Diversity Networks in Digital Investigations

P. Bednar[1] and V. Katos[2]

[1]University of Portsmouth, UK
[2]Democritus University of Thrace, Greece
e-mail: peter.bednar@port.ac.uk, vkatos@ee.duth.gr

Abstract

This paper is built upon the need that digital forensic investigators are required in many cases to investigate, understand and report on all kind of cyber-crime including novel security breaches which have not been performed in the past. When an investigator is faced with the challenge to explore a new threat, we argue that the inquiry dynamics do not differ from an organisational employee challenged to perform innovation. This is not just about challenging one's own assumptions; not just challenging the assumptions of one's colleagues but creating a dialogue among colleagues about the processes of questioning assumptions in order to uncover a richer appreciation of the uncertainties of the problem-space to be the subject of inquiry. This paper draws upon the approach of diversity networks which is used to support inquiry into complex problem spaces including the necessary requirement for innovation, and it is shown how this paradigm could be adopted by the forensic investigator to shed light on the uncertainty aspects of a cyber crime scene.

Keywords

e-discovery, digital investigation, structuring uncertainty, contextual analysis, complex cyber-crime investigation

1. Introduction

When it comes to digital investigations, the cyber crime scene can exhibit a high amount of complexity and uncertainty and these characteristics add to the challenges investigators face for collaborating at an international level, as introduced by Bednar *et al.* (2008a). The influence of the uncertainty element led to the need to revise the reductionist's view of gradually narrowing the scope of the investigation (ERDM, 2009) and as such the solution or approach of complexification was proposed (Bednar *et al.* 2008a). Naturally, uncertainty is found in an organisational context and a typical area is within the creativity and innovation process. There, complexification can support and highlight the diversity of opinions, promoting the genesis of unconventional and potentially groundbreaking ideas. Accepting that the cyber criminals may use ingenious and unconventional ways to construct attack vectors, it follows that first responders should not rely solely on conventional "by the book" practices, as in principle these will be outdated. It would therefore be necessary to establish means of supporting the e-discovery process by facilities that will give a competitive edge to them.

This paper explores the possibilities of incorporating the use of diversity networks which is applied in the creativity and innovation domain, in the area of digital investigations. In order to perform this task, we first reflect on the dynamics of innovation to examine the suitability, epistemological commonalities and coupling between innovation and electronic discovery. We then consider diversity networks in the context of investigations.

2. Dynamics of innovation

Innovation can be seen as a product of human reasoning. An important characteristic of human reasoning is that it allows contradictory evidence to be accepted as valid in problem resolution (Bednar *et al.* 2008b), but many problem solving supporting processes from the conventional Decision Support Systems to the E-Discovery models (EDRM) require early choices to exclude some alternatives from further consideration. Research focusing on knowledge and learning, and to human reasoning in an organisational context, includes work by Bateson (1972) on orders of learning and critical systemic inquiry. Argyris and Schon (1978) have contributed work on learning organisations seen from a practitioner perspective. Weick (1995) discusses organisational change and uncertainty; and Lytras and Sicilia (2005) give an overview of knowledge and learning, highlighting the contextual complexities found in individual and team dynamics. Organisations have no distinct embodiment beyond that of interactions among individuals within social, communicational networks. 'Knowing' in an organisational context is formed through continual construction and reconstruction of meanings by individuals, as they encounter new experiences and synthesise resultant data with existing 'knowledge' acquired from past experiences (Langefors, 1966). Forensic investigators need space to explore their own deeply embedded and inaccessible understandings, if they are to become able to express their 'knowing' in such a process of e-discovery (Table 1).

- Rush to achieve consensus
- Focus on 'best practice'
- Convergent thinking
- *There is need for a discourse of diversity*

Table 1: Complex Problem Spaces: Problems for Analysis

Innovation needs support from people throughout an organisation. Many approaches to 'knowledge management' have been suggested, to encourage creativity and sharing. Knowledge resides in human beings and epistemic uncertainty is fundamental to their experience. To seek a solution, we must first explore a problem-space, knowing that many valid alternatives may exist. Such activities have been described as a negotiation of differing perspectives (Weltanshauungen) held by individuals (Checkland and Holwell, 1998). Ciborra discusses this approach to human inquiry using concepts such as bricolage, tinkering and improvisation. He suggests that, when confronted with a problem space they experience as complex, people turn first to existing knowledge, and familiar competences (that which is recognised), then gradually move outwards from this base towards the unfamiliar

(that which is cognised) (Ciborra, 1992). As Habermas (1989) points out in his Theory of Communicative Action, any negotiation requires a discourse supporting co-creation of language upon which a communicative process may be built. The authors believe that use of four-valued logic in the creation of diversity networks, provides a springboard for such a language to be developed (Table 2).

• Focus on Narrative • Information poorness • Dialogue • Self-informing System • Clarification and Complexification • Information richness

Table 2: Structuring Uncertainty

In a situation where a set of malicious cyber activities or events are assumed to have taken place, the investigator would need to face the problem space equipped with their knowledge and due to the inherent uncertainty, they should accept that many alternatives may exist and some of them can be contradictory.

The typical inquiry and cyber-crime investigation is full of complexities and uncertainty; not only questions such as "what is the problem"; or "is this a relevant problem to investigate"; and "what kind of problem it"; but also "how do we assess what is relevant problem space to be concerned about" etc. It is often by definition a multi-perspective problem which will be appreciated and judged dependent on socio-cultural and national boundaries. These issues are so much more relevant in cyber-crime as it often has a scope beyond any local or national boundaries. The process of elimination of irrelevant activities, reasoning, and understanding of the state of the crime. Or how a technical system was breached, is not in principle different from a company employee being asked to innovate in a financially uncertain global and cultural environment, as both individuals would need to move towards the unfamiliar. An important difference could be the fact that in the case of any one isolated security event, there would be possibly only one correct alternative (that is one actual threat vector at a given time), whereas in the case of defining relevant problem-spaces to investigate and innovation in general there could be many "correct" alternatives. In both cases though, correctness is established *a posteriori,* after ratifying the respective verdicts. During the investigatory process itself, correctness as a "fact" is evasive (and should be).

3. Diversity networks

Cyber crime investigations are expected to involve a number of individuals, with different competences and roles (Bednar *et al.* 2008a). Therefore, during the analysis it is expected that each forensic investigator would welcome ideas from their peers and colleagues. These ideas could be accepted and incorporated with their own views, irrespective of the fact that they can be conflicting, since this is allowed in

human reasoning, as mentioned earlier. A process which can result to the creation of diversity networks is explained below and is based on the SST framework (Table 3).

• Intra Analysis: Expanding descriptions of a problem-space Creating possible resolutions • Inter Analysis: Structuring uncertainty into ambiguity through communication with others Limiting the number of alternatives to be discussed (Puts narratives into context of problem-space) • Value Analysis: Creating a frame of reference with which to assess alternatives (Puts narratives into context of environment) • Communication in inter analysis and reflection in value analysis together support creation of a learning spiral

Table 3: Structuring Uncertainty into Ambiguity

The individual's reflection and creation of their own ideas is referred to as intra-analysis. 'Intra-analysis' (Bednar, 2000, Katos and Bednar, 2008) is focused on exploration and creation of individual investigators perspectives. 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.

The group sharing of ideas and theories is referred to as inter-analysis. 'Inter-analysis' (Bednar, 2000, Katos and Bednar, 2008) is focused on group sharing, communication and development of perspectives. 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-troughs 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 the 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.

Clearly at some stage there needs to be a prioritisation of ideas and views. 'Value-analysis' (Bednar, 2000, Katos and Bednar, 2008) is focused upon validation and prioritization from socio-cultural perspectives. 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 (Table 4).

• Different categories of (un-)certainty • Type ('level) of commitment to assertion • Type ('level') of assertion • Multi-valued logic (e.g. four-valued)

Table 4: Paraconsistent Logic

We advocate that the language which is suitable to capture and express the above processes should at least allow four valued logic reasoning. 'Multi-valued logic' (Bednar *et al.* 2005;2006a;2007a;2007b;2008) is used and may incorporate alternatives such as: compatible, incompatible, complementary or unidentified. It can also include concerns related to values such as: correctness (true), incorrectness (false), uncertainty (information deficit) and structured uncertainty (information overload).

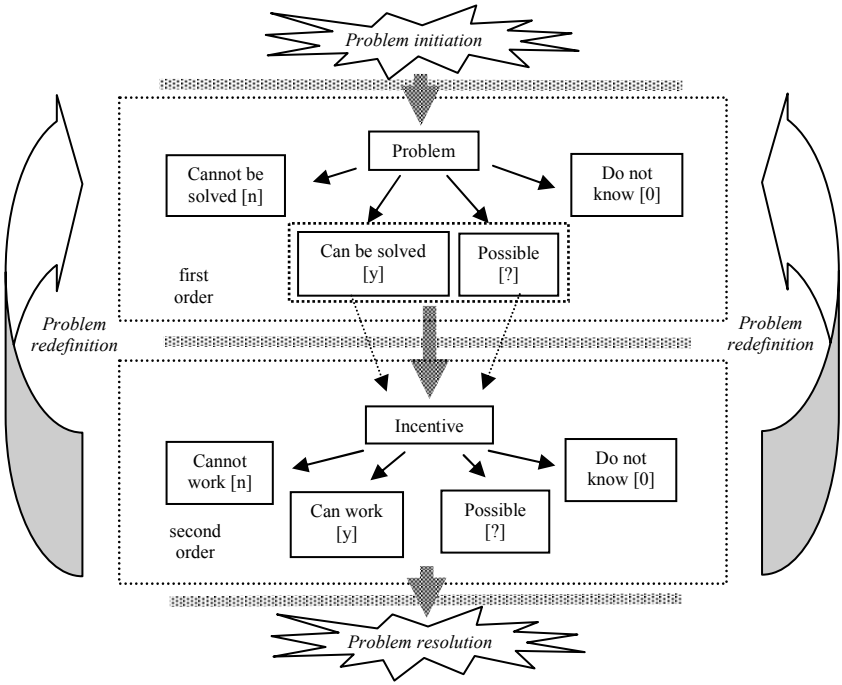

Figure 1. Process overview

The use of multi-valued and inconsistent logic does support 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 (figure 1).

Assertions of negative belief *I do not believe that the suspect hard drive contains admissible evidence*	Assertions of positive belief *I do believe that the suspect hard drive contains admissible evidence but I am not sure how it can be recovered*
Assertions of positive belief *I do believe that the suspect hard drive contains admissible evidence which can be recovered*	Assertions of no belief *I can offer no opinion whether the suspect hard drive contains admissible evidence*

Table 5. A logic model allowing for variants of individual judgement

Table 5 is an example of how four-valued logic can be used in supporting a dialogue in different aspects of the e-discovery process, in order to develop diversity networks as a base upon which better informed decision-making can be founded. When a collective problem space is to be explored, it is important to examine the element of choice available to participants (Figure 2.).

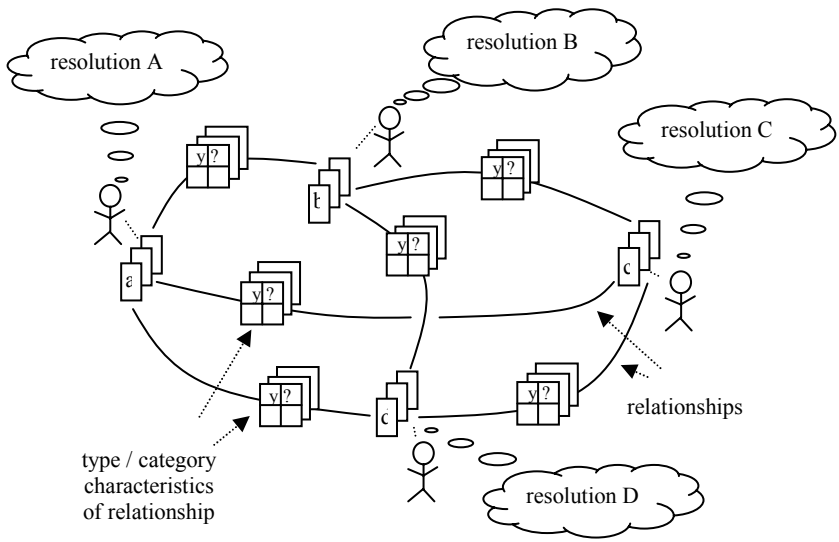

Figure 2. Diversity network (adapted from Bednar *et al.* 2008)

A phenomenon must be recognised, that decision makers can bear in mind that they are asserting beliefs about truths, rather than truths themselves, i.e., exercising

judgement. When asked for an opinion, an individual may often give the answer 'it depends'. If we explore this response further, we can discern four alternative variants. The main difference between them lies in the character and degree of certainty that each represents. (We also recognise that logic implies (1) that choices need to be made for each separate alternative, and (2) that any assertions made are not assumed to be valid under all conditions, or out of a specific context).

Each assertion requires a decision. Each decision is chosen by means of an attempt to assess risk of being 'wrong', taking into account fit between assumptions of context and possibility of generalisation.

Through the stages of intra-analysis, inter-analysis and value analysis, opinions and theories with respect to the attack vector will be generated, shared and prioritised. It should be noted that the table 5 would merely represent a snapshot of a situation.

An investigator could initially consider that a hard disk may not contain admissible evidence (assertion of negative belief). However during the information osmosis between the other participants or even their own progressing investigation, they may change their opinion and agree that the disk may indeed contain admissible evidence (assertion of positive belief).

Through this process of debate, in which assertions are signified and documented, a diversity network will eventually emerge, as represented in Figure 2. Each investigator reflects upon the relationships between their own understanding of the attack and the alternative attacks described by other individuals. The use of four-valued logic would help them signify the characteristics of these relationships. By adopting this approach, we believe that they would be in a better position to determine that actual attack and modus operandi of the attacker.

4. Conclusions

The high amounts of complexity and uncertainty contained in cyber crime scenes mandate the forensic investigator to somehow structure uncertainty in order to organise the problem space and cope with the various alternatives (solutions) to the problem (attack). An attack in many cases may be a new one, unknown to the investigator or their team, who are challenged to discover, and sometimes may be equipped with incomplete information. Pushing the boundaries of their understanding of the problem space shares commonalities with innovation exercises and requires a number of considerations and practices, some of which were presented in this paper. As logging and in general capturing and documenting information is of paramount importance in forensics, we argue that the investigators must adopt approaches that will support rather obstruct the communication and sharing of ideas. This would at the very least allow contradictory evidence to be captured and processed in a way that it will not cancel out any views and statements, but instead would support the creation of diversity networks through complexification. It is expected that in the longer term this practice would create a base for more informed decisions (Table 6).

• Structuring uncertainty • Problem exploration • Expression • Reflection • Creation • Contradictory evidence • Complexification • Creating a base for more informed decisions

Table 6. Concluding points

Ongoing research focuses on incorporating the described framework in digital forensics analysis systems, in order to further the empirical aspects of this research and examine the emerging hypotheses. Anyone who wishes to expand the practice of investigation will have to take into consideration complexity and uncertainty in context. This requires concerns to be highlighted which relate to the quality of such an investigation. This means that reflection over the process of inquiry is a necessity and philosophical doubt must be part of any development of investigation practice. Indeed philosophical doubt must be part of investigation practice itself.

5. References

Argyris, C. and Schon, D. (1978) Organisational Learning, Reading, MA: Addison Wesley.

Bateson, G. (1972) Steps to an Ecology of Mind, Chicago: University of Chicago Press.

Bednar P. M. (2000) A Contextual Integration of Individual and Organizational Learning Perspectives as Part of IS Analysis. Informing Science, 3(3): 145-156.

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.

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.

Bednar P., Welch C. and Katos V. (2007a). 'Dealing with Complexity in Knowledge Sharing Processes'. ECKM 2007, Proceedings. Barcelona, Spain, 6-7 September.

Bednar P., Katos V. and Welch C. (2007b). 'Systems analysis: exploring the spectrum of diversity', ECIS 2007. Proceedings Information Systems: Rigorous Relevance - Relevant Rigour, St Gallen, Switzerland, 7-9 June 2007.

Bednar P. M., Katos V. and Hennell C. (2008a) 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

Bednar P., Welch C. and Katos V. (2008b). Innovation management through the use of diversity networks. Int. J. Knowledge and Learning.

Checkland, P. and Holwell, S. (1998) Information, Systems and Information Systems: Making Sense of the Field, Chichester: Wiley.

Ciborra, C.U. (1992) 'From thinking to tinkering: the grassroots of strategic information systems',Information Society, Vol. 8, pp.297–309.

Electronic Discovery Reference Model (2009), http://edrm.net

Habermas, J. (1989) The Theory of Communicative Competence: The Critique of Functionalist Reason, Vol. 2, Cambridge: Polity Press.

Langefors, B. (1966) Theoretical Analysis of Information Systems, Studentlitterature.

Lytras, M.D. and Sicilia, M.A. (2005) 'The knowledge society: a manifesto for knowledge and learning', Int. J. Knowledge and Learning, Vol. 1, Nos. 1–2, pp.1–11.

Katos V. and Bednar P. M. (2008) A cyber-crime Investigation Framework. Computer Standards & Interfaces, Elsevier, 30(4), pp. 223-228

Weick, K. (1995) Sense-making in Organizations, London: Sage.