Financial Aspects of Network Security: Malware and Spam

ITU Seminar on the Economics of Cybersecurity
Brisbane, Australia
15 July 2008

Johannes M. Bauer*
With Michel van Eeten**, Tithi Chattopadhyay*

* Michigan State University, USA,
** Delft University of Technology, Netherlands

Objectives of report

- Malware and spam have multifaceted and far-reaching, direct and indirect, financial effects
  - Costs for individuals, organizations, nations
  - Revenues for legal but also illegal players
  - Direct costs could be as high as 0.2-0.4% of GDP
  - Worst case scenario, including indirect effects, could be as high as 0.5-1% of global GDP
- Available information is incomplete and potentially biased by stakeholder interests
- The report aims at documenting the state of knowledge of these financial aspects

Overview

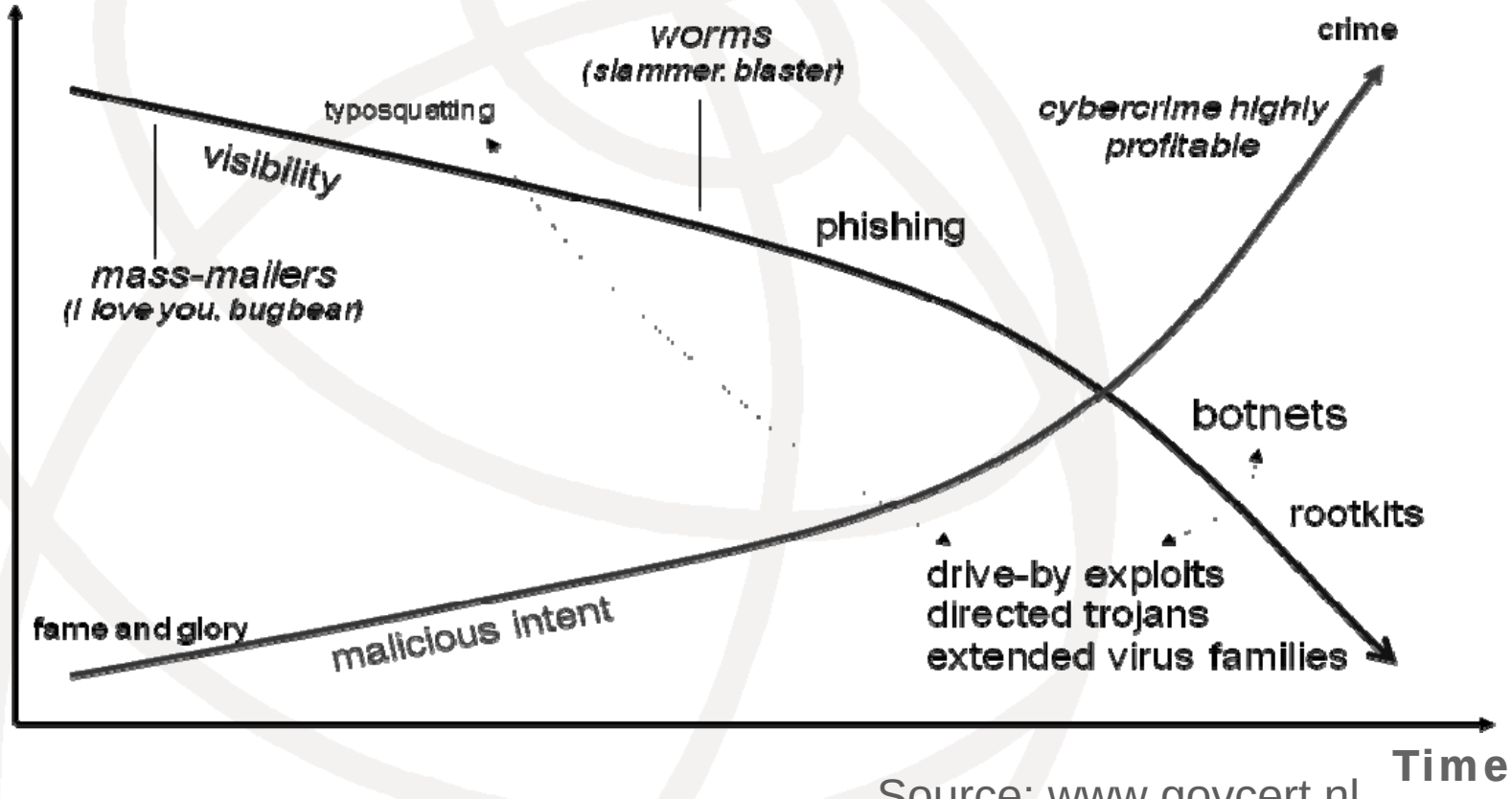
- Malware and spam developments
- A framework for analyzing financial flows related to malware/spam
- Synopsis of empirical findings
- A preliminary welfare assessment
- Appendix: the malware/spam underground economy

Malware and spam developments

Background

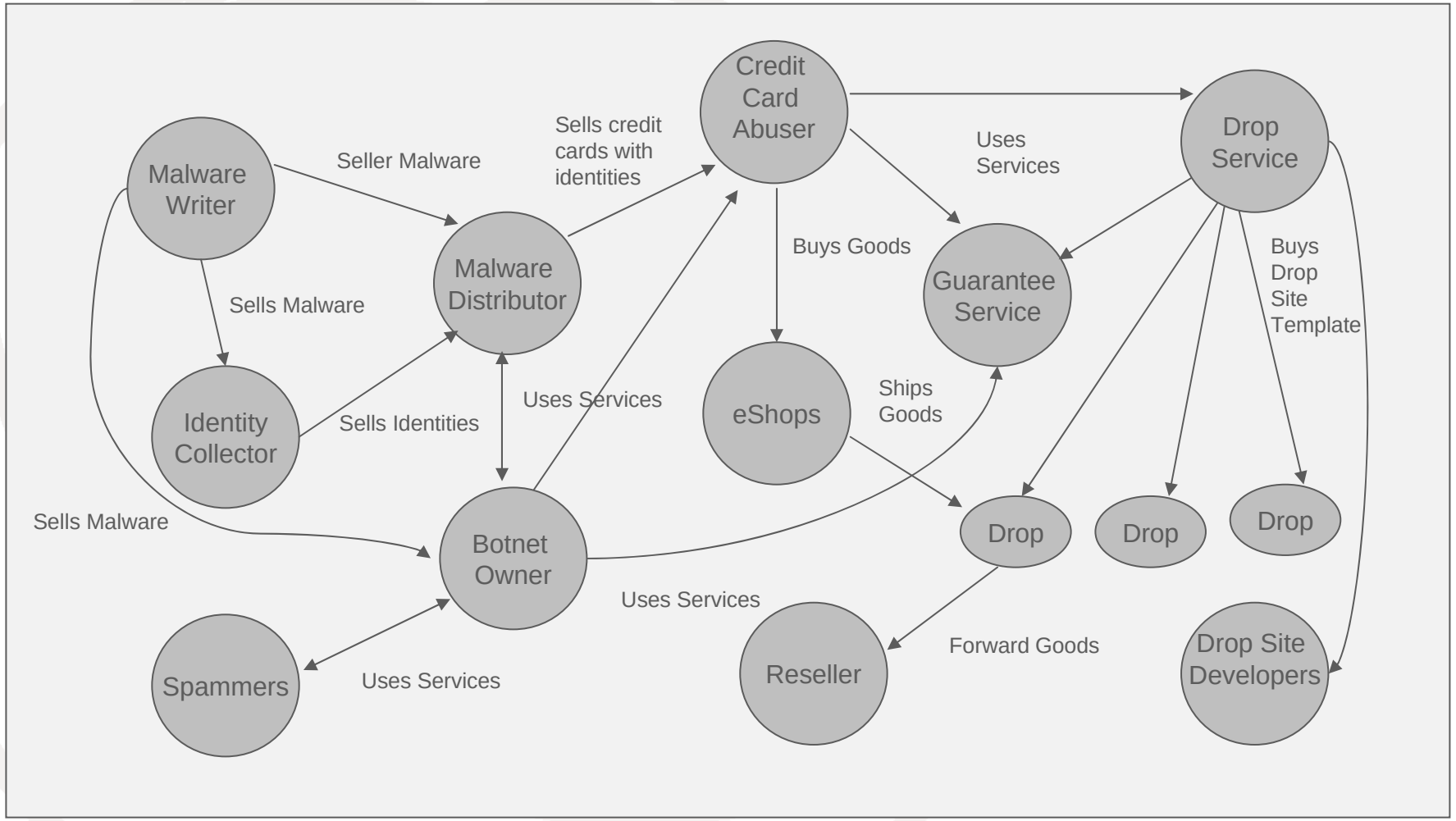
- Convergence of malware and spam
- Malware and spam are increasingly organized for financial gain
- Division of labor and specialization has increased sophistication and virulence of threats
- Inefficient security decisions of some players within the ICT value net ("externalities")
- Many spillovers between market players, nations, and regions → global problem

Visibility vs. malicious intent



Source: www.govcert.nl

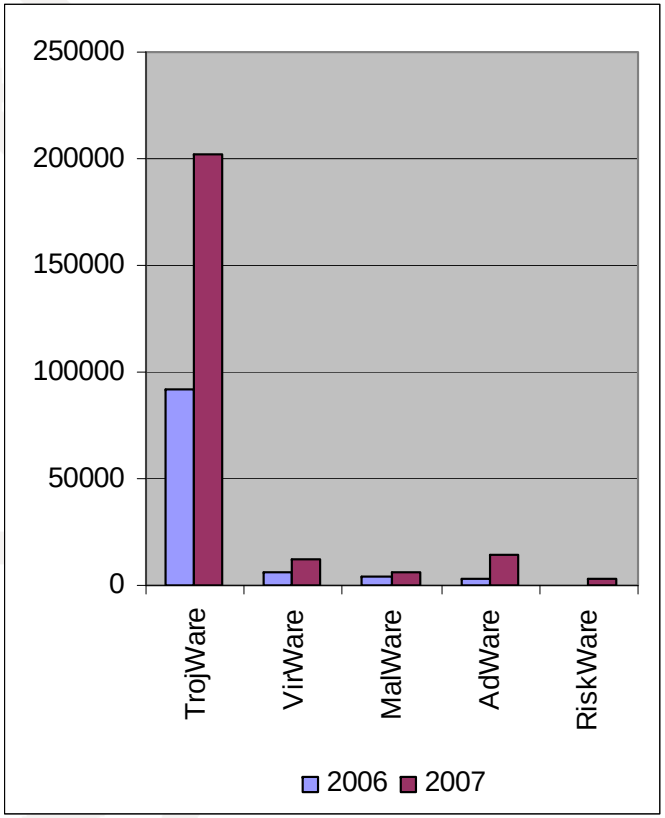
Division of labor



Source: Based on MessageLabs, 2007

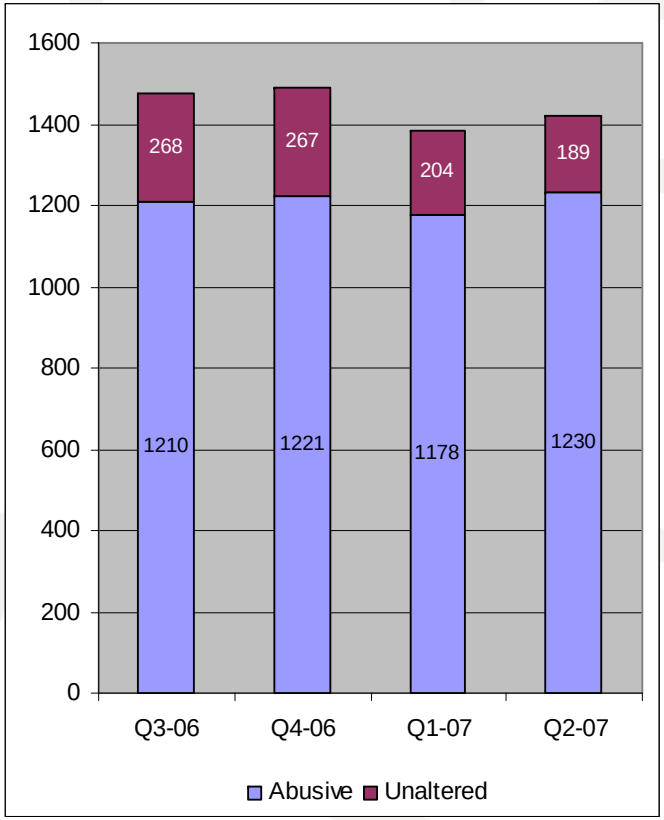
Malware attack trends

- Overall increases
- Monthly growth
  - trojans, rootkits slowing toward end of 2007
  - worms, viruses, AdWare and other accelerating
- As of 3/2008 (Panda)
  - 30% of computers on internet infected
  - about 50% active
- Postini reports 10% of websites as infected



Source: Based on Kaspersky Labs, 2008

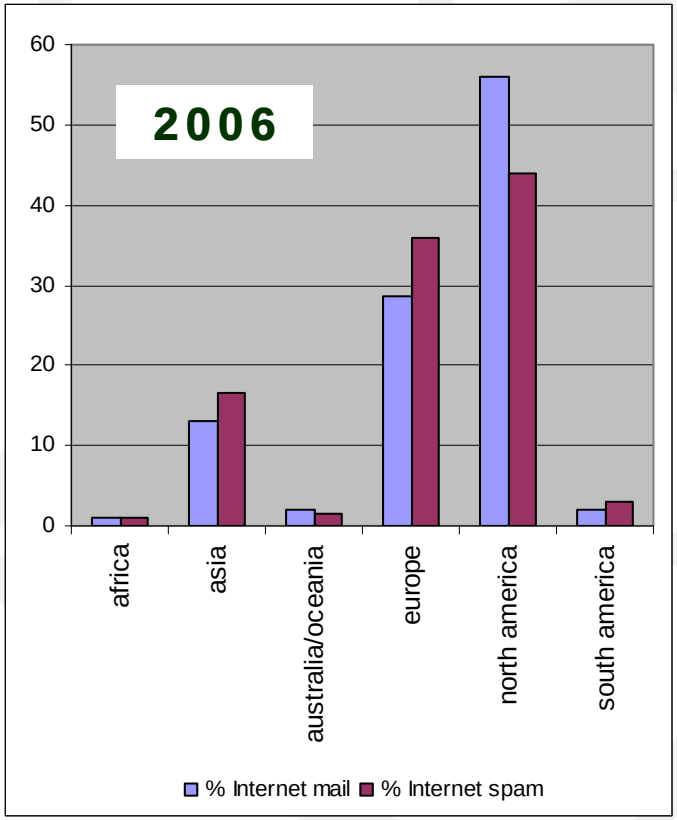
Spam trends

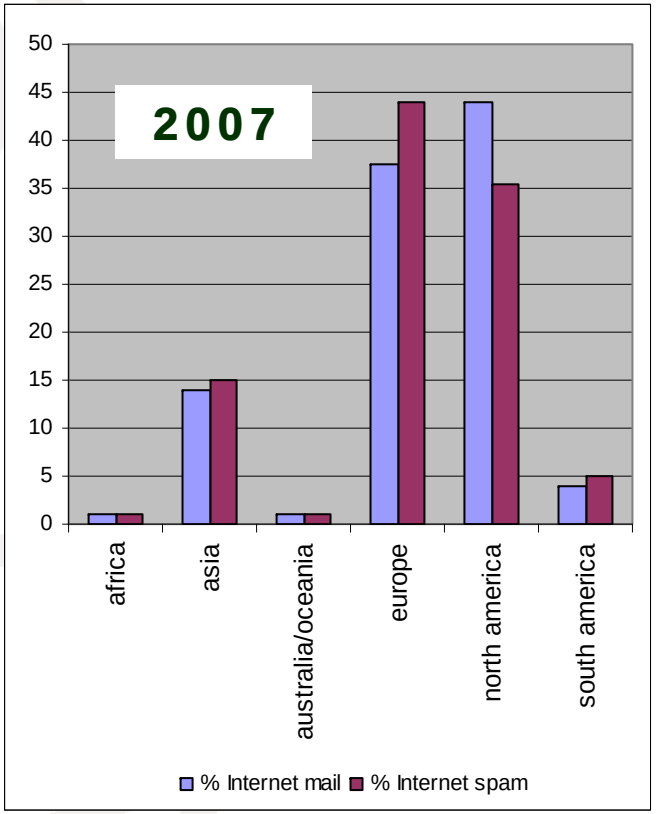


Source: MAAWG 2007

- Different metrics
- "Abusive" messages (MAAWG)
- MessageLabs new and old spam
- Symantec
- Fairly consistent numbers (85-90% of total messages)
- Spamhaus Project (IP addresses)

Geography of spam

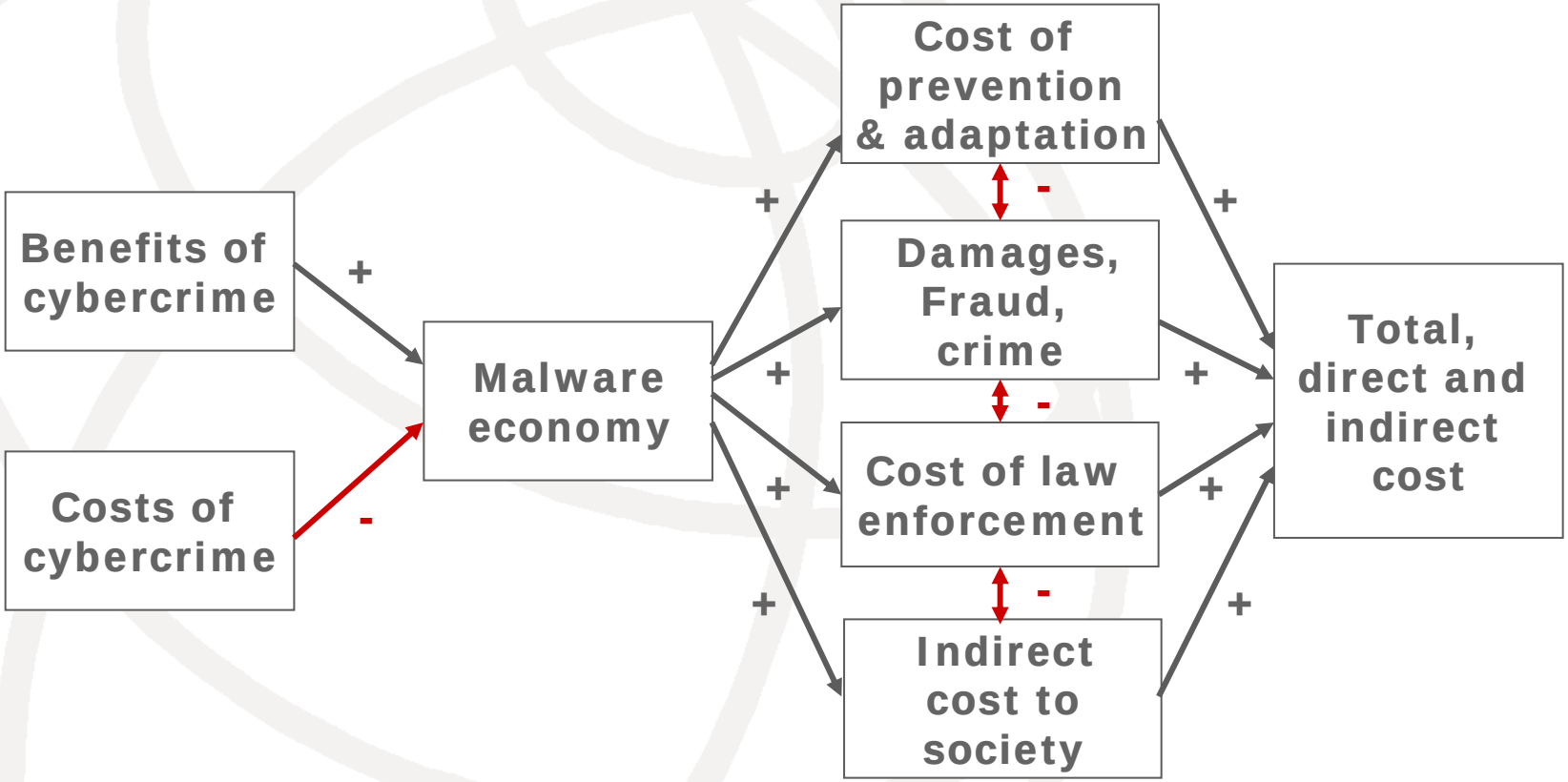




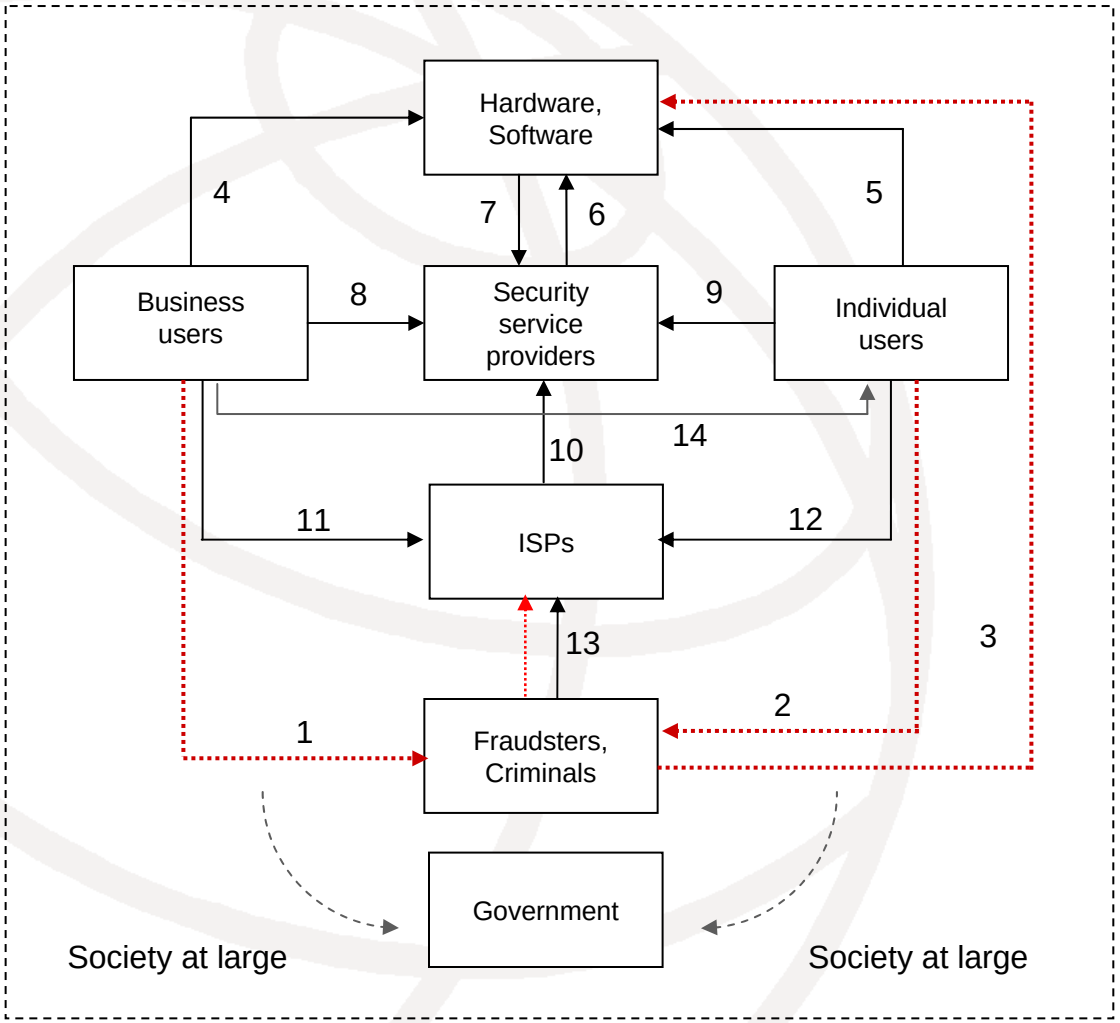
Source: Symantec, 2007, 2008

Financial aspects of malware and spam

Cost of spam and malware



Selected financial flows



Direct and indirect cost

- Direct cost include
  - Cost of prevention and adaptation
    - cost of preventative measures (e.g., security software and hardware, personnel training)
    - cost of infrastructure adaptation (network capacity, routers, filters, ...)
  - losses from fraudulent and criminal activity
- Indirect cost such as
  - cost of service outages
  - cost of law enforcement
  - opportunity cost to society (lack of trust)

Legal and illegal revenues

- Legal business activities
  - Security software and services
  - Infrastructure equipment and bandwidth
  - Legal, spam-induced sales revenues

Illegal business activities

- Writing of malicious code
- Renting of botnets
- Profits from pump and dump stock schemes
- Fraudulent commissions on spam-induced sales
- Money laundering (illegally acquired goods)

Main empirical findings

Cost of preventative measures

- Percentage of IT budget spent on security (2007 CSI Report)
  - 35% of respondents: <3% of IT budget
  - 26% or respondents: 3-5% of IT budget
  - 27% of respondents: >5% of IT budget
- TU Delft/Quello Center study indicates similar orders of magnitude
- 2006 global revenue of security providers estimated to $7.5 bn
- No reliable global figures on overall IT budgets and the increase caused by malware and spam

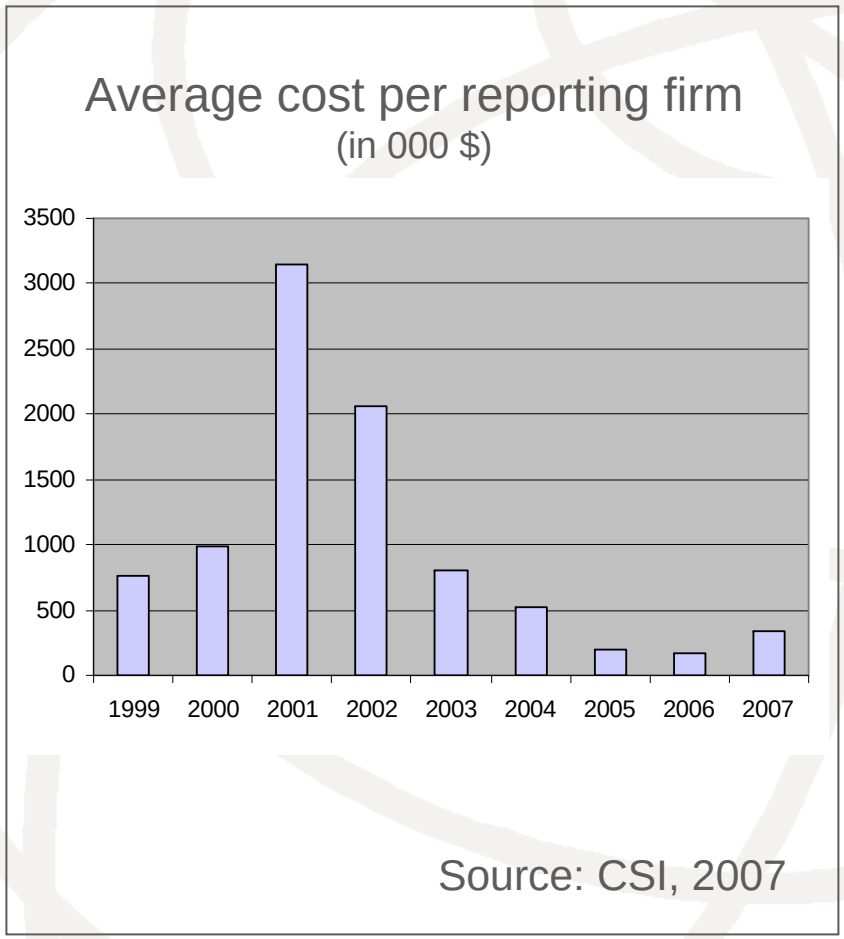
Damages, fraud, crime (1)

- Worldwide direct damage due to malware in 2006: $13.2 bn (Computer Economics)
  - Decline from $17.5 bn in 2004
  - Effects of anti-malware efforts and shift from direct to indirect costs
- U.S. Federal Bureau of Investigation estimated cost of computer crime to U.S. economy in 2005 to $67.2 bn (upper ceiling, not all malware-related)

Damages, fraud, crime (2)

- Global cost of spam in 2007: $100 bn, of which US$ 35 bn U.S. (Ferris Research)
- Cost of spam management to U.S. businesses in 2007: $71 bn (Nucleus Research)
- Direct costs to U.S. consumers in 2007: $7.1 bn (Consumer Reports)
- Range of estimates on online consumer fraud
  - $240-340 million for U.S.
  - £33.6 for financial fraud in UK
- Cost of click fraud in 2007: $1 bn (Click Forensics)

Direct losses to business



- Surveys of Computer Security Institute (CSI) members since 1996
- In 2007, 494 respondents of which 194 provided damage estimates
- Leading categories:
  - financial fraud
  - damage by viruses, worms, spyware
  - System intrusion
- Incomplete picture

Law enforcement & social costs

- Costs of law enforcement (positive but unknown)
  - Diffusion of costs among agencies (regulatory, civil law, criminal law)
  - Self-regulation, co-regulation (e.g., CSIRTS)
- Costs to society at large (positive but unknown)
- Incremental costs due to cybercrime are not known

A preliminary welfare assessment

Determining welfare effects

- Complicated by the legal and illegal revenues associated with cybercrime
- Total costs due to malware and spam
  - Direct costs (damages, prevention, …)
  - Indirect costs (law enforcement, trust, …)
- Illegal underground transactions (~ $105 bn) are costs to society
- Parts of legal revenues are “economic bads”, no net contribution to GDP

Assessing global effects

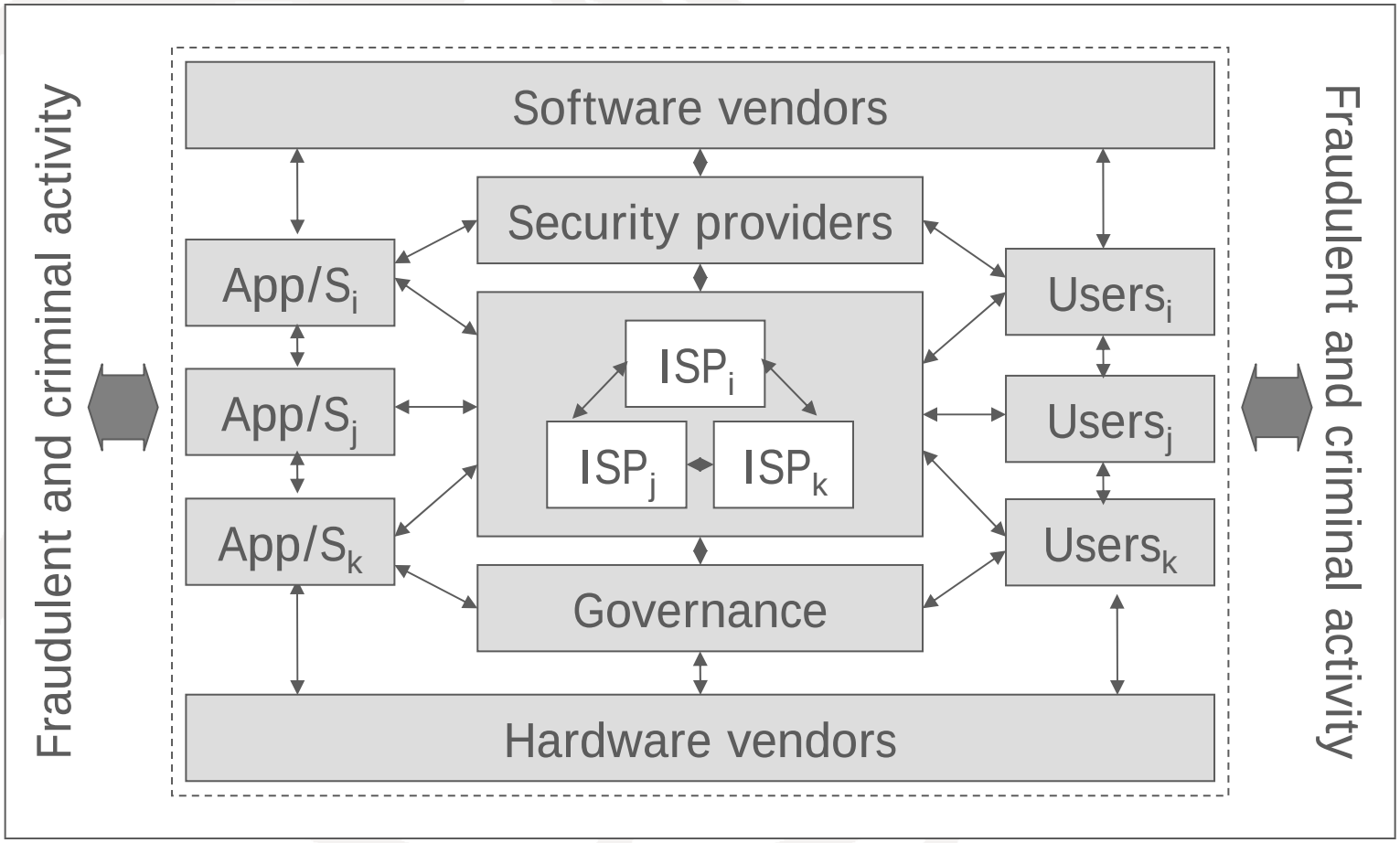
- Aggregation, projection to global level
  - Projection from country to global level?
  - Avoidance of double-counting
- A preliminary global estimate
  - Global direct costs as high as 0.2-0.4% of global GDP (in 2007 ~ $66 trillion)
  - In worst case scenario costs could be as high as 0.5-1% of global GDP
- Effects on industrialized, emerging, and developing countries varies greatly

Appendix
The malware/spam underground economy

Malware / spam

- Players in the underground economy include
  - Malware writers and distributors (trojans, spyware, keyloggers, adware, riskware, …)
  - Spammers, botnet owners, drops
  - Various middlemen
- Emergence of institutional arrangements to enhance “trust” (e.g., SLAs, warranties)
- Steady stream of new attacks (e.g., drive-by pharming, targeted spam, MP3 spam, …)

Interdependent value net



Efficient & inefficient decisions

- Instances where incentives of players are well aligned to optimize costs to society
  - ISPs correct security problems caused by end users as well as some generated by other ISPs
  - Financial service providers correct security problems of end users and software vendors
  - Negative reputation effects of poor security disciplines software vendors, ISPs, and other stakeholders
- Instances where incentives are poorly aligned
  - Individual users (lack of information, skills, …)
  - Domain name governance/administration system

More Information

- ITU-D ICT Applications and Cybersecurity Division
  - www.itu.int/itu-d/cyb/
- ITU-D Cybersecurity Activities
  - www.itu.int/itu-d/cyb/cybersecurity/
- Study Group Q.22/1: Report On Best Practices For A National Approach To Cybersecurity: A Management Framework For Organizing National Cybersecurity Efforts
  - www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf
- National Cybersecurity/CIIP Self-Assessment Toolkit
  - www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
- ITU-D Cybersecurity Work Programme to Assist Developing Countries:
  - www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf
- Regional Cybersecurity Forums
  - www.itu.int/ITU-D/cyb/events/
- Botnet Mitigation Toolkit
  - http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

International Telecommunication Union

Helping the World Communicate