Boundary Management and Integration Framework for a Joint Cyber Defence Capability for Military Forces: Analysis and Synthesis from a Through-Life Capability Management Perspective

J H S Roodt[1], R Oosthuizen[2], J C Jansen van Vuuren[1]

[1]Defence Peace Safety and Security: CSIR, Pretoria, South Africa
[2]Monzé Consultants, Pretoria, South Africa

jan.roodt.nz@gmail.com
monze@mweb.co.za
jjvvuuren@csir.co.za

Abstract: An Operational Capability for Joint Cyber Defence (JCD) must be extended in South Africa and an investigation was launched firstly to direct current Information Warfare definition and capability management activities toward establishing a Required Operational Capability (ROC) statement for a JCD capability, and secondly to provide a framework for the development of a directed and sustainable JCD capability.

Currently the focus is on two areas; one is aimed at the lower levels of the systems hierarchy to develop the capabilities needed in information infrastructure defence and the second is aimed at establishing a capability at the strategic and operational levels, to aid in decision making at the level of force design. The paper reports on the development of a framework for the JCD system. The motivation for the framework is to support a cost effective and innovative approach to capability development in this area, and to develop an understanding of the operational and functional interdependencies of widely accepted domains of cyber defence.

With this in mind, an assessment and decision support capability is proposed and discussed, relying on simulation and modelling tools amongst others, noting current thinking in organisational dynamics and complexity theory. An initial model is described that shows how mission requirements and the JCD Capability (and in fact, any other similar capability) may be synthesised into a coherent capability design. It is recommended that a mission-based, through-life capability management-driven acquisition approach be adopted toward establishing an effective and sustainable JCD capability, supported by a national decision making and analysis competence.

Keywords: Information Warfare, Joint Cyber Defence, Capability Life Cycle, Capability Management, Capability Readiness Levels, Joint Cyber Defence Framework

1. Introduction

Delineation of boundaries is an important first step in the development of a conceptual model and understanding of a system (Rosenhead & Mingers 2001). It delimits the scope of the problem space of interest, it implies the time frame relevant to the investigation and it shows how the system fits into the environment (Mingers 2006). More-over, boundaries may be used to establish where other systems connect to the system or how it is open to communication (messages). Establishing the boundary of a complex system-of-systems (the JCD capability may be viewed as such a system) is a rather difficult exercise and one can safely claim that the boundaries will be fuzzy and permeable. This is expected to be the case for a man-made organisational system where the boundaries are often a function of the views of the original boundary setting agent or as it evolved from “natural requirements”, and although there may be physical boundaries, the more subtle societal and organisational boundaries my change over time and under the investigative eyes of later designers and managers of such systems.

This paper reports on definition and capability management activities toward establishing a ROC statement for a JCD capability, and secondly, it will describe a framework for the development of a directed and sustainable JCD capability within the South African context, which is not much different from the needs of other nations (Kerr, Phaal & Probert). The "as-is" situation and boundaries are described in the next section, the integration framework is established in section 3 and in section 4 the conceptual model is discussed. The paper concludes with proposals for future work.

2. The current situation and boundary definition

2.1 Current strategic capability design and changing environment

South Africa is a rapidly developing economy with a stated goal by government to roll out internet connectivity to the nation. The access to a new data link on the east coast of Africa will increase bandwidth availability, with the expected increase in cyber attacks on the civil networks in the country. As in other countries, the Department of Defence (DoD) is well aware of this threat, and it is also aware of the role of the cyber domain in modern defence missions. The current strategic level design is depicted in Figure 1 (adapted from Schür) and highlights the importance of the cyber dimension.

Figure 1: Typical strategic design of a defence capability

Although the Effecting Portfolio is shown as four discrete elements, it is understood that the integration is implied at the mission level.

2.2 The current JCD design

In South Africa the current JCD capability design consists of six domains (Brazzoli). This design was developed about 10 years ago from a theoretical understanding (Libicki) of what defence capability would be needed in the cyber or information domain and is decidedly similar to designs in other countries. The model is shown in
Figure **2** and it is described on the next page.

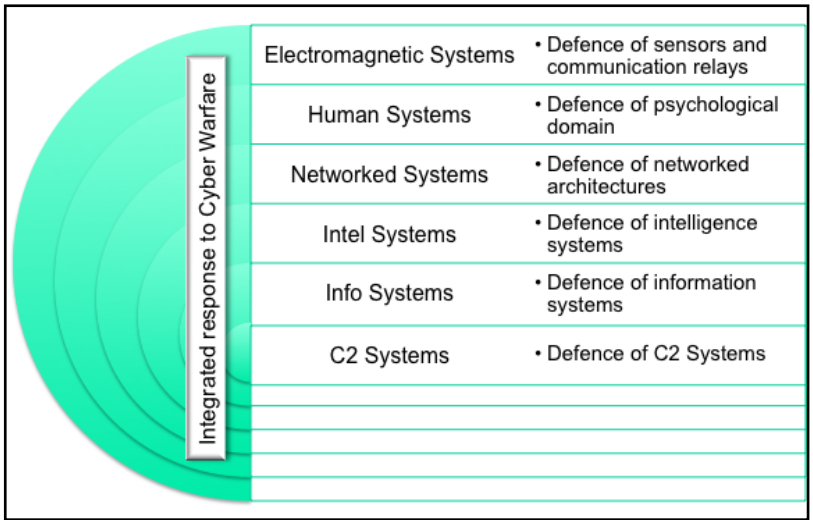

Figure 2: JCD design elements

The six domains can be described as follows (Brazzoli) in the context of Libicki's original work on Information Warfare. For clarity and reference purposes we stick to the terminology used in the work of Brazzoli:

- *Network Warfare (NW).* This signifies the ability to exploit or use the Information Systems (offensive) of an adversary and to protect all Information Systems (defensive) to ensure use of own forces.
- *Electronic Warfare (EW).* The military action involving the use of electromagnetic energy to determine, exploit, reduce or prevent hostile use of the electromagnetic spectrum while retaining its friendly use.
- *Psychological Operations (PO).* Psychological activities, including political, economic and military actions, in peace, military operations other than war, and war, directed to an enemy and/or foreign friendly and neutral audiences (internal audiences in exceptional mandated circumstances), in order to influence their emotions, motives, objective reasoning and ultimately, attitudes and behaviour, to secure the achievement of national and military objectives.
- *Information Infrastructure Warfare (IIW).* IIW involves the protection of own information systems, information-based processes and computer-based networks and attacks on the opponent's information systems, information-based processes and computer-based networks. This can be achieved via the network or by means of physical attacks.
- *Intelligence Based Warfare (IBW).* IBW concerns itself with enhancing situation awareness at the operational and tactical level. It enhances own sensor to shooter effectiveness and timeliness, as well as degrades that of the enemy.
- *Command and Control Warfare (C2W).* It is the military directive that implements IW on the battlefield and integrates physical destruction. Its objective is decapitating the enemy's command structure from its body of command forces.

The six domains are divided into two categories, namely application and enabling domains, which relate to one another in a "cause and effect" manner as illustrated in Figure 3 (derived from Willers).

- *Enabling Domain.* This domain consists of the mechanisms contained within the force structure elements to conduct cyber defence. These mechanisms are contained within the domains of NW, EW, and PO.
- *Application Domain.* This domain consists of application elements, which utilises one or more mechanisms of the enabling domain. These elements are contained within the domains of C2W, IBW, and IIW.

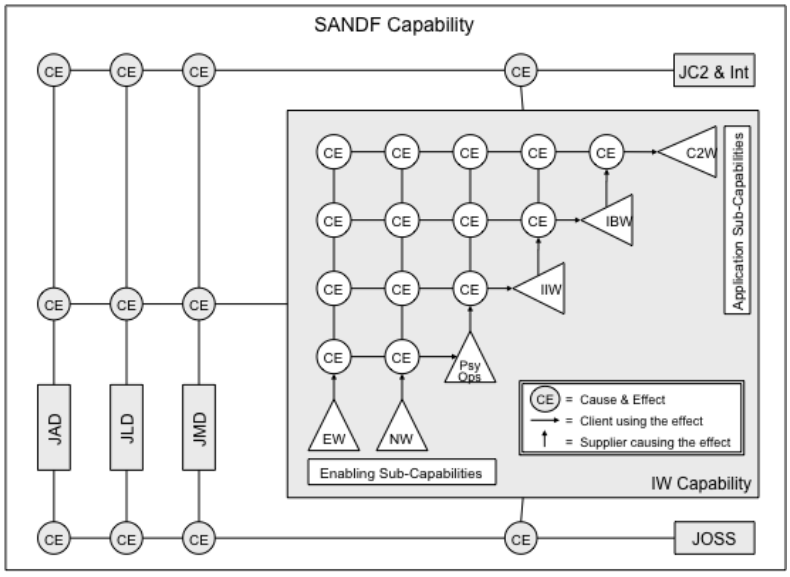

Figure 3: Enabling and Application domains of a JCD

Initial theoretical work and the basic applications thereof in the information domain focus mainly in the area of NW and broadly at the strategic/operational level of Command and Control (C2). The third domain that has traditionally received much attention is EW. This domain will be assumed to be adequately populated for the purposes of this paper.

However, there is something far more perturbing about the previous figure. This diagram shows the inherent connectedness of the field and it demonstrates vividly why one cannot focus on one domain alone at a time and expect to make impact. This is the hallmark of a classic wicked problem and it calls for artful culling and pruning of interdependencies so as to retain the core characteristics of the problem whilst modeling it in such a way that one can start to understand the system. Only once it is understood can one start to develop an appropriate body of knowledge for it (Cilliers 2007).

3. Integration framework and views

From another perspective, the JCD capability must fit, broadly seen, within a life cycle of technologies, organisational process and the human component. In this paper only the capability life cycle, the core C2 process and organisational readiness will be discussed, although a much broader selection of views were considered.

3.1 Capability life cycle

The JCD capability is addressed in context of the Capability Life Cycle (CLC) illustrated in Figure 4. It is important to note that elements of the JCD capability may be in different CLC stages at any particular point in time. The process is briefly described in the ensuing sub-paragraphs.

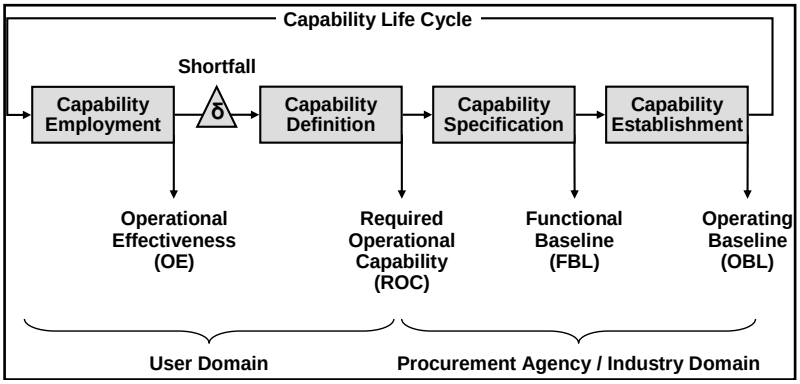

Figure 4: Capability Life Cycle concept

Note that the process is also continuous if legacy systems are in operation.

- *Capability Employment:* Systems are commissioned and their operational effectiveness (OE) is regularly assessed to determine any shortcomings.
- *Capability Definition*: If an OE shortfall is identified, the capability needed to rectify the shortfall is defined, leading to a ROC, which is the trigger for the acquisition process.
- *Capability Specification:* This stage encompasses translation of user requirements as documented in the ROC to technical requirements representing a Functional Baseline (FBL), the basis for contracting to industry.
- *Capability Establishment:* The contracted capability requirements are transformed into Products Systems that are fielded into the operating environment where they are employed as User Systems. Delivery is associated with an Operating Baseline (OBL) documenting the baseline of the “as-delivered” Products System.

The EW and NW domains have been receiving disproportionate attention. In terms of the CLC this is interpreted to imply that EW and NW exist in all CLC stages, whilst care must be taken to ensure that

other domains are developed in a balanced manner to the required level so as to ensure an integrated JCD capability.

3.2 Command and Control at the core

Cyber Defence is by definition directed at information protection and as such has a strong bearing on C2 functionality in any system. It is therefore contended that the C2W domain should be regarded as the pinnacle of the JCD capability from an operational perspective. This is borne out by the information process relationships described below:

- *Information Sensing:* For information to exist, it needs to be gathered in some way or another. This is achieved via the enabling components of the capability, namely EW, NW and PsyOps.
- *Information Processing: Data and information gathered is processed into relevant and usable information*/intelligence.
- *Command & Control:* Processed information/intelligence is utilised to establish situation awareness in the minds of decision makers or commanders, which enables planning, tasking and control.
- *Infrastructure*: Data and information are disseminated and processed by means of an infrastructure comprising communications media and computers.

From the above it is evident that the entire process of data and information gathering, dissemination, processing and presentation is aimed at informing the decision maker or commander responsible for the operation. As was mentioned, these elements are highly interconnected, with negative and positive feedback loops ingrained in them. This process underlying decision making lies at the heart of C2 and must be protected at all cost.

3.3 Capability design and readiness

An effective capability comprises elements as typically described in a framework for strategic military capabilities (Kerr, Phaal & Probert). The framework used in South Africa - Figure 5: (Schür) - is called POSTEDFIT (Personnel, Organisation, Sustainment, Training, Equipment, Doctrine, Facilities, Information and Technology). This implies that all POSTEDFIT elements should be addressed during acquisition in order to ensure an effective and sustainable JCD capability.

Figure 5: JCD Capability in acquisition context

The concept of capability readiness levels depicted in Figure 6 is a means of managing the readiness levels of the capability system elements commensurate with the perceived level of threat, or the actual probability of utilising (employing) the capability (Oosthuizen & Roodt). Capability readiness is directly related to cost and therefore the cost of a specific capability at any particular point in time may be moderated by pitching at a lower level of capability readiness. For example, it may be sufficient to retain a capability at a demonstrator level in times of peace, allowing the capability to be enhanced to a core force or war fighting capability in times of escalating hostilities. In the latter case the government will be inclined to appropriate additional funds to the defence budget as the imperative to protect the country rises.

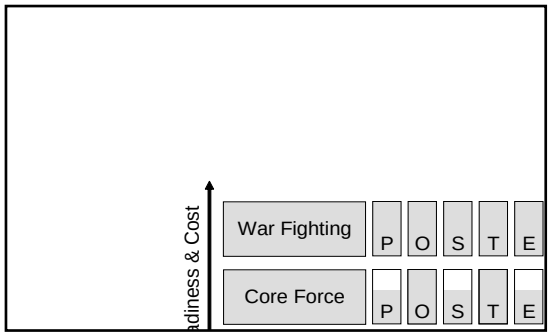

Figure 6: Concept of JCD capability readiness

3.4 Summary

Several dimensions must be considered as part of the framework for JCD capability establishment, integration and utilisation. The strategic design of the force and its life cycle, the core process of C2 and the level of readiness commensurate with the threat were discussed. Combining this with the current state of the capability may be used to construct a decision process to develop a JCD capability. This will be discussed in the next section.

4. Development of a decision support model for JCD capability establishment

Uncertainty surrounding decision-making is highest in the earlier phases of the CLC due to the long time span between requirements definition and the realisation thereof. It is suggested that different levels of capability acquisition are represented in the Cynefin framework illustrated in Figure 7.

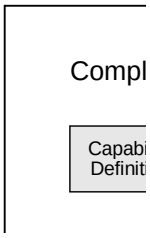

Figure 7: CLC Stages in Cynefin Context (Snowden 2007)

- *Simple:* The relationship between cause and effect is obvious to all. Entities may be categorised, this is the domain of “Best Practice”. There are clear causal relationships, easily discernable by everybody.
- *Complicated:* The relationship between cause and effect requires analysis or others form of investigation and/or the application of expert knowledge. Multiple “right” answers exist and although causal relationships are there, not everybody can see them.
- *Complex:* The relationship between cause and effect cannot be perceived in advance, but only in retrospect. This is known as emergence, and by doing experiments in a so-called

"safe-to-fail" environment, it is possible to discern instructive patterns. Appropriate models in the right simulation environments may be used as laboratories to discover these patterns.

- *Chaotic:* There is no relationship between cause and effect at systems level. Here it is pointless looking for the right answers or cause of action and rapid response is often the only way of dealing with the situation.
- *Disorder:* Multiple perspectives may exist we are in a position of not knowing what type of causality exists, in which state people will revert to their own comfort zone in making a decision.

Decision making in the CLC Capability Definition stage is immersed in a complex environment, requiring problem solving approaches and tools suitable for complex environments (Pidd 1996). A possible solution is to follow the approach below, which structures wicked problems from the Cynefin Complex region into manageable elements (Roodt 2007).

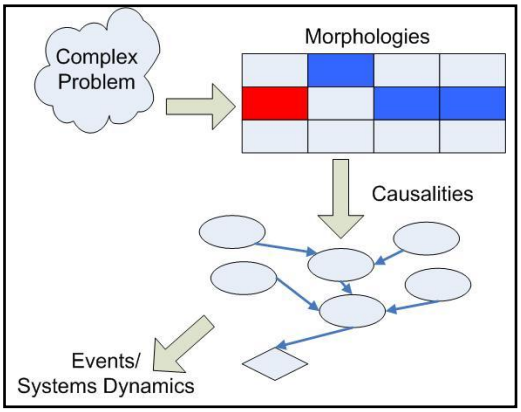

Figure 8: Cascading a wicked problem into manageable solution spaces

It was stated earlier that the inherent reliance of each element on most other elements is cause for concern. A way must be found to chunk together pieces of the system that makes sense within a certain context.

Starting with a set of scenarios focused on the JCD domains it is possible to develop a morphological field (Ritchey 2006) with interdependencies that may possibly be cascaded onto a causal network (Pearl 2000, Jensen 2001, De Waal & Ritchey 2007), effectively moving from a non-quantitative model to a quantitative model. At the same time, using the arguments around the importance of C2W, it is possible to devise a model framework to show how the six domains influence each other, and how Boyd's OODA (Observe, Orientate, Decide and Act) loop influences it, effectively guiding the development of the causal networks that follows from the morphological map. At this time the possibility of automated discovery of the causal networks are being considered (Neapolitan 2004), but the concept is being tested with more traditional human-in-the-loop approaches for now

The framework illustrated in Figure 9, based on the integrated JCD capability diagram in Figure 3 is proposed as a point of departure. In Figure 9 the logical (and possibly causal) relationship between JCD constituents and their association with JCD implementation layers is suggested. The layers represent different aspects of the sensing, disseminating, processing and presentation functions underlying the transformation of sensed data into information/intelligence presented in the form of situation pictures to decision makers at different levels and positions (C2 nodes) throughout the organisation. These layers are capped by the cognitive layer, which as the name suggests, addresses the decision maker who is the user of the information/intelligence presented and a key determinant in the efficiency and effectiveness of the decision cycle represented by the OODA loop.

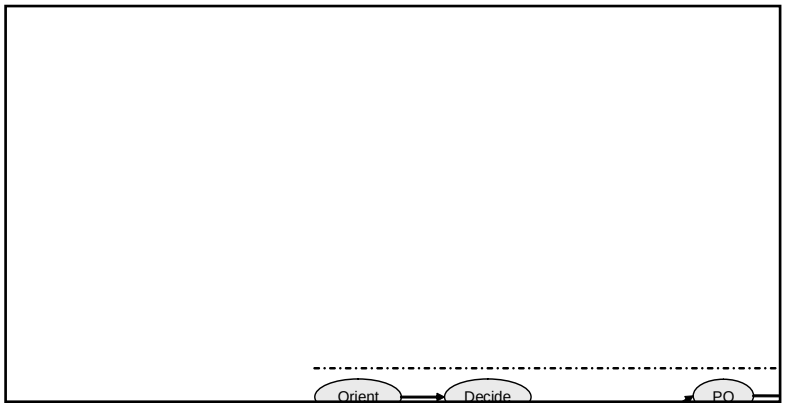

Figure 9: JCD analysis framework

It is understood that the system under investigation here is not decomposable in some of its functions, but that it is also decomposable along other lines. There is definitely a certain hierarchical view that can be employed when one attempts the modeling of the system. This is to be expected of a complex system (Simon 1962, interpreted by Cilliers 2007). Using this understanding and the view depicted in Figure 9, it is possible to attempt the cascading approach discussed earlier. This cascading will allow us to do the chunking of coherent pieces of the system, maintaining the “meaning” and “intent” of the system.

It is suggested that C2W is the "leading" area in the causal relationship amongst domains, the reason for this being that it addresses the very essence of “traditional” IW, ie all JCD actions are directed toward supporting the decision maker’s objectives that live in the C2 domain as indicated by the OODA loop surrounding the C2W domain in the diagram. This framework could serve as the basis for developing a "generic benchmark" model for JCD at various levels of abstraction.

This approach was implemented using a hypothetical set of scenarios and a simple hypothetical JCD capability. The results are shown below to illustrate the approach.

In the first morphological map (Figure 10), a set of scenarios is described in terms of five (perceived) key dimensions. Each dimension has several “states” and in each dimension, any number of the states may be found to be coherent with a scenario. The consistency is arrived at by consensus of a small group of subject matter experts.

Scenario	**Sanctioning Agent**	**Coalition Role**	**Cultural Climate**	Environment an Supply Chain	Types of Ops
Lawrence of Arabia	AU	Leader	Religion & ethnic driven strain	Desert and arid regions	Peace Keeping
Horn of Africa	UN	Equal	Dictator driven	Jungle	Peace Enforcement
West Africa	SADC	Follower	Natural resource exploitation	Savanna	Election support
SADC	South Africa			Coastal	Resource policing
Naval Safety and Security				Urban	
Neighbouring States					
Casablanca: Francophone North Africa					

Figure 10: Scenario morphology

In the second map (Figure 11), the scenarios are linked to dimension of interoperability, electronic warfare and the remaining five JCD domains. As was stated, the model is simplistic to say the least, but was developed to demonstrate the approach.

It is now possible to develop a causal diagram with the scenarios at the centre, an axis through which the required level of capability may be linked to the specifics of a scenario. The model uses a Bayesian inference engine and will allow forward and backward propagation of "probabilities". In the example shown in Figure 12, the question to be answered is: "Under what scenarios would a full jamming capability be needed?". The answer is that it would most probably be needed during a naval campaign, or that it would be deployed during such a campaign, and typically during a resource policing operation.

Interoperability	EW Capability	IW Capability	Scenarios
Coalition (international civilian & governmental (Integration)	Advanced, full integration Offensive (O)	NW: Full info assurance CERT (D)	Lawrence of Arabia
National (civilian, military & private public) Integration	Advanced, full protection Defensive (D)	PsyOps: Total Defensive Mil & Civ – Total awareness & monitoring (D)	Horn of Africa
Government Departmental	Full counter measures Offensive (O)	IBW: Information jamming (O)	West Africa
DoD (Inter-Services & Inter-Divisions)	Full jamming Defensive (D)	C2W: Own OODA protection Decision support tools(D)	SADC
Intra-Service & Inter-Divisions)	Basic offensive. No spread spectrum (O)	IIW: Full own FMECA on NII (D)	Naval Safety and Security
No Integration	Basic Defensive No crypto (D)		Neighbouring States
	No capability		Casablanca: Francophone North Africa (Maghreb)

Figure 11: Interoperability and cyber dimensions linked to scenarios

The value of such a simple model is that it stimulates debate and develops the story lines and needs statements that can subsequently be used to develop more elaborate models and derive requirements. It is also possible to develop operational level models using system dynamics models to test assumption in the arguments used to develop these models.

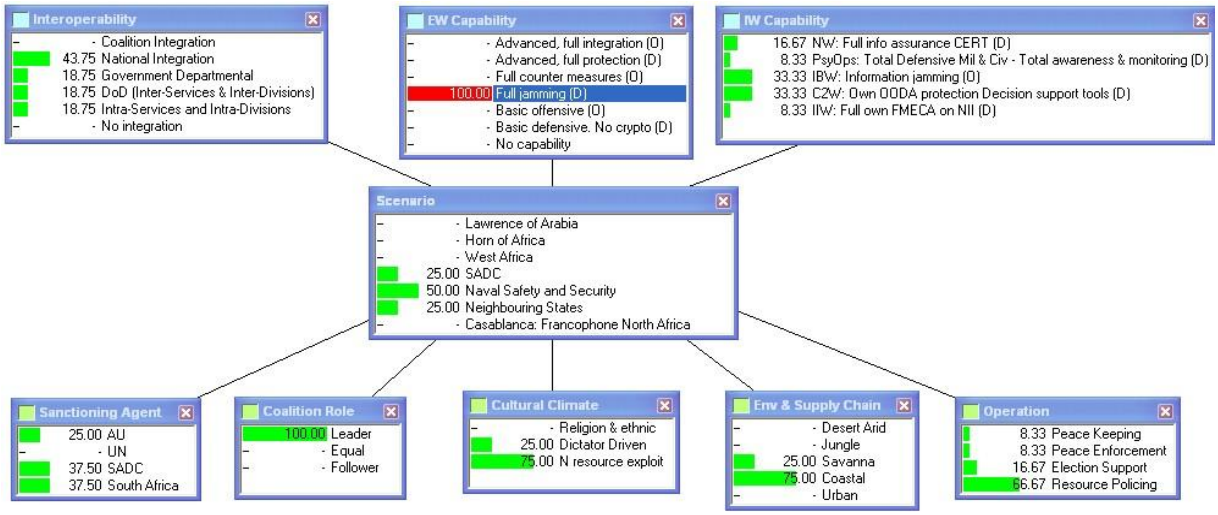

Figure 12: Using the inference engine to establish capability requirements.

5. Conclusion

The development of a framework for establishing an effective, integrated and sustainable JCD capability was discussed. The framework builds on current "traditional" IW and modern JCD concepts and design whereby the JCD capability is expressed in the form of six domains, with a "cause and effect" relationship amongst them.

The capability establishment framework is based on a whole life approach expressed in the form of the CLC, which gives context to the possibility that different domains of the capability may be in different CLC stages and thus at different levels of maturity. It is contended that JCD must be considered in C2 context with the decision cycle at the core.

Furthermore, the JCD capability is expressed in the form of nine POSTEDFIT organizational system elements (congruent with the current drive for integrated capability design), which must all be in place in order to ensure an effective capability. The concept of capability readiness is presented whereby the realised JCD capability may be linked to the perceived level of threat in order to manage the cost dimension over the CLC.

The decision support model for establishing a JCD capability is based on the premise that capability definition is a wicked problem residing in the complex domain of the Cynefin framework. This requires problem solving approaches and tools suitable for complex environments, including Morphological Analyses and Bayesian Belief Networks. A JCD analysis framework is proposed based on the OODA decision cycle and JCD capability implementation layers as was graphically illustrated.

Finally, It is proposed that the JCD analysis framework be used as basis for further work in order to develop an understanding of the operational and functional interdependencies of the JCD domains. Once this has been achieved the establishment of a JCD capability can commence based on modeling and simulation tools underlying current thinking in organisational dynamics and complexity theory. One would then also start to seriously consider the system dynamics.

References

Brazzoli, M.S. (2007). *Future Prospects of Information Warfare and Particularly Psychological Operations,* in Le Roux, L. (Ed.). *South African Army Vision 2020: Security Challenges Shaping the Future South African Army,* Institute for Security Studies, Tshwane, South Africa.

Cilliers, P. (2007). *Knowledge, Complexity and Understanding,* in Cilliers, P (Ed) *Thinking Complexity-Complexity and Philosophy Vol 1,* ISCE Publishing, Mansfield, MA.

De Waal, A. and Ritchey T. (2007). *Combining morphological analysis and Bayesian networks for strategic decision support,* ORiON Vol 23(2), http://www.orssa.org.za

Jensen, F.V. (2001). *Bayesian Networks and Decision Graphs,* Springer, New York.

Kerr, C., Phaal, R. & Probert, D. (2006). *A Framework for Strategic Military Capabilities in Defense Transformation,* 11th ICCRTS Track 9: Network Centric Metrics, last accessed on the World Wide Web at http://www.dodccrp.org/events/11th_ICCRTS/iccrts_main.html

Libicki, M.C. (1995). *What is Information Warfare,* National Defence University Publication, USA Government Printing Office, Washington.

Mingers, J. (2006). *Realising Systems Thinking*, Springer, New York.

Neapolitan, R.E. (2004). *Learning Bayesian Networks,* Pearson Prentice Hall, Upper Saddle River NJ.

Oosthuizen, R., Roodt J.H.S. (2008). *Credible Defence Capability: Command and Control at the Core*, Land Warfare Conference 2008, Brisbane, Australia.

Pearl, J. (2000). *Causality: Models, Reasoning and Inference,* Cambridge University Press, Cambridge.

Pidd, M. (1996). *Tools for thinking - modeling in management science,* Wiley, New York.

Ritchey, T. (2006). *Problem structuring using computer-aided morphological analysis,* Journal of the Operational Research Society.

Roodt, J.H.S. (2007). *Non-quantitative modeling as a framework for the analysis of complex systems* in Richardson, K.A. & Cilliers, P. (Eds) *Explorations in Complexity Thinking*, ISCE Publishing, Mansfield MA.

Rosenhead, J. and Mingers, J. (Eds) (2001). *Rational Analysis for a Problematic World Revisited*, Wiley, New York.

Schür, O.A. (2007). *Presentation on Department of Defence Acquisition Process, Revised Acquisition Priorities and Strategic Industry Requirements,* South African Aerospace, Maritime and Defence Industries Association, Centurion, South Africa, last accessed on the World Wide Web at http://www.amd.org.za/docs/Acquisition_Process_-_30_Aug_07.pdf

Simon, H. (1962). *The architecture of complexity,* As reprinted (2007) with introduction by Paul Cilliers in Richardson, K.A. & Goldstein, J.A. (Eds) *Classic Complexity – From the abstract to the concrete,* ISCE Publishing, Mansfield MA.

Snowden, D.J. and Boone, M.E., (2007). *A Leader's Framework for Decision Making*, [online], Harvard Business Review Reprints, R0117C, last accessed on the World Wide Web at www.hbrreprints.org.

Willers, C.J. (2006), *Integrated Information Warfare in the Context of Situational Awareness and Command and Control,* ISSUP Bulletin – Institute for Security Studies, University of Pretoria, South Africa.