Cyber-Crime Investigations: Complex Collaborative Decision Making

Bednar, Peter; Katos, Vasilios; Hennell, Cheryl

Published in:
[Host publication title missing]

DOI:
10.1109/WDFIA.2008.7

2008

Cyber-Crime Investigations: Complex Collaborative Decision Making

Peter M. Bednar
Department of Informatics
Lund University
Sweden
peter.bednar@ics.lu.se

Vasilios Katos
Department of Electrical and Computer Engineering
Democritus University of Thrace, Greece
vkatos@ee.duth.gr

Cheryl Hennell
BT Openreach, UK
cheryl.hennell@openreach.co.uk

Abstract

This paper reports on the challenges computer forensic investigators face in relation to collaborative decision making, communication and coordination. The opportunities, operational environment and modus operandi of a cyber criminal are considered and used to develop the requirements in terms of both skill sets and procedural support a forensics investigator should have in order to respond to the respective threat vectors. As such, we show how a published framework for systemic thinking can be fit for purpose for supporting the collaborative enquiry and decision making process.

1. Introduction

The ontological perspectives of the 20th Century criminal investigator have in the 21st Century evolved further in response to the advances in IT which have created and facilitated malfeasant activities with a global nature. Such changes require a paradigm shift in the mind of the investigators as they are required to both understand and comply with legal frameworks and cultures, from a multi-national perspective. 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 dictated such an approach [1]. 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 [2] and in turn the global nature of cyber-crimes, have exacerbated the need for investigators to engage in complex inter-group communication on a multinational basis as they and criminals alike take advantage of these interconnected technologies. Furthermore, the need to navigate between different judicial systems throughout the world creates a challenging environment for crime scene investigators. Where criminals are using information technologies in any capacity across national boundaries, it is unsatisfactory for investigators to operate on a lone basis. The lead investigation team will require collaboration between members of different socio-cultural communities and experts in different areas. These aspects are in conflict with the idea of the concept of the highly promoted and marketed ideal of McLuhan's Global Village [3]. In practice the 'global community' is helping to create a heterogeneous world of a multitude of competing and possibly contradictory value and belief systems. This phenomenon raises the level of complexity making the cyber-crime scene a greater challenge for any investigator and a more pertinent area for research than before [4].

Axiomatically, collaboration in forensic investigations is grounded in the theory of both legal tradition and complex technical implementations. However, against the above, it can be argued that a typical crime scene investigation can be viewed as a special case of collaborative decision-making. In summary, cyber-crime scene investigations potentially draw together participants from a variety of national and potentially cosmopolitan backgrounds. The interactions of diverse socio cultural backgrounds of the participants as well as the different legal frameworks increase the complexity of communicative collaboration underpinning the decision-making processes [5].

The main goal of this paper is to highlight some of the issues involved in collaborative decision making as part of a digital forensic discovery process in practice, focusing on the particular problem of determining the scope of inquiry and problem space (electronic crime scene). Furthermore, this is illuminated by specific instances where the communications may be international in conjunction with a multi-role perspective. Within this context, it is relevant to explore the following issues:

- How do we incorporate key elements in investigatory practices/experiences to deal with the complexity of supporting investigatory teams' collaborative decision making activity?
- How do we decide where relevant data/evidence for investigation (decision making) come from and how is it assembled?
- Who is or should be involved in determining the scope and boundary of the investigation, and how?
- How do forensic investigators collaborate with each other and other key stakeholders to build up common understanding of boundary problems and unequivocal language?
- The logistics and complexity of negotiations; how is reductionism and complexity dealt with in the investigation and decision making processes?

This paper focuses on the complex collaborative decision making processes in context of cyber-crime investigations. There is a clear distinction between data processing and decision making processes. The main concern therefore is not on the management of data or information, but on the support of human decision making with respect to the judgment of relevance.

The issues highlighted above are studied using aspects of a reference model for e-Discovery as an example. By elaborating on the "Information Management" and "Identification" stages of this model, we highlight examples of requirements for a collaborative decision support system within the forensic investigation process. We outline an approach which incorporates strategies that inherently take these types of requirements under consideration.

In this paper we use the terms cyber-crime investigation, e-discovery and digital forensics. Since there is no unequivocal agreement behind the particular meaning of these terms, in this paper we mainly refer to cyber-crime investigation as a general term with a particular focus on the inquiry process and boundary setting of problem space. E-discovery is a special case of a cyber-crime investigation dealing with any type of analysis and documentation of electronic evidence. Digital forensics is used as a reminder of the requirement of performing the investigation and analysis in a way that the findings would be admissible in a court of law.

The remainder of this paper is structured as follows. Section 2 grounds our discussion of the need for collaborative communication in cyber-crime investigations. In Section 3 we further develop the requirements and attributes of the forensic investigator in order to participate in the collaborative cyber-crime investigation process. In Section 4 we present a framework which draws together the threads from the discussion of the previous sections. In Section 5 an e-discovery reference model is introduced in the discussion and used to highlight the current limitations in relation to the inquiry stages for setting the scope of an investigation. Finally, Section 6 contains the concluding remarks.

2. Identifying the need for collaborative enquiry and communication

As with many traditional crime scene investigations, a cybercrime investigation may need to inquire into private spaces of individuals who may or may not be proven guilty of a crime which is being investigated. As risks in encroaching on innocent individual's rights are recognized in traditional inquiries, there are many safeguards in place to protect individuals from overzealous efforts and traditional investigatory practices. However, because of its newness, in cybercrime investigations there is still much confusion over practices and their boundaries. These issues are adding to the complexities surrounding the decision making process engaged in cybercrime investigations and require additional expertise.

When it comes to combating online fraud and cyber criminal activities in general, it has been recognized that existing procedures and practices in forensic investigations are in need of further development [6]. Advances in information technology and the pervasiveness of digital media whilst serving to promote access to and facilitate processing of data have also provided the criminal mind with extended opportunities [7]. An individual or group of individuals commits new variants of traditional crimes, and more recently cyber-crimes, in the privacy of their own homes using personal IT equipment or in the workplace using business facilities. These malfeasant activities may exploit digital media to capture, store, orchestrate and present all forms of data in an effective and efficient manner. Statistics on the frequency of computer/Internet crimes point to the value of the

enactment of computer crime-specific laws and illustrate how computer crime has moved towards the front of crime concerns for the nation [8,9]. In recent times, cyber-crime is considered to be the world's biggest growth industry [10]. The impact of digital advances has changed the landscape of the crime scene, amplifying further the need for cross-boundary collaboration, revised sound forensic practices and surrounding procedures. Technology is advancing so rapidly that few people ever realize the complexity [11]. The menace of organized crime and terrorist activity grows ever more sophisticated as the ability to enter, control and destroy electronic and security systems develops [11]. A digital forensic investigation is a special case of a digital investigation where the procedures and techniques that are used will allow the results to be entered into a court of law [12]. A crime scene for an investigator is any area where they believe they may be able to identify facts or evidence which they can produce to a court or from which other inferences can be made [13].

There has been considerable discussion regarding the definition of the crime scene and more recently the cyber-crime scene. Blurring of distinctive boundaries occurs due to the ubiquitous nature of digital media and the skills needed to manipulate data, together with the varying contribution made by use of such media to any given crime. The term cyber-crime has no specific reference in law [14] but is axiomatically associated with criminal activities involving information and communications technologies. Changes in society, technology and behavior have influenced the environment and opportunity for crime and therefore the boundaries of the crime scene. Furthermore these changes also serve to extend the investigation team requiring additional skills. Despite the significant progress in multiagent teamwork, existing research does not address the optimality of its prescriptions nor the complexity of the teamwork problem [15]. A central challenge in the support for and coordination of forensic investigators is enabling them to work together, as a team, toward a common goal (see for example [15]).

3. Cyber-crime scene investigation

As described in [7], "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 believe that there is a small chance of being prosecuted, let alone being caught for their actions". This is further supported in [16], where it is colorfully stated that "for the first time, criminals can cross international boundaries without the use of passports or official documentation". Furthermore, as recognized as far back as 1989 by the Council of Europe [17], cyber-crime is transnational by nature. As efforts for international harmonization of the various legal frameworks are made (see for example [18,19]), the need for operational co-ordination and collaboration across socio-cultural boundaries should not be overseen. Traditional crime is noticeably different from cyber-crime as a phenomenon. The intangible and abstract nature of the problem space results into significant challenges for the forensic investigator. While an experienced forensic investigator would recognize best practices in dealing within a traditional crime scene, few recognize how to set boundaries and select what is relevant in such an abstract and intangible cyber environment. This is not only a technical problem, but a significant socio-cultural and collaborative problem which becomes even more complex due to its trans-national nature [16].

To make the challenges of a cyber-crime investigator even more intense, the advances in the use of digital technology to support corporate and personal activities have created potentially vulnerable operating environments. Digital forensics is concerned with the investigation, analysis, preservation and presentation of digital evidence as part of the judicial process [20]. In addition, information systems security approaches can be used to promote business continuity and recovery to mitigate the effects of unauthorized intrusion [21]. The opportunities for criminals to use digital means for their modus operandi are many, e.g. the Internet is used to distribute child pornography; sophisticated fraud is carried out by identity theft. The combination of availability, simplicity of use, mobility, high performance, affordable technology, coupled with the lack of user awareness to protect their systems, offers the criminal imagination considerable possibilities.

As previously discussed, the characteristics of crime scene investigations have evolved over the last few decades such that the skills and attributes also require reflection. We contend that those involved in forensic investigations will need to have a holistic view and knowledge of their domain from four perspectives: technical (what is possible); professional (what is permissible); practice (what is appropriate); ethical (what is right and legal). Technical expertise is concerned with understanding digital information and communication technologies. More precisely, knowledge required would 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 / server programming.

The crime scene investigation (physical or cyber) should be conducted professionally. In the UK for instance, investigators are bound by the Association of Chief Police Officers guidelines [22]. In summary these guidelines encompass; ethics and its relation to the law and computing, computer law, legal processes, digital evidence and include a regulatory framework for digital investigation.

In practice where specific scenarios are to be investigated, technical and professional strands merge and may be applied in a private or public setting, i.e. in an individual suspect's home, corporate site etc., this may be required to pursue in an international environment. Additionally where incidents are suspected to have occurred in a commercial environment, forensics investigators would need to examine and take into account business considerations such as business continuity plans, disaster recovery plans and information security plans. This is required not only because these considerations might provide the technical evidence to support the investigation, but also to avoid creating a disaster themselves through the intervention of their investigation. Successful prosecutions may be achieved where appropriate collaborative communication has been adopted in conjunction with: 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 depend on situation and technology but also on socio-cultural contexts and applied legislative frameworks. These issues are clearly also dependent on national and inter-national contexts. Historically, international organized crime, terrorist activities and other high profile crimes would often be targeted by specifically formed groups and organizations of experts and at times task forces. This may have been successful as long as there were relatively small numbers of people which could be targeted with exceptional centralized resources. The problem with cyber-crime is that it is something which 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 and thus its consequent ubiquity more or less any existing crime can in one way or other 'become' transformed or extended into a cyber-crime. In addition there are new previously unheard of activities that are difficult to classify in existing legislature frameworks. One could say that today cyber-crime is the 'everyday' crime of the new era. It is not anymore the specialist groups of experts who will have to be able to target cyber-crime but your local investigator in collaboration with local investigators possibly in a different country.

The points above make it fairly obvious that when it comes to considering cyber-crime, the problem space for forensic investigators may become extended and significantly complex in comparison with a traditional crime scene. Setting aside current tentative and at times confusing activities, even with robust set of skills and legal frameworks in place, 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 cyber-crime scene transcends national boundaries and traditional legal jurisdictions. Below we briefly introduce an overview of a framework for the purpose to facilitate a complex inquiry with high requirements on its collaborative working environment among members of investigatory teams and between investigatory teams.

4. A case for strategic systemic thinking

In [6] it is stated 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". The framework for Strategic Systemic Thinking (SST) described in this section, supports both the involvement of all stakeholders in a multi-facetted enquiry. The SST framework was developed as a vehicle to promote and assist in organizational sense-making processes and provide support for inquiry; leading to a richer knowledge base on which informed decision making / action might be founded (e.g. [23]). It was developed specifically to help teams of users to deal with analysis of complex problem spaces and to embrace multiple levels of uncertainty. These features make it a suitable candidate for incorporation into cyber-crime scene investigating practice. Earlier work with the cyber-crime scene in mind shows some promise [13]. In the Crime Scene Investigation context the SST framework could provide complex inquiries led by teams and groups of investigators systemic support for their interaction, analysis and synthesis efforts, and work during the investigation.

The SST framework involves three aspects, which are not sequential and may be applied in any order [23]. It is intended to be iterative and it is possible to move from one analysis to another repeatedly and in any direction, at any time. A first pass through the framework may be undertaken in order to promote creation of a version specifically adapted to the requirements of a particular problem space. The process thus created is then applied in the inquiry. Care

is needed to ensure that investigators feel empowered and safe within their fields of expertise and responsibility, in order to express their world views. It must be recognized that any intervention involves risk. An investigator's sense-making strategies are also dependent upon the organizational culture within which they are set [24]. Differences between organizational cultures have a strong influence on what kind of individual autonomy is acceptable.

It is an essential characteristic of the SST framework that ownership of the ongoing inquiry should rest with the investigators involved. A team of investigators who engage in the inquiry would be comprised of specialists, and one or more external facilitators (experienced in systemic methods for inquiry etc) who provide support and guidance. The framework supports investigation of a problem space through inquiry into multiple levels of contextual dependencies. With the support of the framework, each individual investigator involved is enabled to explore their personal unique perspectives. These individuals are then supported to examine, and discuss as a group, the range of individually-created narratives, in order to discover the range of opinion. The aim with the framework is not to seek for a consensus, but to enrich the base from which informed action could proceed. A range of methods might be used by investigators seeking to articulate their worldviews, e.g. creation of mind-maps, effective rich pictures or role playing etc. in order to support visualization and communication of mental models. The aim is to bring about a constructive dialogue between different investigators and investigatory teams; whoever will be engaged professionally in the investigation by any change resulting from action based on the ongoing inquiry.

If an investigator is asked about features of her problem experience, this may reveal only those aspects of which the person is explicitly aware and remembers at a particular time. A description which is at best imperfect is likely to result. In order to explore the 'know how' residing in a collaborative team of crime scene investigators (in order to promote strategic thinking), it is necessary to adopt methods which enable individual team members to explore multiple experiences of dynamic roles, and tease out a range of shifting, reflective perspectives to expand and illuminate their ideas. In seeking to explore professional experience, rather than to describe a culturally filtered and thus unwittingly censored scenario, tacit as well as implicit knowledge can be supported to emerge. The aim of an investigation may be to uncover what is not known. However, without opportunities to reflect and evaluate what emerges, creativity cannot be supported. Individuals need opportunities to explore multiple, simultaneous and dynamic roles and competencies, and consequent differing perspectives, in their experiences [25]. This is an active, creative process rather than a discovery of something pre-existing. Problems which arise in investigations into cyber-crime tend to be complex. Many different dimensions impact on one another and are difficult to disentangle. It would be possible for those engaged in the investigation to become discouraged in the face of complexity and to wish to find ways to simplify. However, we suggest that a better approach is to 'complexify' analytical investigatory approaches. It is recognized in cybernetics that every distinct dimension of a complex system needs to be controlled in a way which is appropriate to its characteristics [26]. By extension, every dimension of a complex environment needs to be explored with appropriate methods for analysis/synthesis.

One aspect of the SST framework is intra-analysis, which addresses individual perspectives on structuring uncertainty in any perceived problem situation. Individual investigators are supported to explore their own unique perspectives on contextually-relevant aspects of the scenario in which they are involved. Questions derived during preliminary analysis by investigators in the inquiry team may be used to empower individual investigators to explore their situation, using methods such as rich pictures. A further element of SST is inter-analysis. This part of the inquiry represents a collective reflection on alternative narratives created during intra-analysis, and the aim is to derive and consider the range of world views derived through intra-analysis. At this point, no particular perspective is excluded. Similar views are consolidated into categories in order to support creation of a dialogue about the range of views. This represents an investigation into contextual dependencies by the whole investigatory team, producing a collective map of the problem space from each unique individual point of view. The purpose is not to achieve a consensus or to establish common ground (regarding 'solutions'). It is however intended to help in creating support for establishing common ground for communication about 'understanding' and sense-making'. It is recognized that good ideas for promoting analytic understanding may initially appear to be unrealistic or 'off-the-wall' and that consensus may focus on what is known and safe, to the exclusion of creativity and productive learning. The third aspect of the framework is a value analysis, or evaluation. Evaluation represents an examination of what is assumed to be known, i.e. the results of analysis. Here, team of investigators and analysts reflect upon the range of perspectives derived through inter-analysis to consider what they may have overlooked, under-

estimated or over-estimated, and to what extent their individual competences, prejudices, etc. may have impacted on the results of the inquiry.

One significant aspect of the SST framework is its capability to incorporate multi valued logic (see for example [27]). In digital forensics there is a need to apply an extended model of logic which goes beyond the limitations of traditional bi-valued logic. This is becoming necessary for everyday analytical practice to support decision making efforts. Even simple dualistic decisions (enforced bi-valued logic, e.g. guilty vs. not-guilty) require as preparation an analysis and decision base covering a multi valued landscape (problem space).

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. Boundary issues which become relevant include the following question: what is the scope of the investigation? Additional issues have to do with fuzziness of exclusion, assumptions of what is not evidence. From a formal perspective, this could be approached by applying fuzzy logic which, however, does not manage to help the users to escape from assumptions that something has to be on some scale of "certainty". In the development of the complex situation unfolding when it comes to cyber-crime investigations, the investigation as such is in need to introduce uncertainty in the following way:

- unstructured uncertainty: assumption of not having enough information to commit to a decision
- structured uncertainty: assumption of too much information, conflicting information, ambiguities, paradox (can be true and false at the same time).

Not only can an expert 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 others is one of several reasons for why bi-valued logic is inappropriate and in practice not applied in investigations. Elements of the SST Framework have been designed to accommodate four-valued logic and therefore this framework is a good candidate for addressing the requirements set within the forensics investigation context.

5. E-Discovery

In this section we discuss e-discovery as this is becoming an integral part of cybercrime investigations. In this paper we use the EDRM reference model as an example for examining the properties in such investigations.

The Electronic Discovery Reference Model (EDRM) shown in Figure 1 is an initiative to address primarily the need for evaluating electronic discovery solutions. There reference model currently involves nine distinct stages.

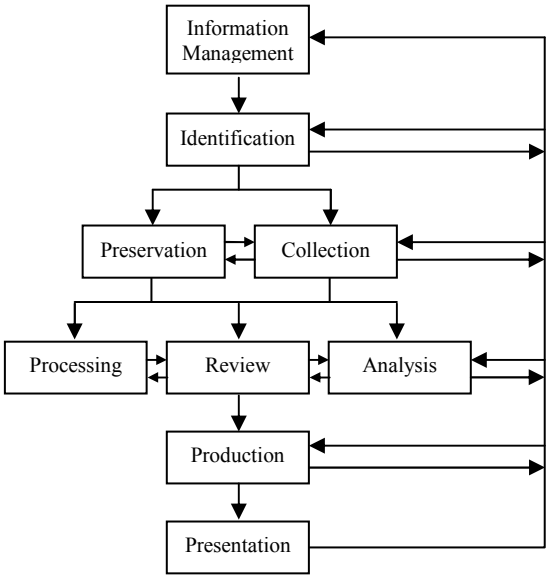

Figure 1. The Electronic Discovery Reference Model, EDRM (adapted from: [28])

Preservation, Collection, and the stages following these two have received significant attention both from practitioners and vendors.

However, we contend that the first two stages, namely information management and identification, have certain limitations which could undermine the e-discovery process as a whole, as explained in the remainder of this section.

According to EDRM, Information Management focuses on effective record management and documentation. The reference model adopts a direction of rational inquiry focusing on a rigorous investigation protocol. For instance, a representative set of guidelines includes the following:

"*1. Ensure that all needed business records are retained;*

2. Ensure that all records that are required to be retained by stature, regulation, or contract are retained for the appropriate and approved period of time;

3. ..." (edrm.net)

It can be seen from the previous excerpt, that the directions of the guidance explicitly highlight the importance of a protocol, whereas the actual feasibility is not challenged. For example, the first point requires that all needed business records are retained. Rather than facilitating, this point ignores the problem of determining the scope of the relevant context. In other words, it is suggested that the investigator has *a priori* knowledge of the problem space boundary (eg. scope and relevance).

The Identification stage consists of four steps, Initiate, Interview, Assess, Document (Figure 2). The model describes an ideal scenario by assuming that these four steps are sequential. This constraint is a direct consequence of the a priori knowledge assumption as described above. This mindset is followed up in the Interview step: by definition the concept of interview assumes that one person – typically the interviewer – leads the inquiry by knowing which questions to ask. Furthermore, the nature of an interview as an example of asymmetric communication, excludes by definition a more fully developed symmetric engagement. It cannot be expected to deliver an inquiry based on asymmetric communication when the scope is unknown (if we don't know what we are looking for, how do we know what questions to ask?). The EDRM guidelines suggest in the Interview stage, that there is a need to seek advice when determining the scope of the problem space. This shows an admission that the problem scope is unknown to the investigator. Consequently, if this is the case, it would be necessary to admit that the focus of the investigation is also unknown.

Nevertheless, knowing what questions to ask implicitly assumes that the answer exists in the perceived problem space. In essence, such an assumption leads to exclusion of uncertainty within the investigation process. This can be illustrated by showing that in the case of the EDRM analysis approach, classic probability is sufficient to be used as the underlying analysis primitives. More specifically, if the answer exists within the original scope (prior to any reduction activity), the forensic investigator may at the very least invoke a non-deterministic process to find the answer; if the answer is not found, the scope is reduced by excluding the wrong assumption. It can be trivially shown that if the answer did not exist within the original scope, then any reductions would be pointless. An equivalent statement would be to consider that the investigator adopted a closed system view.

On the contrary, if the investigator accepts uncertainty with respect to the inclusion of the answer to the problem under investigation (i.e. adopts an open system view), then it can be seen that Probability Theory would be handicapped in modeling the reasoning and analysis of the investigator, whereas primitives that allow uncertainty such as Dempster-Shafer's Theory of Evidence [29] would be the appropriate choice.

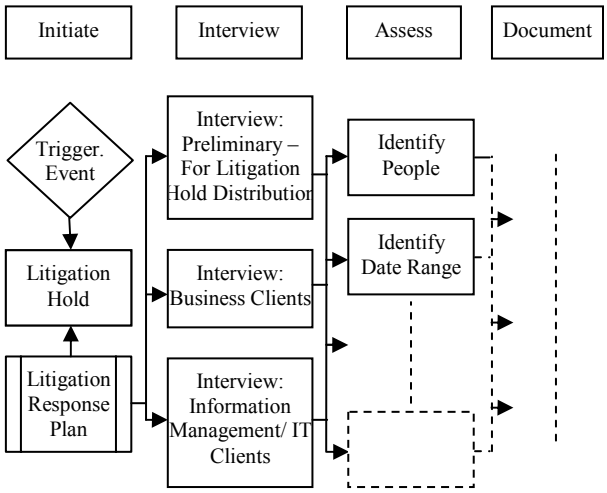

Figure 2. The identification stage (adapted from: [28])

Once it is recognized (accepted) that an investigation is not only complex because of inquiry into a problem, but also due to the uncertainty on what is a relevant problem space, the possibilities for inquiry should be widened rather than narrowed. Obviously, an investigation to be realistically resourced and managed, needs to be narrowed, e.g. a reductionist's approach should be considered at some stage. This reduction cannot be done before the problem space (e.g. the scope of the problem) has been determined. On the contrary, there needs to be an allowance of complexification. This is justifiable, as an investigator may not initially have considered a scope that may include the problem and therefore his/her worldview would merit expansion. Such an exercise is necessary when there is uncertainty in determining the relevant problem space. Figure 3 shows graphically: (a) the original EDRM proposition which represents a paradigm supporting the monotonic property of scope reduction; and (b) the complexification/reduction approach to cater for the inherent uncertainty in defining the scope, which represents a paradigm supporting possible non-monotonic property. The vertical axis represents the complexity and size of the problem space. The EDRM approach starts with a given (maximum size) problem space which is gradually reduced as the investigation moves into the later stages. We advocate that in a realistic investigation the problem (or solution) may not

necessarily be within what is initially assumed to be the problem space and therefore subsequent reductions of that space would have no particular relevance.

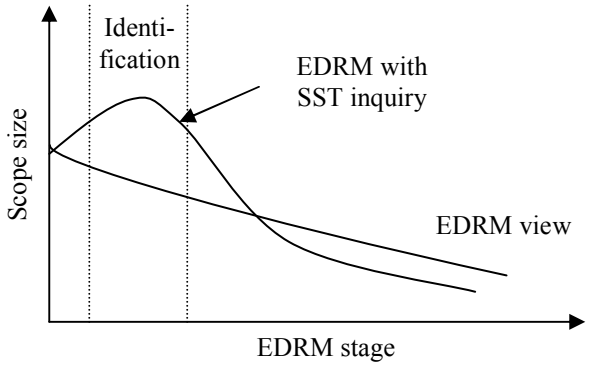

Figure 3. Complexification and reduction (monotonic vs. non-monotonic)

The contribution of the SST framework is to aid the investigators in their efforts to expand and reframe the scope of cyber-crime investigation (e.g. complexification). One of the main features of the framework is to support investigators in challenging the initially perceived problem space and problem description.

The EDRM is a generic investigation framework and does not accommodate support for context awareness. The SST framework with its supporting questions can help participants to develop and negotiate the redefinition of the problem space. By focusing the effort of analysis and synthesis on boundary issues, judgment on relevance can be then accommodated. More particularly, in the identification stage "interview" should be traded with "interaction" since an interview would expect the interviewer to have a predefined understanding of the boundaries of the problem space. In complex problem spaces the boundaries are unclear and non-trivial to draw. Therefore there is a need for co-development and co-creation of relevant questions to guide the inquiry process. As such, SST can be used to inform the EDRM identification stage by introducing contextual analysis, to avoid premature conclusions.

6. Conclusions

Systematic practice in the cyber-crime investigation context is a green field when it comes to addressing the following aspects: defining, understanding, agreeing (negotiating) an investigation scope. It also includes the requirement to port well known forensic investigation principles and methodologies, e.g. Locard's principle [30], into the cyber-crime problem space. This includes taking into consideration issues such as those dependent on any isomorphism of Heisenberg's uncertainty principle, for example how to investigate e.g. a digital content without observing it, in order to preserve it. The arena for the digital forensic field becomes not only systematically complex but also significantly overwhelming even for experienced investigators, rich of systemic uncertainties. An experienced forensic analyst makes an effort to successfully contextualise the investigation for the purpose of transforming information from unstructured to structured uncertainty. This happens in a multitude of context and trans-nationally from a multitude of socio-cultural environments. Any approach which is to support investigators to make decisions and to communicate with each other must be able to incorporate different stakeholders with different worldviews, languages and cultures. But this is not enough; an approach must do more than support interaction, it must also enable individual stakeholders to embrace uncertainties in their everyday information creation and efforts to exchange information. We support that these problematic issues make the SST framework worth a while contender to be developed and applied for the purpose of supporting complex cyber-crime investigations.

7. References

[1] C. Valier, "True Crime Stories: Scientific Methods of Criminal Investigation, Criminology and Historiography", *Brit. J. of Criminology*, vol. 38, no. 1, 1998, pp.88-105.

[2] S. Mitropoulos, D. Patsos, C. Douligeris, "Incident Response Requirements for Distributed Security Information Management Systems", *Information Management and Computer Security*, vol. 15 no.3, 2007, pp. 226-240.

[3] M. McLuhan, *Understanding Media*. New York: Mentor, 1964.

[4] R. Broadhurst, "Developments in the Global Law Enforcement of Cyber-Crime", *Policing: An International Journal of Police Strategies & Management*, vol. 29, no.3, Emerald, 2006, pp. 408-433.

[5] J. Sliter, "Organized Crime in Business", *Journal of Financial Crime*, vol. 13, no.4, Emerald, 2006, pp. 383-386.

[6] J. Mulholland, Message from the Guest Editor, Special Issue: Phishing and Online Fraud part 2, J. Digital Forensic Practice, vol. 1, no.3, 2006, pp. 151-2.

[7] M. Karyda and L. Mitrou, "Internet Forensics: Legal and Technical Issues", in *Proceedings of Second International Annual Workshop on Digital Forensics and Incident Analysis*, Preneel, B. Gritzalis, S., Kokolakis, S., Tryfonas, T. (ed), IEEE Computer Society, 2007, pp. 3-12.

[8] G. R. Gordon, C. D. Hosmer, C. Siedasma, and D. Rebovich, *Assessing Technology, Methods and Information for Committing and Combating Cyber Crime*, The Computer Forensics Research & Development Centre (CFRDC), Utica College & Wetstone Technologies, Inc, National Institute of Justice, 2000-9614-NY-IJ, 2002.

[9] D. Gooding, (2008, April). Securing cyberspace against war, terror and red tape. *The Register* [On line], 2008. Available: http://www.theregister.co.uk/2008/04/25/greg_garcia_interview/

[10] T. Ghaffer, Keynote, in *2nd International Conference on Global e-Security* (ICGoS), April 2006, University of East London.

[11] H. Jahankhani, *Waking Up to the Threat of Cyber Crime*, Information Security, 2006.

[12] R. Baker, D. S. Beaupre, W. Cassaday, D. J., Icove, H. Stambaugh, and W. P. Williams, "Electronic Crime Needs Assessment for State and Local Law Enforcement", *Research Report* NCJ 186276, National Institute of Justice, Washington, DC, 2001.

[13] V. Katos, and P. M. Bednar, "A cyber-crime Investigation Framework", *Computer Standards & Interfaces*, Elsevier, vol 30, no.4, 2008, pp 223-228.

[14] M. Yar, "The Novelty of 'Cybercrime': An Assessment in the Light of Routine Activity Theory", *European Journal of Criminology*, vol. 4, no.2, 2005, pp 407 – 427.

[15] D. Pynadath, and M. Tambe, "The Communicative Multiagent Team Decision Problem: Analyzing Teamwork Theories and Models", *Journal of Artificial Intelligence Research* 16, 2002, pp. 389-423.

[16] M. Britz, *Computer Forensics and Cyber Crime*. New Jersey: Prentice Hall, 2004.

[17] 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.

[18] OECD, *Recommendation of the Council concerning Guidelines for the Security of Information Systems*, OECD/GD(92) 10, Paris, 1992.

[19] United Nations, *United Nations Manual on the Prevention and Control of Computer-Related Crime*, UN: New York, 1994.

[20] W. G. Kruse II and J. G. Heiser, *Computer Forensics: Incident Response Essentials*, Addison Wesley, 2001.

[21] K. Scarfone and P. Mell, (2007, February). Guide to Intrusion Detection and Prevention Systems (IDPS), *Special Publication* SP800-94, [On line], National Institute of Standards and Technology, Available: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[22] ACPO, Association of Chief Police Officers (2007). *Good Practice Guide for Computer based Electronic Evidence*. [On line] Available: www.7safe.org

[23] P. M. Bednar, "A Contextual Integration of Individual and Organizational Learning Perspectives as Part of IS Analysis", *Informing Science Journal,* vol. 3, no.3, 2000, pp. 145 - 156.

[24] E. Schein, *Organizational Culture and Leadership*, 2nd edition, Jossey-Bass, 1992.

[25] P. M. Bednar, "Individual Emergence in Contextual Analysis", *Systemica*, vol 1-6, no. 14, 2007, pp. 23-38.

[26] R. Ashby, *An Introduction to Cybernetics*, Methuen: London, 1964.

[27] P. M. Bednar, C. Welch, and V. Katos, "Four valued logic: supporting complexity in knowledge sharing processes", in *Proceedings of 7th European Conference on Knowledge Management, ECKM 2006*, Corvinus University of Budapest, Hungary, 4-5 September, 2006.

[28] EDRM, Electronic Discovery Reference Model, [On line] Available: http://edrm.net/

[29] G. Shafer, *A mathematical theory of evidence* Princeton University Press, Princeton, 1976.

[30] R. E. Saferstein, *Criminalistics: an introduction to forensic science*, 6th edition, Prentice Hall, Upper Saddle River, NJ, 1998.