INFORMATION-BASED CONFLICT IN AFRICA

Brett van Niekerk and Manoj S Maharaj
School of Information Systems and Technology,
University of KwaZulu-Natal

Abstract

For a long time, the African continent was regarded as the 'Dark Continent'. The rapid assimilation of information technologies into the African economies has placed Africa firmly on a trajectory that will see it compete and integrate with the developed world. As nations and organisations become more information-centric, it is natural that conflicts and competition amongst the various nations or organisations will become increasingly information-based. In this article, the authors reflect upon information-based conflict in Africa. Areas of information conflict that are discussed include censorship, communications intercepts, the use of information and communications to instigate violence and uprisings, and the possibility of cyber-warfare. The article shows that the use of technology to conduct information conflict in Africa is prevalent, and that it is likely to increase.

Introduction

The current Information Age is characterised by rapid advances in telecommunications and networking technologies, which are driving globalisation. Multi-national corporations, previously geographically, economically and politically confined, now find themselves competing with each other amongst a myriad of national and international laws and frameworks. Additionally, political and religious ideologies compete for dominance and survival, while nations compete economically, politically and militarily. In such a milieu, conflict is inevitable, and with the reliance on information, this conflict will become increasingly information-based. Information-based conflict can therefore be seen as a major factor in the effectiveness of nations and organisations.[1]

Information conflict is 'concerned with how information is used in disputes, disagreements, conflicts, and survival contests and with how the information technology infrastructure influences such situations'.[2] Information warfare is defined as 'actions taken to defend the military's information-

Scientia Militaria, South African Journal of Military Studies, Vol 41, Nr 2, 2013, pp. 24-41.
doi : 10.5787/41-2-1066

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'.[3] From these definitions, information-based conflict can be considered actions to compete against an adversary where the primary tool is information or information technology. Information-based conflict is not necessarily limited to a military context, but is applicable to all forms of competition where information is the defining factor of success.

Information-based conflict is shifting in the direction of cyber-based conflict. Three instances of politically motivated national-scale distributed denial-of-service (DDoS) attacks have occurred: Estonia in 2007, Georgia in 2008, and Myanmar in 2010.[4] Websites in South Korea and the United States also experienced DDoS attacks in 2009, and social media websites were reportedly targeted in order to silence political statements in posts.[5,6]

This article reflects on incidents of information-based conflict in Africa and factors affecting information-based conflict on the continent. The discussion focuses on communications interceptions, censorship, socio-political power dynamics, the instigation of violence, and cyber-warfare. The following section presents a historical background to information conflict in Africa.

Historical background

Africa has a long history of conflict and political intrigue. During the years of the Cold War, there was a proxy conflict in Africa between the ideologies of the United States and those of Cuba and Russia. In many instances, information was the main commodity in these conflicts. This section provides a background to the role of information and related technologies in conflict and political competition across the African continent.

One of the longest and most infamous conflicts was that of the struggle against the oppression of the Apartheid government of South Africa. This government imposed strong censorship on the media.[7] Images or sound recordings of anti-Apartheid protests were banned so as to deny the protestors a stage from which to gain international sympathy.[8] During this period, South Africa, Rhodesia (now Zimbabwe, and colonial Mozambique were involved in a border war against insurgents and in the Angolan conflict. What is interesting to note is that acts of international terrorism (acts of terrorism where individuals from more than one nation are involved) in South Africa that were recorded by the United States Department of State increased after the end of Apartheid.[9,10] This is potentially due to the freeing of the press, where the bombings that occurred achieved wider publicity than they would have previously, and these were symbolically anti-American. Attacks during the Apartheid era were used as an excuse by the South African government to continue their oppressive policies.[11] The military campaigns often required detailed information. Specific addresses or locations were required before a raid could be mounted on an insurgency route; broad information on which route was to be targeted was not sufficient. At times, the South African Air Force sorties had to be timed to coincide with the times that the Soviet-manufactured fighters in Angola were refuelling to prevent casualties, as the South African aircraft were outclassed.[12] This illustrates that information (in the form of intelligence) was crucial for the South African Air Force remaining effective in the Angolan conflict. Information also had a strategic dimension: during this conflict, a Soviet-manufactured air defence system was captured by South African forces. As this was the first captured device, South Africa had important intelligence to trade.[13] Towards the end of Apartheid, the African National Congress (ANC) began employing computers and modems to form an underground communications network, codenamed Operation Vula.[14] The introduction of computers as part of the ANC's communication network is a signifier that eventually information technology will inevitably play a role in any conflict where information is a key asset.

During Rhodesian counter-insurgency operations, a Special Forces unit known as the Selous Scouts was deployed. They used information from captured insurgents or recruited former insurgents to learn the location of training camps and supply routes and the protocols to gain entry to the bases. Operatives then impersonated guerrilla fighters and infiltrated the insurgent's networks, and passed intelligence to other forces that carried out the actual raids.[15] Such a unit illustrates two points: the importance of current and accurate intelligence in a conflict, and the relevance of deception as an information weapon. During the Rwandan genocide in 1994, the most common weapon was the machete. As there was an arms embargo on the country, it was easier to import agricultural equipment and then use those as weapons. Those arms that were being imported prior to the embargo were re-routed through Zaire.[16] This was also a form of deception, as it appeared that Rwanda was conforming to the restrictions; however, the true intention was to gather improvised weapons or re-route arms through another country.

During the Rwandan genocide, the violence needed to be incited. This was done through radio broadcasts, which advocated the genocide and spread hate messages against particular ethnic groups.[17] This illustrates the use of mass communications in a conflict where ethnic populations were mobilised against each other to commit genocide. In Somalia, the mass media also proved to be an effective tool. After the incident commonly known as ‘Black Hawk Down’, the bodies of US servicemen killed in the skirmish were defiled in front of CNN cameras. The shock of these images resulted in the US public pressurising their government to withdraw from Somalia.[18] These incidents illustrate the power of information broadcast via the mass media. A few strategic images or words can sway a large population, who react and pressure the respective governments or militaries into specific actions. During the peacekeeping and aid missions in Somalia, the US forces were also at a disadvantage due to the lack of intelligence and cultural understanding. Sophisticated electronic surveillance equipment was deployed, but was ineffective as the Somalis used drums and hand-held radios to communicate.[19]

Chau describes how the People’s Republic of China (PRC) used various actions in Ghana from 1958 to 1966 to further their strategic objectives in what was termed ‘political warfare’.[20] This included using non-governmental organisations and an acrobatic troupe to gather information and provide positive perceptions of the PRC. Ghana provided international support for the admittance of the PRC to the United Nations, and in return, China operated training camps for guerrilla operations and political ideology to produce freedom fighters for operations against South Africa, Mozambique and Rhodesia. There were also public communications between the PRC and the Ghanaian government and the people. The PRC involvement in Ghana appeared to be a short-term failure when diplomatic relations soured in 1966 after the Ghanaian government was ousted by a coup. However, these relations were restored in 1972 and appeared strong in the early 2000s, indicating that the political warfare was a long-term success.[21] This case illustrates that information gathering and perception management may have long-term benefits in addition to any obvious short-term benefits. Despite the ending of a temporary cessation of diplomatic relations, the PRC had some platform from which to renew those relations and the PRC has been able to continue with its strategic objectives.

In a public address, Museveni, a president of Uganda, described the requirements and actions of revolutionaries in Africa. A number of points raised were concerning information.[22] Concepts such as making quick decisions, the fact that revolutionaries are primarily ideologically inclined, and the need to ensure the population had good perceptions of the revolutionaries were mentioned. Basic information security practices were also raised, which reduced the risk of plans being captured and leaks through communications intercepts occurring.[23] From this description, three main areas of information conflict were prominent: a conflict of ideologies, a conflict of perception management, and an intelligence-based conflict.

Wardini indicates that information technology is slowly being introduced into Senegal; however, it is not established enough for full information warfare capabilities. Therefore, the basis of information warfare in Senegal is psychological warfare.[24] Brazzoli warns that it may be possible to purchase and rapidly implement technological solutions; therefore, it is perilous to assume African nations will be technologically inferior.[25] An illustration of this point is that two of the world's poorest nations, Eritrea and Ethiopia, fielded advanced military platforms in their border war.[26] Whilst Africa is considered as a developing continent, historical examples illustrate that information conflict still occurs, and can be won against a technologically superior adversary through the improvised use of available technologies.

Political conflict and instigation of violence

This section discusses information in political conflict and violence. The historical background described the genocide in Rwanda, information-related concepts for revolution in Africa, and Chinese strategic political positioning in Ghana. The examples covered in this section include the incitement of ethnic violence, popular social uprisings, and other forms of political protest occurring in Africa during the 21st century.

Following the December 2007 Kenyan elections, attempts to incite political and ethnic violence occurred. While radio broadcasts were used in Rwanda, text-messaging services on mobile phones were used in Kenya in addition to radio broadcasts. The text messages incited violence against specific ethnic groups or told the recipients to join a march opposing the election results and asking for the message to be resent to others. The incitement did have some traction, and tribal attacks occurred. The opposition leader was investigated by human rights commissions for inciting the violence.[27] The text messages may simply have provided the impetus for an already fragile political situation. South Africa experienced xenophobic violence that was incited by creating a perception that foreigners were taking jobs and South Africans were then faced with unemployment, and other attempts to dehumanise foreign nationals.[28] Reports indicated that local leaders instigated the attacks to further their personal political and economic objectives, and that reports and images of the violence in the media further enticed this activity.[29] Such violence and conflict are based on the creation of a perception or idea that the target group is the cause of the negative aspects of any situation. The conflict is further inflamed by dehumanising the target population. Ethnic violence is thus clearly an ideological and perceptual conflict. That this type of conflict can now take on national, regional and possible greater dimensions is largely due to communication technologies enabling the distribution of messages inciting populations to protest or commit violent acts.

In 2010, Mozambique experienced violent protests against rising food prices. Text messages were used to incite the protests.[30] In 2011, a popular uprising began in Tunisia against perceived government corruption and poor living conditions, which spread to Egypt and then Libya. The mass protest in both Tunisia and Egypt exhibited large-scale use of social media and mobile devices.[31,32] These incidents further illustrate the power of perception and the role of modern communication technologies in political conflicts. When a large portion of a population shares discontent and this is spread with an incitement to action, popular uprisings against a government can occur. Such tactics could potentially be used by opposition political parties to create political instability from which they could benefit. While South Africa has also experienced protests (sometimes violent) over poor service delivery due to perceived incompetence or apathy of government officials, these have been largely localised.[33] However, it is entirely possible and likely that rapid and persistent communications between disgruntled communities could cause these protests to become widespread; thus, increasing political pressure on the national government. An example that this has already occurred is the spreading of labour unrest from the mining sector to the manufacturing and farming sectors in South Africa.[34,35] The hacktivist[36] group Anonymous uses social media to distribute anti-government messages, and some of these are directed at the South African government.[37,38] Anti-government messages do not necessarily originate from the majority population; however, through the effective use of technology they can be made more visible and influence the perceptions of wider audiences. Such use already has had an impact on the political landscape in Africa due the Tunisian and Egyptian protests, and has potential to become an effective and prominent political tool in Africa.

Both Brazzoli and Wardini focus on social and psychological aspects as an important component of information warfare in Africa. Brazzoli considers the ability to influence the perceptions of a target audience through psychological operations as a fourth instrument of power in addition to the military, political and economic powers.[39] As an illustration of the importance of the psychological component of information conflict, Wardini comments that Senegal’s priority is not the technical aspects of information warfare (such as cyber-warfare or electronic warfare), but winning the confidence of their domestic population with respect to an internal conflict.[40]

Censorship and tracking

Information conflict in Africa often constitutes strong censorship or tracking of people and their information. The example of the Apartheid regime in South Africa and the white minority Rhodesian government was presented in the historical background. Such activity of censorship and the tracking of social groups that are considered malicious by the state continue in Africa, and will be discussed in this section. For the purposes of this article, 'tracking' will comprise both the gathering of information about the location of a person or an object, or the interception of communications.

Eritrea is listed as the country with the most press censorship globally, and Equatorial Guinea is listed in the top ten nations with strict censorship. Eritrea reportedly controls all domestic media and has banned any foreign media.[41] During the March 2012 military coup in Mali, the media experienced "an hours-long blackout".[42] Mavhunga reports a number of actions denying accessibility to information and monitoring of communications in an internal information conflict in Zimbabwe. Incidents include anti-government hacktivism, where legitimate information on webpages is replaced by anti-government slogans, and attempts at monitoring or blocking web pages, emails, mobile phones and the nation's Internet gateway by government, possibly with foreign assistance, and DDoS attacks against online newspapers were also reported.[43]

In South Africa, the Regulation of Interceptions of Communications Act (RICA) makes allowance for law enforcement to intercept communications, and ensures that communication service providers make provision for law enforcement to access the required information.[44] The South African government is attempting to pass bills that could potentially result in more powers to censor information and monitor communications. The proposed Protection of State Information Bill has received criticism and there are claims that it is unconstitutional.[45] It has also received criticism from a number of countries at the United Nations due to concerns that the proposed acts could be used to impede freedom of speech and the media under the guise of national security.[46] There were also reports of a new bill, the Intelligence General Laws Amendment Bill, proposed in 2012, which would provide intelligence services in South Africa with the legal grounds to intercept domestic communications without a warrant.[47] Like with the Protection of State Information Bill, the Intelligence General Laws Amendment Bill has been criticised as being unconstitutional, and there are claims that the two bills will turn South Africa into a police state.[48] However, dialogue has been entered into to alleviate fears and clauses in these acts, and the Intelligence General Laws Amendment Act restricts the intelligence agencies to adhere to RICA[49]. The Protection of State Information Bill seeks to restrict when state information can be released, and therefore can be seen as a form of censorship. It is not clear how this Bill will cater for information made publicly available external to South Africa. The Intelligence General Laws Amendment Bill seeks to provide additional legal power to the state to monitor communications and potentially track individuals. A danger with such laws is that government could abuse the intelligence and security services to conduct political warfare against opposition political parties. Legislation is an important aspect of information conflict, as it either limits or makes provision for certain activities, which can be used to conduct information-based conflict.

During the Arab Spring events of 2011, the affected governments attempted to monitor or block communications. The Tunisian government attempted to gain access and then delete the social media profiles of the protest leaders.[50] The Egyptian government blocked all mobile phone, social media and Internet connectivity.[51] Since the removal of the Libyan government, details have become available of the advanced communications interception capabilities of the Libyan intelligence services. The intercept technologies allowed the intelligence services to monitor browsing histories, instant messaging, file transfers, emails, and voice-over-IP communications, and cross-referenced these intercepts with phone taps. The gathered intercepts could be searched using a variety of criteria, and it appears the system was operational since 2009.[52] Due to the fear of political protests being sparked through social media, Uganda also blocked access to these websites.[53] There were also reports of a website reporting irregularities in the 2011 Zambian elections being blocked for a few hours.[54] During the 2012 food riots in Mozambique, the government blocked SMS services in an attempt to reduce the rioting.[55] The Sudanese government threatened to “unleash cyber jihadists” against any online political dissent following growing criticism of the government on social media; however, no evidence of online retaliation by the government was reported.[56] The effectiveness of government attempts in blocking the communications to limit the protests was mixed. The attempts in North Africa ultimately failed, with changes in government being affected in all countries. This could be attributed to the fact that the protests had gained significant momentum and the use of social media had become a support mechanism rather than a primary instigation method by the time the governments began restricting their use. Other attempts that were proactive rather than reactive appeared to have a measure of success; however, the dissatisfaction may never have reached the levels on the North African protests. A strategy to mitigate protests would be to engage disgruntled populations proactively with dialogue on the relevant communication mediums. Should this fail, then these mediums could be restricted in an attempt to prevent escalation into widespread protests.

Piracy has become a problem off the East coast of Africa, particularly in the Gulf of Aden. Due to the armed nature of piracy, and the military response to it, piracy is considered as a conflict. From an information perspective, this is conflict of hiding and tracking the movements of pirates and shipping, and sharing information. The pirates are able to work effectively and co-ordinate attacks or negotiate for the release of hostages through the use of mobile phones.[57] There are reports that the pirates are able to identify their targets by receiving shipping information via satellite phones from informants in Europe.[58] Various other open sources of information also provide information on shipping, such as http://www.sailwx.info/shiptrack/shiplocations.phtml. The availability of shipping information and international communications, enables pirates to select targets and time their attacks. Restricting this information may assist in hindering the pirate attacks. A number of nations have responded to the threat of piracy; however, there are political tensions between some of them. Therefore, a neutral communications channel has been introduced to allow naval vessels from all nations operating against the pirates to co-ordinate their efforts. Combined with increased aerial surveillance, the ability of the pirates to attack shipping has been hindered.[59] Both the Somali pirates and the insurgency group Al-Shabaab report on their activities through social media, which could provide a means of tracking them. By collecting data from various online sources, the media and security organisations, a representation of the Somali pirate’s social networking web has been created. However, as shipping companies are required to disclose information, similar techniques could be used by the pirates.[60] Despite being required to make some information available, shipping companies often do not report pirate attacks because of fears that their reputation will be damaged and to avoid the insurance costs.[61] There are also reports of the United States running surveillance from unmarked aircraft in Northern Africa. These aircraft support intelligence and Special Operations Forces in Africa, and are tracking suspected radical groups. The equipment the aircraft carry can intercept mobile phone and radio signals, and record video and heat signatures.[62] These issues of piracy and the related use of information indicate that information conflicts in Africa can have global economic and military impacts.

The incidents described in this section and the historical background indicate that censorship and monitoring of communications is a prevalent and on-going theme in Africa. Social media has proved to be a useful tool for advocating social and political ideologies; however, it also aids those who wish to monitor communications and track individuals. Both Zimbabwe and Libya have shown that sophisticated surveillance and jamming equipment can be obtained and rapidly deployed to affect the availability and confidentiality of communications en masse. Due to the possible continuing socio-economic and political dissatisfaction in a number of African countries,[63] online dissent may continue, thereby necessitating increased surveillance capabilities in the eyes of the respective governments. As many of these incidents are related to online actions, the next section provides a more detailed discussion on cyber warfare and cyber security in Africa.

Cyber-warfare and cyber-security

The previous sections have illustrated that the online aspects of information conflict in Africa are becoming increasingly prevalent. Therefore there is a need to discuss the capabilities for cyber-warfare and cyber-security in Africa.

Giacomello provides two lists ranking the cyber-warfare capabilities of nations: South Africa was the only listed African nation on the modified US Department of Defense list, ranked at 22. The list generated by Giacomello ranks five African countries out of a total of 59. The Ivory Coast and Madagascar were listed amongst twenty countries with insufficient data to rank.[64] A more recent study conducted by the Technolytics Institute lists six African countries out of a total of 67.[65] The rankings are compared in Table 1.

Table 1: Cyber-warfare capability rankings of African nations

	2009 ranking[66]	**2003 ranking**[67]
Angola	65	
Egypt	18	
Ghana		56
Kenya		56
Libya	30	
Morocco	32	
Nigeria		48
South Africa	34	37
Uganda	63	
Zimbabwe		55

As South Africa is the only nation listed in all three rankings, it can be said to have the most consistent capability, and appears to have improved from 37 of 59 to 32 of 67. Given the concerns regarding Zimbabwe’s internal cyber-conflict, and the Arab Spring events in 2011, it is clear that Egypt, Libya, Tunisia, Uganda and Zimbabwe have some cyber-capability. All of these nations, other than Tunisia, appear on one of the lists in Table 1.

Carr raised concerns that computers in Africa are susceptible to infection by malicious software (‘malware’), which can be exploited to form a large botnet (a network of infected computers controlled by an attacker). Such a botnet could be used as a cyber-weapon to launch large-scale DDoS attacks, or to distribute large quantities of spam or fraudulent emails.[68] Microsoft reports show that African countries have high infection rates of malware, and in particular South Africa had a very high rate of botnet infections from October 2009 to June 2010.[69,70] In addition to the high infection rates, a combination of other factors could also contribute to Africa being targeted. These include a high prevalence of software piracy and a low awareness of information security amongst the general population in Africa, which result in a high vulnerability to malware infections.[71] The rapidly increasing international bandwidth along the coast of Africa due to multiple new undersea fibre cables being laid also makes Africa a more viable target.[72]

Tunisia, Kenya, Mauritius, the Ivory Coast, Sudan and Egypt have operational computer security incident response teams (CSIRTs), with South Africa and Ghana in the process of developing national CSIRTs. First National Bank in South Africa also has a CSIRT.[73] Such facilities provide much-needed support in recovering from security incidents, and distributing research and warnings of possible incidents, and can provide community awareness training. As so few African nations have CSIRTs there is a vulnerability across the continent in that major cyber-security incidents may go undetected. In addition to CSIRTs, national cyber-security policies and legislation aid in reducing incidents by forcing organisations into compliance with information security regulations. In Africa, these policies and legislations are also lacking, again resulting in a vulnerability whereby organisations can use Africa as a data repository to escape stricter regulations in other parts of the world.[74] For example, Europe largely has compatible legislation, whereas the varying nature of the cyber legislation in Africa provides legal gaps for cyber-attackers to launch attacks using hosts in Africa. A number of African countries, including South Africa, have consistently appeared among the top ten of the Internet Crimes Complaint Centre.[75] This indicates that there is existing vulnerability to cyber-based attacks. As Africa becomes further connected to the global networks, the increase in opportunity for cyber-attackers will not only make Africa a prime target, but also a tool by using compromised systems in Africa as a platform to launch attacks against other targets globally.

The capability of cyber-warfare in Africa can be seen to be increasing as more nations continue to introduce more sophisticated technology. However, the general lack of CSIRTs and cyber-security policies, combined with other factors such as software piracy and lack of awareness, leaves Africa vulnerable. This vulnerability may result in the infected computers in Africa being used in large-scale cyber-attacks from outside of the continent. The increasing availability of communication technologies in Africa is likely to increase the occurrences of information conflict across the continent. In December 2012, a number of South African government websites were attacked and replaced with a message. This was apparently perpetrated by a foreigner protesting the South African government's stance on political issues in Morocco.[76] In June 2013 a group calling itself Anonymous Africa attacked various websites in South Africa and Zimbabwe it protest against claimed abuses of human rights in Zimbabwe.[77] These incidents provide early indicators that a cyber-based conflict between African nations or by an African non-state entity on an African nation is possible.

Conclusion

Africa has a long history of information-based conflict, largely based on ideological or political differences. This often results in misinformation, censorship and mass monitoring of political opponents and national populations. Information technologies are further enabling this conflict. Dissatisfied populations began online dissent, sparking mass protest in some instances, and African governments have increased their capabilities to monitor and control access to communications platforms. The increasing capability is not uniform across Africa, and there are still gaps in African cyber-security, which could result in systems in Africa unwittingly being used in an international cyber-conflict. The increasing prevalence of information and communications technologies will exacerbate information conflict in Africa and expose populations to global political and social ideologies. Whilst the population will also be exposed to mediation and conflict resolution strategies, some entities may choose to employ cyber-protest and cyber-attacks in Africa.

Endnotes

[1] Westwood, C. "The future is not what it used to be: Conflict in the Information Age". Air Power Studies Centre. 1997. <http://airpower.airforce.gov.au/Publications/Details/174/The-Future-is-Not-What-It-Used-To-Be-Conflict-in-the-Information-Age.aspx?p=print> Accessed on 21 May 2012.

[2] Monash University. "Advanced topic module 468 – Information Conflict, 2005". <http://www.csse.monash.edu.au/courseware/cse468/2006/subject-info.html> Accessed on 21 May 2012.

[3] Brazzoli, MS. "Future prospects of information warfare and particularly psychological operations." In Le Roux, L (ed.), *South African Army vision 2020*, Pretoria: Institute for Security Studies, 2007, 217–232, 219.

[4] Ragan, S. "DDoS: Myanmar attacks larger than those against Estonia and Georgia". *The Tech Herald*. 4 November 2010. <http://www.thetechherald.com/article.php/201044/6381/DDoS-Myanmar-attacks-larger-than-those-against-Estonia-and-Georgia> Accessed on 11 November 2010.

[5] Sudworth, J. "New 'cyber attacks' hit S Korea". *BBC News*. 9 July 2009. <http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm> Accessed on 1 September 2009.

[6] Miquel, RS. "Russian hackers besiege social sites to silence pro-Georgian blogger". *E-Commerce Times*. 7 August 2009. <http://www.ecommercetimes.com/story/67809.html> Accessed on 13 August 2009.

[7] Merrit, C. "A tale of two paradoxes: Media censorship in South Africa, pre-liberation and post-apartheid". *Critical Arts* 15/1. 2001. 50–68.

[8] Saleh, I. "The impact of ICT on peace, security & governance in Africa". United Nations Alliance of Civilizations Media Literacy Education. <http://uct.academia.edu/DrIbrahimSaleh/Papers/367192/The_impact_of_ICT_on_Peace_Security_and_Governance_in_Africa> Accessed on 22 May 2012.

[9] Sabastenaski, A (ed). *Patterns of global terrorism 1985–2005: US Department of State Reports with supplementary documents and statistics.* Great Barrington: Berkshire Publishing, 2005.

[10] Global Terrorism Database. "START". 2009. <http://www.start.umd.edu/gtd/> Accessed on 9 July 2009.

[11] Ramluckan, T & Van Niekerk, B. "Terrorism/mass media symbiosis". *Journal of Information Warfare* 8/2. 2009. 1–12.

[12] Stannard, C. *Beyond the edge of the sky.* Valhalla: Crowbar Enterprises, 2008.

[13] *Ibid*.

[14] Saleh *op. cit.*

[15] Reid-Daly, R & Stiff, P. *Selous Scouts: A top secret war.* Johannesburg: Galago, 1982.

[16] McNulty, M. “French arms, war, and genocide in Rwanda”. *Crime, Law, and Social Change* 33. 2000. 105–129.

[17] Hutchinson, W, Huhtinen, A & Rantapelkonen, J. “The impact of perspective on the effects and outcomes of conflict”. *Journal of Information Warfare* 6/1. 2007. 1–6.

[18] Adams, J. *The next world war.* London: Arrow Books, 1998.

[19] *Ibid*.

[20] Chau, DC. “Assistance of a different kind: Chinese political warfare in Ghana, 1958–1966”. *Comparative Strategy* 26/2. 2007. 141–161.

[21] *Ibid*.

[22] Museveni, YK. “The strategy of Protracted People’s War: Uganda”. *Military Review.* November–December 2008. 4–13.

[23] *Ibid*.

[24] Wardini, A. “Information operations in Senegal”. *IOSphere.* Special Edition 2008. 53–56. <http://www.au.af.mil/info-ops/iosphere/08special/iosphere_special08_wardini.pdf> Accessed on 29 May 2012.

[25] Brazzoli *op. cit.*

[26] Du Toit, B. “The African battlespace: Challenges for air defence”. Paper delivered at the 4th South African Joint Air Defence Symposium, Pretoria, October 2003.

[27] Okeowo, A. “SMSs ‘tool of hate in Kenya’”. *Mail and Guardian Online.* 19 February 2008. <http://www.mg.co.za/article/2008-02-19-smss-used-as-a-tool-of-hate-in-kenya> Accessed on 4 March 2009.

[28] Citizenship Rights in Africa Initiative. “Tolerating intolerance: Xenophobic violence in South Africa”. July 2009. <http://www.citizenshiprightsinafrica.org/Publications/2009/CRAISAReport.July2009.pdf> Accessed on 30 May 2012.

[29] Karrim, Q. “Local leaders ‘behind xenophobic attacks’”. *Mail and Guardian Online.* 11 March 2009. <http://mg.co.za/article/2009-03-11-local-leaders-behind-xenophobic-attacks> Accessed on 18 September 2011.

[30] Jacobs S & Duarte, D. “Protest in Mozambique: The power of SMS”. *Afronline.* 16 September 2010. <http://www.afronline.org/?p=8680> Accessed on 5 November 2010.

[31] Bay, A. “Tunisia's remarkable revolt”. *StrategyPage.com On Point Blog.* 18 January 2011. <http://www.strategypage.com/on_point/20110118224752.aspx> Accessed on 19 January 2011.

[32] Kravets, D. "Internet down in Egypt, tens of thousands protest in 'Friday of wrath'". *Wired.com ThreatLevel Blog.* 27 January 2011. <http://www.wired.com/threatlevel/2011/01/egypt-internet-down/#z> Accessed on 1 February 2011.

[33] Brooks, C. "SA hit by service delivery-protests". *Mail and Guardian Online.* 22 July 2009. <http://mg.co.za/article/2009-07-22-sa-hit-servicedelivery-protests> Accessed on 18 September 2011.

[34] Amadhila, N. "Western Cape's De Doorn farmers continue to protest low wages". *Political Analysis South Africa*. 9 November 2012. <http://www.politicalanalysis.co.za/2012/11/09/western-capes-de-doorns-farm-workers-continue-to-protest-low-wages/> Accessed on 27 November 2012.

[35] Perry, A. "Africa Rising". *Time.* 3 December 2012. 30–37.

[36] The terms 'hacktivist' and 'hacktivism' are a combination of the terms 'hack' and 'activist/activism'. This terminology arose to describe online activism, particularly where webpages or networks have been hacked to make a point. The most common form is the defacement of webpages; however, sometimes sensitive details are stolen and leaked to embarrass the targeted organisation.

[37] Windsofchangersa. "Message from anonymous: To the South African people". *YouTube*. 25 August 2011. <http://www.youtube.com/watch?v=53tCd4jusxo> Accessed on 2 March 2012.

[38] AnonymousZa65. "Anonymous message to fight the ANCYL". *YouTube*. 25 August 2011. <http://www.youtube.com/watch?v=1O4EJQaaPiw> Accessed on 2 March 2012.

[39] Brazzoli *op. cit.*, p. 223.

[40] Wardini *op. cit.*, p. 54.

[41] Committee to Protect Journalists. "10 most censored countries". 2 May 2012. <http://www.cpj.org/reports/CPJ.Ten.Most.Censored.5.2.12.pdf> Accessed on 11 June 2012.

[42] Kouyate, H. "Renegade Mali soldiers claim control of palace". *The Citizen.* 22 March 2012. <http://www.citizen.co.za/citizen/content/en/citizen/world-news?oid=266760&sn=Detail&pid=40&Renegade-Mali-soldiers-claim-control-of-palace> Accessed on 25 March 2012.

[43] Mavhunga, C. "The glass fortress: Zimbabwe's cyber-guerrilla warfare". *Concerned African Scholars* 80. 2008. 21–27.

<http://concernedafricascholars.org/docs/acasbulletin80.pdf> Accessed on 26 November 2010.

[44] Republic of South Africa. *Regulation of the Interception of Communications Act (Act 70 of 2002)*. Pretoria: Government of South Africa.

[45] South African Press Association. "Info bill unconstitutional – George Bizos". *News24.com*. 12 March 2012. <http://www.news24.com/SouthAfrica/Politics/Info-bill-unconstitutional-George-Bizos-20120312> Accessed on 11 June 2012.

[46] Kenny, P. "SA earns praise and criticism from its UN peers". *The Daily News*. 1 June 2012. 4.

[47] Forrest, D & Brummer, S. "Spooks bid for new powers". *Mail and Guardian Online*. 3 February 2012. < http://mg.co.za/article/2012-02-03-spies-bid-for-new-powers/ > Accessed on 16 February 2012.

[48] *Ibid.*

[49] Republic of South Africa. *Intelligence General Laws Amendment Act (Act 11 of 2013)*. Pretoria: Government of South Africa.

[50] Madrigal, A. "The inside story of how Facebook responded to Tunisian hacks". *The Atlantic*. 24 January 2011. <http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/#> Accessed on 25 January 2011.

[51] Kravets *op. cit.*

[52] Aikins, M. "Jamming Tripoli: Inside Moammar Gadhafi's secret surveillance network". *Wired.com*. 18 May 2012. <http://www.wired.com/threatlevel/2012/05/ff_libya/all/1> Accessed on 24 May 2012.

[53] Malakata, M. "Uganda moves to block social networks". *ComputerWorld Kenya*. 28 April 2011. <http://www.computerworld.co.ke/articles/2011/04/28/uganda-moves-block-social-networks> Accessed on 7 May 2011.

[54] Bosch, M. "Zambians watch the Internet, social media for vote fraud". *Reuters.com*. 20 September 2011. <http://www.reuters.com/article/2011/09/20/us-zambia-election-internet-idUSTRE78J3TW20110920> Accessed on 11 June 2012.

[55] Jacobs & Duarte *op. cit.*

[56] British Broadcasting Corporation. "Sudan to unleash cyber jihadists". 23 March 2011. <http://www.bbc.co.uk/news/technology-12829808> Accessed on 11 June 2012.

[57] Associated Press. “Somali pirates hone their tactics”. *MSNBC.com.* 25 May 2009. <http://www.msnbc.msn.com/id/30930771/page/2/> Accessed on 2 September 2009.

[58] Webb, J. “Somali pirates using London contacts – Spain radio”. *Reuters.com.* 11 May 2009. <http://www.reuters.com/article/2009/05/11/idUSLB570114> Accessed on 4 September 2009.

[59] StrategyPage.com. “Why pirates hate Mercury”. 23 September 2009. <http://www.strategypage.com/htmw/htterr/articles/20090923.aspx> Accessed on 23 September 2009.

[60] Laje, D. “#Pirate? Tracking modern buccaneers through Twitter”. *CNN.* 15 March 2012. <http://edition.cnn.com/2012/03/15/business/somalia-piracy-twitter/index.html> Accessed on 26 March 2012.

[61] Torchia, C. “Pirate attacks go unreported”. *News24.com.* 8 July 2009. <http://www.news24.com/Content/World/News/1073/a770b67c2166425f8e2945057160e3ff/08-07-2009-11-51/Pirate_attacks_go_unreported> Accessed on 13 June 2012.

[62] Whitlock, C. “US expands secret intelligence operations in Africa”. *The Washington Post.* 14 June 2012. <http://www.washingtonpost.com/world/national-security/us-expands-secret-intelligence-operations-in-africa/2012/06/13/gJQAHyvAbV_story.html> Accessed on 15 June 2012.

[63] Alex Perry *op. cit.*

[64] Giacomello, G. “Measuring ‘digital wars’: Learning from the experience of peace research and arms control”. *The Information Warfare Site Infocon Magazine* 1. October 2003. <http://www.iwar.co.uk/infocon/measuring-io.pdf> Accessed on 26 September 2011.

[65] Coleman, K. *Cyber commander’s handbook.* McMurray, PA: Technolytics Institute, c2009.

[66] Coleman *op. cit.*

[67] Giacomello *op. cit.*

[68] Carr, J. *Inside Cyber Warfare.* Sebastopol, CA: O'Reilly, 2012.

[69] Microsoft Corporation. *Microsoft Security Intelligence Report* 9. 2010. <http://www.microsoft.com/security/sir/archive/default.aspx> Accessed on 26 November 2010.

[70] Van Niekerk, B. “Vulnerability of modern ICT infrastructures from an information warfare perspective”. PhD thesis, University of KwaZulu-Natal, 2012.

[71] *Ibid.*

[72] *Ibid*.

[73] AfricaCERT. “Countries”. 2011. <http://www.africacert.org/home/countries.html> Accessed on 14 June 2012.

[74] Van Niekerk *op. cit.*

[75] Internet Crime Complaint Centre. “Annual reports”. 2007–2011. <http://www.ic3.gov/media/annualreports.aspx> Accessed on 5 December 2012.

[76] South African Press Association. “Hack attack on state website”. *Daily News.* 10 December 2012. 5.

[77] Alfreds, D. "ANC Hacker Explains Actions". News24.com. 14 June 2013. <http://www.news24.com/Technology/News/ANC-hacker-explains-actions-20130614> Accessed 17 June 2013.