Interoperability in CNO and EW: Considerations for the African Continent

Brett van Niekerk

School of Information Systems and Technology

University of KwaZulu-Natal

Abstract

With the Internet, email and cellular phones enabled with Bluetooth, MMS and SMS one might take for granted the ease with which information can be distributed and managed. However, in information warfare (IW) environments, a false sense of security may result in simple oversights that could prove disastrous; crucial information is not delivered on time due to compatibility issues, or a new electronic warfare (EW) device rushed into service inadvertently interferes with a coalition partner's communications at a critical moment. Effective management of systems, personnel, equipment, operations, and the electronic spectrum can greatly minimise the risk of incidents and aid in the efficient completion of operations.

This paper focuses on considerations for interoperability in Computer Network Operations (CNO) and EW operations. Whilst these two areas of IW can be considered separate, the increase of wireless technology for networking purposes brings these two areas together. Real world examples from recent conflicts will be used to illustrate possible effects of oversights or mismanagement in joint IW operations, as well as the successes achieved. Concepts and models from Business Information Systems will be used to model and describe CNO and EW systems and their roles, both on the battlefield and in a supporting role. These considerations will be applied to a context for the African continent, with a discussion on potential limitations and solutions to effective interoperability.

1. Introduction

With the advancement in communications technology, where cell phones can connect with computers through WLAN and Bluetooth, or act as portable wireless modems, one may be forgiven for assuming that compatibility issues are a thing of the past, especially as these technologies are becoming more common and standardised. However compatibility oversights may cause delays to projects while the problems are ironed out. In a hostile environment such an oversight could prove to be fatal, or seriously jeopardise missions.

To successfully achieve interoperability, be it a multinational military task force or between the military and industry, there needs to be a minimum level of compatibility with the respective systems employed, and effective management and administration policies and procedures to aid seamless integration amongst the various parties involved. With EW and CNO the probability of electronic fratricide are greatly increased due to the very nature of the disciplines; they have the capability of disrupting communications and information systems, and can therefore accidentally interfere with friendly systems and operations.

Whilst EW and CNO can be considered different disciplines, there are a number of underlying principles that are common to both, which will be introduced. Information systems models and management tools will be described in order to analyse interoperability in CNO and EW. Real world and hypothetical examples are used to illustrate limitations and hindrances, in the form of incompatibility, and possible solutions to interoperability in EW and CNO. These limitations and solutions are then applied to the unique and complex environments of the African continent.

1.1 Definitions

Information Warfare can be defined as "*all actions taken to defend the military's information-based processes, information systems and communications networks and to destroy, neutralise or exploit the enemy's similar capabilities within the physical, information and cognitive domains*" (Brazzoli, 2007). Information Operations (IO) is an extension of IW to include the use of information in warfare (or business) – such as the collection, dissemination and storage of information and data.

Electronic Warfare can be defined as preventing hostile use of the electromagnetic (EM) spectrum whilst preserving its availability for 'friendly' use. It is traditionally based on radio-frequency jamming and counter-jamming, for both radar and communications. It is comprised of three main components: Electronic Attack (EA) – actively disrupting and denying an adversary's use of the EM spectrum via use of jamming, deception and directed energy weapons; Electronic Protection (EP) – using passive and active methods to protect friendly EM spectrum accessibility and war fighting units from both adversary and friendly EW; and Electronic Support (ES) – this constitutes threat warning, direction finding and collection in support of EW.

There is no standard definition for CNO; Zehetner (2004) describes CNO and Brazzoli (2007) describes Computer Network Warfare (CNW) as comprising of Computer Network Attack (CNA) and Computer Network Defence (CND), whereas the U.S. Department of the Army (DoA) (2003) considers CNO to be separate from CNA and CND. Borque (2008b: 38) quotes the Principle Undersecretary of Defense in defining CNO or "Operations in Cyberspace" as "*digitally-based operations designed to attack, defend, exploit and maintain Cyberspace and the data within it.*" Smith & Knight (2005) propose a new term: Computer Network Support (CNS), which, like ES, comprises of threat warning and collection in aid of CNW. For the purposes of this paper a similar definition will be used for CNO, will be considered to comprise of CNW (CNA and CND), CNS and general management and operation of networks and information systems to "maintain cyberspace" (Borque, 2008b).

Interoperability is the ability of various 'groups' to 'connect' and work together as a single unit. For the purposes of this paper interoperability will include; multi-service within the military, multi-national military, military-civilian (such as emergency services, industry, and universities). At a systems level, interoperability is "the capability of information systems working together as a system-of-systems" (DoA FM 100-6, cited in: Curts & Campbell, 2001: 38).

1.2 Business and Management Information System Models

Information systems can be broken into three distinct areas or domains: Hardware, Software and Persware. Hardware consists of the physical computers, communications links, cables, routers and other devices that form the information system. This can form the physical domain of IW. Software is the operating systems, applications and code that runs on the hardware, and corresponds to the information domain of IW. The software provides an 'interface' between the hardware and persware. Persware is the people operating the hardware and software (the cognitive domain of IW). This model holds true for CNO. Applying this model to an EW system, we can arrive at the antennae and displays forms the hardware component, the operator is the persware, and the software processes information from the receiver to present to the operator on the displays, and in turn process inputs from the operator to provide the required output at the transmitter.

In management information systems an enterprise system is an integrated organisation-wide information system that coordinates key internal processes of the organisation (Laudon & Laudon, 2004). It acts as middleware and integrates and coordinates different information systems and processes, and can model and automate processes within the organisation, thereby reducing inefficiencies and addressing incompatibility between different information systems.

The IFIP-IFAC Task Force (1999) developed a framework for integrating enterprises called the Generalised Enterprise Reference Architecture and Methodology (GERAM). The GERAM framework

aims to integrate enterprises by removing boundaries and promoting interoperability, and focuses on three domains: the human, technology, and processes. This is again analogous to the cognitive, physical and information domains; however there is allowance for modelling the interaction between the domains, such as the human-technology interaction and technology supporting the processes. To allow for maintaining and improving interoperability there is a 'feedback loop' where the models can be analysed and evaluated and adapted to a changing environment as needed.

2. EW versus CNO

Borque (2008a, 2008b) argues that CNO and EW are separate entities; that EW is older and more established, has been proven to be able to operate in some areas of CNO and in broader areas, whereas Cyberspace only overlaps in a very small range of the EM Spectrum (and therefore cannot incorporate the EW mission area; it is a "client" of EW) and is still a new and developing concept. This is supported by Kunkel (2008), in that it has been proposed that the definition of Cyberspace Operations no longer encompass EW. Borque (2008b) does acknowledge that EW can operate in support of CNO, and that it also has the ability to create effects in or through cyberspace. It should be noted therefore, that as wireless is becoming more prevalent in cyberspace, they are presenting themselves more readily as targets for EW, as indicated in Joint Chiefs of Staff (JCS) (2007):

> "*Computer network operations (CNO) may be facilitated and/or enabled through EW. The increasing prevalence of wireless internet and telephone networks in the operational environment has created a wide range of opportunities and vulnerabilities when EW and CNO tactics, techniques and procedures are used synergistically.*"

Wireless transmitters are susceptible to direction finding, and can be more easily interfered with and intercepted through EW methods than wired communications networks. EW and CNO can therefore complement each other in that EW can interfere with or deny use of the physical network (the wireless communications link) and CNO can interfere with the information content. For example, a radio broadcast can be jammed using EW, and CNO can disrupt any attempts to allowing 'streaming' audio over the internet.

Hoad & Jones (2004) discuss possible EM threats to information security, in particular information systems and networks; whilst they distinguish these threats from EW, many of the concepts presented may be conducted using EW systems. Smith & Knight (2005) illustrate parallel concepts of EW and CNW, a summary of which can be seen in Table 1.

Table 1.: Analogies Between EW and CNW

EW	CNW
Jamming	Denial-of-Service (DOS) Attack
Decoys & Chaff / Flare Dispensers	Honey Pots & Honey Nets
Identification Friend or Foe (IFF)	Public Key Infrastructure & Firewalls
Low-Observability Platforms	Virtual Private Network, Root-kits
Radar Warning Receiver	Firewalls
Electronic Intelligence (ELINT)	Sniffers, Scanners & Backdoors
Radar, Electronic Support System	Intrusion Detection Systems & Firewalls
Adapted from Smith & Knight (2005)	

Just as EW can act into or through cyberspace, it may be possible for the effects of CNW to be felt in the EW sphere; for example if a CNA disrupts an air defence network, thereby removing the threat of radar. From these examples we can consider EW and CNO to be 'closely related.' As there are

parallels in concepts, therefore one can develop parallels in command and management considerations for EW and CNO, which can be extended to joint operations.

3. CNO and EW 'Management' for Interoperability

To fully understand the complexities of managing EW and CNO, some examples should be mentioned to illustrate what can be achieved through effective command, management and administration, and potential problems due to oversights and uncertainty. Luddy (2005) gives the examples of Special Forces using laptops to call in B-52 strategic bombers for close air support, and UAVs networking with other surveillance platforms to provide real-time strategic intelligence and in support of manoeuvre forces. However, Luddy (2005) also points out that there are still shortcomings; in-compatible communications had to be routed through E3 AWACS aircraft, and there were incidents of fratricide. Huber et al. (2007) also mention the problem of fratricide due to accidentally detonated Improvised Explosive Devices (IEDs), and goes on to describe how an Improvised Explosive Device (IED) jammer interfered with radio communications and an EW aircraft accidentally jammed friendly psychological operations broadcasts during Operation Desert Storm due to uncertainty of frequencies and operating times. Vanden Brook (2007) and Eshel (2007) also mention the IED jammers interfering with friendly communications. Eshel (2007) comments on EW aircraft prematurely detonating IEDs along convoy routes, however Huber et al (2007) warn that the transmissions from the aircraft could encroach on adjacent areas of operation.

After the 9/11 attacks, various US agencies were unable to share required data due to technical issues (Adams, 2003). Methods for collecting, classifying and disseminating data that are incompatible may hinder inter-agency responses to crises. More recently, a US Navy section of a multi-service information sharing system was found to be incompatible as a newer standard was used compared to the other services (Hodges, 2009). Other possible scenarios may include DOS attacks interfering with friendly network scanners and sniffers, or lack of co-ordination 'wasting' EW assets on an air defence or command and control (C2) network that has already been neutralised by CNA operations. CNA specific software could be developed using a Microsoft Windows operating system, and in the field it is found that it does not produce the desired effects due to the target utilising a different operating system, and no compatibility has been designed into the software. When liasing with industry, CAD models were supplied which were, in theory, fully compatible with the software that the industry was using, however there were problems opening the files due to the fact that the computer hardware was not sufficient and the software did not have the required resources. During disaster relief the military may be called in to assist emergency services, and direct co-ordination may be hampered by the military and emergency services using different communications frequencies and incompatible information systems.

From these examples two main issues arise; compatibility and co-ordination. When various services and nationalities are involved, one cannot expect all the systems employed to be fully compatible. It may be simpler to promote cross-compatibility across branches within a single nation's military, as multi-service standards can be set in place to ensure a minimum level of compatibility in systems and procedures. Multi-national co-ordination may prove to be more difficult, as one nation cannot force another to use certain methods, systems or design criteria. Therefore the co-ordination of operations is essential.

According to Curts & Campbell (2001), the systems themselves do not need to be fully compatible; the focus should be interface and interoperable standards and procedures. This lends itself to a "middleware backbone" as proposed by Seymour et al. (2000), where a central database structure is used interface directly to various Situational Awareness (SA) systems, Command Support Systems (CSS), EW systems and other sensors through interface bridges. The middleware backbone, called the Information Management Engine (IME) is capable of basic bandwidth management and prioritisation, and should be able to be adapted to a variety of systems through the bridging interfaces.

Such a system can be considered CNO, as it helps 'maintain' cyberspace. The GERAM framework may be applied to design and assess the procedures and models and supporting infrastructure.

To deconflict the EM spectrum, Huber et al. (2007) describe a Global Electromagnetic Spectrum Information System (GEMSIS) that can provide network and spectrum management in real-time. A similar system, combined with a 'smart' IME-type information system would be able to minimise the occurrences of EM or network 'fratricide.' Such systems could improve tasking management to enable EW and CNO to better co-ordinate operations and support each other.

Prior to deployment, new technologies should be tested to determine if their EM characteristics and protection is suitable for the environment. Pfeffer (2000) advocates designing EM protection for current and future generation electronic systems, so if there is a systems upgrade, the EM protection for the systems can be re-used. Whilst the protection methods and test validation procedures he describes is primarily for the design stage, they can be adapted to determine the suitability of electronic devices prior to deployment in an attempt to assess and prevent possible interference points.

There are other limitations to interoperability for EW and CNO that can affect compatibility. The availability and cost of suitable technologies may restrict the possible solutions to less-than-ideal scenarios. Certain nations may not have the budget for basic reliable telecommunications, therefore they cannot possible acquire state-of-the-art technologies for EW or CNO. This may allow for hardware deficiencies that allow for greater interference from friendly systems. Some industries, which are predominantly profit driven, may only spend enough so that their networks and computers are only capable for their everyday requirements. Then, as in a previous example, when interoperability with the military is required their systems are not completely capable.

Another limitation to interoperability is cultural differences. Various cultures have different views on technology, and their training (or lack thereof,) doctrine and leadership regarding technology could reduce the possibility of effective interoperability, especially in CNO and EW. Each service within the military may have different views of how CNO and EW are to be employed on the battlefield and in support of operations, and their systems may have slightly different focuses. Slay (2002) extends the GERAM framework described above to include cultural differences with the aim of providing qualitative information for planning and risk assessment. This modification to the GERAM framework caters for cultural differences in general, however it does allow for different attitudes and capabilities regarding technology.

Borque (2008a) states that command of Joint EW should never fall to a single branch of the military, as the EW capabilities will favour their forces (and 'culture') and neglect the other branches. This holds true for joint CNO and the multi-national scenario, where a commander may favour his own nationality to the possible detriment of the others within the coalition. This also illustrates the need for joint training, so that possible problem areas in EW and CNO operations can be identified and resolved, and the standards and procedures can be refined. Different focus areas may be beneficial of properly co-ordinated, as this allows for mutual support and a more holistic approach.

Appendix B of JCS (1998) provides guidelines to the implementation of a Joint Operation Planning and Execution System (JOPES) for IO and some constituents, including EW. The guidelines provide considerations in terms of the situation, mission and execution thereof, administration and logistics, and C2. These planning tools take a holistic approach, and support interoperability by promoting mutual support from the various aspects of IO. The appendices of JCS (2000) provide in-depth guidance for joint EW operations planning, frequency deconfliction, EW modelling, and other methods to aid EW interoperability. Different service perspectives for EW are also catered for in Appendix F of JCS (2000). Using the analogies for EW and CNO presented above, similar procedures and tools may be derived for CNO, as in Appendix 1. The development of structured planning procedures and

standards amongst all participants in a joint operation will provide a degree of 'manageability' and decrease the opportunities for electronic fratricide.

3.1 Summary

The limitations and considerations discussed above are over and above the concerns of language barriers, logistical and 'conventional' network management. To summarise, interoperable EW and CNO may be limited by compatibility in all three domains of an information system:

Hardware/Physical – there may be incompatibility in hardware due to improper testing and validation, prohibitive costs and availability, or different design criteria.

Software/Information – different communications protocols or software may prohibit interoperability of systems, or inefficient procedures result in incorrect or insufficient information being available, increasing the probability of accidental fratricide.

Persware/Cognitive – cultural differences result in negative attitudes towards technology and its use, or inadequate training, poor leadership and inadequate doctrinal concepts may impact on the capability of the operators.

Possible solutions to these limitations is the deployment of a common 'middleware' that connects to various systems through interface bridges; those with a limited budget or availability problems will only need to be concerned with the interface bridge, while the benefit of improved information accessibility and flow would improve co-ordination. More advanced systems may be used to automate frequency deconfliction and the management of information flow, thereby reducing the risk of fratricide and enhancing co-ordination. The development of joint procedures, standards and doctrine through a GERAM-style framework and JOPES, combined with joint training and exercises will promote co-operation and mutual support, narrow cultural divides and identify potential problem areas in a controllable environment. These solutions can provide a solid platform for EW and CNO to support C2, and the some of the solutions can be expanded and applied to promote interoperability in C2 systems.

4. Considerations for the African Continent

The African Battlespace is a complex and unpredictable one; du Toit (2003) points out that it is dualistic in nature. The majority of conflicts on the continent are based on guerrilla warfare as opposed to large force-on-force wars, and the African militaries in general do not train or exercise for joint or combined operations, yet two of the poorest nations, Ethiopia and Eritrea, managed to field an array of modern weaponry. Most of the recent conflicts have revolved around ethnic clashes and civil war, and sometimes anarchy. However, despite the apparent lack of advanced militaries, there are instances where these nations can hold their own against technologically superior forces, such as in Somalia, where cellular phones were effectively used as an improvised C2 network. The genocide in Rwanda also exhibits this duality; it was carried out with ‘primitive’ machetes, yet it was instigated via radio broadcasts (Hutchinson et al., 2007). Most recent joint operations in Africa are peacekeeping efforts.

The infrastructures on the continent vary drastically; one may find that the majority of fixed-line telecommunications infrastructures are unreliable at best, yet to compensate the nations have rolled out serviceable cellular networks, which become the mainstay of their telecommunications infrastructure. The technology gaps between neighbouring countries (or even within the country itself) may be vast. Likewise, the cultural scenario is just as complex and this usually results in the ethnic clashes mentioned above, spreading to full-scale genocide in some instances.

Such conditions may make interoperability amongst African nations complicated; the limitations discussed above may come into play in the extreme; the technological and cultural gaps between allied nations could be vast. One may easily find latest-generation equipment allied with that of the Soviet-era. Even if an IME-type system could be made available and the 'legacy' equipment integrated

into the network, unfamiliarity with the concepts of interoperable CNO and EW could prevent effective integration and management of forces.

South Africa has developed the Link ZA digital network protocol, a 'home-grown' version of the North Atlantic Treaty Organisation Links 11, 16 and 22. All SA National Defence Force (SANDF) communication systems are required to be compliant with the Link ZA protocol (Anon, 2008). Link ZA, the Combat Net Interoperability Standard (CNIS), and the *XMLGateway* proposed by Duvenhage and Terblanche (2008) can provide interoperability amongst the services within the SANDF, including EW and CNO areas, and will be an enabler for effective CNO. Such protocols could be expanded to interface with other, international protocols and standards, allowing for multinational interoperability.

The actual need for EW and CNO may be limited. The host nation may not have infrastructure capable of supporting the CNO of a fully 'network-centric' task force. Here CNO may be relegated to a supporting role, providing an increased interoperability capacity for the task force. However, it may be employed outside the host nation, tracing and intercepting possible financial transactions supporting acts of aggression and/or ethnic cleansing. EW may be tasked with jamming broadcasts of hate-messages advocating ethnic violence and genocide, such as those in the Rwandan genocide, or monitoring and hindering cellular calls and CB radios to deny an improvised C2 network, such as in Somalia. Planning and co-ordination of operations still important; some coalition equipment may be more susceptible to the effects of electronic fratricide due to differences in quality, and 'legitimate' media broadcasts should be left unhindered. EM spectrum deconfliction will therefore still play an important role. However, due to the unpredictable nature, there should be a degree of adaptability in planning and modelling tools. One would not want to be found lacking against an adversary who manages to field advanced EW and CNO equipment, thereby disrupting coalition capabilities. It is therefore necessary to plan for both spectrums of conflict.

5. Conclusion

Whilst EW and CNO are considered separate entities, they are related and there are significant analogous concepts that allow the established methods of EW to be applied to CNO; this extends to the management and administration of EW and CNO. Examples were given to illustrate the real-world and potential consequences of poor mission planning and oversights, as well as what is possible to achieve. A series of limitations were raised, mainly compatibility and co-ordination issues; where cultural differences or hardware and software compatibility could hinder interoperability, mission success or result in fratricide. Solutions may include a middleware information system to facilitate information dissemination and network management, and EM spectrum management systems. Joint training and exercises, and standardised modelling and planning tools such as the modified GERAM framework and JOPES will help promote interoperability and reduce the risk of fratricide. These limitations and solutions were applied to the complex and unpredictable 'African Battlespace.' Here the scope of EW and CNO may be limited, yet can still play a vital role. Due to the diverse cultures, infrastructure and military systems found in Africa, effective planning, co-ordination and joint training is just as crucial as it is elsewhere.

Appendix 1: Proposed JOPES for CNO

The following JOPES is modified from Appendix B, Annex B of Joint Publication 3-13 (1998).

1. Situation

   a) Enemy Forces.

   - What are the capabilities, limitations, and vulnerabilities of enemy information and communications systems?
   - What is the enemy capability to interfere with accomplishment of the CNO mission?

b) Friendly Forces.

- What friendly CNO facilities, resources, and organisations may affect CNO planning by subordinate commanders?
- Who are the friendly foreign forces with which subordinate commanders may operate?

c) *Assumptions.* What are the assumptions concerning friendly or enemy capabilities and course of action that significantly influence the planning of CNO?

2. Mission

What is the CNO mission (who, what, when, where, why)?

3. Execution

a) Concept of Operations.

- What is the role of CNO in the commander's IO strategy?
- What is the scope of CNO?
- What methods and resources will be employed? Include organic and non-organic capabilities.
- How will CNO support the other elements of IO?

b) *Tasks.* What are the individual CNO tasks and responsibilities for each component or subdivision of the force? Include all instructions unique to the component or subdivision.

c) Coordinating Instructions.

- What instructions, if any, are applicable to two or more components or subdivisions?
- What are the requirements, if any, for the coordination of CNO actions between subordinate elements?
- What is the guidance on the employment of each activity, special measure, or procedure that is to be used but is not covered elsewhere?
- What is the bandwidth control and system or cyberspace intrusion guidance? Provide detailed guidance.
- What coordination is required to accomplish the restricted systems and cyberspace list?

4. Administration and Logistics

a) Administration.

- What, if any, administrative guidance is required?
- What, if any, reports are required? Include example(s).

b) Logistics. What, if any, are the special instructions on logistic support for CNO?

5. Command and Control

a) Feedback.

- What is the concept for monitoring the effectiveness of CNO during execution?
- What are specific intelligence requirements for feedback?

b) After-Action Reports. What are the requirements for after-action reporting?

c) Signal. What, if any, are the special or unusual CNO-related communications requirements?

References:

Adams, R., 2003, "New Threats Trigger 'Transformation'," *Military Simulation & Training*, Issue 6, 2003, pp. 35-38.

Anon, 2008, *Fact File: Link ZA*, Defenceweb, available at: http://www.defenceweb.co.za/index.php?option=com_content&task=view&id=801&Itemid=390, last accessed 23 March 2009.

Borque, J., 2008a, "A (Pragmatic) Future for Joint Electronic Warfare: Does EW + CNO = Cyber?" *Journal of Electronic Defense*, vol. 31, no. 9, September 2008, pp. 30-38.

Borque, J., 2008b, "Why EW is not Part of Cyberspace," *Journal of Electronic Defense*, vol. 31, no. 9, September 2008, pp. 38-39.

Brazzoli, M.S., 2007, "Future prospects of information warfare and particularly psychological operations," *South African Army Vision 2020*, In: ed. Len le Roux, Institute for Security Studies, Pretoria, pp. 217-232.

Curts, R.J., and Campbell, D.E., 2001, "The Impact of Architecture and Interoperability on Information Warfare Systems," *Journal of Information Warfare*, vol. 1, no. 1, pp. 33-41.

Du Toit, B., 2003, "The African Battlespace: Challenges for Air Defence," *4th South African Joint Air Defence Symposium*, Pretoria, October 2003.

Duvenhage, A., and Terblanche, L., 2008, "The Evolution of a C2 Protocol Gateway," *Proceedings of the Simulation Interoperability Standards Organization (SISO) Euro SIW 2008 Conference*, Edinburgh, Scotland, 16-19 June 2008.

Eshel, D., 2007, "Defeating IEDs," *Journal of Electronic Defense*, vol. 10, no. 12, December 2007, pp. 38-42.

DoA, 2003, *Information Operations: Doctrine, Tactics, Techniques and Procedures*, Field Manual 3-13.

Hoad & Jones, 2004, "Electromagnetic (EM) Threats to Information Security – Applicability of the EMC Directive and Information Security Guidelines," In: *3rd European Conference on Information Warfare and Security*, London, 28-29 June 2004, pp. 129-138.

Hodges, J., 2009, "Getting on Board," *C4ISR Journal*, vol. 8, no. 1, January-February 2009, pp. 24-25.

Huber, A.F., Carlberg, G., Gilliard, P., & Marquet, L.D., 2007, "Deconflicting Electronic Warfare in Joint Operations," *Joint Forces Quarterly*, Issue 45, 2nd Quarter 2007, pp. 89-95.

Hutchinson, W., Huhtinen, A., & Rantapelkonen, J., 2007, "The Impact of Perspective on the Effects and Outcomes of Conflict," *Journal of Information Warfare*, vol. 6, no. 1, pp. 1-6.

IFIP-IFAC Task Force, 1999, *Generalised Enterprise Reference Architecture and Methodology.* IFIP-IFAC Task Force.

Joint Chiefs of Staff, 1998, *Joint Doctrine for Information Operations*, Joint Publication 3-13.

Joint Chiefs of Staff, 2000, *Joint Doctrine for Electronic Warfare*, Joint Publication 3-51.

Joint Chiefs of Staff, 2007, *Electronic Warfare*, Joint Publication 3-13.1.

Kunkel, M., 2008, "New Cyber Definition Excludes EW," *Journal of Electronic Defense*, vol. 31, no. 11, November 2008, pg. 26.

Laudon, K.C., and Laudon J.P, 2004, *Management Information Systems: Managing the Digital Firm*, 8th ed., Prentice Hall, New Jersey.

Luddy, J., 2005, *The Challenge and Promise of Network-Centric Warfare*, Lexington Institute, February 2005.

Pfeffer, R., 2000, "Digital C4I Interoperability: The EM Protection Issue," In: DOD CCRP, *5th International Command and Control Research and Technology Symposia*, Canberra. Available at: www.dodccrp.org/events/5th_ICCRTS/papers/Track3/075.pdf

Seymour, R. et al., 2000, "Achieving Interoperability through an Information Management Architecture," In: DOD CCRP, *5th International Command and Control Research and Technology Symposia*, Canberra. Available at: http://www.dodccrp.org/events/5th_ICCRTS/papers/Track3/046.pdf

Smith, R., and Knight, S., 2005, "Applying Electronic Warfare Solutions to Network Security," *Canadian Military Journal*, Autumn 2005.

Slay, J., 2002, "A Cultural Framework for the Interoperability of C2 Systems," *Journal of Information Warfare*, vol. 2, no. 1, pp. 38-49

Vanden Brook, T., 2007, "Signals Foil IEDs but also Troop Radios," USA Today, 23 January 2007, in *Information Operations Newsletter*, vol. 7, no. 10, 19-28 January 2007, pp. 18-19.

Zehetner, A.R., 2004, "Information Operations: The Impact on C4I Systems," *AOC International Symposium and Exhibition*, Adelaide, 2004.

Brett van Niekerk completed his B.Sc. in Electronic Engineering in 2002 at the former University of Natal, and graduated with a M.Sc. Electronic Engineering dissertation in next-generation communications in 2006 at the University of KwaZulu-Natal. He started his PhD research in 2006, analysing potential vulnerabilities in 3G communication infrastructures from Information Warfare and Electronic Warfare perspectives. He worked at ThoroughTec Simulation on mining and military projects, managed the Electronic Design Department. He is currently completing his PhD and is a part-time lecturer and researcher at the Management College of Southern Africa.