Individual security, contagion, and network design

Diego A. Cerdeiro, Marcin Dziubiński, Sanjeev Goyal

PII: S0022-0531(17)30058-3
DOI: http://dx.doi.org/10.1016/j.jet.2017.05.006
Reference: YJETH 4669

To appear in: *Journal of Economic Theory*

Received date: 3 November 2015
Revised date: 19 April 2017
Accepted date: 1 May 2017

Please cite this article in press as: Cerdeiro, D.A., et al. Individual security, contagion, and network design. *J. Econ. Theory* (2017), http://dx.doi.org/10.1016/j.jet.2017.05.006

Individual Security, Contagion, and Network Design*

Diego A. Cerdeiro†
Marcin Dziubiński‡
Sanjeev Goyal§

Abstract

Individuals derive benefits from their connections, but these may expose them to external threats. Agents therefore invest in security to protect themselves. What are the network architectures that maximize collective welfare? We propose a model to explore the tension between connectivity and exposure to an external threat when security choices are decentralized. We find that both over-investment and under-investment in security are possible, and that optimal network architectures depend on the prevailing source of inefficiencies. Social welfare may be maximized in sparse connected networks when under-investment pressures are present, and fragmented networks when over-investment pressures prevail.

Keywords: Network design; Individual security; Inefficiencies; Networks
JEL: D85; D62; C72

1 Introduction

Individuals derive benefits from being connected to others. These connections may, at the same time, transmit external threats. Online networks reflects this tension: connectivity facilitates communication but is also used by hackers, hostile governments, firms, and 'botnet' herders to spread viruses and worms which compromise user privacy and jeopardize the functioning of the entire system.[1] [2]

*This paper is based on a chapter in Diego Cerdeiro's doctoral thesis submitted to Cambridge University in June 2014, titled "Individual Security and Network Design".

†International Monetary Fund. E-mail: dcerdeiro@imf.org
‡Institute of Informatics, Warsaw University. E-mail: m.dziubinski@mimuw.edu.pl
§Faculty of Economics & Christ's College, University of Cambridge. E-mail: sg472@cam.ac.uk

[1]In the United States, the Department of Homeland Security (DHS) is responsible for cybersecurity. Its mission statement reads,"Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace. We rely on this vast array of networks to communicate and travel, power our homes, run our economy, and provide government services."

[2]Moore et al. (2009) estimate that in 2009, roughly 10 million computers were infected with malware designed to steal online credentials. The annual damages caused by malware are very large: in the US