Technological Forecasting & Social Change 80 (2013) 541–555

Contents lists available at SciVerse ScienceDirect

Technological Forecasting & Social Change

The cybercrime ecosystem: Online innovation in the shadows?

Erika Kraemer-Mbula [a], Puay Tang [b], Howard Rush [a,*]

[a] CENTRIM — Centre for Research in Innovation Management, University of Brighton, Freeman Centre, Brighton BN1 9QE, UK
[b] SPRU — Science and Technology Policy Research, University of Sussex, Freeman Centre, Brighton BN1 9QE, UK

ARTICLE INFO

Article history:
Received 29 September 2011
Received in revised form 8 June 2012
Accepted 4 July 2012
Available online 30 November 2012

Keywords:
Innovation
Networks
Digital ecosystems
Cybercrime
Value chains
Capabilities
Business models

ABSTRACT

With the growing sophistication and use of information technology, the past decade has witnessed a major growth in financial cybercrime. This paper focuses specifically on credit card fraud and identity theft, examining the globalisation of these activities within a 'digital ecosystem' conceptual framework. The relevance of concepts and analytical tools typically used to study legitimate businesses, such as value chains, dynamic capabilities and business models, is explored and tested for their relevance in understanding the scale and nature of illegal activities which are dependant upon innovation and the collective activities of global participants. It is argued that developing a better understanding of how such illegal activities are organised and operate will assist policy makers, law enforcement agencies and security firms to identify trends and concentrate limited resources in a most effective manner.

© 2012 Elsevier Inc. All rights reserved.

1. Introduction

Innovation is at the heart of the growth of illegal Internet-based activities commonly known as cybercrime [40,50,60]. Criminal organisations are not only incorporating emerging technologies in their activities, but are increasingly pioneering and seizing opportunities for new illegal enterprises made possible by the Internet and the continuing growth of electronic commerce.

Arguably, many of these innovations represent the cutting edge of global criminal activity. They provide higher prospects for illicit profits at seemingly lower degrees of risk. Security analysts can have difficulty in identifying the locations from where the cybercriminals may be operating (see Table 1 below) and find it difficult to identify the perpetrators. Cybercrime thus represents the growing sophistication of existing criminal behaviour and the emergence of novel illegal cyber activities. It presents unique and difficult challenges for law enforcement officers charged with countering such activities.

Despite being an innovation-driven phenomenon, most analysis of cybercrime has been undertaken from the perspectives of criminology, information and communications technology (ICT) security firms and journalists, rather than innovation scholars. The aim of this paper is to examine the evolution of cybercrime through the lens of innovation studies in order to develop a framework which aims to contribute to a new perspective on how cybercriminals innovate, organise and operate, and how law enforcement agencies must change to combat this growing trend.

The lack of systematic innovation-based analysis of cybercrime has left gaps in the understanding of how cybercrime has evolved into a large global 'business' within and connected to the Internet. To contribute to filling these gaps, this paper analyses the evolution

* Corresponding author. Tel.: +44 1273 877912; fax: +44 1273 877977.
E-mail address: H.J.Rush@Brighton.ac.uk (H. Rush).

0040-1625/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
doi:10.1016/j.techfore.2012.07.002

Table 1
Cybercrime activity by country.

Overall rank			Percentage		2009 malicious code rank			
2009	2008	Country	2009	2008	Malicious code	Phishing hosts	Bots	Attack origin
1	1	United States	19	23	1	1	1	1
2	2	China	8	9	3	6	2	2
3	5	Brazil	6	4	5	12	3	6
4	3	Germany	5	6	21	2	5	3
5	11	India	4	3	2	21	20	18
6	4	UK	3	5	4	7	14	4
7	12	Russia	3	2	12	5	19	10
8	10	Poland	3	3	23	8	8	17
9	7	Italy	3	3	16	18	6	8
10	6	Spain	3	4	14	11	7	9

Source: [61].

of cybercrime through the borrowed concept of a "digital business ecosystem" [16, p. 3].[1] We suggest that by deepening our understanding of the cybercrime ecosystem it may be possible for the relevant authorities to more rapidly identify trends and forecast new developments. In so doing they should be able to more effectively concentrate their limited resources in dealing with cybercrime.

James Moore [39], in his McKinsey award-winning article, introduced this concept which has become widely used by social scientists and students of business and organisational management and design. Moore defined a business ecosystem as:

> "a loose network of suppliers, distributors and outsourced firms that work cooperatively and competitively to support new products, satisfy consumer needs and incorporate innovation".[2]

According to his view, firms do not belong to a single industry, but their activities cut across multiple industries. Refining his concept further [40: 26], he added that an ecosystem is:

> "an economic community supported by a foundation of interacting organisations and individuals—the organisms of the business world. The economic community produces goods and services of value to customers, who are themselves members of the ecosystem. The member organisms also include suppliers, lead producers, competitors, and other stakeholders".

Other scholars have further elaborated on this concept by emphasising that entities of a business ecosystem have different interests but are interconnected through cooperation and competition, for their mutual survival and effectiveness [62]. Analogous to natural ecosystems, business ecosystems are characterised by "interconnectedness" and "shared fate" among diverse organisations, "that contributes to their collective productivity and robustness" [45: 104].[3]

Drawing on this concept, we argue that there is merit to analysing the cybercrime network in terms of a digital business ecosystem, which depends on information and communication technologies, responds to its environment, is interdependent on various entities and continually innovates in order to be effective and survive. We label this ecosystem as the "cybercrime ecosystem".

Furthermore, the business ecosystem provides a perspective that can be used to analyse interconnected businesses, that is "by looking at the relationships or interactions among the members and their environment and at the roles and interests of the members of the system" [8,11,18].[4] As will be discussed, financial cybercrime is an "interconnected" business, with different roles and interests of the constituents of this network. In addition to a variety of criminal participants, the cybercrime ecosystem includes legitimate businesses, such as IT security firms, banking and financial services. For instance, IT security firms interact with organisations in the financial services when they have to develop new measures to identify new attacks and to deal with the vulnerabilities found in network infrastructures. Cybercriminals, in turn, have to further hone their skills and develop ever more sophisticated malicious tools to infect the digital networks and to circumvent security measures. In a sense, these two communities, perversely, have a shared fate, as if participating in a game of innovation leapfrogging as one set of actors in the ecosystem attempts to counter the advances and responses of another set of actors.

Drawing from existing literature and the results from an exploratory study involving academics, IT security firms, law enforcement officers, financial institutions and policymakers [46], this paper first defines the types of cybercrime before examining the conceptual foundations of the cybercrime ecosystem and its three core elements. They are (1) the international value chains (networks) which link activities and actors; (2) the changing capabilities that underlie the ecosystem; and (3) the business models that arise from the changing capabilities and concomitant innovations and strategies.

[1] The conceptual framework in this article was developed and validated in a pilot study funded by the National Endowment for Science, Technology and the Arts (NESTA). This article draws upon and updates Rush, H; Smith, C; Tang, P. and Kraemer-Mbula, E. "Crime online: Cybercrime and illegal innovation", NESTA, 2009. As argued below, this particular framework promises valuable and comprehensive innovation insights because it combines elements of innovation study, value chain analysis, capability theory and business model examination.

[2] Quoted in [16].

[3] It is worth noting that these authors, particularly Iansiti and Levien [62], with whom the term ecosystem is also much associated in the strategy literature, adopt the ecosystem concept to provide a perspective on business strategy and business networks.

[4] We acknowledge that there is a plethora of literature on business networks, which among other things, study the 'connectedness' of business networks and the diffusion of innovation. However we differ from these studies by focusing on the ecosystem's evolving and dynamic characteristic through 'internal innovation'.

Download English Version:

https://daneshyari.com/en/article/896645

Download Persian Version:

https://daneshyari.com/article/896645

Daneshyari.com