Why Cybercrime?

Vaibhav Garg
www.vaibhavgarg.net
me@vaibhavgarg.net

L. Jean Camp
Indiana University, Bloomington
ljcamp@indiana.edu

ABSTRACT

How do cybercrime markets emerge, evolve, and persist? How can cybercrime be prevented, decreased and mitigated? Extant anti-cybercrime efforts have concentrated on deterrence through criminal prosecution and technical mitigation. Deterrence-only strategies, however, may be more expensive for the network than for attackers, particularly considering the asymmetric nature of computer security. The implicit assumption of deterrence, i.e. criminals are strictly self-optimizing rational agents cognizant only of a cost-benefit function, is contentious. Criminal actions are constrained/enabled by the institutional structures of their immediate neighborhood. Exposure to crime (or probability of victimization is similarly influenced. Thus, this paper examines the respective economic, structural, and cultural theories in criminology and explores their relevance online. We discuss the implications for technical solutions, security design, as well as public policy. An intuitive position is to lower the entry cost of legal enterprise, and thereby increase the opportunity cost of cybercrime engagement. We also discuss solutions that allow simultaneous investments (to reduce crime online) by both public and private entities, while mitigating for potential moral hazard. Our concluding argument, then, is for complementing deterrence with policy solutions that preemptively engage potential criminals as legitimate market stakeholders. In addition to the explicit examination of deterrence theories of cybercrime, this work offers a broader consideration of cybercrime that is grounded in theories of crime offline.

Categories and Subject Descriptors

K.4.1 [**Computers and Society**]: Public Policy Issues – *Abuse and Crime Involving Computers*

K.4.2 [**Computers and Society**]: Social Issues – *Abuse and Crime Involving Computers*

General Terms

Economics, Security, Legal Aspects.

Keywords

Cybercrime, Economics, Cultural Theories.

1. INTRODUCTION

The myriad explanations of criminal (non-rational) behavior offline are grounded, not only in the economic, but also the structural and cultural factors that facilitate criminal enterprise [47]. For example, crime is often endemic to specific neighborhoods in urban communities, irrespective of the prevailing residential group or associated characteristics, such as ethnicity [51]. Cybercrime, enabling infrastructure, and resulting victimization are similarly geographically concentrated. Nigeria is noted as a nation of 419 scammers. Eastern European towns, such as those in Romania, have earned a reputation of being 'Hackervilles' in popular media. In terms of cybercrime infrastructure, India persistently has a high percentage of systems infected by malware, while Sweden does not.

Consider the possibility that criminals online are not the strictly rational beings of economic theory, engaged in a calculus of profit maximization. This allows both policy makers and technologists to frame a response that is not merely grounded in deterrence. The limitations of deterrence-only approaches to crime have been widely illustrated [3], for example in the War on Drugs [36]. Offline deterrence is limited by corruption as criminals become organized [6], and empirical research argues that this also applies online [23, 24]. When cybercrime is welfare increasing in immediate jurisdictions, then there are inherent (i.e. not corruption-related) disincentives for local law enforcement to implement the deterring legislation [23]. Even when deterrence is effective, its impact is limited in time and mitigated by displacement [46]. For example, when households in one region acquire guns to protect their homes, criminals simply start targeting nearby communities [1]. Similarly, if the German anti-botnet initiative is successful, criminals can simply target malware at nations that do not or cannot feasibly make similar investments fighting cybercrime.

Crimes committed over or with the help of the Internet are usually termed "cybercrime". Myriad definitions of cybercrime are often inchoate and overly broad [26]. The European Commission definition for cybercrime [3] includes: 1) traditional crimes that are committed with the aid of computers or the Internet; 2) posting illegal content such as child pornography; and 3) crimes that are new and would not exist without computers or Internet. However, the United Nations definition extends it to sabotage, cyber espionage, etc. Cybercrime, in this paper, refers to criminal activity that either impacts digital networks or is committed with the aid of such networks.

Anderson et al. note that cybercrime constitutes traditional crime, transitional crime, and new crimes specific to the Internet [3]. Traditional crimes include, for example, tax fraud, which has simply moved online as more people have started using the Internet to submit tax returns. Transitional crimes include those that were traditionally committed offline, but now have moved online for scalability and convenience, e.g. credit card fraud. Finally, criminal activity, such as botnets, are new crimes contingent on the Internet and do not exist offline.

The extant investigations of all three categories of cybercrime posit a rational imperative for criminal enterprise online [5]. The foci of cybercrime investigations have been threefold. First, empirical investigations aim to understand cybercrime markets, invested stakeholders, and associated profits. Second, technical solutions (or deterrents) aim to lower these profits by increasing the cost of criminal engagement. Finally, coordinated policy actions, also grounded in deterrence theory,

enable legal prescriptions against criminal activity online or subsidize/regulate/mandate security investments.

Empirical investigations have found that the returns from criminal activity online are high, while the probability of prosecution is low. Estimates of returns from phishing correspond to $178.1 million a year [37]. Similar investigations of pharmaceutical spam and fake anti-virus report revenues of $3.5 million [32] and $130 million dollars [53], respectively. Technical deterrents such as CAPTCHAs (Completely Automated Public Turing tests to tell Computers and Humans Apart), increase the costs of criminal enterprise, as they limit the ability of automated attacks. The economic efficiency of such deterrents in the aggregate, however, is unknown, especially when accounting for the cost to legitimate services. Many individuals complain that not only do CAPTCHAs deter automated criminal responses, but they are difficult or impossible for some disabled humans and are at best a time sink for fully capable users. These deterrents also create alternative cybercrime markets [24], again increasing potential pay-offs for criminal activity. For example, CAPTCHA solutions are now crowd-sourced through websites such as Freelancer [38] that connect people in need of a job with those looking for people to work for them. A number of jobs posted on sites such as Freelancer are not legitimate businesses. Also in the mix of the cost-benefit analysis are policy actions, e.g. the American Computer Crime and Abuse Act and the Council of Europe's Convention on Cybercrime which seek to improve the efficacy of enforcement actions against cybercrime.

All of these approaches embed (implicitly or explicitly) the assumption that deterrence is the appropriate response to cybercrime. However, explicit analysis of deterrence theory has been absent. In this work we expand the view of cybercrime by viewing the phenomena through multiple lenses provided by (sometime disparate, sometimes complementary) theories of crime. This illuminates questions that have not previously been considered; for example, current research does not address the opportunity cost of cybercrime. Why is it that individuals choose to engender profits through cybercrime rather than legitimate enterprise? An offline analogy is, "why do certain individuals choose to sell illegal drugs such as cocaine vs. legal alternatives such as alcohol?" The answer to these questions may suggest new strategies to prevent crime online.

Deterrence is much needed but inherently limited. Deterrence-based measures such as IP blacklisting have, for example, increased the cost of sending spam. Arguably, spamming is economically rational only if the cost of sending bulk email were eight times cheaper than current technologies permit [32]. Alternatively, spam and the corresponding spam architecture must be vertically integrated, i.e. those who send bulk email also extract the monetary value from the (e.g. phishing) scams advertised in those emails [32]. Given that it is no longer profitable to be a stand-alone spammer, clearly deterrence-based approaches are not without virtue. However, does decreased profitability correlate with reduced crime? Decrease in spam is not evident; in fact spam volumes have increased, as much unsolicited bulk email does not bypass spam filters. Both theoretical and empirical analyses suggest that monetization in cybercrime is difficult, marginal returns are diminishing, and that criminals over-consume the limited resource of vulnerable end-users [27, 28]. The real question then becomes does criminal behavior strictly correspond to economic rationality?

The evidence (offline) argues that deterrence alone is inadequate to address crime. Despite the rising costs of deviant behavior, individuals continue to engage in criminal activities both collectively (e.g. as gang members) as well as individually [56]. For example, gang members accrue higher earnings as legitimate hourly workers at fast food joints than through drug peddling on street corners [56]. Simultaneously, while the United States has one of the highest population percentages of incarcerated individuals it also has one of the highest rates of violent crime in the developed world [36]. Thus, while deterrence is much needed, a one-dimensional approach may not be the solution. (It is arguably not even rational; given diminishing marginal returns, investments in anti-spam technologies may cost more than the financial impact of unsolicited bulk email [3].)

Thus, we argue for complementary approaches, which are informed by decades of scholarship in crime offline. By examining the economic, structural, and cultural factors that discourage legitimate online participation and thereby facilitate criminal enterprise we build upon theories of crime beyond deterrence. Intuitively, theories of crime offline should be able to explain traditional and transitional crime, which is now facilitated by information technologies, e.g. thetInternet. However, the applicability of these theories towards the investigation of new cybercrime is not obvious.

In Section 2 we discuss the extant policy and technical solutions to cybercrime; showing how these are grounded in deterrence. In section 3 we discuss economic factors, such as poverty and income inequality, and their ability to facilitate cybercrime, as they influence crime offline. In Section 4 we provide an overview of the research on structural theories of crime; we enumerate how these may apply to cybercrime. We consider factors such as informal social control and the strength of non-economic institutions. In Section 5 we discuss cultural theories of crime, such as sub-cultural theory, illuminating the potential impact of previously unexamined factors (e.g. gender) on cybercrime. In Section 6 we discuss the implications for technical design and policy formulation grounded in economic, structural, and cultural determinants of cybercrime. We conclude in Section 7.

2. DETERRENCE & ITS LIMITS

All the current school of cybercrime research models attackers as rational agents, maximizing their cost-benefit ratio and utility functions [5]. This has shaped responses to cybercrime, which have been grounded in deterrence, both from a technical and policy perspective. Regulatory solutions have focused on prosecution and punitive prescriptions, e.g. fines, incarceration, or both. Norbert Wiener noted the four goals of such sanctions [59]. First, these solutions impinge on the cost-benefit analysis of criminal enterprise by increasing the cost of deviant behavior. Second, they deter a potential criminal with the fearful prospect of punitive prescriptions. Third, they directly decrease crime, as criminals behind bars are unlikely to be able to further engage in criminal enterprise (for the duration of the sentence). Finally, incarceration serves as a corrective facility for offenders and offers appropriate education for rehabilitation.

These positive effects of punitive prescriptions are only partially realized in practice. For example, often instead of serving as correctional facilities, prisons expose individuals to hardened criminals and prove a venue for successful criminal and mutually

profitable alliances. Further, the labeling of individuals as "criminals" may prevent their reintegration into society, as they are denied (employment) opportunities. Arguably, it would be difficult to trust an individual as the head of IT operations, if they have previously served time for installing backdoors in systems. Criminals may also not take the cost of prosecution into account when engaging in criminal enterprise. Hacking, for example, has been argued as another instantiation of juvenile delinquency [61]. Deterrence would have limited impact on such behavior [52].

Deterrence-based approaches often do not account for the cost of enforcement and misalignment of incentives that may undermine such efforts. Becker indicates that if the cost of punitive measures through law is x dollars, then a rational criminal would be willing to invest that same amount to avoid prosecution [6]. Often this investment manifests as bribery and corruption. However, corruption requires implicit and explicit contracts between offenders and enforcers. The creation of this trust requires repeated transactions between the same set of offenders and enforcers. Thus, it is imperative for offenders to become organized. This is evident in cybercrime, which has progressed from individual ego-driven activity to organized and profit-driven activity.

The deterrence effect of bribery would be equivalent to that of punitive measures prescribed by law so long as the monetary worth of the bribe and that of the legal punishment were equivalent. Competition amongst enforcers may lower the effective price of bribes. This may be mediated by the increased probability of detection, as bribes, unlike punishments, are personally salient to enforcers. Thus, the deterrent effect of legal prescriptions is often mitigated by corruption [6]. For example, skewed incentives due to bribes, may color the efforts of law enforcement officers to prosecute criminals. An online analogy is that of the website certification industry as embodied by TRUSTe. Competition within the industry has arguably lowered the standards by which certifications were to be provided. Consequently, certified sites are more likely to be malicious [4].

Cybercrime may also be social welfare increasing in immediate jurisdictions [23]. Then, law enforcement is discouraged from prosecuting criminal behavior online, as the loss of local income would be immediate, while the negative externalities of such socially undesirable behavior are less tractable and delayed. Given equilibrium between extant cybercrime and legitimate enterprise, the former would act as a prohibitive tariff and prevent legal Information and Communication Technology (ICT) initiatives from being successful. Further, if legal enterprise is present, then it may be suppressed, as the marginal costs of cybercrime decrease faster than those of legitimate participation.

Simultaneously, while deterrence may be successful at diminishing the supply of cybercrime services, demand is not similarly impinged [24]. In the absence of legitimate affordable alternatives, offenders would simply be displaced to an alternative opportunity. Consider the persecution and resurgence of Megaupload. There may have been a decrease in copyright infringement, but only in the short term. The resurgence of Megaupload illustrates clearly that demand remains. Instead reduction in music piracy has been attributed to cheaper streaming services [33].

The goal of deterrence is to reduce crime. Deterrence is effective in the short term and limits the supply of cybercrime based goods and services. It also forces individual cyber-criminals to organize and thus makes prosecution more feasible. However, the deterrence only approach is more expensive than the negative effects of crime itself [3]. Deterrence is inherently limited in that it is reactive. A complementary approach proactively engages potential criminals as legitimate market participants [58].

3. POVERTY, UNEMPLOYMENT, AND INCOME INEQUALITY

If crime is not only the result of profit maximization by rational agents, then what additional explanations could there be? A Marxian explanation of crime argues that delinquent behavior is a function of underclass resentment of oppression [9]. This perspective on crime considers absolute and relative economic deprivation, including the examination of factors such as poverty and unemployment.

Absolute deprivation may result in prohibitively high entry costs for the community, which then would rationally resort to a low cost/high benefit venture, viz. cybercrime. If successful, the profits would be re-circulated into the local economy, making such activities socially acceptable [55] and economically rational [23]. For example, Venkatesh et al. notes that gangs in Blackstone used the illegal gains from drug distribution to fulfill community needs post–1980 and thus became more acceptable [55]. 419 scammers may be similarly relevant to Nigerian economy. Arguably, a limited amount of Windows piracy is welfare increasing even for Microsoft, due to network effects such as lock in (customer dependence on a specific vendor) and the development of local expertise [41]. Simultaneously, those who pirate software may become ICT professionals[1].

Crime may also be a function of relative deprivation within a community. When income inequality is high, individuals with limited economic resources would experience this relative deprivation as a prohibitive tariff on legitimate participation. If we consider the Internet a community without borders, the inequality between developed nations vs. developing or underdeveloped nations may be salient. For example, a licensed copy of Windows operating system that appears to be affordable in United States may cost up to $2000 in the local currency of another country (or 3 months salary). In this case the combination of income inequality and local limited resources can prevent an individual from buying a legal copy of a piece of software, forcing them to infringe on copyright [41].

The impact of economic deprivation is aggravated by lack of social support. Cullen argued that, despite being an affluent nation, United States suffers from disproportionate levels of crime, both violent and otherwise, due to the lack of adequate social support [16]. American society can undermine communitarian ideals by strongly embracing utilitarian individualism (and therefore self-interest). Cullen notes that the result may be limitations on the social bonds that engender trust and provide informal support. Formal social support provided by public bodies (for example governmental assistance which alleviates the impact of poverty, unemployment, and income inequality) lessens (violent) crime. Thus, the deterrence-based

[1] http://www.neowin.net/news/editorial-how-piracy-changed-my-life, Retrieved May 6th, 2015.

effort of the 'War on Drugs' is appropriately complemented by the 'War on Poverty'.

Social support can similarly facilitate legitimate participation in ICT markets. For example, private entities can alleviate the incidence of copyright infringement through appropriate pricing. It has been noted that copyright infringement of music in United States has decreased as cheaper options have become available [33]. Additional social support by private entities may include access to patches for machines running pirated copies of software. For example, Microsoft allows pirated copies of Windows operating system to access security critical patches. However, this could be extended to other patches and updates. The direct impact of this would be reduction in the overall harm created by having unpatched systems, decreasing botnet participation and incidents of zombies. When these patches are applied to systems running as servers, the risk mitigation is arguably more significant.

Social support can be provided by public bodies both online as well as off. Public adoption of technology could provide the necessary boost to a developing local ICT market. Such markets would in turn provide legitimate employment for those who would otherwise be engaged in criminal enterprise. For example, quality broadband can be subsidized and thus made affordable and accessible. Highly connected individuals can pursue appropriate employments opportunities outside of their immediate local ICT markets, for example through crowd-sourced labor markets [24]. Simultaneously, security solutions can be subsidized, e.g. cheap or free anti-virus software, which can discourage the exploitation of local systems. Current examples include American universities providing free access to anti-virus software and the American government providing access to NSA Security-enhanced Linux.

Criminals, much like everyone else, are not the strictly rational agents of economic models. Even well meaning individuals may resort to cybercrime when legitimate opportunities are too expensive to be pursued or otherwise effectively blocked. The negative impact of economic inequality, both absolute and relative, can be limited by social support from public and private entities. This implies that one approach to decreasing cybercrime is to subsidize legitimate participation, especially in developing ICT markets.

4. A STRUCTURAL EXPLANATION FOR CYBERCRIME

Section 3 discussed the economic imperatives that facilitate crime. However, neither economic inequality nor crime is uniformly geographically distributed. Crime is often endemic to specific neighborhoods. The foremost and most easily available characteristic of these neighborhoods is often poverty. However, other defining characteristics, i.e. 1) lack of informal social control, 2) residential mobility, 3) racial heterogeneity, 4) family disruption, and 5) urbanization, are equally relevant to the incidence of crime [48]. Structural theories of cybercrime address the implications of these characteristics offline, and may apply online as well.

Residential mobility is a measure of the frequency with which older residents are replaced by new individuals in a community. High residential mobility prevents neighbors from forming personal ties and engendering trust from long-term friendships. Racial heterogeneity may segment a community and impede communication. Such communities may often imbue common aspirations, e.g. lower crime rates. However, they simultaneously lack a consensus on the acceptable methods for realizing such aspirations. To the degree that two-parent households provide increased monitoring, family disruption impinges the quantity of guardianship, if not its quality. Similarly, urban neighborhoods would demonstrate lower social control, due to weak kinship. Together these distinct variables measure (the lack of) non-economic social support or guardianship from immediate family and the community at large. Are these relevant online?

Arguably, the evidence for mobility online is limited. In fact, communities are often forced to persist in suboptimal situations (e.g., in the face of decreasing privacy or increasing disruption) due to network effects, e.g. lock-in. Trust, however, cannot scale over a community as large as the Internet. Thus, technical solutions often incorporate notions of transitive trust, e.g. through certification authorities. However, these 'trust chains' are often opaque to end-users. The lack of transparency, allows attackers to hijack trust chains and enable attacks such as phishing. Certainly there are indicators of guardianship, e.g. SSL lock sign, TRUSTe certifications. The former is inappropriately used, for example by Paypal; their website includes a technically meaningless lock in the middle of the page. Simultaneously, TRUSTe certified websites tend to be less trustworthy due to incentive misalignment. In TRUSTe's case, their customer base is the website providers, not the customers. Thus, TRUSTe is economically invested in serving the providers rather than the community of users. It is rationale for TRUSTe to award certifications even when the website under consideration does not provide adequate privacy [19]. Certification authorities manifest similar problems [57].

Non-economic guardianship must then be enabled by alternative market and public mechanisms. In markets where public/private adoption of ICT goods and services is higher, such guardianship would be deemed important. For example, institutions that adopt ICTs would invest in adequate personnel training. Higher public/private adoption would also lead to (positive) externalities. First, by amortizing the cost over a larger set of users, the access to affordable legitimate software would be possible. Becoming a licensed windows vendor in a market of 1 is not economically rational, but would be in one that numbers in millions. Second, in such markets local after sales support would also become available, making legitimate software more valuable. Finally, a developed local ICT market would impinge the social acceptability of illegal participation.

Structural factors that facilitate crime have also been examined from the perspective of a routine activity theory [14], which argues that it is the structure of routine activities that enables crime. Routine activities are then considered ancillary to criminal enterprise. For example, property theft, due to breaking and entering, is dependent upon individuals leaving their homes unguarded to go to their respective jobs. Predatory crime is then not an indicator of social breakdown but rather a by-product of opportunity. For example, Parikka et al. argue that spam and viruses, while being anomalies, are a necessary (albeit dark) facet of the digital culture [45]. A trivial but necessary hypothesis then is that the increasing use of ICTs should be positively correlated with higher levels of cybercrime. However, incidence of crime is not simply correlated with size of market, be it at the ISP or national level.

The structure of routine activities may increase the prevalence of crime, as it impinges on the convergence of motivated offenders, suitable targets, and the absence of capable guardianship. For example, given that routine activities online often involve downloading attachments and clicking links embedded in email messages, the end-user is put at risk of downloading malware and accepting phishing links. Security tasks, such as patching, are in contrast often a distraction from routine activities and are thus ignored.

Community structures influence the incidence of crime and victimization. While trust is inherent to Internet usage, trust chains are easily compromised. Informal social guardianship is limited. For example, ISPs may not punish subscribers for knowingly hosting malicious websites; nor assist the recovery of those unknowingly hosting such sites. Even when guardianship is available, incentive misalignment may lead to adverse outcomes. The implication of the routine activity approach is that designs that impinge on trust should aim for transparency. Regulation should seek to enable guardianship through relevant local stakeholders. One approach is through community-based governance [42], by considering security to be a common pool resource [11]. Criminal actors often leverage extant structures, of routine activities, to attack both individuals and systems. Measures to enable security and reduce cybercrime must be similarly grounded, rather than being a distraction from the activities of the end-user.

5. A CULTURAL EXAMINATION OF CYBERCRIME

Another explanation of crime is grounded in culture. Cultural explorations of crime began with the examination of the prevalence of violence in the American South [47]. Arguably, specific cultural values of the South, such as historical traditions of chivalry, are critical to making aggression more acceptable in society. The deep embedding of such values has been explained by the loss in the Civil War, which may have resulted in a stronger desire for independent identity and the resulting cultural rigidity.

Explanations for crime in urban areas have also been grounded in the notion of identity and cultural rigidity. As urban areas expand an increasing number of culturally diverse communities interact [21]. These subcultures, thus co-located, compete to define the emerging identity of the group. While such disputes between subcultures are clearly problematic, the presence of a unique cultural identity may be problematic as well. Culturally desirable goals would then be uniformly acknowledged but access to the institutions and resources that enable such goals may be limited. For example, if there is a shared goal of Internet access then the lack of affordable access to the Internet could increase the acceptability of cybercrime. When the community values access to information, subversion of digital rights management systems may be lauded. Online opportunities may be further restricted by language [24]. A skewed distribution of opportunities could encourage non-conformity, which some scholars consider to be the natural response [31].

Similar arguments have been made for the prevalence of cybercrime in eastern European countries, specifically former U.S.S.R. and the respective loss in the Cold War. An authoritarian communist regime may encourage the thwarting of established institutions by asserting values or controls in conflict with the local culture. Thus, subverting the establishing institutions is seen as admirable or even necessary. This may subsequently transfer online. For example, an intellectual property regime may be perceived as an institutional structure that prohibits information access. Thus, copyright violations would then become socially acceptable. Further, the cultural understanding of capitalism may be myopic, valuing personal gain over societal values. Exploiting the Internet commons would then be socially justified.

Conformity is arguably the result of either unreasoned conditioning or a rational result of a utilitarian calculus [35]. Merton notes that while culturally desirable goals reflect humans' primitive drives, they are also determined by social structures that regulate and define the culturally acceptable means to achieve these goals. Thus, social institutions constrain the set of expedients (or a potential set of solutions).

There are two potential polar alternatives. First, there is the possibility that the institutions, which regulate behavior, are weak. In this case, criminal alternatives are constrained only by technical limitations. Thus, the failure of ICT markets in Romania may potentially encourage individuals to explore criminal as well as legitimate options online, as institutional forces may be weakened by misaligned incentives [23].

Second, appropriate conduct can become an end in itself and thus prescribes 'ritualistic conformity'. Online this can be seen as the prescription of password policies, such as mandatory password resets and guidelines for strong passwords. These policies are arguably both unrealistic as well as ineffective. Simultaneously, ritualistic conformity to cultural values, such as empathy, might increase the vulnerability to victimization as cybercriminals use legitimate charity credentials to con individuals, e.g. for disaster relief. According to the 2011 Internet Crime report, the most frequent scam online is individuals posing as FBI agents[2]. Here again ritualistic adherence to authority may perversely increase victimization.

These opposing conceptualizations do not manifest so long as the individuals who conform to the dichotomy of constraints are rewarded. Messner and Rosenfield argue that the primary source of increased crime in the US (compared to other Western democracies) is situated in the notion of the American Dream. The Dream of individual success invests excessive value in the notion of monetary success without providing for facilitating institutions [36]. While the culturally aspirational goal of the self-made man remains, social mobility is ever decreasing [7].

Consider an application of this to sharing material protected by copyright. Before the LaMacchia[3] rule, file sharing was the norm online . A ritualistic adherence to the values of free information nudged LaMacchia to share software to which he had access. While aligned with extant academic and Internet norms, his behavior was an extreme interpretation of acceptable practices. After the LaMacchia ruling, a host of legislation has discouraged file sharing, even when it is welfare increasing. Individuals are forced to break the rules to follow the norms, as the legislation has adopted the alternate extreme. Silverberg has observed that an

[2] http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf, Retrieved May 6th, 2015.

[3] http://www.loundy.com/CASES/US_v_LaMacchia.html, Retrieved May 6th, 2015.

average Internet user commits three felonies a day in the normal conduct of reading, browsing, and interacting with others. Thus, copyright infringement is the result of an anomie twixt the Internet's (perceived) goal of open access to information and intellectual property structures that constrain the set of legitimate expedients. The tragic death of Aaron Swartz brought this conflict of values again to the fore. The putative victim of his aggressive downloading, JSTOR, asked that no charges be filed. However, the Department of Justice, ironically, too demonstrated ritualistic adherence and pursued Aaron Swartz as a multiple felon.

Cultural and subcultural values also guide the actions of individuals and communities online. For example, while certain groups of people engage in online activism, others resort to hacktivism. An example of legitimate activism online would be the protests against proposed bills like SOPA and PIPA. The protests against these bills were a grassroots campaign that was subsequently supported by various corporate entities such as Google. Websites such as sopastrike.com provided a convenient method for individuals to express their concern over the bills.

In contrast to this, the protests against the increasing influence of the American military have leveraged the hacktivist ethic through institutions such as Wikileaks and Anonymous. Arguably, individuals did not have the same freedom to voice their antipathy towards American military action in Iraq or Afghanistan, as they did for SOPA and PIPA [44]. Freedom of expression is a cultural imperative, not only in United States, but also in most Western democracies. Thus, the absence of channels for legitimate protest encouraged individuals to explore alternatives such as Anonymous' Low Orbit Ion Canon (LOIC) and subsequent Distributed Denial of Service attacks against the Department of Justice [40].

It would be disingenuous to posit that absence or ineffectiveness of legitimate protest always leads to digital civil disobedience through hacktivism. For example, the 1994 protests against Clipper did not succeed per say [17]. Clipper was a chipset developed by the NSA to provide encryption for audio transmission. However, instead of witnessing the birth of a vigilante electronic group, Clipper met its death due to extensive lobbying from the industry. Simultaneously, when cultural aspirations are not supported by institutional structures, there can be positive innovation. For example, the arguably draconian nature of the extant copyright regime has encouraged individuals and organizations alike to provide their digital goods for free and instead ask for donations. However, it is important to recognize that in this case it was possible to create new institutional structures, such as Creative Commons, that aligned with evolving cultural values (of at least a subset of end-users).

Cultural factors also prevent the standardization of cybercrime definition across countries [20]. An expression of speech that is protected under the First Amendment in United States may be considered criminal in another country with more conservative values. The occupation of University of California campuses to protest against budget cuts in education in March 2010 was complemented by virtual sit-ins organized by Prof. Ricardo Dominguez and Electronic Disturbance Theater [25]. In the United States this was protected under political speech. However, this act of Electronic Civil Disobedience could also be perceived as a Distributed Denial of Service (DDoS) attack [60]. Similarly, while the DeCSS Haiku was perfectly legitimate, the distribution of code itself would invite prosecution [50].

Perfect enforcement is neither possible nor desirable. Cultural values frame the degree to which enforcement is desired. Breaking certain laws is often socially acceptable. Merely increasing punishments would not alter the social acceptability of non-compliance. Thus, cultural values should first be addressed by education and awareness. Simultaneously, the cultural rewards of non-conformity must be replaced with structural rewards; i.e. either reduce the costs of compliance or increase the rewards. These rewards must, however, be culturally situated. Thus, these rewards should replace what is culturally acceptable with what is culturally desirable.

6. IMPLICATIONS: TECHNICAL, POLICY, & DESIGN

Current investigations of cybercrime often differentiate it from crime in general. Cyber-criminals are assumed to be well educated and resourceful who choose to indulge in deviant behavior. Historically, white-collar crime was similarly differentiated in research and practice alike [54]. For white-collar crime, this differentiation was initially necessary to indicate that crime is not just a function of poverty and lack of legitimate opportunity [8], i.e. even the rich and powerful can indulge in deviant behavior. However, this differentiation limited the understanding of white-collar crime, as it suffered from a myriad of often-conflicting definitions and theories that explain its nature [15]. Arguably it is only useful to distinguish between white-collar crime and traditional crime, as between any specific category of crime and crime in general [29]. In fact, much of white-collar crime is explained by traditional theories of crime [30], e.g. general strain theory [2]. Cybercrime, while novel, might similarly have causes grounded in traditional forces of crime. Ignoring previous research might limit our understanding of the underlying driving factors and lead to an atheoretical mire similar to that experienced by white collar crime.

Traditional criminologists grappling with crime offline often ask: Why are crime rates high even though conditions that apparently engender criminal enterprise are being addressed? Online the questions are different. Why hasn't crime online increased exponentially, even though cybercrime appears to be a low-risk and high-returns enterprise? A potential argument is that cybercrime may not be profitable [27, 28, 32].

Cybercrime, however, remains a relatively low-risk enterprise, as prosecution is marred by jurisdictional boundaries. The cost of deterrence is also non-negligible and often greater than the losses from successful criminal enterprise [3]. To improve the efficiency of anti-cybercrime efforts, we must then explore alternatives to deterrence. Arguably, engagement in cybercrime is not always the result of a cost-benefit optimization by a rational agent. Potential explanations of crime online may then be explored in the economic, structural, and cultural theories that explain similar behavior offline.

A successful example of non-deterrence-based initiatives to reduce criminal activity online is given by the study of massive copyright infringement. Osorio concluded that massive copyright violations for software are a function of access and affordability, as explained by GDP per capita and the availability of post-sales software support in local markets [41]. Thus, infringement is the result of the consumer's inability to pay or lack of legitimate access to the resource, due, for example, to the absence of a legal distributor in local markets. Potentially successful solutions are

then price cuts, differential pricing [12], or providing local after-sales services [41]. Arguably, initiatives such as Netflix would be more successful at combating piracy than deterrence through misguided legislation such as SOPA [49] or an overly stringent Digital Millennium Copyright Act [22]. It has been noted, for example, that music piracy has gone down as cheaper alternatives for streaming have become available [33].

Along with income inequality, a second factor to address is community structure. It is evident that social organization is effective in curbing criminal enterprise. It enables the community to identify strangers and prevent predatory behavior. Such organization can be utilized to alleviate victimization online. Simultaneously, informal social control can act as constraints for potential delinquent behavior. Dong et al. propose technical solutions that leverage such social control [18]. A first proposal is to consider security as a club good, whereby a community of systems (considered as a neighborhood) would monitor each other for potential subversion, thus alleviating deviant behavior. The second solution is to consider security as a common-pool resource. Thus, patches available on an individual machine are considered to be a common pool from which individual members of the community, i.e. individual systems on a common network can engender guardianship in the form of timely and consistent updates.

Indicators of (security) guardianship are currently provided without accounting for incentive misalignment. Website certifications such as TRUSTe would thus be ineffective in the absence of legislation that hold such certification bodies accountable, e.g. through audits. Alternatively, guardianship for the community could arguably engender from its peers. Thus, technical solutions to peer produce security indicators should be made available [10]. An example of this is the Web of Trust plugin for web browsers. Simultaneously, the misuse of proven signals by private enterprise may need to be regulated. The SSL lock sign is an example of a signal that took years to be successfully culturally embedded in the common consciousness. However, its inappropriate usage by corporations such as Paypal has arguably reduced its effectiveness.

Addressing cultural norms may appear to be a herculean task, but it has been successfully achieved offline. For example, Iron Eye Cody's classic one-eyed tear has done much to alleviate the problem of littering in United States. It is important, however, to remember the limitations. Cultural values manifest inertia, and thus change is often slow. It took decades to tackle littering, while smoking is still being addressed. However, mediating cultural imperatives may be possible through a new cyber security doctrine, for example one grounded in analogies from public health [39]. This includes providing education about the causes and effects of insecurity, subsidizing security solutions both in terms of access and affordability, and identifying those infected with mandatory reporting requirements for specific incidences.

Initiatives such as STOP, THINK, CONNECT are addressing education but need to be scaled. Further, their methodology must be public and investigated with academic rigor to enable us to learn from both potential failures as well as successes. The practice of making anti-virus software free and available by certain educational institutions can be extended to a broader national policy to enable subsidized security. For example, Germany recently initiated the Anti-Botnet-Advisory Centre, whose goal was to identify zombies and subsequently clean the infected machines. The need for mandatory reporting was first acknowledged when California required companies to report security breaches and has now been taken up by (at least) forty-six US states.

Another potential solution is soliciting participation in open-source projects, where individuals who do not have formal training can learn through limited mentoring. This limited mentoring would also expose individuals to social norms about (un)desirable behavior outside of their immediate geographic community. Nigerian scammers, on interaction with ICT professionals from across the globe, may reconsider 419 scams. Simultaneously, legitimate participation would prompt such individuals to protect the resources they create. Finally, contribution to open-source projects may allow them to explore legitimate employment opportunities that would be less costly to pursue with established work experience as well as professional networks.

Finally, it would be a mistake to consider deterrence a wasted effort and thereby ignore the impact of litigation and enforcement. Becker proposes two apparently intuitive solutions. First, the monetary worth of punishments should be equivalent to the amount of damage (incidental as well as direct) caused by the criminal activity. This amount should be adjusted for the probability that the offender would evade detection or capture [5]. Second, the impact enforcement has can be improved by raising the salaries of public enforcers as well as encouraging a regime of private enforcers that are paid on a per enforcement basis [6]. An example of such private enforcement has been seen in academic investigations of the bug auctions markets [43], which has resulted in arguably successful practical initiatives such as the Google's Vulnerability Reward program.

7. CONCLUSION

Why are individuals in certain countries more likely to participate in cybercrime, either willingly as 419 scammers or unwillingly as in botnets? Are they merely rational actors choosing cybercrime when benefits outweigh costs? Or does the lack of resources and, thus, limited opportunities in local markets to support legal enterprise drive individuals? Alternatively, cybercrime may not be a characteristic of individuals but rather a function of jurisdictional dynamics. Cybercrime may also be driven by the strain between culturally important goals and the social structures that should facilitate such goals. It may be that individuals in all countries are similarly criminally motivated online, but only those with ample opportunity engage. Or is cybercrime a function of lack of social support for legitimate activity? Finally, cybercrime may be an artifact of either the prevailing local culture or in turn that of countercultural acceptance.

The argument to complement a narrow perspective of rational choice is non-trivial, and particularly relevant to policy. For example, a key argument, guided by rational choice, in copyright infringement has been that as piracy rates increase, offending individuals would spend less on legitimate media consumption. But in fact observed behavior indicates irrationality, as those who violate copyright more frequently also spend more on purchasing music legitimately [33]. Arguably, then policies such as SOPA would reduce economic activity by punishing those who contribute most to the market. Since human behavior is not strictly rational, policy prescriptions that are not adequately

accommodating could not only be rendered ineffective, but in fact have adverse outcomes.

The solutions to cybercrime are contingent on the distinct research threads available in criminological theories offline. Depending on the nature of cybercrime activity, all may apply, albeit to varying degrees. Technical solutions as well as policy prescriptions must be similarly informed to be effective in the long term. A first solution is to raise the cost of cybercrime. Simultaneously, the entry barrier for legal enterprise must be lowered. Existing legal enterprise must be discouraged from displacement. Engagement in cybercrime should be discouraged not just by law, but also alleviated culturally, for example through public service campaigns. Legal punitive measures should be complemented by community-based awareness campaigns, both to decrease the acceptability of cybercrime as well as to enable, acknowledge, and encourage legal enterprise.

8. REFERENCES

[1] A. Acquisti, C. Tucker, et al. Guns, privacy, and crime. In Proceedings of 9th Annual Workshop on the Economics of Information Security. WEIS, 2010.

[2] R. Agnew, N. Piquero, and F. Cullen. General strain theory and white-collar crime. The criminology of white-collar crime, pages 35–60, 2009.

[3] R. Anderson, C. Barton, R. Bohme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage. Measuring the cost of cybercrime. In Proceedings of 11th Annual Workshop on the Economics of Information Security. Springer, 2012.

[4] R. Anderson and T. Moore. The economics of information security. Science, 314(5799):610–613, 2006.

[5] G. Becker. Crime and punishment: An economic approach. The Journal of Political Economy, 76(2):169–217, 1968.

[6] G. Becker and G. Stigler. Law enforcement, malfeasance, and compensation of enforces. J. Legal Stud., 3:1, 1974.

[7] P. Blau and O. Duncan. The American occupational structure. John Wiley & Sons, 1967.

[8] W. Bonger. Criminality and economic conditions. Little, Brown, and Company, 1916.

[9] W. Bonger. Race and crime. Patterson Smith, 1969.

[10] L. Camp. Reliable, usable signaling to defeat masquerade attacks. ISJLP, 3:211, 2007.

[11] L. Camp. Re-conceptualizing the role of security user. Daedalus, 140(4):93–107, 2011.

[12] Y. Chen and I. Png. Software pricing and copyright enforcement: private profit vis-a-vis social welfare. In Proceedings of the 20th international conference on Information Systems, ICIS '99, pages 119–123, Atlanta, GA, USA, 1999. Association for Information Systems.

[13] R. Cloward and L. Ohlin. Delinquency and opportunity. Criminology Theory: Selected Classic Readings, page 149, 1998. 13

[14] L. Cohen and M. Felson. Social change and crime rate trends: A routine activity approach. American sociological review, 44(4):588–608, 1979.

[15] J. Coleman. Toward an integrated theory of white-collar crime. American Journal of Sociology, pages 406–439, 1987.

[16] F. Cullen. Social support as an organizing concept for criminology: presidential address to the academy of criminal justice sciences. Justice Quarterly, 11(4):527–559, 1994.

[17] D. Denning. Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. Networks and netwars: The future of terror, crime, and militancy, pages 239– 288, 2001.

[18] Z. Dong, V. Garg, A. Kapadia, and L. J. Camp. Pools, clubs and security: Designing for a party not a person. In Proceedings of the 2008 Workshop on New Security Paradigms. ACM, 2012.

[19] B. Edelman. Adverse selection in online "'trust" certifications. In Proceedings of the 11th International Conference on Electronic Commerce, ICEC '09, pages 205–212. ACM, 2009.

[20] K. M. Finklea and C. A. Theohry. Cybercrime: Conceptual issues for congress and U.S. law enforcement. Technical report, Congressional Research Service, 2012.

[21] C. Fischer. Toward a subcultural theory of urbanism. American Journal of Sociology, 80(6):1319–1341, 1975.

[22] M. Fortunato. Let's not go crazy: Why Lenz vs. Universal music corp. undermines the notice and takedown process of the digital millennium copyright act. Journal of Intellectual Property Law, 17:147–445, 2009.

[23] V. Garg, N. Husted, and J. Camp. Smuggling theory approach to organized digital crime. In eCrime Researcher's Summit. IEEE, 2011.

[24] V. Garg, C. Kanich, and L. J. Camp. Macroeconomic analysis of eCrime in crowd-sourced labor markets: Mechanical Turk vs. Freelancer. In 11th Annual Workshop on the Economics of Information Security. WEIS, 2012.

[25] D. Goodin. 'Virtual sit-in' tests line between DDoS and free speech. Technical report, The Registrar, 2012.

[26] S. Gordon and R. Ford. On the definition and classification of cybercrime. Journal in Computer Virology, 2(1):13–20, 2006.

[27] C. Herley and D. Florencio. A profitless endeavor: phishing as tragedy of the commons. In Proceedings of the 2008 Workshop on New Security Paradigms, pages 59–70. ACM, 2009.

[28] C. Herley and D. Florencio. Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. Economics of Information Security and Privacy, pages 33–53, 2010.

[29] T. Hirschi and M. Gottfredson. Causes of white-collar crime*. Criminology, 25(4):949–974, 1987.

[30] T. Hirschi and M. Gottfredson. The significance of white-collar crime for a general theory of crime. Criminology, 27(2):359–371, 1989.

[31] E. Jones. A valedictory address. International Journal of Psycho-Analysis, 27:7–12, 1946.

[32] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage. Spamalytics: an empirical analysis of spam marketing conversion. In Proceedings of the 15th ACM conference on Computer and communications security, CCS '08, pages 3–14, New York, NY, USA, 2008. ACM.

[33] J. Karaganis. Copy culture in the U.S. and Germany. Technical report, The American Assembly, Columbia University, 2012.

[34] R. Kornhauser. Social sources of delinquency: An appraisal of analytic models. University of Chicago Press, 1978.

[35] R. Merton. Social structure and anomie. American sociological review, 3(5):672–682, 1938.

[36] S. Messner and R. Rosenfeld. Crime and the American dream. Wadsworth Pub. Co., 1997.

[37] 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.

[38] M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage. Re: Captchas–understanding CAPTCHA-solving services in an economic context. In USENIX Security Symposium, volume 10, 2010.

[39] D. Mulligan and F. Schneider. Doctrine for cybersecurity. Daedalus, 140(4):70–92, 2011.

[40] Q. Norton. Anonymous tricks bystanders into attacking justice department. Technical report, Wired, 2012.

[41] C. Osorio. A contribution to the understanding of illegal copying of software: Empirical and analytical evidence against conventional wisdom. In Program on Internet and Telecoms Convergence. MIT, 2002.

[42] E. Ostrom. Reformulating the commons. Swiss Political Science Review, 6(1):29–52, 2000.

[43] A. Ozment. Bug auctions: Vulnerability markets reconsidered. In Proceedings of 3rd Annual Workshop on the Economics of Information Security, 2004.

[44] J. Padilla and A. Wagner. The outing of Valerie Plame: Conflicts of interest in political investigations after the independent counsel act's demise. Geo. J. Legal Ethics, 17:977, 2003.

[45] J. Parikka and T. Sampson. The spam book: on viruses, porn, and other anomalies from the dark side of digital culture. Hampton Press, 2009.

[46] I. Png, C. Wang, and Q. Wang. The deterrent and displacement effects of information security enforcement: International evidence. Journal of Management Information Systems, 25(2):125– 144, 2008. 15

[47] T. Pratt and F. Cullen. Assessing macro-level predictors and theories of crime: A meta-analysis. Crime and Justice, pages 373–450, 2005.

[48] R. Sampson and W. Groves. Community structure and crime: Testing social-disorganization theory. American Journal of Sociology, pages 774–802, 1989.

[49] J. Sanchez. SOPA, Internet regulation and the economics of piracy. Technical report, CATO Institute, 2012.

[50] S. Schoen. The history of the DECSS haiku. Technical report, Loyalty, 2012.

[51] C. Shaw and H. McKay. Juvenile delinquency and urban areas. Chicago, Ill, 1942.

[52] S. Singer and D. McDowall. Criminalizing delinquency: The deterrent effects of the New York juvenile offender law. Law & Society Review, 22:521, 1988.

[53] B. Stone-Gross, T. Holz, G. Stringhini, and G. Vigna. The underground economy of spam: a botmaster's perspective of coordinating large-scale spam campaigns. In Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats, LEET'11, pages 4–4, Berkeley, CA, USA, 2011. USENIX Association.

[54] E. Sutherland. White-collar criminality. American Sociological Review, 5(1):1–12, 1940.

[55] S. Venkatesh. The social organization of street gang activity in an urban ghetto. American Journal of Sociology, 103(1):82–111, 1997.

[56] S. Venkatesh. Gang leader for a day: A rogue sociologist takes to the streets. Penguin Pr, 2008.

[57] N. Vratonjic, J. Freudiger, V. Bindschaedler, and J. Hubaux. The inconvenient truth about web certificates. Economics of Information Security and Privacy III, pages 79–117, 2011.

[58] B. Wible. A site where hackers are welcome: Using hack-in contests to shape preferences and deter computer crime. Yale Law Journal, 112:1577–1623, 2003.

[59] N. Wiener. The human use of human beings: Cybernetics and society. Da Capo Series in Science, 1954.

[60] S. Wray. On electronic civil disobedience. Peace Review, 11(1):107–111, 1999.

[61] M. Yar. Computer hacking: Just another case of juvenile delinquency? The Howard Journal of Criminal Justice, 44(4):387–399, 2005.