

C4ISR, THE FINC METHODOLOGY, AND OPERATIONS IN URBAN TERRAIN

Anthony H. Dekker¹

Abstract. In this paper, we describe the FINC methodology for analysing C4ISR and NCW architectures. We utilise the “Black Hawk Down” incident in Mogadishu as a case study, in order to demonstrate how the FINC Intelligence Coefficient metric is calculated. We show how the FINC methodology can be used to evaluate possible improvements to the C4ISR architecture used in Mogadishu, and to NCW architectures more generally.

INTRODUCTION

The topic of C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) architectures is of enduring importance for military operations. This is particularly so given the current interest in Network Centric Warfare (NCW) [1] and the increasing requirement for new kinds of Operations Other Than War (OOTW) in complex and urban terrain.

The FINC (Force, Intelligence, Networking, and C2) methodology [2–4] analyses NCW or C4ISR architectures in terms of:

- Force nodes, which conduct activities (F);
- Intelligence or information-generating nodes (I);
- Network links (N); and
- C2 nodes (C).

Figure 1 shows an example (discussed in more detail in the body of the paper). C2 nodes are indicated by circles, Intelligence nodes by rounded boxes, and Force nodes by square boxes (Force nodes can also generate information, as well as carrying out activities). Network links provide communication between nodes, indicated by lines or arrows in Figure 1, depending on whether information flow is bidirectional or unidirectional.

The FINC methodology provides a way of quantifying the information sources and network links in a C4ISR architecture. This allows the calculation of a number of metrics for evaluating C4ISR architectures, including the Intelligence Coefficient, described below.

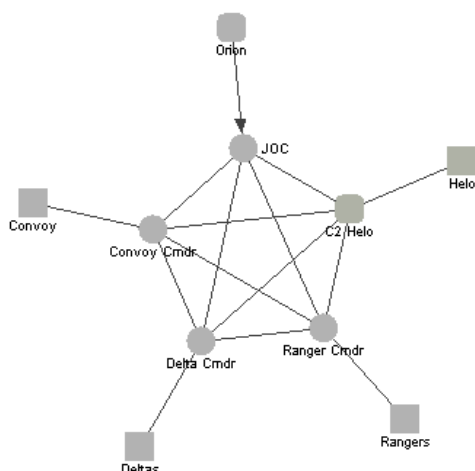


Figure 1. Simplified architecture for Mogadishu scenario.

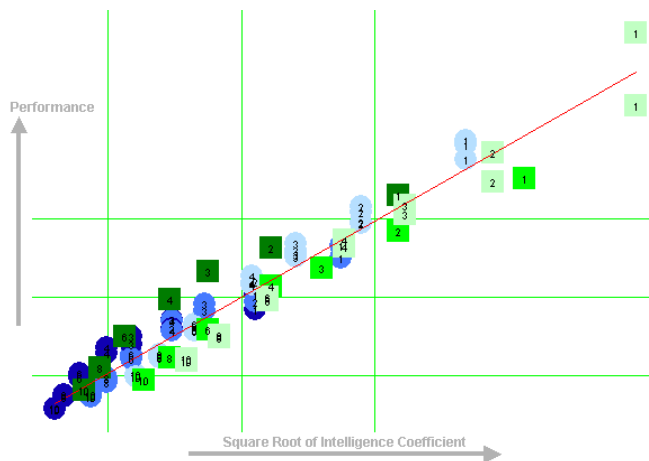


Figure 2. Prediction of performance by the Intelligence Coefficient for a target search scenario.

The FINC methodology provides a way of quantifying the information sources and network links in a C4ISR architecture. This allows the calculation of a number of metrics for evaluating C4ISR architectures, including the Intelligence Coefficient, described below.

The FINC methodology has been validated through a number of simulation experiments [2–4] and has been effective in predicting performance in several different kinds of scenario. In particular, the Intelligence Coefficient correlates well with performance in simulations of an air-strike scenario [2], a target-search scenario [3], and a combat scenario [4]. Figure 2 shows the prediction of performance by the Intelligence Coefficient in the second case. In each of these simulations, increasing the Intelligence Coefficient has led to an increase in performance. A study of the US Civil War [3] suggests that this relationship continues to hold in the real world.

In this paper, we describe the FINC methodology by working through another real-world example, based on the well-known “Black Hawk Down” incident in Somalia in 1993. The lessons of this incident are worth re-examining, since C4ISR for operations in urban terrain is a topic of great importance in the current era. This incident also provides a good example for illustrating the methodology, since the various features of the FINC methodology need to be explained in terms of a concrete example.

Although the FINC methodology still requires further validation and refinement, the Mogadishu case study provides a demonstration of its potential for examining improvements to C4ISR and NCW architectures.

¹ Defence Science and Technology Organisation (DSTO) Fern Hill, Department of Defence, Canberra ACT 2600, Australia.

THE MOGADISHU SCENARIO

On 3 October 1993, a US task force entered central Mogadishu in order to apprehend two senior members of the Aidid organisation [5,6]. The mission was a Pyrrhic victory: although the tactical objective was achieved, the high level of casualties led to the US leaving Somalia (10% of personnel died, 45% were injured, and one helicopter pilot was captured and used as a hostage).

A decade later, such operations in urban terrain are increasingly important, and so we will use this Mogadishu scenario as a case study in order to demonstrate the FINC approach to C4ISR metrics. Specifically, we will examine a simplified architecture, shown in Figure 1, incorporating the major elements of the task force:

- Elements of the 1st Special Forces Operational Detachment-Delta (Delta Force) from Fort Bragg, North Carolina [7–9] (*Deltas* and *Delta Cmdr* in Figure 1).
- Elements of the 75th Ranger Regiment, from Fort Benning, Georgia (*Rangers* and *Ranger Cmdr*).
- Elements of the 160th Special Operations Aviation Regiment (SOAR) from Fort Campbell, Kentucky [10], including a C2 helicopter carrying the ground and air commanders (*Helo* and *C2 Helo*).
- A convoy of ground vehicles (*Convoy* and *Convoy Cmdr*).
- The commanding general in the Joint Operations Centre (JOC), equipped with a video feed from a US Navy Orion aircraft flying overhead (*JOC* and *Orion*).

The JOC and the various commanders were tied into a command radio network. Separate radio networks also existed within each element.

C4ISR in this operation was inadequate, and this was one factor in the outcome of the mission. Particular issues [5] included:

- Confusion as to the chain of command, with direct command from the JOC as well as from the C2 helicopter.
- Organisational interoperability problems.
- Relaying information across different radio networks, causing delays which were sometimes fatal.
- Confusion as to location, resulting in the ground convoy becoming lost and travelling in circles at one point, while under heavy fire.

These issues make the Mogadishu scenario a good choice for demonstrating the potential benefits of C4ISR metrics in general, and the FINC methodology in particular.

MODELLING THE SCENARIO WITH FINC

Technology Factors on Links

For the FINC methodology, we give each link a technology rating, based on the scale in Table 1. This scale is based on the findings of Sproull and Kiesler [12], that the time to complete a distributed task using face-to-face contact, chat,

and e-mail is approximately in the ratio 1:2:4 (averaged over several experiments). We have interpolated other technologies into the scale, and so further laboratory experiments would be necessary to confirm the validity of this scale in a military environment.

For the Mogadishu example, we have voice communication (level 4) on most links, together with level 2 for the video feed from the Orion aircraft.

Organisational Factors on Links

Together with the technology rating, we also give each link an organisational rating, based on a variation of the Organisational Interoperability Model or OIM [11], as shown in Table 2. The OIM was developed based on the Australian experience with coalition operations, and provides a useful mechanism for assessing organisational and cultural differences. The OIM proper has a fourth column, “Understanding,” which we instead model through the technology factors described above. For each link in the network, we classify the pair of people or groups involved in terms of all three columns of Table 2. We take the **lowest** of these three numbers as the OIM value for that link (note that the OIM scale has 4 as the highest level, in contrast to the technology rating).

Table 1. Technology ratings for use with the FINC metrics.

Rating	Technology
Level 1	Face-to-face contact
Level 2	Video-conferencing, or voice plus video feed
Level 3	Voice plus limited data feed
Level 4	Plain voice, or rich email
Level 5	Plain text email, or limited data feed

Table 2. The Organisational Interoperability Model (OIM) adapted for use with the FINC metrics.

	Preparedness	Command Style	Ethos
Level 4 Unified	Complete: normal day-to-day working	Homogeneous	Uniform
Level 3 Combined	Detailed doctrine and experience in using it	One chain of command and interaction with home organisation	Shared ethos but with influence from home organisation
Level 2 Collaborative	General doctrine in place and some experience	Separate reporting lines of responsibility overlaid with a single command chain	Shared purpose; goals, value system significantly influenced by home organisation
Level 1 Ad hoc	General guidelines	Separate reporting lines of responsibility	Shared purpose
Level 0 Independent	No preparedness	No interaction	Limited shared purpose

For the Mogadishu example, we have $OIM = 4$ for links between units and their commanders. We also have $OIM = 4$ for links where organisational factors are not an issue, in this case the video feed from the Orion aircraft to the JOC.

Within the Mogadishu command network, we have $OIM = 2$ because of confusion about the chain of command. It was never clear whether the person commanding troops on the ground was the ground commander in the C2 helicopter, or the general in the JOC. We therefore model “Command Style” as level 2 (collaborative) for links in the command network, and hence $OIM = 2$.

For the Delta–Ranger link, we have $OIM = 1$ because of differences in ethos and limited preparedness. Delta Force is an unconventional unit with a particular focus on hostage rescue and counter-terrorism. The founder of the unit, Col Charlie Beckwith, modelled it explicitly on the British Special Air Service (SAS) [7,8]. The Rangers, on the other hand, are an elite regular US Army unit (intended to be “the best light infantry unit in the world”). Both Deltas and Rangers had trained to operate with SOAR (indeed, SOAR was formed as a result of recommendations arising from the failed 1980 Delta rescue of US hostages in Iran). We would model this combined training as “Preparedness” level 3. However, Deltas and Rangers had not trained to operate with each other (“Preparedness” level 1). There were also differences between Deltas and Rangers in clothing, haircuts, saluting, formality, and approaches to carrying out a mission. Although relationships between these units was friendly, and Deltas assisted Ranger training in Mogadishu, the differences led to communication difficulties and to some blue-on-blue incidents [5]. We therefore also model “Ethos” as level 1 for the Delta–Ranger link, and so (for two different reasons) $OIM = 1$ on that link.

Information Quality Factors on Nodes

For each information-generating node (the five force nodes in Figure 1, plus the C2 helicopter and Orion aircraft), we assign an information quality based on the answers to four questions as shown in Table 3:

- Where am I?
- Where are my buddies?
- Where is the immediate threat?
- What is the big picture?

We rate each information source as absent = 0, lo = 1, med = 2, or hi = 4 against all four questions, and total the results to give an estimate of overall information quality. Again, further experiments are necessary in order to validate this scale.

Table 3. Information quality ratings for the Mogadishu example.

Node	Where am I?	Buddies?	Immediate Threat?	Big Picture?	Total Score
Rangers, Deltas & Convoy (voice)	lo	lo	lo	–	3
Helicopters (video)	lo	med	med	lo	6
Orion (video)	med	med	hi	hi	12

The Intelligence Coefficient

For each link, we obtain an overall “delay” factor, which estimates the combined effect of organizational and technical obstacles to effective information flow:

$$\text{delay} = (5 - OIM) \times \text{technical} \tag{1}$$

Essentially this delay factor is an estimate of the time to get across understanding, i.e. to develop shared awareness across the link. For pairs of nodes without a direct link, we estimate the delay factor by adding delays on the shortest path between them. We then calculate the intelligence coefficient by considering each combination of an information source and a force node which might use the information, and add up the *quality / delay* ratios for each such combination (where the quality factor for the information source is as described in the previous section). For example, the Orion aircraft has information quality = 12, and the Orion–Ranger path has delay = 18, resulting from the combination of three links:

- Orion–JOC, $OIM = 4$, tech = 2, delay = $(5-4) \times 2 = 2$
- JOC–Ranger Cmdr, $OIM = 2$, tech = 4, delay = 12
- Ranger Cmdr–Rangers, $OIM = 4$, tech = 4, delay = 4

It thus adds $12/18 = 0.667$ to the total. Adding up the quality/delay ratios for all the other such paths gives the Intelligence Coefficient. The CAVALIER network analysis and visualisation tool that we have developed [4,13] performs these calculations at the touch of a button.

Previous work has shown that the Intelligence Coefficient correlates well with performance in several different simulation experiments, including an air-strike scenario [2], a target-search scenario [3], and a combat scenario [4]. We would therefore expect the Intelligence Coefficient to be generally useful as predictor of performance, including in the Mogadishu scenario examined here.

C4ISR Improvements

The Intelligence Coefficient is only useful if we are comparing changes to it as a result of C4ISR improvements. For the Mogadishu scenario, we consider two improvements:

- Organisational improvement, including resolving the cultural differences and confusion about the chain of command. This is modelled by making the OIM value on each link at least 3.
- Technical improvement. The option we consider is giving key personnel GPS units which broadcast their locations. This can be done by piggy-backing position information on voice traffic, which is feasible for packet radio systems. Commanders can then be issued laptops or PDAs which overlay unit positions on a map. Such a system might have prevented the convoy getting lost, and would also ensure commanders knew where key personnel were located. We model this improvement by setting the technology factor on links to be at most 3 (corresponding to voice plus data), and setting the information quality factor on the relevant nodes to 4 (corresponding to an improved medium score for the question “Where am I?”).

The FINC methodology can also examine the impact of improvements in sensors, and in network topology (such as adding additional communication links).

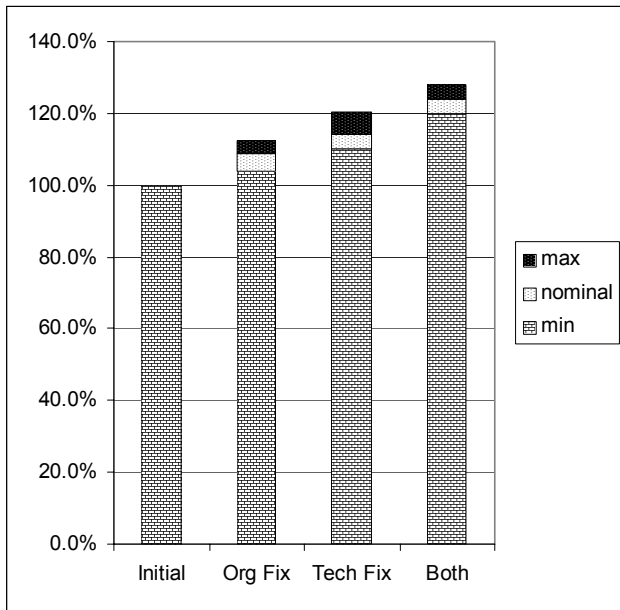


Figure 3. Intelligence Coefficient comparison for two improvements to Mogadishu scenario.

Figure 3 compares the intelligence coefficient for the initial configuration, for both improvements, and for the combination of both improvements. Figure 3 incorporates confidence intervals resulting from a sensitivity analysis on the two most uncertain aspects of our modelling:

- The information quality associated with the Orion aircraft (12 in Table 3) is varied from 8 to 16 (the value for the helicopters remains half of this value).
- The combination of OIM value and technology rating on links is varied to give greater weight to one or the other factor.

Figure 3 indicates that either improvement would have noticeably improved C4ISR, and hence provided an increase in operational effectiveness. These improvements, in combination with others, may have been enough to tip the balance in terms of operational outcome. Because of overlapping confidence intervals, Figure 3 does not allow us to say which of the two improvements would have had the greatest impact. Further refinement of the FINC methodology is required before such assessments can be made. However, Figure 3 does indicate that the combination of both C4ISR improvements would be more beneficial than either on its own.

Naturally, weapons limitations also have an impact on mission success, and the FINC methodology does not attempt to compare the relative impacts of C4ISR improvements and weapons improvements. However, the FINC methodology is able to compare the impact of changes to communications technology, network topology, and organizational issues.

CONCLUSIONS

We have described the FINC methodology for analysing C4ISR and NCW architectures and illustrated it by working through an example based on the events in Mogadishu on 3 October 1993. This is a particularly relevant example because of the increasing requirement for new kinds of Operations Other Than War (OOTW) in complex and urban terrain.

Working through this example has allowed us to show how the FINC methodology evaluates possible organizational and technical improvements to a C4ISR architecture.

The FINC methodology has been validated through a number of simulation experiments [2–4] and has been effective in predicting relative performance in several different kinds of scenario.

Although the FINC methodology still requires further validation and refinement, this example provides a demonstration of its potential for evaluating improvements to C4ISR and NCW architectures.

ACKNOWLEDGEMENTS

The author is indebted to Bernard Colbert, Gina Kingston, and Robert Mun for helpful comments on an earlier draft of this paper.

REFERENCES

- [1] D. Alberts, J. Garstka and F. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, (US) Department of Defense C4ISR Cooperative Research Program Publications Series, 1999. Available online at http://www.dodccrp.org/publications/pdf/Alberts_NCW.pdf.
- [2] A. Dekker, *C4ISR Architectures, Social Network Analysis and the FINC Methodology: an Experiment in Military Organisational Structure*, DSTO Report DSTO-GD-0313, Jan 2002. Available online at www.dsto.defence.gov.au/corporate/reports/DSTO-GD-0313.pdf.
- [3] A. Dekker, *Applying the FINC (Force, Intelligence, Networking and C2) Methodology to the Land Environment*, DSTO Report DSTO-GD-0341, Oct 2002. Available online at www.dsto.defence.gov.au/corporate/reports/DSTO-GD-0341.pdf.
- [4] A. Dekker, "Simulating Network Robustness: Two Perspectives on Reality," *Proceedings of SimTecT Conference*, National Convention Centre, Canberra, 2004. Available at www.acm.org/~dekker/Dekker.SimTecT.pdf.
- [5] M. Bowden, *Black Hawk Down*, Bantam Press, 1999.
- [6] R. Neillands, *In the Combat Zone: Special Forces Since 1945*, Orion, 1998.
- [7] C. Beckwith and D. Knox, *Delta Force*, Harcourt Brace Jovanovich, 1983.
- [8] E. Haney, *Inside Delta Force*, Bantam, 2002.
- [9] P. Harclerode, *Secret Soldiers: Special Forces in the War against Terrorism*, Cassell, 2000.
- [10] T. Clancy and J. Gresham, *Special Forces: A Guided Tour of U.S. Army Special Forces*, Sidgwick & Jackson, 2001.
- [11] T. Clark and T. Moon, "Interoperability for Joint and Coalition Operations," *Australian Defence Force Journal*, No. 151, pp. 23–36, Nov/Dec 2001. Available online at www.defence.gov.au/publications/dfj/adfj151.pdf.
- [12] L. Sproull and S. Kiesler, "Computers, Networks, and Work," *Scientific American*, Sep 1991.
- [13] A. Dekker, "Visualisation of Social Networks using CAVALIER," *Proceedings of the Australian Symposium on Information Visualisation*, Sydney, Australia, 3–4 Dec 2001. Available at crpit.com/confpapers/CRPITV9Dekker.pdf.

Anthony Dekker obtained his PhD from the University of Tasmania in 1991. Following a number of years as a lecturer in Computer Science at Griffith University and the National University of Singapore, he joined the Defence Science and Technology Organisation (DSTO) in Canberra, where his interests include agent-based simulation, NCW, network theory, and organisational issues. He can be contacted by email at dekker@ACM.org.