View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Portsmouth University Research Portal (Pure)

On the complexity of collaborative cyber crime investigations

By

Peter M. Bednar, Vasilios Katos and Cheryl Hennell

This article considers the challenges faced by digital evidence specialists when collaborating with other specialists and agencies in other jurisdictions when investigating cyber crime. The opportunities, operational environment and modus operandi of a cyber criminal are considered, with a view to developing the skills and procedural support that investigators might usefully consider in order to respond more effectively to the investigation of cyber crimes across State boundaries. Carrying out blackmail by using a computer, for example, is a particularly popular category of computer crime which involves the coordination of law enforcement and investigatory groups on an international level. A representative case was that involving three Russian individuals who extorted up to 4 million US dollars from United Kingdom based on-line casinos and bookmakers.[1] The criminals were taken into custody in September 2004 following the successful joint efforts of the National High Tech Crime Unit in the UK, Interpol, the FBI, Russia's Interior Ministry and the Prosecutor General's office. The authors propose in this article that the Electronic Discovery Reference Model (EDRM), which is a useful framework for systemic thinking, can used to support the need for collaboration during the investigation process.

Introduction [Heading type A]

Historically, an investigation was in principle a self contained, self-controlled, self-centered, solitary activity. Typically, communications of findings were limited to internal (local) members from the same team, each member familiar with the terminology and vocabulary. Lack of scientific procedures in criminal investigations in the early years

[1] John Layden, 'Russian bookmaker hackers jailed for eight years', *The Register*, 4 October 2006, available at http://www.theregister.co.uk/2006/10/04/russian_bookmaker_hackers_jailed/.

dictated such an approach.[2] However, advances in science such as fingerprinting, blood analysis and trace evidence resulted in increasing numbers of specialists becoming involved in crime scene investigations, in turn increasing the complexity and size of the communication channels. The advances in, pervasiveness and ubiquitous nature of, information technologies[3] and in turn the global nature of cybercrimes, have increased the need for investigators to engage in complex inter-group communication on a multinational basis as they investigate criminal acts using interconnected technologies.

Furthermore, the different judicial systems throughout the world create a challenging environment for the investigators of cybercrimes. Whilst criminals use information technologies as they see fit across national boundaries, it is no longer possible for investigators to operate individually. It is now necessary to collaborate across State boundaries, which makes the cybercrime scene a greater challenge for any investigator and a more pertinent area for research than before.[4]

The main aim of this article is to highlight some of the issues involved in investigating cybercrimes across State boundaries and the need to collaborate on the particular problem of determining the scope of inquiry, and what can or cannot be investigated in connection with the crime scene. Within this context, it is relevant to explore the following issues:

a. How to incorporate important elements in the investigatory practice to deal with the complexity of investigations across jurisdictions.

[2] Claire Valier, 'True Crime Stories: Scientific Methods of Criminal Investigation, Criminology and Historiography', *British Journal of Criminology*, Volume 38, Number 1, (1998), pp 88-105.

[3] Sarandis Mitropoulos, Dimitrios Patsos and Christos Douligeris, 'Incident Response Requirements for Distributed Security Information Management Systems', *Information Management & Computer Security*, (2007), Volume 15, Issue 3, pp 226-240.

[4] Roderic Broadhurst, 'Developments in the Global Law Enforcement of Cyber-Crime', *Policing: An International Journal of Police Strategies & Management*, (2006), Volume 29, Issue 3, pp 408-433.

b. How to decide where relevant data or evidence in relation to an investigation is located and how it is recovered.

c. Establishing who is or ought to be involved in determining the scope of the investigation.

d. How investigators collaborate with each other and other relevant agencies to provide for a common understanding of the problems, and the use of a language that is clear to all parties.

e. The logistics and complexity of negotiating the collection of digital data when investigating a cybercrime.

The main concern is not on the management of data or information, but on how digital data is judged to be of relevance, and how this is communicated to other jurisdictions when investigating a cybercrime.

Identifying the need for collaborative enquiry and communication [Heading type A]

As with many traditional crime scene investigations, a cybercrime investigation may need to investigate hardware, software or storage (whether physical devices or virtual areas) that contain private data. Whether an investigator has the authority to investigate private data will depend on the nature of the crime and the substantive and procedural laws of the jurisdiction in which the investigation takes place.

It has been recognized that existing procedures and practices in forensic investigations are in need of further development when investigating on-line fraud and cybercrime in general.[5] The take-up of digital technology has changed the landscape of the crime scene, increasing the need for cross-jurisdiction investigation and collaboration, and the use of sound forensic practices and procedures. It may be that the procedures and techniques used in a digital crime investigation are so flawed that that will be excluded from legal proceedings.

[5] Judie Mulholland, Message from the Guest Editor, Special Issue: Phishing and Online Fraud Part II, *Journal of Digital Forensic Practice*, Volume 1, Issue 3, 2006, pp 151-2.

There has been considerable discussion regarding the definition of the crime scene and, more recently, the cybercrime scene - see for example the distinction between 'live versus dead systems'[6] from which the problem of defining the actual cyber crime scene boundaries becomes evident. The blurring of distinctive boundaries containing the cybercrime scene occurs due to the ubiquitous nature of digital media, the investigator's experience and skills needed to manipulate the data, together with the context and type of the respective crime. Changes in society, technology and behaviour have influenced the environment and opportunity for crime and therefore the extent of the crime scene. Furthermore, these changes also serve to extend the skills that the investigation of cybercrime requires. Despite the significant progress in teamwork between different agencies, existing research does not address the complexity of the problem.[7] A central challenge in the support for and coordination of forensic investigators is to enable them to work together, as a team, for a common purpose.

Cybercrime scene investigation [Heading]

Cyber crimes are not new, as illustrated in:[8]

> 'cyber-crimes are not necessarily new crimes; many cases involve rather classic types of crimes where criminals exploit computing power and accessibility to information. However, it seems that the anonymity provided through the Internet encourages crimes that involve the use of computer systems, since criminals

[6]Eoghan Casey, editor, *Handbook of Computer Crime Investigation*, (Academic Press, 2002), p 2.

[7] David V. Pynadath and Milind Tambe, 'The Communicative Multiagent Team Decision Problem: Analyzing Teamwork Theories and Models', *Journal of Artificial Intelligence Research*, Volume 16, (2002), pp 389-423.

[8] Maria Karyda and Lilian Mitrou, 'Internet Forensics: Legal and Technical Issues', in *Proceedings of Second International Annual Workshop on Digital Forensics and Incident Analysis*, Bart Preneel, Stefanos Gritzalis, Spyros Kokolakis, and Theodore Tryfonas (ed), IEEE Computer Society, 2007, p 4.

> believe that there is a small chance of being prosecuted, let alone being caught for their actions.'

This is further supported by researchers from a variety of disciplines, as well as lawyers. Professor Noel Cox suggests that cybercrime is by nature a cross border crime,[9] and Professor Marjie T. Britz comments that 'for the first time, criminals can cross international boundaries without the use of passports or official documentation'.[10] Cyber crime has long been recognized as being transnational by nature, and attempts have been made to provide for an international framework.[11] It follows that there is a need for operational co-ordination and collaboration across state boundaries by investigating authorities.

While an experienced forensic investigator would recognize best practices in dealing with a crime scene in the physical world, setting boundaries and selecting what is relevant in such an abstract and intangible cyber environment is in its infancy.[12] This is not only a technical problem, but also a significant socio-cultural and collaborative problem that

[9] Noel Cox, 'Cyber-crime Jurisdiction in New Zealand', in Bert-Jaap Koops, Susan Brenner and Paul de Hert (eds), *Cybercrime Jurisdiction: A Global Survey*, (T.M.C. Asser Press, 2006), pp 177-188.

[10] Marjie T. Britz, *Computer Forensics and Cyber Crime*, (New Jersey, Prentice Hall, 2004), p 5.

[11] For three examples of many, see the United Nations Manual on the Prevention and Control of Computer-Related Crime, (UN, New York, 1994); OECD, Recommendation of the Council concerning Guidelines for the Security of Information Systems, OECD/GD(92) 10, Paris, 1992, and in the European Union, Council of Europe, Computer Related Crime, Recommendation No. R(89)9 on Computer Related Crime and Final Report of the European Committee on Crime Problems, Strasbourg, 1990.

[12] Alastair Irons and Anastasia Konstadopoulou, 'Professionalism in digital forensics', *Digital Evidence and Electronic Signature Law Review*, 4 (2007) 45 – 50 and Stephen Mason, *Electronic Evidence: Disclosure, Discovery & Admissibility*, (LexisNexis Butterworths, 2007), Chapter 3.

becomes even more complex due to its trans-national nature.[13] Digital forensics is concerned with the investigation, analysis, preservation and presentation of digital evidence as part of the judicial process.[14] However, because of the complexity of technical architectures and the approach to information systems security to promote business continuity, and recovery to mitigate the effects of unauthorized intrusion, the investigation process becomes even more complex.[15] The opportunities for criminals to use digital means for their modus operandi are legion, and the criminal imagination is offered considerable possibilities when taking into account the combination of availability, simplicity of use, mobility, high performance, affordable technology, and the lack of user awareness to protect their systems.

The characteristics of crime scene investigations have evolved over the last few decades such that the skills and attributes also need to be reconsidered. It is suggested that those involved in digital forensic investigations will need to have a holistic view and knowledge of their domain from five perspectives: technical (what is possible); professional (what is permissible); practice (what is appropriate); ethical (what is morally right) and legal. Technical expertise is concerned with understanding digital information and communication technologies. More precisely, the range of knowledge should, for example, include any or all of the following aspects: data storage, data representation, data communication, computer processes, operating systems, access controls, security, the internet, protocols, client and server programming. The plethora of technologies means there is a need for suitable expertise which cannot be expected to be found in a

[13] Judie Mulholland, Message from the Guest Editor, Special Issue: Phishing and Online Fraud Part II, *Journal of Digital Forensic Practice*, Volume 1, Issue 3, 2006, pp 151-2.

[14] Warren G. Kruse II and Jay G. Heiser, *Computer Forensics: Incident Response Essentials*, (Addison Wesley, 2001) and Eoghan Casey, *Digital Evidence and Computer Crime*, (Academic Press, 2004).

[15] Karen Scarfone and Peter Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), (Special Publication SP800-94, National Institute of Standards and Technology, February 2007), available on-line at http://csrc.nist.gov/publications/PubsSPs.html.

single investigator. This is reflected, for example, in the ACPO guidelines[16] and more specifically with the second Principle, which provides that obtaining access to the original data should only be performed by a person competent in the specific underlying domain. In summary these guidelines encompass the following: ethics and its relation to the law and computing, legal processes, digital evidence and includes a regulatory framework for digital investigation. Although there are series of guidelines[17] and Standard Operating Procedures[18] that are widely available, these are not sufficient if they are performed by a person that is not competent in the respective subject.

In practice, technical and professional strands can merge, depending on the nature of the investigation, and may be conducted in an individual suspect's home, a corporate site and across international boundaries. Additionally where it is thought that incidents occurred in a commercial environment, forensics investigators will need to take into account business considerations such as business continuity plans, disaster recovery plans and information security plans. This is because such considerations might provide the technical evidence to support the investigation, and avoid creating a disaster through the intervention of the investigation. Successful investigations are possible where appropriate collaborative communication has been adopted in conjunction with some or all of the following: the use of appropriate tools for the investigation, compatible working practices when handling evidence, and a forensic approach to the detection, preservation, analysis and presentation of evidence. What is appropriate in any one situation does not only

[16] *Good Practice Guide for Computer based Electronic Evidence* (v4, 2007); see also Stephen Mason, general editor, *Electronic Evidence: Disclosure, Discovery & Admissibility*, (LexisNexis Butterworths, 2007), Appendix I for a longer international list of guidance.

[17] For example see the NIST Special Publication Series, 'Guidelines on Cell Phone Forensics', 2007, 'Guidelines on PDA Forensics', 2004 and 'Guide to Integrating Forensic Techniques into Incident Response', 2006.

[18] George Mohay, Alison Anderson, Byron Collie, Olivier de Vel and Rodney D. McKemmish, *Computer and Intrusion Forensics*, (Artech House, 2003), Chapter 3.

depend on the particular problem and technology, but also on socio-cultural contexts and the legal framework. These issues are clearly also dependent on complex national and international contexts, including the way legislation is interpreted, applied and acted upon, which differs between States. Historically, specifically formed groups and organizations of experts and, occasionally, a task force would often target international organized crime, terrorist activities and other high profile crimes. This may have been successful where there were relatively small numbers of people that could be targeted with the use of exceptional resources. The problem with cybercrime is that it is something that is not limited to a (relatively small number) of organized gangs or international criminals or terrorist groups. The point is that because of the success of ICT related technology, more or less any existing crime can in one way or other ‘become’ transformed or extended into a cybercrime. In addition, new activities occur that are difficult to classify or are not catered for in existing legal frameworks.

It is possible to suggest that cybercrime is now the ‘everyday’ crime of the new era. It is no longer the preserve of specialist groups of experts who should be responsible for investigating cybercrime, but local investigators in collaboration with local investigators in a different country. This leads to the conclusion that forensic investigators face a significantly more complex task when investigating cybercrime and crimes involving digital technology, in comparison with a traditional crime scene. Thus the need for collaboration and communication between different specialist individuals and teams on a national and international level is often unavoidable. Additional challenges arise because a cybercrime scene tends to transcend national boundaries and legal jurisdictions. With this in mind, an overview of a possible framework to facilitate a complex inquiry with the intent to encourage collaborative working amongst members of investigatory teams and between investigatory teams is discussed below.

A case for strategic systemic thinking [Heading]

Mulholland suggests that ‘…there are no quick fixes. To solve the problem of online fraud or at least bring it down to a manageable level requires a multi-facetted approach by all the stakeholders involved'.[19] The framework for Strategic Systemic Thinking (SST) described in this section, supports the involvement of all those participating in an investigation. The SST framework was developed to help organizations to formulate appropriate processes to investigate effectively, and to provide support for an inquiry. It was developed specifically to help teams of users to analyze complex problems. It is for this reason that the SST framework is, arguably, suitable for use with cyber crime scene investigations. Earlier work by two of the authors with the cyber crimes in mind shows some promise.[20]

The SST framework involves three aspects, which are not sequential and may be applied in any order. It is intended to be repeatable, and it is possible to move from one analysis to another repeatedly and in any direction, at any time. A theory of the case can be established, which can be adapted as more information is obtained, analyzed and assessed.

The strategy adopted by an investigator will be dependent upon the organizational culture, which influences the amount of autonomy an investigator is permitted. It is an essential characteristic of the SST framework that the investigators control the investigation. A team of investigators may comprise of specialists, and one or more external facilitators (experienced in systemic methods for inquiry) who provide support and guidance. The framework supports the investigation of complex problems. With the support of the framework, each investigator can explore their perspective on the theory of the case. The outside individuals are present to act as the central coordinator to discuss the various individual theories. The aim is to bring thoughts about the case together to enable the investigation to proceed, having taken into account different opinions. Investigators can use a range of methods, which are well known in the disciplines of Information Systems (IS) and organizational studies, for instance. In order to deal with

[19] Judie Mulholland, Message from the Guest Editor, Special Issue: Phishing and Online Fraud Part II, Journal of Digital Forensic Practice, Volume 1, Issue 3, 2006, pp 151-2.

[20] Vasilios Katos and Peter M. Bednar, 'A cyber-crime Investigation Framework', *Computer Standards & Interfaces*, Volume 30, Issue 4, (May 2008), pp 223-228.

complex and uncertain problems, systems analysts have used methods and techniques such as Brainstorming, Mind-Maps and Effective Rich Pictures. These techniques have been successfully used as part of IS methodologies such as Soft Systems Methodology, SSM,[21] Effective Technical and Human Implementation of Computer Supported Systems, ETHICS[22] and Client-Led Design.[23] These methods have been used for years to assist people in making sense of complex problems. The various techniques and tools have different approaches to analysis. McFazdean has defined brainstorming as follows:[24]

> 'Brainstorming relies on the absence of evaluations in the ideas phase. Moreover, free-wheeling is encouraged so that an extensive list of ideas can be generated. The group members must be allowed to communicate an idea, however mundane, strange or wild, to the rest of the group. An idea that may seem impractical may contain a germ of a great solution.'

A brainstorming session will produce an unstructured collection of (lists of) ideas and concepts relating to a problem.

Mind Mapping has a long history (it is thought that Porphyry of Tyros from the third century CE used a form of mind-mapping). More recently, however the semantic network theory of human understanding (associated with Allan M. Collins and M. Ross Quillan)[25] included a development of Mind Mapping as an explicit technique. Mind Mapping has

[21] Peter Checkland and Sue Holwell, *Information, Systems and Information Systems: making sense of the field* (Wiley, 1998).

[22] Enid Mumford with Steve Hickey and Holly Matthies, *Designing Human Systems*, (lulu.com, 2006).

[23] Frank Stowell, and D. West, *Client-led Design: a systemic approach to information systems definition* (McGraw-Hill, 1994).

[24] E. McFazdean, 'Enhancing creative thinking within organisations', *Management Decision*, Volume 36, Issue 5, (1998), p 312.

[25] Allan M. Collins and M. Ross Quillan, 'Retrieval Time from Semantic Memory', *Journal of Verbal Learning and Verbal Behavior*, (1969), Volume 8, 240-247.

been described as ‘a powerful technique which provides a universal key to unlocking the potential of the brain’.[26] Mind maps are recognizable by their depiction of relationships between ideas and concepts, often radiating from a central concept and gathering details and associations along ‘branches’. Analysts are able to identify and describe relationships and associations in the form of a Mind Map. Rich Pictures is a technique that is favoured by many systems analysts, especially those using SSM.[27] One of the benefits of this technique is to enable the user to take a more holistic view of a problem. Another benefit is that it promotes the elaboration and exploration of meanings between relations and associations of a complex problem.[28] Rich Pictures can be described as ‘pictorial, cartoon-like representations of the problem situation that highlight the significant and contentious aspects in a manner most likely to lead to original thinking…’[29] These techniques aim to bring about a constructive dialogue between the investigators and teams involved in the investigation.

Aspects of the SST framework [Heading]

Intra-analysis is a phrase used to describe the ability of investigators to have their own perspective on the theory of the case. Inter-analysis is the part of the inquiry where alternatives are discussed collectively. The third aspect of the framework comprises the evaluation. The evaluation represents an examination of what is assumed to be known, that is, the results of analysis.

[26] Tony Buzan, and Barry Buzan, *The Mind Map Book*, (BBC, 2003), p 55.

[27] Andrew Monk and Steve Howard, ‘Methods & tools: the rich picture: a tool for reasoning about work context’, *Interactions*, Volume 5, Issue 2, (March/April 1998), pp 21-30.

[28] Peter Bednar, and Lynn Day, ‘Systemic combinatory use of Brainstorming, Mind-Maps and Rich Pictures for analysis of complex problem spaces’, Proceedings of ECRM 2009 Malta, 22-23 June: http://www.academic-conferences.org/ecrm/ecrm2009/ecrm09-home.htm.

[29] Michael C. Jackson, *Systems Thinking: Creative Holism for Managers*, (John Wiley and Sons, 2003), pp 186-187.

One significant aspect of the SST framework is its capability to incorporate a number of different conclusions, which is particularly useful, because digital forensics requires the investigator to consider that there may be more than one conclusion to any given set of facts. Forensic investigations are required to incorporate the ability to deal with issues such as fuzziness of inclusion, for example. That is, being able to identify which digital data would be part of the digital evidence, proving or refuting a user's actions or intentions. In dealing with complex cyber crime investigations, it is conceivable that the investigators will explore uncertainty in the following way:

a. unstructured uncertainty: the assumption of not having enough information to commit to a decision;

b. structured uncertainty: the assumption of too much information, conflicting information, ambiguities, paradox (can be true and false at the same time).

Not only can an investigator never know for sure whether what she or he investigates is the right thing to investigate, but also the scope of investigation is uncertain. This, among other reasons, is one reason why it is not appropriate to use bi-valued logic, and in practice it is not applied in investigations. While this might appear to be obvious from an abstract generic point of view, the problem becomes significant when logically rational work processes and supporting IT solutions are developed. The more complex and uncertain any one problem becomes, the more people tend to apply ('scientific') reductionist techniques and models focusing on the rigour of analysis. This behavioural pattern leads people to *unwittingly* undermine their own human ability to deal with uncertainty and paradoxes when dealing with complex problems. So when processes and mechanisms are developed to support such an investigation process, they tend to omit *obvious* human activity and reasoning that is contextually necessary. Ironically, if implemented and used as intended, because of the nature of such support systems, they would tend to undermine efforts to focus on questions related to individual judgment and understanding of the relevance of the problem. Elements of the SST Framework have been designed to accommodate four possible logical possibilities, and it is argued that this framework is a good candidate for addressing the requirements of digital forensics investigations.

Conclusions [Heading]

Cyber crime investigations can benefit from more advanced methods of thinking about how to investigate a complex cyber crime. An experienced forensic analyst aims to place any investigation into context for the purpose of transforming information from unstructured to structured uncertainty. Any approach that is aimed at supporting investigators to make decisions and to communicate with each other must be able to incorporate a number of different people with different worldviews, languages and cultures. But this is not enough; an approach must do more than support interaction, it must also enable individuals to embrace uncertainties in their everyday life as investigators. It is suggested that the SST framework is a worth while contender to be developed and applied for the purpose of supporting complex cyber crime investigations.

Peter M. Bednar is a Researcher at the Department of Informatics at Lund University, Sweden and a Senior Lecturer in Systems and Information Systems at the School of Computing, University of Portsmouth. His main research area is in systems analysis, focusing on how humans deal with complex and uncertain problems.

peter.bednar@ics.lu.se

Vasilios Katos is Assistant Professor in Information and Communication Systems Security at Democritus University of Thrace, Greece; previously he was a Principal Lecturer at Portsmouth University. He was an expert witness in computer security for a trial in the United Kingdom. His research interests are in computer security and forensics.

vkatos@ee.duth.gr

http://utopia.duth.gr/~vkatos

Cheryl Hennell, Openreach, United Kingdom

cheryl.hennell@openreach.co.uk