Convergence of functional areas in information operations

Author:
Brett van Niekerk[1]

Affiliation:
[1]School of Management, IT and Governance, University of KwaZulu-Natal, South Africa

Correspondence to:
Brett van Niekerk

Email:
brettvn@gmail.com

Postal address:
Private Bag X54001, Durban 4000, South Africa

Dates:
Received: 11 Dec. 2013
Accepted: 02 April 2015
Published: 18 Sept. 2015

How to cite this article:
Van Niekerk, B., 2015, 'Convergence of functional areas in information operations', *South African Journal of Information Management* 17(1), Art. #605, 7 pages. http://dx.doi.org/10.4102/sajim.v17i1.605

Background: Contemporary technology and its rapid rise to a ubiquitous nature are affecting the way in which technology is used. This holds implications for military information operations and information warfare concepts as the previously separate functional areas are increasingly overlapping due to the increased convergence of information technology. Objective: The aim of the article is to illustrate the convergence of the functional areas of information operations through the use of reported examples and descriptive models.

Methods: A qualitative review and analysis of practitioner documents, academic publications, and other reports is conducted. The diverse views of this phenomenon are contrasted and discussed. The possible implications of the convergence and possible management techniques are proposed and discussed.

Results: There is strong opinion that the domains are not converging, however practice shows that there is an increasing overlap of operational considerations and organisational structure.

Conclusion: It is concluded that the domains are not converging, but the operations and management of the information operations functional areas may converge, and this has an impact across all functional areas that needs to be taken into consideration.

Introduction

Contemporary technology such as social media, the rapidly growing prevalence of wireless networking technology and the expanding capabilities of smart mobile devices result in what is termed as digital convergence. This has an impact on the military use of information technology, namely information operations (IO) and information warfare (IW), as the technology upon which the different functional areas are based converge and evolve. Through the use of examples and descriptive models, the convergence of the functional areas of information warfare and information operations is discussed.

An overview of information operations, information warfare and their constituent functional areas is provided, after which the existing relationship amongst the main functional areas is described through the use of generally accepted models of information technology and reviews of existing debates on the topic. The convergence through the prevalence of contemporary information technology is illustrated through the use of reported examples, and the implications of the convergence and management thereof are discussed.

Methodology

The convergence of information operations, in particular between electronic warfare and computer network operations, is being debated, mostly in practitioner forums. There is limited academic contribution to these debates, but it has been indicated that there is a need for academic models for information operations (Armistead 2010:108). This article aims to fill the gap by providing an academic perspective on the debate and by proposing an alternative model to those discussed previously.

The research takes an interpretivist stance in that the analysed documents that consider convergence in information operations are often authored by practitioners whose reasoning is not only intended to understand the concept but to actively participate in defining it. The approach taken is inductive, seeking to develop theory on the convergence amongst the functional areas in information operations. A qualitative document analysis of reports and examples, combined with logical argument, is used to derive on-going convergence and the potential impact thereof. Rouse and Dick (1994:51) illustrate the importance of qualitative research for information systems '… to capture holistic real-world answers to real-world

problems in a way that is not possible in a quantitative context'. Publication databases and search engines were used to identify academic and practitioner publications and documents which consider the topics of interest. Search engines were used to identify relevant news reports that illustrate the existence of the concepts under discussion. A total of 11 academic or practitioner publications and 18 news reports were identified. All of these are considered in the article.

Functional areas in information operations

This section describes the various functional areas of information operations. The definition of IO and IW varies by country and organisation. Usually this reflects the specific strategy or focus that is employed. For this paper, two definitions will be considered. Denning (1999) defines IW as the following:

> … offensive and defensive operations against information resources of a 'win-lose' nature. It is conducted because information resources have value to people. Offensive operations aim to increase this value for the offence while decreasing it for the defence. Defensive operations seek to counter potential losses in value. (p. 21)

Brazzoli (2007) considers IW to be as follows:

> 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. (p. 219)

These definitions highlight the value of information and that certain activities seek to change or maintain the current value or status of the information through activities relating to information assets and related infrastructure and systems. The notion of different domains is also raised: people or psychological, virtual and physical aspects of information. Whilst the military aspect is emphasised, Cronin and Crawford (1999) indicate that information operations can be applied to non-military situations, supporting the views considering information operations as an extension of IW to non-conflict scenarios (such as peacetime and periods of increased competition).

Computer network operations (also known as cyber-warfare) focus on computer networks and the Internet. It comprises of computer network exploitation (intelligence gathering), computer network attack, computer network defence and computer network support. In some instances, this is extended to include the protection of critical infrastructure from attacks through computer networks (Brazzoli 2007:221; Van Niekerk 2011:39–40). This functional area is the newest functional area and is yet to be fully established.

Electronic warfare (EW) focuses on the electromagnetic spectrum, comprising of electronic protection, electronic support and electronic attack. This most commonly includes the jamming, detection and interception of signals (Joint Chiefs of Staff 1998:II–5).

Psychological operations (PSYOP) are actions taken to influence a population's perceptions, attitudes and behaviour (Brazzoli 2007:221). PSYOP can be considered to be limited to military operational areas whereas strategic communication and propaganda can be considered to be of a larger scale, aimed at national or international audiences ranging from competition to conflict scenarios.

Other notable areas deal with intelligence gathering, command and control and the network support to operations and decision-making. It also includes data and audio and imagery communication via wired and wireless networks and infrastructure (Brazzoli 2007:221). This results in a shift from the traditional platform-centric operations and command and control to the network-centric form where information can be shared amongst platforms so that everyone has access to the same information. The intelligence process of gathering, analysing and disseminating data and information to support the decision-making process (command and control) is therefore key. Offensive operations attempt to disrupt these capabilities of the adversary, and defensive operations seek to maintain these capabilities in allied and own forces (Brazzoli 2007:221).

Porche *et al*. (2013:25–28) indicate that there are problems with the current definition and construction of IO: There is a lack of common vision ranging from too focussed to too broad. Many functional areas are treated as compartmentalised (Porche *et al*. 2013:24), and there is no explanation as to how it will act as a co-ordinating function or as to the relationships amongst the different functional areas. The next section describes the relationships between different functional areas of IO through the use of examples and positions advocated in documents.

Relationships amongst functional areas

There has been much debate regarding the relationship between EW, cyber-warfare and computer network operations and the implications of the various forms of terminology. Smith and Knight (2005:53) apply EW concepts to network security. This indicates a number of parallels between EW and cyber-warfare such as jamming and denial-of-service (DoS) or flares and honeypots.

A report by the US Government Accountability Office indicates that the two domains should be considered as separate (Chabrow 2012). Knowles (2013:48) proposes that cyber-space is a man-made physical environment, including telecommunication, data, networks and processors. In contrast, the electromagnetic spectrum is natural. Wireless communication is seen as the human exploitation of an existing natural space whereas cyber-space is a purely

man-made construct. However, it can be argued that the physical components of the telecommunication and data networks that form cyber-space are based upon guided or radiated electromagnetic signals and therefore part of the electromagnetic spectrum (Clifford 2011:41; Hahn 2010: 44–46). Clifford (2011:41) argues that it is incorrect to say that cyber-space and the electromagnetic spectrum are equivalent due to the fact that they are based on similar physics. Some of the discussion revolves around terminology: Borque (2008:30–40) discusses whether cyber-operations are a combination of EW and computer network operations and concludes that EW and cyber-operations are separate. Cloud (2007:10–12) takes the contradictory view that cyber-operations entail a broader domain and include the electromagnetic spectrum, indicating that EW is a subset of cyber-operations.

The use of the psychological and cyber-domains is also related. The concept of hacktivism can be considered a combination of two areas: Activism can be seen as a form of psychological operation, and hactivism combines it with cyber-warfare concepts. Therefore website defacement can be described as cyber-enabled PSYOP. In some instances, the cyber-attack is meant to create the psychological impact such as the tactics used by the group Anonymous. The attack on the website of the South African Police Service was a cyber-attack with the intent to cause a psychological impact. It is reported that sensitive information on whistle-blowers was publicly released and that the attackers claimed that it was in retaliation for slow investigations in the Marikana mine shooting (Tubbs 2013). Anonymous Africa targeted a number of websites in Zimbabwe and South Africa with DoS attacks in protest against the Zimbabwean Government (Alfreds 2013; Daily News Correspondent 2013). There are reports of Israel hacking into phone voicemail systems to leave messages (StrategyPage.com 2009). This can be seen as an example of cyber-delivered PSYOP. There is also a possible relationship with EW and PSYOP in that radio or television broadcasts could be jammed to prevent them from being used to incite violence as happened in Rwanda (Van Niekerk & Maharaj 2009:6).

A number of espionage operations have been conducted over the Internet. These are cyber-attacks based on malicious, code-infecting targeted systems which then copy files onto a server from where the attackers can retrieve them. Major attacks of this type are the GhostNet cyber-espionage in 2009 and Red October, discovered in 2013 after an estimated five years of operation (Higgins 2013; Information Warfare Monitor 2009). In 2013, details surfaced of data-collection activities by US intelligence agencies that were monitoring telecommunications meta-data and online communications (Greenwald & MacAskill 2013). However the most recognised case is that of Wikileaks, a website which posts information from whistle-blowers online. The major releases which created both support and condemnation of the website internationally were the series of releases of US military information and diplomatic cables (Gragido & Pirc 2011:193–195; Van Niekerk & Maharaj 2011:7–8). These incidents indicate a strong relationship between intelligence, counter-intelligence and cyber-space.

BOX 1: Relationship of IW Areas to the OSI Model and IP Layers

OSI Layers	IP Layers	Functional Area
Application	Application	PSYOPs, C2W
Presentation		Network Warfare
Session		
Transport	Transport	
Network	Network	
Data-link	Data-link	Electronic Warfare
Physical	Physical	

TABLE 1: Proposed Layer Model for IW.

Layer	Functional area
Utility	C2W, PSYOPs
Grey area	
Connection	Network warfare
Grey area	
Access (wired and wireless)	Electronic warfare

Source: Maasdorp, F. & Du Plessis, W., 2012, 'Using a layered model to place EW in context within the informationsphere', *Proceedings of the 4th Workshop on ICT Uses in Warfare and the Safeguarding of Peace 2012 (IWSP 2012*), 16 August 2012, Sandton, pp. 29–33.

As EW targets primarily radiate the use of the EMS (but can conceivably have an effect on guided transmissions as directed-energy) and are concerned with the modulation and frequency of these transmissions, it is applicable to the physical layer of the OSI model and may extend to the data-link layer. As cyber-space is the interconnection of systems and networking, it can be considered to extend from the data-link layer to the presentation layer, and in some cases, it overlaps with the application layer. Other areas, such as PSYOP and command and control, occur at the application layer, as these are ultimately end-user functions where the key aspect is their presentation of information. The functional areas can similarly be mapped to the Internet Protocol (IP) layers as illustrated in Box 1.

Maasdorp and du Plessis (2012:29–33) propose another layered model to describe the relationship amongst the various aspects of IW and IO. This is shown in Table 1. Three layers are proposed: the utility layer, which is what humans will work with and consciously use; the connection layer, which is the logical connections of a network; and the access layer, which is the electromagnetic transport of analogue or digital bits. Overlap between the layers and their corresponding IW functional areas are allowed through the grey areas (Maasdorp & du Plessis 2012:29–33).

The convergence of functional areas through contemporary information technology

Contemporary technology such as the ubiquitous nature of mobile and wireless technology and social media are

increasing the overlap amongst the domains and may therefore result in the convergence of IW functional areas.

The most discussed area for potential convergence is cyber-operations and EW, largely due to the evolution of wireless and mobile technology. Retired General Cartwright expressed views regarding the links between EW and cyber-operations (Freedberg 2013b), which are corroborated by reports that the development of new EW technology for the US Army is being complicated by the role of cyber-warfare and new attack methods. Chabrow (2012) also indicates that the management of EW is being complicated by the role and synergies with computer network operations. In conjunction with the development of the new EW systems, a new doctrine for cyber-electromagnetic operations is being developed (Freedberg 2013a), and a new training centre for the US Army is to incorporate aspects of cyber-operations, EW and other communications-related actions (Gould 2013). This culminated in a US Army doctrine for cyber-electromagnetic activities where such operations are seen as the overlap amongst cyber-space operations, electronic warfare and spectrum management operations (Department of the Army 2014:1–2). Similarly, the US Air Force is developing systems for 'spectrum warfare' which will cover EW, cyber-operations and other aspects. Some of the associated programs include research into 'net-enabled electronic warfare technologies' (Keller 2013). This indicates that the electromagnetic spectrum, traditionally the focus of EW, is now being related to computer networks. Another project is aimed at detecting cyber-attacks through the use of radio-frequency measurement and signals intelligence (Prince 2012). This can be seen as an intersection of intelligence, EW and cyber-operations.

Mobile technology, in particular smartphones and tablets, has integrated a number of forms of technology, which would previously have been separate tools for conducting espionage. They have integrated navigation, camera and video capture and the ability to transmit these wirelessly. They support Web browsing, have integrated social media connectivity and can function as a basic telephone in addition to having a variety of other applications. These include a hacking tool and a method for PSYOP message delivery (Van Niekerk & Maharaj 2012:4–7).

The mobile-phone infrastructure is different from traditional fixed-line communications where the data and voice channels are separate. With mobile phones, it is feasible that data-based attacks can impact the voice channels (Amoroso 2013:102). In addition, by targeting the wireless transmission using EW, both voice and data can be simultaneously disrupted or compromised. The introduction of voice over IP (VOIP) allows voice to be carried over the data networks. Many instant-messaging applications provide support for text, voice, video or a combination of these, which are transmitted over data networks. These forms of communication are susceptible to standard network attacks. Examples may include disruption by DoS and possible interception of and eavesdropping on communication.

TABLE 2: Mentions of areas converging.

Cyber-EW	Cyber-intelligence	Cyber-PSYOP	EW-PSYOP
12	4	7	1

TABLE 3: Sentiment regarding convergence.

Pro-convergence	Anti-convergence
6	4

Social media is a useful tool for PSYOP, and as it is cyber-based, it can be seen as a combination of these two as cyber-security concerns to protect the accounts used in such operations will also be relevant. The open nature of social media enables operators to gather intelligence on targeted individuals or groups to enable them conduct PSYOP on these targets (Van Niekerk 2012). Social media can be used on a large-scale in what can be called social IW by allowing groups to protest online with global support and organise and guide physical protests. Examples of this are the Arab Spring demonstrations and the related Occupy movement (Kamzi 2011; Madrigal 2011).

A number of cases discussed in this section will commonly be called convergence. However, Knowles (2013:48) suggests that convergence as a term is over-used and often misused and that sharing is a more appropriate term when discussing this phenomenon. The motivations for separate domains discussed in this section are largely limited to the domains. It is possible that the domains themselves remain separate, but the operations and management related to those domains converge. Therefore, the functional areas of IO can converge. Maasdorp and du Plessis (2012:32–33) support this view to an extent, indicating that there should at least be interaction between researchers and operators in the various fields to increase the efficiency and effectiveness of efforts. The increase in combined training for electronic warfare and cyber-operations indicates that there is a strong view that operations, or the management thereof, in these domains can be combined or integrated from a practical perspective.

Summary of convergence concepts regarding information operations

This section summarises the prior discussions regarding convergence. Table 2 illustrates the number of discussions related to the convergence between specific functional areas. As is evident, the focus is on cyber-operations and the electromagnetic spectrum. There is also some focus on the psychological aspects of cyber-operations, probably due to the number of hacktivist or propaganda-motivated cyber-attacks. The weakest overlap is between EW and PSYOP. Whilst there is some possible overlap between this two, the scope is very limited.

Table 3 illustrates the sentiment regarding convergence: Documents that take a pro-convergence perspective slightly outnumber those that take an anti-convergence perspective.

Implications of the convergence of functional areas in information operations

This section discusses the implications of the convergence of the functional areas of IO. These affects could be ethical, legal and operational and could affect the structuring of units or organisations and require specific management techniques.

The disruptive nature of networked communications

Whilst cyber-operations are still emerging and not yet fully established, they are having disruptive effects on previously established functional areas. The result of the shift to network-centric operations is a primary driver of convergence. This results in an upheaval of previously established functional areas. As was described above, computer network operations are complicating the management of EW, and this may also be the case for other functional areas such as PSYOPs. In addition to the other implications discussed below, specialists in many functional areas are required to adjust their thinking, and many may be dissatisfied with or resistant to some of the implications of convergence.

Legal and ethical considerations

The availability of information due to networked communication has increased drastically, and the open nature of social media has hastened this. A legal issue with conducting PYSOP on social media is that it may be difficult to restrict the operation to a specific target population due to its global availability. Therefore, it is highly likely that unintended audiences could access the content. This becomes problematic when there are legal restrictions on the population that is to be targeted. In addition, whilst a specific website may be for a specific nationality, it may be hosted in a different country that is off-limits. Therefore, targeting the audience of the webpage may fall into a grey area, legally speaking. The implications of this are that, when conducting cyber-enabled PSYOP, very careful legal analyses should be conducted to ensure that some legal boundary is not inadvertently crossed, which could result in severe embarrassment should a public outcry result.

The use of social media for mass influence or mass surveillance has additional ethical and legal concerns, particularly surrounding the misuse of these capabilities. An example is the use of social media by Pakistanis to threaten Indian citizens living in a particular area (Abbas 2012). These citizens then left the area in panic, causing a humanitarian crisis. Social media can be used to frame or misrepresent people as fake profiles can be created under names or legitimate profiles can be compromised with the specific goal of using these profiles to conduct misbehaviour for which the real person will then be blamed. Mass surveillance, legitimate or otherwise, has the real possibility of infringing on personal rights, particularly on privacy. The revelations that the US intelligence agencies were accessing a variety of communications resulted in a massive international outcry (Leyden 2013; Vijayan 2013). The very revelations of the communication intercepts and the information released by Bradley Manning and Wikileaks (Gragido & Pirc 2011:192–195) fall within an ethical grey area. Their actions can be seen as a severe breach of security and irresponsible behaviour. However, their claimed motives and the views of their supporters are that this information is of public interest and illustrate governments' misuse of power. The releases were a form of IO in that the perpetrators were aiming to alter perceptions against the various governments and agencies. However, there seems to be an attitude that mass surveillance and cyber-espionage are allowable as long as you do not get caught: The US often complained about apparent Chinese incursion into their networks, and then the intercept revelations were made (Leyden 2013). French authorities are also showing anger. However, there are reports that they are involved in similar activities (Crowley 2013:12; Leyden 2013; Vijayan 2013). Many nations conduct espionage on competitors and allies alike (Crowley 2013:12), and the vast array of interconnected digital and telecommunications networks makes it easier to intercept or steal that information.

Legal jurisdiction over data and signals may become problematic. Data may cross multiple national boundaries between the sender and receiver, and with cloud computing, data may permanently reside outside of the owner's national borders. Likewise, radiated electromagnetic signals may cross national borders. These signals or data transfers may then be subjected to a wide variety of data or communication laws. If psychological or data attacks transit via a third nation, can this nation consider itself as under attack (when the attack is not aimed at it)? If this question can be answered, it still needs to be proved who the actual perpetrator is, as one of the problematic aspects of cyber-warfare is the difficulty of attribution (Liff 2012:412). This indicates that other attacks delivered through cyber-warfare tactics will probably be difficult to attribute. This perceived difficulty in attributing attacks may provide a feeling of invisibility and encourage activity which borders or crosses the line into being unethical whilst the perpetrators make the assumption that they will not be discovered.

Another issue with the difficulty of attribution is retaliation against an innocent party. This becomes more likely with the attacker actively framing a third party, hoping that the latter will get the blame. Should the retaliation against an attack be destructive in nature, it is imperative that the attribution information is accurate as this may inadvertently target innocent civilians whose system had been compromised by the attacker.

Organisational restructuring

In a business environment, Dennis and Durcikova (2012:109, 452) indicate that technological convergence of voice, video and data results in the audiovisual, IT and telecommunication departments of organisations merging to cope with the integrated technology. In a similar way, military units

for PSYOP, EW, communication and cyber-warfare may find themselves strongly supporting each other, and joint-functionality IO cells may be formed for operations.

In a corporate setting, the corporate-communication and public-relations functions need to be concerned with the cyber-dimension in a more dynamic fashion. Not only do they need to run email communications to stakeholders and maintain traditional webpages, but they need to protect the organisation's image on social media. This entails an element of business intelligence where corporate-communication departments need to monitor the social media profiles run by them for negative comments. They also need to have intelligence on other potentially 'hostile' websites and profiles where disgruntled clients or employees could complain or behave in a manner damaging to the corporate image.

From an operational perspective, there is now a broader range of technology that need to be managed, integrated into operations and secured. Due to overlaps in domains and technology, the impact of operations may be broader than expected, and it may become difficult to contain operational effects. This then calls for improved business and competitive intelligence, particularly in the areas of assessing operational impacts. New committees may be required, or existing committees may need additional members with more or different specialities.

IO units or cells could therefore be comprised of a number of specialists working together, each of whom are experts in a specific area. Each specialist provides in-depth knowledge of their individual area. However, their expertise in other areas may be limited, and different views may cause conflict. An alternative is that the IO unit or cell is comprised of generalists who have grounding in multiple (or all) areas but are not necessarily experts in any. The generalists may be able to work together better due to common training and expertise. However, they may not have the depth of understanding that specialists would, potentially resulting in mistakes.

Porche *et al*. (2013) suggest separating the technical and psychological components in IO, and making commanders responsible for the integration of these when required. These authors indicate that the convergence of electronic warfare and cyber-operations requires personnel to have new specialities, pointing to a tendency to having generalists in technical areas (Porche *et al*. 2013:25). This will then effectively require two sets of specialists: those who deal with the technical aspects (cyber and EW) and those who deal with the psychological aspects (PSYOPs, strategic communications and public affairs). As the commanders are expected to be responsible for integration, they could then be considered as generalists.

Management techniques

The convergence of IO functional areas provides those with hostile intent with a variety of 'payloads' and delivery methods. At a strategic level, this may be managed to a certain degree by international policies and agreements. Operations including cyber and psychological aspects should be clarified in international law, particularly as it relates to armed conflict.

At the operational and tactical levels, the use of management information systems for command and control of cyber-operations and EW, such as the proposed systems described by Keller (2013) and the integrated cyber and electronic warfare system (Hatamoto 2013), will increase the efficiency of these operations by providing commanders with decision-support tools. These support systems can be utilised for both technical (EW and cyber) and psychologically based (including strategic communication) operations. These systems will necessitate efficient knowledge management and intelligence, which can be supported by the operations themselves (cyber-espionage and electronic intelligence) for data acquisition.

Training will need to be adjusted to cater for the converging operations. Those with technical skills will need to learn both EW and cyber-warfare concepts, as well as some of the psychological aspects of IO. The psychological operators will need to have combined training for PSYOP and more common public affairs practices with an introduction to the technical aspects, particularly the limitations regarding their use. The extent to which the cross-training is implemented will be determined by the structure of IO units and the extent to which they comprise of specialists or generalists as discussed above. Commanders, who will need to co-ordinate and ensure the integration of operations, will need to have extensive cross-training.

To ensure that operations do not cross any legal or ethical boundaries, legal advisors should be attached to IO cells or should advise commanders overseeing the activities.

Conclusion

IO consists of various functional areas, and a number of operational relationships exist amongst them. The overlaps are becoming larger due to the rapid uptake of wireless technology and social media. The article presented a qualitative document analysis to determine the nature of the convergence and the views thereof. There are many views on the convergence of functional areas in IO. Some strongly advocate that the cyber and electromagnetic domains should be kept separate. This article motivates that the domains can remain separate, but the operations and management thereof must be converging. This has management implications such as legal and ethical considerations for operations, organisational structure and training.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationships which may have inappropriately influenced them in writing this article.

References

Abbas, M., 2012, 'Web 2.0: Pakistan's new weapon?', CIOL.com, 21 August, viewed 23 August 2012, from http://www.ciol.com/ciol/news/108402/web-pakistans-weapon

Alfreds, D., 2013, 'ANC admits website hack attack', News24, 14 June, viewed 17 June 2013, from http://www.news24.com/Technology/News/ANC-admits-website-hack-attack-20130614

Amoroso, E.G., 2013, *Cyber attacks: Protecting national infrastructure*, Elsevier, Waltham, M.A.

Armistead, L., 2010, *Information operations matters*, Potomac Books, Washington, D.C.

Borque, J., 2008, 'A (pragmatic) future for joint electronic warfare: Does EW + CNO = Cyber?', *Journal of Electronic Defence* 31(9), 30–40.

Brazzoli, M.S., 2007, 'Future prospects of information warfare and particularly psychological operations', in L. le Roux (ed.), *South African army vision 2020*, pp. 217–232, Institute for Security Studies, Pretoria.

Chabrow, E., 2012, 'Aligning electronic and cyber warfare', viewed 11 July 2012, from http://www.govinfosecurity.com/aligning-electronic-cyber-warfare-a-4930

Clifford, J., 2011, 'What electronic warriors should know about physics, language and concepts', *Journal of Electronic Defense* 34(3), 40–47.

Cloud, D.W., 2007, 'Integrated cyber defenses: Towards cyber defense doctrine', Master's dissertation, Naval Postgraduate School.

Cronin, B. & Crawford, H., 1999, 'Information warfare: Its application in military and civilian contexts', *The Information Society* 15(4), 257–263. http://dx.doi.org/10.1080/019722499128420

Crowley, M., 2013, 'Spy vs. spy', *Time Magazine*, 11 November, p. 12.

Daily News Correspondent, 2013, 'Hackers target Zimbabwe government', *Independent Online*, 14 June, viewed 14 June 2013, from http://www.iol.co.za/dailynews/news/hackers-target-zimbabwe-government-1.1532349#.UbtKI1EaKM8

Denning, D.E., 1999, *Information warfare and security*, Addison-Wesely, Boston.

Dennis, A. & Durcikova, A., 2012, *Fundamentals of business data communications*, 11th edn., Wiley, New York.

Department of the Army, 2014, *Field Manual 3–38: Cyber electromagnetic activities*, US Department of Defence, Washington, D.C.

Freedberg, S., 2013a, 'Army electronic warfare goes on the offensive: New tech awaits approval', 29 January, viewed 01 April 2013, from http://defense.aol.com/2013/01/29/army-electronic-warfare-new-tech/

Freedberg, S., 2013b, 'Gen. Hoss Cartwright talks immigration, cyber, China & Afghans with iPhones', 25 March, viewed 27 March 2013, from http://defense.aol.com/2013/03/25/gen-hoss-cartwright-talks-immigration-cyber-china-and-afghans-w/

Gould, J., 2013, 'New center, school to bring signals, cyber, EW together', *Army Times*, 25 June, viewed 07 September 2013, from http://www.armytimes.com/article/20130625/CAREERS/306250002/New-center-school-bring-signals-cyber-EW-together

Gragido, W. & Pirc, J., 2011, *Cybercrime and espionage*, Elsevier, Burlington.

Greenwald, G. & MacAskill, E., 2013, 'NSA Prism program taps in to user data of Apple, Google and others', *The Guardian*, 7 June, viewed 09 June 2013, from http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data

Hahn, R., 2010, 'Physics of the cyber-EMS problem: Why we have the language wrong', *Journal of Electronic Defence* 33(11), 44–46.

Hatamoto, M., 2013, 'U.S. Army developing cyber, electronic war arsenal', *Daily Tech*, 31 October, viewed 13 November 2012, from http://www.dailytech.com/US+Army+Developing+Cyber+Electronic+War+Arsenal/article33660.htm

Higgins, K.J., 2013, '"Red October" attacks: The new face of cyberespionage', *Dark Reading*, viewed 17 January 2013, from http://www.darkreading.com/attacks-breaches/red-october-attacks-the-new-face-of-cybe/240146237

Information Warfare Monitor, 2009, 'Tracking GhostNet: Investigating a Cyber Espionage Network', viewed 01 September 2009, from http://128.100.171.10/modules.php?op=modload&name=News&file=article&sid=2386

Joint Chiefs of Staff, 1998, *Joint publication 3–13: Information operations*, 09 October, US Department of Defence, Washington, D.C.

Kamzi, A., 2011, 'How anonymous emerged to occupy Wall Street', *The Guardian*, 27 September, viewed 06 October 2013, from http://www.guardian.co.uk/commentisfree/cifamerica/2011/sep/27/occupy-wall-street-anonymous

Keller, J., 2013, 'Industry: Get ready for spectrum warfare program to cover EW, optics, GPS, and cyber operations', *Military and Aerospace Electronics*, viewed 18 July 2013, from http://www.militaryaerospace.com/articles/2013/07/usaf-answer-presolicitation.html

Knowles, J., 2013, 'Why two domains are better than one', *Journal of Electronic Defence* 36(5), 48–50.

Leyden, J., 2013, 'A post-Snowden US had better not squeal about Chinese cyber-spying', *The Register*, viewed 02 November 2013, from http://www.theregister.co.uk/2013/11/01/snowden_effect_us_china_cyberespionage/

Liff, A.P., 2012, 'Cyberwar: A new "absolute weapon"?: The proliferation of cyberwarfare capabilities and interstate war', *Journal of Strategic Studies* 35(3), 401–428. http://dx.doi.org/10.1080/01402390.2012.663252

Maasdorp, F. & Du Plessis, W., 2012, 'Using a layered model to place EW in context within the informationsphere', *Proceedings of the 4th Workshop on ICT Uses in Warfare and the Safeguarding of Peace 2012 (IWSP 2012*), 16 August 2012, Sandton, pp. 29–33.

Madrigal, A., 2011, 'The inside story of how Facebook responded to Tunisian hacks', *The Atlantic*, viewed 06 October 2013, from http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/#

Porche, I.R., Paul, C., York, M., Serena, C.C., Sollinger, J.M., Axelband, E. *et al*. 2013, *Redefining information warfare boundaries for an army in a wireless world*, RAND Institute, Santa Monica.

Prince, B., 2012, 'Project aims to detect cyber attacks using radio frequency', *Security Week*, viewed 21 November 2012, from http://www.securityweek.com/project-aims-detect-cyber-attacks-using-radio-frequency

Rouse, A. & Dick, M., 1994, 'The use of NUDIST, a computerized analytical tool, to support qualitative information systems research', *Information Technology & People* 7(3), 50–62.

Smith, R. & Knight, S., 2005, 'Applying electronic warfare solutions to network security', *Canadian Military Journal* 6(3), 49–58.

StrategyPage.com., 2009, 'Gaza cell phones targeted', 02 January, viewed 27 July 2009, from http://www.strategypage.com/htmw/htiw/articles/20090102.aspx

Tubbs, B., 2013, 'SAPS hack spells negligence', viewed 22 May, from http://www.itweb.co.za/index.php?option=com_content&view=article&id=64268:SAPS-hack-spells-negligence&catid=265

Van Niekerk, B., 2011, 'Vulnerability analysis of modern ICT infrastructure from an information warfare perspective', PhD thesis, University of KwaZulu-Natal.

Van Niekerk, B., 2012, 'Tools for conducting operations on social media', South African National Defence Force Psychological Operations Expertise Register Workshop, 12 October, Pretoria.

Van Niekerk, B. & Maharaj, M.S., 2009, 'The future roles of electronic warfare in the information warfare spectrum', *Journal of Information Warfare* 8(3), 1–13.

Van Niekerk, B. & Maharaj, M.S., 2011, 'The information warfare life cycle model', *South African Journal of Information Management* 13(1), 1–9. http://dx.doi.org/10.4102/sajim.v13i1.476

Van Niekerk, B. & Maharaj, M.S., 2012, 'Mobile devices and the military: Useful tool or significant threat?', *Journal of Information Warfare* 11(2), 1–11.

Vijayan, J., 2013, 'Is French outrage against U.S. spying misplaced?', Computer World, viewed 25 October 2013, from http://www.computerworld.com/s/article/9243414/Is_French_outrage_against_U.S._spying_misplaced