The Smuggling Theory Approach to Organized Digital Crime

Vaibhav Garg
School of Informatics and Computing
Indiana University
Bloomington, IN 47408
Email: gargv@indiana.edu

Nathaniel Husted
School of Informatics and Computing
Indiana University
Bloomington, IN 47408
Email: nhusted@indiana.edu

Jean Camp
School of Informatics and Computing
Indiana University
Bloomington, IN 47408
Email: ljcamp@indiana.edu

***Abstract*—Governments and inter-governmental organizations are developing cross-jurisdictional mechanisms to decrease global digital crime. The underlying assumption is that the loss incurred from ODC decreases social welfare in every jurisdiction. In this paper we test this assumption by using a framework from economic theory that addresses smuggling in the physical world. Using botnets as a case study we argue that ODC is analogous to smuggling. We then enumerate the conditions under which a model of ODC as smuggling leads to an increase in social welfare using a classic economic model of smuggling. Thus, we show that to the extent ODC is comparable to smuggling, there are situations where ODC increases social welfare. This implies that there will always be some jurisdictions or locales where ODC could rationally be supported. One possible policy implication is that jurisdictions should invest in domestic network reliance and securing the machines within their own jurisdictions.**

I. Introduction

The Internet is a not a safe place. The list of online risks faced by an end user is extensive. Initially, digital crime was a niche for the technically adept. The advancement of technology, however, has made it easier for people with limited technical prowess to profit from digital crime. The increasing revenue from these activities has changed the nature of the crime from being individual ego-driven to a group profit-driven activity with the advent of Organized Digital Crime (ODC) [1], [2], [3]. ODC, based on estimates from various studies, causes significant losses to institutions and individuals alike [2]. To prevent these losses, many countries, including United States and those in the European Union, are developing legislation, international cooperative agreements, and supporting NGOs to curb these activities by reducing incentives and/or increasing penalties [4].

Choo et al. [1] provide an overview of online organized crime in their paper. They discuss three different categories of organized criminal groups operating on the Internet. They include traditional organized crime groups, organized groups of cyber criminals, and organized groups of ideologically and politically motivated individuals. The notion of organized crime being involved in illicit Internet activity is also mentioned by Moore [2]. They find that the annual loss due to phishing, and possible gain to phishers, is $178.1 million dollars a year. Other profit making activities include selling trojan making packages, credit card numbers, and other personally identifiable information [5].

Researchers are trying to analyze the impact of enforcement on such criminal activity. Png et al. [6] found that increased enforcement reduces attacks against computer networks by an average of 36% during a fifteen day window. This implies that theoretically it would be possible to have enforcement levels that would reduce online crime to zero. Li et al. [4] investigated the use of uncertainty in order to reduce the profits generated by botnet masters and those renting the botnets. While the former paper looks at legal enforcement the latter looks at a technical enforcement. The underlying assumption of enforcement, both technical and otherwise, is that losses incurred due to ODC are bad for the society i.e. it reduces social welfare. This assumption is, however, largely unexamined.

In this paper, we argue that certain ODC activities are analogous to smuggling in the physical world. For example, botnets are an illegal alternative to legitimate networked services. There is evidence that legitimate networked services such as cloud computing can be used by ODC agents to conduct the same illegal activities as with botnets[1]. We analyze the social welfare provided by ODC under a framework of economic theory developed to study smuggling in the physical world. For the purpose of this paper we will refer to this framework as *smuggling theory*. Using smuggling theory we show that under certain conditions, enforcement against ODC can decrease social welfare in geographic areas where ODC agents are based. This has been shown true in at least one case with ODC leading to higher social welfare in the town of Râmnicu Vâlcea in Romania[2]. This social welfare, however, is limited to the local economy of ODC actors' immediate jurisdiction. Section II demonstrates how certain ODC have the same economic properties as offline smuggling. In section III we introduce the motivation for our approach as well as

[1]http://cacm.acm.org/news/109938-botclouds-a-cyberattackers-dream/fulltext, *July 19th, 2011*

[2]http://www.wired.com/magazine/2011/01/ff_hackerville_romania/, *Last accessed: July 19th, 2011*

978-1-4577-1339-2/11/$26.00 2011 IEEE

smuggling theory as applied to smuggling offline. In section IV we apply smuggling theory to ODC. In section V we discuss the limitations of our work and the implications of our findings. Section VI concludes and discusses future work.

II. eSMUGGLING

Smuggling is the act of the clandestine transportation of goods in or out of a country illegally. This practice allows the smuggler to bypass the tariffs (e.g. import duties) in the target country and sell the goods at a lower price than the legal market would allow for. Prohibition is effectively an extreme form of tariff. The economic losses incurred from this activity, due to lost tax revenue, were traditionally considered to be bad for all parties. While similar analogies for security may not be perfect, there are several instances of shared attributes between legal online services and digital crime. Here we argue for botnets as an illegal analogue of legitimate networked services. While legitimate networked services and botnets are not perfectly analogous, they share several attributes that we enumerate in this section. We further discuss the limitations of this analogy and the implications for our results in Sec. V.

Botnets are being used for various illegal activities like spam, phishing and distributed denial of service attacks. ODC agents have used botnets as a way to harvest computation power to launch bigger attacks. The IMDDOS botnet has even started selling its services as 'pressure test software'[3]. It would be a small jump for botnet masters to open their botnets to other services for pay. While botnets have been used for illicit activity in a vertically integrated structure, the portfolio of services being offered is becoming more diverse. As botnets become more prevalent and the ODC community becomes better structured, it would not be a stretch to assume botnet masters would increasingly offer legitimate services to generate revenue.

The legal analog to a botnet is a legitimate networked service. Legitimate networked services, similar to botnets, are used to harness the power of several machines in a network. Legitimate networked services harvest computational power legally and the platform owner is aware that its resources are being used. For botnets, however, the individual 'bots' and their users tend to be unaware that their resources are being used by someone else. Thus, the physical resource cost to the legitimate provider is more expensive than to the botnet master. While the legitimate provider must pay infrastructure and production costs, the botnet master is not so constrained. While botnet masters may bear the additional cost of criminal prosecution, there is little evidence to suggest that such costs are accounted for when pricing for services. Criminals when prosecuted are forced to surrender all profits generated through the respective illegal activities. Thus, there is little rationale to account for these costs. Botnet masters do, however, bear the cost of capturing a bot. It is, however, reasonable to assume that these costs are lower than purchasing an additional system. If this were not true, botnets would not exist under classical economic theory. New evidence suggests that botnet masters are buying individual bots, just as legal networked services would purchase individual systems[4]. The cost to recruit bots would, however, be mediated by the existing vulnerability market. It must be noted that these costs are *considerably different* than the cost to the end-consumer themselves. Determining the social optimum of botnet computation pricing is beyond the scope of this paper.

Botnets and legitimate networked services both provide computational power and thus can provide similar services. They can both be used for 'good' or 'bad' purposes. For example both botnets and legitimate networked services can be harvested to break WPA passwords[5][6] and for other password cracking activities[7]. The Amazon cloud was even used to temporarily host the WikiLeaks website during the U.S. cable leak incident[8]. While Amazon claims such illicit uses are against its policies, it is unlikely that Amazon actively monitors all processes running on its cloud. It is computationally infeasible for Amazon to determine the exact purpose and functionality of all these processes. Thus, one cannot make a definitive argument that legitimate networked services will never be used for illicit activities. While legitimate networked services have to pay tariffs, e.g. infrastructure costs, botnets provide a mechanism to avoid those tariffs. Thus, by comparing botnets to legitimate networked services, it can be argued that certain ODC activities are analogous to smuggling. We note that botnets provide anonymous services, under which the price of self-authentication and accountability could be considered a part of the price of legitimate networked services. In general, whenever an ODC activity allows avoidance of tariffs (monetary or otherwise), we observe the creation of a smuggled analog of the legal good or service. Thus certain ODC activities, termed as eSmuggling, are analogous to smuggling as a Directly Unproductive Profit (DUP) seeking activity [7]. Thus, like smuggling, it is possible that these can paradoxically increase the social welfare in areas where smugglers spend their ill-gotten gains.

Avoidance of tariffs due to ODC activities, similar to smuggling, results in loss of trade gain. However, they also lead to an increase in production gain and consumption gain. Specifically the impact on production gain for digital goods would be much higher than for real goods since the marginal cost of producing digital goods approaches zero. The goal of enforcement, legal, technical or otherwise, is to raise the cost of ODC (eSmuggling) or make the transformation curve less

[3]http://www.damballa.com/downloads/r_pubs/Damballa_Report_IMDDOS.pdf, *Last accessed: July 19th, 2011*

[4]http://www.boingboing.net/2011/04/08/marketplace-for-hija.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed\%3A+boingboing\%2FiBag+(Boing+Boing) Last Accessed: July 19th, 2011

[5]http://www.securecomputing.net.au/News/162378,ethical-hacker-starts-wpa-cloud-cracking-service.aspx, *Last accessed: July 19th, 2011*

[6]http://www.reuters.com/article/2011/01/07/us-amazon-hacking-idUKTRE70641M20110107, *Last accessed: July 19th, 2011*

[7]http://www.darknet.org.uk/2009/11/using-cloud-computing-to-crack-passwords-amazons-ec2/, *Last accessed: July 19th, 2011*

[8]http://www.guardian.co.uk/technology/2010/nov/29/wikileaks-amazon-ec2-ddos, *Last accessed: July 19th, 2011*

favorable to the terms of trade and thereby lead to a decrease in ODC (eSmuggling). Thus enforcement against ODC activities is analogous to confiscations and fines against smuggling.

We must also demarcate between *socially desirable* and *social welfare increasing*. For example, weapons or illicit substance may not be socially desirable. Smuggling prevents redistribution through tariffs and allows direct welfare transfer from one jurisdiction to another. It is a mechanism for tax evasion or prohibition evasion. Thus, smuggling of weapons or illicit substances is not socially desirable but may increase social welfare as it prevents redistribution through tariffs or concentrates wealth in one jurisdiction. Similarly, ODC activities such as spam or 419 scams are not socially desirable but can increase social welfare in local jurisdictions.

III. Computer Crime And Its Relation To Smuggling Theory

Information security was traditionally considered a technical problem. Anderson [8] demonstrated that security is mediated not only through technology but also by the incentives that individuals and institutions have to protect themselves and others (and the lack thereof) [9]. Digital Crime enjoys the advantage of the weakest link [10]. There is often little incentive for individuals to protect themselves, as they are not directly effected, rather their systems are used to attack institutions. Kunreuther et al. [11] further question the incentives for an institution to invest in an endeavor where success depends on the actions of others. While there may be little incentive to defend, the incentives for attackers have become stronger with a paradigm shift from 'hacking for fun' to 'hacking for profit' [5]. Thomas et al. [3] provide a detailed description of how the underground economy utilizes tools like IRC channels for cooperation and collaboration between individuals who indulge in digital crime. They provide examples of different activities that are involved in profiting from digital crime including discussions about offshore accounts where the money earned through such illicit means could be transferred.

Lack of empirical data, however, makes it difficult to evaluate the impact of security proposals. There has traditionally been a lack of incentives for organizations to disclose security breaches [9]. The current state of security reporting is poor and suffers from the lack of a central clearinghouse where all the data would be stored. Thus, we need to complement empirical research endeavors with theoretical models that help to predict the outcomes of policy and legislation against ODC. This includes research into how enforcement effects the social welfare of countries with ODC groups. Classic economic models have been criticized for being reductionist and thereby providing an inaccurate or incomplete picture of real world behavior. This is, however, a limitation of any scientific approach that is reductionist by nature and precludes assumptions to facilitate analysis. Irrespective of whether these models reflect real life behavior, we feel that applying macroeconomic theories of trade to digital crime can often provide critical insights to inform both policy and empirical research.

The traditional viewpoint held in the macroeconomics of smuggling was that it reduced social welfare. This is similar to the traditional view amongst the security community when discussing the social welfare provided by digital criminals. However, the view on smuggling's effect on social welfare has changed. For smuggling, this premise was first tested in the seminal paper by Bhagwati et al. [12]. They used a model based on international trade and welfare economics[9] to show that smuggling can increase social welfare and the lack of anti-smuggling regulations can be desirable. They consider smuggling as a transformation of exportable goods to importable goods. The corresponding transformation curve is considered less favorable than the terms of trade. They also assume perfect competition leading to two traded goods and fixed terms of trade. They argue that the loss due to smuggling, i.e. trade loss, can be compensated or even surpassed by production and consumption gains. In particular they state that when tariffs are excessively high, smuggling is superior to no smuggling. The limitation of the model is that it presumes legal trade, smuggling, and price disparity cannot coexist. If legal trade and smuggling coexists then smuggling always lowers welfare under their model. These assumptions are highly restrictive since in a realistic situation legal trade and smuggling would coexist.

Thus, Pitt [13] proposed that legal trade must necessarily exist to allow smuggling. Despite a less restrictive model, Pitt concluded that smuggling can increase welfare. In particular, if the cost of smuggling is fines and confiscation, and the fines are not equivalent to tariffs, then smuggling is welfare increasing. He also argued that if lowering smuggling is costless then maximizing tax revenue might require a certain amount of smuggling. In this paper, we use the argument presented by Bhagwati et al. in light of ODC with botnets as a case study of a smuggled analog to legitimate networked services. We use this model due to the foundational nature of the work that would allow us to further our conclusions through later works such as Pitt[13] and Lovely et al. [14].

IV. eSmuggling and Smuggling Theory

Here we translate the model proposed by Bhagwati et al. [12] and apply it to botnets as a smuggled analog of legitimate networked services. Similar to the original model, we assume perfect competition between two traded goods, botnets and legitimate networked services, where legitimate networked services are the exports and botnets are the now transformed imports. We also assume that ODC actors are operational in a nation based on the observation that many botnets can be traced back to a single region, e.g. GhostNet[10], Zeus2[11]. This paper assumes a well-behaved community indifference map. This means that utility is monotonic as well as continuous

[9]Bhagwati et al. use the Hicks-Samuelson value theoretic framework

[10]http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network, *Last accessed: July 19th, 2011*

[11]http://www.theinquirer.net/inquirer/news/1726221/zeus-botnet-spotted-wild, *Last accessed: July 19th, 2011*

and the consumer does not prefer one good over the other[12]. Just like in the original paper this has been assumed only to facilitate exposition and our conclusions would be valid without it. For convenience we assume a constant rate of transformation. Our model also assumes that an increase in enforcement against ODC activities representing eSmuggling would act as fines or confiscations against smuggling. We assume that individuals will rationally choose illicit behavior if it provides a greater monetary benefit than abiding by the law. This situation could arise in countries where regulations cause the costs of providing online services to be higher than the revenue that a business could reasonably produce and the probability of being subject to enforcement is low. ODC would decrease the demand for legitimate markets in the purchase of computational resources or bandwidth. However, the profits generated would likely be reintroduced in the local economy to support the lifestyles of the ODC actors. Unlike the original model, the trade-and-transformation curves are assumed to be convex i.e. bulging in towards the origin. We make this assumption since running a botnet or a legitimate networked services requires similar skills, thus the opportunity costs are either constant or decreasing[13]

a) Notation:: The two goods in this paper are exports or legitimate networked services (C) and transformed imports or illegal networked services in the form of botnets (B). We assume that an increase in demand for botnets would lead to a decrease in demand for legitimate networked services[14]. We hypothesize that ODC activities, representing eSmuggling being analogous to smuggling, are illegal activities both initially and finally distorted[15]. Thus ODC activities can paradoxically lead to increased welfare [7]. P_T and P_S are used to represent the production points on the Trade-and-Transformation Curve[16] in each figure. P_T represents the optimum production point of legal trade. P_S is the desirable production point for smuggling. U_T and U_S are the corresponding utility curves. C_T and C_S are the respective cost points. Tangential to C_T and C_S are the corresponding price lines.

[12]A counter example would be of cars. As a car gets older its value decreases. However, a really old car becomes an antique and the value increases.

[13]This is a deviation from the analysis presented by Bhagwati et al. [12]. They assume that opportunity costs are increasing. Their assumption is for physical goods. For most digital goods, specifically for botnets and legitimate networked services, individuals with similar skill sets would be considered experts, i.e. the same individuals who would maximize production in botnets would be able to maximize production for legitimate networked services. Thus, opportunity costs to transform goods from botnet to legitimate networked services would either be constant or decreasing.

[14]Alternatively, if an increase in demand for botnets would cause the demand for legitimate networked services to increase or remain constant, ODC would always lead to more welfare since there would never be any trade loss.

[15]Distortion implies a deviation from perfect competition that causes suboptimal social welfare when individual welfare is maximized.

[16]A transformation curve also known as production possibility curve shows the amount of two goods or services that can be produced by an entity, e.g. a country. The two good or services are in competition, i.e. they need the same resources for production. Due to this competition, the increase in production of one would lead to a decrease in production of another.

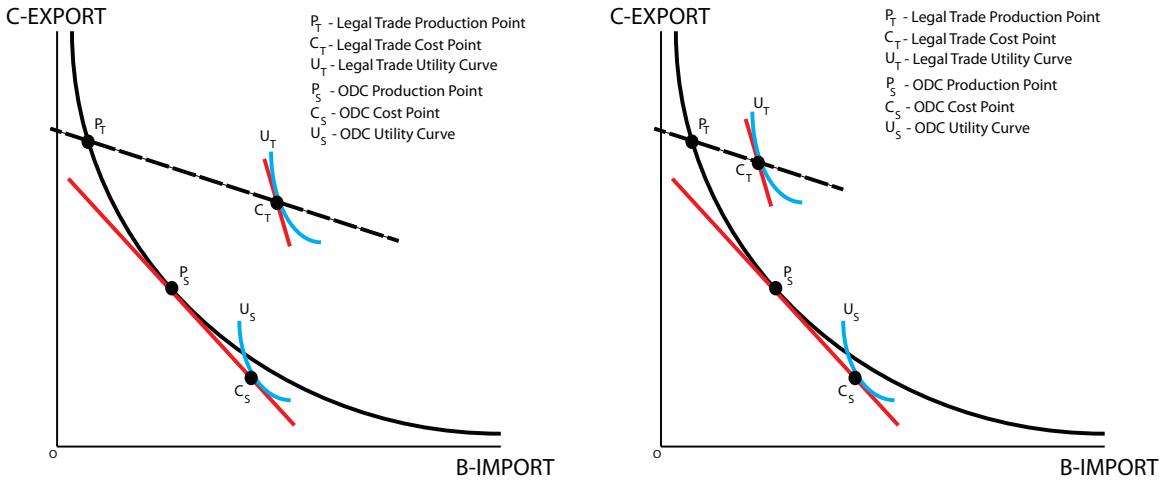
Notation Summary	
P_T	Legal Trade Production Point
C_T	Legal Trade Cost Point
U_T	Legal Trade Utility Curve
P_S	ODC Production Point
C_S	ODC Cost Point
U_S	ODC Utility Curve

TABLE I: Summary of the notation used in Trade-and-Transformation Curves

b) Constant Costs:: Here we consider two cases: either the utility of legal trade or the utility of eSmuggling is higher. In Fig. 1a, the utility of legal trade is higher. In Fig. 1b, the utility of eSmuggling is higher than legal trade. While in the former case $C_T > C_S$ in the latter $C_T < C_S$. Thus, based on whether the utility derived from legal trade is higher or lower than eSmuggling, ODC can be welfare reducing or welfare increasing. In both the cases the price line for eSmuggling has a more gradual slope than that of legal trade. When there are constant costs, eSmuggling is likely to suppress legal trade. Conversely, if the constant costs for ODC agents are lower than legal trade then eSmuggling would be supplanted by legal trade.

c) Decreasing Costs:: In the previous section we considered a constant cost of production. In reality, the cost of production in regards to digital goods is almost always decreasing over time. For legitimate networked services, the cost of the first transaction, or computational unit sold, is extremely high as it includes the cost of building the data center and purchasing servers. Each subsequent transaction has a negligible cost in comparison, as it only must account for the cost of electricity. For botnets, the first transaction too, has a high cost as it must account for the costs associated with forming the botnet. Each subsequent transaction has a negligible cost in comparison as it must only account for the cost of managing the botnet and membership churn. The price lines for digital goods would tend to become nearly asymptotic due to decreased costs of production over time. In Fig. 2a both legal trade and botnets have costs decreasing at an equal rate, though utility from legal trade is higher. In Fig. 2b the utility from legal trade is lower compared to botnets. From Fig. 2a and 2b, it is unclear whether eSmuggling reduces social welfare. The results are similar to those seen for constant costs.

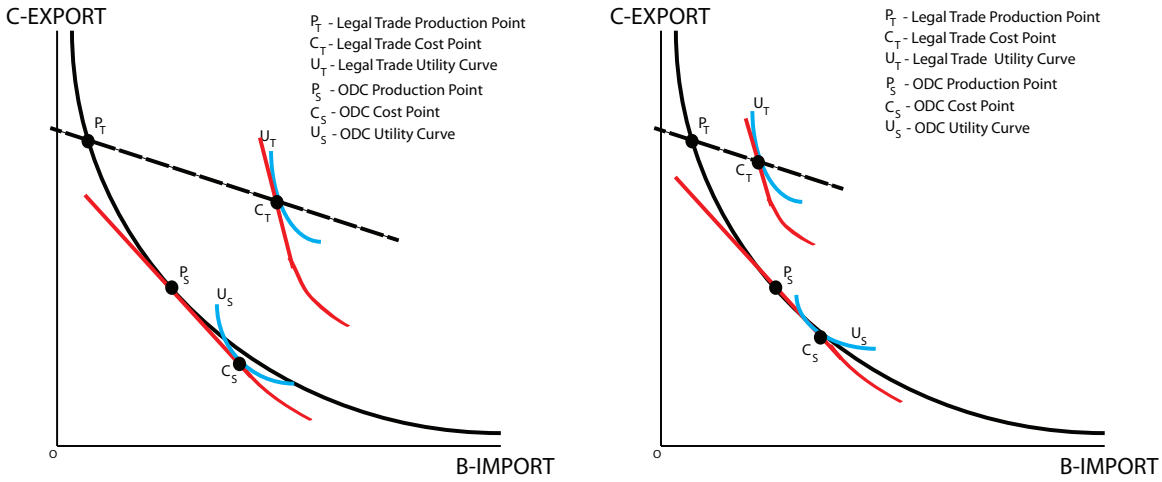
d) Unequal Decreasing Costs:: In the previous section we assumed that the rate of decreasing costs for both legal trade and botnets would be equal, i.e. the rate of change of slope of the price lines for both legal trade and botnets would be equal. A more realistic scenario is one where botnet costs decrease faster than legal trade. The faster decrease in botnet costs is due to legitimate networked services' higher marginal costs of production per transaction. Legitimate networked services would have to pay for infrastructure upkeep, electricity, bandwidth, and other costs. Conversely, marginal costs of production for botnets are lower since they are not paying for either the physical systems, the electricity,



(a) Inexpensive Legitimate Networked Services

(b) Expensive Legitimate Networked Services

Fig. 1: Perfect Competition at Constant Costs



(a) Inexpensive Legitimate Networked Services

(b) Expensive Legitimate Networked Services

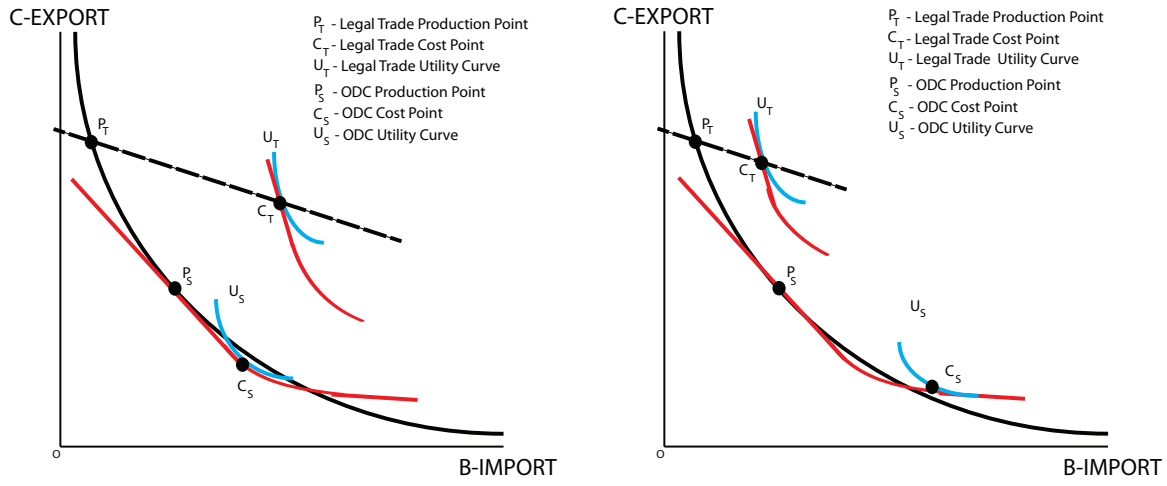
Fig. 2: Perfect Competition at Decreasing Costs

or the bandwidth. Figures 3a and 3b show that it is again unclear whether eSmuggling reduces social welfare as in the previous cases. However, due to sharper decreasing costs for eSmuggling than for legal trade, at some point eSmuggling would always supplant (in fact, theoretically eliminate) legal trade. In the case of eSmuggling supplanting legal trade, ODC would always be welfare increasing. For decreasing costs and perfect competition, eSmuggling can always be scaled to decrease legal trade and become welfare increasing. The policy implication here is that when legitimate network services and ODC co-exist, it is imperative to keep ODC growth in check to avoid an equilibrium that favors ODC. Thus, anti-ODC policies as well as technical measures would be desirable to counter ODC.

V. Discussion

From the analysis given above, *we infer that ODC is not always welfare reducing*[17]. In particular, *ODC is welfare increasing when the utility derived from legal trade is less than from illegal alternatives*. ODC is also always welfare increasing in case of prohibitive tariffs. Prohibitive tariffs, in terms of inadequate digital infrastructure or existing inexpensive illegal trade, would impede the development of legal alternatives. In general there are nations that currently do not have large network services industries or high levels of network readiness,

[17]We must note that the social welfare under discussion is generated from the profits made from selling services rather than by the use of these services. For example, we are considering the revenue generated by botnets rather than that generated by spam sent using those botnets.



(a) Inexpensive Legitimate Networked Services

(b) Expensive Legitimate Networked Services

Fig. 3: Perfect Competition at Unequal Decreasing Costs

but have a disproportionately high number of bot-masters[18]. Those countries would suffer from reduced social welfare in the near term if they either encouraged legitimate networked services as an industry, enforced laws against botnets, or both. These nations have no near term incentive to crack down on ODC agents. For countries where legal trade dominates the market, as long as eSmuggling is not allowed to scale to a point where the utility derived from eSmuggling is higher, social welfare would increase with higher enforcement. Due to the nature of digital goods, we have decreasing costs for both legal and ODC agents. In situations of decreasing costs, it is much more likely that ODC would suppress legal alternatives. In this paper, we take the example of botnets. However, for other ODC activities, like widespread copyright violations, this effect could be more pronounced since not only marginal costs for production are approximately zero, but for the ODC agent the cost of getting the first copy would also be almost negligible[19].

We are left with the question of why ODC activities have not destroyed the legal market? This model does not not take into account the qualitative difference in the nature of transactions done on legitimate networked services as opposed to botnets. Transactions made on botnets provide anonymity. This may not be true for legal services where an enterprise such as Amazon would store credit card details. Amazon can also be subpoenaed. We assumed that botnets and legitimate networked services are the same good. This not entirely correct. Legitimate networked services or legal trade provides services like trust and reliability. This is not necessarily true for botnets. For example, there would never be a botnet based Google Docs because no person would trust their sensitive documents to an entity that is criminal in nature. For certain ODC activities the illegal alternative might not be a substitute but a complementary good or service. In the case of botnets, they might offer computational services that legitimate networked services would not offer due to legal reasons. For such activities a different economic framework, for example those used to study the market of legal vs. illegal drugs, may provide a better insight. However, we posit that legitimate networked services and botnets offer some set of services that provide equal value on either platform: processing power, data hosting etc.

We find that the more IT is developed and available, the less interested the local market would be in having IT crime. It would both be desirable and socially optimum to have legislation that prohibits ODC. However, if crime is the driving cost then there would be an enforced scarcity for legal alternatives. The existing illegal market would act as a prohibitive tariff distorting the incentives for the legal market. Thus, the counterintuitive policy implication is that when ODC dominates legal alternatives, it would be social welfare decreasing to suppress digital crime.

VI. Conclusion & Future Work

The problem of investment in security has been widely studied. Schneier argues that individual decision-makers prefer uncertain larger loss over certain smaller loss [16]. Thus, individual decision-makers would have limited incentive to invest. Similarly, Varian recognizes the problem of the free rider on an organizational level. Thus, in a free market private entities would be likely to underinvest in security [17]. In this paper, we present another scenario where the incentive to invest in security for a public body are acted upon by improved local social welfare.

Nigerian 419 scams provide one such example. While these scams have universally been recognized as criminal

[18]Bot-masters manage botnets and are the primary beneficiaries of the botnet's profits.

[19]In contrast, copyright violations can also serve as a complement rather than substitute to the legal market [15].

activities and the perpetrators as criminals, there has been limited effort by the Nigerian government to fix the legal loophole that allows the continuation of this activity. From a Nigerian perspective this activity welfare increasing as it bring in a significant amount of money, while it only harms the citizens of other countries. Thus, there is little incentive for the Nigerian government to act. Similarly, with most botnets the systems impacted are located outside the jurisdiction of the local law enforcement. At the same time the botnet masters generate significant revenue that is introduced into the local economy thus improving local social welfare.

A similar anti-intuitive result is also presented by Osorio [18]. With respect to illegal vs. legal copies of software, Osorio notes that ignoring software piracy in countries with emerging IT markets would be a profit increasing in the long term. If such free, though illegal copies of copyrighted software are not available those countries would rationally choose to adopt either open source or lower priced alternatives.

The conclusions of this work are limited by the assumptions of the original model by Baghwati et al. In particular, the assumption that legal trade and smuggling can not coexist is not applicable to ODC as can be seen from botnets existing as the illegal analog of legitimate networked services. The analysis is also limited in that botnets and legitimate networked services are not perfectly analogous. More realistic models as presented by Pitt [13] and Lovely et al. [14] make stronger statements about the increase in welfare seen due to smuggling. We anticipate that the application of these models to ODC would further strengthen our results and bring them closer to observed phenomenon. Further, insight will be provided by considering botnets and legal networked services under the rubric of monopolistic competition [19] as well as game theoretic approaches to investment [20].

In this paper we have presented an argument for considering ODC as a digital equivalent of real world smuggling. Using the economic frameworks used to analyze smuggling we further show that enforcement against ODC is not always desirable as there may be conditions under which ODC would lead to an increase in welfare. We show that for digital goods and services, illegal alternatives could suppress legal trade. For countries that do not have a legal market, ODC would lead to increased welfare and therefore there is no incentive for them to enforce anti-ODC laws.

VII. Acknowledgements

The authors would like to thank Mr. Shaunak Dabadghao who provided necessary insights into our analysis.

References

[1] K. Choo and R. Smith, "Criminal exploitation of online systems by organised crime groups," *Asian Journal of Criminology*, vol. 3, no. 1, pp. 37–59, 2008.

[2] T. Moore and R. Clayton, "An empirical analysis of the current state of phishing attack and defence," in *Workshop on the Economics of Information Security*. Citeseer, 2007.

[3] R. Thomas and J. Martin, "The underground economy: priceless," *USENIX; login*, vol. 31, no. 6, pp. 7–16, 2006.

[4] Z. Li, Q. Liao, and A. Striegel, "Botnet economics: uncertainty matters," *Managing Information Risk and the Economics of Security*, pp. 245–267, 2009.

[5] J. Franklin, V. Paxson, A. Perrig, and S. Savage, "An inquiry into the nature and causes of the wealth of internet miscreants," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*. Citeseer, 2007.

[6] I. Png and C. Wang, "The Deterrent Effect of Enforcement Against Computer Hackers: Cross-Country Evidence," in *WEIS 2007-Sixth Workshop on Economics of Information Security*. Citeseer, 2007, pp. 7–8.

[7] J. Bhagwati, "Directly unproductive, profit-seeking (DUP) activities," *The Journal of Political Economy*, vol. 90, no. 5, pp. 988–1002, 1982.

[8] R. Anderson, "Why information security is hard-an economic perspective," in *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*, 2001, pp. 358–365.

[9] T. Moore, R. Clayton, and R. Anderson, "The economics of online crime," *The Journal of Economic Perspectives*, vol. 23, no. 3, pp. 3–20, 2009.

[10] J. Hirshleifer, "From weakest-link to best-shot: The voluntary provision of public goods," *Public Choice*, vol. 41, no. 3, pp. 371–386, 1983.

[11] H. Kunreuther and G. Heal, "Interdependent security," *Journal of Risk and Uncertainty*, vol. 26, no. 2, pp. 231–249, 2003.

[12] J. Bhagwati and B. Hansen, "A theoretical analysis of smuggling," *The Quarterly Journal of Economics*, vol. 87, no. 2, pp. 172–187, 1973.

[13] M. Pitt, "Smuggling and price disparity," *Journal of International Economics*, vol. 11, no. 4, pp. 447–458, 1981.

[14] M. Lovely and D. Nelson, "Smuggling and welfare in a Ricardo-Viner economy," *Studies*, vol. 22, p. 6, 1995.

[15] M. D. Smith and R. Telang, "Competing with Free: The Impact of Movie Broadcasts on DVD Sales and Internet Piracy," *SSRN eLibrary*, 2008.

[16] B. Schneier, "The psychology of security," in *Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology*. Springer-Verlag, 2008, pp. 50–79.

[17] H. Varian, "System reliability and free riding," *Economics of Information Security*, pp. 1–15, 2004.

[18] C. Osorio, "A contribution to the understanding of illegal copying of software," *Levines working paper archive, David K. Levine*, 2003.

[19] A. Dixit and J. Stiglitz, "Monopolistic competition and optimum product diversity," *The American Economic Review*, vol. 67, no. 3, pp. 297–308, 1977.

[20] K. Lye and J. Wing, "Game strategies in network security," *International Journal of Information Security*, vol. 4, no. 1, pp. 71–86, 2005.