Information **2013**, *4*, 117-123; doi:10.3390/info4010117

OPEN ACCESS

information

ISSN 2078-2489

www.mdpi.com/journal/information

Article

Reliability, Validity, Comparability and Practical Utility of Cybercrime-Related Data, Metrics, and Information

Nir Kshetri

Bryan School of Business and Economics, The University of North Carolina at Greensboro, P.O. Box 26165, Greensboro, NC 27402-6165, USA; E-Mail: nbkshetr@uncg.edu; Tel.: +1-336-334-4530; Fax: +1-336-334-5580

Received: 20 December 2012; in revised form: 7 February 2013 / Accepted: 7 February 2013 / Published: 11 February 2013

Abstract: With an increasing pervasiveness, prevalence and severity of cybercrimes, various metrics, measures and statistics have been developed and used to measure various aspects of this phenomenon. Cybercrime-related data, metrics, and information, however, pose important and difficult dilemmas regarding the issues of reliability, validity, comparability and practical utility. While many of the issues of the cybercrime economy are similar to other underground and underworld industries, this economy also has various unique aspects. For one thing, this industry also suffers from a problem partly rooted in the incredibly broad definition of the term “cybercrime”. This article seeks to provide insights and analysis into this phenomenon, which is expected to advance our understanding into cybercrime-related information.

Keywords: cybercrime metrics; comparability; pay-per-click (PPC) advertisements

1. Introduction

By all accounts, the global cybercrime industry is much bigger than most of the major and well-known underground and underworld industries such as illegal drugs trade and human trafficking [1]. Unsurprisingly, various metrics, measures and statistics have been developed and used to characterize the pervasiveness and severity of cybercrimes. As is the case of any underground economy [2], estimating the size of the cybercrime industry and its subsets, however, has been a challenge. Cybercrime related studies and surveys are replete with methodological shortcomings, conceptual confusions, logical challenges and statistical problems. The reliability and validity of

indicators used to measure cybercrime-related constructs are of major concern. Inter-jurisdictional, inter-category and longitudinal comparisons are even more problematic. It is not unusual to find that estimates of a given indicator differ by a factor of 100. Given such limitations, one may wonder what the practical utility of these indicators might be.

Before proceeding further we first provide a clarifying definition. A cybercrime is defined as a criminal activity in which computers or computer networks are used as the *principal* means of committing an offense or violating laws, rules and regulations [3,4].

2. Inconsistencies in Cybercrime Metrics: Some Examples, Illustrations and Associated Motivations

Empirical findings and conclusions drawn from surveys and studies and experiences of experts, companies and law enforcement agencies are remarkably inconsistent. There are plenty of examples to illustrate this.

First, consider some statistics. *PriceWaterhouseCoopers* estimated that, businesses' costs to fight hackers and viruses were US$300 billion in 2000 and $2.1 trillion in 2004. Similarly, a 2000 study, which surveyed about 5000 IT professionals in 30 countries claimed that that hacker attacks would cost the world $1.6 trillion [5]. In the same year, *Reality Research* suggested that businesses worldwide would lose $1.5 trillion due to computer viruses. Likewise, according to *SecurityStats*, computer viruses cost $570 billion in 2003.

Perhaps the most often cited figure for the global cybercrime industry's size in 2009, including by U.S. Senator Susan Collins in her April 2010 Exception magazine article, is US$1 trillion. *The Organization for Security and Cooperation in Europe* (OSCE), however, put cybercrimes' costs at US$100 billion worldwide in 2009.

Interestingly, a comparison of PriceWaterhouseCoopers' and the OSCE's estimates indicates that cybercrimes' costs to the global economy reduced by over 95% during 2004–2009. This is highly unlikely, especially considering the evolution of new forms of cybercrimes recently.

Estimates of the various cybercrime categories are equally problematic. Consider, for instance, auction frauds. According to Consumer Reports, EBay claims that users face a 1 in 10,000 risk of fraud in online auctions [6]. According to the FBI, however, the auction fraud rate on EBay website is about 1 in 100 [7]. In 2006, auction fraud was the most reported cybercrime category, which comprised of 45% of complaints made to the Internet Crime Complaint Center [8].

A second example comes from click fraud. Illegitimate clicks on pay-per-click (PPC) advertisements constitute an industry of a substantial size. Advertisers and search providers differ widely in their assessment of click frauds. PPC providers such as Google maintain that invalid clicks that aren't proactively detected are less than 0.02% of clicks. Advertisers believe that the proportion is higher and argue that PPC providers' secretive techniques to detect invalid clicks purposely keep them in the dark [9].

As another example, consider average costs to clean virus infection. A 2006 FBI report indicated that the average attack cost US$24,000 including expenses related to repairing infected machines and networks and lost work time. Another study, however, suggested that costs to repair virus-inflicted computers averaged US$81,000 per incident per company in 2002 [10]. The fact that cyber-criminals

are getting cleverer as evidenced by various severe forms of malware, however, contradicts the possibility that such costs decreased during 2002–2006.

Estimates vary widely even for indicators related to concepts that have fairly straight-forward measurements. In 2007, Vinton Cerf, the co-designer of the Internet's basic architecture noted that up to 25% of computers connected to the Internet might be linked to botnets. Other estimates for this proportion are: *The Messaging Anti-Abuse Working Group's* estimate of 7% in 2006; and the *Georgia Tech Information Security Center's* estimates of 10% in 2007 and 15% in 2008.

Many of the cybercrime metrics are developed and used by multiple parties with diverse motivations and objectives. Different estimates related to cybercrime have been widely criticized on the ground that there may be vested interests of the organization which may lead to over or under estimation of the true level. Security and consulting companies may exaggerate risks. The law enforcement agencies may use "purported evidence" of the rapid cybercrime growth "to justify larger budgets and more arbitrary powers" [2]. E-commerce companies such as Ebay and Google, have an incentive to project the image of a safer website, which would help them protect and expand their market shares. Factors contributing to low reporting rates could also be embarrassment, the fear of losing customer trust; the damage in corporate credibility and potential stock prices fall.

As to the tendency of some e-commerce players to portray their websites as safer than they actually may be, prior research in economics indicates that organizational orientation has a built-in bias that favors organized groups compared to those that are unorganized [11]. Businesses and consumers are realizing that it is important for them to engage in organized movements to exert pressure to suppliers of online services such as PPC ads and auctions to be more accountable and transparent. There are some encouraging signs in this direction. Google, for instance, gives advertisers aggregated statistics but no information about whether it identified a particular click as valid or invalid. A coalition of advertisers such as Expedia and LendingTree pressured Google and Yahoo to be more accountable and demanded audited numbers and common measurement standards.

3. Conceptual, Methodological, Logical and Statistical Problems in Estimating Cybercrimes

There is no universally accepted definition of cybercrime. This situation is different from a number of serious, traditional crimes have more or less internationally accepted definitions. For instance, for human smuggling and trafficking, the United Nations protocols have provided common international definitions of these phenomena. Likewise, global anti-trafficking efforts and responses are guided by a common international definition of the term "trafficking in persons" [12]. Experiences of other areas such as the banking and insurance industry indicate the development of international norms and common international definition is a complex and time consuming process [13]. The efforts to develop international cybercrime norms are relatively new and thus there is a considerable heterogeneity among nations in norms related to cybercrimes as well as in definitions and responses.

In addition to the international differences, the conceptual definitions vary considerably across surveys and studies with regard to their clarity, comprehensiveness and currency. In some cases, definitions of cybercrimes and related terms are not stated in surveys.

Cybercrimes are offences conducted in the "cyberspace". However, "cyberspace" is ambiguous in the first place. Some authors have restricted cybercrime's definition to unlawful activities committed by a private individual [14]. Other analyses are sufficiently general to cover all types of violations.

A logical issue concerns a lack of clear and defensible standards specifying which components of costs constitute the impact of a cybercrime. Estimates regarding the economic impact of Love bug virus varied from $2.6–$15 billion [15]. Different combinations of direct, indirect and opportunity costs such as money and intellectual property stolen, costs of fixing or replacing infected networks and equipment, lost work time and intangible losses associated with the loss of customer confidence are included under cybercrimes' projected losses [8,16].

4. Inter-Jurisdictional, Inter-Category and Longitudinal Comparisons

Definitions and estimates of cybercrimes also differ due to heterogeneity in institutional differences, preferences and constraints across jurisdictions. There has been an absence of international agreement on what constitutes a cyber-criminal activity. Cybercrime-related legal systems and cultural frameworks vary greatly. For instance, contents that are "obscene" in Arab countries are acceptable in the West. An "obscene" website in the U.K. may be acceptable in Scandinavia. Similarly, regulators in some countries would not condemn activities such as piracy [14]. Likewise, while British, French, and German laws prohibit contents related to race hatred or Holocaust denial, the U.S. Constitution protects free speech.

As to the inter-jurisdictional differences, while political or judicial decision-making may quickly change cybercrime related formal rules, informal constraints related to customs and traditions usually tend to be more durable and persistent. There have been international movements to thicken institutions related to cybercrime and cybersecurity [1,17]. As of February 2014, 48 nations had signed and/or ratified the *Council of Europe's* (CoE) Treaty on cybercrime. Likewise, new laws in Russia and China require domain registration applicants to present photo ID to authorities before new domains are allocated. Despite the existence of laws, however, countries may differ in the development of enforcement mechanisms.

Likewise, proportions of reported cybercrimes may vary across jurisdictions because of statutes and administrative regulations related to reporting. For instance, since 2004, South Korea has mandated that Internet-related hacking incidents must be reported. Likewise, as of 2006, over 30 U.S. states had laws that require businesses to report cybercrimes.

Similarly, the country of origination of a cyber-attack is extremely fuzzy. Many cybercrimes originate in one country but are initiated by criminals in different jurisdictions. The July 2009 cyberattacks on U.S. and South Korean websites, for instance, involved 167,000 compromised computers in 74 countries. A command-and-control server was on an U.K.-based IP address. The master server, which distributed instructions to eight other command-and-control servers, however, was located in the U.S. [8].

A final issue that deserves mention relates to longitudinal comparisons. More recent indicators perform better in terms of comprehensiveness and detail while it is not clear whether accurateness has improved. While the early measures mainly focused on cybercrimes involving technological elements, there are recent attempts to classify in terms of the relative roles of human and technology elements.

There are some metrics related to comparison *vis-à-vis* traditional crimes. A 2009 *Gallup* survey indicated that more U.S. adults were worried about being an identity theft victim than about 11 other crime types [18]. A 2006 IBM survey found that U.S. businesses worry more about cybercrimes than about physical crimes [19].

5. Concluding Comments

The challenge in comparing various surveys conducted to study the cybercrime industry is analogous to the comparison of apples and oranges. This is to say that all metrics related to the cybercrime industry are not the same. This means that when politicians and others refer to "cybercrimes' adverse impacts to the society", different sets of characteristics may be implied in different countries. While the measurement problems associated with the underground economy are equally common and valid for the cybercrime economy, the latter poses additional challenges such as the lack of a universal definition.

As noted earlier, many organizations studying the cybercrime industry have tendency to over- or under-estimate this industry depending upon which side of the issue they would like to emphasize. In this regard, a proper understanding of the contexts, mechanisms and processes associated with various forms of cybercrimes would steer businesses and consumers away from a false sense of risk and/or security.

The cyberspace may not be as dangerous as some consulting companies would regard it to be. Information about cybercrimes provided by players in the electronic market place, however, should not be accepted at the face value. The most obvious danger is that such information may make consumers feel safer than they actually are. In general, organizations and individuals with a greater understanding of cyber-criminals' modus operandi, structure and style of engagement are likely to decrease their chances of being victimized.

The various limitations of existing cybercrime metrics would imply that a proper approach to dealing with cyber-threats is also a matter of knowing what to do with the available information. Businesses and consumers need to use various techniques to evaluate, sort out and filter the information from various sources in order to obtain a truer assessment of the risks associate with various forms of cybercrimes. If estimates from multiple sources exist for a given indicator, it is wise to rely more on the source that is likely to be the least biased. In the above example on auction frauds, for instance, EBay's and the FBI's estimates for the same indicator differ by a factor of 100. While there might be arguments regarding law enforcement agencies' tendency to exaggerate the risks and e-commerce companies' motivations to under report frauds associated with their websites, it would be safe to assume that FBI's estimates of the auction fraud risks would be more reliable than those of EBay.

Finally, a significant proportion of cybercrimes that victimize businesses and consumers are in novel and new forms. A phenomenon known as *rare enemy syndrome* [20], provides a helpful perspective for understanding how victims often fall to new unfamiliar baits or lure. Cyber-criminals' manipulations tactics are so rare that victims have not developed an effective counter poison. Businesses and consumers thus need to consider unusual online activities as processes associated with

cyber-criminals' new manipulative techniques. In many cases, metrics might have been developed to capture such activities.

References

1. Kshetri, N. *Cybercrime and Cybersecurity in the Global South*; Palgrave Macmillan: Houndmills, Basingstoke, UK, 2013.
2. Naylor, R.T. The Rise and Fall of the Underground Economy. *BJWA* **2005**, *11*, 131–143.
3. Kshetri, N. Positive externality, increasing returns and the rise in cybercrimes. *CACM* **2009**, *52*, 141–144.
4. Moore, R. *Cybercrime: Investigating High-Technology Computer Crime*; Anderson Publishing: Burlington, MA, USA, 2011.
5. McDonald, T. Report: Year's Hack Attacks To Cost $1.6 Trillion. In *E-Commerce Times*, 11 July 2000. Available online: http://www.ecommercetimes.com/story/3741.html?wlc=1257274891 (accessed on 20 December 2012).
6. Winning at eBay: How to bid smart & play safe. *Consumer Reports* **2007**, *72*, 12–14.
7. Bauerly, R.J. Online auction fraud and eBay. *Mark. Manag. J.* **2009**, *19*, 133–143.
8. IC3. *Internet Fraud Crime Report*, 1 January 2006–31 December 2006; National White Collar Crime Center and the Federal Bureau of Investigation, 2007. Available online: www.ic3.gov/media/annualreport/2006_IC3Report.pdf (accessed on 20 December 2012).
9. Kshetri, N. The economics of click fraud. *IEEE Secur. Priv.* **2010**, *8*, 18–26.
10. Roush, W. The internet reborn: The internet has transformed the way we find information, shop, and do business. But it is a dumb network built for a bygone age. A university-industry coalition is designing a vastly smarter and more secure Internet: PlanetLab. *Technol. Rev.* **2003**, 28–37.
11. Mitra, D. Endogenous Lobby formation and endogenous protection: A long-run model of trade policy determination. *Am. Econ. Rev.* **1999**, *89*, 1116–1134.
12. David, F. Building the infrastructure of anti-trafficking: Information, funding, responses. *Criminol. Pub. Policy* **2010**, *9*, 235–243.
13. Brown, E.F. Development of international norms for insurance regulation. *Brook. J. Int'l L.* **2008**, *34*, 953–955.
14. Rho, J. Blackbeards of the twenty-first century: Holding cybercriminals liable under the alien tort statute. *Chi. J. Int'l L.* **2007**, *7*, 695–719.
15. Kshetri, N. *The Global Cyber-Crime Industry: Economic, Institutional and Strategic Perspectives*; Springer-Verlag: Heidelberg, Germany, 2010.
16. The Government Accountability Office. *Public and Private Entities Face Challenges in Addressing Cyber Threats*; RPT-NUMBER: GAO-07–705; GAO Reports: Washington, DC, USA, 2007.
17. Kirk, J. Countries Move Forward on Cybercrime Treaty. *PC World*, 11 March 2009. Available online: http://www.pcworld.com/article/161067/countries_move_forward_on_cybercrime_treaty.html (accessed on 20 December 2012).

18. Saad, L. Two in three Americans worry about identity theft. *Gallup*; 16 October 2009. Available online: http://www.gallup.com/poll/123713/Two-in-Three-Americans-Worry-About-Identity-Theft.aspx (accessed on 20 December 2012).
19. When the Law Chases the Internet. *Christian Science Monitor*, 17 March 2006.
20. Dawkins, R. *The Extended Phenotype*; Oxford University Press: New York, NY, USA, 1982.