The Information Warfare Life Cycle Model

Authors:
Brett van Niekerk[1]
Manoj S. Maharaj[1]

Affiliations:
[1]School of Information Systems and Technology, University of KwaZulu-Natal, South Africa

Correspondence to:
Brett van Niekerk

Email:
vanniekerkb@ukzn.ac.za

Postal address:
University Road, M-Block, Westville Campus, Durban 4000, South Africa

Dates:
Received: 01 Mar. 2011
Accepted: 30 Aug. 2011
Published: 10 Nov. 2011

How to cite this article:
Van Niekerk, B. & Maharaj, M.S., 2011, 'The Information Warfare Life Cycle Model', *SA Journal of Information Management* 13(1), Art. #476, 9 pages. http://dx.doi.org/10.4102.sajim.v13i1.476

Information warfare (IW) is a dynamic and developing concept, which constitutes a number of disciplines. This paper aims to develop a life cycle model for information warfare that is applicable to all of the constituent disciplines. The model aims to be scalable and applicable to civilian and military incidents where information warfare tactics are employed. Existing information warfare models are discussed, and a new model is developed from the common aspects of these existing models. The proposed model is then applied to a variety of incidents to test its applicability and scalability. The proposed model is shown to be applicable to multiple disciplines of information warfare and is scalable, thus meeting the objectives of the model.

Introduction

Information warfare is a construct that was brought to prominence by the United States Department of Defence in the 1990s (Kopp 2000:31). The concept of information warfare brings together a number of disciplines that revolve around information and information systems; a number of these disciplines have existed since antiquity; however, the rapid evolution of information and communications technology has made them more prominent in a globalised society. Information warfare is a dynamic and developing concept, and is still prone to changes and debates; consequently there is no coherence in the definitions, constructs, or models. However, it is clear that information warfare is a global phenomenon. The implementation of information warfare may be hindered by the lack of a standardised taxonomy or nomenclature (Armistead 2010:109). The purpose of this article is to develop a life cycle framework for information warfare that incorporates the common aspects of the various disciplines, is scalable, and may be applied to both the civilian and military domains where information warfare tactics are employed. By doing so, it is intended that the existing models are related and brought together in a single framework in an attempt to further standardise the information warfare concept in a global context. This model forms the second step and consists of consolidating the various levels of models into a single framework. The first step was submitted in a companion paper, which compares the variations of individual models (Van Niekerk & Maharaj in press). For the purposes of this paper, the background will provide the information relevant to the proposed model.

Information Warfare

This section provides the background theory to information warfare and presents the models previously proposed to describe aspects of Information Warfare (IW). Existing models and frameworks to describe IW cycles are then presented and discussed.

Background

Information Warfare can be defined as:

> 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.
>
> (Denning 1999:21)

From the aforementioned definition it can be seen that the use of IW is an attempt to gain an advantage over a competitor or adversary by either leveraging one's own information resources or denying the opponent the ability to fully leverage their information resources. The first definition mentions that information warfare can be conducted in the physical, information and cognitive domains; this illustrates that information warfare may include traditional physical destruction of information-related resources and may also target the human mind.

Six functional areas or 'pillars' of IW have been identified (Brazzoli 2007:221):

- Command and control warfare entails actions to preserve the ability to command your own forces whilst hindering the adversary's similar capabilities. In a corporate environment it would

refer to the management of employees and departments.
- Intelligence based warfare entails the ability to gather and process intelligence, and disseminate it to the relevant end-users whilst disrupting similar capabilities of the adversary.
- Information infrastructure warfare entails protecting the information infrastructure (and those infrastructures upon which it is dependant) whilst exploiting those of an adversary.
- Psychological operations entail influencing a target audience to ultimately behave in a manner favourable to your objectives and countering attempts to influence the audience against those objectives.
- Network warfare entails preserving the use of the information networks whilst exploiting those of an adversary or degrading their networks.
- Electronic warfare entails preserving the availability of the electro-magnetic spectrum for one's own use whilst degrading the ability of an adversary to utilise it. This has far greater applicability to the military environment than the corporate sphere.

A seventh pillar has been proposed by some researchers and has been adopted by India (Chatterji 2008:10); this is 'economic IW'. Chatterji describes this as a blockade of economic information, where a competing nation would be starved of external information relevant to its economy. Economic and industrial espionage may also form part of economic IW.

The 'CIA Triad' model (Denning 1998:41; Waltz 1998:22) describes three attributes of information and the supporting information infrastructures that need to be preserved:

- Confidentiality – only those who have the required authority or clearance may gain access to sensitive information or knowledge of the functioning, operations or characteristics of infrastructures.
- Integrity – only authorised persons should be able to alter information or systems settings that could affect the infrastructure, and the authenticity of the information and alterations should be ensured.
- Availability – the information and its supporting infrastructure should be available when required.

There are extensions to this model; however, those are more applicable to information security in general and are not relevant to the information warfare discussion presented in this paper.

To counter the 'CIA Triad' there are three main strategies that may be used to attack information and the supporting infrastructure. Waltz (1998:23), Borden (1999), Hutchinson and Warren (2001:3), and the United States Air Force (1998:9) all provide similar models, with variations in the terms used and sometimes there is a sub-division of the strategies. The three strategies and some of their sub-divisions are:

- deny, disrupt or degrade access to information, or destroy the information
- steal, exploit or intercept the information
- corrupt the information by modifying the contents, inserting additional false information (fabrication), altering the context in which the information is viewed and changing the perceptions of people towards the information.

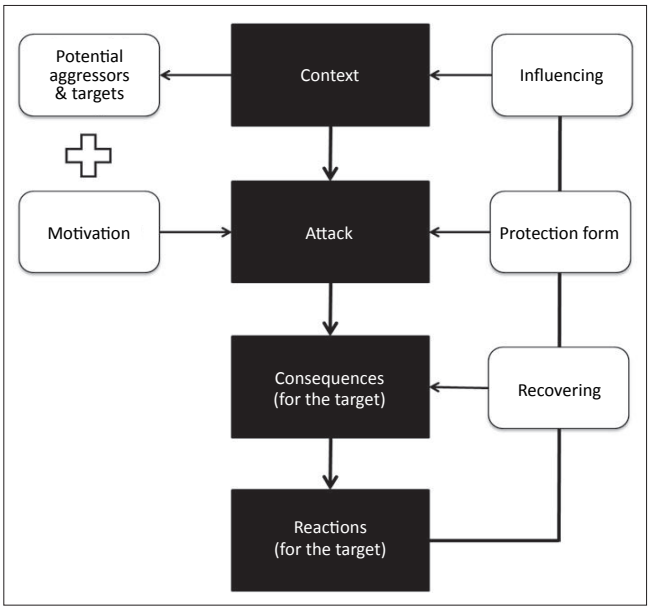
Existing Information Warfare models and frameworks

This section presents selected existing models and frameworks from which the proposed IW Life Cycle Model may be generated. Two models describing IW in general are discussed, followed by the Message Flow Model for psychological operations and a discussion of a proposed framework for network warfare.

General Information Warfare models

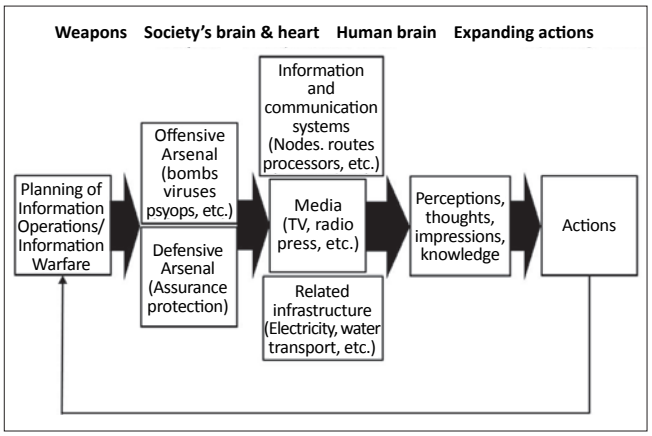
Ventre (2009:276) contends that many confrontations over computer networks and the Internet are a result of tense political situations; and proposes a model shown in Figure 1. Whilst it was developed specifically for the case of politically motivated cyber-attacks it can be used to model any incident where an IW attack has occurred. Some context results in potential adversaries and motivations, which may result in an IW attack. This has ramifications for the target, which will react in an attempt to recover and gain protection from current and future attacks. Any reaction of the target, and any active retaliation, will result in the overall context being influenced.

The disciplines and capabilities relevant to information warfare may be employed outside the traditional military command and control target set (Wik 2002:617). Figure 2 illustrates a process for information warfare developed from this. Once the operations have been planned, the available 'weapons' are applied to the target set: primarily infrastructure and systems which modern society revolves around, such as communications systems, the mass media and other infrastructures in society (Wik 2002:617). The attack on these target sets will create affects that impact on humans themselves, altering or creating new thought



Source: Adapted from Ventre, D., 2009, *Information warfare*, ISTE, London, UK.

FIGURE 1: Information warfare cycle.



Source: Adapted from Wik, M.W., 2002, 'Revolution in Information Affairs: Tactical and Strategic Implications of Information Warfare and Information Operations', in A. Jones, G.L. Kovacich & P.G. Luzwick (eds.), *Global information warfare*, pp. 579–628, Auerbach Publications, Boca Raton/London/New York.

FIGURE 2: The Information Operations Process.

processes and ultimately actions and re-actions. This model is a detailed version the attack, consequences and reaction blocks in Figure 1.

Psychological operations: The Message Flow Model

The model for psychological operations proposed by Cox (1997:42) takes the form of a message flow, which is illustrated Figure 3. The message will be constructed in such a way that it coerces, deters or provides incentives to the target audience with regards to a specific behaviour or action (Cox 1997:42). The sender delivers the message via an instrument of power, such as the mass media or pamphlets, which results in a phenomenon that can be observed, interpreted and internalised by the target audience. The target audience react according to whether they support or oppose the message; the sender then re-evaluates the message by assessing this reaction (Cox 1997:42).

Network warfare

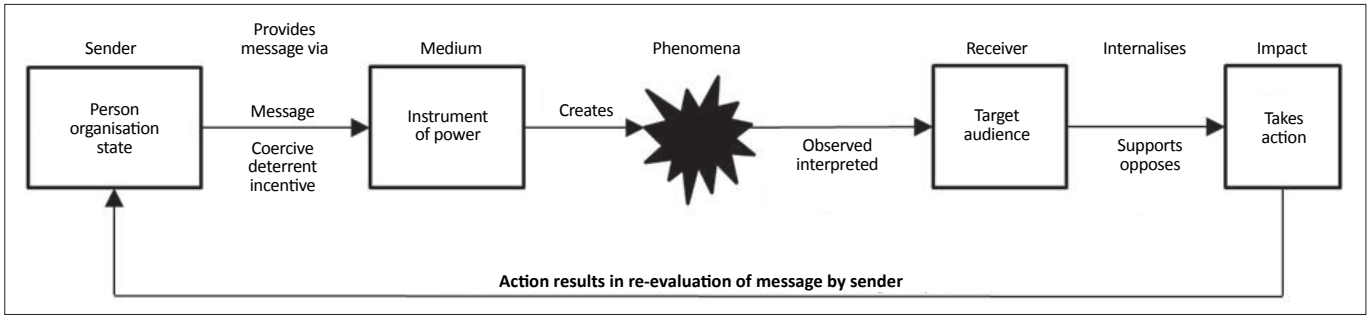
Veerasamy and Eloff (2008:100) proposed a network warfare framework; this can be seen in Figure 4. The framework includes factors that may constrain the use of network warfare and the intended target set. The syntactic level denotes the structured organisation of the networks, and the semantic level denotes the meaning of the received data (Veerasamy & Eloff 2008:103) and could be seen as related to the cognitive domain as it involves trust. Many of the principles contained in the framework are standard information security principles that should be internal to any organisation. Important concepts are covered under the 'approach' block: the defensive approaches may be preventative, where it is attempted to secure vulnerabilities to prevent an attack; the detective approach attempts to detect when an attack is occurring to take measures to mitigate the effects; and the reactive approach will focus on recovering from the attack once it has occurred. Generally, a combination of all three strategies is employed in what is known as 'defence-in-depth'.

Proposed Information Warfare Life Cycle Model

This section presents the proposed Information Warfare (IW) Life Cycle Model, which is illustrated in Figure 5. The model was generated by identifying common aspects from the models discussed in the earlier sections. The objective of generating this model is to create one that is scalable for various 'sized' incidents, has a mix of high-level concepts and detail to adequately describe the incident and is applicable to various forms of IW which may be distinct from each other, such as psychological operations and electronic warfare.

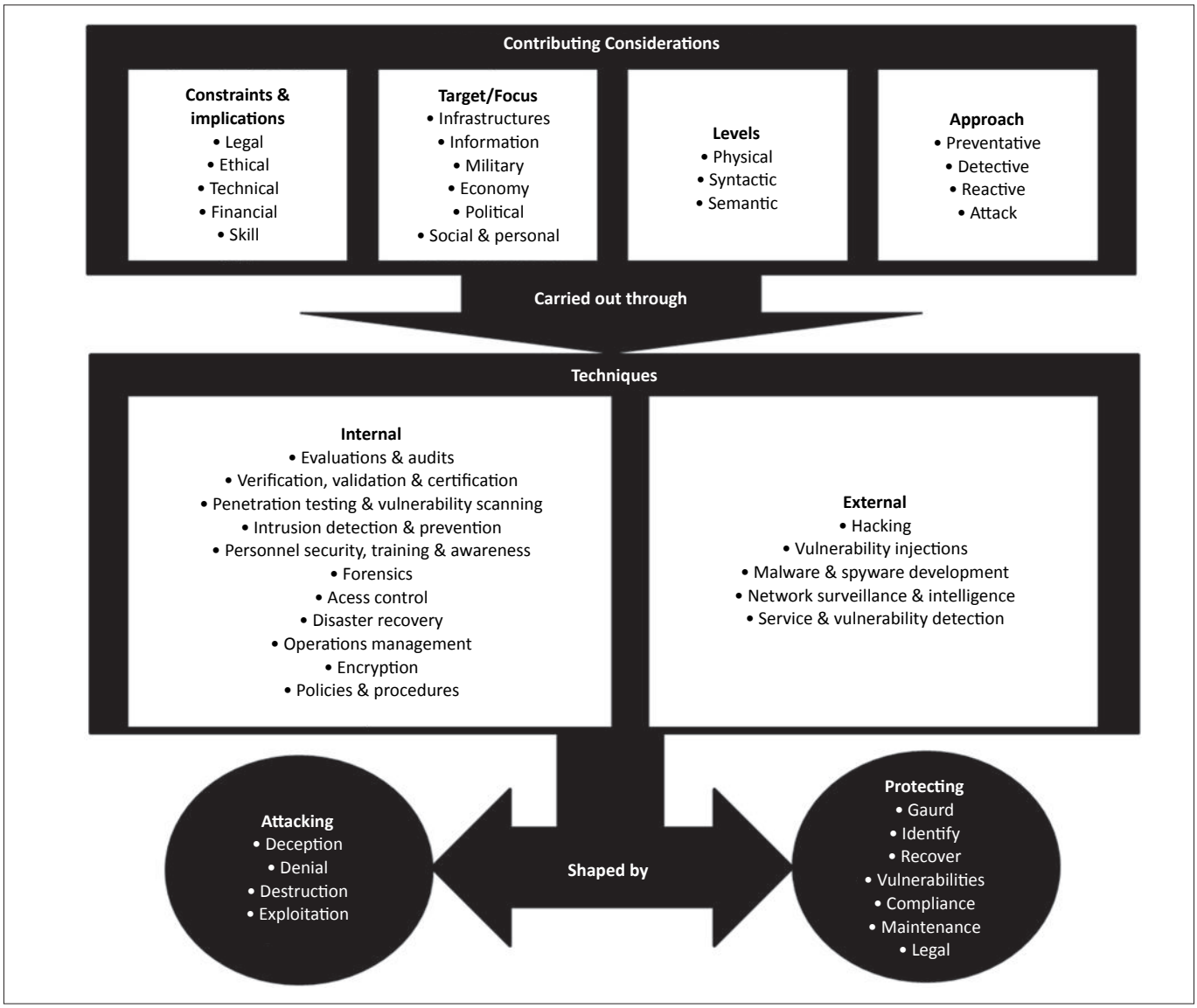
Through a review of the available literature, four models were identified which describe IW incidents or actions, as opposed to the models that described IW structures or attributes (presented in the background section). It appears that attempts to relate the IW structures and attributes to broader contexts and actual operational planning is limited to the four models identified; this corresponds to the claim by Armistead (2010:63) that there is still a disconnect between the technical issues and the broader context.

From Figures 1 to Figures 4, it can be seen that there are common aspects: there is some context to the IW operations, which includes an aggressor with a motivation to attack a target. Some planning is required for the operations, which include some restrictions, limitations and other considerations that may affect the operation and target selection. The attack commences against a target set, using offensive techniques and tools, whilst the target defends and protects against the attack with associated tools and techniques. The attack



Source: Adapted from Cox, L.-V., 1997, *Planning for psychological operations: a proposal,* Air Command and Staff College, Maxwell Air Force Base, Montgomery, Alabama, and Ramluckan, T., & van Niekerk, B., 2009, 'The Terrorism/Mass Media Symbiosys', *Journal of Information Warfare* 8(2), 1–12.

FIGURE 3: Message Flow Diagram.



Source: Adapted from Veerasamy, N. & Eloff, J., 2008, 'Understanding the Elementary Considerations in a Network Warfare Environment: An Introductory Framework', in *Proceedings of the Workshop on ICT uses in Warfare and the Safegarding of Peace*, pp. 95–108, CSIR, Pretoria.

FIGURE 4: Network Warfare Framework.

will result in some phenomena that will have an impact on the target set which has consequences for the society; this results in a reaction by the members of the target, their allies and observers. The reaction will by necessity constitute a bolstering of defences and an attempted recovery from the attack. The reactions and ability of the target to defend itself will result in a re-evaluation of the attack by the aggressor, and there will be some influence on the overall context. This may result in the initial target becoming the aggressor and retaliating against their attacker.

As many detailed models may overlap with multiple high-level concepts, a dual-layered cycle was developed. The high-level cycle contains the basic blocks of the IW life cycle the context, attack and defence, the consequences, reactions, recovery and influence on the context. This is overlaid with a more detailed cycle, which shows the applicability to multiple high-level concepts; for example the planning of operations would be performed with consideration to the current context and may be conducted for both attack and defence. The 'Attack' block contains multiple detailed constructs:

- the possible target set
- the functional areas that may be employed
- the offensive tactics
- the tools with which to conduct them.

The 'Defend and Protect' block similarly has the defensive techniques and tools. The society block overlaps four high-level concepts:

1. attack
2. defence
3. consequences
4. recovery.

The impact on society results in an impact on humans, who react; this results in the feedback to the 'Recovery', 'Defence' and 'Influence' blocks.

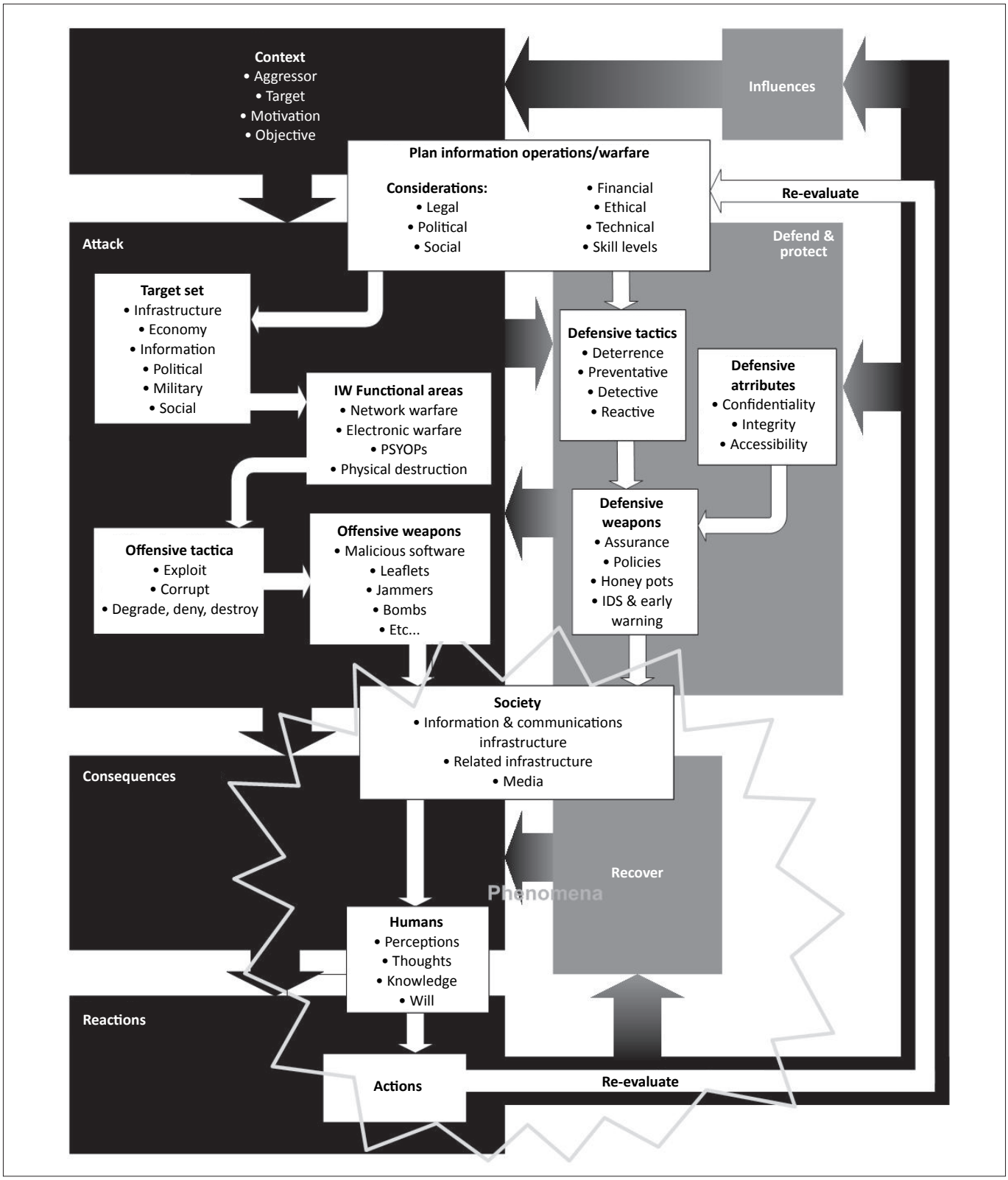


FIGURE 5: The Information Warfare Life cycle.

According to Armistead (2010:63), there is still a need to relate the issues surrounding many aspects of information operations and IW to broader contextual issues; the retention of the context block and the considerations in the planning block is an attempt to address that. These two blocks were drawn from the 'context' block proposed by Ventre (presented in Figure 1), the 'planning' block proposed by Wik (presented in Figure 2) and the consideration proposed by Veerasamy and Eloff (presented in Figure 4). The individual contexts and considerations will be unique to each incident or

situation and also for each national or organisational outlook. As a result, an in-depth discussion of such considerations is beyond the scope of this paper.

Application of the Information Warfare Life Cycle Model

This section illustrates the application of the proposed Information Warfare (IW) Life Cycle Model to historical and current examples of IW incidents. The following sections each focus on a specific incident; each incident falls within a different functional area of IW. These sections will provide a brief background to the incident and then apply the IW Life Cycle to the incident. As IW is a global phenomenon, the incidents will not be restricted to any one region or nation.

Estonia: Cyber-based attack on infrastructure

The background provided for this incident is a summary of the following sources: Landler and Markoff (2007), Rolski (2007), Germain (2008), and StrategyPage.com (2010b). The Estonian government decided to relocate a war memorial from the Second World War which also honoured Russian soldiers; many Ethnic Russians took offence to the relocation and the Estonian Embassy was attacked amidst street riots. On 26 and 27 April 2007, the signs of a distributed denial of service (DDoS) attack from botnets were becoming apparent; a few days later several newspaper websites were brought down. Estonia raised suspicion of Russian government involvement or backing in the attacks, which was denied. Defensive preparations began and many Internet service providers (ISPs) aided in blocking the traffic relating to the attacks. Prior to a public holiday celebrating the Soviet victory in the Second World War, additional defensive preparations were made; on 09 and 10 May 2007 a severe DDoS attack hit Estonia, the major bank had to shut down its online services, losing over $1 million. The government websites and email systems were also targeted and badly affected. The attacks subsided on 16 May 2007. As a result of the attacks, a cyber-defence centre was established in Estonia, and NATO members extended the alliance to include cyber-attacks.

The incident will now be analysed using the Life Cycle Model:

- **Context:** The aggressor(s) are ethnic Russians; the target is the Estonian Government; the motivation is to show political dissatisfaction and revenge for the relocation of a war memorial.
- **Attack:** Network warfare denial tactics were used against many websites; some psychological warfare was employed through network warfare by defacing government websites. Botnets were used to flood target websites with traffic.
- **Defence:** Initial defensive preparations by the Estonians were preventative; by requesting aid from international ISPs in blocking the denial-of-service traffic.
- **Consequences:** The impact of the initial attacks was relatively minor; a few newspaper websites were brought down. Later attacks managed to severely disrupt the major Estonian bank's online services; and damages exceeded $1 million.
- **Reaction:** Initial reaction by the Estonians was to increase defensive preparations for future attacks. After the incident was concluded, a cyber-protection centre was established.
- **Influence of context:** The influence on the initial context was minimal; however, political tensions were raised as Russia was accused of participating or sanctioning the attacks. The attacks eventually subsided; the international impact was that several nations expanded war treaties to include cyber-attacks.

The Channel Dash: Electronic warfare operations

This is a summary of a description of the 'Channel Dash' by Radloff, quoted by Sikwane (2010). In 1942 three German capital ships and a number of destroyers were ordered to return to their home base from a port in France, which necessitated transit through the English Channel. The German forces incrementally increased noise jamming (electronic warfare) against British radar stations in order to mimic atmospheric disturbances; the British fell for the deception and reduced the gain of the radar stations, and the German warships were therefore able to transit the English Channel undetected. When the British realised the deception, it was too late to intercept the warships.

What follows is an analysis of the incident using the IW Life Cycle Model:

- **Context:** German warships were required to transit the English Channel; the German electronic warfare units were the aggressor, with the aim of disrupting the English radar stations. As this was a time of war, there was very little in terms of restrictions that could possibly effect planning, other than technical capability.
- **Attack:** German units broadcast signals in such a manner that the English radar appeared to be malfunctioning due to atmospheric interference. The Germans used electronic warfare jamming equipment to interfere (degrade) the functionality of the British radar systems in such a manner to deceive the radar operators to further reduce the radar capability.
- **Defence and consequence:** The English radar operators reduced the gain on the radar units to mitigate the effects of the German interference. The German warships were able to transit the English Channel with the English radar unable to fully detect them.
- **Recovery and reaction:** The British realised there was deception and returned the radars to their normal operating conditions; however, it was too late to intercept the warships.
- **Influence on context:** The Germans successfully completed their objective.

Somalia (Blackhawk Down): Psychological operations

United States (US) forces entered Somalia to assist the United Nations forces that were providing aid and were continuously being raided by the Somali militias; the US forces began

targeting a specific warlord, Mohammed Farah Aidid. After a series of raids, the incident known as 'Black Hawk Down' occurred, where a US serviceman was captured and five killed in the skirmish (Adams 1998:67–75). Televised images of the bodies of the US servicemen were broadcast by CNN; the shock to the US public resulted in them successfully pressuring the government into withdrawing the remaining troops from Somalia (Adams 1998:74–75; Taylor 2002:24). The US government and public were completely unprepared for this type of attack; the incident and the withdrawal also resulted in negative media towards the US government, military command, and policies (Adams 1998:75–77).

What follows is an analysis of the incident using the IW Life Cycle Model:

- **Context:** United States servicemen had been involved in a skirmish infamously known as the 'Black Hawk Down' incident. Mohammed Farah Aidid (the Somali warlord) wished to drive US forces out of Somalia; his target was the US public.
- **Attack:** The bodies of US servicemen killed in the skirmish were dragged in front of CNN cameras to psychologically shock the US public (psychological operations); the mass media was the 'weapon' of choice. The planning was to affect the morale, will and society of the US public.
- **Defence:** This type of attack came as a surprise; consequently there was no defence. Once the images were released, there was nothing the United States of America could do to defend themselves from this attack. There was a reactive defence in terms of locating and extracting any servicemen held hostage before the withdrawal.
- **Consequences and reaction:** The US public were horrified by the images; and put pressure on the US government to withdraw from Somalia. This was eventually done; however, there was continuing negative media and reactions by the US public.
- **Influence on context:** The Somali warlord was able to effectively defeat the US forces through the strategic use of the media resulting in the withdrawal of the troops; the existing context in Somalia was therefore completely altered as well as the political context in the US.

Wikileaks incidents – cyber-based conflict

This is the most complex of the case studies as it comprises of a number of 'sub-incidents', where sets of compromised documents were released online by the Wikileaks, eventually provoking a retaliation by the US government, which in turn resulted in a series of cyber-based attacks and counter-attacks by the supporters of the different 'factions'. Whilst this is by no means a cyber-war between nation states, it can be seen as a cyber-conflict and has the characteristics that a major cyber-war may exhibit in terms of the action-reaction cycle of the main protagonists and their supporters.

Wikileaks attempts to make available information that is not usually accessible to the public, primarily on occurrences or activities that may be considered irregular, claiming to be advocating for greater transparency. Throughout the course of the year, there have been major releases of compromised documents that have targeted the US military and to some extent the government. Some of the releases received media attention from a number of media 'partners' across the world. The initial responses to the release of the war log documents only appeared to have been met with public condemnation and an internal investigation into the source of the leak; there did not appear to be any direct retaliation against Wikileaks. The release of the diplomatic cables was met by a far stronger reaction. The following is a chronological list of occurrences that contribute to this incident.

- In April 2010 a video of a US helicopter gunship firing on what turned out to be journalists was released (Bronstein 2010); however, there was debate around some claims that arose from the video (StrategyPage.com 2010a).
- In June 2010 a US intelligence analyst was arrested for releasing classified documents after a probe (Poulsen & Zetter 2010). He appears to have also taken the blame for later releases.
- In July 2010 Wikileaks released logs of the conflict in Afghanistan (Poulsen 2010).
- In October 2010 similar logs were released for the Iraq conflict (Stewart 2010).
- On 29 November 2010 Wikileaks released a series of diplomatic cables. A pro-US hacker conducted a DDoS attack against Wikileaks (Goodwins 2010).
- The US puts pressure to remove Wikileaks from the Internet domain registry, and block the financial accounts, notably PayPal, Visa, Mastercard, Amazon and a Swiss bank called Post Finance in a period from 04 to 08 December 2010. Most of the organisations do cancel the accounts and registrations (Walker 2010). Rape accusations also re-surfaced against Julian Assange and queries over some of Wikileaks finances are raised (Gilligan 2010).
- On 04 December 2010, the PayPal blog experiences a DDoS attack by a pro-Wikileaks group called Anonymous; on 06 December 2010 the main PayPal website and the website of the Swiss bank are attacked, and Anonymous's website is counterattacked (Walker 2010).
- On 07 December 2010 Anonymous attacks the website of Assange's prosecutors, EveryDNS (for delisting Wikileaks), a US Senate website, the lawyers of the rape accusers and the Swiss bank; there was a counter-attack against Anonymous which appears to be retaliation for the attack on the Senate website (Walker 2010).
- On 08 December 2010 Anonymous attacks the Mastercard, Visa and Paypal websites, the attack on the lawyer's website is ongoing, and Twitter disables Anonymous' account (Walker 2010).
- On the 09 December 2010 Amazon is attacked and the attack on PayPal continues; counter-attacks against Anonymous are also ongoing (Walker 2010).

The following is an application of the IW Life Cycle Model to the first iteration of the incident:

- **Context:** Wikileaks claims to promote transparency and may have been motivated to attempt to discredit the USA.

- **Attack:** Sensitive documents were obtained by an insider, breaching confidentiality of a sensitive intelligence network. Wikileaks release these documents in a number of batches, each release being publicised though the media and online; this appears to be a pseudo-psychological operation.
- **Defence and reaction:** The primary defence strategy appeared to be reactive. The initial response was to publicly denounce the releases. An internal investigation resulted in the arrest of the alleged source of the leak. The release of the diplomatic cables was met with a stronger reaction; a pro-US hacker conducted a DDoS attack against Wikileaks and a number of organisations were pressured into removing support for Wikileaks. These appear to be a combination of reactive and preventative measures.
- **Consequences and influence on context:** International society was impacted (and divided) in that a 'superpower' had been discredited and the source of the attacks was controversial; there is some support for both factions. The context became more politically heated and a number of vigilante groups became involved.

What follows is an application IW Life Cycle Model to the second iteration of the incident:

- **Context:** Wikileaks released a series of sensitive documents in an attempt to discredit the USA. Global opinion over the releases is divided. The USA attacks Wikileaks through diplomatic pressure and a vigilante group also targets Wikileaks.
- **Attack:** A vigilante hacker conducts a DDoS against Wikileaks to disrupt the ability to release the store of the diplomatic cables. The USA pressures various organisations to withdraw support from Wikileaks.
- **Defence:** Wikileaks reacted by trying to preserve the accessibility to the information; visitors were directed to the main website by the IP address; and many other websites that had managed to access the content made it available.
- **Consequences and influence on context:** The global community became more polarised into those who supported the USA and those who supported Wikileaks. Vigilantes began targeting organisations that submitted to US pressure and withdrew support and services from Wikileaks.

What follows is an application of the IW Life Cycle Model to the first iteration of the incident:

- **Context:** The USA reacted to the document releases by pressuring organisations to withdraw services and support of Wikileaks; and a vigilante had attacked the Wikileaks websites. As a result, a group of vigilante hackers counter-attacked the pro-USA hacker and the organisations that withdrew support.
- **Attack:** The vigilante hacker group known as Anonymous launched DDoS attacks against PayPal, Amazon, Visa, Mastercard, a Swiss bank and various other websites.
- **Defence:** The targeted organisations appear to have attempted to 'ride out' the DDoS attacks. The pro-US hacker counter-attacked Anonymous. Twitter disabled the Anonymous account.
- **Consequences and influence on context:** Many individuals were unable to use or access the websites targeted; this proved a source of frustration for them; this probably reduce support for the Anonymous group to some degree. A series of web-based DDoS attacks and counterattacks between pro-USA and pro-Wikileaks hackers resulted.

Summary

The IW Life Cycle Model was applied to five incidents of varying scale and with different focus areas that fall within information warfare. The model could describe each incident in sufficient detail (which is limited to the information available for the respective incident) for different functional areas of information warfare namely, (1) psychological operations, (2) network warfare, (3) electronic warfare and deception and (4) the Wikileaks incident that constitutes a number of functional areas. The model was capable of describing the incidents; and for larger and more complex incidents such as Wikileaks, was able to describe them through multiple iterations. The model therefore meets its objectives of being scalable, applicable to different functional areas, and providing both high-level and detailed descriptions of incidents.

Conclusion

Information warfare comprises a number of disciplines and the existing models that are used to describe incidents where information warfare tactics are employed are either specific to a discipline or of a high-level nature. The need for a standardised model of IW was identified. This paper proposes a scalable model that incorporates characteristics that are common amongst existing models; it was intended to exhibit both high-level and detailed concepts to accurately describe the life cycle of an information warfare incident. The objective of the model was to consolidate the various theories of which IW comprises into a single model. The proposed IW Life Cycle Model was applied to a number of historical and current incidents to illustrate its scalability and applicability to various disciplines. The model adequately described these incidents.

Acknowledgements

The first author has received grants from the South African Department of Defence and Armscor Ledger Program through the Cyber Defence Research Group at the Council for Scientific and Industrial Research, Defence, Peace, Safety and Security (CSIR-DPSS), and the University of KwaZulu-Natal for his PhD research, of which this paper forms part.

Authors' contributions

The first author provided the content as part of a PhD thesis. The second author is the PhD supervisor and provided fact checking and suggestions.

Author competing interests

The authors declare that they have no financial or personal relationship(s) which may have inappropriately influenced them in writing this paper.

References

Adams, J., 1998, *The next world war,* Arrow Books, London.

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

Borden, A., 1999, 'What is information warfare?', in *Air & Space Power Journal*, viewed 02 July 2009, from http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html

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.

Bronstein, P., 2010, *The Wikileaks incident: how social media has changed warfare coverage*, The Huffington Post, viewed 07 April 2010, from: http://www.huffingtonpost.com/phil-bronstein/the-wikileaks-incident-ho_b_527788.html

Chatterji, S.K., 2008, 'An Overview of Information Operations in the Indian Army', *IOSphere,* special edition, 10–14.

Cox, L.-V., 1997, *Planning for psychological operations: a proposal,* Air Command and Staff College, Maxwell Air Force Base, Montgomery, Alabama.

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

Germain, J.M., 2008, *The art of cyber warfare, part 1: the digital battlefield*, TechNewsWorld, viewed 01 September 2009, from http://www.technewsworld.com/story/The-Art-of-Cyber-Warfare-Part-1-The-Digital-Battlefield-62779.html

Gilligan, A., 2010, 'Now Wikileaks suffers its own leaks', in *The Telegraph*, viewed 13 December 2010, from http://www.telegraph.co.uk/news/worldnews/wikileaks/8196946/Now-Wikileaks-suffers-its-own-leaks.html

Goodwins, R., 2010, *Wikileaks shows US cyber intelligence at work, gets DDoS attack*, ZDNET, viewed 29 November 2010, from http://www.zdnet.co.uk/blogs/mixed-signals-10000051/wikileaks-shows-us-cyber-intelligence-at-work-gets-ddos-attack-10021175/

Hutchinson, B. & Warren, M., 2001, *Information warfare: corporate attack and defense in a digital world*, Butterworth Heinemann, Oxford/Auckland.

Kopp, C., 2000, 'A Fundamental Paradigm of Infowar', *Systems*, 31–38.

Landler, M. & Markoff, J., 2007, 'Digital fears emerge after data siege in estonia', in *The New York Times Online*, viewed 14 April 2010, from http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1

Poulsen, K., 2010, *Wikileaks Releases Stunning Afghan War Logs - Is Iraq Next?,* Wired.com Threatlevel, viewed 26 July 2010, from http://www.wired.com/threatlevel/2010/07/wikileaks-afghan/

Poulsen, K. & Zetter, K., 2010, *U.S. intelligence analyst arrested in Wikileaks video probe*, Wired.com Threatlevel, viewed 07 June 2010, from http://www.wired.com/threatlevel/2010/06/leak/

Ramluckan, T., & van Niekerk, B., 2009, 'The Terrorism/Mass Media Symbiosys', *Journal of Information Warfare* 8(2), 1–12.

Rolski, T., 2007, 'Estonia: ground zero for World's first cyber war', in *ABC News*, viewed 23 September 2009, from http://abcnews.go.com/print?id=3184122

Sikwane, B., 2010, 'The art of hide and seek in warfare', in *Aardvark AOC*, viewed 29 December 2010, from http://aardvarkaoc.co.za/index_files/Page316.htm

Stewart, P., 2010, 'Pentagon braces for huge wikileaks dump on Iraq war', in *Yahoo News*, viewed 18 October 2010, from http://news.yahoo.com/s/nm/us_usa_iraq_leaks

StrategyPage.com, 2010a, *What was not said*, viewed 12 April 2010, from http://www.strategypage.com/htmw/htiw/articles/20100411.aspx

StrategyPage.com, 2010b, *The NATO cyber war agreement*, viewed 03 May 2010, from http://www.strategypage.com/htmw/htiw/articles/20100501.aspx

Taylor, P.M., 2002, 'Perception Management and the "War" Against Terrorism', *Journal of Information Warfare* 1(3), 16–29.

United States Air Force, 1998, *Information Operations*, (Air Force Doctrine Document 2–5), United States Air Force, Washington, DC.

Van Niekerk, B. & Maharaj, M.S., (in press), 'Relevance of Information Warfare Models to Critical Infrastructure Protection,' *Scientia Militaria.*

Veerasamy, N. & Eloff, J., 2008, 'Understanding the Elementary Considerations in a Network Warfare Environment: An Introductory Framework', in *Proceedings of the Workshop on ICT uses in Warfare and the Safegarding of Peace*, pp. 95–108, CSIR, Pretoria.

Ventre, D., 2009, *Information warfare*, ISTE, London, UK.

Walker, R., 2010, *A brief history of operation payback*, Salon.com, viewed 21 December 2010, from http://mobile.salon.com/news/feature/2010/12/09/Waltz, E., 1998, *Information warfare: principles and operations*, Artech House, Boston/London.

Wik, M.W., 2002, 'Revolution in Information Affairs: Tactical and Strategic Implications of Information Warfare and Information Operations', in A. Jones, G.L. Kovacich & P.G. Luzwick (eds.), *Global information warfare*, pp. 579–628, Auerbach Publications, Boca Raton/London/New York.