14th ICCRTS: C2 and Agility

INFORMATION CAPTURE AND KNOWLEDGE EXCHANGE: THE GATHERING, TESTING AND ASSESSMENT OF INFORMATION AND KNOWLEDGE THROUGH EXPLORATION AND EXPLOITATION

Cdr Simon Reay Atkinson, RN, satkinson.hq@da.mod.uk
Mr Steve Lesher, leshersm@centcom.mil
Professor Dale Shoupe, dale.shoupe@MAXWELL.AF.MIL

Point of Contact
Simon Reay Atkinson
BSc MPhil (Cantab) CEng FIET
PhD Researcher Dynamic social Networks, CUED-EDC UKDA Senior Research
Fellow - Asymmetrics ARAG Scholar Practitioner - Dynamic social Networks Cdr,
RN Advanced Research Assessment Group Defence Academy Faringdon Road
Shrivenham Swindon, Wilts
SN6 8TS
(+44)01793-788819
96161-8819 (mil)

Paper ID 194
Track 4: Collective Endeavors

INFORMATION CAPTURE AND KNOWLEDGE EXCHANGE: THE GATHERING, TESTING AND ASSESSMENT OF INFORMATION AND KNOWLEDGE THROUGH EXPLORATION AND EXPLOITATION

Commander Simon Reay Atkinson[1], Royal Navy, Mr Steve Lesher[2], Professor Dale Shoupe[3]

[1]*UK Defence Academy, Research & Assessment Branch, University of Cambridge,* [2]*Deputy Chief J6, USCENTCOM,* [3]*MAXWELL USAF, Air Education and Training Command, Air War College*
{satkinson.hq@da.mod.uk, leshersm@centcom.mil, dale.shoupe@MAXWELL.AF.MIL}

This paper represents the unclassified deliberati ons of Atkinson, Lesher and Shoupe emerging from Phases I-III of the US CENTCOM [Joint Strategic] Assessment Team, C2 & KM C ell, Oct – Dec 08. This assessment, under the lead of General Davi d Petraeus and C olonel 'H.R.' McMaster, was established in the Fall of 2008; running through to Spring 2009. Its purpose was to provide US / Coalition views on the CENTCOM AO R. As part of this work, Atkin son, Lesher and Shoupe were attached to the C2 & KM Cell w here th eir initia l appreciation beg an with an examination of the principles of Knowledge Management. It was thei r assessment that, despite the recommendations arising from both the 9/11 and Butler reports, that there had been in sufficient analysis, modelling and work done to develop what the 9/11 report righ tly observes as the 'Need-to-Know; Need-to-Sh are; Need-to-Use' model (we called the Three Needs M odel (3NM)) and which both reports recom mend, within 'trust based, virtual networks' that encour age interaction, 'dissent and alternative or minority hypotheses, or uncertainty' to majo rity reporting. This we judged to be the hallmarks of a healthy organisation where dissent is seen also to be an expression of loyalty to the organisations represented and their people; to be encouraged. Moreover, it is also our assessment that the Need-to-Know model is not replaced by the Three Needs Model. Or ganisations and states have certain knowledge – the crown jewels – tha t they have every right to pro tect. Our assessment sug gested that there is a need to develop new methodologies for sharing and using information – creating transparencies as opposed to transparency – across domains, which we describe in terms of new unde rstandings for Knowledge Management, Communities of Interest and Information Capture and Knowledge Exchange (ICKE).

1.   Been There

The 9/11 Report [1] writes: 'as presently configured, the national security institutions of the U.S. government are still the institutions constructed to win the Cold War. The United States confronts a very different world today. Instead of facing a few very dangerous adversaries, the United States confronts a number of less visible challenges that surpass the boundaries of traditional nation-states and call for quick, imaginative, and agile responses[1:399]'. It is our assessment that similar configurations have continued to impair Unity of Effort and Command in our operational theaters; most notably in Coalition enterprises where international legitimacy is often sacrificed at the expense of efficiency and effectiveness – and so unity of effort. 'The problem is nearly intractable because of the way the [national government and international institutions are] currently structured. Lines of operational authority run to the expanding executive departments, and they are guarded for understandable reasons….The result is that each agency or department needs its own intelligence apparatus to support the performance of its duties. It is hard to "break down stovepipes" when there are so many stoves that are legally and politically entitled to have cast-iron pipes of their own. Recalling the Goldwater-Nichols legislation of 1986, Secretary Rumsfeld reminded us that to achieve better joint capability, each of the armed services had to "give up some of their turf and authorities and prerogatives." Today, he said, the executive branch is "stove-piped much like the four services were nearly 20 years ago." He wondered if it might be appropriate to ask agencies to "give up some of their existing turf and authority in exchange for a stronger, faster, more efficient government wide joint effort [2]."[1:403]'. The 9/11 Commission went on to observe [1:417] that the: '…system …requires a demonstrated "**need to know**" before sharing. This approach assumes it is possible to know, in advance, who will "**need to use**" the information. Such a system implicitly assumes that the risk of inadvertent disclosure

outweighs the benefits of wider sharing. Those Cold War assumptions are no longer appropriate. The culture of agencies feeling they own the information they gathered at taxpayer expense must be replaced by a culture in which the agencies instead feel they have a duty to the information—to repay the taxpayers' investment by making that information available…Each agency's incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long-term costs of overclassifying information, though these costs—even in literal financial terms— are substantial. There are no punishments for *not* sharing information. Agencies uphold a "**need-to-know**" culture of information protection rather than promoting a "**need-to-share**" culture of integration[1]. A recommendation arising from the 9/11 Commission was that: 'The President should...coordinate the resolution of the legal, policy, and technical issues across agencies to create a "**trusted information network**." [1:418]'

In the UK and as a result of the investigation into Iraqi Weapons of Mass Destruction, the Butler Report [3] was commissioned. Building on the 'need-to-share', the report stated: '…it will be essential to continue to bring to bear all sources of intelligence in a coordinated way. We have noted…that success in the cases we studied came through close collaboration between all involved to piece together the intelligence picture, **with teams able to have shared access to all available intelligence**'. The report went on to say:, 'However we consider that it would be helpful through day-to-day processes and the use of new information systems to create a **'virtual' network** bringing together the various sources of expertise in Government on proliferation and on activity to tackle it, who would be known to each other and could consult each other easily [3:142]'. The Butler Report also raised the question of 'better machinery for bringing to the attention of the Joint Intelligence Committee (JIC) dissenting opinions' and recommended, inter alia, the: 'consideration of the provision of proper channels for the expression of dissent within the UK MOD Defence Intelligence Service through the extension of the remit of the Staff Counsellor, who provides a confidential outlet for conscientious objection or dissent within the intelligence agencies, to cover DIS civilian staff and the Assessments Staff [3:143]'. The Report went on to state: '…we note that the US Government does from time to time attach degrees of confidence and notes of dissent to its National Intelligence Estimates. These may help to prevent readers from attaching more certainty to judgments than is justified and intended. While not arguing for a particular approach to the language of…assessments and the way in which **alternative or minority hypotheses, or uncertainty, are expressed**, we recommend that the intelligence community review their conventions again to see if there would be advantage in refreshing them.[3:145]'

1.2 Knowledge Management and Communities of Interest

An understanding derived from the US Army [4] by the C2 & KM Cell for Knowledge Management was as:

> 'A cross-disciplinary organic enterprise connecting and integrating social, cultural, communication and technical processes – including trust, obligation, commitment, and accountability – to facilitate creative learning and adaptation and leverage information capture and knowledge exchange (ICKE) by connecting communities 'who-need to-know' with those 'who-need-to-share' with those 'who-need-to-use'.

Based upon DoD CIO Memorandum [5], DoD 8320.02-G [6], the UK MoD's Applied Research Programme, Shared Information Environment work [7], Markham [8], Tirrell [9], Fischer [10], Chirala [11] and Atkinson and Moffat [12]   COIs were considered to be:

---

[1] For the information technology architecture, see Ruth David 9/11 Report interview (June 10, 2003). For the necessity of moving from need-to-know to need-to-share, see James Steinberg 9/11 testimony, Oct. 14, 2003. The Director still has no strategy for removing information-sharing barriers and—more than two years since 9/11—has only appointed a working group on the subject. George Tenet prepared 9/11 statement, Mar. 24, 2004, p. 37.

'Distributed, collaborative and inclusive groupings working to discover, synthesize and exchange knowledge through the sharing of information in order to: take better decisions; implement change and create effects.'

As we envisaged, Communities of Interests form in order to 'discover, synthesise and exchange knowledge through the sharing of information' and it is the role of Knowledge Management to facilitate, aid and support these, principally, social processes in order to 'facilitate…learning and adaptation'.

1.3   Integration versus Interaction
Many social scientists call for integration without really understanding the costs of integration and when, in actuality, they are calling for a new model to replace an existing model that has failed in some way [13]. This form of assimilation – often based upon non causal and non-empirical 'evidence' – essentially replaces integration with what might be termed multi-modelling. Work undertaken by UK MoD [14], considered the following idea for integration, which was used in preparing the Defence Strategic Guidance, 2005:

'The ability of <u>networked</u> systems, units or forces to provide and accept services from other systems, units or forces by uniting procedures, rules and information so that, when formed, the force operates together more effectively, capably and seamlessly as a whole.'

Nonetheless, Integration comes at a cost very often of flexibility and agility as one moves from high end interactivity within groups and across their seams and boundaries to a position where substitution – or interoperability – is no longer an option. For example, in a Coalition Enterprise certain nations may bring specific capabilities or permissible means of approaching issues or problems that would be impermissible and, or, not tenable within an integrated environment, as expressed below:
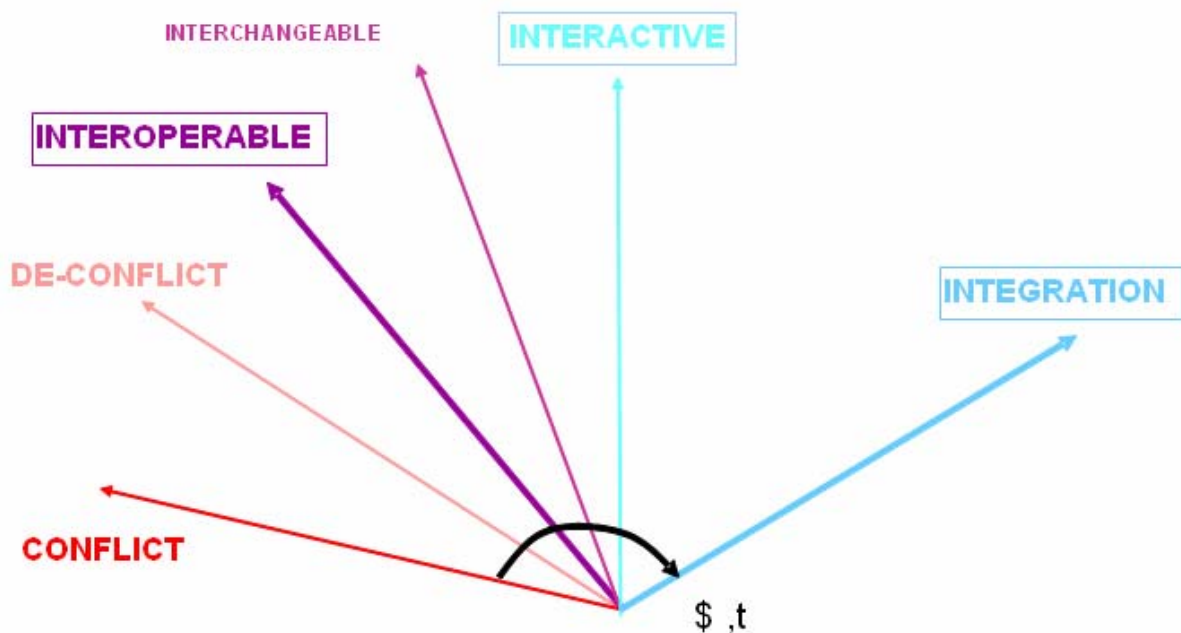

Figure 1: The Arc of Interoperability

The above Arc of Interoperability suggests that for many organisations, 'high-end Interaction' is the best that they might achieve – even within national institutions – and that integration (which essentially means becoming subordinate in some way) is a step too far. We see this not just between intelligence organizations and states but also between the military and other Inter Agencies; between coalition partners and frequently between the Inter Agencies and NGOs and NGOs and the Military[2]. The fact that Integration, however defined, comes at a cost means that most organisations will be willing to share information if it is to be used for a common understandable purpose but are not willing for their partners to know all they have to know about subjects and matters that represent and define their own Intellectual Property. It is these networks we assess that both the Butler and 9/11 Reports had in mind when they spoke of 'trust based, virtual networks' that, in our view, encourage interaction. It is exactly this type of healthy interaction that we had in mind with regard to the combination of COI and KM. As we envisage, Communities of Interests form in order to 'discover, synthesise and exchange knowledge through the sharing of information' and it is the role of Knowledge Management to facilitate, aid and support these, principally, social processes in order to 'facilitate…learning and adaptation'.

2.   Transparencies, Needs and Exchanges

When many of us older soldiers, sailors, Marines and airmen grew up, we used acetates to build up complex operational pictures. In effect, this was achieved by building up different operational layers by laying transparencies on top of each other to build up the final picture. This was through a process of interactive information exchange and knowledge capture (ICKE), that we see as being typical within a Community of Interest. Essentially, each picture – acetate or view-foil – was declaratory of the position of a particular agency with regard to a specific objective or target. Information was declared so as to de-conflict activities and, more specifically, to avoid conflict (for example blue-on-blue). This was an interactive process that enabled integration of resources for a specific purpose, often geographically and temporally defined. It did not mean full access to every one's information or a right to know by all parties to everything known by each other. Indeed such systems, where they exist, are rapidly swamped by information to the point where they can often barely deconflict; sometimes resulting in so called, 'friendly fire' incidents. Calls for transparency, we therefore concluded, are often misplaced and even nonsensical when what may actually be needed is 'transparencies; not transparency, per se'. In other words, the building up of an integrated picture through the interactive-declared 'transparencies' of individual positions – through a COI – rather than demanding transparency from, by and to all. This leads to an integrated approach to a specific problem – without the costs of global integration, which will nearly always be impossible to achieve in any case.

2.1   Needs

As identified, we assessed that there was an increasing need to re-examine existing and develop new methods for information capture and knowledge exchange as also mandated in the 9/11 [1] and Butler (UK) [3] Reports. This needs to find ways of respecting rights and privileges established previously in terms of *need-to-know*, whilst developing procedures for *sharing* and for *using*. This, in turn, led us to the concept of the Three Needs Model (3NM) described in terms of *Need-to-Know*; *Need-to-Share* and *Need-to-Use* – as identified but not specified in the 9/11 Report. Previous recommendations had been made to move from 'need-to-know' to 'need-to-share' but we concluded that little work had been done to develop these concepts, or implement them, whilst recognising and preserving understandable need-to-know rights and privileges. It was our assessment, that Communities of Interest as we consider them to be, have a specific role to play regarding information capture and knowledge exchange, as supported by Knowledge Management. Furthermore, we envisaged effective Communities of Interest combining

---

[2] Although interestingly it was observed that, probably for reasons of proximity, relations between NGOs and the Military at the tactical and operational levels were often far closer and more understanding than between NGOs and their Inter Agency contacts.

the three needs: 'Need-to-Know (N2K); Need-to-Share (N2S) and Need-to-Use (N2U)' within their constructs, building upon and from their 'declared transparencies' to achieve an integrated picture.
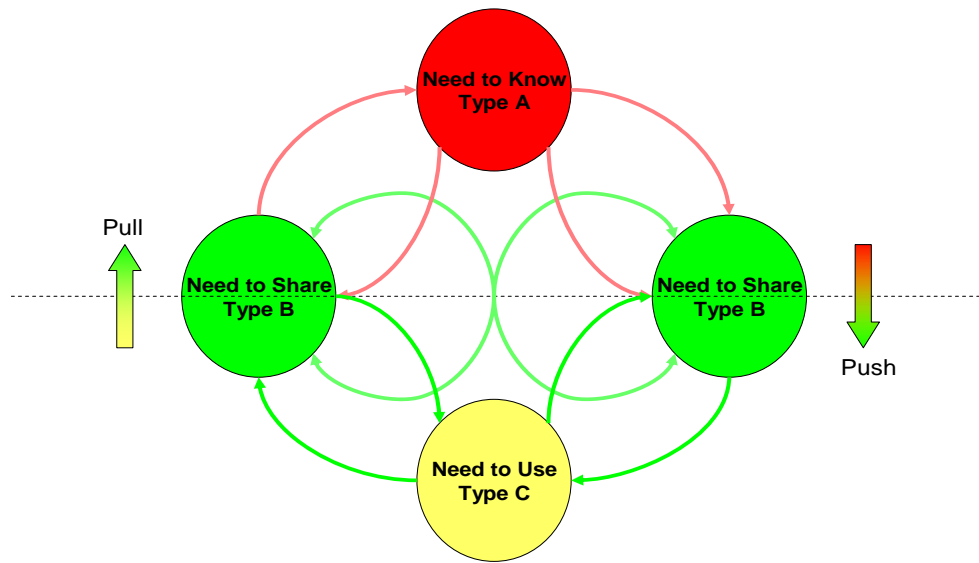

Figure 2: Need-to-Know; Need-to-Share; Need-to Know (3NM) Model

Communities of Interest can exist to Know or to Share or to Use Information and exchange Knowledge. It was our opinion that they can only be effective when all three come together in a COI. As example, during the Foot and Mouth epidemic in the UK in 2001, the UK Government was able to combine its departments in order that they knew what was happening and could share information between them at the strategic level. The problem was that they did not have the 'doers' at the operational and tactical levels to implement change and so affect the course of the infection. This was ultimately and largely supplied by the British Army (with sailors and airmen); frequently operating at the junior officer and corporal level. This remains the case when comparing military organisations, who have depth at the strategic, operational and tactical levels; with Inter Agencies, who frequently have depth at the strategic level but patchily at the operational and little at the tactical levels; with NGOs, who are often tactically rich but operationally constrained. If we can find ways of combining these different needs to know, share and use within a COI, it should be possible to affect the changes we all know and desire to deliver.

2.2   Exchanges
Proposals were developed for what was termed an 'information vectored exchange' which sought to identify and so, to an extent, distinguish between different types of information and opportunities for exchange. The model also built upon concepts for the serial vectoring opportunities [15] for such information exchange, to develop a seven stage IVE model (in GMS[3]) detailed in Figure 3. This model, in turn, combined notions for Type A (Control); Type B (Command) and Type C (Informal) networks[4] in terms of Need-to-Know (A); Need-to-Share (B) and Need-to-Use (C) [16]. In this model, Figure 2, the Command function is seen to both connect and arbitrage between the Need-to-Know (Type A) and Need-to-Use (Type C), i.e. between Control and Informal Networks. In an effective and competent

---

[3] Graphical Modeling System (GMS) developed by the Office of Naval Research (ONR) and being taken forward in collaborative partnership with, amongst others, SPAWAR, Dstl and the UK Defence Academy.
[4] The idea for different forms / types of networks (A, B and C) is emerging from work undertaken by Simon Reay Atkinson as part of his PhD Research at the University of Cambridge, Engineering Department.

organisation, Type B networks are seen to have emergent properties resulting from and contributed to by healthy interaction between Type A and Type C Networks. The Three Needs Model shows both multi-loop exchange and the push and pull of information, see Figure 2.

Figures 2 and 3 examine what a 3NM and IVE model might look like and how it may possibly operate. The Need-to-Share network is shown acting as the vectoring component within the model; pulling, pushing and so enabling information flow from and between the Need-to-Know and Need-to-Share models shown in Figure 2. Essentially, the Need-to-Share network is shown acting as the vectoring component within the model; pulling, pushing and so enabling information flow from and between the Need-to-Know and Need-to-Share models shown above. Figure 3 below suggests such a seven layered IVE model for information and exchange.
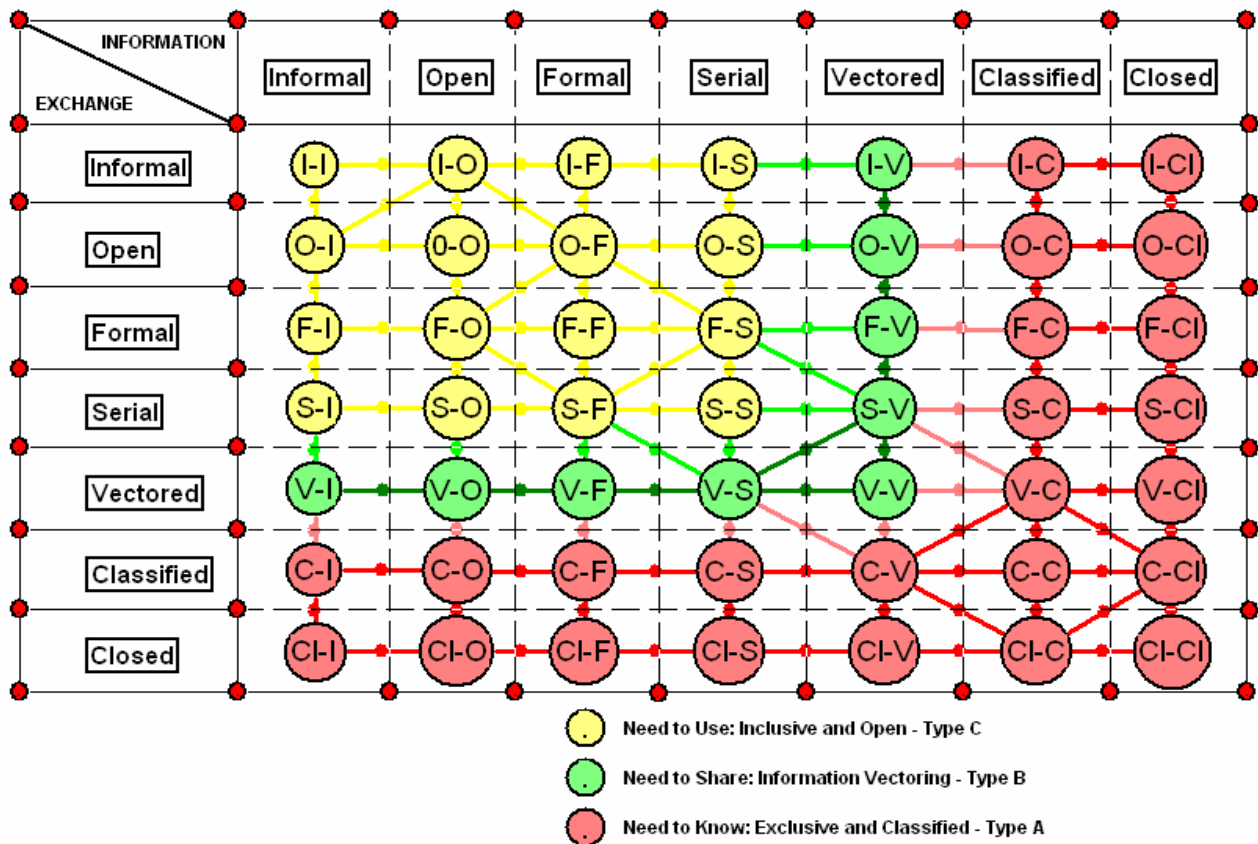
INFORMATION / EXCHANGE

	Informal	Open	Formal	Serial	Vectored	Classified	Closed
Informal	I-I	I-O	I-F	I-S	I-V	I-C	I-CI
Open	O-I	O-O	O-F	O-S	O-V	O-C	O-CI
Formal	F-I	F-O	F-F	F-S	F-V	F-C	F-CI
Serial	S-I	S-O	S-F	S-S	S-V	S-C	S-CI
Vectored	V-I	V-O	V-F	V-S	V-V	V-C	V-CI
Classified	C-I	C-O	C-F	C-S	C-V	C-C	C-CI
Closed	CI-I	CI-O	CI-F	CI-S	CI-V	CI-C	CI-CI

Need to Use: Inclusive and Open - Type C
Need to Share: Information Vectoring - Type B
Need to Know: Exclusive and Classified - Type A

Figure 3: Information Vectored Exchange (IVE) for Information Capture and Knowledge Exchange

The IVE Model developed in Table 1 and Figure 3 posits a way of moving towards a more *inclusive* exchange of information between tightly controlled Type A Networks (N2K) and the informal and less controlled Type C Networks (N2U) – whilst protecting and preserving rights and privileges. Command and Control, Coordination, *Focus* and *Convergence* – CFC vice C2 – Type B (N2S) Networks are seen to occupy the *vital space* between the N2K and N2U models. The main intention of the N3 model is to provide the informal-formal processes and protocols for resolving factional differences that exist in any healthy organisation.

Level	Information	Exchange
Informal	Non-formalised information	Ad hoc meetings, gatherings, gossip
Open	Freely accessible information	Non-exclusive gatherings
Formal	Formalised information (papers, news etc)	Inclusive Membership
Serial	Information streams – newscasts etc	Streamed (consecutive-temporal) meetings
Vectored	Calibrated / directed Information	Calibrated / directed meetings and discussions
Classified	Codified information	Meetings held in camera at pre-determined levels
Closed	Limited access information	Limited access meetings

Table 1: Information Exchange

3. Organising for Information Capture and Knowledge Exchange

It is feared that widescale ignorance of the principles of data, information, knowledge and their communication has probably bedevilled many IT programmes. Yet still there is pressure for these programmes to be made yet bigger and more global. Why and at what cost? This ignorance extends to issues of command and control; often making it harder to command. Managerialism in its various constructivist-methodological guises, from the Soviet Union onwards, has wished to impose centrality and control – orthodoxy – upon people and organisations. In many organisations, IT systems have essentially taken the pay, promotion and reporting structures from individual managers and leaders and placed them with the information-data-entities under the tag of KM. Promotion, pay and selection can only now occur within and in adherence to these processes and compliance with them. The very core tenets and rational of many successful organisations may have been ceded to process – command has essentially been lost. There is no room here for adaptation – field promotion – or selection / promotion of those who do not fit the process-mold. Agility has essentially been squeezed out by the conjoining processes of evidence-basing and performance management. Essentially, these processes have locked such organisations into a process of metricated-reductionism; rewarding, principally, process and adherence to it. Dissent is not seen to be an expression of loyalty to be encouraged. This is not the fault of processes or systems per se but of the ways in which training, methods, processes and centralising ambitions have been used to subordinate and control. This has been exacerbated by the lack of technical knowledge within many senior managers and leaders and their inability to recognise what is being done to them and their failure to work the processes or do anything about them. As a result, 'ruthlessness is reaching its most sublime levels' [17]. Of equal concern, it should be recognised that such organisations may 'no longer be under command'.

3.1 The Costs of Enterprise

Just as many organisations have apparently embarked upon the almost wilful dereliction of duty they may have also embarked on exercises of knowledge and information destruction. As example, taking Bunge's social-knowledge model – '…cognition is personal, but knowledge is social [18]' – and applying it to many organisations, for years there has been downward pressure on numbers. This, in turn, has led to the displacement of people – through re-location and redundancy. Up and until the late 1990s, information was stored in the tactile – frangible – form of paper, files / packs. These packs were stored in local cabinets – in the 'custody of' originators and 'librarians / registries' alike. They were occasionally weeded by an expert and, as occasionally, sent off for archiving. Knowledge was 'held in being' by the organisation; its people and the mental-physical (paper and cabinet) datums established. People knew where to look – they were situation aware. Sold the myth of 'knowledge management [19]', senior management were persuaded that they could recreate their 'networks-in-being' [16] by a) getting rid of the people (experts and librarians) and b) scanning all the old frangible

packs to create new, 'exciting' KM data bases, with access to all. Now, no one knows where to look – they can no longer sensemake[5] [20] – and staff officers are left frequently either a) recreating the wheel or b), spending hours trawling old data bases. Inevitably, it is easier for them to build new models – multi-modelling – which the organisation prefers them to do. So careers are advanced; billions wasted and lives lost.

3.2 ICKE – A New Razvédka Bóyem

Information and data give the impression of being without cost or value. Neither is true. Szilard [21] maintains that 'information is costly to acquire and use'. Combining this with Bunge's observation, the following useful maxim is seen to apply: 'that knowledge is social and, like information, it is costly to acquire and use [22]'. It is this idea of both cost and thereby value in its wider social sense that led to a re-examination of Soviet, Red Army concepts for Razvédka Bóyem. In the initial sense, this was taken to describe intelligence gathering through battle. In its wider understanding, as possibly applied to Cyber-, it may be thought of as 'the gathering, testing and assessment of information and knowledge through exploration and exploitation (battle)'. This line of thinking has led to the concept of 'Information Capture and Knowledge Exchange (ICKE)', as developed by the C2 and KM Cell, with its emphasis upon the active capture of information and social exchange of knowledge. There is a considerable way to go before these ideas and concepts are understood let alone adopted or taken up by senior management for education, training and application. At the same time, displacement activities continue apace while the unforeseen consequences of actions driven more often by despair than knowledge, further limit the capacity and will to act. Put simply, we have frequently been blinded by our own processes and this, in turn, may be further encouraging the flight to Cyber-.

3.3 Organising for ICKE

Type A (Control) Networks outlined previously, see also Keller et al [16], lend themselves to technological applications, specifically where rules and procedures are required to determine and protect information flows. Over the past fifteen years or so, technology has often been seen to drive the science, with the result that data-based-technologies have been seen more as 'ends in themselves' than as means. More an end result than an aid to achieving it. This has had the effect of displacing the social dimensions of the network: increasingly, Type A networks have become unknowing and, worse perhaps, unknowable. And as this has occurred, the opportunities for leaking or suborning the system may have increased. Almost the reverse has been the case for Type C (Informal) networks which have exploded because they are seen as a means and not an end to communication and social interaction, for example Facebook.

Most governments have, in their *being*, departments that occupy part of the Need-to-Share networks, such as StratCom. A perceived problem is that frequently these departments / agencies may not be part of a comprehensive, 'whole' programme. They are often individually located, poorly structured and controlled in such a way that they are made more 'pink than green – closed than open' (see Figure 3). In such an environment, they are rarely respected (or trusted) and can frequently become the scapegoats – useful messengers to be shot. Consistency of message and continuity of people becomes erratic and difficult to sustain – further disrupting and weakening the narrative. This has been exacerbated by the apparent dysfunctional nature of many institutions, reaction to failure has rarely been to 'learn and adapt' but rather to 'react and control'.

In actuality, it is our assessment that Type B Need-to-Share Networks exist on the edge of Type A, Need-to-Know, networks and, similarly, on the edges of Type C networks (not centrally as shown): they are 'double-edge' networks. Other work has possibly identified that Type B networks have

---

[5] Alberts [14]: 'Planning is part of Sensemaking.'

emergent properties – emerging from the combination of functional Type A and Type C networks. When Type A and C networks are non-functional and interaction between the two is constrained and untrusting, it has been observed that functional Type B networks may not emerge. Moreover, whilst an organisation might determine its Type A networks it can, at best, only influence its Type C networks. Therefore, through its Type A Networks, the main responsibility for creating Type B edge-networks probably rests more with the organisation itself.

To place people on the edge of an organisation and keep them there, three principle requirements are seen to exist – each of which has to be operating, simultaneously:

➢ There needs to be underlying (extra-organisational) 'societal' trusts in processes, procedures and protocols – in some instances rules – to encourage and protect edge-individuals. Current mandated (what is not prohibited is permissible type) legislation does not achieve or provide for this.

➢ Organisations need to be able to recognise, create, reward and promote ability within their formal, ranked structures – to be, primarily, ability as opposed to rank conscious – and to identify, recruit and select individuals on the basis of 'capability not preference'. Specifically, these individuals need to be protected and separated from formal career lines and processes – in some cases individual managers. On selection and appropriate positioning, organisations then need to create 'secure, sure and safe' reporting and 'handling lines' that will enable edge-individuals and their associated networks and programmes to exist – 'to be' – over the long term.

➢ Individuals need to be identified, educated, trained and kept alive but, at the end of the day, their organisation needs to understand that only a small percentage of people, perhaps between 2-10%, can or indeed would wish to work in such domains. And they can easily be prevented from doing so. Their reward is often little more than 'being' enabled and allowed to be members of such networks.

3.3 Needing to Know, Share and Use

Need-to-Share networks, working essentially between and across the 'open-to-closed' information domains, need to have certain protected privileges, protocols and processes. This is essentially what is meant by vectoring. In other words, contained within the serial streams are meta-state vectors that relate directly – and so can be immediately distinguished – to the meta-datums [23] established within both the Type A and Type B networks. In this way, information can be processed and acted upon accordingly; knowledge formed and information exchanged [24]. Simply creating an organisation and placing it on the edge without previously establishing appropriate meta-datums within both networks and the connecting meta-state vectors (protocols, processes and procedures) will not allow for the organisation as a whole to function. The Type B networks will quickly be killed off. Similarly, expecting the Type B networks to cover the complete edge without concentrating on key nodes, will spread resources too thinly and lead to dis-functionality. The solution would appear to be to create the conditions from which Type B networks might emerge and be scaled and then coupled appropriately.

Bletchley Park is a case in point. Created very much to work on-the-edge (as a Type B network), by all accounts it functioned brilliantly from its inception up and until 1942. Then it went into sharp decline and, by the end of the war, was a shadow of its former self. Why? Four reasons appear uppermost: first, its very success caused jealousies within the otherwise privileged Type A communities; secondly, these jealousies led to rules and processes being introduced that, thirdly, acted to prevent the Type B networks forming and so, fourthly, inhibited the sharing and using of information and so the exhibiting of emergent behaviour. This may also have been impacted by the US infusion occurring at around

same time (change on change); the organisational-cultural changes this brought with it and the weakness of Churchill's position in 1942 (after Singapore). The combined effect was to reduce the trusts and increase the controls and rules placed upon Bletchley Park – although, interestingly, its outstations were largely unaffected and, it is our assessment, some continued to perform well long after the end of WWII.

4.   A Call for Re-Integration

Significant questions remain regarding *system identification*, *enabling* and *disabling* and *composition* and *de-composition*. As has been suggested, organisations have often not done the vital system identification work, first, in terms of what is incoming and outgoing and what is wanted and, as importantly, not wanted. Equally, peoples' perceptions of information and information systems vary significantly, frequently to the detriment of the organisation as a whole. For example, the development of Strategic Communications within government structures. At the same time, a lack of scientific [*decompositional*] understanding (when it comes to the creation and sustaining of successful edge-networks capable of undertaking this type of work effectively) has led to stasis and sometimes worse. Effectively, organisations and networks have been disabled rather than enabled. Re-integration will require a scientific understanding of what we want to do in terms of system identification; broken down further with respect to enabling / disabling and composition / decomposition. A better understanding of information; what it represents and how it is exchanged will greatly assist this work. It is our assessment that, whilst more work is required to develop the above models – including moving from transparency to transparencies and from value to values based judgements – that the above models, including our understanding of Communities of Interest and Knowledge Management offer us a way to re-engage our institutions in ways and means that might truly deliver Unity of Effort; Unity of Command and so Unity of Action.

References:

[1] 9/11 Commission Report (2004).

[2] Donald Rumsfeld prepared statement to 9/11 Commission, Mar. 23, 2004, p. 20.

[3] Review of Intelligence on Weapons of Mass Destruction Report of a Committee of Privy Counsellors. (2004). Chairman: The Rt Hon The Lord Butler of Brockwell KG GCB CVO Ordered by the House of Commons to be printed 14th July 2004.

[4] US Army CIO/G-6.(2008).KM Principles. Army Knowledge On-Line (AKO). https://www.us.army.mil/suite/page/doc/10713107.

[5] DoD CIO Memorandum.(2003).DoD Net centric Data Strategy. May 9, 2003.

[6] DoD 8320.02-G.(2006).Guidance for Implementing Net-Centric Data Sharing. April 12, 2006.

[7] Johnson, K. (2001).Initial Version of the Information Concept (Shared Information Environment). QINETIQ/KI/SEB/CR010172, October 2001.

[8] Markham, G.(2004).Communities and their contribution to agile mission grouping. 2004 Command and Control Research and Technology Symposium.

[9] Tirrell, R.P., Lt Col USMC.(2001).Amphibious Expeditionary Warfare C4I Modernization. 2001 Command and Control Research and Technology Symposium.

[10] Fischer, G.(2001) Communities of Interest. Department of Computer Science and Institute of Cognitive Science University of Colorado, Boulder24th Annual Information Systems Research Seminar In Scandinavia (IRIS'24), Ulvik, Norway, August 2001.

[11] Chirala, R.C.(2004). A Service-Oriented Architecture-Driven Community of Interest Model. Department of Computer Science & Engineering Arizona State University.

[12] Atkinson S.R. and Professor J. Moffat.(2005).The Agile Organization. CCRP.

[13] Tooby, J. and L. Cosmides.(1992).The Psychological Foundations of Culture. Chapter 2 in: The Adapted Mind: Evolutionary Psychology and the Generation of Culture. Editors, Jerome, H., L. Cosmides and J. Tooby, OUP, p. 2, 3, 27.

[14] As Briefed (2002) in: The Policy Perspective. UK MOD, DFD, 20021031_NEC_Presentation.

[15] Logan, B and P.J. Moreno.(1997).Factorial Hidden Models for Speech recognition: Preliminary Experiments. Cambridge Research Laboratory, Technical Report Series, CDR 97/7 September 1977.

[16] Keller, R., N Carrigan, S. Reay Atkinson, P. Johnson and P.J. Clarkson (2008). Collaboration and Information Sharing in NEC Networks. NECTISE Conference, Leeds University, Oct 08.

[17] Wiener, N. (1948). Cybernetics or Control and Communication in the Animal and the Machine. Wiley, New York, NY.

[18] Bunge, M. A. (2000). Ten Modes of Individualism - None of Which Works - And Their Alternatives. Philosophy of the Social Sciences 30(3): 384-406.

[19] Wilson, T.D.(2002).The nonsense of Knowledge Management. Information Research, Vol. 8, No.1, October 2002.

[20] Alberts, D. S. and R. E. Hayes (2007). Understanding Command and Control. DoD Command and Control Research Program, CCRP publications, p. 63.

[21] Szilard, L.(1964 (1929)).One the Increase of Entropy in a Thermodynamic System by the intervention of Intelligent Beings – the Critique.(Rapoport A. and M. Knoller trans.). Behavioural Science 9:302-2310.

[22] Atkinson, S.R.(2008).The Study and Instrumentation of Decision Taking in Dynamic Social Networks. University of Cambridge Engineering Department-EDC First Year Report, p. 51.

[23] McOwat, D. and D.J. Holland Smith.(2003).A Business Model for Knowledge Services. Presented to Dstl, 23 October 2003.

[24] Marsay, D.(2001).Distributed Intelligence Fusion. DERA Internal Paper.