Digital forensic investigations: a new frontier for Informing Systems

Bednar, Peter; Katos, Vasilios

Published in:
[Host publication title missing]

2008

Digital forensic investigations: a new frontier for Informing Systems

P.M. Bednar[1] [2], V. Katos[3]

Abstract: Digital forensic investigators experience a need for support in their everyday struggle to overcome boundary problems associated with cyber crime investigations. Traditional methods are socio-culturally and physically localised and dependent on strict and historically prescriptive political management. The new internet-worked cyber-world creates unprecedented difficulties for digital forensic investigations. This is directly linked with the inherently complex uncertainties and ambiguities related to a constant need for framing and re-framing of problem spaces under investigation. As such, in this paper we propose the recruitment of the discipline of Informing Systems in the context of digital discovery. Early findings of such an exercise indicate that informing systems approaches can assist the investigation process by offering means for structuring uncertainty. As it is accepted that uncertainty is an inherent element in a crime scene, not least in a cyber crime scene, we consider the contribution of Informing Systems vital for the effectiveness of digital forensic investigation practices.

Introduction

Digital forensic investigations present a new international frontier for Informing Systems research and practice. This is due to the inherent, complex uncertainties involved in boundary setting and framing of an investigatory problem space [1]. Informing Systems (Information Systems which incorporate Human Activity Systems) intended to support digital forensic investigations are often discussed in relation to generic problem of large and complex investigations. However, very little research seems to be available focusing on support for cyber crime investiga-

1 Lund University, Department of Informatics, Lund, Sweden, email: peter.bednar@ics.lu.se

2 University of Portsmouth, School of Computing, Portsmouth, UK, email: peter.bednar@port.ac.uk

3 Democritus University of Thrace, Department of Electrical and Computer Engineering, Xanthi, Greece, email: vkatos@ee.duth.gr

tions. For example, in the UK, successive versions of Home Office Large Major Enquiry Systems (HOLMES), for managing and processing data in complex investigations, date back to 1986 [2]. While use of such systems could be productive in pursuing an inquiry, it does not help investigators as they struggle to overcome boundary problems associated with cyber crime [3,4]. Research into relationships between new technology forensic experts and traditional investigators has tended to focus primarily on the difficulties of managing large quantities of material (e.g. forensic images, extracts, non-computer evidence rendered into digital form, metadata, etc). Further challenges in this context have included retention of documents and management of relevant digital evidence that must be served to the opposing legal team before a trial [3,4,5,6,7]. This body of research does not in any way address the difficulties an investigator may face in (re)framing relevant problem spaces for investigation, with their inherent ambiguities and uncertainties [8]. This paper presents an approach to an issue that has been researched very little: the difficulties posed by decision-making among investigators attempting to collaborate in cases of digital, cyber or electronic crime.

The authors show how the framework for Strategic Systemic Thinking (SST), which is a valuable tool for contextual inquiry, can be applied to the specific context of digital forensics [1,9,10]. This is especially relevant where the organization of investigatory practice needs to adapt and "reinvent" itself, e.g. through innovation and communication across organizational and national borders. In these cases, SST could be applied as a means to identify and support individual engagement and to facilitate interaction/communication, especially in socio-cultural systems of high complexity. The authors demonstrate the usefulness of this approach for decision-making in the context of digital investigations. Some suggestions for putting this approach into practice are put forward. An internationally, recognized Electronic Discovery Reference Model (EDRM) is used as an example [11]. The difference in scope between HOLMES and EDRM is shown in Figure 1. The SST framework is integrated with the first two stages of EDRM (Information Management and Identification) to show how it could contribute to overcoming the inherent limitations and difficulties of boundary setting and scoping of cyber crime investigations.

However, efforts to combine the EDRM model with the SST framework are by no means straightforward. The EDRM model is a systematic, structured model whereas SST is a context-aware, systemic approach. These are significant differences, not only of character but of epistemological perspective. The authors discuss and elaborate upon ways in which these two complementary approaches could be combined successfully, despite their differing philosophical foundations. The main focus of this paper is on collaborative decision-making activities and processes in cyber crime investigation. An effort is made to apply SST in order to provide support in cyber crime investigation practice. This is complemented with some clarification on ways in which SST could be applied in such an investigation, and efforts to integrate SST with EDRM are described. This is explored through an elaboration of requirements for a collaborative decision support system

for digital forensics, always keeping in view the need to deal with the inherent uncertainties that prevail in a digital crime scene.

A New Frontier

In their professional life, digital forensic investigators may be confounded by the complexity and uncertainty they experience in 21st century cyber-crime investigations. This human experience of uncertainty has been described with the help of a metaphor of an information frontier: *"Why a frontier metaphor? Because it aptly captures recent experience: a decades-long period of progressive and lasting change, rich with opportunity and fraught with uncertainty. Frontiers are new terrains in which people roam, settle, and create value. Frontiers fundamentally alter not only what we do, but also how we see the world around us… By their nature, frontiers are confusing, volatile and – above all – unpredictable"*[12, p.6]. In this context models for systematic and robust decision making are promoted for the purpose to support rigour and eliminate uncertainties (e.g. the EDRM project). Then people often appear to think that a natural step follows – just invoke the power of combining a robust decision making with an IT project (e.g. the HOLMES project) and suddenly the failing digital forensic investigations will thrive, the difficult decisions will resolve themselves and the digital forensic practices will meet with success. It appears that people are looking for solutions to help them reduce complexity to simplicity and uncertainty to predictability. Leaders turn to projects in the expectations of finding a solution to life at the frontier. There appears to be a widespread fallacy that suggests rigorous practice of the "*correct*" procedures with the "*right*" IT system will automatically lead to delivery of value for an investigation. Unfortunately, in digital forensic practice, it is only when decision making and IT systems are utilised in conjunction with embedded competencies of analysts and investigators that genuine progress is made. It could be argued that: *"a critical weakness of these approaches is that they assume that the investigator is the consumer of methods and services, failing to acknowledge the value derived is not only co-created but also context dependent."* [13, p338].

Ciborra pointed out how situated perspectives in information systems research call for methods of inquiry which capture the inner life of the actor: mind and heart [14]. Knowledge creation has been described as: *"complex responsive processes, and processes of reproduction and transformation of identity, … an understanding of the processes of interaction of which we are a part"*[15, p98]. This description puts the emphasis on the immersion of individuals in the business of everyday living. Ciborra [16,17], drawing on Heidegger [18], highlights the experiences of everyday life as it is lived (Heidegger's "*Befindlichkeit*") and contrasts these with the formalised models and methodologies promoted in management literature. He suggest that, in organisations we: *"listen to practitioners and*

we participate in their dealings with puzzles and riddles; on the other hand we do not confer any particular relevance on words like 'strategy', 'processes', 'data', or 'system'. In so doing, and in putting aside the models and methods of management science, we come closer to the everyday life of the manager, which is made up of frustrations, accomplishments, gossip, confusion, tinkering, joy, and desperation" [17, p.19]. The success of the Internet, for Ciborra, is due to the strategic importance of the ordinary, e.g. bricolage, heuristics, serendipity, make-do – rather than scientific 'ideals'. This improvisation, as a de facto knowledge management system, supports knowledge creation, sharing, capture and exploitation. Such modes of operating occur at the '*boundary between competence and incompetence*', and require an element of licence, or even play, to be available to actors in order to be achievable within their communities of practice [19,20]. Activities that are situated, close to 'the dance' [16], tend also to be invisible, marginalised by management since they are difficult to control or to replicate outside of the immediate context within which a (local) community of practice resides. Improvisation when seen as a special, privileged case of cognition is reserved for spur of the moment or emergency decision making, to which normal considerations do not apply. However emergencies can be viewed as an extreme example of *life as it is lived* (Befintlichkeit). A cognitive view would be that quick thinking is involved in dealing with a situation (situated action). When asking politely in German '*Wie ist Ihre Befindlichkeit*' (How are you), a person is really inquiring into another's existential situation – '*How do you feel?*' [16]. Some views of situated action (e.g. AI) see an individual person as a kind of cognitive automaton. However, Ciborra suggests that appeals to situated/embodied knowledge need to take into account of the whole person who is *in the stream of living* – "*moods, feelings, affections, and fundamental attunement with the action*" [17, p.32]. As we encounter the world, certain aspects of it will matter to us – people, things, conditions. This possibility is grounded in how a person is affected, and this affectedness discloses the world in an intrinsically social way: as a threat, as a source of boredom, or as a thrill perhaps. As Ciborra says: *"If we are able to accept the messiness of the everyday world's routines and surprises without panicking, we may encounter business phenomena that deeply enrich the current 'objective' and reified models of organization and technology. We can then start to build a new vocabulary around notions closer to human existence and experience."* [17, p.19]. Ciborra emphasises the importance of mood throughout his later work. Concepts like '*hospitality'* are used to emphasise the affective domain. He makes use of the metaphor of treating new technology as a stranger, needing hospitality within the organization. This metaphor emphasises tolerance, welcome, being receptive, i.e. human feelings. Being a Luddite is, of course, also an emotional response to a perceived threat.

From HOLMES to EDRM

Since 1986 the Home Office Large Major Enquiry System (HOLMES) project (Figure 1) has been employed in order to support the UK police with their investigations. This system was primarily used to support investigations in major incidents including serial murders, multi-million pound fraud cases and major disasters [2]. HOLMES2, the current version of the investigation support system, is an operational level system with document management and context of inquiry dependent analysis tools. HOLMES2 has shown to have effectively supported crime solving through the systematic application of investigation procedures at a national level. As such, it can be argued that the discovery process can benefit from a system like HOLMES when it comes to investigating conventional crimes.

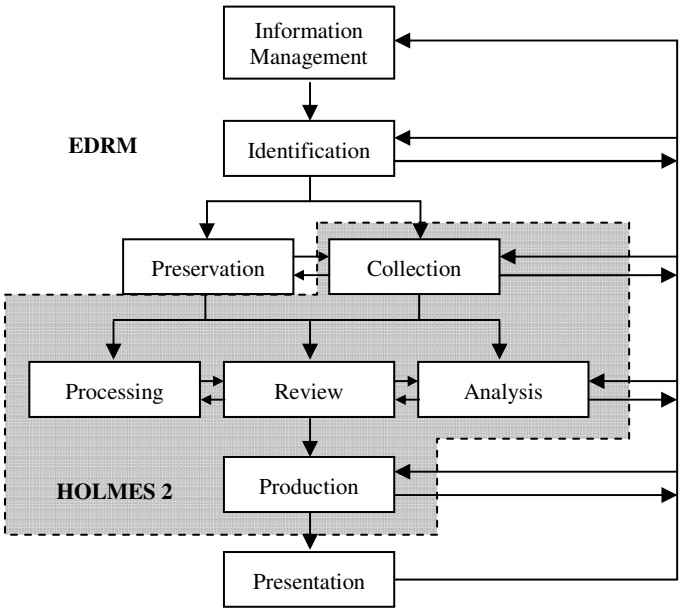

Figure 1. Scope of HOLMES within the EDRM.

In its essence, HOLMES2 is a collection of applications comprised mainly of a database and a type of a fulfilment centre performing the automated processing such as indexing. The following three applications have been deployed [21]:

1. *Casualty Bureau:* is used for assisting forces' coordination when dealing with the aftermath of major disasters;
2. *Incident Room:* is an application for capturing the information provided by the public (i.e. from witnesses);

3. *National Mutual Aid Telephony:* is used for the distribution of the telephone calls, between the host police force and the members of the public and other police units.

The user interface is mainly a collection of web forms. The end users who contribute with the user requirements are not surprisingly members of the UK Police Community [21]. However, when it comes to cyber crime investigations the key differences between the cyber-crime scene and the conventional crime scene may render a system like HOLMES unsuitable for the former type of investigations. More specifically, the trans-national flavour of a cyber crime where an offender may be in a different country or jurisdiction framework than that of the victim may increase the underlying communications complexity. Furthermore, the definition of crime, or boundary setting of a cyber crime scene, is a non-trivial exercise. The assessment of problem scope regarding inquiries into digital evidence and other electronic activities may involve not only disparate IT systems, but also engage across different socio-cultural environments, norms and legal frameworks. An attempt to respond to the pitfalls presented above was made by the Electronic Discovery Reference Model [11]. EDRM, being a model rather than an application, was developed at an abstraction level much higher than that of HOLMES in order to capture the electronic discovery processes and complexities. The EDRM is currently comprised of nine distinct stages which are fitted to the generic "preserve-acquire-analyse-report" crime scene management cycle. As such, the HOLMES system would cover the stages of Collection, Processing, Review, Analysis and Production of the EDRM model as shown in Figure 1. The first two stages, namely Information Management and Identification is of a particular interest to this paper because of the inherent focus on uncertain and complex problem spaces.

As the stages of Information Management and Identification relate to the recognition of the problem space, it is of paramount importance to ensure that these stages acknowledge the existence and influence of uncertainty. A closer look at these stages as specified by the reference model reveals that the inquiry process proposed makes assumptions that could lead to a degenerated problem space with an "event singularity" that would not necessarily be the answer. The adoption of the famous Sherlock Holmes paradigm "…when you have eliminated all which is impossible, then whatever remains, however improbable, must be the truth" is not necessarily applicable in modern complex crime problem space, since *all* events cannot be enumerated in principle. Therefore any model that subscribes to Mr. Sherlock Holmes's paradigm is handicapped, as it is presented below [22] for the case of the first two stages of EDRM.

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. …" [11]

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).

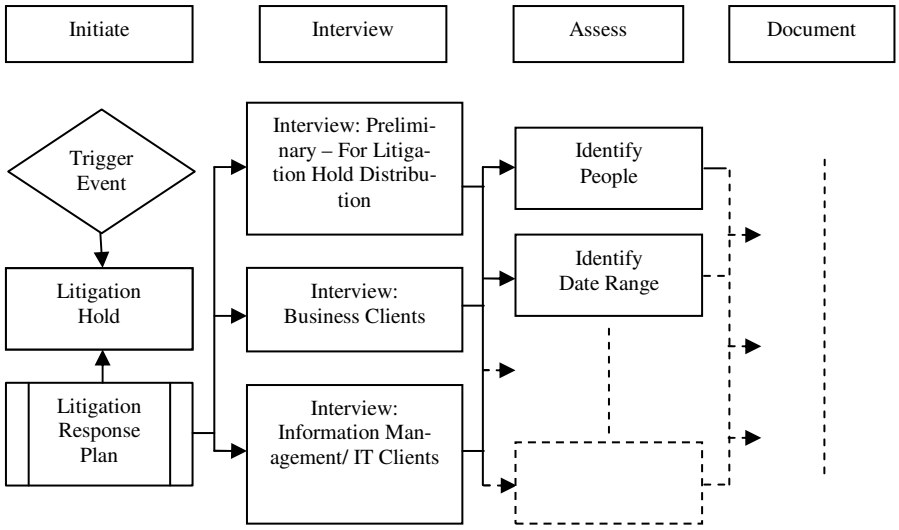

Figure 2. The identification stage (adapted from: [11])

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.

In any case, 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 modelling the reasoning and analysis of the investigator, whereas primitives that allow uncertainty such as Dempster-Shafer's Theory of Evidence [23] would be the appropriate choice.

A Framework for Digital Forensic Investigations

The SST framework is specifically suited to support the Information Management and the Identification stages. In these stages the complexity and uncertainty is not only due to a requirement to support investigators in finding the correct answers to relevant questions, but also dealing with the problem of not knowing what are the relevant questions to ask. On one hand it is about not knowing what is an appropriate definition of a problem and on the other hand it is about appreciating that the inquiry is about not even knowing what the problem "space" might be. The purpose with using the SST framework is to support the capacity of a human activity system in processing the information created by the different members of the investigatory team in such a way that [1,9,10]:

1. *Complement*, conflicting or incompatible ideas will not be mutually cancelled or demoted;
2. *Communication,* can take place on different orders of weltanschauung, between individuals, groups and super-groups.
3. *Socio-cultural,* dependent policy and legal constraints could be incorporated as part of the process.

4. *Expansion,* of understandings of different viewpoints is supported and not unnecessarily pre-constrained.

In the context of a Digital Forensic Investigation the SST framework can provide systemic support for dealing with complex inquiries with the following features:

'Intra-analysis' is focused on exploration and creation of individual investigators perspectives [1,9,10]. Each investigator has the opportunity to develop and consolidate descriptions and narratives of the problem space from their own unique perspectives. They do so by systematically using tools and methods such as brainstorming, mind maps and rich pictures etc. As each individual makes efforts to develop their own understanding about relevant problem spaces, several hypotheses may be created. Each individual may have not only several but also often incompatible narratives. The relationships between the different narratives can be elaborated upon through the creation of diversity networks drawing upon multi-valued logic etc. While any one human expert may create narratives which can be incompatible with each other they can still be individually justifiable. This is due to situated-ness, contextual dependencies, complexity and uncertainties in general. The narratives are used as a foundation for further elaboration, story-making and self-reflection.

'Inter-analysis' is focused on group sharing, communication and development of perspectives [1,9,10]. Each investigator has the opportunity to describe, explain and exchange each others descriptions and narratives. Each of the narratives created are inquired into and re-created. This can be done by using walk-throughs drawing upon the same tools and methods as the intra-analysis but now in collaboration with others. The inter-analysis is supporting each individual analyst in their creation of an understanding of other investigators narratives. The vehicles for this are language games and co-creation of new narratives. The analysis is supported through the co-creation of diversity networks as part of the systematic and systemic inquiry into each and every narrative presented.

'Value-analysis' is focused upon validation and prioritization from socio-cultural perspectives [1,9,10]. Each investigator attempts to develop and share their understandings of the specific conditions under which each unique narrative can be acknowledged as valid or acceptable. The rationalization and classification in the value analysis is supported through the same tools and methods as the other intra- and inter-analysis. This classification exercise is based on negotiation regarding what characterizes each narrative.

'Multi-valued logic' is used and may incorporate alternatives such as: compatible, incompatible, complementary or unidentified [24,25,26,27,28]. It can also include concerns related to values such as: correctness (true), incorrectness (false), uncertainty (information deficit) and structured uncertainty (information overload). The use of multi-valued and inconsistent logic supports analysts and investigators in their sense-making efforts and supports them in their creation of diversity networks etc. It also makes it possible to deal with a multitude of relationships

between different narratives describing complex problem spaces and still having some kind of overview.

'Spirality' is used to bring order into reflections over complex and uncertain problem spaces [29,30]. It is important to break away from a prescriptive process as described in the EDRM. It is necessary to treat the Information Management and the Identification stages as intertwined and recursive when approaching a complex and uncertain problem space as part of an ongoing inquiring process.

Conclusions and outlook

When it comes to digital forensic investigations, it appears that research and practice in the area of Informing Systems can be called upon to support the investigation process. This is due to the long history of Informing Systems study of structuring uncertainty. Furthermore, just like any application of systems, research in decision support systems for digital investigations is required to consider systems' challenges in order to avoid missed opportunities. As such, interdisciplinary research between systems and digital forensics would not only promote Informing Systems, but is of paramount importance to the viability of the electronic discovery processes, due to the explosion of the complexity of the problem spaces which underlie a digital crime scene.

References

1. Katos V. and Bednar P. M. (2008) A cyber-crime Investigation Framework. *Computer Standards & Interfaces*, Elsevier, 30(4): 223-228.
2. Unisys (2007). What is HOLMES 2? From: http://www.holmes2.com/holmes2/whatish2/ (September 2008).
3. Valier C. (1998). True Crime Stories: Scientific Methods of Criminal Investigations, Criminology and Historiography. *Brit. J. of Criminology*, 38(1), 88-105.
4. Broadhurst R. (2006). Developments in the Global Law Enforcement of Cyber-Crime. *Policing: An International Journal of Police Strategies and Management* 29(3), 408-433 Emerald.
5. Karyda M. and Mitrou L. (2007). Internet Forensics: Legal and Technical Issues. Proceedings of the 2nd International Annual Workshop on Digital Forensics and Incident Analysis. Preneel B., Kokolakis S. and Tryfonas T. (eds.), IEEE Computer Society Press.
6. Yar M. (2005). The Novelty of 'Cybercrime': An assessment in the Light of Routinge Activity Theory. *European Journal of Criminology* , 4(2), 407-427.
7. Mitropoulos S., Patsos D., Douligeris C. (2007). Incident Response Requirements for Distributed Security Informatino Management Systems. *Information Management and Computer Security,* 15(3), 226-240.
8. Jahankhani H. (2006). Waking Up to the Threat of Cyber Crime. *Information Security*, 2006.
9. Bednar P. M. (2000) A Contextual Integration of Individual and Organizational Learning Perspectives as Part of IS Analysis. *Informing Science.*, 3(3): 145-156.

10. Bednar P. M., Katos V. and Hennell C. (2008) Cyber-Crime Investigations: Complex Collaborative Decision Making. Proceedings of the *Third International Annual Workshop on Digital Forensics and Incident Analysis*. Tryfonas, T. (ed), IEEE Computer Society Press.
11. EDRM (2008) *EDRM: Electronic Discovery Reference Model*. From: http://edrm.net/ (June, 2008).
12. Benko C. and McFarlan W. (2003). *Connecting the Dots*. Harvard Business School Press, Boston: MA.
13. Peppard J. (2007). The conundrum of IT management. *EJIS* 16: 336-345.
14. Ciborra C. U. and Willcocks L. (2006). The mind or the heart? *J. of IT*. 21(3): 129-139.
15. Stacey R. and Griffin D. (2005). *A Complexity Perspective on Researching Organizations*. Sage.
16. Ciborra C. U. (2002). *The Labyrinths of Information*. Oxford University Press.
17. Ciborra C. U. (2004). Encountering information systems as a phenomenon. In C. Avgerou C. Ciborra and F. Land (eds.), *The Social Study of Information and Communication Technology*. Oxford University Press.
18. Heidegger M. (1962). *Being in Time*. Harper and Row.
19. Brown J. S. and Duguid P. (2002). *The Social Life of Information*. Harvard Business School Press.
20. McDermott R. (1999). Why information technology inspired but cannot deliver knowledge management. *California Management Review*. 41(4): 103-117.
21. NPIA, National Policing Improvement Agency. (2008). HOLMES 2 overview. From: http://www.npia.police.uk/en/5962.htm (September 2008).
22. Bednar, P., Katos, V., Hennell, C. 2008. Cyber-Crime Investigations: Complex Collaborative Decision Making. *Workshop on Digital Forensics and Incident Analysis*, IEEE CS Press, Malaga, Spain, 10 October:3-11.
23. Shafer, G. (1976) *A mathematical theory of evidence.* Princeton University Press, Princeton.
24. Bednar, P.M., Anderson, D. and Welch, C. (2005). 'Knowledge Creation and Sharing – Complex Methods of Inquiry and Inconsistent Theory'. *ECKM 2005*. Proceedings. Limerick, 8-9 September.
25. Bednar P., Welch C., and Katos V. (2006). 'Four valued logic: supporting complexity in knowledge sharing processes,' *ECKM 2006*. Proceedings, Budapest, Hungary, 4-5 Sept.
26. Bednar P., Welch C. and Katos V. (2008). Innovation management through the use of diversity networks. *Int. J. Knowledge and Learning*, (to appear. 2008)
27. Bednar P., Welch C. and Katos V. (2007). 'Dealing with Complexity in Knowledge Sharing Processes'. *ECKM 2007*, Proceedings. Barcelona, Spain, 6-7 September.
28. Bednar P., Katos V. and Welch C. (2007). 'Systems analysis: exploring the spectrum of diversity', *ECIS 2007*. Proceedings *Information Systems: Rigorous Relevance - Relevant Rigour*, St Gallen, Switzerland, 7-9 June 2007.
29. Bednar, P. and Welch, C. (2007). 'A Double Helix Metaphor for Use and Usefulness in Informing Systems'. *Informing Science*. 10, 273-295.
30. Nissen H-E. (2007). Using Double Helix Relationships to Understand and Change Informing Systems, Monograph of *Informing Science*, 10, 21-62.