Concentrating Correctly on Cybercrime Concentration

Richard Clayton[1] **Tyler Moore**[2] Nicolas Christin[1]

[1] Computer Laboratory, University of Camabridge, UK
[2] Southern Methodist University, Dallas, TX
University of Tulsa, OK (from August 2015)
[3] ECE & CyLab, Carnegie Mellon University, Pittsburgh, PA
tyler-moore@utulsa.edu

Workshop on the Economics of Information Security
Delft, Netherlands
June 23, 2015

McColo: an example of cybercrime concentration

The Washington Post

washingtonpost.com > Technology > Security Fix

Security Fix

Brian Krebs on Computer Security

About This Blog | Archives | Security Fix Live: Web Chats | E-Mail Brian Krebs

Search This Blog

Go

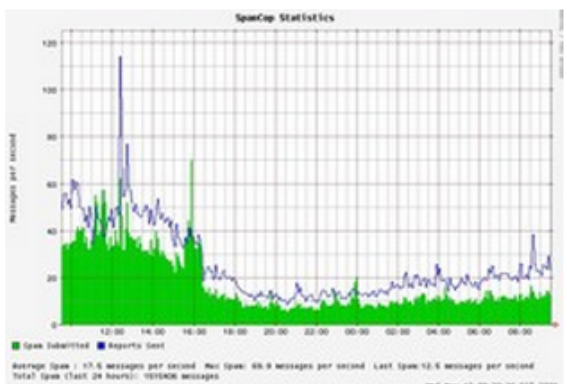
Recent Posts

- Farewell 2009, and The Washington Post
- Hackers exploit Adobe Reader flaw via comic strip syndicate
- Twitter.com hijacked by 'Iranian cyber army'
- Group IDs hotbeds of Conficker worm outbreaks
- Hackers target unpatched Adobe Reader, Acrobat flaw

Entries By Category

Spam Volumes Drop by Two-Thirds After Firm Goes Offline

The volume of junk e-mail sent worldwide plummeted on Tuesday after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity was taken offline. (**Note**: A link to the full story on McColo's demise is available here.)



Experts say the precipitous drop-off in spam comes from Internet providers unplugging **McColo Corp.**, a hosting provider in Northern California that was the home base for machines responsible for coordinating the sending of roughly 75 percent of all spam each day.

In an alert sent out Wednesday morning, e-mail security firm **IronPort** said:

In the afternoon of Tuesday 11/11, IronPort saw a drop of

Our motivation

- Krebs reports that the criminals previously on McColo simply moved onto other services, taking care to not concentrate as much
- Only long-term damage was a loss of valuable email address lists

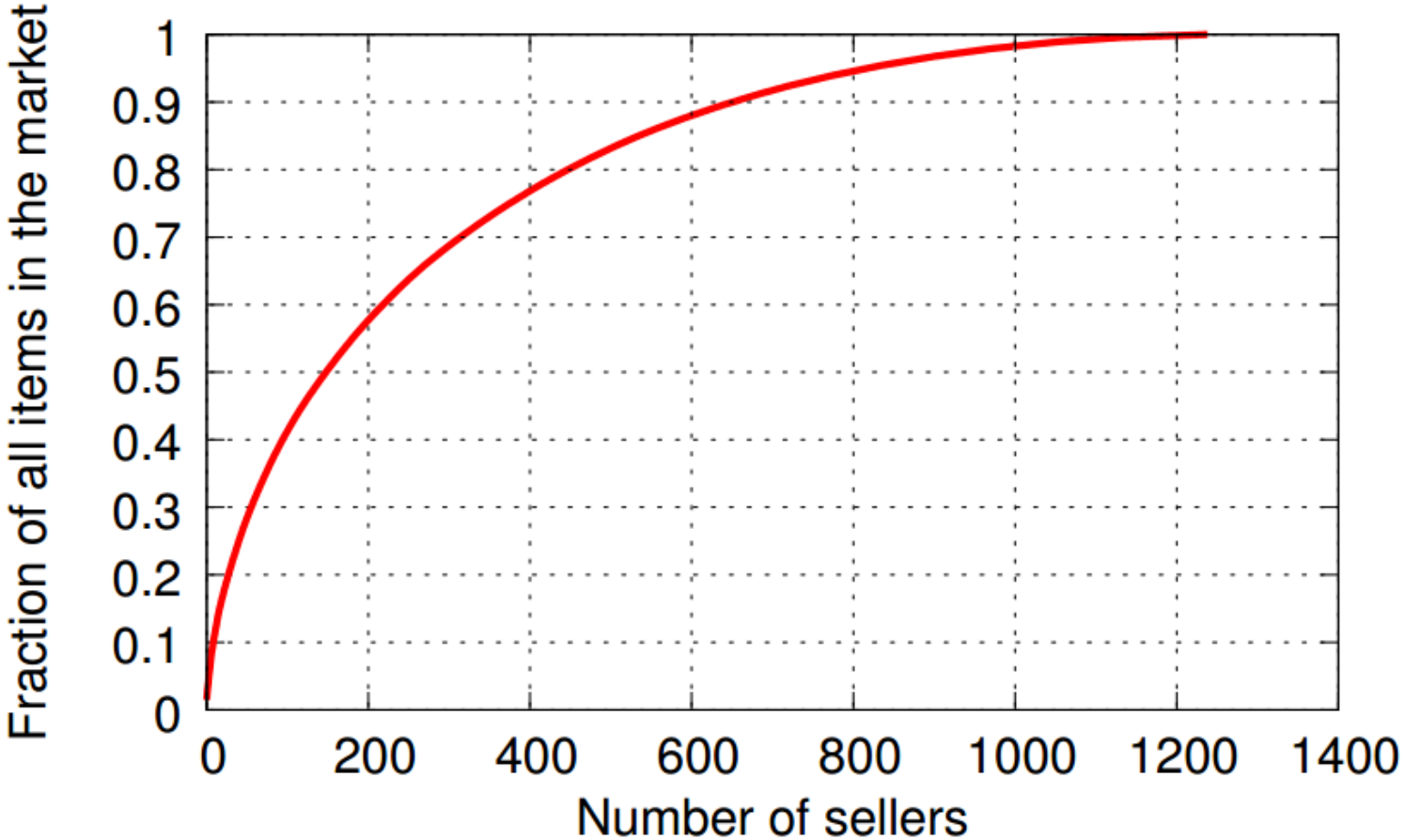
Our motivation

- Krebs reports that the criminals previously on McColo simply moved onto other services, taking care to not concentrate as much
- Only long-term damage was a loss of valuable email address lists
- Motivation
  - Why does concentration emerge so often in cybercrime?
  - How can we tell if the observed concentration is a product of convenience or a structural limitation that is difficult to avoid?
  - Our goal is to articulate why concentration emerges and use this to inform viable intervention strategies

Outline

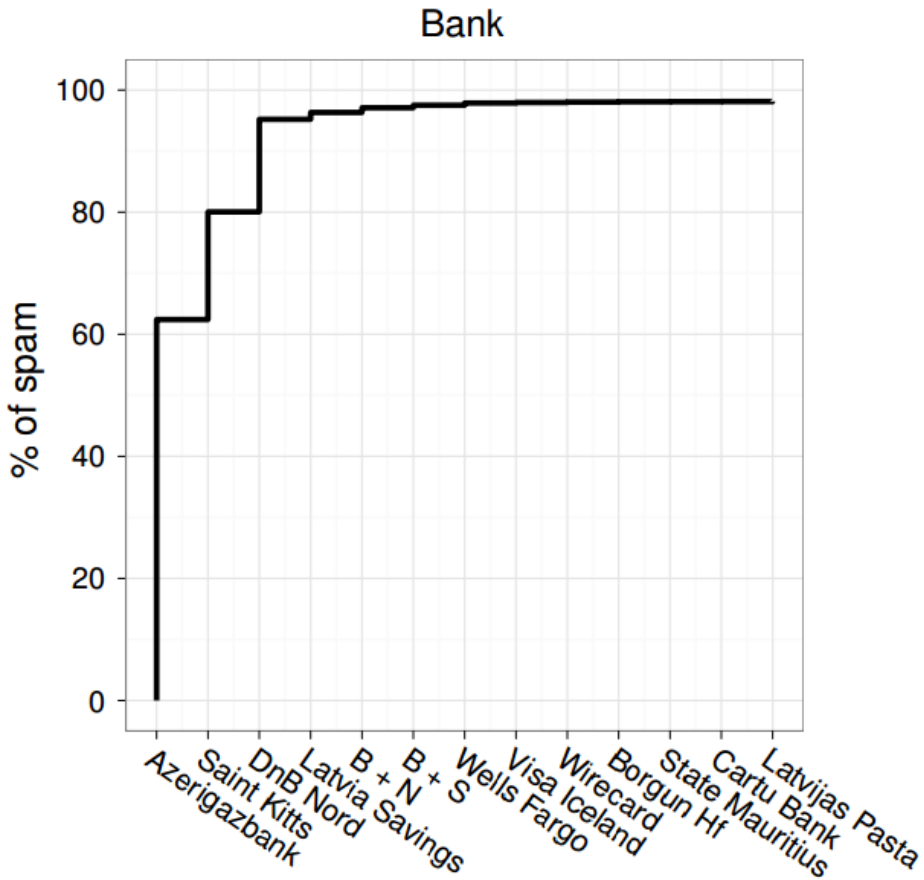
Outline

Concentrations emerge for many types of cybercrime

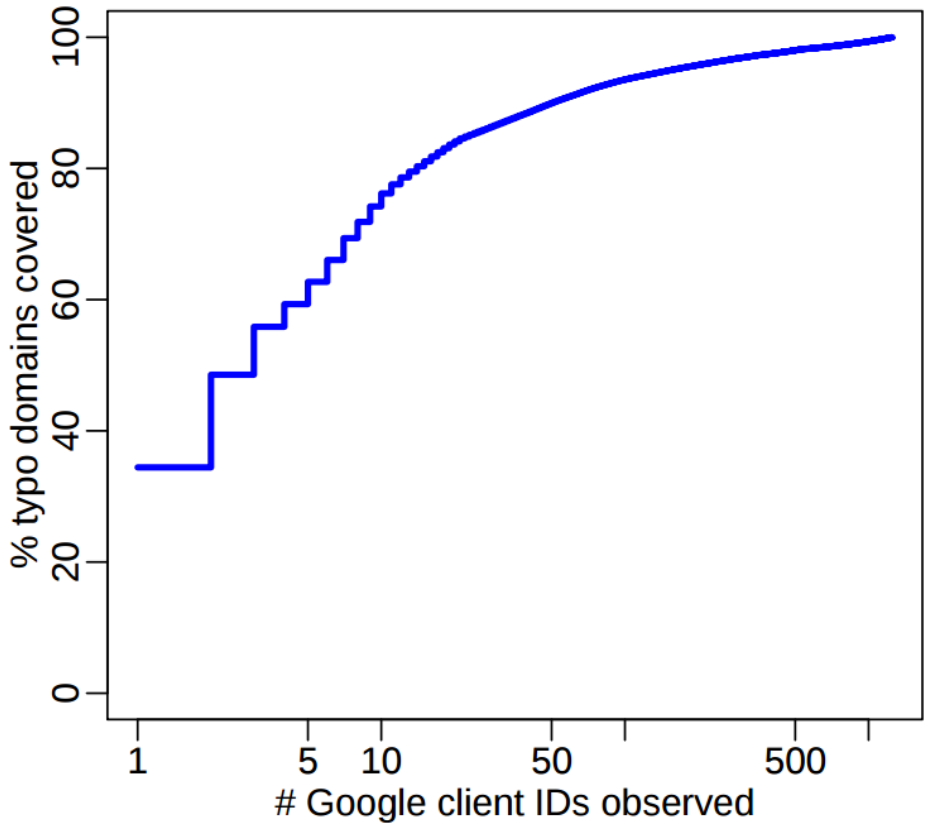


Sellers on anonymous marketplaces
(Christin 2014)

Concentrations emerge for many types of cybercrime



Payments for spamvertised goods
(Levchenko et al. 2011)



Typosquatters
(Moore and Edelman 2010)

Concentrations by cybercrime category

- **Spam-sending botnets:** Van Eeten et al. estimated that 10 ISPs account for 30% of email spam, 50 for over half
- **Counterfeit luxury goods:** Wang et al. found 52 SEO campaigns targeting 16 brands accounting for most activity
- **High-yield investment programs:** Moore et al. found concentration in payment mechanisms, domain registration and reputation sites; Neisius and Clayton identified one company's templates, Gold Coders, accounted for 75% of observed HYIPs

Concentrations by cybercrime category

- **One-click frauds:** Christin et al. identified 8 groups accounting for half of scams over 4 years
- **Fake antivirus:** Stone-Gross et al. reported that a few affiliates make the bulk of profits (only 4 made >$500K)
- **Pharmaceutical inventories:** Leontiadis et al. showed half of surveyed unlicensed pharmacies source inventories from at most 9 production facilities

Concentrations by infrastructure components

- **Payment system intervention:** Levchenko et al. found 95% of payments for spam-advertised goods were handled by 3 banks; after intervention, McCoy et al. presented evidence that moving onto new payment processors is difficult for criminals
- **Domain name intervention:** Liu et al. document shifting by spammers to new CC TLDs and registrars
- **Hosting provider shutdowns:** Following the McColo shutdown, spam fell 50-75% but soon recovered

Outline

Economic explanations for concentration

- **Comparative advantage:** individuals and firms who can most efficiently produce a good tend to specialize and trade with others
  - Online, companies specialize in providing certain services cheaply or by making services attractive to criminals
  - Criminals naturally concentrate at (i) the cheapest place or (ii) the place that tolerates or is slow to react to criminality
- **Network effects:** service becomes more attractive as more people use it
  - Certain types of criminality concentrate in geographic regions (e.g., fraud in West Africa, auction fraud in Eastern Europe, financial malware in Russian-speaking countries)

Economic explanations for concentration

- **Economies of scale:** reduces cost per quantity
  - Scale is everything in online crime: high upfront costs reward attackers who can reduce per-unit costs
- **Barriers to entry:** crimes with high fixed costs can deter entrants after the "winners" who leverage scale and network effects have emerged
  - For many online crimes, barriers appear in the sophistication required to enter and be effective (arms race between attackers and defenders have resulted in the surviving criminals being technically proficient)

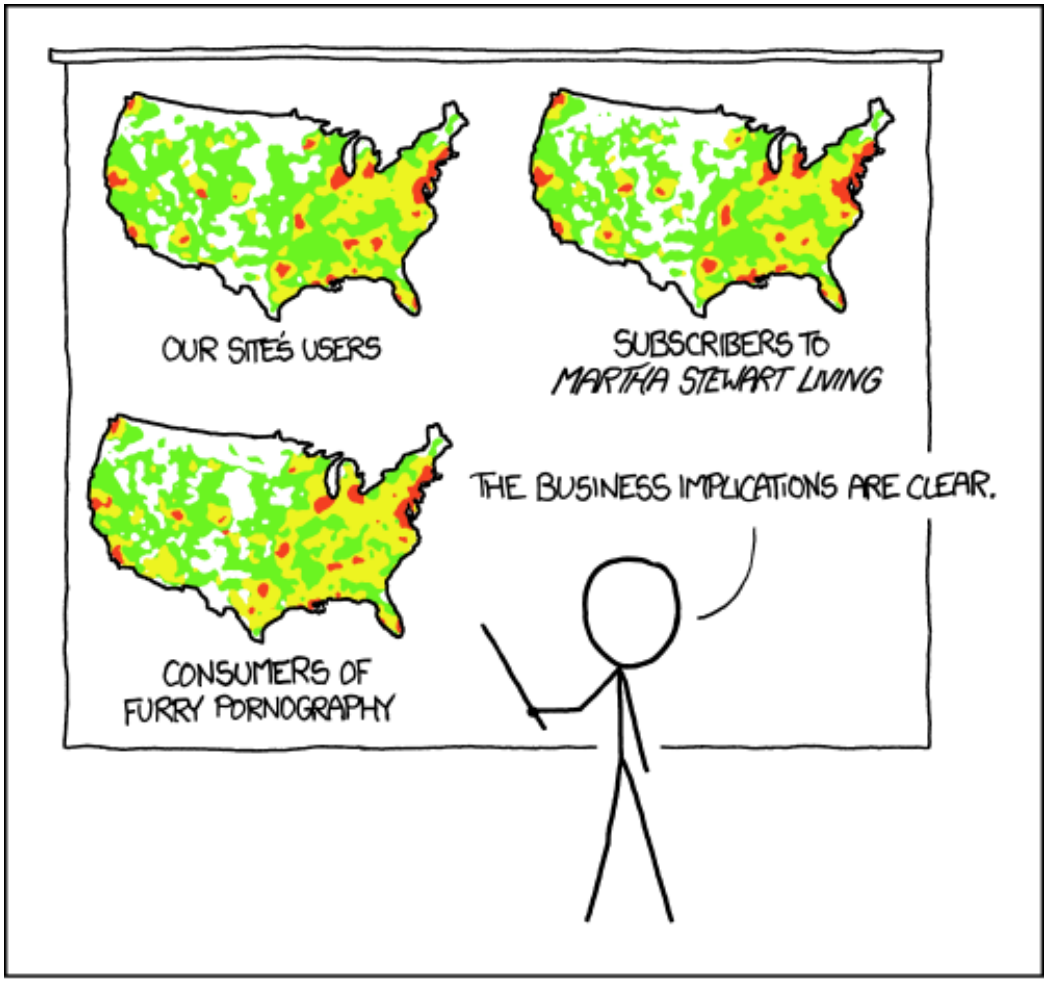
Non-economic explanations for concentration

- **Whack-a-mole**
  - Most infrastructure operators do the right thing and respond to abuse reports (though they may have to gain clue first)
  - Criminals naturally concentrate on platforms that tolerate abuse or are slow to act
- **Copying successful patterns**
  - Success inspires copycats – there is no honor among thieves
  - The corollary is that failure will spur innovation – so the concentration will naturally dissipate following intervention

Measurement artifacts falsely suggesting concentration

- **Measurement bias**
  - Apparent concentrations may arise from hidden characteristics of how the data was collected
  - PhishTank reports 40% of phishing URLs, but 100% of PayPal phish so it appears that criminals overwhelmingly target PayPal
- **Small numbers of participants**
  - When only a handful of criminals operate a scam, concentrations naturally appear
  - In 2007–08, RockPhish gang accounted for 2/3 of phishing spam, so their techniques suggested concentrations for most phishing criminals

Measuring something else altogether



Source: http://www.xkcd.com/1138/

Measurement artifacts falsely suggesting concentration

- **Measuring something else altogether**
  - Concentrations exist everywhere online
  - Finding that some online wickedness is concentrated at the largest ISPs is not surprising
  - Because getting good data to normalize can be very hard, it is tempting to rely on absolute frequency to identify concentration

Reviewing concentration causes in online crime

Category	Perpetrators	Payments	Registrar	Hosting	ISP	Phone	Ad Platform
Spam-sending botnets							
Typosquatting							
HYIPs							
Luxury goods							
Media piracy							
One-click frauds							
Fake A/V							
Unlicensed pharmacies							
Goods sold on anon. mkts.							
Phishing							

Table : Legend of concentration factors: E: Economic, W: Whack-a-mole, C: Copycats, B: Bias, S: Small number of participants.

Reviewing concentration causes in online crime

Category	Perpetrators	Payments	Registrar	Hosting	ISP	Phone	Ad Platform
Spam-sending botnets	E						
Typosquatting	E						
HYIPs	E						
Luxury goods							
Media piracy							
One-click frauds	E						
Fake A/V							
Unlicensed pharmacies							
Goods sold on anon. mkts.	E						
Phishing							

Table : Legend of concentration factors: E: Economic, W: Whack-a-mole, C: Copycats, B: Bias, S: Small number of participants.

Reviewing concentration causes in online crime

Category	Perpetrators	Payments	Registrar	Hosting	ISP	Phone	Ad Platform
Spam-sending botnets	E						
Typosquatting	E C						
HYIPs	E						
Luxury goods							
Media piracy							
One-click frauds	E						
Fake A/V							
Unlicensed pharmacies							
Goods sold on anon. mkts.	E C						
Phishing							

Table : Legend of concentration factors: E: Economic, W: Whack-a-mole, C: Copycats, B: Bias, S: Small number of participants.

Reviewing concentration causes in online crime

Category	Perpetrators	Payments	Registrar	Hosting	ISP	Phone	Ad Platform
Spam-sending botnets	E						
Typosquatting	E C S						
HYIPs	E S						
Luxury goods	S						
Media piracy							
One-click frauds	E S						
Fake A/V	S						
Unlicensed pharmacies	S						
Goods sold on anon. mkts.	E C						
Phishing	S						

Table : Legend of concentration factors: E: Economic, W: Whack-a-mole, C: Copycats, B: Bias, S: Small number of participants.

Reviewing concentration causes in online crime

Category	Perpetrators	Payments	Registrar	Hosting	ISP	Phone	Ad Platform
Spam-sending botnets	E				E		
Typosquatting	E C S		E				
HYIPs	E S						
Luxury goods	S		E	E			
Media piracy							
One-click frauds	E S						
Fake A/V	S			E			
Unlicensed pharmacies	S						
Goods sold on anon. mkts.	E C						
Phishing	S		E	E			

Table : Legend of concentration factors: E: Economic, W: Whack-a-mole, C: Copycats, B: Bias, S: Small number of participants.

Reviewing concentration causes in online crime

Category	Perpetrators	Payments	Registrar	Hosting	ISP	Phone	Ad Platform
Spam-sending botnets	E				E		
Typosquatting	E C S		E W				
HYIPs	E S						
Luxury goods	S		E	E			
Media piracy							
One-click frauds	E S		W				
Fake A/V	S		W	E			
Unlicensed pharmacies	S			W			
Goods sold on anon. mkts.	E C						
Phishing	S		E	E			

Table : Legend of concentration factors: E: Economic, W: Whack-a-mole, C: Copycats, B: Bias, S: Small number of participants.

Reviewing concentration causes in online crime

Category	Perpetrators	Payments	Registrar	Hosting	ISP	Phone	Ad Platform
Spam-sending botnets	E				E		
Typosquatting	E C S		E W				
HYIPs	E S						
Luxury goods	S		E	E			
Media piracy							
One-click frauds	E S		W				
Fake A/V	S		W	E			
Unlicensed pharmacies	S			W			
Goods sold on anon. mkts.	E C						
Phishing	S		E B	E B			

Table : Legend of concentration factors: E: Economic, W: Whack-a-mole, C: Copycats, B: Bias, S: Small number of participants.

Reviewing concentration causes in online crime

Category	Perpetrators	Payments	Registrar	Hosting	ISP	Phone	Ad Platform
Spam-sending botnets	E				E		
Typosquatting	E C S		E W				S
HYIPs	E S	S					
Luxury goods	S		E	E			
Media piracy							
One-click frauds	E S		S W			S	
Fake A/V	S		W	E			
Unlicensed pharmacies	S	S		S W			
Goods sold on anon. mkts.	E C			S			
Phishing	S		E B	E B			

Table : Legend of concentration factors: E: Economic, W: Whack-a-mole, C: Copycats, B: Bias, S: Small number of participants.

Outline

Methodology for proposing interventions

1. Is the concentration real?
2. Identify how a viable intervention would work
3. Predict the criminals' response
4. Assess the practicality of the intervention

Step 1: Is the concentration real?

- Check for measurement bias, small number of participants, or correlation to stakeholder size distribution
- Even when concentration caused by small criminal populations or being located at large intermediaries, law enforcement intervention may make sense
- Must recognize that intervening could enable others to fill the vacuum

Step 2: Identify how a viable intervention would work

- Structural concentrations are better suited to intervention
  - If it is difficult for criminals to receive payments, then we might expect concentrations there that are hard to avoid
  - Counterfeit pharmaceutical suppliers have high fixed costs and require access to equipment that is hard to obtain
- 'Convenience' concentrations have short term impact
  - If many criminals are using the same registrar because of a low price for domains, intervening won't make much difference given so many substitute providers
  - Dispersing such activity can make law enforcement's job harder

Step 3 and 4

- Step 3: Predict the criminals' response
  - Successful criminals don't give up easily
  - Anticipate what the next move is, and determine if operation costs will rise sufficiently to justify intervention

Step 3 and 4

- Step 3: Predict the criminals' response
  - Successful criminals don't give up easily
  - Anticipate what the next move is, and determine if operation costs will rise sufficiently to justify intervention
- Step 4: Assess the practicality of the intervention
  - Just because law enforcement can disrupt a crime doesn't mean that they will want to: crime must be sufficiently important
  - Just because an intermediary is uniquely capable of disrupting criminal activity doesn't mean they will be willing to cooperate
  - Evaluate incentives of defenders
    - Where law enforcement personnel are promoted by numbers of cases solved or arrests made, shutting down repeated instances of a cybercrime can be rewarded more than disrupting an intermediary once

Outline

Concluding remarks

- Concentration appears to emerge frequently in cybercrime
- We have reviewed a range of economic and non-economic explanations for why it emerges
- We have proposed a methodology for gauging whether prospective interventions are likely to be effective over the long-term
- Web: `http://lyle.smu.edu/~tylerm/`,
  Email: `tyler-moore@utulsa.edu`