# Honor Among Thieves: A Common's Analysis of Cybercrime Economies

Sadia Afroz*, Vaibhav Garg*, Damon McCoy† and Rachel Greenstadt*
*Drexel University
†George Mason University
sadia.afroz@drexel.edu, me@vaibhavgarg.net, mccoy@cs.gmu.edu, greenie@cs.drexel.edu

***Abstract*—Underground forums enable technical innovation among criminals as well as allow for specialization, thereby making cybercrime economically efficient. The success of these forums is contingent on collective action twixt a variety of stakeholders. What distinguishes sustainable forums from those that fail? We begin to address these questions by examining underground forums under an economic framework that has been used to prescribe institutional choices in other domains, such as fisheries and forests. This framework examines the sustainability of cybercrime forums given a self governance model for a common-pool resource. We analyze five distinct forums: AntiChat (AC), BadHackerZ (BH), BlackhatWorld (BW), Carders (CC), and L33tCrew (LC). Our analyses indicate that successful/sustainable forums: 1) have easy/cheap community monitoring, 2) show moderate increase in new members, 3) do not witness reduced connectivity as the network size increases, 4) limit privileged access, and 5) enforce bans or fines on offending members. We define success as forums demonstrating small world effect.**

## I. Introduction

Cybercrime is singular in that criminals collaborate with each other, providing competitive services, such as technical insight for attacks, goods, e.g. rootkits, albeit for a price. This collaboration is enabled by underground forums, which are essentially markets for criminals online to sell credit card numbers, botnets etc. These forums often specialize; for example, Carders is a forum that specializes in harvesting information regarding stolen credit card numbers and then monetizing it [1]. These forums are primarily analyzed as markets; a complementary perspective considers these forums as self organizing communities, which are governed by social norms twixt distinct stakeholders. In this paper, we analyze these underground communities of cyber-criminals under an economic framework, which prescribes five conditions for such communities to self-govern and be sustainable [2].

It has been noted that cybercrime is no longer an individual ego driven phenomena, instead it is now organized and profit driven [3]. What form does this organization take? A widely studied phenomena is that underground forums allow cyber-criminals to do technical innovation and reduce the cost of engaging in cybercrime through specialization [3]. The benefits of specialization in an industry are well documented [4] as well as that of specialized individuals to self organize as firms [5].

The assumption underlying much of the anti-cybercrime effort, both academic and practitioner, is that criminals are economically motivated [3], [6]. Thus, the proposed solutions are typically grounded in deterrence theory of crime, i.e. the goal is to either reduce the revenues from crime or increase its costs. Deterrence itself when successful leads to organized crime as then the interactions between criminals and law enforcement become repeated transactions which can be manipulated [7]; for example, through corruption of enforcement officials. This has been noted for cybercrime as well. For example, as the cost of sending spam has increased due to technical measures like black listing, it has become critical for spam and scam architecture to be vertically integrated to be economically feasible [8].

Previous work, thus, establishes both the need for and the existence of collaboration or organization between cyber-criminals. The nature of this organization is, however, understudied. In this paper we begin to study collaboration between cyber-criminals by grounding it in the theoretical foundation of commons governance through local stakeholders [2]; this framework would be referred to as Ostrom's framework as it is grounded in Elinor Ostrom's seminal research [9]. Typical application of this theoretical framework to resources such as fisheries and forests have been useful in developing novel policy responses for sustainability [10]. Here, we examine whether this framework can explain successful underground forums and contrast them with those that fail. Most analyses of cybercrime ask whether crime is profitable. Our contribution is asking the distinct but complementary question- **are cybercrime communities sustainable?**

We begin by introducing the related work. In the following section we describe Ostrom's economic framework of commons governance through local stakeholders. Then we analyze five underground forums under Ostrom's framework. We discuss the implications of our analysis. Specifically we provide technical and policy insights for both public stakeholders such as law enforcement as well as private agents, e.g. Microsoft, McAfee. We conclude with proposal of future work and reification of key findings.

## II. Related Work

Information security problems while technical in nature are significantly impinged by economics [11]. From a defender's perspective anti-cybercrime efforts are constrained by economic resources [12]; for example, it may be rational for most security investments to be reactive rather than proactive [13]. Proactive investments in anti-cybercrime efforts might be economically suboptimal when the loss from criminal activity is not known [14].

On the attacker side, while cybercrime historically began as an individual and ego driven activity, it is argued that today it is both **organized** and **profit driven**. This organization is typically examined as markets; therefore deterrence efforts have concentrated on reducing the profits of cybercrime or increasing the cost of criminal participation. Market based analysis have provided some critical insights: the size of the markets, loss to legitimate entities, potential gain for criminals, and how successful deterrence based efforts have been.

For example, Moore et al. note that the profits from phishing activity may be as high as $178.1 million [15]; Holz et al. [16] estimated the worth of stolen credentials from key loggers and dropzones to be any where between $793,318-$16,604,605. Simultaneously, it has been noted that the cost of sending spam can only be justified if spam and scam infrastructures are vertically integrated; alternatively spamming should be eight times cheaper than it currently is [8]. The need for agencies with specialized skills has even noted in niche cybercrime markets such as dating website fraud [17].

The focus on profits of cybercrime have shaped the response of deterrence strategies, which have primarily targeted attacks rather than attackers. For example, researchers have developed automated techniques for detecting phishing websites [18], malware [19], countermeasures for click fraud [20]. Merely targeting attacks, however, has a limited benefit in deterring cyber-criminals and can even be counterproductive. Nero et al. note that takedown of phishing websites usually happens after the criminals have gathered valuable customer information; simultaneously, these takedowns often forgo forensic information that lead to the arrest of responsible cyber-criminals [21]. Unfortunately, even when individuals are arrested, the deterrence is limited as criminals move to more benevolent jurisdictions [22]. Places where crime is an incumbent industry have limited incentive to prosecute, as criminal activity is locally social welfare increasing [23].

A second perspective targets attacker organization as communities facilitated through underground forums. Given the specialization of cybercrime skill sets, these forums are needed for different attackers to collaborate and provide the entire ecosystem to run, for example, a phishing campaign in a manner that is economically justifiable [24]. A market based perspective of cybercrime examines underground forums as production by firms [5]. Firms exist to reduce transaction costs and business overhead. Schelling [25] and Dick [26] argue that criminal organizations provide similar services to criminals, who incur higher transaction costs because they cannot rely on the legal system to enforce contracts and must spend resources avoiding law enforcement. A community perspective is grounded in peer production. In "Coase's Penguin [27]," Benkler argues that peer production in online communities can reduce transaction costs and replace many of the services of the firm.

Peer-production by communities in the context of Internet and software is quite well known; Wikipedia and Linux being some canonical examples. For security and privacy online, albeit less known, examples exist; e.g. vulnerability sharing through Bugtraq [28]. Jones argues for community policing against cybercrime through a virtual neighborhood watch of open source software [29]; Rustad suggests private enforcement through tort remedies [30]; Huey et al. notes the benefits of coordinated action between private vigilantes and public enforcement [31]. Rustad and Huey et al., however, take a narrow view of community action, where individual actions are sanctioned and enforced by a central agency. Such agencies are, in practice, unwilling enforcers [17], often due to lack of resources [12]. Simultaneously, Jones' solution is difficult to operationalize given the lack of theoretical underpinnings and that many users have incomplete and inadequate mental models of security [32].

On the other hand Camp proposes solutions that empower users, allows for self-organization of interested stakeholders, accounts for their mental models, and is theoretically grounded in Ostrom's framework [28]. The operationalizations of Camp's reconceptualization of the end-user have manifested as technical systems for security [33] and privacy [34]. However, this previous research is primarily focused at empowering defenders through community frameworks.

Crime is rarely analyzed as a community phenomena in cyberspace. Offline, however, criminological theories often investigate community structures and their relevance towards encouraging criminal activity. A few exceptions have investigated communities of victims and not attackers; for example, Garg et al. note that communities with higher proportion of uneducated Caucasian males witness higher reporting of Craigslist scams [35]; Pratt et al. found that fraud targeting is correlated with individual Internet use frequency of online purchases [36]. Such analyses, targeting communities of attackers, could provide complementary insights to a purely market based approach. If phishing is a tragedy of the commons [37], how do phishers peer produce governance of the limited resource and prevent a winner-take-all market [38]? Market based analysis have identified bottlenecks in terms of profits [39]; we aim to provide similar insights in terms of sustainability.

## III. Collective Action Under Ostrom's Framework

In the classic paper, Hardin noted that individually rational decisions can lead to socially suboptimal outcomes [40]. For example, let us assume that there is a pasture, where a group of farmers take their sheep to graze. If too many sheep graze on the pasture, the rate of consumption would be greater than the rate at which the pasture replenishes. Thus, the pasture would not be a sustainable resource. Unless all farmers agree to limit the number of sheep each farmer can bring to the pasture, an individual farmer is rational in bringing the maximum amount of sheep to the pasture. Since the farmers cannot be certain that other farmers would honor such an agreement, all of them rationally over consume the resource, leading to short term benefits, but long term depletion of the resource.

This 'tragedy of the commons' is not limited to grazing pastures, but can be applied to a diversity of resources, e.g. forest, fisheries. It has been argued that to the extent the network is a combination of two resources, bandwidth and computational power, Internet too can suffer from suboptimal outcomes as, for example, the effectiveness of security and privacy decisions is contingent on collective action. Camp [28] argues that the many security problems of the Internet are an artifact of its design which requires collaborative action between multiple stakeholders, often non-experts. The problem of collective action online is not singular to defenders but also impinges attackers. Herley [37] argues that cybercrime is a limited resource economy. Specifically there is a limited number of individuals that can be phished. This limited resource of vulnerable end-users is being over-consumed by phishers, who are individually rational in sending out the maximum number of phishing emails that they can.

Two classic solutions were proposed to avoid this suboptimal outcome, or Nash equilibrium, due to collective action. First, the pasture can be managed by the government, which can regulate and enforce the number of sheep each farmer can bring to the pasture. This solution considers the sustainable pasture to be a *public good*. A second solution argues that the pasture can be bought and managed by a private entity. This entity can then divide up the pasture and allow property rights on independent sections of the pastures to individual farmers. In would be in the self interest of these individual farmers to ensure that their section of the pasture is sustainable. Therefore, they would ensure that only a limited number of sheep graze. This solution considers the pasture to be a *private good*.

In practice, however, a public good or a private good solution to the tragedy of the commons has been found to be inadequate. From a defender perspective a public goods solution to cybercrime manifests itself as laws, which is limited by the expense and difficulties of cross-jurisdictional prosecutions [12]. Private enforcement is similarly limited, as criminals still manage to collect valuable information [21]. Even co-ordinated enforcement between public and private entities can be problematic as it creates externalities for the market, possibly creating a higher cost than the crime itself [41]. For example, takedowns often impact legitimate market participants whose services are rendered terminated, often without warning. Simultaneously, botnet herders can rebuild given the modest costs of Pay per Install services [24].

Ostrom then proposes a third solution to the commons that of self-governance through local stockholders [9]. For the case of pastures, individual farmers could have established and enforceable social norms regarding the appropriate number of sheep each farmer is allowed to bring. The success of these social norms in regulating the behavior of individual community members, Ostrom argues, is based on whether the community (or its institutions) meet these five criteria [2], [9]: 1) low cost of monitoring, 2) moderate rates of change of the resource, 3) frequent communication between resource members, 4) low costs of enforcement, and 5) exclusion. This framework has previously been applied to generate new solutions for security [33] and privacy [34] decisions from the context of defenders. Here we examine its applicability to a community of attackers.

*Low cost of monitoring* implies that it should be possible to monitor the behavior of individual community members. For example, it must be easy and cheap to monitor the number of sheep being brought to the pasture by individual farmers. If we consider individual members of an online network to be nodes, then in that context it must be easy or cheap for the network to monitor the behavior of its constituent nodes as well as the edges, as defined by the relationships between those nodes. In the context of underground forums it must be possible for the community to be able to monitor the communications and transactions between different parties.

*Moderate rates of change of the resource* relates to sustainable consumption. If the rate of consumption of the resource is greater than that at which the resource replenishes, then the resource would eventually be exhausted. Thus, the rate of change of resource should have an upper bound. Simultaneously, the *rate of change of the resource consumers* should be relatively small. If the individuals that consume the resource change constantly then it would be (prohibitively) costly to either establish or enforce social norms. For underground forums this means that the core group of cyber-criminals should remain relatively constant, i.e. the rate at which new members join as well as the rate at which existing members leave should be relatively low; the smaller the rate the more sustainable the community would be.

*Frequent communication between resource members* is needed to ensure that there is *social capital* associated with individual identity. This kind of communication is rarely possible for online networks, especially as they cross over political boundaries. It is, however, possible to have other measures of social capital online, e.g. reputation systems. If the same cyber-criminals on an underground forum have repeated transactions then they would have a mutual level of trust, i.e. they would a higher belief in that they would not be ripped off in a transaction. For example, someone buying credit card numbers could be more certain that they are not fake. If, however, transactions are not repeated but in general one time, then other measures of reputation would have to be employed. For example, cyber-criminals could assign satisfaction ratings for each transaction (much like on eBay).

*Exclusion* should be possible. The commons are distinctly different from open resources in that it is possible to prevent individuals from being part of the community as well as using the resource. In the case of the pasture, for example, it is possible to put a fence around it and give keys to only those individuals who are a part of the immediate community. It would be interest of the members of an underground forum to be able to exclude certain individuals. For example, cyber-criminals would likely be unhappy if law enforcement could easily be on the same forum and monitor their activities. Additionally, they would also be invested in keeping out cyber-criminals who prey on their own kind, e.g. rippers who sell fake credit card numbers to gullible members of the underground forum.

*Enforcement* of social norms should be possible at relatively low costs and should be supported by community members. This means that community members should be able to identify when someone breaks a social norm, for example by bringing more sheep to the pasture than is allowed. The community should then be able to punish the offending member. For example, the offending member could be refused pasture privileges for a certain amount of time, based on the seriousness of his offense. Underground forum member would most likely be invested in protecting their community as it makes engagement in cybercrime economically and technically feasible. Thus, they should be able to identify when a member is breaking the community norm. For example, if a member is repeatedly ripping off other member by selling them fake goods or unreliable services. Lack of reliability can make specialization difficult. For example, Li et al. discuss the possibility of creating fake bots to make botnets unreliable [42]. If botnets do not perform then it would be difficult for another cyber-criminal to run spam and scam campaigns.

## IV. Underground forums

In this section we give an overview of the forums we analyzed. We have complete database SQL dump of the 5 forums. Each of these SQL forum dumps has been publicly leaked and uploaded to public file downloading sites by unknown parties. The forum dumps include registration information of all the users with their email address, IP address (in some cases) along with all the public posts and private messages. Table IV shows date covered, primary language, number of users and lurkers (i.e. users who post neither public nor private messages), public posts and private messages in the forums.

AntiChat is the largest forum in terms of number of active users (15165) and public posts (total post 2160815). It is a predominantly Russian language forum and is the only one in our study that is both informational and commerce based. Unlike the rest of the forums in this study AntiChat does not specialize on a single topic, but rather covers a broad array of underground cybercrime topics from password cracking, stolen online credentials, email spam, search engine optimization (SEO), and underground affiliate programs.

BlackhatWorld is primarily an English speaking forum that focuses on blackhat SEO techniques. At the time of our forum dump in Oct 2005, it was largely an informational forum for exchanging tips on how to improve SEO methods. However, it currently is both a discussion and commerce hub for the blackhat underground community.

Carders and L33tCrew are primarily German language forums that are more commerce oriented and specialized in the sale and monetization of stolen credit card information and online credentials.

BadhackerZ is a mixed English/Hindi language forum where users are engaged in trading copies of pirated movies. Though the forum was created in Nov 2003, it stayed dormant for until Oct 2005 (shown in Figure 3). We did not notice any commerce-based activities in BadhackerZ. Moreover, we noticed that over 90% of the private messages were sent in one day and were spam.

AntiChat is the longest running forum in this dataset, has the maximum number of active users, and can thus be characterized as the most successful. BadhackerZ on the other hand is an example of a failed forum; i.e. it is highly dysfunctional with few users and limited (almost non-existent) trading. AntiChat and BlackhatWorld are the two forums that are currently live. Carders and L33tCrew were closed after they were hacked [1]. BadhackerZ is currently defunct; at the time of submitting this manuscript the reasons are not known.

The success of a community is quantitatively measured by the presence of small world characteristics on a social network [43], [44]. For example, small world networks are more commercially successful [44], economically efficient [43], and creative [45]. A network is called *small world* if it is highly clustered ($C \gg C_{random}$) with small path length ($L \approx L_{random}$) given $C_{random} \sim \frac{k}{N}$ and $L_{random} \sim \frac{logN}{logk}$, where $k$ = mean degree (average private message interaction per member) and $N$ = total nodes. We noticed small world

[1] http://www.exploit-db.com/papers/15823/

| Forum | Primary Language | Date covered | Posts | Pvt msgs | Users | Lurkers |
|---|---|---|---|---|---|---|
| Antichat (AC) | Russian | May 2002-Jun 2010 | 2160815 | 194498 | 41036 | 15165 (36.96%) |
| BadhackerZ (BH) | English/Hindi | Nov 2003-May 2008 | 37074 | 5171 | 8149 | 3026 (37.13%) |
| BlackHat (BW) | English | Oct 2005-Mar 2008 | 65572 | 20849 | 8718 | 4229 (48.5%) |
| L33tCrew (LC) | German | May 2007-Nov 2009 | 861459 | 501915 | 18834 | 9306 (46.41%) |
| Carders(CC) | German | Feb 2009- Dec 2010 | 373143 | 197067 | 8425 | 3097(36.76%) |

Table I
SUMMARY OF FORUMS (DATE REPRESENTS POST DATE)

effect in all the forums except BadHackerZ (Table II).

| Forum | $C$ | $C_{random}$ | $L$ | $L_{random}$ |
|---|---|---|---|---|
| Antichat | 0.015 | 0.0004 | 5.06 | 4.71 |
| BadHackerZ | 0.019 | 0.0004 | 4.7 | 11.02 |
| BlackHat | 0.032 | 0.0014 | 4.02 | 5.06 |
| Carders | 0.127 | 0.0045 | 3.26 | 2.74 |
| L33tCrew | 0.14 | 0.0053 | 3.12 | 2.39 |

Table II
"SMALL WORLD" EFFECT ($C \gg C_{random}$ AND $L \approx L_{random}$)

## V. ANALYSIS

### A. Monitoring

In all forums, there are three ways to monitor members' activities, 1) by administrators and moderators, 2) by forum bot, and 3) by the community. Admins are generally the members who started the forum and moderators are chosen among the active members. The number of admins and moderators are shown in Table III, taken from the corresponding database tables for admins and moderator. Each forum had 1-3 administrators and 5-9 moderators except AntiChat which had 89 moderators. The reason is that AntiChat had section-wise moderators in charge of one particular section of the forum, whereas other forums' moderators handle the whole forum.

The forum bot refers to automated plugins that are installed in the forum for specific tasks, for example, to identify multiple accounts and to filter posts with specific words. All of the forums have automated filtering to catch posts in wrong threads and posts with blacklisted words. Only Carders uses an Alter Ego (AE) detector[2] to detect duplicate accounts.

Members of the community can report bad behavior by other members. This could be done by giving positive or negative reputation score to a member, by tagging a post of a member as spam/off-topic/offensive, by posting complaints in a specific thread, and by provide ratings for each trade. Additionally, Carders and L33tCrew have dedicated threads to report "rippers" (members who cheated other members) and spammers with sufficient proofs, e.g., chat logs, screenshots, pictures of the product sold. Moderators verify these complaints and take appropriate action like giving warnings or banning the member. Blackhat maintains a "shitlist" for members with bad report and a "VIP zone" where only certain reputed members are allowed to trade.

The commercial forums (AntiChat, BlackHat, Carders and L33tCrew) also monitor the quality of the products and services being traded in the forum. AntiChat has paid "guarantors" who provide guarantees of products and services at the cost of 0% to percentage of the value of one unit of goods/services[3]. In the other forums admins and moderators verify the products before they are posted in the trade section.

| Forum | Admin | Mod |
|---|---|---|
| Antichat | 3 | 89 |
| BadHackerZ | 2 | 5 |
| BlackHat | 3 | 9 |
| Carders | 3 | 11 |
| L33tCrew | 1 | 8 |

Table III
SUMMARY OF MONITORING IN THE FORUMS

### B. Rates of Change

According to Ostrom's framework a sustainable community should have moderate rate of change of resources and resource consumers. In the context of underground forums, the common-pool resource is characterized by the community members themselves and their (close) relationship with each other. These members provide goods and services, such as stolen debit/credit cards, tutorial on blackhat SEO techniques, or monetizing stolen cards. We describe the rate of change in the forums in terms of members and connectivity among the members per month.

The percentage of members per month is calculated by collecting the join date of each member from the corresponding member table in the database. The percentage of members in a month is the ratio members joined until that month and total members of the forum (Figure 3). The rate of change in terms of new members is low, 1.02%-3.57% (Table IV). BadHackerZ has the highest percentage of new members on average. Antichat has a slow and steady change in number of members.

To calculate the average clustering coefficient ($C$) and path length ($L$) of the forums we represented the private

[2] http://www.vbulletin.org/forum/showthread.php?t=107566

[3] Rules for using guarantors is described in http://forum.antichat.ru/thread63165.html

| Forum | Avg. new members | Avg. C | Avg. Path length |
|---|---|---|---|
| Antichat | 418.73 (1.02%) | 0.013 | 3.08 |
| BadHackerZ | 301.81 (3.7%) | 0.003 | 1.49 |
| BlackHat | 290.6 (3.33%) | 0.014 | 2.03 |
| Carders | 300.89 (3.57%) | 0.035 | 1.38 |
| L33tCrew | 437.98 (2.32%) | 0.123 | 3.15 |

Table IV
RATE OF CHANGE PER MONTH

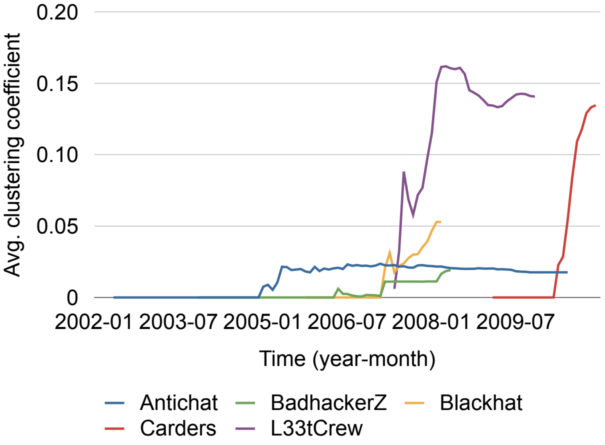

Figure 1. Average clustering coefficient per month

message interaction network of an underground forum as a graph $G = (V, E)$, where $V$ is the set of members and each $e_{ij} \in E$ represents a private message from member $i$ to member $j$. The clustering coefficient of a node in a graph quantifies how close its neighbors are to being a complete graph. The average clustering coefficient ($C$) for the whole network is the average of the clustering coefficients of all the nodes in a graph. Suppose a member $v \in V$ has $k_v$ neighbours, then at most $k_v(k_v - 1)/2$ edges can exist between them. The clustering coefficient of $v$ ($C_v$) is the ratio of number of existing edges and all possible edges[46]. If every node in $v$'s neighbours are connected with each other, clustering coefficient would be 1 and if none of the nodes are connected clustering coefficient would be 0. Path length ($L$) is defined as the number of edges in the shortest path between two nodes, averaged over all pairs of nodes. In AntiChat, both $C$ and $L$ stayed constant with very small change (Figure 1 and 2) which shows that connectivity among members does not change over time. L33tCrew had rapid growth of $C$ over time but relatively constant path length. Carders also had rapid growth of $C$ and decreasing path length among members.

### C. Social Capital

Social capital in a community is established by the frequency and ease of communication between two members. On underground forums there are two kinds of communication: public posts and private messages; public messages were for advertising purposes and private messages are for negotiation. Figure 4 and 5 show percentage of public and private messages per month.

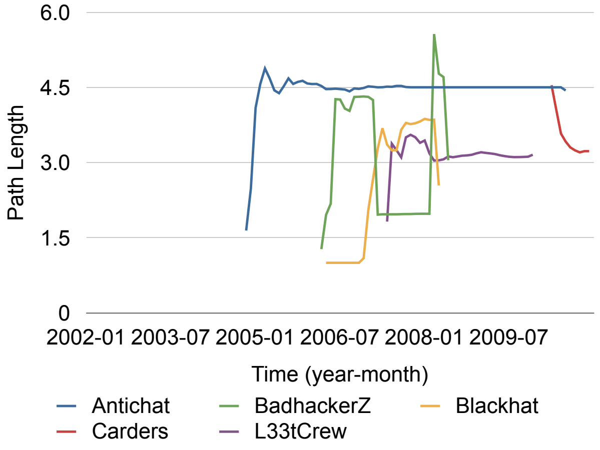

Figure 2. Path length per month

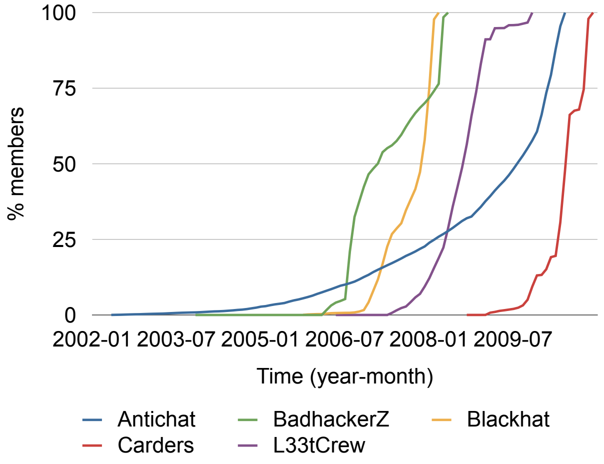

Figure 3. Percentage of members per month

### D. Exclusion

Exclusion refers to property of a resource that prevents use by non-members. To the extent underground forums are common-pool resources (and not open access), different forums employ distinct strategies to meet exclusion.

Each forum has specific membership and access rules stated in the "forum rules" or "FAQ" sections. We will discuss exclusion in three cases: general membership, ranking of the members and access restriction.

*1) Membership criteria:* In all of the forums, anyone can become a member by registering with a valid email address. In L33tCrew, disposable email addresses (e.g., trashmail) are not allowed.

*2) Member rank:* Each forum maintains member rankings which come from reputation in the forum. Reputation

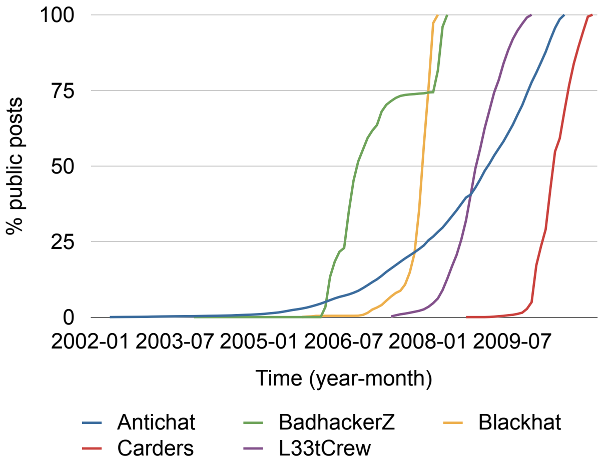

Figure 4. Percentage of public posts per month

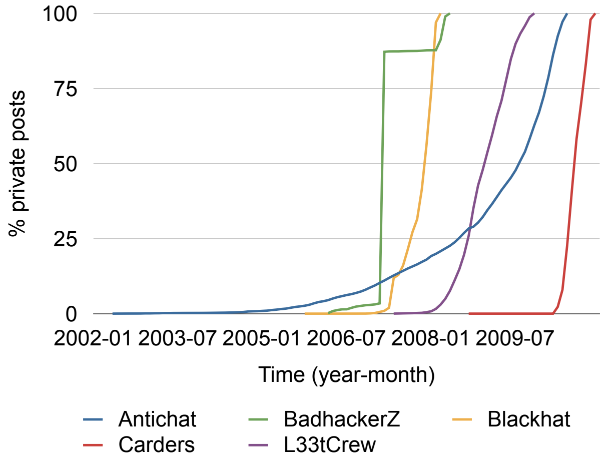

Figure 5. Percentage of private messages per month

is quatified by posts counts, "thank" counts and trader ratings provided by other community members and warnings/infractions received from moderators. In some forums, e.g., Blackhat and Carders, members can pay to get a specific status in the forum.

*3) Access restrictions:* Membership in a forum does not gurantee full access in the forum. Access to some specific sections of a forum is often restricted to either active member or paid members. For example, on Blackhat members need to pay \$25-\$30[4] non-refundable fees to post in a public thread and \$15 or 25 posts to download from the download section. On Carders, members can buy a "Verified vendor license" for 150+ euro per month which is required to sell certain products, e.g., drugs, permanently. The price of the license depends on the product. For selling drugs and Paypal accounts license is 200 euro per month. For some products, there is a trial period associated where the vendor is monitored for his trading behavior. In that case the vendor has to pay 50 euro extra during the trial period. Money is accepted via WebMoney, Ukash, and PaysafeCard (33% fees). When complaints are lodged against a vendor, he needs to pay extra money as penalty. On L33tCrew, at least 15 posts (excluding "thanks" posts) in the public thread is required to access the trade section, and at least 150 posts is required to be a "2nd level" member. "3rd level membership" is invited only to member who "proved" themselves as trusted 2nd level members and possess nonpublic tools.

Each forum has specified sections for specific purposes, e.g., a special thread for trading, a special thread for tutorials. On Blackhat world, posts related to trading are only allowed in a specific thread ("buy, sell, trade"). To post in the buy, sell and trade thread a member needs at least 40 posts and good standing for 2 months. Every product is reviewed by at least one of the admins and/or moderators. Carders also has a special trade section. Certain section of the Carders marketplace have restricted access and members need special ranking to be able to view it. For example, medicine and drug trading sections are only visible to "full members." Members get penalties for posting in the wrong threads. If member receives too many penalty points, his access is restricted to certain section of the forum. For example, posting in wrong thread costs 5 points, unauthorized selling costs 10 points, spam is 1-15 points, and trading outside the marketplace is 15 points.

### *E. Enforcement*

To enforce the community norms, each forum monitors members' activities and punishes offending members. There are three ways to punish a member: warnings with/without negative points (known as infractions), temporary bans and permanent bans. On some forums, members with enough negative points are automatically banned. Among the forums, Carders had the highest percentage of permanently banned members and BadHackerZ had the lowest percentage of banned members (Table V).

| Forum | % Banned | Temp. banned | % Warnings |
|---|---|---|---|
| Antichat | 7.37%(3023) | NA | NA |
| BadHackerZ | 0.07% (6) | 0.29% (24) | 0.79% (41) |
| BlackHat | 0.49% (43) | NA | 0.45% (95) |
| L33tCrew | 4.84% (913) | 0.11% (22) | 0.65% (3251) |
| Carders | 21.94% (1849) | 0.07% (6) | 2.04% (4023) |

Table V
SUMMARY OF ENFORCEMENT IN THE FORUMS

## VI. Discussion

This paper examines cybercrime as a community phenomena and thus underground forums as a common-pool resource that needs to be managed. Thus, we ask the question are cybercrime forums sustainable? We analyze the

[4] The cost was \$25 in our dataset, but has been increased to \$30 in the present Blackhat world forum.

success of these forums on five dimensions identified by Ostrom: 1) monitoring, 2) rates of change, 3) social capital, 4) exclusion, and 5) enforcement.

The foremost vector of monitoring is top down, through forum owners themselves; i.e. administrators and moderators. However, there is not much difference across forums for such monitoring; table III. The one exception is AntiChat, which can be explained by the large size of the forum itself. Additionally, unlike other forums AntiChat has topic specific moderators.

A second vector is bottom up, that of monitoring by community members. We note that with the exception of BadHackerZ all forums in this study have dedicated threads to report rippers. These threads alleviate the cost for other community members to identify the those who may not be trustworthy. Given that BadHackerZ is a less successful, and arguably dysfunctional forum, in this analysis we can hypothesize that reduced cost community monitoring can improve sustainability outcomes for underground forums (presuming that top down monitoring, e.g. by administrators, meets some lower bound.)

The rate of change of percentage of forum members similarly correlates with the success of individual forums. The most robust forum AntiChat has a gradual increase in it membership; figure 3. On the other hand BadHackerZ has staccato periods of growth, i.e. the percentage increase in member happens in bursts; table IV.

The rate of change of connectivity for individual forum members is simultaneously important. We examined this using average clustering coefficient and average path length. The former metric, average clustering coefficient, is not very informative; figure 1. Both robust forums, such as Antichat, and unsuccessful forums, e.g. BadHackerZ, have low clustering coefficients, which appear to be relatively constant across time. On the other hand average path length clearly indicates the difference; figure 2. More robust forums have a relatively stable average path length, while for unsuccessful forums there is marked and sudden decline/appreciation of the average path length.

Social capital was examined by the number of public and private messages sent by forum members. For forums such as L33tCrew this operationalization is straight forward as a certain number of public posts correlate with the level of membership and privileges. For other forums, such as AntiChat, such postings act in an information economy, where posting answers to other member's questions allows you to build trust within the community. From figures 4 and 5 we note that there appears a correlation between percentage of public posts and private messages for most forums. The one exception is BadHackerZ. Furthermore, the more successful forums note a gradual increase in the percentage of communications. BadHackerZ, however, has spurts of growth; e.g. there is a significant increase in the percentage of private messages for a single month in 2006, figure 5.

At a first pass it appears that exclusion is not a property of cybercrime communities, i.e. anyone can create an account on these underground forums. However, it seems exclusion in these communities is managed in terms of privileges, i.e. the actions that individual account holders are allowed to perform on the forum. Most forums have member rankings for example. A key problem in these forums is bootstrapping trust. On certain forums this is addressed by extracting an economic cost from the participant. For example, BlackHat and Carder require individuals to pay in order to use the forum. On L33tCrew the cost is in terms of information, where individuals are required to have a certain number of posts to get access to specific areas of the forum. AntiChat and BadHackerZ have no explicit requirement for posts or monetary payment. However, AntiChat is both and information and transactional forum. Thus, members can build reputation by answering questions from the community. BadHackerZ does not allow for similar trust/privilege escalation through community engagement. It is unclear whether monetary payment is better or worse than non-monetary entry costs, e.g. minimum number of public posts. However, it appears that at least one such entry cost is needed.

Enforcement is usually done in terms of banning members. In fact all communities ban members; table V. In addition some communities also prescribe temporary bans and individual warnings. The more successful forums non-fractional percentages of banned members. The exception is BlackHat, which substitutes bans with $50 fines.

It is evident that the five characteristics of sustainable commons offline also correlate with successful underground forums online. Most forums are similar in top down monitoring. Successful forums, however, engage community members for self governance. The rate of change of both the resource and resource consumers also correlates with better managed forums. Smaller average path length obviously corresponds to a more efficient network. In the context of a community the ancillary requirement is that average path lengths are static as the network grows, i.e. for an observed increase in the number of resource users there is no corresponding increase in the inefficiency of the community. Social capital as captured by frequency of communication is also found to be associated with the success of individual forums. The frequency of communication in successful forums remains relatively constant. Surprisingly, none of the forums do not explicitly exclude individuals from participating. However, privileged and open access is limited to individuals with greater capital, monetary as well as non-monetary (e.g. in term of number of posts). The raised cost of participation does lead to better outcomes for the forums. Finally, enforcement both monetary, such as through fines, and non-monetary, e.g. bans are also needed.

## VII. Conclusion & Future Work

The costs of cybercrime are alleviated by underground forums, which enable lower transactions costs through collaboration between cyber-criminals with specialized skill sets. The question that anti-cybercrime efforts ask is whether cybercrime is profitable? In this paper we ask a fundamentally distinct, though complementary question, i.e. **are underground forums sustainable?** By changing the focus from profits to sustainability there is a potential for creating new interventions that impinge cybercrime communities, rather than individual incidences of cybercrime; thus potentially informing a longer term deterrence approach.

In this paper we analyzed the organization of cybercrime as communities of cyber-criminals through underground forums. The sustainability of these forums is contingent on adequate governance of the cybercrime commons. Typically successful governance of the commons can be mapped on to five characteristics; 1) the cost of monitoring should be cheap; 2) the rate of change of the resource and/or resource consumers should be moderate; 3) there must be frequent communication between community members to enable social capital; 4) it must be possible to exclude individuals from using the resource; 5) finally, members that fail to adhere to community norms should be punished. We find that these five characteristics are also relevant for the success of cybercrime communities, i.e. forums that performed better on these five dimensions were more functional. An exception is explicit exclusion, which is not implemented by any of the forums, though privileged access is limited to those with higher social capital.

The findings here indicate that traditional measures of sustainability when appropriately operationalized can distinguish between successful and failed forums. New deterrence measures can then target the stated five characteristics of sustainable communities (in addition to the profits of cybercrime. For example three distinct deterrence strategies can be: (1) high cost deterrence through enforcement and prosecution, (2) medium cost deterrence by adding targeted goods to the network that collects information and conduct surveillance for anti-cybercrime efforts, and (3) low cost deterrence by creating Sybil identities in the market that adds noise and thus increases transaction costs for legitimate cyber-criminals. On a social network graph are be modeled as (1) removing a node (and associated edges), (2) converting attacker nodes to defender nodes, and (3) adding defender nodes. The application and thus economic efficiency of these strategies would differ based on whether they aim to reduce profits or sustainability.

Future work will target three properties of underground cybercrime communities: 1) profitability, 2) connectivity, 3) and sustainability. We will identify qualitative and quantitative metrics for these properties as well as discuss the relative effectiveness of distinct operationalization of these metrics under different levels of data granularity. The goal will be to develop metrics that provide meaningful indicators even when data is limited. For example, if public posts are available but not private messages between individual cyber-criminals. We also will combine linguistic techniques, e.g. topic modeling, social network analysis, and analysis to provide a repeatable, verifiable, and systematic framework that enables a scientific exploration of these forums and the impact of distinct interventions at mitigating underground forums.

Finally, there are two limitations of this research. First, given that the forums trade different goods and services, our findings may be an artifact of the forums in question. In future work we will replicate these results with additional forums. Second, the notion of a successful forum is qualitatively defined. Quantitatively, success is only examined in terms of whether the forums are small world or not. Future work would look at more direct measures of success, e.g. trading volume.

## Acknowledgement

This research was supported by Intel through the ISTC for Secure Computing, the National Science Foundation under grant 1237076, and a gift from Google. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsors.

## References

[1] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. Voelker, "An analysis of underground forums," in *Proceedings of the 2011 SIGCOMM Conference on Internet Measurement*. ACM, 2011, pp. 71–80.

[2] T. Dietz, E. Ostrom, and P. C. Stern, "The struggle to govern the commons," *Science*, vol. 302, no. 5652, pp. 1907–1912, 2003.

[3] 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.

[4] A. Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations*. London, U.K.: Methuen and Co, 1776.

[5] R. H. Coase, "The nature of the firm," *Economica*, vol. 4, no. 16, pp. 386–405, 1937.

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

[7] G. S. Becker and G. J. Stigler, "Law enforcement, malfeasance, and compensation of enforcers," *The Journal of Legal Studies*, vol. 3, no. 1, pp. 1–18, 1974.

[8] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage, "Spamalytics: an empirical analysis of spam marketing conversion," *Communications of the ACM*, vol. 52, no. 9, pp. 99–107, 2009.

[9] E. Ostrom, J. Burger, C. B. Field, R. B. Norgaard, and D. Policansky, “Revisiting the commons: local lessons, global challenges,” *Science*, vol. 284, no. 5412, pp. 278–282, 1999.

[10] A. R. Poteete and E. Ostrom, “Heterogeneity, group size and collective action: The role of institutions in forest management,” *Development and change*, vol. 35, no. 3, pp. 435–461, 2004.

[11] R. Anderson and T. Moore, “The economics of information security,” *Science*, vol. 314, no. 5799, pp. 610–613, 2006.

[12] D. S. Wall, “Policing cybercrimes: Situating the public police in networks of security within cyberspace,” *Police Practice and Research*, vol. 8, no. 2, pp. 183–205, 2007.

[13] R. Böhme and T. Moore, “The iterated weakest link,” *Security & Privacy, IEEE*, vol. 8, no. 1, pp. 53–55, 2010.

[14] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage, “Measuring the cost of cybercrime,” in *Proceedings of the Workshop on the Economics of Information Security*. Springer, 2012.

[15] 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*, 2007.

[16] T. Holz, M. Engelberth, and F. Freiling, “Learning more about the underground economy: A case-study of keyloggers and dropzones,” *Computer Security–ESORICS 2009*, pp. 1–18, 2009.

[17] A. Rege, “What’s love got to do with it? exploring online dating scams and identity fraud,” *International Journal of Cyber Criminology*, vol. 3, no. 2, pp. 494–512, 2009.

[18] A. Blum, B. Wardman, T. Solorio, and G. Warner, “Lexical feature based phishing url detection using online learning,” in *Proceedings of the 3rd ACM Workshop on Artificial Intelligence and Security*. ACM, 2010, pp. 54–60.

[19] M. Christodorescu, S. Jha, S. A. Seshia, D. Song, and R. E. Bryant, “Semantics-aware malware detection,” in *Symposium on Security and Privacy*. IEEE, 2005, pp. 32–46.

[20] A. Juels, S. Stamm, and M. Jakobsson, “Combating click fraud via premium clicks,” in *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*. USENIX Association, 2007, pp. 1–10.

[21] P. J. Nero, B. Wardman, H. Copes, and G. Warner, “Phishing: Crime that pays,” in *eCrime Researchers Summit*. IEEE, 2011, pp. 1–10.

[22] I. P. Png, C.-Y. Wang, and Q.-H. Wang, “The deterrent and displacement effects of information security enforcement: International evidence,” *Journal of Management Information Systems*, vol. 25, no. 2, pp. 125–144, 2008.

[23] V. Garg, N. Husted, and J. Camp, “The smuggling theory approach to organized digital crime,” in *eCrime Researchers Summit*. IEEE, 2011, pp. 1–7.

[24] J. Caballero, C. Grier, C. Kreibich, and V. Paxson, “Measuring pay-per-install: the commoditization of malware distribution,” in *Proceedings of the 20th USENIX conference on Security*, ser. SEC’11. Berkeley, CA, USA: USENIX Association, 2011, pp. 13–13. [Online]. Available: http://dl.acm.org/citation.cfm?id=2028067.2028080

[25] T. C. Schelling, “Economics and criminal enterprise,” *Public Interest*, vol. 7, 1967.

[26] A. R. Dick, “When does organized crime pay? a transaction cost analysis,” *International Review of Law and Economics*, vol. 15, 1995.

[27] Y. Benkler, “Coase’s penguin, or, linux and the nature of the firm,” *The Yale Law Journal*, vol. 112, no. 3, 2002.

[28] L. J. Camp, “Reconceptualizing the role of security user,” *Daedalus*, vol. 140, no. 4, pp. 93–107, 2011.

[29] B. R. Jones, “Comment: Virtual neighborhood watch: Open source software and community policing against cybercrime,” *The Journal of Criminal Law and Criminology*, pp. 601–629, 2007.

[30] M. L. Rustad, “Private enforcement of cybercrime on the electronic frontier,” *S. Cal. Interdisc. LJ*, vol. 11, p. 63, 2001.

[31] L. Huey, J. Nhan, and R. Broll, “uppity civilians and cyber-vigilantes: The role of the general public in policing cyber-crime,” *Criminology and Criminal Justice*, vol. 13, no. 1, pp. 81–97, 2013.

[32] R. Wash, “Folk models of home computer security,” in *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, 2010, p. 11.

[33] Z. Dong, V. Garg, L. J. Camp, and A. Kapadia, “Pools, clubs and security: designing for a party not a person,” in *Proceedings of the 2012 workshop on New security paradigms*. ACM, 2012, pp. 77–86.

[34] V. Garg, S. Patil, A. Kapadia, and L. J. Camp, “Peer produced privacy protection,” in *International Symposium on Technology and Society*. IEEE, 2013.

[35] V. Garg and S. Nilizadeh, “Craigslist scams and community composition: Investigating online fraud victimization,” in *Proceedings of the International Workshop on Cyber Crime*. IEEE, 2013.

[36] T. C. Pratt, K. Holtfreter, and M. D. Reisig, “Routine online activity and internet fraud targeting: Extending the generality of routine activity theory,” *Journal of Research in Crime and Delinquency*, vol. 47, no. 3, pp. 267–296, 2010.

[37] C. Herley and D. Florêncio, “A profitless endeavor: phishing as tragedy of the commons,” in *Proceedings of the 2008 workshop on New security paradigms*. ACM, 2009, pp. 59–70.

[38] C. Herley, “Small world: Collisions among attackers in a finite population,” in *Proceedings of the Workshop on the Economics of Information Security*, 2013.

[39] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu *et al.*, "Click trajectories: End-to-end analysis of the spam value chain," in *Symposium on Security and Privacy*. IEEE, 2011, pp. 431–446.

[40] H. Garrett, "The tragedy of the commons," *Science*, vol. 162, no. 3859, pp. 1243–1248, 1968.

[41] V. Garg and L. J. Camp, "Ex ante vs. ex post: Economically efficient sanctioning regimes for online risks," in *Telecommunications Policy Research Conference*. SSRN, 2013.

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

[43] V. Latora and M. Marchiori, "Economic small-world behavior in weighted networks," *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 32, no. 2, pp. 249–263, 2003.

[44] P. V. Singh, "The small-world effect: The influence of macro-level properties of developer collaboration networks on open-source project success," *ACM Transactions Software Engineering Methodology*, vol. 20, no. 2, pp. 6:1–6:27, 2010.

[45] B. Uzzi and J. Spiro, "Collaboration and creativity: The small world problem," *American Journal of Sociology*, vol. 111, no. 2, pp. 447–504, 2005.

[46] D. J. Watts and S. H. Strogatz, "Collective dynamics of small-worldnetworks," *nature*, vol. 393, no. 6684, pp. 440–442, 1998.