Counterinsurgency Through Civil Infrastructure Networks

David Walker, Simon Reay Atkinson
Complex Civil Systems Research Group
Faculty of Engineering and IT
University of Sydney, NSW 2006, Australia
[david.walker, simon.reayatkinson]@sydney.edu.au

Liaquat Hossain
Department of Informatics
Lund University, Sweden
Liaquat.hossain@ics.lu.se

***Abstract*—We investigate opportunities and risks to counter-insurgency (sometimes referred to as COIN) that are inherent in the civil networks surrounding infrastructure projects. It is argued here that a) successful counter-insurgency largely comprises the 'engineering' of robust and trusted civil networks that are capable of re-channelling insurgent designs; and b) introduction of externalized-exclusive control networks poses a significant risk to such network development. In this conceptual paper, we propose a number of network models, each hypothesizing a risk and / or opportunity. These models will be tested and refined using a case study methodology that draws on documentary evidence and interviews with subject matter experts. We propose two fundamental relationships: Coordination by rule and control (CRC), and; Collaboration by social influence (CSI). CRC is based on mechanical (rule and time based) structures, while CSI is based on organic (informal, trusted and shared aware) social networks. We posit that COIN is primarily a CSI interaction / exchange that can be supported (but also obstructed) by CRC. We therefore propose that the design of successful COIN operations must adhere to the hybrid notion providing an interface between CRC and CSI.**

Keywords - civil networks; infrastructure; insurgency; coordination; collaboration

I. BACKGROUND AND CONTEXT

A. Introduction

Organisational communication literature maintains that hierarchical structures, e.g. organograms, provide a superficial representation of how work actually gets done [1]. Here, we posit (after Hossain and Wigand [2]) that organisations need to be seen as dynamic (elastic and plastic) social-influence networks. In these collaborative [3] networks of complex operations, requiring tacit knowledge exchange [4], which is achieved through social (and in this regard civil) interactions beneath and sometimes masked by the formal hierarchical organisational chart. Organisational co-adaptive [5] viability in maintaining operational effectiveness and efficiency may therefore be largely dependent on how we synergistically socialise and capitalise 'our' formal (hierarchical) and informal (social) networks to achieve shared common goals. In this paper, we set the context as relating to counterinsurgency which we then explore through the mediation of hierarchical-formal and informal-social networks as applied to civil infrastructure projects. In this paper we also ask whether the success and/or failure related to COIN is attributed to the conceptual misunderstandings of how we provide synergy between hierarchical formal-control-rule (CRC) and informal-collaborative-social-influence (CSI) networks. In this regard, we distinguish between Command, as in Leadership and Control, as in Management and consider, after Reay-Atkinson and Moffat, that: Control is a function of rules, fidelity, time and bandwidth whereas command is a function of trusts, shared awareness, influence and agility [6].

Securitization emerged along with Contractorization from the 'politics' of Privatization put in play in many democracies from the 1980s onward. Whereas contractorization (of security) was manifested through Private Finance Initiatives (PFIs) and Private Security / Military Companies (PS/MCs); privatization was more often introduced through Public-Private Partnerships (PPPs), for example the privatization of British Defence Research into Dstl and QinetiQ. Building on Grotius [7], we posit three interconnected and interactive conflict phases: jus bello (justice to war); jus bellum (just war) and jus post bellum (justice after war). In our understanding, the trusts established before during and after conflict underpin the public assurances, trusts, safety and security subsequently established. No one phase trumps the other. This has specific implications for how counter-insurgencies are engaged, or not. The Civil Infrastructure Networks we identify in this paper are not limited in scale and connect the social (people) with civil programmes; including IT, transport, Cyber-, water and energy networks. Post Privatized forces tended to optimise out these very skills / trusts through PPPs, PFIs and PS/MCs. This had a number of effects. The first was to create warrior cast structures with front line troops at the top of the pyramid and engineering / logistics even health care at the bottom. Secondly, it created incoherence in command / collaboration between divided force structures for which many of the 'enablers' were now under contract, e.g. tank transportation. Thirdly it created a reliance of the fighting force on structures that a) could not necessarily be put 'under disciplined control' and / or b) expected to be collaboratively deployed into hazardous areas. Fourthly, it created private and sometimes competing armies – very often employed by other government departments (OGDs), such as the UK Foreign and Commonwealth Office. Fifthly, the opportunity to contract one's own security / reconstruction programmes removed the need for healthy local collaboration and mutuality between government departments, e.g. between the state department and the Department of Defence.

This paper is organised as follows: first, we discuss COIN and its context; secondly, we discuss the application

Copyright (c) IARIA, 2012. ISBN: 978-1-61208-228-8

of social networks in modelling risks and opportunities for COIN; thirdly, we discuss the social influence model within the context of COIN and provide conclusions, implications and future directions.

B. Counterinsurgency

US Military doctrine considers an insurgency to be: 'an organized, protracted politico-military struggle designed to weaken the control and legitimacy of an established government, occupying power, or other political authority while increasing insurgent control' [8]. Counterinsurgency is every effort to stop an insurgency, once started. The primary objective of COIN is to maximise the support of the civilian population for the legally constituted government [8-13]. Insurgents depend on the civilian population for sustenance, shelter, concealment and recruitment. Insurgents (almost always clandestine in nature) employ a number of strategies to shift the objective demographic in their favour, including political and judicial subversion, terrorism, guerrilla warfare, organised crime / the Black economy (extortion, corruption, smuggling etc), propaganda, and public service provision (including governance, security and judiciary) [8, 13]. Technological advances and demographic trends over the last several decades have significantly changed the nature of conflict. In a contest between a small-scale, agile, poorly funded but technically literate and socially aware clandestine movement and a large technologically advanced and hierarchical rule-based military, these trends have tended to support the former. They include urbanisation, globalisation, proliferation of NGOs and other civilian organisations, ubiquity of news media, revolutionary advances in information technology, social media, increased lethality of highly mobile weaponry, and global [religiously based] insurgency [14].

Contemporary insurgencies (considered by this paper) may lack the ideological appeal of classical insurgencies against 'local' colonial forces and therefore rely on causing existential intervention by government / coalition forces to generate localised conflict – essentially localising the conflict for 'home' advantage. Kilcullen [10] develops the idea of an 'accidental guerrilla syndrome'. He theorizes that 'the accidental guerrilla emerges from a cyclical process that takes place in four stages: infection, contagion, intervention, and rejection.' Importantly, this insurgent strategy assumes counterinsurgents will generate interstitial conflict when they enter local networks.

Effective COIN requires coherent and collective (unifying) input from a multiple stakeholders including military, other government agencies / departments, non-government organisations, private contractors, and most importantly any functioning civil networks remaining embedded in local populations. Yet usually there is no remaining control structure and legal authority by which networks can be coordinated – even and although the local population continue to feed and fend for themselves. *The inescapable corollary is that coordination of counterinsurgent organisations and local civil networks needs to be achieved by something other than rule and control. We call this collaboration by social influence (CSI).* This paper addresses two questions: 1) How can the efforts of such a diverse array of actors be influenced and / or coordinated? 2) What are the implications for the internal networks of counterinsurgent organisations? To address these questions, a number of network models are developed, each representing a key opportunity or risk to COIN.

Civil infrastructure projects have a number of crucial characteristics that make them ideal for COIN and ideal for research into the dynamics of civil networks. Firstly, they provide justification for large scale information transfer to and from the population. Secondly, project stakeholders and their networks cover almost every facet of society and outside influence; including military forces, end-users, contractors, suppliers, NGOs, local government, tribal and religious leaders, political opposition, financial service providers, donors, and land owners. Thirdly, projects have clear boundaries and objectives. Fourthly, they provide economic stimulus for development and maintenance; and fifthly, the tangible benefits of the infrastructure itself remains. Most importantly from a research perspective, infrastructure projects: a) give rise to a large quantity of reliable network data; and b) provide identifiable boundaries.

II. Modelling Opportunity and Risks to Counterinsurgency

A. Social Networks and Their Impact on Risk and Opportunity

Opportunities for CSI may be considered a type of social capital (SC). Coleman defines SC as 'a variety of different entities, with two elements in common: they all consist of some aspect of social structures, and they facilitate certain actions of actors' [15]. Coleman provides a few clarifications that are particularly important to the present study: 1) SC can constrain as well as enable action; 2) SC that is beneficial to one activity may be detrimental to another; 3) SC, like all capital, need not be utilised; and 4) SC created for one purpose can be used for another. With regard to stabilising reform in COIN, it may be hypothesised that the 'low hanging fruit' is made up of two basic types of existing social capital: 1) that which could have a stabilising effect but is currently not being utilised or is being utilised for some other purpose; and 2) pernicious structures that constitute relatively trivial social capital and will therefore not be vigorously defended. This 'low hanging fruit' represents the opportunities for reform that counterinsurgents find so difficult to identify. Social network analysis is one way of modelling social capital.

Social network analysis (SNA) is 'a distinct research perspective', which includes 'theories, models and applications that are expressed in terms of relational concepts and processes' [16]. A network is made up of actors (individuals, organisations, or some other social unit) and relational ties between them. SNA attempts to model and predict patterns of relational ties (network structures), and to understand the causes and effects of these patterns. Laumann et al [17] observe two ontological perspectives of networks: realist and nominalist. From a realist perspective, a 'network is treated as a social fact only in that it is consciously experienced as such by the actors composing it'. With a nominalist approach

Copyright (c) IARIA, 2012. ISBN: 978-1-61208-228-8

the analyst 'imposes a conceptual framework constructed to serve his or her own analytic purposes' [17]. This paper adopts the nominalist approach, which provides greater flexibility in network definition and enables the analysis of disconnected networks.

1) Network Dynamics. Balance Theory developed by Austrian psychologist Fritz Heider specifies that a triad (group of three actors) is balanced if all ties are positive or if two are negative and one is positive [18]. In SNA, the well observed tendency for triads to become 'balanced' is called transitivity [16]. In the present study we are particularly concerned with the effect of new actors entering a social network. If actors A and B are friends and new actor C becomes an enemy of A, by the theory of transitivity it can be expected that B and C will become enemies. This is a risk for C. Less obviously there is also risk to C in creating positive (friendship) ties. If A and B are enemies and new actor C becomes friends with A, it can be expected that B and C will become enemies. Homophily, which is the tendency of people to make connections with others that are similar to themselves [19, 20], may amplify or dampen the effects of transitivity.

The dynamics of conflict pacification and escalation within networks are crucial. Humans tend towards a 'tit-for-tat' strategy in response to acts they consider unreasonable [21]. In relation to the actions of others, humans have a tendency to perceive their own contributions more significant, their own gains more deserved, and their own losses more unjust. The logical (and observable) outcome of these human conditions is a positive feedback cycle within which animosity and conflict (once initiated) escalates between two actors. Importantly, an actor responds to his/her *perceptions* of another actor's behaviour and intent, so the positive feedback loop can begin without any *actual* acts (or even intent) of aggression. Transitivity also dictates that conflict relationships may cause other actors in the network to become conflicted.

Trust, like conflict, may propagate or collapse exponentially through a network. Dasgupta [22] concludes that "trust is a public good, a social lubricant which makes possible production and exchange...[It] is based on reputation...acquired through behaviour over time in well-understood circumstances." Trust is dependent on social networks, and it "is this interconnectedness which makes trust such a fragile commodity." Individuals place trust according to their (often intuitive) calculations of risk and return. A significant element of that risk exists in relation to the reliability of their information on a potential exchange partner. Therefore, significant gains in social capital are made by the provision of reliable information to all parties. This may lower the cost of trusting below some point of criticality and so generate a chain reaction (or cascade) of trusting relationships. Such an effect is a worthy objective of temporarily intervening actors.

Knowing how people 'connect' makes collaboration work better; see Mintzberg et al [3]. They suggest that collaboration may ultimately depend on trust. Collaboration depends on the ability to trust each other, and to appreciate one another's expertise. Perhaps, surprisingly, they argue, the best collaboration may be the least realised as collaborative, giving the example of interdepartmental collaboration for new product development. In the best of such collaborations of joint learning whilst designing, people focus intently on 'shaping' but may not even realise they are collaborating, so that shifting their focus to formal techniques of collaboration may, in fact, reduce their capacity and propensity to collaborate. Building on this concept of trust, Marsh [23] suggested the following definition of trust:

> '…trust, (or symmetrically, distrust) is a particular level of the "subjective probability" with which an "agent" will perform a "particular action", both before he can monitor such action (or independently of his capacity to monitor it) and in a "context" in which it "affects" his own action.'

2) Information and Control. Building on the theory of transitivity, Granovetter [24] proposed that most novel information is attained through weak ties. The Strength of Weak Ties (SWT) theory is based on the relatively simple logic that a person's strong ties most likely lead to people that are also strongly tied (due to transitivity). This means that information coming to an individual through one strong tie is likely to be the same as information coming through another strong tie. Weak ties on the other hand are more likely to lead to people that would otherwise be only distantly connected or not connected at all. In Granovetter's seminal study he provides empirical evidence for this theory by showing that people are more likely to find a job through a weak tie than a strong one.

Ronald Burt's structural holes (SH) theory also seeks to explain how network structure contributes to an individual's access to novel information. Structural holes are the gaps in a social network between two actors that are not connected. If another actor manoeuvres into that gap by forming a relationship with each of those actors, he or she is then in a position to control the flow of information and resources between them [25]. One's network is *effective* to the extent that it reaches many other actors (through primary contacts and their close ties) and *efficient* to the extent that the ratio of total contacts reached to total primary contacts is large. The *effective size* of one's network is deemed to be the total number of non-redundant contacts. Non-redundant contacts are those between which there is a structural hole and therefore those that provide access to novel information.

Burt considers the SH explanation superior to that of SWT because "the causal agent in the phenomena is not the weakness of a tie but the structural hole it spans…[and] the weak tie argument obscures the control benefits of structural holes" [25]. The control benefits of structural holes are indeed very important to SH theory and very important to this study. If actor A spans a hole between actors B and C, actor A has control benefits to the extent that B and C make mutually exclusive demands (or requests) on A. The traditional auction is a simple case in which an offer from B is used to raise the offer from C. For most negotiations, however, it is

Copyright (c) IARIA, 2012. ISBN: 978-1-61208-228-8

secondary holes that infer most control. Secondary holes exist between an actor's contacts and others that could replace that contact. Where one actor could substitute for another, they are considered to be *structurally equivalent*. The simplest example is a market. A buyer has power to drive the price down to the extent that there are multiple sellers competing for that sale. The competing sellers are structurally equivalent. Structurally equivalent actors can avoid being played against one another by coordinating their actions. This type of coordination takes many forms within the economy, e.g. labour unions and price fixing cartels.

Network exchange theory provides an alternative way to examine power relations and brings to light at least one counterintuitive insight that is not easily identified through SH theory.

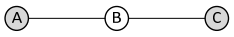

Figure 1. Powerful Central Actor

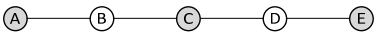

Figure 2. Weak Central Actor

While "centrality measures have typically been used as indicators of power, influence, popularity and prestige" [26, 27], Markovsky et al [28] demonstrate that under certain conditions central actors may be considerably weaker than those that are not particularly central. In Figure 1 actor B is the most central and the most powerful in negotiations. In Figure 2, however, the most central actor (C) is less powerful than B and D. This is because B and D can extract very high returns from A and E respectively and so reduce their dependence on C, possibly cutting C out altogether: social power can thereby depend on connections to others in weaker positions.

Network models of power are highly relevant to our understanding of COIN. As well as competition with the insurgency, counterinsurgents can find themselves in competition with one another (they are structurally equivalent and not coordinated). 'Competition' may also come from other global powers posturing for influence in a region and from NGOs reluctant to cooperate with any central or Government or International authority, or even from local coalition allies. In Afghanistan, there were examples of some Coalition partners refusing / being unable within their [control] rules-of-engagement to collaborate with local partners due to their previous criminal / conflict linkages and records. In some cases, local partners turned to another Coalition ally who, while maintaining their political and bureaucratic influence, also inadvertently preserved the power base and rationale for the insurgency in the first instance.

B. *Network Models of Social Influence*

Building on the context and theory, in this section we present a number of network models that hypothesise on the dynamics of social influence during COIN. Through these models we identify risks and opportunities inherent in the structures of social networks and the actions of key players. In accordance with the nominalist approach, networks may be defined on any conceivable tie. Conceiving possible networks is a crucial task of domain experts. Productive use of these models requires close cooperation between domain experts (practitioners) and theoretical experts (academics). The inevitable shortcomings of each type of expert acting without the other has been recognised as an important barrier to research [29].

1) Unintended Exclusion (the danger of strong ties). Figure 3 presents network dynamics in response to counterinsurgents entering a network and forming a strong tie with one actor while inadvertently (or deliberately) excluding structurally equivalent others.

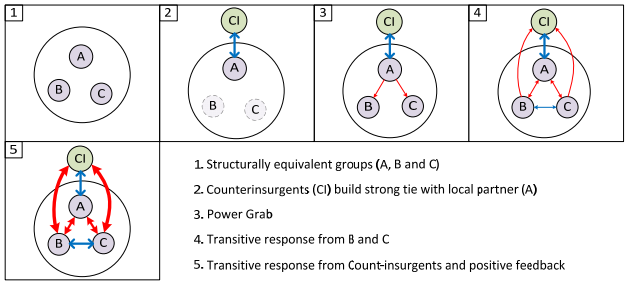

Figure 3. Unintended Exclusion

From a 'realist' perspective Figure 3 may show three tribes or three warlords (A, B and C). However this is only one of many possibilities, even if a valid interpretation. From a nominalist perspective it is posited that such a dynamic might be observed within any network built on inferred power relations.

Structural equivalence provides the capacity and intent to perform some function and exercise some control. Networks that make up structurally equivalent actors vary depending on the type of tie under consideration. Networks may be formed by ties that, for example, determine land tenure, opium production, trucking (or other goods and services), spiritual guidance, political leadership, judicial authority and policing. Each type of tie produces a different network signature which may be observed. We suggest that insurgents may be 'spread' throughout local networks. Insurgents seek to infiltrate and suborn ('infect') local networks by breaking down their immune systems and occupying traditional roles, marrying into tribes, creating business partnerships and converting susceptible minds to their cause.

From this model it is hypothesised that: 1) strong ties increase the likelihood of negative response from unknown others; 2) Weaker ties with all actors may result in more positive (or neutral) ties (collaboration) with unknown others; but 3) Maintaining weaker ties requires counterinsurgents to look beyond the rather more obvious / recognisable (like) and accessible / attractive strong ties generally available.

2) Self Fulfilling Prophecy. The network model presented in Figure 4 represents the inadvertent escalation

of conflict that may begin with nothing more than a perceived display of hostility. Instigating this dynamic through deception and intimidation is a key strategy of insurgents. The presence of counterinsurgents provides the insurgency with 'initiation' opportunities. Through their detailed understanding of collaborative-co-adaptive and cooperative-competitive relationships, insurgents can shape the ecology to their advantage by convincing otherwise peaceable citizens that their way of life is under attack. The easy thing for counterinsurgents to do is to target an insurgent. Yet often an insurgent may also be part of other Black Economy type activities essential for supporting the well-being of the local population. In this instance the counterinsurgents will frequently be better off observing and not contesting these agents; while working to convince networks to reject more malign or un-reconcilable actors.

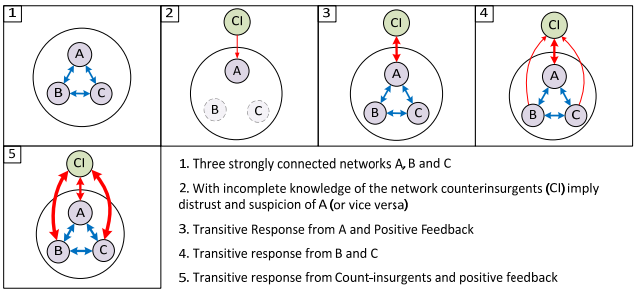

Figure 4. Self Fulfilling Prophecy

3) Coercion. A key task of COIN is to identify local civil system-networks that are capable of resisting / being immunised against coercion. In this model (Figure 5), coercion is perceived as a star network with a coordinated coercer at the centre connected to a number of other networks that might (if sufficiently collaborative) be able to reject (or rechannel the designs of) the coercer.

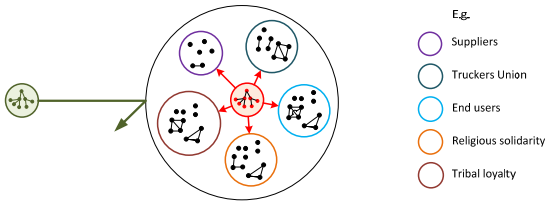

Figure 5. Coercion

Each of the networks is defined on a different tie, so a single actor may exist in more than one network. We assume that within any given population there exists a number of networks through which power and influence is distributed. Networks will reject malign actors to the extent that they are capable, motivated and immunised to do so. The capability of each network to reject (or rechanneled the designs of) malign actors is a function of the network's coordination, social power (implicit in the type of tie that forms the network), and reach (collaboration). We assume motivation is based on cost / benefit appreciation with some appropriate weighting for risk aversion / acceptance.

The tacit knowledge necessary to build this model is a *critical information requirement* of COIN. Importantly, this is information about licit networks, not clandestine insurgent networks. We assume coercion exists. The information we seek to attain and distribute is that which will influence existing networks to collaboratively coordinate and exclude malign elements. Military organisations (particularly intelligence assets) have deeply entrenched tendencies towards information control; often precluding the kind of knowledge exchange and shared awareness required to build such a model. See Flynn et al [30] for a cathartic account of military intelligence failures.

The potential of a given network to improve its capability, capacity and intent is also critical. Some networks are fixed, while others may have potential to dynamically change size, power-relationships and purpose. An example may be the National Solidarity Programme (NSP) in Afghanistan. It was designed to decentralise the control of civil infrastructure projects and disaggregate legitimacy and control to the local level. In the absence of trusted [nationwide] judicial and political systems, it became a common source of impartial judgment so a) preventing and b) resolving local disputes through collaborative social influence [31].

4) Ideal Instance of CSI. Figure 6 represents a network dynamic that is a key objective of COIN. Based on theory and the risk profiles previously identified, we posit that opportunity for these network dynamics may emerge from a number of conditions. Firstly, counterinsurgents are sufficiently coordinated to avoid being played against one another - so enabling them to make explicit and credible promises of withdrawal. Secondly, counterinsurgents avoid empowering any single local network that is structurally equivalent to multiple others. Thirdly, local civil networks are identified which: a) have a significant collaborative interest in sustained support from counterinsurgents, and b) are capable of rejecting / being immunised against (or rechanneling the designs of) malign actors. Fourthly, hostile action or intent (and the impression thereof) towards any individual or group is minimised through shared awareness and the threat being seen as an attack on the whole.

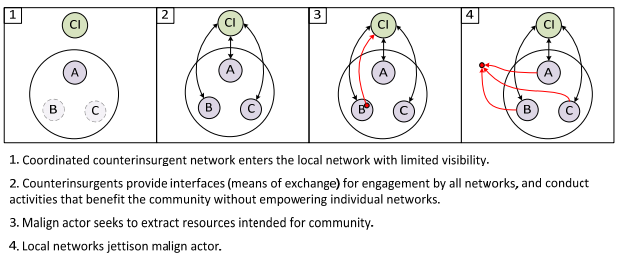

Figure 6. Local Networks Rejecting Malign Actor

Infrastructure projects provide the ideal context to study and exercise this process. Black Market / criminal elements

Copyright (c) IARIA, 2012. ISBN: 978-1-61208-228-8

will seek to extract resources as long as they can portray themselves as enemies of counterinsurgents as opposed to the public good. Such a 'posture' requires a very high standard of project management (to identify, prevent and prosecute hostile activity) while collaborating effectively with the civil networks within which some black marketeers / criminals will inevitably seek to hide. This scenario is an example of CRC (to produce evidence with high legitimacy) supporting CSI (to influence perceptions and motivate actions by local networks).

III. CONCLUSION AND FUTURE RESEARCH DIRECTION

Drawing on theories of social capital, strength of weak ties, structural holes, network balance, and network exchange we have developed a set of models of network dynamics in COIN. The hypotheses of this paper are implicit in these models and the deductions drawn from them. We recognise the underlying moral requirements underpinning the effective deployment and use of Armed Forces in a counter-insurgency. And this moral / ethical underpinning – identified in just war theory – underpins not only the success of the operations but also the ability of our Armed Forces and the local population to recover from instability. In this respect we can see the significant reduction in the extent and subsequent impact of PTSD on deployed forces. We see civil infrastructure networks – at all scales from the Cyber- to 'bridge building' – as underpinning a successful counterinsurgency and re-connecting shattered communities after conflict; an example being the Mostar Bridge.

From this conceptual starting point, the study will progress through two phases. An interview protocol will be developed and an initial set of interviews with subject matter experts will be used to test that protocol and further refine the theoretical models. The second phase will be a rigorous testing of these models through case studies selected for theoretical replication; utilising the case study framework developed by Yin [32]. This qualitative approach is considered most appropriate because it allows us to "retain the holistic and meaningful characteristics of real-life", which is important when investigating complex social phenomena [32].

REFERENCES

[1] R. Stacey, "Creative Organizations: The Relevance of Chaos and Psychodynamic Systems," Social creativity, vol. 2, 1999, pp. 61.

[2] L. Hossain and R. T. Wigand, "Ict Enabled Virtual Collaboration through Trust," Journal of Computer-Mediated Communication, vol. 10(1), 2004.

[3] H. Mintzberg, J. Jorgensen, D. Dougherty, and F. Westley, "Some Surprising Things About Collaboration-Knowing How People Connect Makes It Work Better," Organizational Dynamics, vol. 25(1), 1996, pp. 60-71.

[4] S. Reay-Atkinson, S. Lesher, and D. Shoupe, Information Capture and Knowledge Exchange: The Gathering, Testing and Assessment of Information and Knowledge through Exploration and Exploitation, 2009, DTIC Document.

[5] S. Reay-Atkinson, A. Goodger, N. Caldwell, and L. Hossain, "How Lean the Machine: How Agile the Mind?," The Learning Organization, vol. 19(3), 2012, pp. 183 - 206.

[6] S. Reay Atkinson and J. Moffat, "The Agile Organization," Publication of the US Department of Defense Command and Control Research Program (CCRP), 2005.

[7] H. Grotius, De Jure Belli Ac Pacis - on the Law of War and Peace. 2nd ed. Paris (2nd ed. Amsterdam 1631), 1625.

[8] US-Army, Field Manual 3-24 Counterinsurgency Washington, DC: HQ Department of Army, 2006.

[9] D. Kilcullen, "Counter-Insurgency Redux," Survival, vol. 48(4), 2006, pp. 111-130.

[10] D. Kilcullen, The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One. Melbourne: Scribe Publications, 2009.

[11] B. Hoffman, "Insurgency and Counterinsurgency in Iraq," Studies in Conflict & Terrorism, vol. 29(2), 2006, pp. 103-121.

[12] K. I. Sepp, Best Practices in Counterinsurgency, 2005, DTIC Document.

[13] D. Galula, Counterinsurgency Warfare: Theory and Practice. Westoprt, CT: Praeger Security International, 1964.

[14] ADF, Complex Warfighting: Future Land Operating Concept. Canberra 2006.

[15] J. Coleman, "Social Capital in the Creation of Human Capital," American Journal of Sociology, vol. 94(S1), 1988, pp. 95.

[16] S. Wasserman and K. Faust, Social Network Analysis: Methods and Applications. Cambridge University Press, 1994.

[17] E. O. Laumann, P. V. Marsden, and D. Prensky, "The Boundary Specification Problem in Network Analysis," Research methods in social network analysis, vol. 61, 1989, pp. 87.

[18] F. Heider, "Attitudes and Cognitive Organization," The Journal of Psychology, vol. 21(1), 1946, pp. 107-112.

[19] M. McPherson, L. Smith-Lovin, and J. M. Cook, "Birds of a Feather: Homophily in Social Networks," Annual review of sociology, 2001, pp. 415-444.

[20] P. F. Lazarsfeld and R. K. Merton, "Friendship as a Social Process: A Substantive and Methodological Analysis," Freedom and control in modern society, vol. 18, 1954, pp. 18-66.

[21] R. Axelrod and W. Hamilton, "The Evolution of Cooperation," Science, vol. 211(4489), 1981, pp. 1390-1396.

[22] P. Dasgupta, "Trust as a Commodity," Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, 2000, pp. 49-72.

[23] S. Marsh, "Formalising Trust as a Computational Concept," University of Stirling, Department of Mathematics and Computer Science, PhD dissertation, 1999.

[24] M. Granovetter, "The Strength of Weak Ties," American Journal of Sociology, vol. 78(6), 1973, pp. 1360-1380.

[25] R. S. Burt, Structural Holes : The Social Structure of Competition. Cambridge, Mass: Harvard University Press, 1992.

[26] J. Scott and P. Carrington, The Sage Handbook of Social Network Analysis. Sage Publications Ltd, 2011.

[27] L. Hossain, A. Wu, and K. K. S. Chung. Actor Centrality Correlates to Project Based Coordination. 2006. ACM.

[28] B. Markovsky, D. Willer, and T. Patton, "Power Relations in Exchange Networks," American Sociological Review, 1988, pp. 220-236.

[29] R. C. van der Hulst, "Terrorist Networks: The Threat of Connectivity," The SAGE Handbook of Social Network Analysis, 2011, pp. 256.

[30] M. Flynn, M. Pottinger, and P. Batchelor, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Center for a New American Security, Washington DC, Jan. 2010.

[31] Economist, "Democracy in Afghanistan - Wise Council," in The Economist, 25 Mar. 2010.

[32] R. K. Yin, Case Study Research: Design and Methods. Vol. 5. Sage publications, INC, 2009.

Copyright (c) IARIA, 2012. ISBN: 978-1-61208-228-8