# From Criminal to Digital Criminal Profiling: Advances in Criminal Profiling in the Digital Age

George Chlapoutakis
SecurityBible Networks
27 Agathovoulou St., Giannitsa, 58100, Greece
george.chlapoutakis@secbible.com

July 31, 2012

**Abstract**

Criminal profiling has seen a rise in both publicity and use in the last few years, having been extensively used in a number of real-world scenarios in the past to inform and aid the authorities in apprehending individuals who have committed one or more crimes.

However, the pervasiveness the Internet nowadays enjoys in individuals personal, social and professional lives has slowly changed the nature of crime to incorporate an increasing digital element. To this effect, there has been relatively much research interest in the transposition of classic criminal and offender profiling theories to Internet-oriented criminal acts.

In this paper, we define criminal profiling, discuss its modern inception and use in the US and follow its progress across the Atlantic to the UK and the rest of the world. We then introduce the application of criminal profiling on the Internet and, in particular, its application to digital crime and digital forensic investigations and policing.

Finally, we attempt to properly define the term digital forensic profile in the form of an explanation of some of the theories and models proposed to define it sociologically and mathematically.

## 1 Introduction

Eventually coined to the process of inferring the physical, mental and behavioural traits of individuals who have committed a crime through the

analysis of various aspects of the crime scene, the crime itself and the victims statement, criminal profiling has been a much discussed subject in most scientific and political circles alike.

Criminal profiles have been used, misused and abused since as early as the years of the purge of the Jews by the Roman Emperor Calligula. After a number of largely politically and religiously-motivated attempts at criminalising people of different nationalities and religions, criminal profiling has been alternatively abandoned and picked up again over the years (Turvey, 2008, pp. 3-70). Turvey further reports that the most serious effort to bring scientific rigour to criminal profiling was organised and implemented by the FBI, and was later adopted by law enforcement agencies in other parts of the world, as we will see below.

Even nowadays, both Ainsworth (2001, pp. 7-8) and Turvey (2008, p. 2) agree that the term has been, and still is, largely vague and ill-defined and that there are a multitude of differing viewpoints on what it should mean. Turvey, specifically, defines it as

> "Inferring the traits of individuals responsible for committing criminal acts" (Turvey, 2008, p. 2)

which requires the belief that the characteristics of an offender can be identified by careful study and use of all the information gathered from the scene of an offence, along with the statements of the victim (where possible) of the offence. However, Ainsworth has been very quick to point out (Ainsworth, 2001, p. 10) that the result of a criminal profile is not the exact identity of an offender but, in essence, a probabilistic tool that can be used to reduce the pool of suspects for a given offence. If taken as a whole, Ainsworth and Turvey's definitions, along with the definition given by Jackson and Bekerian (2006, p. 3) suggest that the value of a criminal profile is (and should be) the intelligence it gives to the investigator.

However, the overriding problem with any transposition of even the above definition, and its further clarifications, to the Internet is that the whole concept of what constitutes a crime and a crime scene has to change to accommodate the virtual and networked form of the Internet. Yar (2005*b*) and Wall (2010), for example, both acknowledge the need to re-think the definitions of what constitutes a crime, a crime-scene and a criminal given the nature of the Internet.

Thus, the contribution of this work is twofold. Firstly, our discussion will enable researchers to consider the progress of criminal profiling from its original intended field of application to the new era of the Internet, and will further stimulate academic interest in this field. Secondly, we hope that our

discussion and the theoretical model produced by the mapping of criminal profiling theory to digital crime will allow the evolution of a properly defined mathematical or statistical model that will allow researchers to properly profile a digital criminal act and its perpetrator.

# 2 Criminal Profiling Models and Practices in the US

As mentioned earlier, the most serious and by far most scientific use of criminal profiling came in the form of what was termed "criminal investigative analysis" by the FBI's Behavioral Analysis Unit (BAU). Its addition to criminal profiling was the injection of behavioral science in the above stated definition of criminal profiling (Turvey, 2008, p. 81) and, more specifically, the study of individual behaviour through the application of knowledge gained from studies of groups of similar offences and offenders. That led to the theory of the "organised/disorganised dichotomy" (Turvey, 2008, p. 83), which is the classification of offenders based on the sophistication, planning and competence exhibited by the offender through analysis of the crime scene. This theory, in turn, led to an offender classification system comprised of four stages, according to Jackson and Bekerian (2006, p. 5), which begin with data assimilation, crime classification and crime reconstruction, and result in the profile generation.

Concurrently with criminal investigative analysis and its profile generation process, the concept of geographic profiling was born out of Canter and Larkin's ideas regarding the application of environmental psychology to the crime scene, as an effort to make data assimilation and crime reconstruction, and thus profile generation, much easier. Canter and Larkin (1993) suggested the idea of separating the types of offenders into two distinct categories based on the distance between the offender's home base and the scene of the crime. Their "marauder" type of offender, thus, was defined as the offender who would commit offences close to his home base, while the "commuter" was defined as the offender who would commit offences further away from his home base.

This addition of environmental psychology and behavioral science to criminal profiling was the starting point used by Land and Felson and Cohen and Felson, in 1976 and 1979 respectively, and later Cantor and Cohen in 1980 during their research on creating a framework on social indicators and then using it to estimate emerging crime rates resulting from social change. Their further work on specific crimes such as larceny (Cohen and Cantor,

1980), property crime rates (Cohen et al., 1980) and homicide (Cantor and Cohen, 1980) allowed them to establish their joint theory on Routine Activity (RAT) defined as

> "any successfully completed violation [that] requires at a minimum an offender with both criminal inclinations and the ability to carry out those inclinations, a person or object providing a suitable target for the offender, and the absence of capable guardians capable of preventing the violation. The lack of any one of these elements is sufficient to prevent a potential direct-contact predatory violation from succeeding."(Felson and Cohen, 1980; Felson, 1987)

Further work by Felson (1995) increases the focus of the power of "guardians" to deter crime in the Routine Activity Theory and further updates it to distinguish between three different types of supervision, namely guardians, handlers and managers. Guardians are those individuals whose purpose is to monitor the targets, while handlers are responsible for monitoring the offenders. Managers, then, are responsible for monitoring the location. Each of those types of supervision, according to Felson is further distinguished by its level of responsibility to personal, assigned, diffuse and general.

Personal responsibility is the individual's (or their family/friends) responsibility to guard themselves or the target (depending on the target in question). Assigned responsibility is that which is assigned to a specific person or group by a higher authority within a locale (eg. security officers). Diffuse responsibility, on the other hand, is that which is more broadly assigned to a person or a group as part of their more general duties in the organisation or locale. Such individuals would, for instance, be employees of the finance department of a company who would be required to report any unauthorised expenditure as part of their duties. Finally, general responsibility is the one broadly assigned to the populace as a whole (eg. citizens).

Felson argues that the distinctions according to types of supervision and levels of importance allows a much more fine-grained (as opposed to arbitrarily set) control over what can be considered as the guardian variable of any model relying on the Routine Activity Theory. Still further work by Felson and Clarke and Felson between 1998 and 2000 brings into focus the factor of opportunity as a measure of the time window the offender has in which to commit a crime, all other factors being optimal for the offender. Finally, Felson also made an attempt to make use of the Routine Activity Theory to model the ecosystem of organised crime, as discussed in (Felson, 2006).

# 3 Criminal Profiling Models and Practices in the UK

As it was said in the previous sections, the FBI's criminal profiling model and process, since its inception and its relatively good rate of success in the field in the US, was adopted by other countries, where it was adapted to fit in with the crimes, investigative and the legal procedures of each country that adopted it.

With the introduction of the FBI's BAU process of criminal profiling in the UK, came the need to not only adapt the BAU model to fit with the existing legal and investigative system, but also attempt to expand on it based on research conducted by a number of research scientists of multiple disciplines in the country. As such, there have been a number of influences of other sciences aside from the environmental and social ones used in the US, where the focus was more on offender profiling through examination of individual offenders as opposed to groups (Jackson and Bekerian, 2006).

An initial effort to gather a coherent account of significant research conducted in the UK was the work of Jackson and Bekerian (2006) in their editorial capacity in the book "Offender Profiling: Theory, Research and Practice", where a number of contributing scientists used clinical psychology, as was the case with Badcock's research (Badcock, 2006) and Boon's research (Boon, 2006). Other research, however, focused on victim and witness descriptions and their validity, such as the research of Jackson et al (Jackson et al., 2006).

However, by far the best work on collecting, shifting through and presenting the UK's version of criminal profiling was performed by Ainsworth in his book on offender profiling and crime analysis (Ainsworth, 2001), where a much more clear and coherent account of the progress, performance and results of such methodologies as the introduction of clinical psychology and profile creation based on victim and witness descriptions was attempted.

As a final note, it has to be said that the contributions of the UK researchers allowed criminal profiling to gain a different point of view, referring to profiling the offender based on research conducted in individuals rather than groups and through the use of victimology and clinical psychology (Ainsworth, 2001). However, the prevalent and predominant model used by forensic profilers, and in point of fact acknowledged as the most scientifically-acceptable by the criminological and policing communities in general has been and still is the FBI's BAU model (Ainsworth, 2001; Turvey, 2008).

# 4 Criminal Profiling Models and Practices in the rest of the world

The introduction of the FBI's BAU process of criminal profiling, and its relatively high success rate allowed its application to other countries around the world with various degrees of success and failure.

One of the more successful applications and adaptations of the FBI's model was the attempt of the National Criminal Intelligence Division (NCID) of the National Police Agency in Holland. Ainsworth (2001, p. 135) identifies the crucial difference between the NCID and the BAU models as the openness of the former to scientific rigour and the scientific community in general, as opposed to the latter. Specifically, the NCID encouraged critical analysis and evaluation of their work and furthermore encouraged the publication of said evaluations to the scientific community. This move allowed the NCID to be guided and corrected in its use of and development of their model by the scientific community's peer-review process. The end result of their divergence was a model much more tailored to the needs of the country, as a whole, and much more rigorously examined than the original FBI model, which was often criticised for its relative lack of scientific rigour, according to Ainsworth.

The NCID model defined offender profiling as the result of the mixture of the knowledge derived from detective work and the knowledge derived from behavioural science work. Furthermore, the model itself is

> "...not an end in itself, but is purely an instrument for steering an investigation in a particular direction."(Jackson et al., 2006)

More recent research from a French perspective is that of Nadal et al. (2010) who developed a generalised framework for simulating the propensity to offend. Their work made use of software agents in order to create a simple criminal behaviour model to study the dynamics of the said propensity by incorporating a "honesty index" rating of each agent's interest in abiding by the law. Their work resulted in what they perceive as the existence of a self-organised state through which social dynamics determine and set the line between offenders and non-offenders in the society as a whole.

# 5 Developing a Criminal Profile

The FBI's BAU model is important in any attempt to create a computational model of a forensic or digital forensic profiling system. The reasoning behind this is the same reasoning which originally led to the definition of the BAU

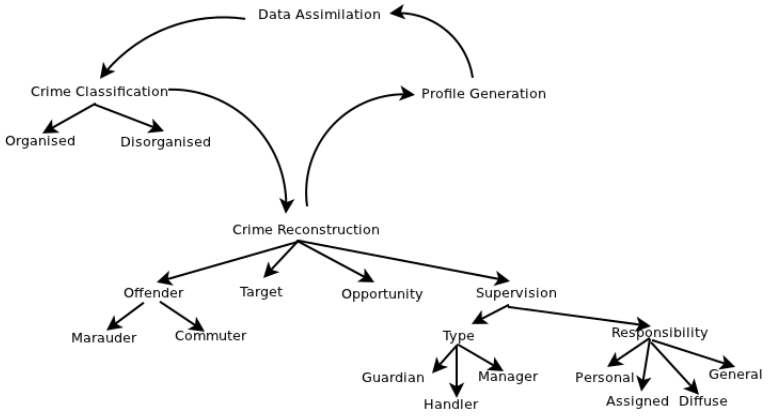


Figure 1: Criminal Profiling

model: the attempt to not only bring an order to the chaos of what would appear to be the different theories regarding digital profiling, but also the functional decomposition of such an attempt. In contrast, from a computer science standpoint, disciplines using studies of individual offenders as opposed to groups of offenders (eg clinical psychology, psychiatry) are largely more difficult to work with as their results are much less clear and more individualised. In short, such disciplines provide models which are not easy to transfer across disciplines.

If we take into account the four steps needed by the BAU to create a forensic profile (data assimilation, crime classification, crime reconstruction and profile generation) and assume that the organised versus disorganised dichotomy theory is part of the crime classification step, we have the basis of a model, which is derived from work that has been peer-reviewed and generic yet detailed enough to be able to be transformed into a computational model.

The model proposed by the Routine Activity Theory and the "marauder"/"commuter" classification are also extremely useful if applied to the BAU's crime classification and crime reconstruction stages, as they allow a greater level of knowledge gained from the said stages. Felson's later work on the RAT, which placed increased emphasis on the factors of guardians and opportunity, and resulted in a more detailed classification of the terms and their relationship with eachother further increases the knowledge gained from the crime classification and reconstruction stages.

If we attempt to map our understanding of all the above in a more coherent form taken from a computer science standpoint, we would end up with a system such as the one below:

In this model, we can clearly see the functional decomposition of the original BAU model with the addition of the offender/marauder and the

much-revised RAT model. In the current form, this model is both detailed enough to allow us to create more accurate profiles and generic enough to transfer from the forensic science sector to the computer science sector.

# 6 Digital Forensic Criminal Profiling Models and Practices in Cyberspace

In the previous section, we discussed a number of theories, models, processes and methodologies applied to offender profiling in the real world, where real-life crimes have real-life victims in real-life scenes of crime.

In his chapter on the novelty of cybercrime, Yar (2005*b*) poses that cyberspace (otherwise known as the Internet) has a number of differences to the real world. Primary amongst them is that it makes communication and interaction possible between widely-spaced individuals in almost real time, and the ability of the offender to attack targets is multiplied by the effects of the Internet. One such effect, Yar states, is the ability of attackers to assume virtual identities that are greatly separated from their normal identities.

According to Yar's research and further research on the phenomenon of music piracy (Yar, 2005*b*) and computer hacking (Yar, 2005*a*), the elements of spaciality and temporality deviate to a certain extent from those of the real world. This means that theories like the Routine Activity Theory need to be modified to address these issues. In his research, Yar argues that the importance RAT places on value, inertia and accessibility need to be modified to accommodate such issues as potentially larger values with much smaller inertia and more global accessibility with little guardianship.

Wall's research into the use of the Internet as a conduit for criminal activity (Wall, 2010) and on the issue of policing cybercrimes (Wall, 2007) further extend Yar's arguments. Specifically, he explains the impact of the Internet on crime and the transformations that were required to be taken into account when policing cybercrimes.

Wall argues that the main transformations that have taken place are the following six: globalisation, distributed networks, synopticism and panopticism, asymmetric relationships, data trails, and changes in the actual organisation of criminal activities to include the new communications medium. Globalisation (and "glocalisation" as Wall states) refers to the trans-national nature of the Internet, which brings information from international sources to one's locale, thus, essentially removing the spatial and distance-related factors a criminal has to take into account when committing a crime. Distributed networks refers to the view that the Internet is essentially a long, trans-national series

of interconnected networks, namely Metropolitan Area Networks (MAN), Wide Area Networks (WAN) and Local Area Networks (LAN) in this order, throughout the world. Wall argues that the distributed nature of the Internet, along with the different legal systems between across countries, and the lack of coordination between police forces and legal systems between countries further errodes the power of guardianship as a deterrent to the commision of a criminal act. Synopticism and panopticism refer to the ability of offenders to closely observe their target from afar in as much detail as they wish and they can achieve by exploiting the ever-increasing amount of information victims and potential victims reveal about themselves and the equally increasing ability of search engines to shift through and categorise that information. Asymmetric relationships between offenders, victims and justice processes, due to the distributed nature of the Internet, can allow offenders to target victims across nations with different justice processes. By data trails, Wall refers to the trails of traffic left on the Internet by both offender and victim which the justice process can take into account. Finally, changes in the actual organisation of criminal activities refers to the new-found ability of offenders to commit offences which they previously could not achieve (due to financial, geographical etc. reasons) and to even automate such offences over a wider area.

Both Wall and Marshall and Tompsett (2002) argue that crime on the Internet can be, much like in the RAT model, classified according to type and level of opportunity. According to type, then, we can have crimes against machines that are integrity-related, crimes against machines that are computer-related and crimes in the machine that are content-related. Integrity-related crimes are defined as those whose aim is to harm the computer system and its integrity. Computer-related crime refers to crimes against computers aimed at acquiring pieces of information for purposes such as theft or deception. Finally, content-related crimes in the machine are those depicting obscenities or violence. Also, according to level of opportunities they afford to the attacker, they can be traditional crime but using computers, hybrid cybercrime where traditional crime uses the new opportunities provided by the Internet, and true cybercrime, where we are dealing with new types of crime specifically using the opportunities afforded to the criminal by the Internet.

Some attempts at profiling cyber-criminals can be seen in Koops (2010), where the author attempts to classify cyber-criminals by using a number of popular self-descriptory terms used in the computer underground such as "white-hat", "black-hat" and "gray-hat" hackers, script kiddies etc.. However, a relatively similar attempt to profile cyber-criminals based on such simple notions as the age of the offender by Yar (2005*a*) resulted in inconclusive results as well.

Marshall and Moor further attempt to use the RAT in order to construct a model to profile criminals according to the scoring of computer and Internet-related crime, as part of their research into the criminalisation of the Internet. This resulted in an empirical mathematical scoring model (Marshall and Moor, 2006) which represents a first real attempt at creating a simplistic yet usable mathematical model to create a digital criminal profile. Their scoring model was developed as an extension to the earlier argument on the need for automation of the collation and analysis phase of a digital forensic investigation. This extension now includes ways to create profiles of the perpetrators and victims of an attack as well as of the attack itself. This model takes the form of

$$L = \frac{C_e * C_f * A}{V_e * (C_g)^x * V_g}$$

where $C_e$ describes the criminal expertise, $C_g$, with an additional modifier $x$ which Marshal and Moor use to explain the importance of the guardianship on the attacker, and $V_g$ the constraints of the environment and the presence or absence of a guardian for those environments. $A$ denotes the nature and elements contributing to a successful attack, $V_e$ the victim's expertise and $C_f$ the criminal's freedom to operate on the network from their home. All the above factors combine to give us the likelihood of an attack $L$.

# 7 Developing a Digital Criminal Profile

Wall's research, if combined with the later research by Marshall and Moore are very important because they seek to essentially transfer the BAU model, the organised/disorganised dichotomy, the marauder/commuter theory and the Routine Activity Theory across disciplines, namely from the forensic science one to the digital forensics one. For the purpose of this chapter, we assume that digital forensic science is the application of forensic science tools, models and methodologies to Internet-related crimes.

As we have seen, both research teams decided to classify digital crimes based on their type and the level of opportunity the criminals have to commit the crimes, in a way similar to the ones we have seen earlier. Both approaches take into account the offender, the target and the opportunity, however, only Marshall and Moore take into account the additional issue of the target's supervision. However, Yar's research reveals that we also have to address the issues of value, inertia and accessibility if we are going to apply such theories as RAT in cyberspace. This means that Marshall and Moore's model will need to be expanded as, while it deals with the issues of value

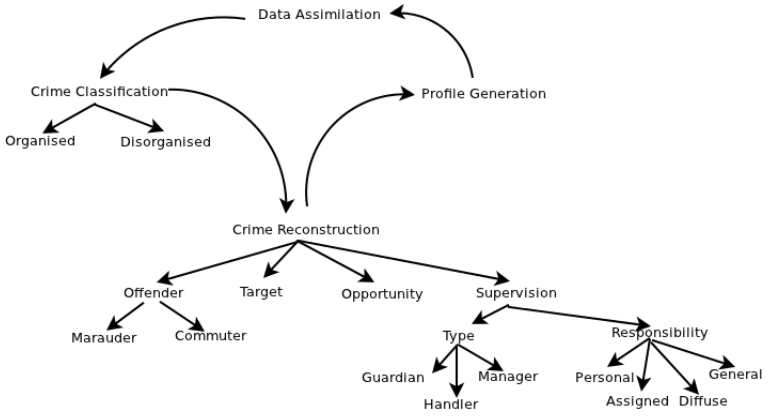


Figure 2: Criminal Profiling

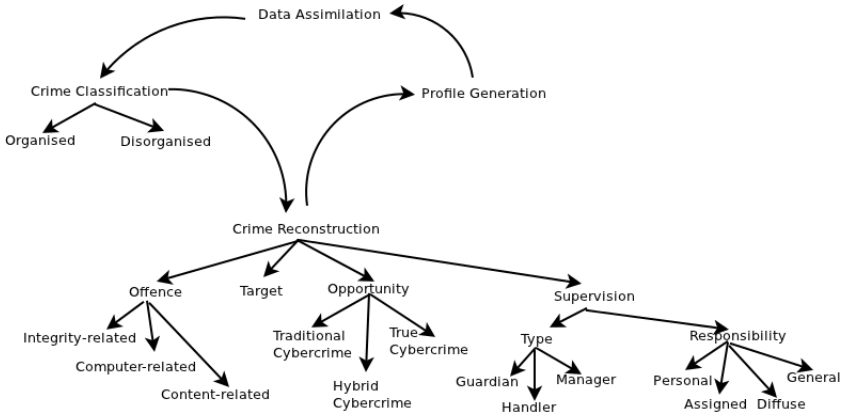


Figure 3: Digital Profiling

and inertia, it fails to address the issue of accessibility. While their model works around Yar's assertion that there is little to no guardianship on the Internet by including the variable $x$ as a way of defining guardianship as software/hardware solutions aimed at protecting the target's computer, it does not scale well when applied to the scenario of a computer network. Specifically, when applied to a networked environment the $x$ modifier would need to be set either at 0 or at 1 (on a scale of 0 to 5) thus making the impact of the modifier minimal to non-existent. So, Marshall and Moore's model will need to be extended in a similar way to that used by Felson (1995) to take into account the networked nature of the Internet.

Based on the above assertions, if we combine the previously discussed forensic profile model with the current models of digital forensic profiling we have been discussing, we end up with the following computational model:

In the previous page we compare the initial computational model for an

offender profile (Fig. 2) with the computational model we derived from our discussion of digital forensic offender profiling (Fig. 3). The computational model shown on the right is very much the same as the end result of the previous section. The main differences (shown in bold) are the deviation from the marauder/commuter offender theory to a more Internet-related one, where we concentrate on the offence rather than the offender, and the change in the types of opportunity the offender has to reflect the Internet-related nature of the model. This allows us to better explain the Marshall and Moore model discussed above in the context of what we know and what we can derive from our study of criminal and digital forensic criminal profiling.

More specifically, $C_e$, which is the criminal expertise, can be derived from the model through a series of algebraic transformations which can derive the equations needed to calculate the values of the remaining variables, with the sole exception of the $x$ modifier. The modifier $x$ will need to be modelled to account for the type and responsibility of the supervision, which is (as Felson states) very much dependent on the social structure of the organisation and country (in other words, the locale) as opposed to a randomly assigned number. Furthermore, opportunity needs to be inserted into the equation in order for the mathematical model to fit our conceptual model.

Marshall and Moore's research suggests that "opportunity" can be factored in to their model if it is assumed to be a composite of failings in the victim, environment (i.e. $C_f$ being the criminal's freedom to operate) and guardian and success in the attacker. However, their research does not take into account the findings of both Yar and Wall, discussed above, with regards to the nature of the Internet and how they affect the concepts of victim, environment and guardian if we combine them with the element of time. Opportunity, Felson suggests, and we thus pose, is by definition also a measure of time, and more specifically is the time window the offender has in their disposal in order to commit the crime, given the medium of the Internet.

In its present form, Marshall and Moore's model is valid if both the criminal and the victim are located in the same country, within the same time-zone and/or comply to the same social structure of the organisation or the country. In such a case, both the criminal and the victim, for example, may follow a 9am to 5pm work schedule or any other set of clearly defined 8-hour shifts (morning, afternoon or night shift). The time-window for the commission of a criminal activity, from the criminal's point of view, then, becomes a matter of identifying the time-window where the victim, environment and guardian are all in a weak state.

If we, however, change our assumption regarding the location of the criminal, victim and guardian to Yar and Wall's observations regarding the global state of the Internet, we can see that the criminal may not necessarily be aware

of the victim's patterns and may not be able to observe the victim's patterns closely enough to clearly calculate the time-window previously mentioned. The same applies to the victim's understanding of the criminal's patterns.

The above will invariably result in the criminal automating the task of committing an offence, given his lack of understanding of (or his failure to take into account) the victim's location and patterns.

One possible vector we can follow to deal with the issues of location and patterns is through the use of methodologies taken from the fields of Intrusion Detection and Computational Statistics, which routinely deal with the issues of location and patterns in data. More importantly, however, both fields see Internet-related activities as time series data, where observations are gathered at regular time intervals and then modelled and analysed. Time series analysis, thus, takes into account both the location and the patterns of both the criminal and the victim. Proper analysis of time series data from Internet traffic and activities can allow the investigator to more easily understand such issues as the victim's or criminal's location and working patterns which can give us the opportunity, as Felson suggests.

An example taken from the field of Network Security is the findings of Kannadiga et al. (2007) and Svendsen and Wolthusen (2009), whose implementations of the E-NIPS IDS and certain SCADA systems, respectively, make use of statistical models as an aide in dealing with intrusions. Specifically, they use statistical modelling techniques in conjunction with intrusion detection modelling techniques to identify not only normal attacks but also those that follow certain patterns related to time series elements such as trend and seasonal effects.

# 8 Conclusions and Further Work

As a tool in the arsenal of criminal investigators, criminal profiling has generally had a chequered history and a relatively vague definition. As it can be seen in this paper, only relatively recently has the analysis of crime scenes, the crime itself and the victims statement started making a widespread impact in both actual criminal investigations and in the public's perception of criminal investigations.

This paper examines criminal profiling from the point of view of a computer scientist, as opposed to a social or forensic scientist. It attempts to more clearly define the term "criminal profiling" and detail and discuss its past and present development and use in the US, the UK and the rest of the world.

Furthermore, an attempt is made to collect and collate all the prevalent theories on criminal profiling in order to create a clearer picture of what the

outcome of the criminal profiling process would look like, in the form of a concise theoretical model, from the point of view of a computer scientist in the process of defining, designing and implementing a digital forensic profile as a computer system. This model, and the thought process that went into its development, was then transferred from its real world setting to the Internet, which shares some attributes of the real world but is substantially different in most other attributes. This transfer required a relatively substantial change in both the actual model as well as the thought process whose outcome the model was, in order to accommodate the rather different aspects of the Internet's form, structure, attributes and capabilities it gives to the criminal, the victim and the investigator alike.

In addition, this paper also attempts to detail and discuss the relatively small number of theoretical and practical digital forensic profiling models built through the adoption and modification of a number of real-world criminal profiling models and techniques. The in-depth discussion that results shows not only the strengths and weaknesses of the current digital forensic profiling models, but also some possible new vectors for researchers to follow when developing such models, through the addition of a number of fields of science, such as intrusion detection, computational statistics and Bayesian inference and forecasting.

Those fields of science and the new vectors they offer to researchers through joint inter-disciplinary ventures, we pose, can easily be used to inform the creation of digital forensic profiles of network attackers as well as offer useful insight and intelligence into other Internet crimes.

# References

Ainsworth, P. (2001), *Offender Profiling and Crime Analysis*, Willan Publishing, Culmcott House, Mill Street, Uffculme, Cullompton, Devon, England.

Badcock, R. (2006), Developmental and clinical issues in relation to offending in the individual, *in* J. Jackson and D. Bekerian, eds, 'Offender Profiling: Theory, Research and Practice', John Willey and Sons Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, England, pp. 9–42.

Boon, J. (2006), The contribution of personality theories to psychological profiling, *in* J. Jackson and D. Bekerian, eds, 'Offender Profiling: Theory, Research and Practice', John Willey and Sons Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, England, pp. 43–60.

Canter, D. and Larkin, P. (1993), 'The environmental range of serial rapists', *Journal of Environmental Psychology* **13**, 93–99.

Cantor, D. and Cohen, L. E. (1980), 'Comparing measures of homicide trends: Methodological and substantive differences in the vital statistics and uniform crime report time series (1933–1975)', *Social Science Research* **9**(2), 121 – 145. http://www.sciencedirect.com/science/article/pii/0049089X80900022, Last seen: 17/02/2012.

Cohen, L. E. and Cantor, D. (1980), 'The determinants of larceny: an empirical and theoretical study', *Journal of Research in Crime and Delinquency* **17**(2), 140–159. http://jrc.sagepub.com/content/17/2/140.abstract, Last seen: 17/02/2012.

Cohen, L. E. and Felson, M. (1979), 'Social change and crime rate trends: A routine activity approach', *American Sociological Review* **44**(4), pp. 588–608. http://www.jstor.org/stable/2094589, Last seen: 17/02/2012.

Cohen, L. E., Felson, M. and Land, K. C. (1980), 'Property crime rates in the united states: A macrodynamic analysis, 1947-1977; with ex ante forecasts for the mid-1980s', *American Journal of Sociology* **86**(1), pp. 90–118. http://www.jstor.org/stable/2778853, Last seen: 17/02/2012.

Felson, M. (1987), 'Routine activities and crime prevention in the developing metropolis', *Criminology* **25**(4), 911–932. http://onlinelibrary.wiley.com/doi/10.1111/j.1745-9125.1987.tb00825.x/abstract, Last seen: 17/02/2012.

Felson, M. (1995), 'Those who discourage crime', *Crime and Place: Crime Prevention Studies* pp. 53–66.

Felson, M. (2000), *The Routine Activity Approach as a General Crime Theory*, Of Crime and Criminality: The Use of Theory in Everyday Life, Pine Forge Place, chapter 11, pp. 205–217.

Felson, M. (2006), 'The ecosystem for organized crime', *European Institute for Crime Prevention and Control, Helsinki, Finland* **26**.

Felson, M. and Clarke, R. (1998), 'Opportunity makes the thief: Practical theory for crime prevention', *Police Research Series Paper 98* .

Felson, M. and Cohen, L. (1980), 'Human ecology and crime: A routine activity approach', *Human Ecology* **8**, 389–406. http://www.springerlink.com/content/l2l93u1346g53g30/, Last seen: 17/02/2012.

Jackson, J. and Bekerian, D. (2006), Does offender profiling have a role to play?, *in* J. Jackson and D. Bekerian, eds, 'Offender Profiling: Theory, Research and Practice', John Willey and Sons Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, England.

Jackson, J., Eshof, P. V. D. and Kleuver, E. D. (2006), A research approach to offender profiling, *in* J. Jackson and D. Bekerian, eds, 'Offender Profiling: Theory, Research and Practice', John Willey and Sons Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, England, pp. 107–133.

Kannadiga, P., Zulkernine, M. and Haque, A. (2007), E-nips: An event-based network intrusion prediction system, *in* J. Garay, A. Lenstra, M. Mambo and R. Peralta, eds, 'Information Security', Vol. 4779 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, pp. 37–52.

Koops, B.-J. (2010), 'The internet and its opportunities for cybercrime', *SSRN eLibrary* . `http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1738223`, Last seen: 17/02/2012.

Land, K. C. and Felson, M. (1976), 'A general framework for building dynamic macro social indicator models: Including an analysis of changes in crime rates and police expenditures', *American Journal of Sociology* **82**(3), pp. 565–604. `http://www.jstor.org/stable/2777340`, Last seen: 17/02/2012.

Marshall, A. and Moor, G. (2006), 'Criminalisation of the internet: an examination of illegal activity online.', *The 4th European Academy of Forensic Science Conference - EAFS2006* .

Marshall, A. and Tompsett, B. (2002), 'Spam 'n' chips: A discussion of internet crime', *Science & Justice* **42**(2), 117–122.

Nadal, J., Gordon, M., Iglesias, J. and Semeshenko, V. (2010), 'Modelling the individual and collective dynamics of the propensity to offend', *European Journal of Applied Mathematics* **21**(Special Double Issue 4-5), 421–440. `http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=7853397`, Last seen: 17/02/2012.

Svendsen, N. and Wolthusen, S. (2009), Modeling and detecting anomalies in scada systems, *in* M. Papa and S. Shenoi, eds, 'Critical Infrastructure Protection II', Vol. 290 of *IFIP International Federation for Information Processing*, Springer Boston, pp. 101–113.

Turvey, B. (2008), *Criminal Profiling: An Introduction to Behavioral Evidence Analysis (3rd Edition)*, 3rd edn, Academic Press, London, UK.

Wall, D. S. (2007), 'Policing cybercrimes: Situating the public police in networks of security within cyberspace (revised feb 2011)', *Police Practice and Research: An International Journal, Vol. 8, No. 2, pp. 183-205, May 2007* .

Wall, D. S. (2010), 'The internet as a conduit for criminal activity', *Information Technology and The Criminal Justice System, Pattavina, A., ed., pp. 77-98, Sage Publications, Inc., 2005* .

Yar, M. (2005*a*), 'Computer hacking: Just another case of juvenile delinquency?', *The Howard Journal of Criminal Justice* **44**(4), 387–399. `http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2311.2005.00383.x/abstract`, Last seen: 17/02/2012.

Yar, M. (2005*b*), 'The novelty of 'cybercrime", *European Journal of Criminology* **2**(4), 407–427. `http://euc.sagepub.com/content/2/4/407.abstract`, Last seen: 17/02/2012.