Criminals and Cyber Attacks: The Missing Link between Attribution and Deterrence

Clement Guitton[1]
Kings College London, UK

Abstract

This paper revisits the claim that the state capacity of attribution works as a deterrent for criminals to launch cyber attacks. Motivated by other empirical evidence for other types of crimes that do not support the claim, this research designed two quantitative analyses to test it. The first experiment looked at macro-level variables at the unit of the state and found that attribution can act as a deterrent. However, a second experiment looking at individual cases distinguished between three types of population and identified only one population for which the attribution-deterrence nexus is valid. Grounded in control theory, the claim is valid for individuals with a sufficient knowledge about the attribution process, who act rationally, and who are concerned about the socio-economic cost of the punishment. Enhancing attribution mechanisms is unlikely to result in any change of behaviours for criminals who act without knowledge or only with a limited perception of the attribution mechanisms, or for individuals who do not fear punishments as society praises their technological skills despite their anti-social and unethical behaviours.

Keywords: attribution, deterrence, cyber-crime, cyber-attacks, policy.

Introduction

Many authors have written about the assumption that in the criminal context (as opposed to the strategic context with states as actors) the attribution problem hinders the application of deterrence. Boebert, an information security expert, imagines a situation in which perfect technical attribution is possible. He considers that attribution will deter criminals and non-state actors as 'punishment will be severe' (Boebert, 2010, p. 51). He writes 'perfect technical attribution and the associated fear of likely and unacceptable retribution will act as a deterrent'. Boebert does not base his claim on any evidence that an increase attribution would lead to deterrence. Other cyber security researchers write similarly about deterrence that 'the expectation of detection and redress inhibits data misuse and complements real-time access controls'(Pato, Paradesi, Jacobi, Shih, & Wang, 2011, p. 1072). The cyber security expert Richard Clayton (2005, p. 36) similarly writes in his PhD thesis that 'since defensive measures are unlikely to be effective, it is crucial to have deterrence through tracking and tracing'. The US 2011 strategy for cyberspace also includes deterrence via attribution mechanisms. The strategy reads: 'In the case of

[1]PhD Candidate, Department of War Studies, King's College London, Strand, London WC2R 2LS. Email: clement.guitton@kcl.ac.uk

criminals and other non-state actors who would threaten our national and economic security, domestic deterrence requires all states have processes that permit them to investigate, apprehend, and prosecute those who intrude or disrupt networks at home or abroad' (The White House, 2011, p. 13). Investigation and prosecution of crimes are part of the attribution process. Robert Knake, the director for cyber security at the White House since 2011, influenced this statement in the strategy. He declared during a hearing in front of the US House of Representatives a year earlier that: 'For deterrence to work, it is critically important that we know who has carried out the attack and thus attribution is a central component of deterrence strategy' (Knake, 2010, p. 2). However, he also acknowledged that deterrence might not be the right way to think for low-level threats (in comparison with nuclear threats), which include criminal attacks. Instead, Knake (2010, p. 2) suggested 'to reduce the scale of the problem by stopping threats as they unfold and by reducing the vulnerabilities that the threat actors make use of in their attacks'.

Yet, none of the authors cited above ground their work in theories of criminal justice and show empirical evidence for their assumptions. Is there any evidence that increasing attribution online will deter criminal behaviors? What theoretical and empirical evidence outside the Internet supports the belief that attribution can lead to deterrence? What evidence on the Internet supports it as well? If there is a lack of evidence that attribution can have a role in deterrence, what role can it play for cyber criminality?

Within the field of cyber criminality, I focus in this paper on cyber attacks. Two quantitative analyses collected evidence to study the missing link between attribution and deterrence. One looked at evidence from data at the unit of the state, while the other looked at data from individual cases. The analyses showed that attribution functions as a deterrent only for a specific population of cyber criminals. Attribution can deter Internet users who have knowledge about attribution mechanisms (legal or technical), and whose perception of the certainty of the police catching them affects their rational decision to commit a crime. Enhancing attribution mechanisms simply for deterrent purposes is likely to fail for other types of criminals. States need therefore to apply different policy to curb cyber crimes than solely based on deterrence.

This paper is divided into four sections. I will first review the different theories of criminal justice that can help explain why and how attribution can be a deterrent. Second, I will explain the methodology of the two experiments. Third I will show the results before discussing and concluding the paper.

Theory of criminal justice

Deterrence 'occurs when a potential offender refrains from or curtails criminal activity because he or she perceives some threat of a legal punishment for contrary behavior and fears that punishment' (Gibbs, 1985, p. 87). It is therefore based on an underlying model that criminals act upon rational choices, and that certain policy to 'heighten the costs of illegal conduct' can turn criminals away from committing their acts (Pratt, Cullen, Blevins, Daigle, & Madensen, 2006, p. 367). Seemingly supporting the argument is the common idea that hackers show a 'strong preference for rational decision-making processes' (Bachmann, 2010). But two arguments may already thwart the rational hypothesis for online criminal behaviors. First, it emerges from discussions with hackers that there are uncertainties about the legality of certain of their actions or the legality of their 'tools' such as a port scanner (Holt, 2007, p. 190). Second, a few hackers consider that their actions should not be illegal (for instance, probing networks to enhance security as a common

good for society), and that they achieve larger educational purposes. As such, they mainly consider the positive outcomes that their hacking brought to society (Turgeman-Goldschmidt, 2008, p. 391). Some who hack for curiosity hold the same argument in defence of their actions (Smith, Grabosky, & Urbas, 2004, p. 112). Sykes and Matza (1957) defined such a defence (albeit in a context of juvenile delinquency) as two of five techniques for neutralizations that they called 'denial of victim' (e.g. 'we weren't hurting anyone'), and 'condemnation of the condemners' (e.g. 'they're crooks themselves'). The neutralization techniques help the offenders justify his actions. The three other techniques are denial of responsibility, denial of injury, and appeal to higher loyalties (Sykes & Matza, 1957). Despite the limitations of the rational model, considering specific cases where it can apply in contrast with other theories of criminal justice can help understand online behaviors, and more specifically cyber attacks.

Critics of the rational model invoke two arguments: that there is little evidence on the role and knowledge of the public of sanctions, and that 'we have much reason to believe that many crimes are committed on impulse, either under the influence of alcohol or simply as the result of opportunity and need intersecting' (Jacob, 1978, p. 584). Cases exist of offenders carrying out their offense not based on rational decision or on the certainty or severity of punishment. It seems therefore reasonable to discern that not all criminals act under reason, and not all crimes are results of impulse and emotions. Even in cases where they would act under reason, the limited information they may have to weigh their decision (e.g. their knowledge of the law), and other limited resources bounds the rationality of the decision.

Considering that a hacker acts rationally and is cognizant of the technical, political and legal details of attribution, this knowledge may push the hacker to take further measure to commit his crime to evade attribution, rather than be deterred. One of the further measure he could take is for instance to route his traffic via a country which does not criminalize cyber attacks, or which does not cooperate with foreign law enforcement agencies. The consequence of such a routing is for the investigative party to notice an apparent, albeit not real, displacement of the source of the crime. The displacement of crime has several implications on how a state will go about to tackle crime. The state will for instance focus on strengthening cooperation with the apparent state of origin. While praise-worthy, such a policy would not address the core issue, namely the criminal still acting, and furthermore still acting from the same location as he used to. The question that remains for the state is hence: can hackers be deterred, and especially by increasing attribution?

As the perception of the likeliness of punishment is a predominant factor in effective deterrence, it is natural to wish to be able to measure such a perception. Media outlets are an important source of influence, and focusing on the media is as such logical as well. Png and Wang (2007), two cyber-security researchers, showed by looking at media reports that an increase enforcement of the law reduces by roughly 35% the number of attacks in the following two weeks. Yet, many cyber attacks, especially on companies, go unreported, as companies fear to suffer further damage to the reputation if the public was to learn about the attack. By basing their research solely on publicly known breaches, the researchers face an important methodological constraint, also limiting the application of their results. They based their research on 49 cases spanning eight countries. They showed that there is a significant negative correlation between the number of cases solved by the police and the crime rates. But a negative correlation between the number of cases solved by the police

and the crime rates does not prove that certainty of punishment acts as a deterrent (problem of simultaneity). It can prove either that criminals responded to police changes of behaviors, or that the police responded to criminal change of behaviors. Simply increasing the number of resources is therefore not enough in many instances to decrease the rate crime. For instance, the Kansas City Patrol Experiment showed that simply increasing the number of police patrolling the Kansas area did not have any 'impact on the level of crime or the public's feeling of security' (Kelling, Pate, Dieckman, & Brown, 1974, p. vii). Further research is hence necessary to support the significance of Png and Wang's findings.

Moving beyond the mere perception of punishment to the actual punishment, many studies have found that increasing the severity of a punishment does not act as an effective deterring factor, especially due to the limited knowledge of the potential offenders of the law (Assembly Committee on Criminal Procedure (California), 1975, p. 78; Tonry & Farrington, 2005; William, Gibbs, & Erickson, 1980). But an increase of the severity of punishment can also be interpreted differently and in a wider meaning. John Braithwaite wrote in 1989 at the very beginning of an influential book that 'societies with low crime rates are those that shame potently and judiciously; individuals who resort to crime are those insulated from shame over their wrongdoing' (Braithwaite, 1989, p. 1). Braithwaite's theory seeks to prevent crime not by deterrence, but by making more salient the feeling of shame for deviant behaviors. How can the state apply reintegrative shame theory for criminal behaviors on the Internet? The anonymity of the medium can prevent the offenders from a community to shame him for his actions. Hence, increasing attribution can result in a decrease of disinhibition (acting as psychological constraints upon crime), but only for individuals who already show strong communitarianism and interdependency. If his actions were to attack a technical device, there is limited evidence that hackers feel shame for their attacks (Turgeman-Goldschmidt, 2008). In many instances, they find new job opportunities as society recognizes and need their technical expertise to prevent further security breaches. The case of Owen Thor Walker, aka AKILL is telling. In December 2007, the New Zealand police arrested him in his bedroom, then aged 17 years old. The New Zealand police arrested him as part of a larger police operation led by the US Federal Bureau of Investigation. They accused Walker of being the leader of a group of hackers that operated a large botnet, and who had swindled £12.5 million (McMahon & Johnson, 2007). Walker faced a 10-year jail sentence. The head of the police electronic crime centre described Walker as very bright and was impressed by Walker's technical skills to write malicious codes that evaded the watch of most commonly used anti-virus software. A year and half later, Walker received his sentence. The court fined him to £5,500 for cost and damages, then discharged him so that he could work with the police to tackle online crime (Johnson, 2008). Paradoxically, society welcomed to some extent Walker's actions. He cannot have felt shamed as a punishment reduction and a job offer praised him for his skills and knowledge, putting aside what he has done with them. Braithwaite writes that 'shaming is needed when conscience fails', but paradoxically, for shaming to be effective also requires the individual to consciously understand the deviancy of his actions. Reintegrating communitarianism and interdependency, for which online identification is not an absolute requisite for online community, is a remedy for the effectiveness of shaming, or the fear of it. A change of policy should not only address Internet behavior, but should also address very broadly the deeper and more complex societal problem of individualism. Braithwaite, especially as he takes family as the first

social sphere for the application of reintegrative shaming, advocates education at an early stage for the conscience to be shaped in certain ethical ways.

To summarize, theory on deterrence informs the assumptions for criminal activities carried through the Internet in the following ways. Assuming that the criminal operates following a rational model, the severity of punishment is unlikely to have any impact on his decision to carry out an action. The difference of treatment of cyber criminals should therefore not affect the collection of data across countries. On the other hand, the certainty of punishment, in this case, the certainty of attribution, may play a role in deciding to act or not. However, weighing the certainty of attribution is not a process that can be easily done. It involves knowing enough about the technical and legal process of attribution, and what their limitations are. Only technological savvy users will be able to carry out a reasonable assessment of the risk this way. Media will mainly influence the other Internet users in their assessment that is more likely to be based on the perception of the likeliness of attribution broadcast by the media rather than on any factual knowledge. From other criminal theories, and first by considering reintegrative shaming, attribution may not play a role for hackers, the most technologically savvy users. Their desire for recognition by their peers, and the respect and needs of Western societies to understand technical systems are all values that contribute to the hackers not feeling shame. The lack of shame that hackers may feel implies that attribution is unlikely to deter them from committing crimes. For other individuals, shame may only play a role insofar as they are aware that their actions are illegal and can be attributable. As other theories of criminal justice (strain, opportunity and learning theory) put the onus on other societal factors to explain criminality, attribution will not play a role within this particular set of theories. I will therefore restrain the interpretation of empirical results on the nexus attribution-deterrence to only the rational model and reintegrative shaming theory.

Methodology

The hypothesis is: if the state increases its mechanisms for attribution, or if the perception of the likeliness of attribution increases, then the number of cyber attacks decreases. I will test this hypothesis through two experiments.

Experiment 1

To replicate empirical results to bring evidence that increasing means for attribution can create deterrence, one must consider specific computer crime data, such as: cyber crime arrest ratio, cyber crime rate, age/sex of offenders, punishment, number of officers in the cyber-team, budget for cyber police. Whereas in Wilson and Boland's study the most appropriate unit of analysis was the city, the most appropriate unit for the Internet is the country. On the Internet, the exact location may not matter as much as the jurisdiction under which an individual operates. Yet, focusing on countries also creates further difficulties for comparison. Policies to curb cyber crime will be different, as well as social and structural constraints that act as factors for crime control. Policies for cyber crime encompass a wide range of technico-legal means, touching upon transactional data retention regimes, to copyright infringement authorities. Ideally, it would be interesting to study changes in regulations to improve attribution and its consequences it had on deterrence. For instance, the European data retention directive (2006/24/EC) stipulating that member states can oblige communication providers to retain transactional data for up to two years. Another example is the generalization of this directive for all content

providers by France in 2011 (*décret* n° 2011-219). But the time frame is too narrow to be able to have data to study the impact of such a regulation. With enough data on arrest ratios and criminal rates, one could consider if legislation to retain transactional data (either for communication providers, or any content providers) has an effect on crime rate. But the problem is that many countries do not separate the means used to conduct a criminal activity from the criminal activity. For instance, many countries do not separate for criminal rates for fraud between carding (reproduction or exchange of data on credit cards), from scams or identity theft. Moreover, if the police in certain countries publish the number of cases they have solved, they do not publish the arrest ratio or the number of unresolved cases. Using surveys carried out by non-official entities allow for extrapolating data, but also introduce a non-negligible bias. Another variable to heed is the rise in opportunities linked with the rise in number of systems available. The rise in crime rate can be reasonably expected to rise following this increase.

Table 1 Gathered data for Experiment 1

	Year	Total number of businesses under attack	Number of cases solved by the police	Number of police	Unemployment rate	Internet penetration rate	Media displaying likeliness of attribution
France	2003	128983	65223	35	9	36.1	0
	2004	125404	59964	35	9.2	39.15	0.105
	2005	134539	51644	35	9.3	42.87	0
	2006	150577	43363	103	9.2	46.87	0.04
	2007	168106	38453	156	8.4	66.09	0.029
	2008	181330	40458	200	7.8	70.68	0.038
	2009	184151	52353	232	9.5	71.58	0
	2010	171112	77646	253	9.8	72	0.054
UK	2003	177076	30000	40	4.6	63	0.037
	2004	291366	36000	40	4.7	65.61	0.02
	2005	405656	48000	40	4.8	70	0.03
	2006	519946	54000	40	5.4	68.82	0.015
	2007	634236	30000	40	5.3	75.09	0.014
	2008	748526	36000	60	5.7	78.38	0.083
	2009	862816	30000	70	7.6	78	0.074
	2010	977106	54000	80	7.8	79	0.027
Germany	2003	120000	57490	20	9.8	62	0.014
	2004	491628	54926	20	10.5	64.73	0.021
	2005	495563	43058	20	11.2	68.71	0
	2006	515245	36550	30	10.2	72.16	0.012
	2007	502308	34180	40	8.8	75.16	0.025
	2008	478031	37900	60	7.6	78	0.014
	2009	454653	50254	80	7.7	79	0.018
	2010	512745	59839	92	7.1	80	0.009

By looking for available data, France, Germany and the UK appeared as appropriate candidate for this research, as they made public sufficient data to apply empirical statistical tests on them. I hence considered the number of attacks carried out on businesses between 2003 and 2010 in France, Germany and the UK as an output variable of a function of: the number of criminals found guilty of cyber offenses, the number of police staff working in a cyber crime unit, the number of articles in a major newspaper in the country relating to the likeliness of attributing cyber attacks, the unemployment rate and the Internet rate. I extrapolated the number of attacks on all businesses from surveys (the *Clusif* in France, *Corporate Trust Studie* in Germany and from *PricewaterhouseCoopers* in the UK) and from the official number of businesses registered in those countries. For years where no data existed, I extrapolated data with a polynomial function of fourth degree or a cubic polynomial function when appropriate. The unemployment rate and the Internet rate are control variables. Furthermore, I assume that the number of media articles pertaining to cyber attacks plays a role in the hacker's perception of the lack of attribution for crimes. The media stance on issues of 'cyber war' for instance often mentioned that attribution online was difficult. Other reports of arrests of cyber criminals, domestic or abroad, similarly shape individual's perception of the likeliness to be caught. Although the number of articles in the media is a biased measure of influence, it is a necessary variable to take into consideration. It is also a similar methodology to the one used by Png and Wang (2007) in their studies. One does not specifically know which media a person follows, and it is fair to assume that not only one source of media will influence a person's perception of the likeliness of attribution. Nevertheless, representative media outlets will reflect a general sense of the perception of the likeliness of the police catching a cyber criminal. The rate is the number of articles discussing cyber criminals being caught against the number of articles discussing hacking or cyber security in general.

Experiment 2

All the hurdles mentioned with the Experiment 1 call for a joint study with another methodology to further prove or disprove the correlation between cyber crime and attribution. A second experiment will look at a set of cases where all individuals went on trial, and attempt to see if they made rational choices to consider evading attribution. The set includes 46 cases where the offense was a breach of an information system committed in France, Germany and the UK between 2003 and 2010, and excluded cases of unintentional or accidental breaches. As the police caught all criminals in this dataset, it is not possible to distinguish if attribution mechanisms deterred potential criminals to commit crimes, or if the police only caught the less able to hide. But as a few criminals made rational and conscious attempts to evade attribution, this means that the anonymity factor is likely to have played a primary role in their decision to pursue crime online. The erasure of log files, and the use privacy-enhancing technology indicate that they would not have committed crime had they not been as certain not to be found. But this concerns only a small proportion of all cases (13%), and other variables can provide a more coherent picture of their behaviors. Such variables will look at the use of real names by the perpetrator, or if they claimed the actions. By claiming the actions (either under a pseudonym, or under their real name), it means that they valued recognition over the certainty of not leaving any trace in order not to be caught. I used initially 52 variables, but not all variables turned out to be significant, or to shed light on the attribution-deterrence nexus (see Appendix A for the variables).

Table 2 List of cases

Name of the criminals or reference	Country	Year
Cedric M	France	2010
Guy R.	France	2010
B. Hugo	France	2009
C. François aka Hacker Croll	France	2009
Damien B. v. FTP	France	2008
Anthony C.	France	2007
L'Agitateur Floral / Réseau Fleuri	France	2007
M. B.	France	2006
Michel M.	France	2006
Hugues B	France	2006
T. Trinh Nghia v. MM. D. Guy et C. Grégoire	France	2005
Smith and Nephew	France	2003
Antoince C v Tati	France	2002
Antoine C. / SA TATI	France	2002
Philipe P.	France	2002
Christian M. Denniz A.	Germany	2011
BGH 4 StR 338/10	Germany	2010
10 Ls 275/10	Germany	2010
3 KLs 1/11	Germany	2010
13 Ls 171 Js 13423/08	Germany	2010
4 StR 555/09	Germany	2009
Sasser-Wurm-Prozess	Germany	2005
James Jeffery	UK	2012
Andrew Jonathan Crossley	UK	2012
Glenn Mangham	UK	2011
Paul McLoughlin	UK	2011
Zachary Woodham and Louis Tobenhouse	UK	2010
Ruth Jeffery v. Shane Webber	UK	2010
Ashley Mitchell	UK	2009
Nick Webber	UK	2009
Dale Trever	UK	2008
Daniel Woo	UK	2006
Matthew Anderson	UK	2006
Balwinder Basran	UK	2006
Robert Campbell	UK	2006
Susan Holmes	UK	2006
Mark Hopkins	UK	2005
Daniel Cuthbert	UK	2005
Joseph McElroy	UK	2005
Matthew Byrne	UK	2004

David Lennon	UK	2003
Aaron Caffrey	UK	2003
Simon Vallor	UK	2003
Raphael Gray	UK	2003
Paul Brogden	UK	2003
William Culbert	UK	2003

Similar to the previous experiment, I applied a linear regression with the output variables 'claim status' and looked at the significance of the relation with the following variables: use of privacy-enhancing technology and deletion of logs, police identification of the criminals (as opposed to a third-party), motivation of the criminal (e.g. curiosity, challenge), the type of target, and punishment received. The assumption in running the regression analysis is that individuals who seek a challenge would want their exploit to be acknowledged and will claim the attacks. By doing so, the possibility of attribution is actually an important part of encouraging them to pursue the criminal activity, regardless of the certainty of punishment or severity of it. Moreover, all the criminals who decided to commit their crime had differences in their modus operandi (e.g. use or non-use of privacy-enhancing technology). These differences can highlight the criminal's perception of the level of believed possible attribution, or his desire for attribution. The significance of the correlations between the variables can inform on these nexus.

Results

Experiment 1

In the first experiment, I considered macro effects of policy. Three of the five variables were significantly related to the total number of attacks, which included the control variable for the unemployment rate (negatively related). The number of cases solved by the police is positively related to the number of businesses undergoing attacks (at the 0.05-threshold). It shows consistency and perseverance of the police in their task of tackling cyber crime, and is a result fairly expectable. But the lower rate with which the police solve crimes in comparison to the rate with which criminals commit them may still encourage criminals in their deviant behavior. Moreover, the rate of articles published by newspapers and showing a lack of attribution over the course of eight years is positively related to the number of attacks (0.01-threshold). It is coherent that the media's number of reports of cyber attacks increases as the number of cyber attacks increases. But by looking at the number of reports that show the lack of attribution, the statistic depicts that media reports play a role in encouraging deviant behavior by showing the lack of attribution. This means that if the perception of likeliness of the lack of attribution decreases (through media reporting more than the police catching cyber criminals, or media reporting that the police caught more cyber criminals), then the number of cyber attacks decreases. Hence, the results of the linear regression converge in showing that an increase in the likeliness of attribution or its perception results in a decrease of cyber attacks. The decrease in cyber attack shows that there is no incentive for attacks, where attribution functions as a deterrent factor.

Table 3 P-values of the correlation with the total number of attacks

	Number of cases solved by the police	Staff for police	Unemployment rate	Internet penetration rate	Media & attribution
p	0.036	0.72	0.01	0.61	4.31E-05
t	-2.26	0.36	-3.30	0.52	5.36
β	1299826	1.15	-1843	9914	16007

I also obtained a further significant statistic by running correlations between the variables. The number of attacks was positively correlated with the number of police staff ($p<0.01$), suggesting that either the number of policemen followed an increase in cyber crime as a policy to reduce it, or that an increase of cyber attacks followed an increase of policemen working on cyber crime. The latter being reasonably unrealistic, it implies that the countries' response of an increase of policemen may have limited the increase of crime, but was not fully functional as to curb it. Hence, the quantitative analysis fail to reject the hypothesis that attribution, or the perception of its likeliness, can act as a deterrent. The variables converged in showing that the lack of attribution can work as an incentive for attacks.

Experiment 2

The second experiment considered case-by-case results, which led to distinguishing two populations of cyber criminals. The linear regression considered the claim status and the output variable. Only the hiding of transactional data by the criminal was significantly correlated with the claim status ($p<0.01$). The criminals claimed the attacks paradoxically also when they tried to hide their transactional data. Only the most technology savvy users caught by the police had the knowledge to hide their traffic data. These users form a distinct population in the research, that I will call population A ('most technology savvy hackers' in other words). Hackers as part of a subculture, seek recognition through claiming attacks. The recognition they seek does not involve receiving a punishment by the state, but recognition by their peers still trumps the potentiality of being punished by claiming their actions. Interestingly, criminals claimed breaches more when they succeeded in stealing information from the victims rather than money. Stealing money, via carding for instance, is not an outcome that hackers seem to enjoy gloating about. They probably perceive the release of information as yielding more praise for their actions, as many people can benefit from them and they are appreciated for their actions.

Of the other correlations, 19 were significant at the 0.01-threshold but not all are of interest for the link attribution-deterrence. Criminals who deleted logs were also cautious of protecting their anonymity by using privacy-enhancing technologies. This nexus is rather trivial, and self-explanatory from the above paragraph. From the datasets, the identification by the police was significantly relevant if the target was an individual rather than an organization, and if the motivate of the criminals was to harm the victim rather than benefit himself or the victim (as in the case of security probes). Moreover, when the police was the entity who identified the individual, there is a strong link with the use of solely digital evidence, but not intercepted during the criminal activity (recorded only). This implies that criminals left enough evidence for the police to catch them. As the police obtained enough digital evidence to solve the cases, it shows that the success of the police was contingent upon the lack of knowledge of the criminals to remove evidence,

or upon the criminal's belief that he would not be caught, or that these factors were irrelevant for the criminals when he decided to carrying out his deviant act.

Table 4 Variables used for Experiment 2

Type of known perpetrator of the breach
Insider (or former insider) to the group targeted/close relation to the individual/group targeted
Number of perpetrator
Age of the attacker(s) (average in case of a group)
Type of believed perpetrator prior to identification
Type of target(s)
Motivation (intended/stated): harm of benefits
Motivation (intended/stated): type
Motivation (intended/stated): unintended or not guilty
Motivation (believed by the prosecution or the attacked party): harms or benefits
Motivation (believed by the prosecution or the attacked party): type
Motivation (intended/stated): unintended or not guilty
Consequences for the perpetrator: harms or benefits
Consequences for the perpetrator: type
Number of people harmed/affected
Number of companies affected
Number of people who benefited or try to benefit
Number of companies who benefited or try to benefit
Consequences for the victim(s) attacked (economic, IP theft, etc.)
Were the perpetrators of the incident identified by a law enforcement agency?
Were the perpetrators reported to the police?
Were the perpetrators of the incident arrested?
Were the perpetrators arrested as part of a larger wave of police arrests?
Did a previous arrest/or seizure of material inform this arrest?
Were the perpetrators found guilty?
How many months in prison/restricted liberty did they receive (average)?
How much fine did they have to pay (average)?
How many hours of community service did they have to serve?
Did the perpetrator try to hide his transactional data (e.g. proxy, IP spoofing)?
Did the perpetrator try to hide his actions (e.g. deleting logs)?
Did the police use recorded transactional data to find the author?
Did the police use live-collected transactional data to find the author?
Was the perpetrator accused of committing identity theft?
Did the perpetrator obtain material enabling him to further commit identity theft?
Did the police use non-digital forensics to find the perpetrators (non-exclusively)?
Did the police use only digital evidence?
Did the police use only non-digital evidence?
Were log files used to find the perpetrators?
In case the perpetrator(s) generally used privacy-enhancing technology was he found because he forgot it once?
or because the technology failed him?

or because he left other information (be them essential to his criminal activity or not)?
In the case of the use of privacy-enhancing-technology, did the police make the link with his previous breaches because he left a name/pseudonym behind?
or because he used a similar modus operandi?
Was the breach declared to be an accident at any point during the investigation?
Was it concluded that the breach was an accident?
Claim status
Funding (from the perpetrator): Economic return
Economic damage for the target
Was/were the perpetrator(s) involved or believed to be involved in any type of fraud to fund other cyber incidents?
Did the perpetrator(s) move money using a complex scheme?
Consequences on the information system
Has any ransom being asked for releasing data?

As there is also a strong evidence of the police using solely digital evidence when no individual claimed the breach, this reinforced the difference between population A and B. Users of population A were savvy enough to delete evidence, but the police still found them as they claimed responsibility for the criminal activity. Improving technical attribution will not affect population B, as it is unlikely that they would consider further how to evade new techniques (current ones being already sufficient). Similarly, improving legal mechanisms for attribution is also unlikely to encourage users of population B to use more advance techniques to evade attribution.

Discussion and Conclusion

The first experiment confirmed that attribution plays a role in deterrence, in opposition to the results from the second experiment. What can explain this discrepancy? The first experiment supports that there is a third population of criminals who breach information systems. This population is characterized by their sufficient knowledge about attribution, and by their desire to avoid any forms of punishment for deviant act. They are as such a sub-category of population A, on which the factor attribution and certainty of punishment is a rationale for deterring them from committing the deviant act. Under control theory, they are opportunists for whom attribution acts as a constraint regulating their correct norms of behavior. To summarize, I identified three populations of cyber criminals. The first one regroups individuals who know about attribution but still act (population A-1). They act upon emotional impulses and do not fit under the rational theory model, or upon an urge to be acknowledged and praised for their actions, which is the prime motivation to take up the challenge. Individuals belonging to the second category know about attribution and this knowledge is sufficient to dissuade them from acting (population A-2). Last, the third population (population B) is characterized by a lack of understanding of the technical or legal systems enabling attribution.

Of the three categories, this research has shown that enhancing attribution can only work as a deterrent for population A-2. It implies that a deterrent strategy for cyber crime must heed other elements than simply trying to enhance attribution capabilities, although other policy can be challenging to implement. Following reintegrative shaming theory, a part of population A-1 could be dissuaded from acting by changing the normative

environment that deals with the perception of highly technically savvy cyber criminals. As the logic goes, they have a deep understanding of cyber security problems and represent therefore an important asset for any entity seeking to enhance their cyber security. Their reintegration into society happens as no shame has been forced upon them, as members of their hacker subcultures and members of the general public praise their actions, regardless of the hacker's genuine motives for their criminal actions. From afore cited previous empirical research, amending the severity of punishment is unlikely to have an effect to dissuade these hackers. Society needs to act at different levels to change the perception of these individuals as being shame-worthy. Last, population B is not responsive to any perception relating to the certainty or of the severity of the punishment. Two different policies are possible to turn individuals of population B away from committing crimes. First, the onus can be put on companies to produce 'secure' products, where the difficulty of perpetrating attacks is levelled up. By reducing the crime opportunity, they would force the individuals to become more technologically savvy to perform a breach. I already identified earlier that the knowledge factor on technology is correlated with the attribution factor, which could act then as a deterrent. Second, following opportunity theory and learning theory, if society can succeed in establishing norms or good behavior online, via formal education or via the media and group behaviors, individuals from population B are likely to turn away from crime.

Acknowledgment

The author wishes to thank Peter McBurney, Fiona Gamble and anonymous reviewers for their helpful comments that helped to revise this paper. A grant from the UK EPSRC through the "Interdisciplinary Informatics: Bridging the Gaps" project (Grant EP/J501657/1 to Department of Informatics, King's College London, 2012) partially funded this research.

References

Assembly Committee on Criminal Procedure (California). (1975). Public knowledge of criminal penalties. In R. L. Henshel & R. Silverman (Eds.), *Perception in Criminology*. New York: Columbia University Press.

Bachmann, M. (2010). The Risk Propensity and Rationality of Computer Hackers. *International Journal of Cyber Criminology, 4*(1&2), 643-656.

Boebert, W. E. (2010). *A Survey of Challenges in Attribution*. Paper presented at the Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, Washington DC.

Braithwaite, J. (1989). *Crime, shame and reintegration*. New York: Cambridge University Press.

Clayton, R. (2005). *Anonymity and traceability in cyberspace*. (PhD), University of Cambridge, Cambridge. (653)

Gibbs, J. P. (1985). Deterrence Theory and Research *Nebraska Symposium on Motivation : The Law as a Behavioral Instrument* (Vol. 33). Lincoln: University of Nebraska Press.

Holt, T. J. (2007). Subcultural evolution? examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior, 28*, 171-198.

Jacob, H. (1978). Rationality and Criminality. *Social Science Quaterly, 59*(3), 584-585.

Johnson, B. (2008, 16 July). Cybercrime: Teenage hacker in global scam discharged, *The Guardian*. Retrieved from http://www.guardian.co.uk/technology/2008/jul/16/hacking.security

Kelling, G. L., Pate, T., Dieckman, D., & Brown, C. E. (1974). The Kansas City Patrol Experiment Washington, D.C.: Police Foundation.

Untangling Attribution: Moving to Accountability in Cyberspace, United States House of Representatives, 2nd Session Sess. 12 (2010).

McMahon, B., & Johnson, B. (2007, 1 December). Teenager accused of leading £12.5m cyber crime team, *The Guardian*. Retrieved from http://www.guardian.co.uk/technology/2007/dec/01/hacking

Pato, J., Paradesi, S., Jacobi, I., Shih, F., & Wang, S. (2011). *Aintno: Demonstration of Information Accountability on the Web*. Paper presented at the International Conference on Privacy, Security, Risk, and Trust, Boston.

Png, I. P. L., & Wang, C.-y. (2007). *The Deterrent Effect of Enforcement Against Computer Hackers: Cross-Country Evidence*. Paper presented at the Workshop on the Economics of Information Security, Pittsburgh.

Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., & Madensen, T. D. (2006). The Empirical Status of Deterrence Theory: A Meta-Analysis. In F. Cullen, J. Wright & K. Blevins (Eds.), *Taking Stock: The Status of Criminological Theory*. New Brunswick: Transaction Publishers.

Smith, R. G., Grabosky, P. N., & Urbas, G. F. (2004). *Cyber Criminals on Trial*. New York: Cambridge University Press.

Sykes, G., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review, 22*, 664-670.

The White House. (2011). *International Strategy for Cyberspace*. Washington, D.C.

Tonry, M., & Farrington, D. P. (2005). *Crime and Punishment in Western Countries, 1980-1999* (Vol. 33). Chicago, London: The University of Chicago Press.

Turgeman-Goldschmidt, O. (2008). Meanings that Hackers Assign to their Being a Hacker. *International Journal of Cyber Criminology, 2*(2), 382–396.

William, K. R., Gibbs, J. P., & Erickson, M. L. (1980). Public Knowledge of Statutory Penalties: The Extent and Basis of Accurate Perception. *The Pacific Sociological Review, 23*(1), 105-128.