A Local Mean Field Analysis of Security Investments in Networks

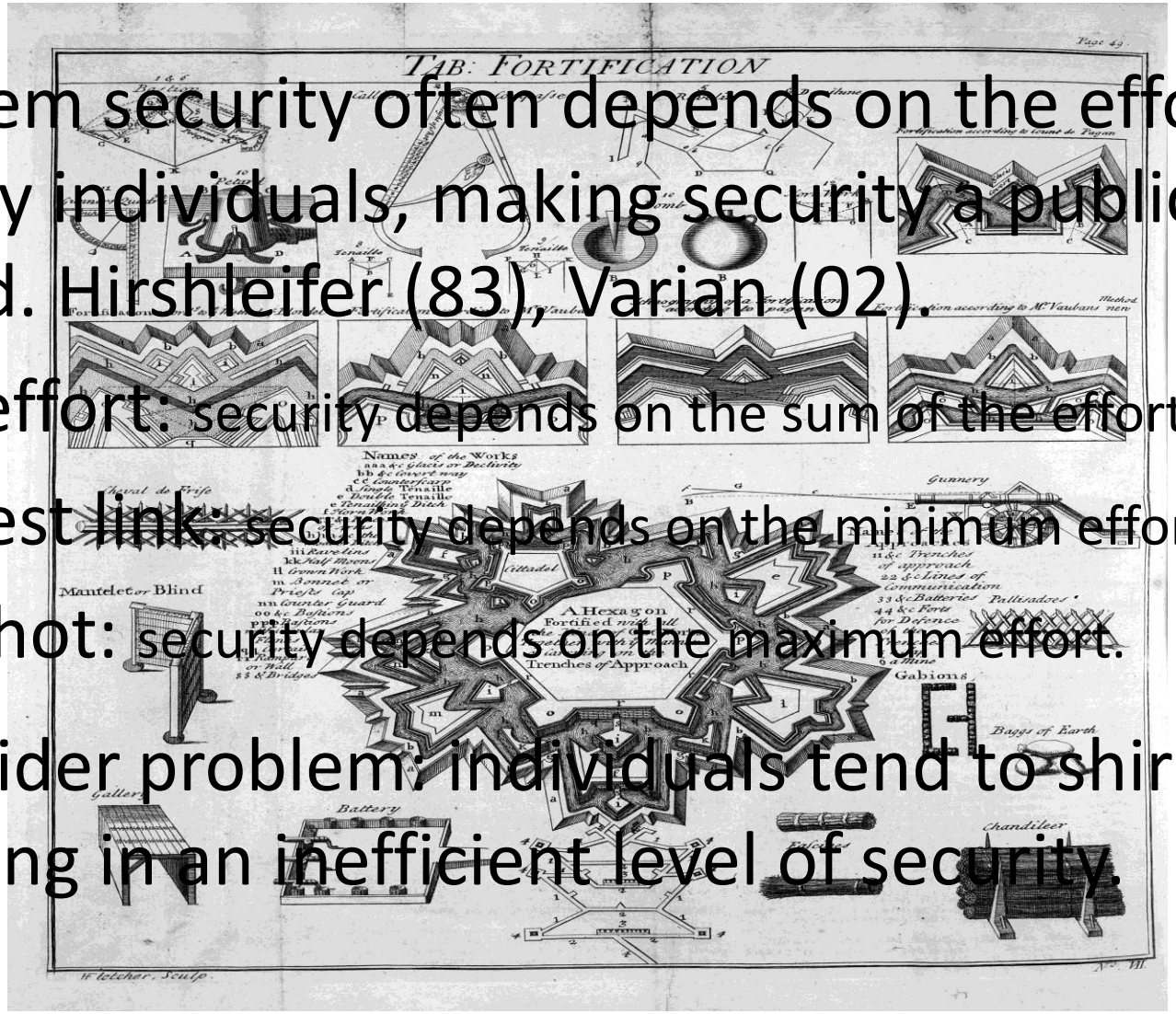
Marc Lelarge (INRIA-ENS)

Jean Bolot (SPRINT)

NetEcon 2008.

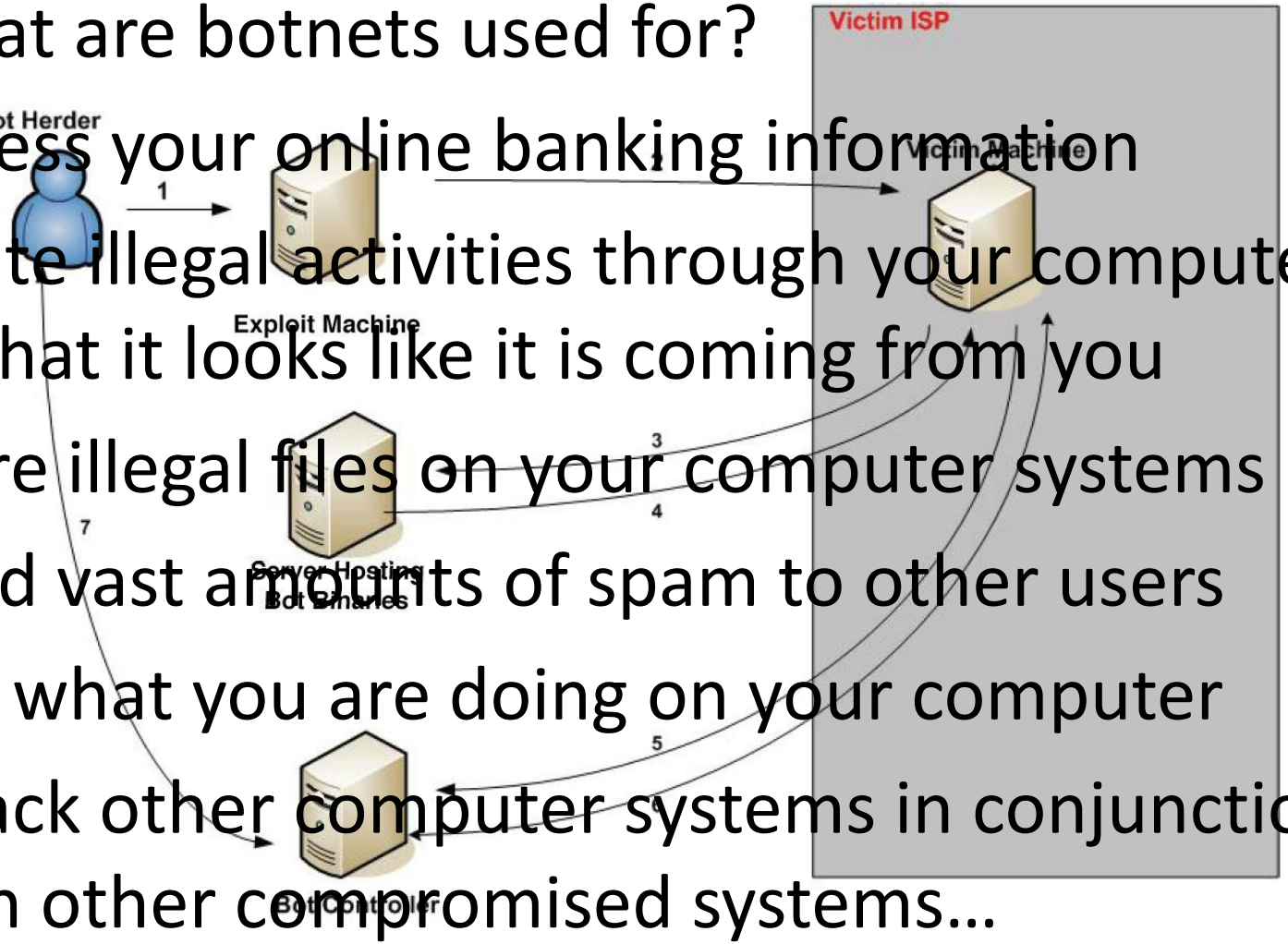
Investments in Network Security

- System security often depends on the effort of many individuals, making security a public good. Hirshleifer (83), Varian (02).
- Total effort: security depends on the sum of the efforts.
- Weakest link: security depends on the minimum effort.
- Best shot: security depends on the maximum effort.
- Free-rider problem: individuals tend to shirk, resulting in an inefficient level of security.



Bot Networks

- What are botnets used for?
- Al
- so
- re
- Access your online banking information
- Route illegal activities through your computer so that it looks like it is coming from you
- Store illegal files on your computer systems
- Send vast amounts of spam to other users
- See what you are doing on your computer
- Attack other computer systems in conjunction with other compromised systems…



An example: Storm Botnet

- The Storm Worm began infecting thousands of (mostly private) computers on Friday, January 19, 2007, using an e-mail message with a subject line about a recent weather disaster, "230 dead as storm batters Europe".
- 5,000 to 6,000 computers are dedicated to propagating the spread of the worm through the use of e-mails with infected attachments.
- The compromised machine becomes merged into a botnet that acts in a similar way to a peer-to-peer network, with no centralized control.
- On 7 September 2007, estimates of the size of the Storm botnet ranged from 1 to 10 million computers.

Source F-Secure

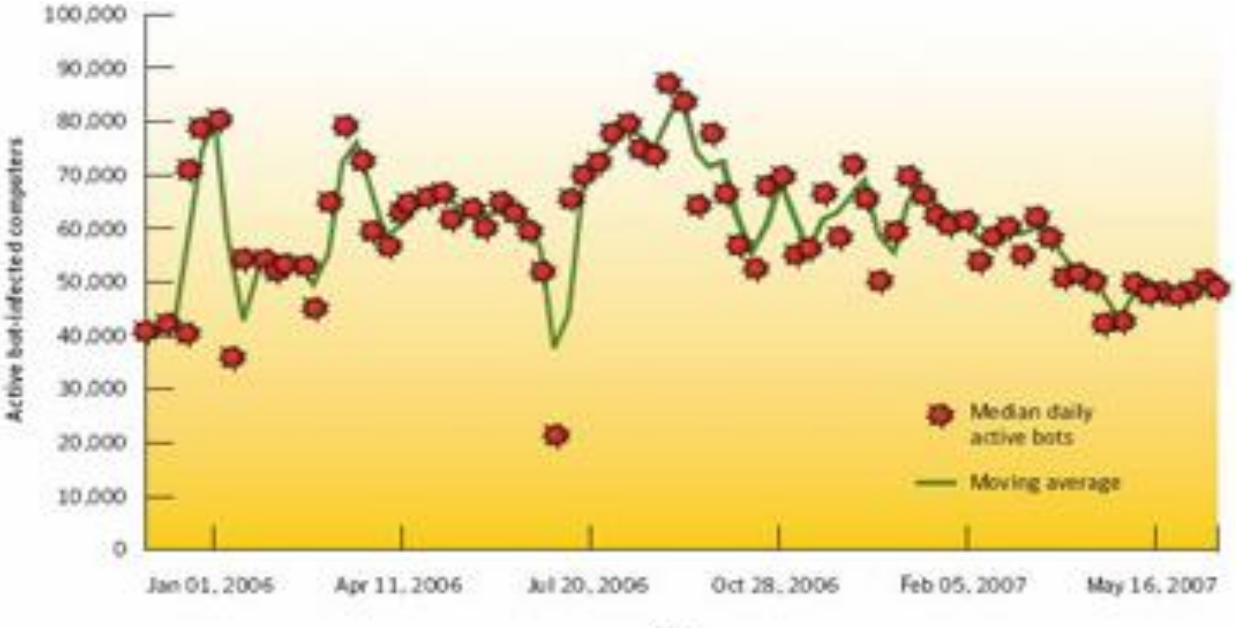
Symantec Internet Security Threat Report

"Between July 1 and December 31, 2007, Symantec observed an average of 61,940 active bot-infected computers per day, a 17 percent increase from the previous reporting period.

An active bot-infected computer is one that carries out an average of at least one attack per day. (...)

Symantec also observed 5,060,187 distinct bot-infected computers during this period, a one percent increase from the first six months of 2007.

A distinct bot-infected computer is a distinct computer that was active at least once during the period."



Motivation

Belief: in 2003, the President's National Strategy to Secure Cyberspace stated that government action is required where "market failures result in under-investment in cybersecurity“.

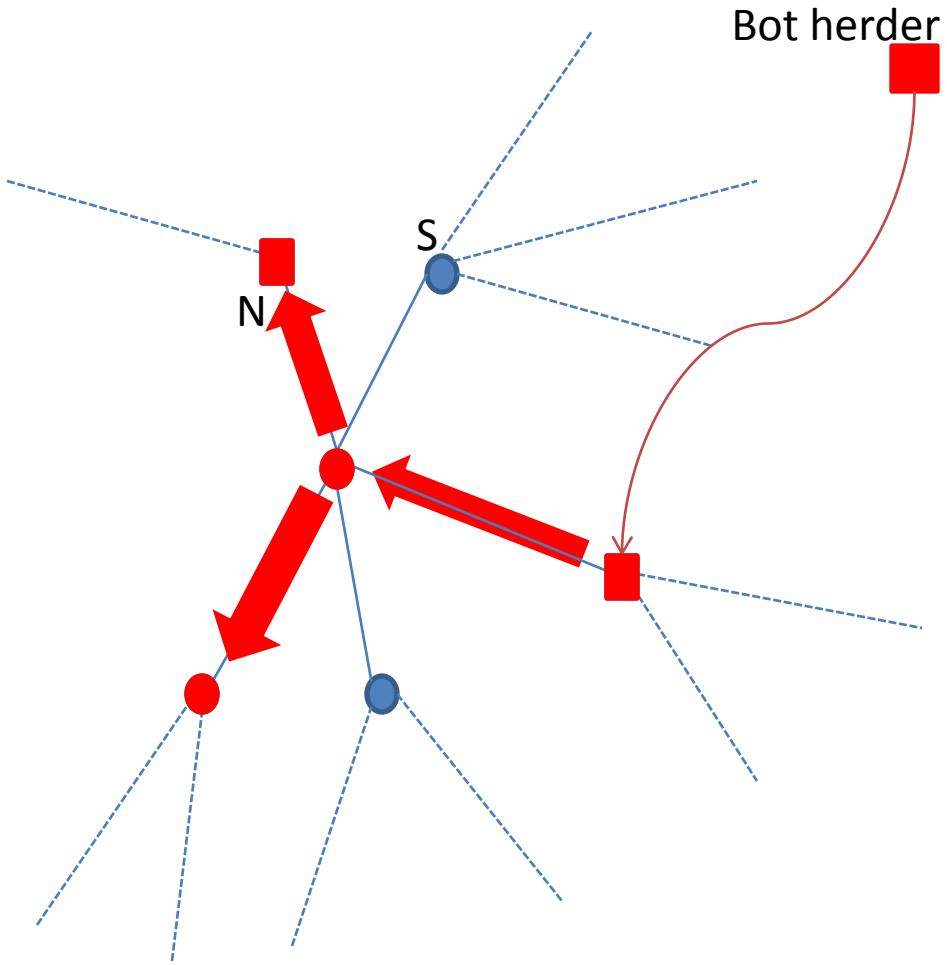
- No appropriate model (restricted to 2 players).
- Our contributions:
  - a micro-model which explains network externalities and scales to the Internet.
  - we are able to compute the Price of anarchy but it is not enough…
  - we show that security is an economic problem and requires proper incentives for technology to be deployed.

Economic Model for the agents

- Each agent faces a potential loss ℓ.
- Investment in security has a fixed cost c and reduces the probability of loss.
- Binary choice:
  - in state N, the probability of loss is p^N.
  - in state S, the probability of loss is $p^S < p^N$.
- Optimal strategy is S if

$$c < \left(p^N - p^S\right) \ell$$

Epidemic Model



- Bot herder directly infects an agent N with prob. p.
- Each neighbor is contaminated with prob. q if in S or $q^+ \geq q$ if in N.

A self-referential model

- The decision for an agent to invest (S) or not (N) in self-protection depends on the probabilities p^N and p^S …
- … but the computation of these probabilities with the epidemic model depends on the decision of each agent.
- Pb. of information available to the agent: we assume that the perceived probabilities are the averaged (over the population) probabilities given the state S/N.

Epidemic risks on a random network

- Underlying graph is a sparse random graph (specified by its degree distribution).
- γ is the fraction of the population investing in self-protection (S).
- p^N / p^S is the probability of loss for an agent not investing/ investing in self-protection.
- Extension of Interdependent Security

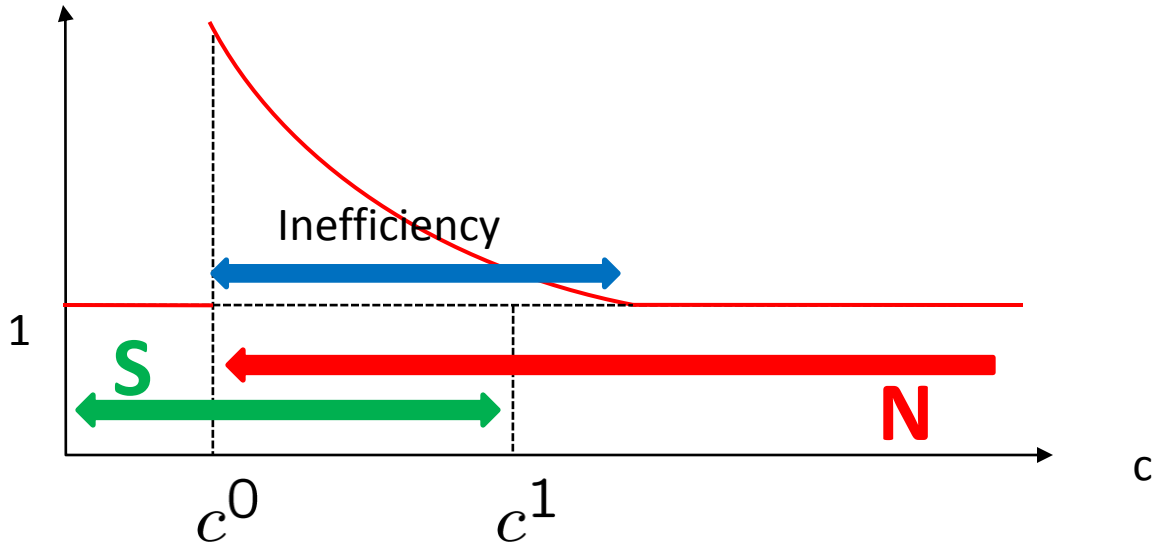
  (2 players) by Kunreuther & Heal (03).

Results

- Strong protection: contagion is possible only if agent is in state N.
  - An agent in state S creates positive externalities: as γ increases, the incentive to invest in security decreases. Free rider problem.
- Weak protection: contagion does not depend on the state N/S.
  - Two Nash equilibria involving everyone or no one investing in security. Coordination problem.

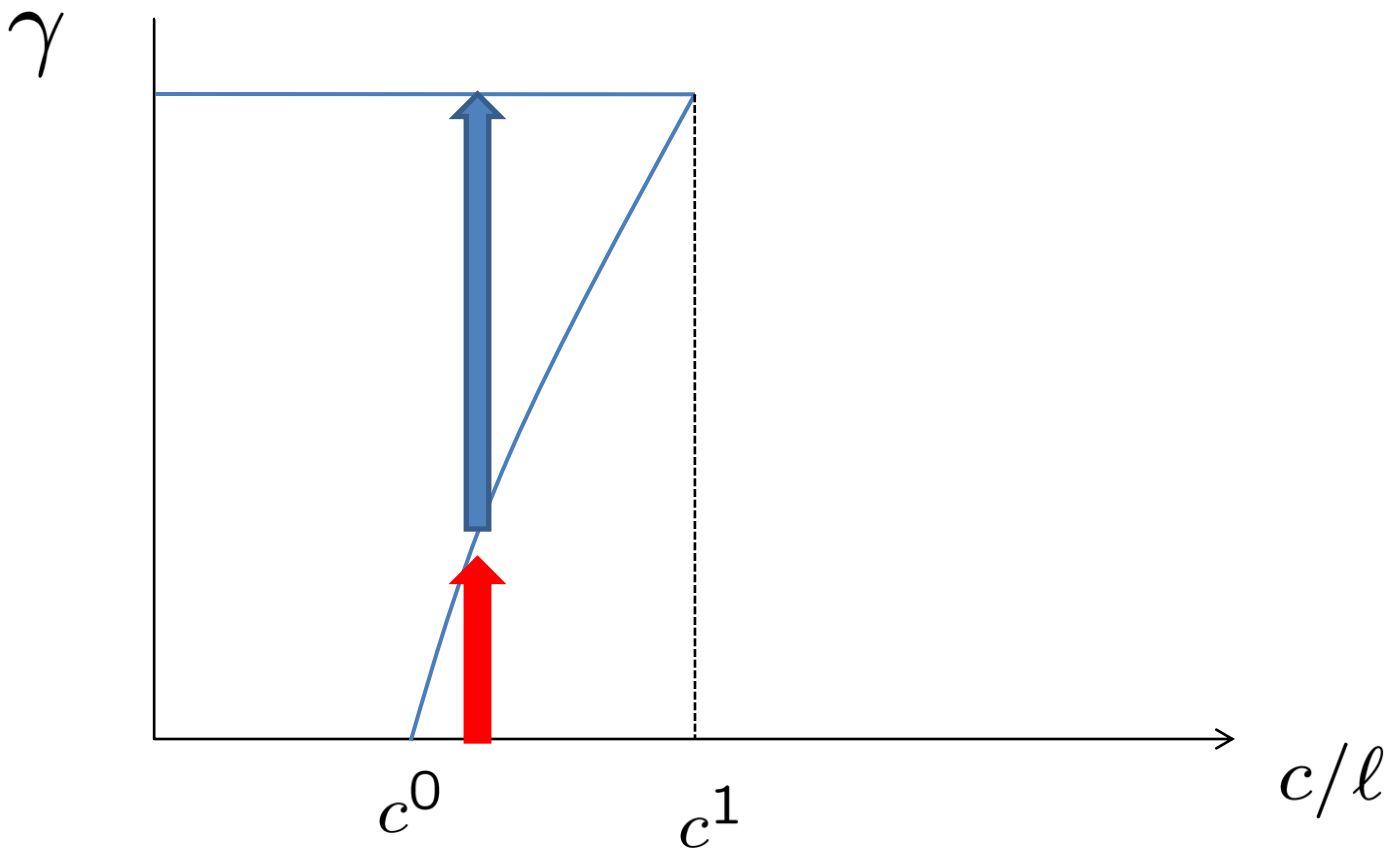
Price of Anarchy

- The price of anarchy is the ratio of the largest (among all equilibria) cost incurred to the population divided by the optimal cost.
- In the case of weak protection:



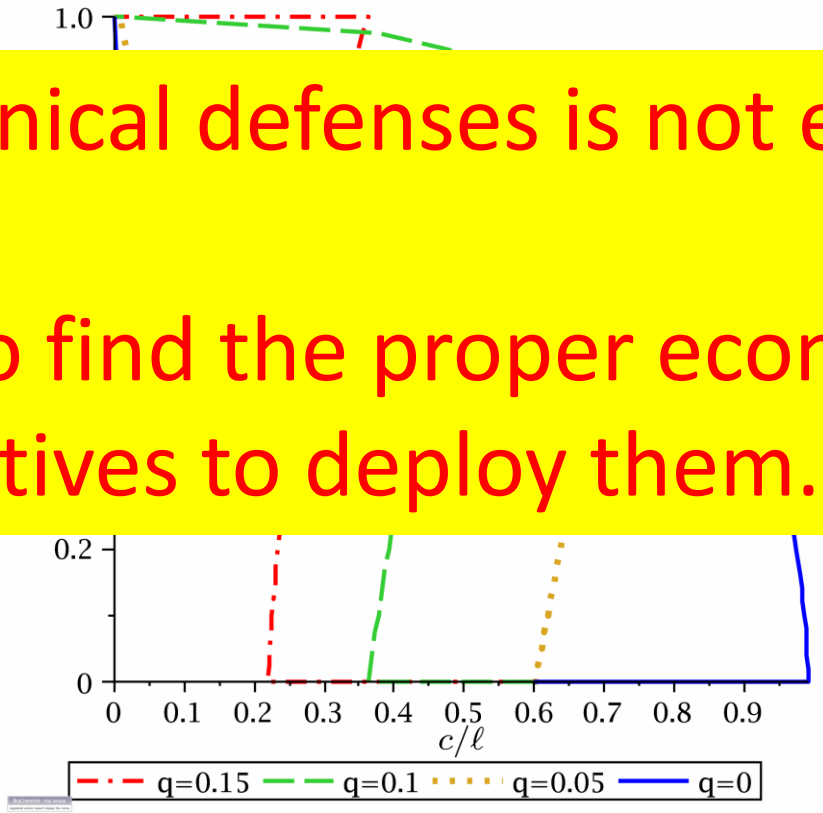
Tipping phenomenon

- Fraction of the population needed to switch?



Adoption vs. quality of protection

- Fraction of population investing in security for various probabilities of contagion in state S.



Improving technical defenses is not enough!

We need to find the proper economic incentives to deploy them.

Conclusions

- Local Mean Field model for epidemic risks on random networks with strategic players.
- Rigorous solution capturing network externalities arising in security problem: free rider problem / coordination game.
- Towards solution for this market failure:

Cyber-insurance is an incentive if moral hazard problem is taken into account (2 players game: INFOCOM'08, multi-players game: WEIS'08).

Thank you!