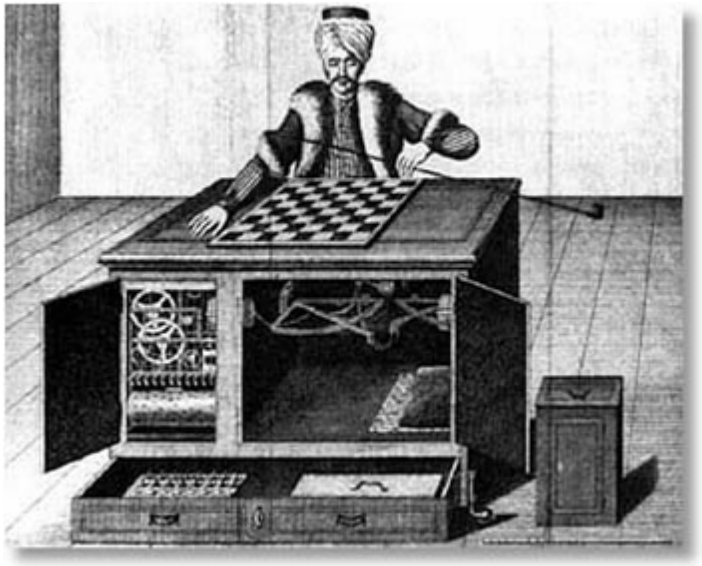
# Analysis of eCrime in Crowd-sourced Labor Markets



freelancer.com

**Vaibhav Garg**, Chris Kanich, and L. Jean Camp

# Why eCrime?

- Kanich et al., Spamalytics: An Empirical Analysis of Spam Marketing Conversion.
  Pharmaceutical Spam = $ 3.5 M
- Moore and Clayton. An Empirical Analysis of the Current State of Phishing Attack and Defence.
  Phishing = $ 178.1 M
- Stone-Gross et al., The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns.
  Fake Antivirus = $ 130 M

# eCrime Solutions

- Deterrence Theory
  - Regulatory
    - Penalties ++
    - Prosecution ++
    - Graduated Response/SOPA/PIPA/ACTA
  - Technical
    - CAPTCHAs
    - IP Filtering
    - Virtual Machine/Fake Bots

# eCrime: A Limited Understanding

- Why do individuals choose to engender profits through eCrime rather than by legal enterprise?

# eCrime: A Limited Understanding

- Why do individuals choose to engender profits through eCrime than by legal enterprise?
- When profits are not pertinent, what (socio-economic) factors facilitate engagement in eCrime?


# eCrime: A Limited Understanding

- Why do individuals choose to engender profits through eCrime than by legal enterprise?
- When profits are not pertinent, what (socio-economic) factors facilitate engagement in eCrime?
- Why are individuals in certain countries more susceptible to voluntary participation in eCrime than other? (e.g. Phishing)

# eCrime: A Limited Understanding

- Why do individuals choose to engender profits through eCrime than by legal enterprise?
- When profits are not pertinent, what (socio-economic) factors facilitate engagement in eCrime?
- Why are individuals in certain countries more susceptible to voluntary participation in eCrime than other? (e.g. Phishing)
- Why are systems in certain countries more susceptible to involuntary engagement in eCrime than others? (e.g. Botnets)

# eCrime: A Limited Understanding

- Why do individuals choose to engender profits through eCrime th
- When pro cio-economic) factors fac
- Why are i more susceptibl Crime than other? (e.
- Why are s e susceptible to involun n others? (e.g. Botnets)
- How do legitimate enterprise and eCrime impact each other?

# eCrime: A Limited Understanding

- Why do individuals choose to engender profits through eCrime than by legal enterprise?
- When profits are not pertinent, what (socio-economic) factors facilitate engagement in eCrime?
- Why are individuals in certain countries more susceptible to voluntary participation in eCrime than other? (e.g. Phishing)
- Why are systems in certain countries more susceptible to involuntary engagement in eCrime than others? (e.g. Botnets)
- How do legitimate enterprise and eCrime impact each other?

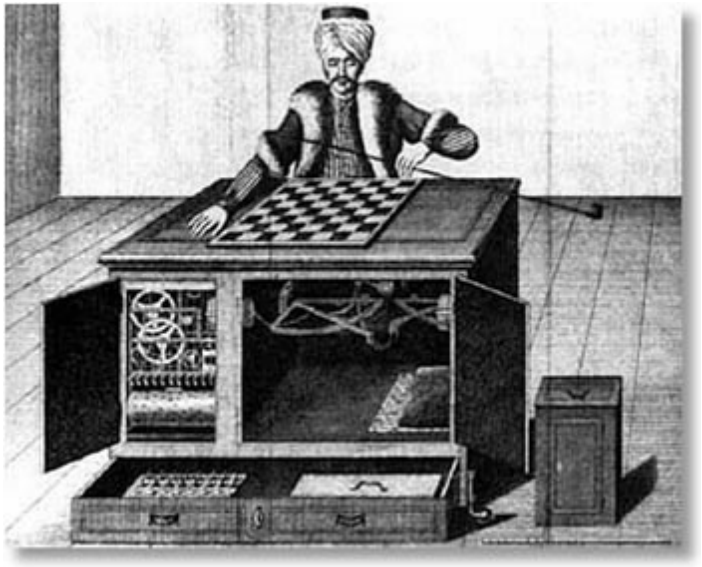
# Smuggling Theory of eCrime

- eCrime
  - Social welfare increasing
  - Prohibitive tariff
  - Suppresses legal enterprise


- Solution: Reduce the costs for legal enterprise!
- Garg et al., Organized Digital Crime: A Smuggling Theory Approach.

amazon mechanical turk™

Artificial Artificial Intelligence



- Transcription
- Translation
- Etc.
- Ipeirotis, Demographics of mechanical turk.
- Ross et al., Who are the crowdworkers?: shifting demographics in mechanical turk.


- 44.6% jobs not legitimate
- Search engine optimization
- Spam
- CAPTCHAs
- Social network links
- Etc.
- Motoyama et al., Dirty jobs : The role of freelance labor in web service abuse.

# Macro-level Model

- Affordability
  - GDP per capita
  - GDP per capita by PPP
- Accessibility
  - Higher quality broadband
  - Reliable access
  - Urban population

# Macro-level Model

- Affordability
- Accessibility
- Population
  - Total Population
  - Number of Internet Users
- Security
  - Secure Internet Servers (SIS)
  - SIS by population

# Macro-level Model

- Affordability
- Accessibility
- Population
- Security
- English
- Legal Framework
  - Alleviates supply not demand
  - Impact of corruption
  - Deterrence and displacement

# Future Work

- High participation vs. Low participation
- Theories of Crime Offline
- Longitudinal Analysis
- Predictive Models
- Other activities, e.g. botnets.

# Summary

- Macro-level analyses
- Limited impact of deterrence
- Higher costs of legitimate enterprise
- Public policy implications
- Private enterprise implications