Financial Aspects of Network Security: Malware and Spam

ITU-T Study Group 3
Geneva, Switzerland
2 April 2008

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

Please send comments to:

ITU-D ICT Applications and Cybersecurity Division
<cybmail@itu.int>

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

Objectives of report

- Malware and spam have far-reaching, direct and indirect, financial effects
  - Costs for individuals, organizations, nations
  - Revenues for legal but also illegal players
  - Direct costs probably 0.2-0.4% of global GDP
  - 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

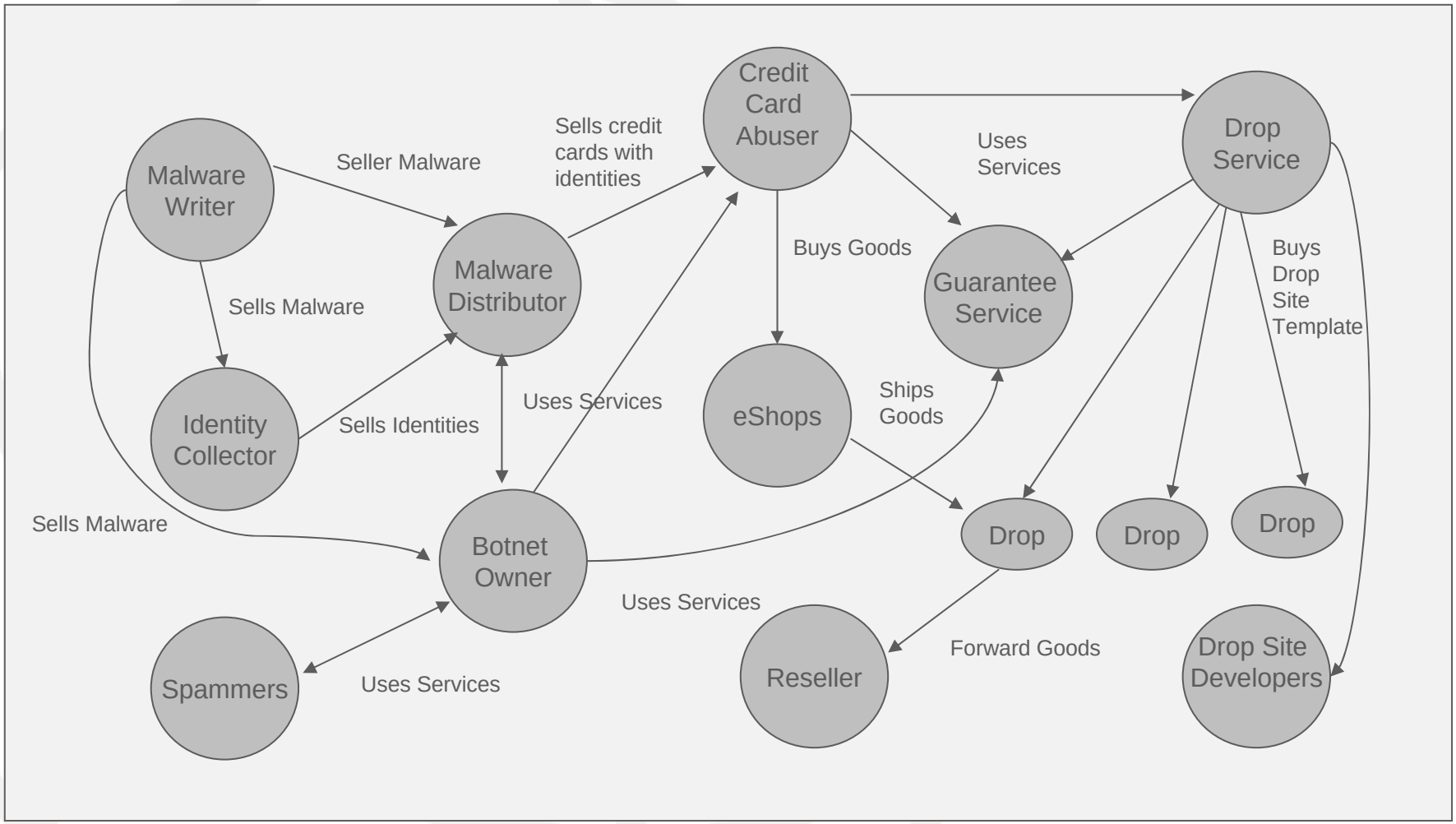
- Malware and spam developments
- A framework for analyzing financial flows related to malware/spam
- Main empirical findings
- A preliminary welfare assessment
- Appendix: the malware/spam underground economy

Malware and spam developments

Background

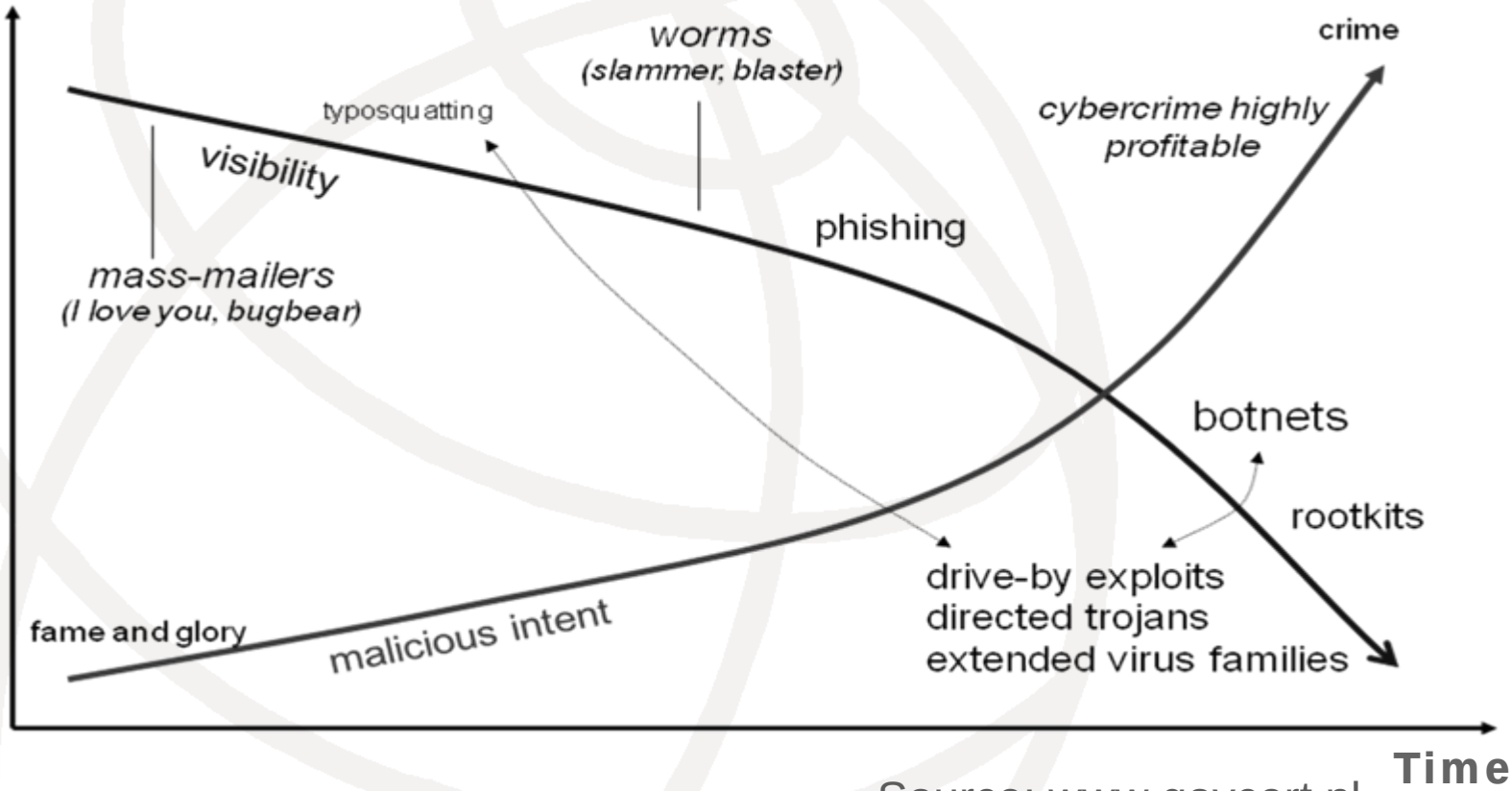
- Payoffs of fraudulent and criminal activity are high and have brought organized crime to malware and spam
- Division of labor and specialization has increased sophistication and virulence of threats from fraudsters and criminals
- Security decisions of some players within the ICT value net do not fully reflect social costs and benefits and only sub-optimally mitigate external threats

Division of labor



Source: MessageLabs, 2007

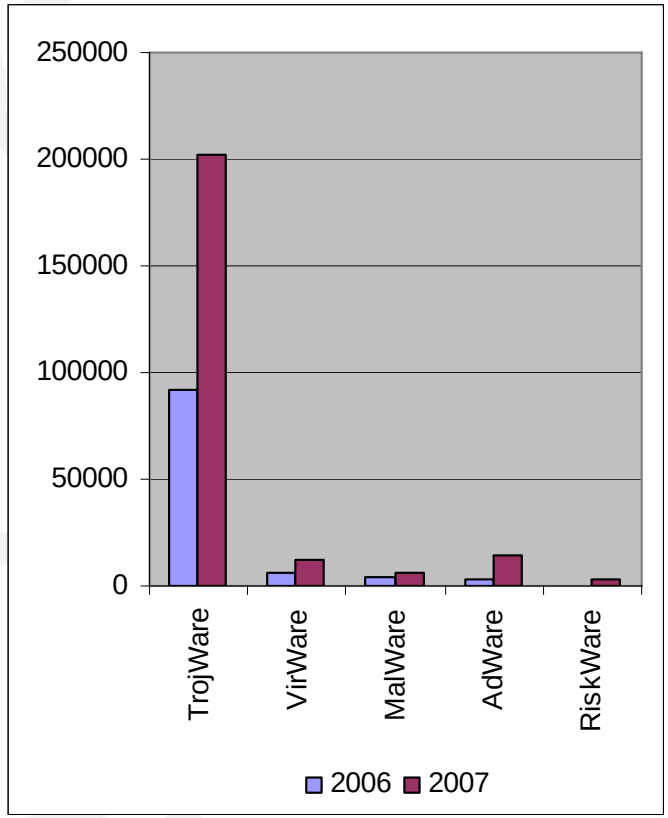
Visibility vs. malicious intent



Source: www.govcert.nl

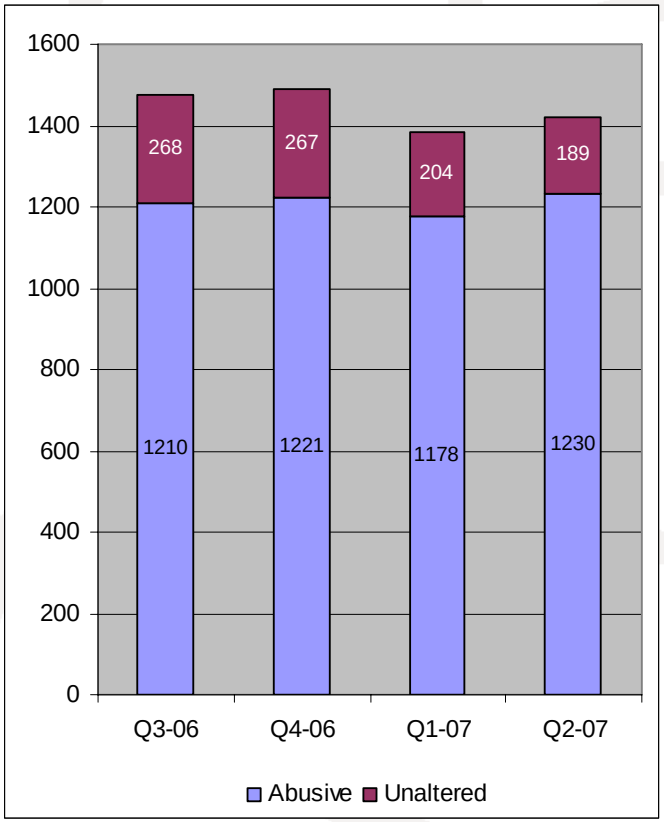
Malware attack trends

- 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: Kaspersky Labs, 2008

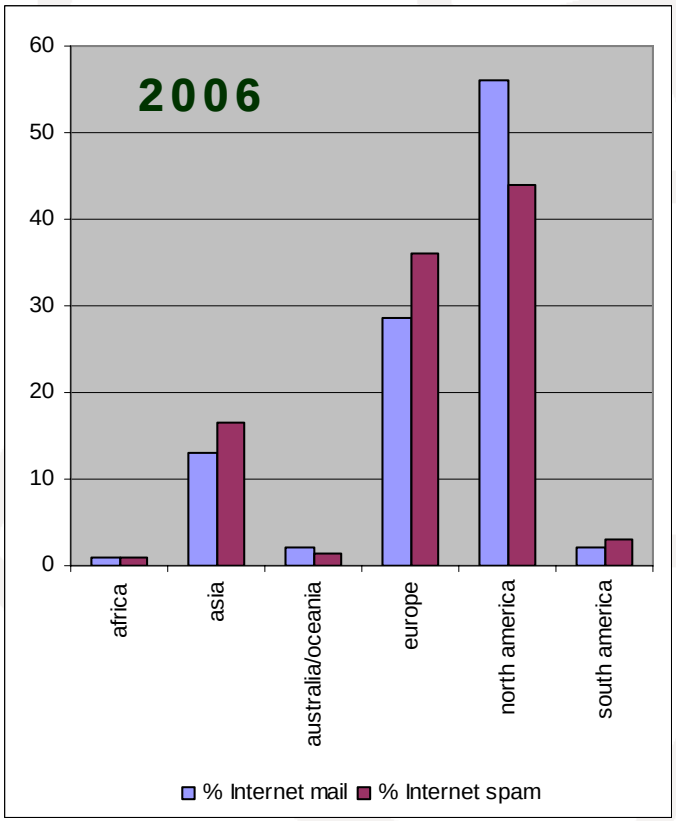
Spam trends

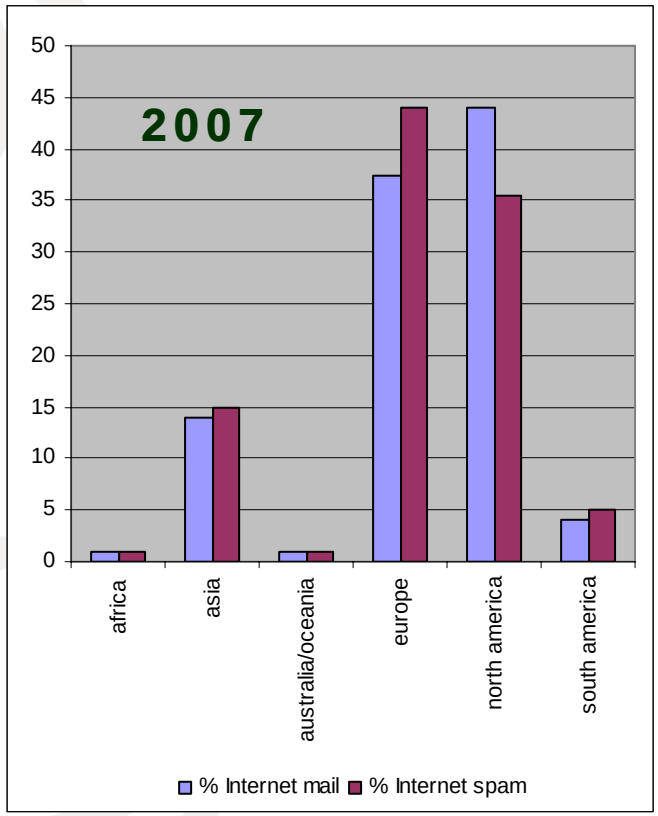


Source: MAAWG 2007

- 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

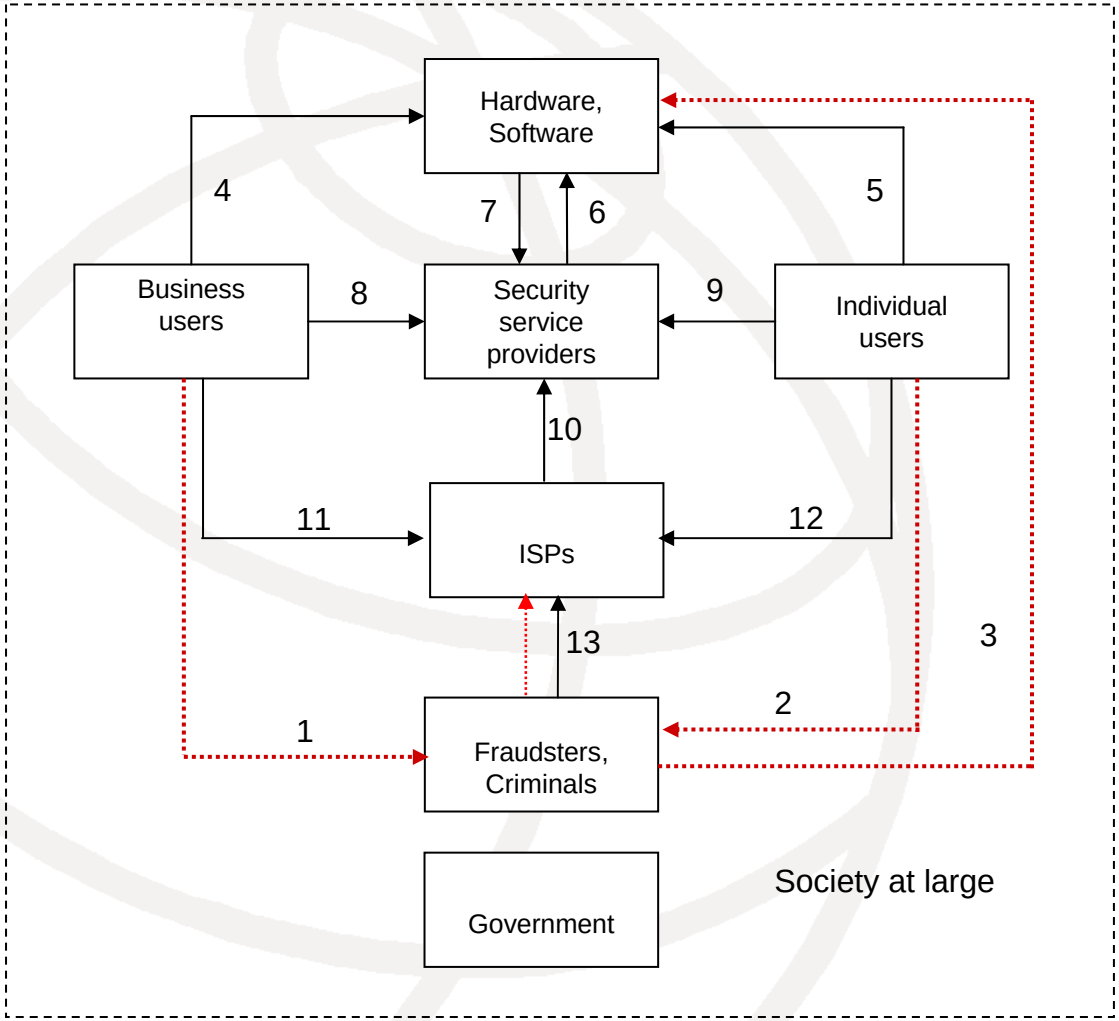




Source: Symantec, 2007, 2008

Financial aspects of malware and spam

Selected financial flows



Direct and indirect cost

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

Legal and illegal revenues

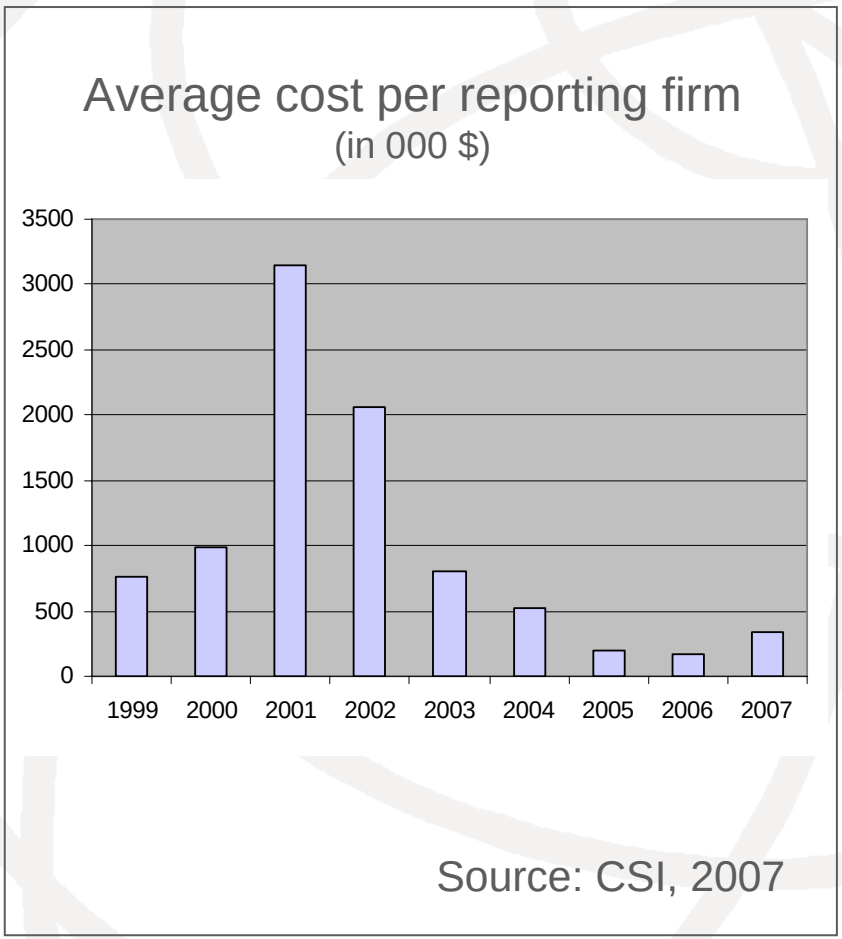
- Legal business activities
  - Security software and services
  - Infrastructure equipment and bandwidth
- Illegal business activities
  - Writing of malicious code
  - Renting of botnets
  - Profits from pump and dump stock schemes
  - Commission on spam-induced sales
  - Money laundering (illegally acquired goods)

Main empirical findings

Cost of malware

- Worldwide direct damage in 2006: $13.2 bn (Computer Economics survey of 52 IT professionals)
  - 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
- No estimates of indirect and of opportunity costs available

Direct losses to U.S. 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

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
- 2006 global revenue of security providers estimated to $7.5 bn (Gartner 2007)
- TU Delft/Quello Center study: 6-10% of IT budget dedicated to security

Cost of spam

- Global cost of spam in 2007: $100 bn, of which US$ 35 U.S. (Ferris Research)
- Cost of spam management to U.S. businesses in 2007: $71 bn (Nucleus Research)
- Cost of click fraud in 2007: $1 bn (Click Forensics)
- Cost to U.S. consumers in 2007: $7.1 bn (Consumer Reports)

A preliminary welfare assessment

Determining welfare effects

- Complicated by the legal and illegal revenues associated with cybercrime
- Costs of malware and spam
  - Direct costs (damages, prevention, …)
  - Indirect costs (law enforcement, trust, …)
- Economic “bads” (e.g., part of security investment), not welfare-enhancing
- Treatment of illegal transactions (estimated to total $105 bn)?

Scaling overall effects

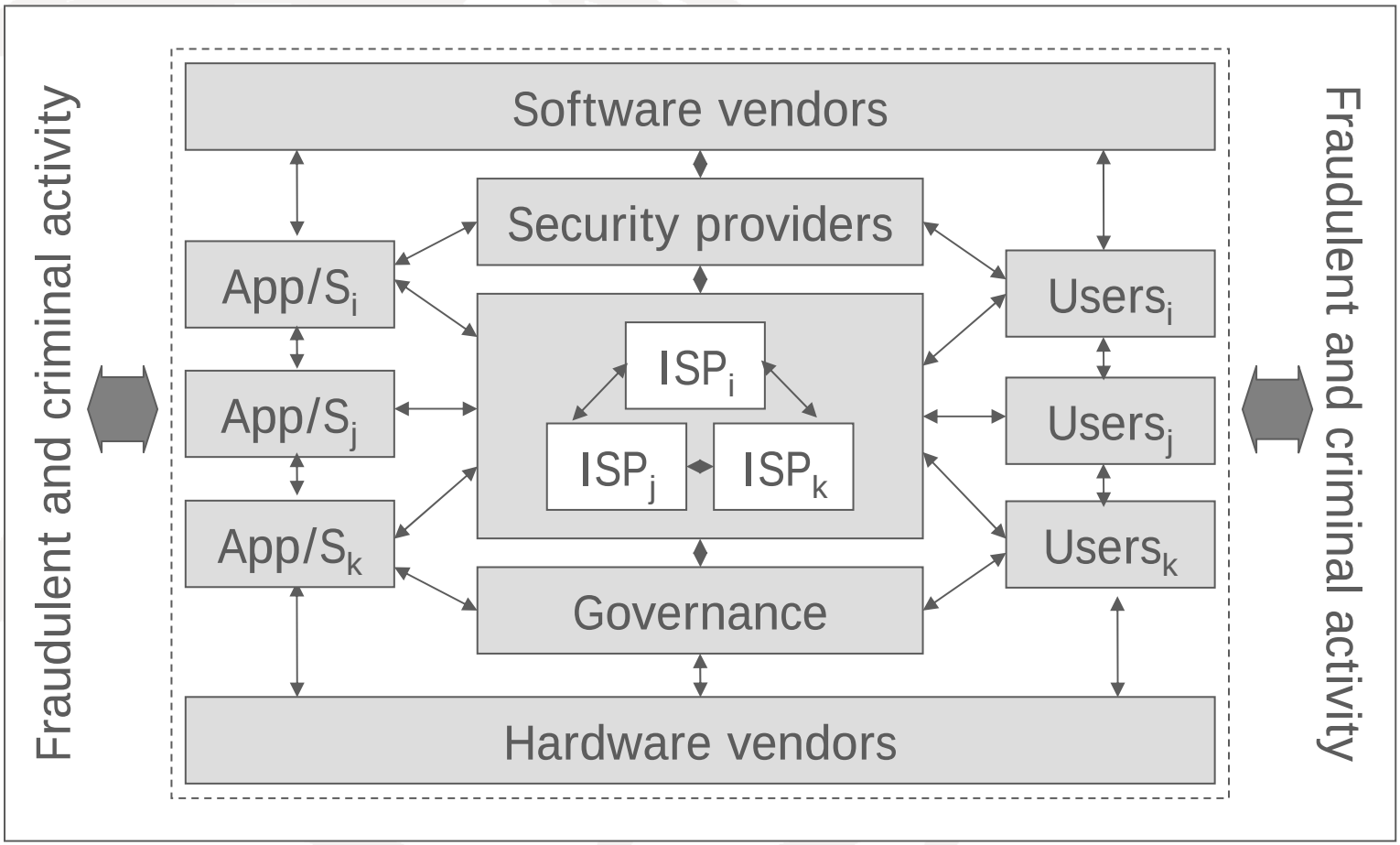
- Costs of malware and spam
  - Most reliable information at country level; how to scale to global level/
  - Avoidance of double-counting
  - Global direct costs probably in 0.2-0.4% range of global GDP ($66 tr)
  - Direct and indirect costs could be as high as 0.5-1% of global GDP
- Probably differential effects on national productivity and growth

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 Development Sector

- 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

More Information: ITU Standardization Sector

- ITU-T Study Group 17 – Lead Study Group on Telecommunication Security
  - www.itu.int/ITU-T/studygroups/com17/index.asp
- Question 17/17 - Countering spam by technical means
  - www.itu.int/ITU-T/studygroups/com17/sg17-q17.html
- Recommendations for approval on 18 April 2008:
  - X.1231 - Technical strategies on countering spam
  - X.1240 - Technologies involved in countering email spam
  - X.1241 - Technical framework for countering email spam

International Telecommunication Union

Helping the World Communicate