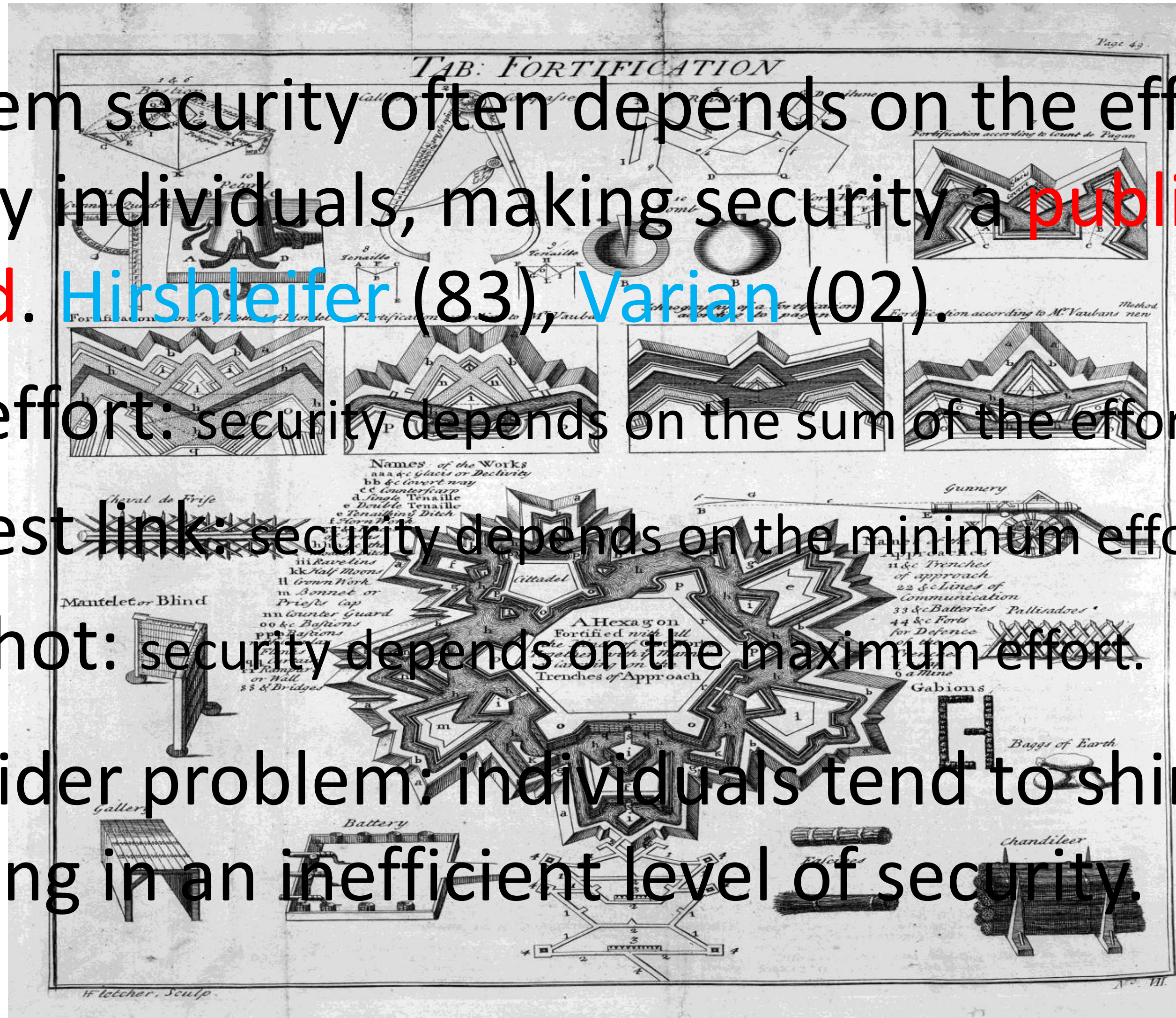
Economics of Malware: Epidemic Risk Model, Network Externalities and Incentives.

Marc Lelarge (INRIA-ENS)

WEIS, University College London, June 2009.

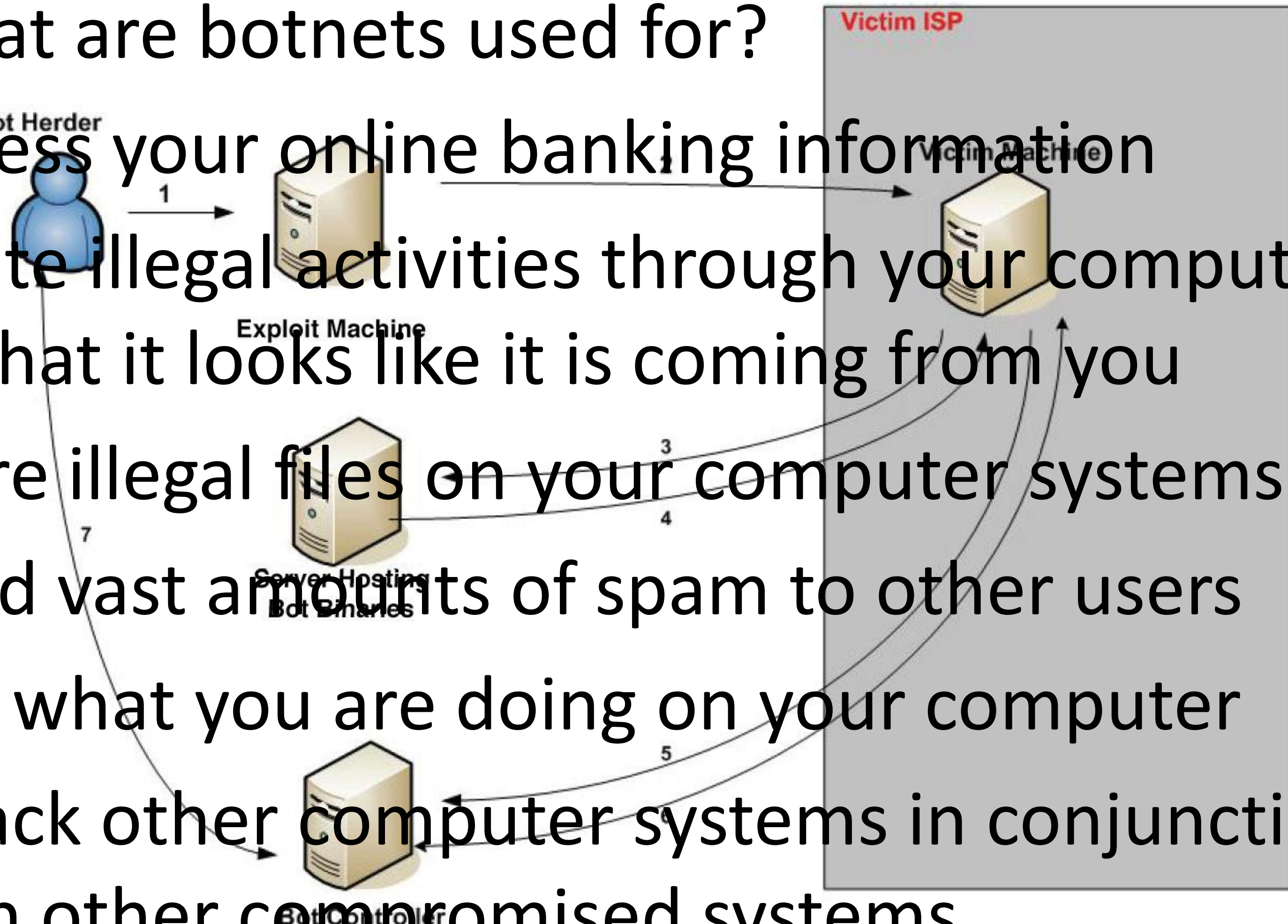
Investments in Network Security



- 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

- A l so re
- What are botnets used for?
- 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

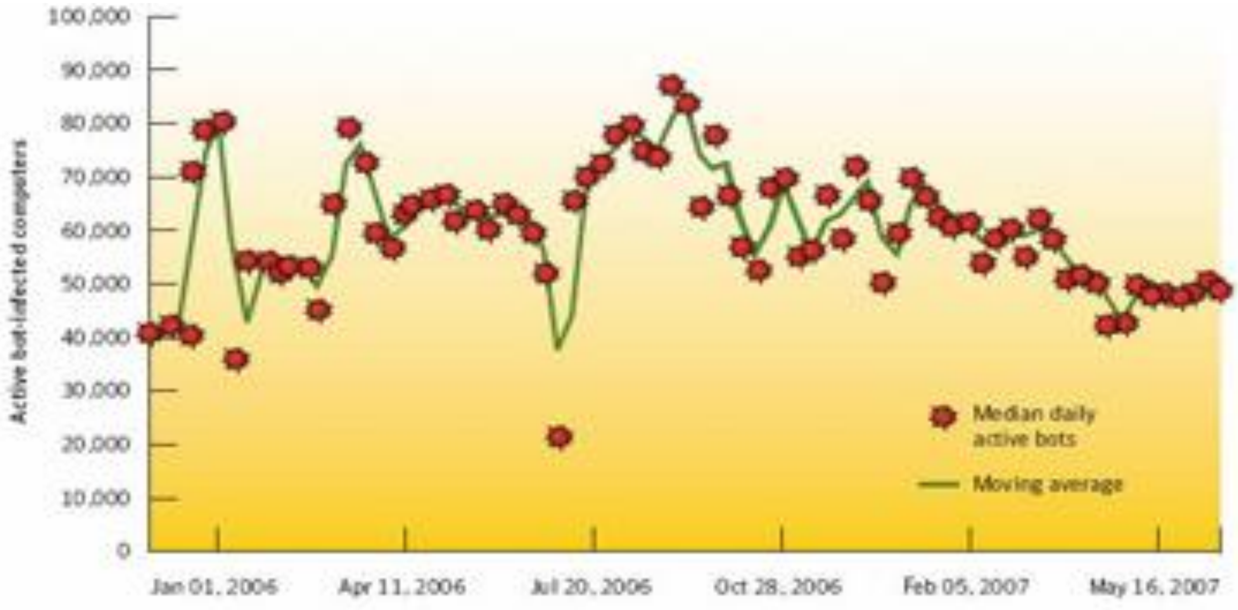
Symantec Internet Security Threat Report

"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."



Contribution

(1) Micro model
- Large population
- Parameters of the epidemic depend on the strategic behavior of agents.

(2) Fulfilled expectation equilibrium with two types of network externalities: private and public.

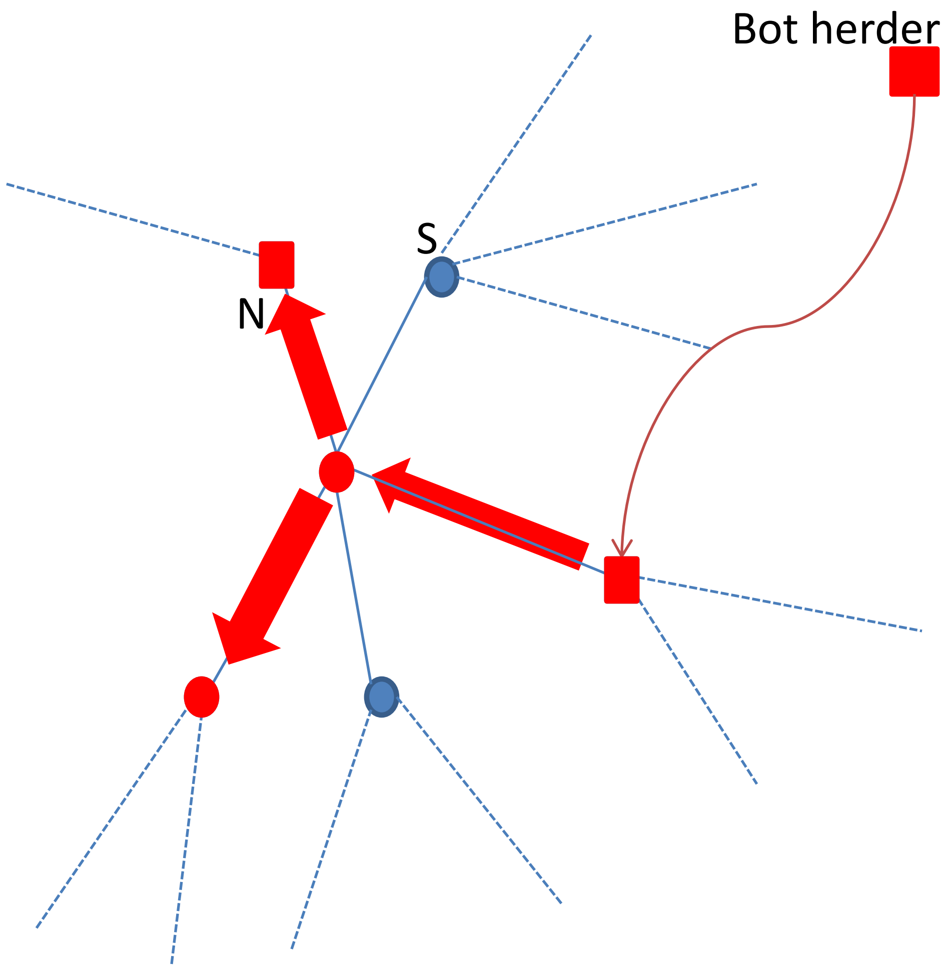
(3) Macro analysis of the model: tipping phenomenon, free-rider problem, interaction with security supplier.

(1) 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

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

(1) 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.

(1) Connecting the 2 models

- Epidemic model
  - Random graph with fixed degree distribution
  - p probability of being directly attacked if in state N
  - $q^+ \geq q$ probabilities of contagion

  Output: $p^N(\gamma) \geq p^S(\gamma)$ probabilities of loss when a fraction γ of the population is in state S.
- Economic model
  - Fixed cost c, type of agent i: ℓ_i
  - Strategic choice: $c < (p^N(\gamma) - p^S(\gamma))\ell_i$

(2) Information available to the agents

- 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.
- Expected fraction of agents investing in security: γ^e. Each agent is able to compute $p^N(\gamma^e)$ and $p^S(\gamma^e)$.

(2) Fulfilled expectations equilibrium

- Concept introduced by Katz & Shapiro (85)
- Willingness to pay for the agent of type ℓ_i :

$$(p^N(\gamma^e) - p^S(\gamma^e))\ell_i$$

multiplicative specification of network externalities as in Economides & Himmelberg (95).

- Willingness to pay for the 'last' agent:

$$d(\gamma, \gamma^e) = h(\gamma^e)F^{-1}(1-\gamma)$$

(2) Fulfilled expectations equilibrium

- In equilibrium, expectation are fulfilled:

$$\gamma = \gamma^e$$

- The fulfilled expectations demand is:

$$d(\gamma) = h(\gamma)F^{-1}(1-\gamma)$$

- Extension of Interdependent Security

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

(3) Price of Anarchy

- The social welfare function:

$$W(\gamma) = \boxed{g(\gamma)\int_\gamma^1 F^{-1}(1-u)du} + \boxed{(g(\gamma)+h(\gamma))\int_0^\gamma F^{-1}(1-u)du} - c\gamma,$$

where F is the c.d.f of types and:

$$\boxed{h(\gamma) = p^N(\gamma) - p^S(\gamma)} \quad \text{Private externalities}$$

$$\boxed{g(\gamma) = p^N(0) - p^N(\gamma).} \quad \text{Public externalities}$$

- Corollary: Because of the public and private externalities, agent under-invest in security (in all cases).

(3) Network externalities function

- For Erdös-Rényi random graphs with asymptotic mean degree λ.
- The network externalities function h is given by:

$$p^N(\gamma) - p^S(\gamma) = \exp(-\lambda q x) - (1-p)\exp(-\lambda q^+ x)$$

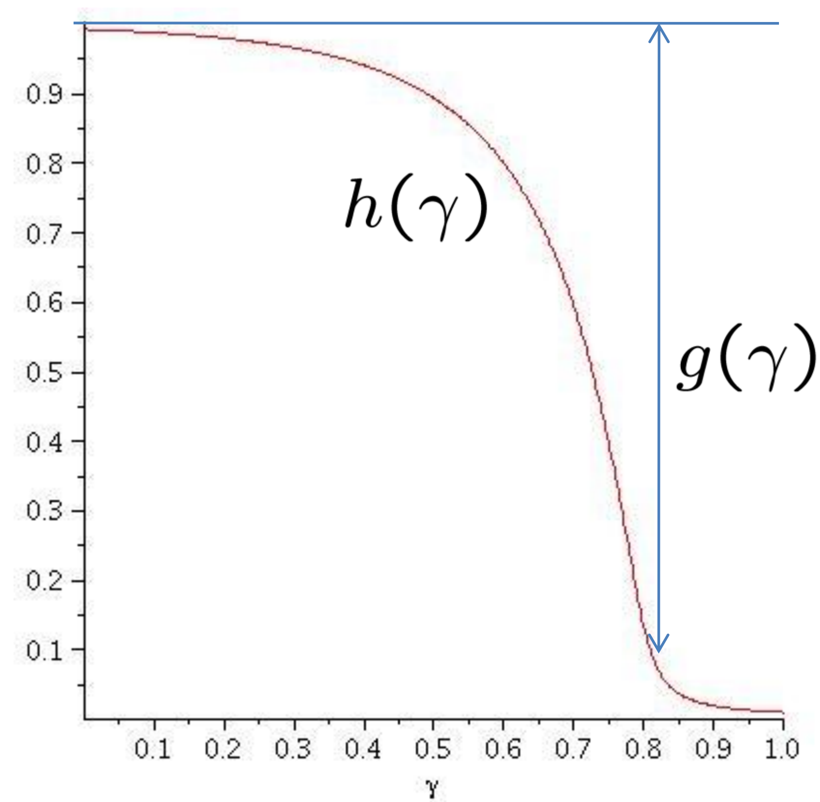
where x is the unique solution of:

$$x = 1 - \gamma \exp(-\lambda q x) - (1-\gamma)(1-p)\exp(-\lambda q^+ x)$$

M.Lelarge, J. Bolot, (SIGMETRICS 08)

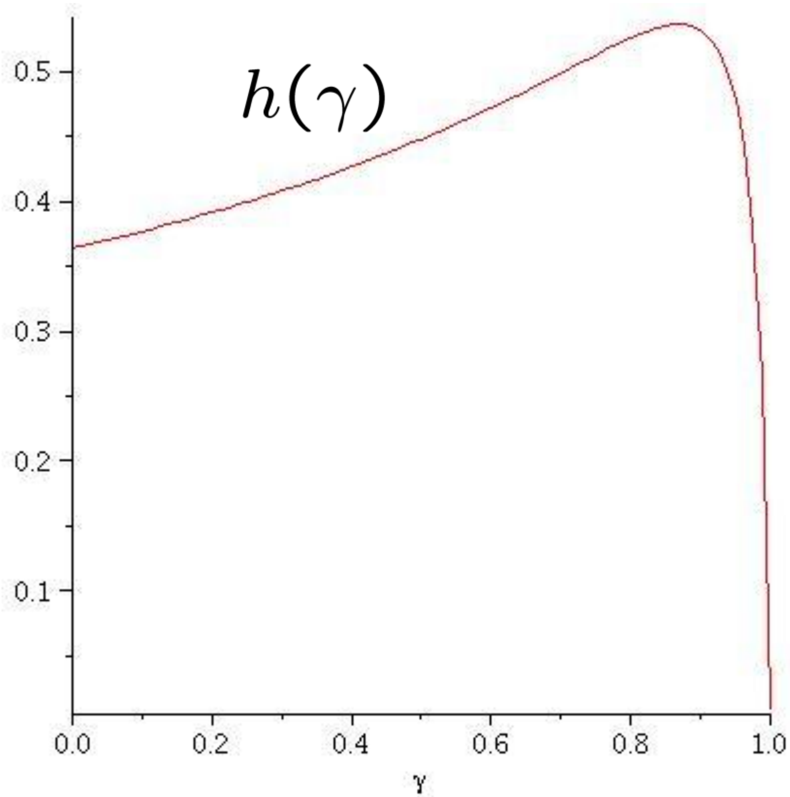
(3) Strong protection

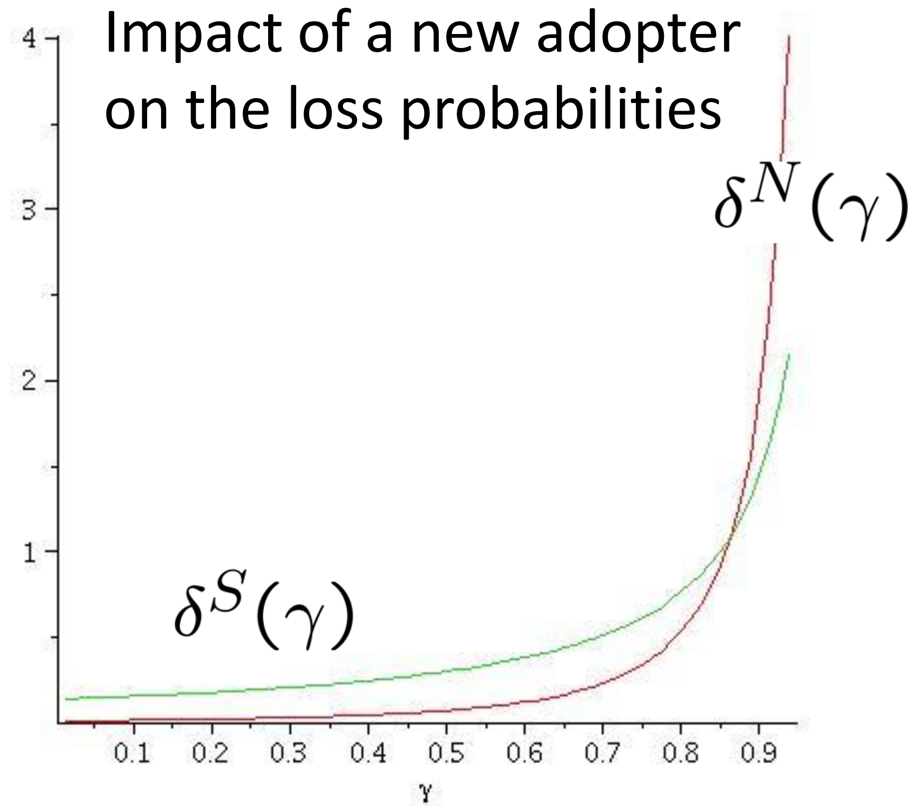
- An agent investing in S cannot be harmed by the actions of others: $q = 0$ in previous equation.
- Decreasing private externalities function and increasing public externalities function.



(3) Weak protection

- If $q > 0$, the network externalities function is:



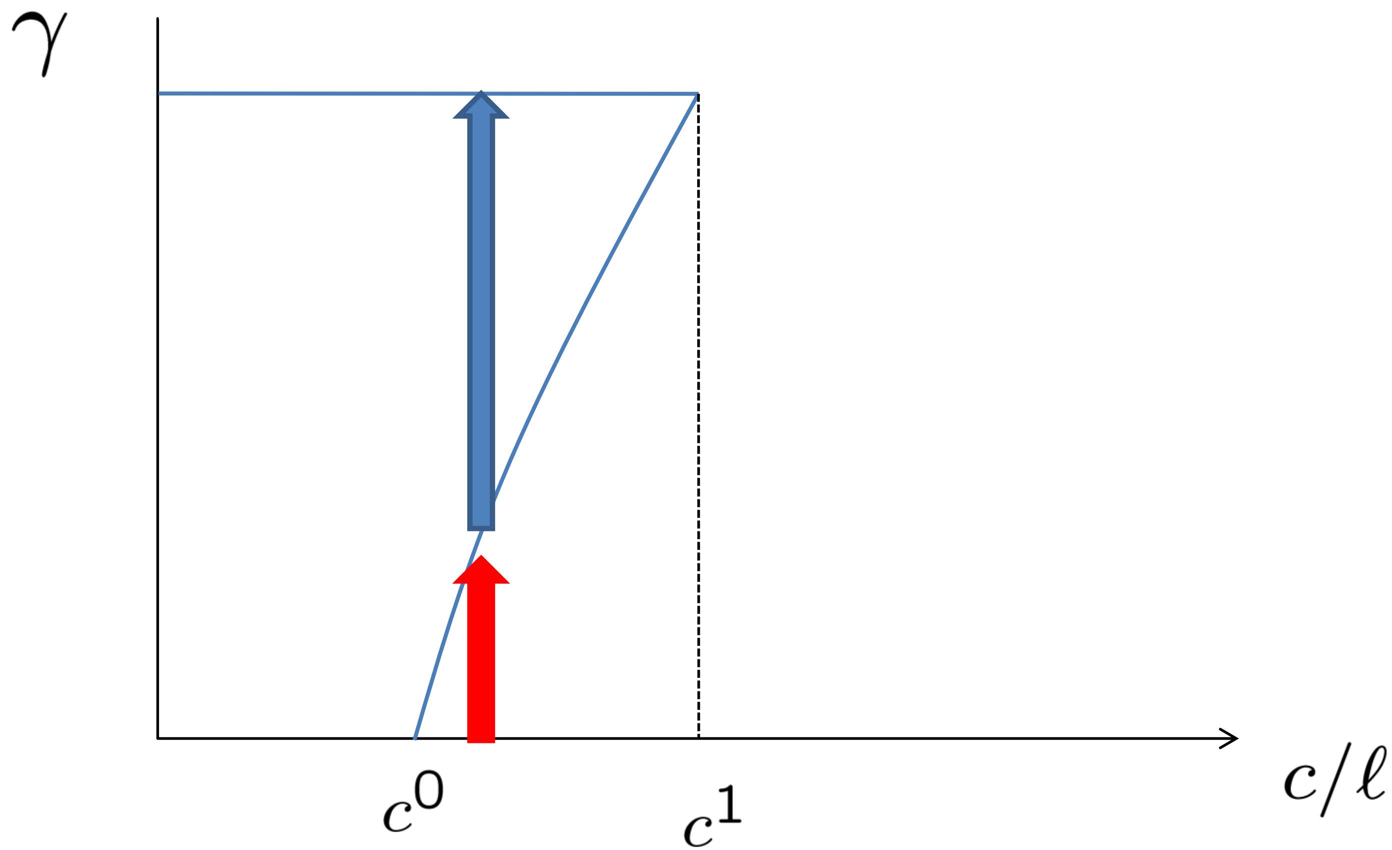


(3) Macro analysis

- Strong protection: contagion is possible only if agent is in state N, $q^{+} > q = 0$.
  - An agent in state S creates positive externalities: as γ increases, the incentive to invest in security decreases. Free rider problem.
- Weak protection: contagion is possible with probability q^{+} in N and q>0 in S.
  - Two equilibria (+ one unstable) are possible. Critical mass/Coordination problem.

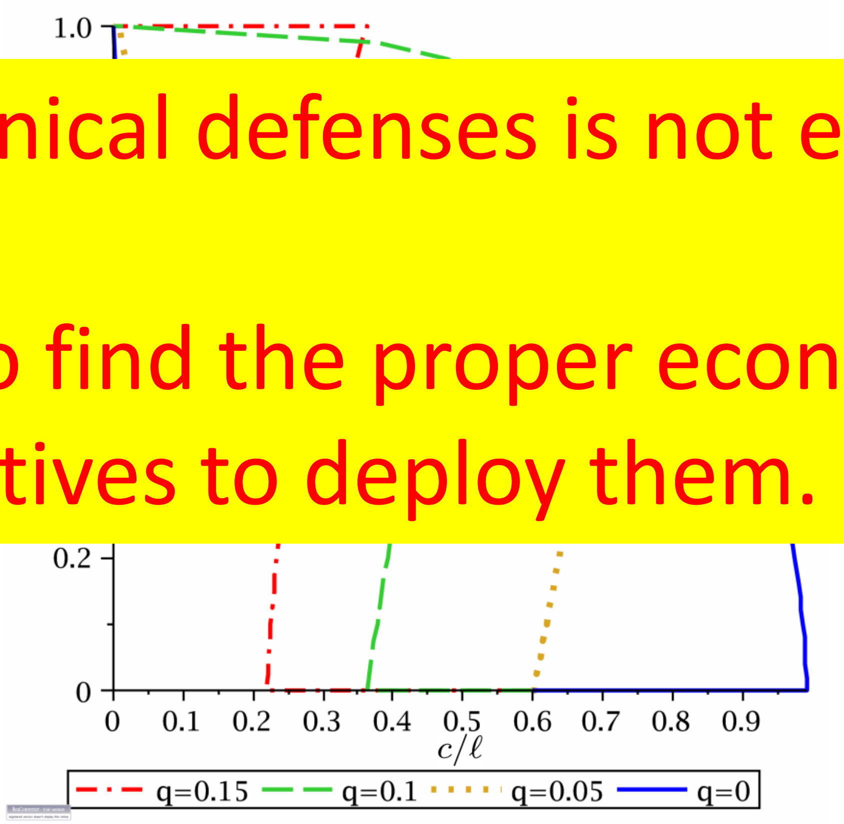
(3)Tipping phenomenon

- In the weak protection case, cascade possible:



(3)Adoption vs. quality of protection

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

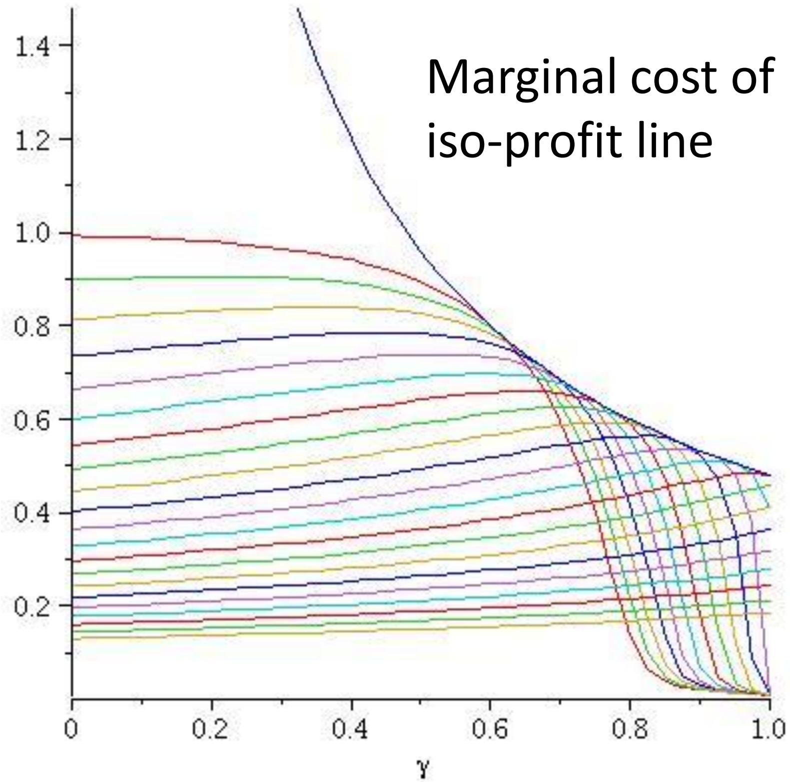


Improving technical defenses is not enough!

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

(3) Monopoly

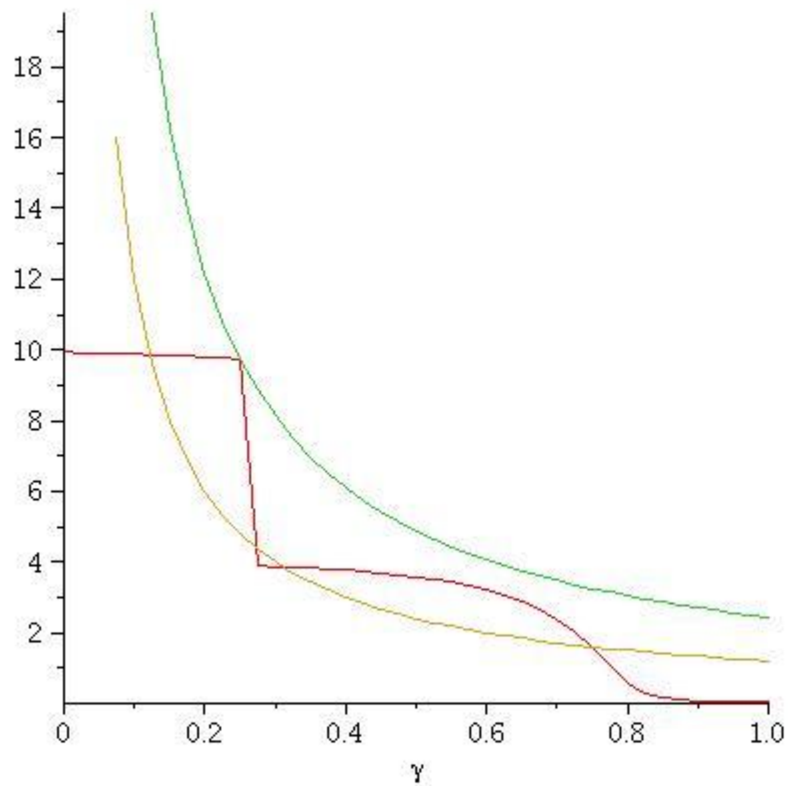
- No incentive to produce high quality software!



Marginal cost of production = zero.
iso-profit line

(3)Multiple equilibria with strong protection

- With two types of agents



Conclusions

- Epidemic risks model on random networks with strategic players shows a non-trivial relation between the fraction of population investing in security and the demand for security: free rider problem / critical mass - coordination game
- Need to distinguish between private and public externalities in security problem.
- Technology is not enough! There is a need to design economic incentives to ensure the deployment of security technologies.