSign director of cyber intelligence. Hackers have been selling stolen social-networking credentials for a while — VeriSign has seen a brisk trade in names and passwords for Russia's VKontakte, for example. But now the trend is to go after global targets such as Facebook, the director said.
Reference: http://www.computerworld.com/s/article/9175936/1.5M_stolen_Facebook_IDs_up_for_sale

Learning Cause and Effect

motive

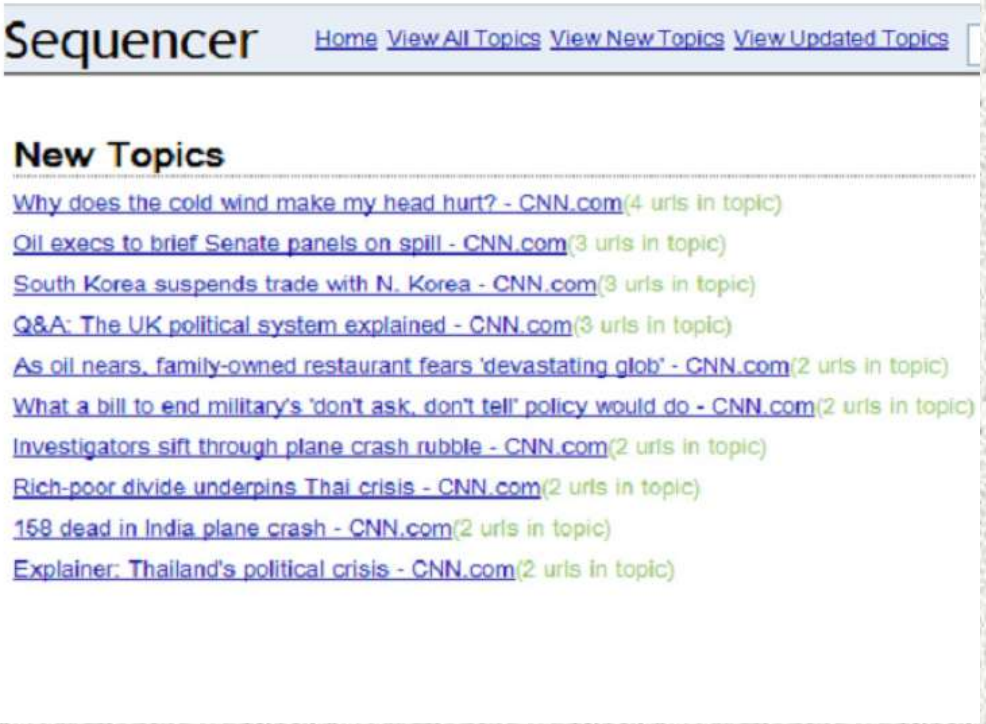
Legend

N: News
A: Agents
M: Motives
MN: Means
O: Opportunities
C: Consequences
V: Victims
AC: Attack co-ordination
TA: Technological aspects

	A1: Insider	A2: Outsider	A3: Vandals/Hack	A4: Cyber mercen	A5: Nations / Stat	A6: Hactivists	M1: Protest against organ	M2: Commemorate hi	M3: Commemorate obse	M4: Motivated by human righ	M5: Protest Web filtering / censorsh	MN1: Denial of Serv	MN2: Spread of ma	MN3: SQL and	O: Weaknesses in th	C1: Confidentiality	C2: Integrity	C3: Availability	V1: Government	V2: Commercial org	V3: Individuals	AC1: Organized attac	AC2: Unorganized at	TA1: Disruption of serv	TA2: Loss of data confi	TA3: Loss of data integ	TA4: Spread of malwar	TA5: Cyber espionage
N1: Web site of China-based journalist club attacked, 4/2/2010					X					X		X				X					X	X			X			
N2: Government sites crumple -Operation Titstorm, 2/10/2010						X					X	X						X	X			X		X				
N3: Climate Change E-mail Hack, 11/23/2009		X	X			X	X								X	X					X	X			X			
N4: Attack Hits Swedish Signals Agency's Website, 11/6/2009						X					X	X						X	X			X		X				
N5: April fool's day, Conficker worm, 4/2009		X	X						X				X		X		X	X	X	X	X		X				X	
N6: Cyber attack to protest against G8, Germany, 6/1999		X				X	X					X						X		X		X		X				
N7: CIH/Chernoby1, 4/1999		X	X					X					X		X		X		X	X	X		X				X	
N8: Chinese human rights Web sites suffer attacks, 1/25/2010					X					X		X						X			X	X		X				
N9: Virus Appears As Response To Craigslist Ad, 8/2009		X	X										X		X		X				X		X			X	X	
N10: DoS attack, Belarus/Eastern Europe, 4/2008			X					X				X						X		X			X	X				
N11:Websites attacked to protest human right abuse in E. Timor,11/1998		X				X				X				X	X		X	X	X			X				X		
N12: Attack on atomic research center, India, 5/1998		X				X	X							X	X		X		X				X			X		
N13: Website of DOJ attack, USA, 1996						X					X			X	X		X		X				X			X		
N14: Web attack against French Government websites, France, 12/1995						X	X					X						X	X			X		X				

Temporal Tracking of Entities

- Using CNN.com as the source of documents
- Three data sets created:
  - 1 week, depth 6 crawl (12k docs per index)
  - 1 month, depth 6 crawl
  - 4 days, depth 3 crawl (300 docs per index)



Temporal Tracking of Entities

Sequencer Home View All Topics View New Topics View Updated Topics Search

Officials warn of potential catastrophe from Gulf of Mexico oil spill - CNN.com

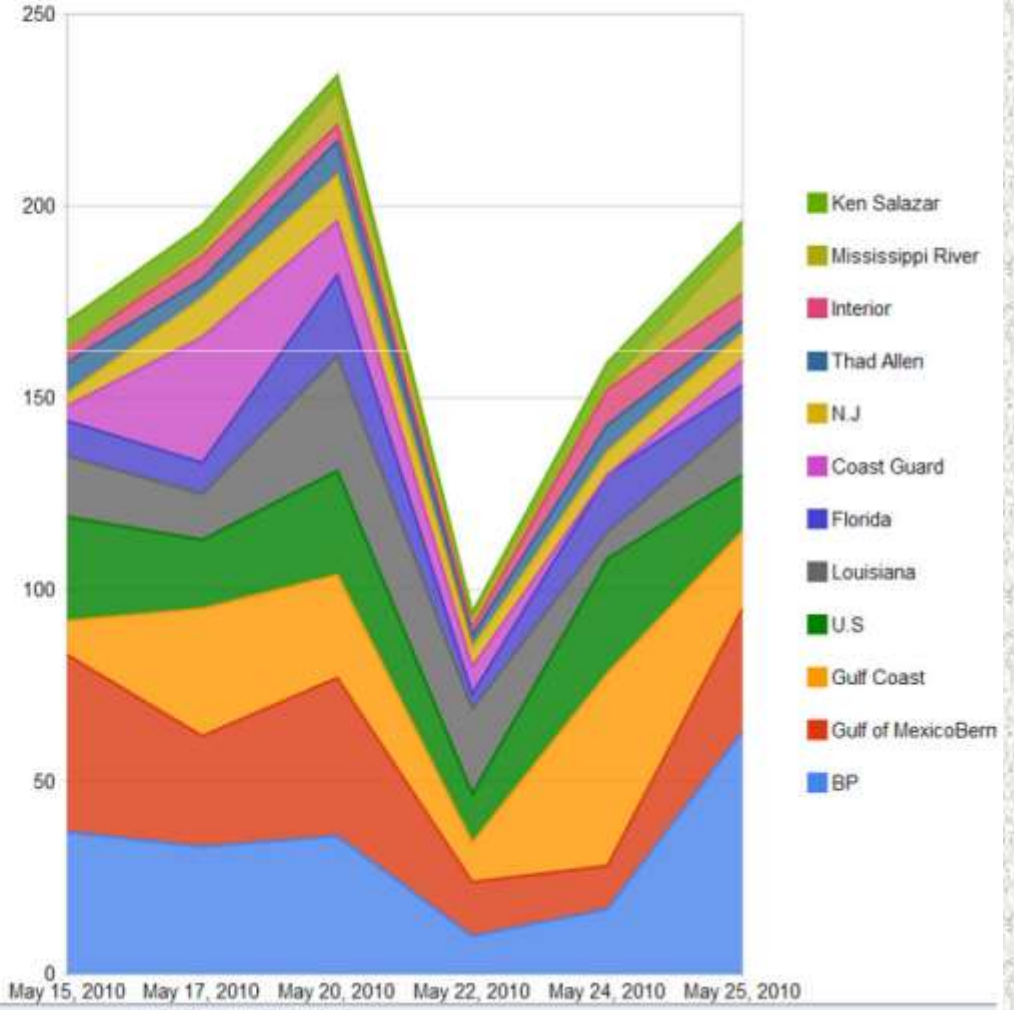
Top federal officials said Sunday that the Gulf of Mexico oil spill is a potential catastrophe and defended the Obama administration's response so far.

Visualizations

Area Chart
TreeMap
Sparkline
Word Cloud

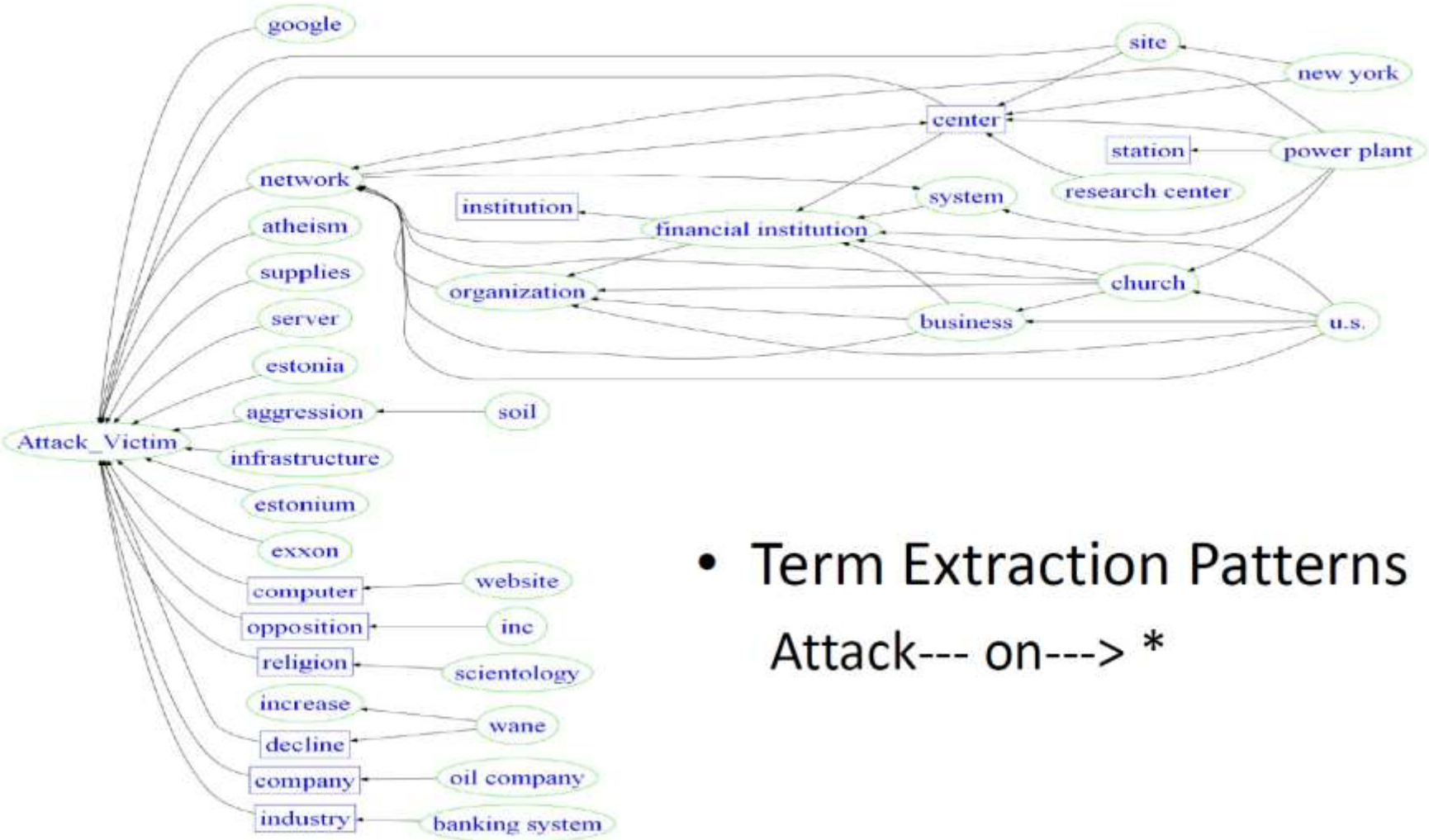
27 urls in topic

http://www.cnn.com/2010/POLITICS/05/02/oil.spill.government/index.html
http://www.cnn.com/2010/POLITICS/05/11/bp.oil.congress.experts/index.html
http://www.cnn.com/2010/US/05/04/gulf.oil.spill.dispersant/index.html
http://www.cnn.com/2010/US/05/15/gulf.oil.spill/index.html
http://www.cnn.com/2010/POLITICS/05/11/gulf.oil.spill.hearing/index.html
http://www.cnn.com/2010/US/05/03/oil.spill.environmental.impacts/index.html
http://www.cnn.com/2010/US/05/13/oil.spill.main/index.html
http://www.cnn.com/2010/US/05/14/gulf.oil.spill/index.html
http://www.cnn.com/2010/US/05/12/oil.spill.main/index.html
http://www.cnn.com/2010/US/05/16/gulf.oil.spill/index.html
http://www.cnn.com/2010/US/05/17/gulf.oil.spill/index.html
http://www.cnn.com/2010/US/05/09/gulf.oil/index.html
http://www.cnn.com/2010/US/05/10/gulf.oil/index.html
http://www.cnn.com/2010/US/05/18/gulf.oil.spill.main/index.html
http://www.cnn.com/2010/US/05/02/louisiana.oil.spill/index.html
http://www.cnn.com/2010/US/05/08/gulf.oil.spill/index.html
http://www.cnn.com/2010/US/05/07/gulf.oil.spill/index.html
http://www.cnn.com/2010/US/05/21/gulf.oil.spill/index.html
http://www.cnn.com/2010/US/05/20/gulf.oil.spill/index.html
http://www.cnn.com/2010/TECH/05/06/crowdsource.gulf.oil/index.html
http://www.cnn.com/2010/US/05/23/gulf.oil.spill/index.html
http://www.cnn.com/2010/US/05/23/oil.spill.response/index.html
http://www.cnn.com/2010/US/05/24/oil.spill.main/index.html
http://www.cnn.com/2010/US/05/03/gulf.oil.spill/index.html
http://www.cnn.com/2010/US/05/06/gulf.oil.spill/index.html
http://www.cnn.com/2010/US/05/25/gulf.oil.spill/index.html
http://www.cnn.com/2010/POLITICS/05/24/oil.spill.government/index.html



Topics Documents Entities

Relationship Extraction



- Term Extraction Patterns

  Attack--- on---> *

CyCast- Cyberattack Forecasting

- R. A. Gandhi, A. Sharma, W. Mahoney, W. Susan, Q. Zhu, P. Laplante, (2010), "The Cultural, Social, Economic, and Political Dimensions of Cyber Attacks," to Appear in the IEEE Technology and Society Magazine.
- A. Sharma, R. A. Gandhi, W. Mahoney, W. Susan, Q. Zhu, (2010), "Building a Social Dimensional Threat Model from Current and Historic Events of Cyber Attacks International Symposium on Secure Computing (SecureCom-10) In conjunction with The Second IEEE International Conference on Privacy, Security, Risk and Trust.
- W. Sousan, Q. Zhu, R.A. Gandhi, W. Mahoney, A. Sharma, (2010), "Using Term Extraction Patterns to Discover Coherent Relationships from Open Source Intelligence," International Symposium on Secure Computing (SecureCom-10) In conjunction with The Second IEEE International Conference on Privacy, Security, Risk and Trust.
- B. Walenz, R.A. Gandhi, W. Mahoney, Q. Zhu, (2010), "Exploring Social Contexts along the Time Dimension: Temporal Analysis of Named Entities," International Symposium on Secure Computing (SecureCom-10) In conjunction with The Second IEEE International Conference on Privacy, Security, Risk and Trust.

In future physical wars there exists the very real possibility of a full blown supporting war in cyberspace by government-backed enemy teams

But in the time of piece there are many opportunities for international collaboration
and many specific research areas for collaborative research that will result in a mutually-assured piece and safety in the cyberspace