THE USE OF COMPUTER WARFARE BY INSURGENT GROUPS: LEARNING LAG OR CONTEXT-BOUND THREAT?

Heinrich Matthee[*]

INTRODUCTION

Since the late 20th century conflicts involving insurgents have proliferated. Extremely destructive and disruptive computer programs are widely available to insurgent groups in most parts of the world. These programs can be used with great effect to attack vulnerable computerised information infrastructures. The article discusses the relevance of such computer warfare in South Africa and the current state response in South Africa to potential computer warfare by insurgents.

In spite of the usefulness and availability of weapons of computer warfare, the perceived threat of computer warfare by insurgent groups has not materialised significantly in South Africa or elsewhere. The article therefore analyses the current uses of computerised information technologies and physical violence by insurgents to explore why computer warfare has not been used to a significant extent. The spectrum of probable use of computerised information technologies by insurgents in the short and medium term is outlined. The influence of the context and dynamics of a particular insurgent group on its use of computer warfare is then explored.

COMPUTER WARFARE AND THE BROADER BATTLESPACE

Insurgency is defined here as protracted low-intensity violence by groups to change patterns of power (Schmid 1983:111; Rabert 1991:11-6). Computerised information technologies and systems can broadly serve three roles during insurgencies. Such systems can be targets, against which bombing and arson are used, or can form the means of support of traditional insurgency activities. Computer programs can also be used as weapons of computer warfare against information infrastructures.

[*] Centre for Military Studies, University of Stellenbosch.

One effect of the new computerised communication and information systems has been to broaden the battlespace for security actors, including insurgents. The computerised systems imply new means, new targets and new effects on the security of people and societies.

The presence of wide area networks means that the effect of attacks on information systems can spread quicker and further than ever before (Luiijf 1999: 141). As a result, access to important networks and information systems expertise can easily become a security actor, at least in a country like South Africa, where sectors of society are dependent on networks.

Interaction within wide area networks makes it difficult to identify an actor. Similarly, distinguishing between amateur hacking, system failures and accidents becomes difficult and arranging appropriate defence measures can therefore be a problem.

The ambiguities of the cyber sphere enable deception and image-manipulation. In addition, new means to attack computer targets are continuously developed. For example, the potential for so-called semantic attacks is researched at present. A system under semantic attack operates and will be perceived as operating correctly. However, such a system will generate false versions of reality, so that the targeted decision-maker makes decisions counter to his objective (Fulghum 1998:58).

Whether the objective of non-state actors is destruction or disruption, potential battlespaces are wherever networked systems allow access (Molander, Riddle & Wilson 1996:4). The broader battlespace currently often favours attackers rather than defenders.

THE CONCERN ABOUT COMPUTER WARFARE OUTSIDE AFRICA

The number, kind and potential of specific disruptive and destructive software programs are mounting since the first computer attacks were recorded in the late eighties in the USA and Germany. For example, in 1999 the Melissa virus allegedly caused $ 80 million in disruption and lost commerce as it made its way through the computers of 20 % of America's biggest businesses (**Saturday Argus** 11/12 December 1999:6).

The advantages of the broader battlefield and the destructive potential of computer warfare have increased concerns about the vulnerability of computerised information infrastructures. Many advanced societies increasingly depend on computerised information processes to control electric power, money flow, air traffic, fuel and health services. This dependence means that damage to information infrastructure can have a strategic impact on the course of a conflict.

As early as 1977, insurgency experts recognised the growing vulnerability of these structures to disruption (Wilkinson 1977:103). By 1988, insurgency experts still recognised the threat but concluded that disruptive insurgency was not appealing to insurgents because their hostility and need for publicity were not satisfied by such disruption (Jenkins 1988:258).

American conventional military dominance in the 1990s meant that few adversaries would confront the USA directly on the battlefield. A number of American security thinkers and bureaucrats began to consider the possibility that American adversaries would use asymmetrical approaches, including information infrastructure attacks, during conflicts (Toffler & Toffler 1994; Flynt 1999:4; Freeh 1999:3). As a result, in 1999 and 2000 president Bill Clinton allocated hundreds of millions of dollars to secure the US from an overwhelming digital surprise attack.

THE RELEVANCE OF COMPUTER WARFARE IN SOUTH AFRICA

By contrast, computer warfare is not much of a concern in most African countries. Over half of Africa's population is illiterate and there is an insufficient pool of experts able to organise information systems. According to some calculations, less than 2% of Africa's population has telephones, leave alone computers (**Africa Confidential** 10 October 1997:3-4). The basic infrastructure necessary for developing computerised telecommunications often is insufficient, with power outages, no or unreliable telephone circuits and few digital systems (De Roy 1997:889-91).

However, in South Africa the current situation is somewhat different. Parts of the country are dependent on computerised information infrastructures while others still lack basic infrastructure. On the whole, South Africa is the country in southern Africa that is most developed but also most dependent regarding information infrastructures. These circumstances have implications for personal, social and state security.

For example, the government intends to establish a countrywide computer network with electronic access points for all citizens. This network is intended as a one-stop shop for identity documents, pensions and fire-arms licences, as well as a means for tele-medicine, tele-education, tele-agriculture and electronic commerce

(Ministry for Posts, Telecommunications and Broadcasting 1998:1; Department of Communications 1999:1).

While attacks on information infrastructures may seem like a concern for industrialised countries with prominent infrastructures only, such attacks may become even more of a concern to developing countries like South Africa. The planned computer network will be established in spaces that often have limited health, education and information infrastructure. Insurgent damage to computerised information infrastructure will therefore tend to have a greater impact on people than in industrialised countries where other services could partly serve as substitutes. The loss of limited and scarce resources in this way will also have a relatively greater impact on development than in the industrialised countries.

In addition, South Africa has the strongest conventional military force in sonthern Africa. Any violent adversary in the region, including an insurgent group, is therefore likely to consider asymmetrical computer warfare too. Computer warfare may of course also be waged against non-state actors in South Africa. The recent attacks that crashed a student website with an anti-Mugabe game may be in this category (**Die Burger** 7 April 2000:9).

THE STATE RESPONSE TO POTENTIAL COMPUTER WARFARE

South Africa did not experience computer warfare during past South African insurgencies. The insurgency led by the African National Congress (ANC) against the white National Party government entered a period of peace talks in the period 1990-1994, before disruptive computer programs became more widely known. In spite of the availability of computer skills, there also is no recorded incidence of the use of disruptive computer programs during the government's campaign against the ANC and its partners in the period 1993-1994 (Kemp 1994:182).

SA legislation criminalises acts of terrorism or sabotage, but not acts of computer warfare. Section 37 of the South African Constitution, Act 108/1996, refers to a "general insurrection" as one ground for a state of emergency (Constitutional Assembly 1996:14). The "general insurrection" mentioned in the Constitution probably includes an insurgency.

The new Constitution, Act 108 of 1996, read together with the interim Constitution, Act 200 of 1993, retains the sections on terrorism and sabotage of the Internal Security Act, Act 74 of 1982. At present, new terrorism legislation is being prepared. However, there are no explicitly defined computer crimes in South African law. Even though the new Anti-terrorism Bill provides for specific types of terrorism, for example nuclear terrorism, it does not address computer warfare by terrorists (South African Law Commission 2000).

While legislation against computer crime was already mooted ten years ago, it is only now under formal discussion. The SA Law Commission has published a position paper on the issue in 1998 (South African Law Commission 1998), which proposes the creation of specific offences to criminalise unauthorised access to computers and unauthorised modification of computer data. Because of the possibility of transnational computer crime, the Law Commission has suggested extradition measures for transnational computer crimes.

Computer warfare by transnational terrorists may also be covered by such measures. From interviews conducted with an author of the position paper, it has emerged that, apart from the position paper, no further steps in the legislative process were taken in 1999 (Van der Merwe 1999; Van der Merwe 2000).

Because of no legislation regarding computer crime or acts of computer warfare, the effectiveness of law enforcement may suffer. The common law on malicious damage to property, as well as sections in the Internal Security Act on physical sabotage, have to be used in prosecutions of cases arising from computer warfare. The current extent of such prosecutions is difficult to ascertain. The statistics of the Crime Information Management Centre of the SAPS, as reflected in quarterly and annual reports, do not yet specifically indicate crimes where computers were involved as tools, objects or subjects.

Furthermore, in common law malicious damage has to do with tangible objects and computer data do not easily fit the definition of being tangible objects. Prosecutors may be hesitant to prosecute cases that do not stand a clear chance of success. According to Advocate John Welch, a deputy attorney general in Gauteng, prosecutions by local prosecutors in cases of computer misuse usually only ensue after consultation with the respective attorney generals (Welch 1999).

Previously, members of the Technical Support Unit assisted SAPS detectives who investigated crimes with a computer dimension. Since April 2000 a computer crime unit of 14 people would be based at the commercial branch at the SAPS headquarters in Pretoria (**Cape Times** 1 March 2000:11). The position of the new unit reflects the area of biggest concern at present, namely computer abuse by white-collar criminals.

During an insurgency, the Scorpions unit (Schönteich 1999:3-12), and the SA National Defence Force will bear most counter-insurgency responsibilities, either separately or in combination. While the state security forces have recently taken steps to prepare for potential computer warfare, there does not seem to be a sense of urgency about providing an appropriate legal framework to handle computer warfare by insurgent groups.

RETHINKING COMPUTER WARFARE AND INSURGENT GROUPS

Perhaps this state response is related to the fact that the use of computer warfare has been much more limited than possible or predicted. No incident of hacking, viruses and computer sabotage in SA since 1994 has been linked to violent politics and there are virtually no cases outside SA where insurgent groups have used computer warfare.

The Liberation Tigers of Tamil Elaam (LTTE), who also enjoy support among the hundreds of thousands of Tamil Indians living in SA, allegedly carried out the first recorded attack by swamping the e-mail systems of Sri Lankan embassies (Furnell&Warren 1998:31-2). However, the Tamil Tigers have used spectacular bombings, assassinations and suicide attacks far more commonly (Joshi 1996:19-42).

Since the means for computer warfare have been available for several years, without being used by much insurgent groups, some rethinking on insurgents and computer warfare may be necessary. Concerns about computer warfare by insurgents are usually based on the availability of offensive abilities, the advantages of the broader battlefield and the vulnerability of information systems. This approach lacks an appreciation of the influence of insurgent context and dynamics on the use of computer warfare.

To link computer warfare to the context and dynamics of insurgent groups, two avenues are explored. The current roles of computerised information systems, as support systems, as a means of psychological warfare and as targets of physical attacks, are analysed. In addition, reasons for using physical violence are discussed to determine whether physical violence may be preferable even if computer warfare could be used with success.

THE WAY IN WHICH COMPUTERISED INFORMATION SYSTEMS COULD BE USED

Support functions of the new information technologies

Insurgent groups can use computerised information technologies for various support functions. The Internet can be used for fundraising and those groups involved in lucrative illicit enterprises, like the Shining Path in Peru, may need money-laundering facilities too. Electronic cash and banking have created new opportunities for money-laundering and computers may become part of this support function (Molander, Mussington & Wilson 1998).

The South African ANC used computer systems for encoded communication and information during its insurgency campaign before 1994 (Kasrils 1993:301, 308, 332). Before 1994 the Internet was not widely accessible in SA, but today insurgent groups can use the Internet to communicate and coordinate operations by e-mail. Software programs like PGP are available for free on the Internet and can protect e-mail from surveillance by encoding or concealing text (Whine 1999: 231-2).

Sources on the Internet provide information on the construction of bombs too. For example, in court cases regarding bombings in the Western Cape, the state has alleged that an accused had downloaded instructions on bomb-making from the Internet (**Cape Times** 13 January 2000:1). This state of affairs does not mean that hidden knowledge is now available, but rather that the information can be obtained easier and cheaper than before. Manuals on assassination and bomb-making have been openly available since the 1970s from commercial publishers in the USA (Livingstone 1982:118-20).

Clandestine collection of information by computer may seem advantageous to insurgents because computers can store and copy information in a small space. In addition, the convergence of computers and telecommunications has enabled the monitoring of telephones and satellites by computer. Nevertheless, human means still seem to dominate espionage activities recorded by the intelligence agencies of computerised societies like Switzerland and Germany (Bundespolizei 17 May 1999; Bundesverfassungsschutz 1997).

Computers can support many tasks of the insurgent organisation but they may also provide a trail of information and evidence for authorities that uncover them. A state operation in Italy in 1996, for example, uncovered several bases of an Algerian insurgent group, containing computers and disks with instructions for the construction of bombs (Arquilla, Ronfeldt & Zanini 1999:99). In December 1999, the SA state security forces considered it necessary to confiscate the computer equipment of Muslim activists allegedly involved in political violence.

Psychological warfare

The Internet, a worldwide network of computer networks, only became prominent in the 1990s. While a state can prohibit the dissemination of certain religious or political messages, the Internet is not at present completely regulated with a system of sanctions. Servers in different countries can be used to relay information. The Internet therefore provides a means for insurgent groups to escape banning, censorship or distortion by hostile media groups and governments.

Insurgent groups can use the Internet to put across their message to a broad audience, appearing larger than they may be (Dartnell 1999:130; Bundesverfassungsschutz 1998). Apparently insurgent groups have not yet made an effort to obtain and use the hacking tools and virus software programs available on the Internet. The use of information systems by insurgent groups to support activities and to conduct psychological warfare seems likely to be the dimensions that will become more important.

Computer systems as insurgent targets

Since the late 1960s insurgents have conducted numerous bombing and arson attacks on computer systems in South America, Europe, the USA and South Africa (Cornwall 1987:182). Most attacks occurred in Europe and the USA and took place in the 1970s and 1980s.

Insurgent groups have already targeted computers and infrastructure because they were used by adversary security agencies or linked to disapproved causes. However, physical means like arson or bombs were used. During the NATO campaign in Serbia in 1999 even the sophisticated armed forces of NATO mostly used bombings rather than computer warfare to attack Serbian computerised information infrastructures (Tilford 1999: 24). Attacks against computerised information infrastructures may become an important part of insurgent activities too, but at this stage such attacks will mostly be by physical means.

CYBERREBELS AND INSURGENCY

In time, new social opposition groups mobilising around different loyalties and cyberspace issues may grow more prominent in connected societies. Old and new social opposition groups and individual discontents in some societies may use hacking and disruptive software programs as a means of rebellion (Arquilla, Ronfeldt & Zanini 1999:83).

Instead of insurgents, new groups of amateur hackers have come to the fore as users of disruptive and destructive computer programs. For example, in 1994 and in May 1999 hacker groups brought down the computer systems of prominent media groups and the American FBI to protest against plans for Internet regulation or investigations against hackers (Hoo, Goodman & Greenberg 1997:143; **Mercury News** 1 June 1999).

The first case of unauthorised hacking that came to the attention of the South African Department of Justice occurred in 1993, but was not related to insurgency. Since 1994 several non-political incidences of hacking have affected Telkom, the Pretoria municipality and multinational companies. In one of the few cases of politically-motivated hacking, protesters against planned anti-gun legislation in SA posted their messages on the SAPS website in 1999 (Welch 1999).

Amateur hacking and insurgency may share certain related incentives and characteristics, like the emotion of empowerment, an element of fantasy, peer recognition, exploration and risk-taking (Bell 1994; Bell 1998). However, the virtual world of hacking does not resemble the experiences of insurgency.

Depending on the context of an insurgency, the attractions of membership in an insurgent group may be exceeded by misery, betrayal, failure, anxiety, psychological fallout from shedding blood, social loneliness and authoritarian insurgent discipline (Bell 1998; Crenshaw 1985). Insurgency puts different and vastly heavier demands on people than hacking does. As a result, hackers may not necessarily be drawn or remain drawn to insurgency.

Nevertheless, amateur hackers may be of importance to security agencies in another sense. Widespread activities by amateur hackers may overload security agencies that operate under budgetary and personnel constraints. Hacking also indicates the presence of skills and system vulnerabilities that may eventually become of use to non-state security actors.

VIOLENCE PREFERRED TO COMPUTER WARFARE

Insurgent strategies and patterns of power

The role of insurgent strategies, personal motives, organisational dynamics and business interests in insurgent violence may partly explain the current non-use of computer warfare by the overwhelming majority of insurgent groups. The successful Tamil Tiger group, who uses the Internet for support functions and psychological warfare and have access to the means of computer warfare, may be instructive in this regard.

Insurgent groups tend to regard existing political arrangements as too oppressive or insufficient to achieve their objectives, and then turn to insurgent methods. For example, the Tamil Tiger leader, Velupillai Pirabhakaran, has referred to the Sri Lankan democracy as being a political tyranny of the Sinhalese group over his Tamil group. The Sinhalese group forms 76% of the population in Sri Lanka and the Tamil group 12% (**The Week** 23 March 1986).

Insurgent strategies are normally linked to the environment and historical context of the insurgent group. The insurgency in Sri Lanka is a battle for the hearts and minds of the Tamil group. Tamil Tiger violence has provoked Sinhalese-controlled state repression, which has reinforced Tamil identity constructs and alienated many Tamils from the government. The communal killings and the military offensives by the Sinhalese-controlled Sri Lankan military since 1997 have given the Tamil Tigers opportunities to show Tamils in Sri Lanka that the Sinhalese government cannot or will not protect them, while the Tamil Tigers pursue Tamil interests.

Spectacular bomb blasts and attempted and successful assassinations of Indian and Sri Lankan prime ministers have occurred as part of the Tamil Tiger strategy. In this context, even though the means and opportunity to conduct computer warfare have been present, the Tamil Tigers have considered the images of bleeding bodies and destroyed buildings as more effective means to achieve their aims (Byman 1998:155; Wardlaw 1982:182).

Violence and personal status

Violent strategies by weak insurgents may mean that their strong adversaries take them seriously for the first time. Violence may also be chosen as part of a strategy of group empowerment. In Sri Lanka, the Tamil Tigers have killed Tamil parliamentarians and social leaders viewed as too close to the Sinhalese government. As a result, pro-secessionist Tamils have attained a prominent leadership position among the Tamils.

In addition, violence may be chosen as a means of personal empowerment and status-seeking. Participation in violence may be experienced as a psychologically exhilarating or a liberating event for those who feel abused or repressed by their adversaries (Morris 1994:195-219; Bell 1998:102). Status-seeking in some social contexts and the desire to appear as soldiers, which is widespread in virtually all the "secret armies" of insurgency, may influence a preference for violence rather than computer warfare (Peters 1994:16-26; Finch 1997:31-41).

Violence and organisational dynamics

Organisational dynamics and interaction with the environment and adversaries influence insurgent strategies and approaches to violence. An insurgent group may start operating with a clear strategy of selective violence, but violence may escalate or become more indiscriminate during the course of interaction with adversaries (Rabert 1991:23-4; Sederberg 1994:261). In addition, competition for authority and publicity between two related insurgent groups or between different factions in a group may motivate violence. For example, the Tamil Tigers have killed leaders in other pro-secessionist movements to ensure its dominance on the extra-parliamentary scene (Joshi 1996:21, 24).

The distribution of beliefs, also regarding violence, among members of an insurgent group is likely to be uneven. However, dissent is dangerous to clandestine insurgent groups. Violence may be employed to ensure discipline and to increase the costs of leaving the organisation for perpetrators (Bell 1998:50-1). New organisational forms like decentralised networks are prominent among current insurgent groups, but the interaction between organisational dynamics and violence has remained.

Violence and money

A whole spectrum of relationships between insurgent and crime groups is possible. Protection of illicit businesses or acquired businesses in conflict-ridden areas, control of trade in different commodities and gaining access to land may also become an important part of insurgent activity, as it has in the case of the Tamil Tigers (Byman 1998:157; Silke 1998:339, 342).

In areas with weak governance, crime groups may become part of local politics and regional insurgencies, as they have in Colombia, Russia or the Congo (Shelley 1995:463-89; Turner 1998:221-3; Sederberg 1994:273). Violence may in such cases serve important functions that computer warfare cannot sufficiently fulfil.

CONCLUSION

Many insurgent groups have access to skills and resources to condnct computer warfare with destructive effectiveness. The dependence of many societies on computerised information infrastructures has created vulnerabilities and therefore there is concern among policymakers in developed countries about computer warfare by insurgent groups.

South Africa is a developing country with some connected spheres and some underdeveloped parts, but computer warfare nevertheless is of concern in SA too. The effect of computer warfare on planned infrastructure and social development may be even larger than in the developed countries. SA's relative strength in the region also means that prospective enemies may consider computer warfare to attack structural vulnerabilities with more success.

The SA state's response to potential computer warfare has been uneven. State security forces have lately taken new measures to prepare themselves for computer warfare, but the lack of a clear legal framework for law enforcement agencies will hamper the prosecution of insurgents acting locally.

However, the approach that focuses on the general potential of computer warfare by insurgent groups seems overrated at present. For the last six years or more, insurgent groups have been able to inflict huge disruption and destruction by computer warfare on vulnerable infrastructure, but they have not used the advantages of a broader battlefield. A new approach to insurgent groups and computer warfare that places more emphasis on the context and dynamics of specific insurgent gronps may be necessary.

Insurgent groups currently use new information technologies to support group activities and will probably continue to do so. In many cases the Internet will become increasingly important for information, communication and coordination. Clandestine collection of information by computer may be fruitful but does not seem very widespread at this stage. If insurgents need funds or cooperate with organised crime, computer crime and electronic money-laundering may become part of their activities in some societies too.

Computerised systems may become far more important as a means for insurgent mobilisation and psychological warfare than a means of computer warfare. Insurgent groups beyond 2000 will have an interest in attacking some computerised information systems but maintaining others like the Internet and World Wide Web.

Otherwise non-violent social opposition movements may under certain circumstances start to consider the use of computer warfare against specific targets. Such movements may remain separate from an insurgency. They may also be part of insurgent groups or the forefield of insurgency.

The patterns of power in societies and the effectiveness of violence to promote insurgent aims may influence insurgent groups to use violence. Violence can demonstrate the inability of a government to protect people with more psychological effect than computer warfare. The images of bleeding bodies and destroyed buildings after insurgent violence may be deemed more effective in weakening the opponent's will.

Violent means and computer warfare may achieve equal physical disruption and destruction. However, violent means may have a greater psychological impact than computer warfare. In cases where computer warfare may be more effective in causing physical disruption, insurgent groups may still prefer violent methods because of he search for status or the dynamics of illicit business or the underground organisation.

The non-use of available means of computer warfare may be due to the current predominance of insurgent leaders and insurgent fighters who do not understand computer warfare. Nevertheless, even if the learning lag is closed, as in the case of the Tamil Tigers, physical violence will remain useful to fulfil the spectrum of needs in most insurgent groups.

To determine the potential for computer warfare among insurgent groups, it is insufficient to merely extrapolate from the availability and advantages of the means of computer warfare. A contextualised case-by-case study will be more fruitful to determine the threat, if any, of computer warfare. If insurgent groups use computer warfare at all, such methods will for the time being mostly form a subordinate part of violent campaigns. For the next five years or so most insurgencies, also in South Africa, will therefore remain the domain of the bullet and the bomb.

REFERENCES

Abarder G 2000. Court bomb: 'Third force trying to frame Pagad'. **Cape Times**, 13 January 2000: 1.

Africa Confidential, 10 October 1997: 3-4.

Arquilla J, Ronfeldt D and Zanini M 1999. Networks, netwar, and information-age terrorism. In: Khalilzad Z and White J. **The changing role of information in warfare**. Santa Monica: RAND.

Bell J 1998. **The dynamics of the armed struggle**. London: Frank Cass.

Bundesamt für Verfassungsschutz 1998. **Extremistische Bestrebungen im Internet**. <http://www.verfassungsschutz.de>

Bundespolizei 1999. Pressemitteilung 17 May 1999. http://www.bupo.admin.ch

Business Software Alliance 1999. **Internet software piracy**. <http://www.nopiracy.com>

Byman D 1998. The logic of ethnic terrorism. **Studies in conflict and terrorism** 21(2) April-June:149-70.

Coetzee H 2000. Kuberkapers wis studentetuiste uit. **Die Burger**, 7 April 2000: 9.

RSA1997. **The Constitution of the Republic of South Africa**, Act 108 of 1996. Wynberg: State Printers.

Cornwall H 1987. **Datatheft: Computer theft, industrial espionage and information crime**. London: Heinemann.

Dartnell M 1999. **Insurgency online: Elements for a theory of anti-government internet communications. Small wars and insurgencies** 10(3) Winter 1999: 116-35.

Department of Communications 1999. **Electronic commerce policy process**. http://www.doc.gov.za

De Roy O 1997. The African challenge: internet, networking and connectivity activities in a developing environment. **Third World Quarterly** 18(5): 883-98.

Electronic Privacy Information Center s.a. **Critical infrastructure protection and the endangerment of civil liberties.** http://www.epic.org

Flynt B 1999. Threat convergence. **Military Review** 79(5) September-October 1999: 2-7.

Freeh L 1999. Responding to terrorism. **FBI Law Enforcement Bulletin** March 1999: 2-3.

Fulghum D 1998. Computer warfare offense takes wing. **Aviation Week & Space Technology** 19 January 1998: 56-8.

Furnell S and Warren M 1998. Computer hacking and cyber terrorism: The real threats in the new millennium? **Computers and Security** 18(1): 28-34.

Gilford G 2000. Cybercops on the job. **Cape Times** 1 March 2000: 11.

Jenkins B 1988. Future trends in international terrorism. In: Slater R and Stohl M (eds). **Current perspectives on international terrorism.** London: Macmillan.

Joshi M 1996. On the razor's edge: The Liberation Tigers of Tamil Eelam. **Studies in Conflict and Terrorism** 19(1) January-March 1996: 19-42.

Kasrils R 1993. **"Armed and dangerous": My undercover struggle against apartheid.** London: Heinemann.

Kemp A 1994. **Dritter Burenkrieg: Der Kampf der südafrikanischen AWB und ihres Führers.** Coburg: Nation Europa-Verlag.

Kovavich G 1999. I-way robbery: Crime on the internet. **Computers and security** 18(3): 211-20.

Libicki M 1997. **Defending cyberspace and other metaphors.** http://www.ndu.edu/ndu/inss/actpubs/dcom/dcomch00.html

Livingstone N 1982. **The war against terrorism.** Lexington: Lexington Books.

Luiijf E 1999. Information assurance, a long way to go. In: Bosch J and Mollema A. **Information operations**. Breda: Tilburg University Press.

Ministry for Posts, Telecommunications and Broadcasting 1998. **South Africa's national information and communication superhighway**. <http://www.doc.gov.za>

Molander R, Mussington D and Wilson P 1998. **Cyberpayments and money laundering**. Santa Monica: RAND.

Molander R, Riddle A and Wilson P 1996. **Strategic information warfare: A new face of war**. Santa Monica: RAND.

Morris D 1994. **The naked ape trilogy**. London: Jonathan Cape.

Rabert B 1991. **Terrorismus in Deutschland: Zum Faschistenvorwurf der deutschen Linksterrorismus**. Bonn: Bernard/Graefe Verlag.

Saturday Argus 5/6 December 1999:18.

Saturday Argus 11/12 December 1999: 6.

Schmalleger F 1996. **Criminology today**. Englewood Cliffs.

Schmid A 1983. **Political insurgency: A research guide to concepts, theories, data bases and literature**. Leiden: Centre for the Study of Social Conflict.

Schönteich M 1999. How organised is the state's response to organised crime. **African Security Review** 8(2) 1999: 3-12.

Sederberg P 1994. **Fires within: Political violence and revolutionary change**. New York: Harper Collins.

Shelley L 1995. Transnational organized crime: An imminent threat to the nation-state? **Journal of International Affairs** 48(2) Winter 1995: 463-89.

Soo Hoo K, Goodman S and Greenberg L 1997. Information technology and the terrorist threat . **Survival** 39(3) Autumn 1997: 135-55.

South African Law Commission 1998. **Computer related crime.** Issue Paper 14. Pretoria: State Printer.

South African Law Commision 2000. **Anti-terrorism bill.** Discussion Paper 92. Pretoria: State Printer.

The Week 23 March 1986. <http://eelam.com>

Tilford E 1999. Operation allied force and the role of air power. **Parameters** 29(4) Winter 1999-2000: 24-38.

Toffler A and Toffler H 1994. **War and anti-war: Survival at the dawn of the 21st century.** London: Little, Brown and Co.

Turner J 1998. **Continent ablaze: The insurgency wars in Africa 1960 to the present.** Johannesburg:Jonathan Ball.

Wardlaw G 1982. **Political terrorism: Theory, tactics and counter-measures.** Cambridge: Cambridge University Press.

Van der Merwe D 1999. **Interview** 25 January 1999.

Van der Merwe D 2000. **Telephone interview** 5 January 2000.

Welch J 1999. **Telephone interview** 15 June 1999.