Anti-Colonial Hacking: The Case Study of An Autonomous Encrypted Communication Network Developed During the Struggle Against Apartheid in South Africa[1]

Introduction

It is September 1989. Janet Love, an MK commander infiltrated in South Africa is sitting anonymously in an office in Johannesburg holding a tape recorder next to a land-line phone. Earlier in the morning, she had typed a message from a laptop computer. The laptop and the encrypted disk had been infiltrated a few months before by Antoinette an anti-apartheid Dutch flight attendant. After typing her message she enciphered it and then pass it out through the computer's serial port to an acoustic coupler modem. This way she converted the digital data to sound and the audio stream was captured on a small cassette tape recorder. She dialed freedom fighter and hacker Tim Jenkin in London who had in his apartment a special answering machine attached to his phone to receive messages from South Africa. Working on his computer Jenkin would receive the message by playing the received audio message back through a similar acoustic modem attached to its computer, to convert it back to digital. The digital data would be deciphered using a matching key disk which would make the plaintext appear on Jenkin's computer screen. The message read: "All is fine. Safe houses have been established securely. I have recruited one new trusted person to work under my command. She will be working out of Durban. I might need more money to be equipement. Can you send?" While reading the message Jenkin assessed that it needed to be passed on to Lusaka, Zambia and be seen by the senior leadership of the African National Congress (ANC). At the Lusaka receiving end, Lucia a Dutch anti-apartheid activist, received Jenkin's enciphered messages, decipher it and printed it out. A courier picked up and brought it to the senior ANC members.

This case study shed light on one of the most exciting, but untold story of anti-colonial hacking. It is the story of anti-apartheid activists including freedom fighter and hacker Tim Jenkin, who in exiled in London in the 1980s, crafted an autonomous encrypted communication network that would end up being part of Operation Vula. The network enabled operatives infiltrated on the ground in South Africa to report back and communicate secretly to and with the African National Congress (ANC) leadership in exile in Zambia. This communication network was born at a time when the personal computer was just emerging, when cryptography was still classified by many countries as a weapon, and when countries such as the United States were boycotting South Africa's sell of computers, among other goods, as they

[1]

were deemed to support apartheid by providing automation capabilities [2] (NARMIC/American Friends Service Committee 1982; Edwards & Hecht 2010).

Operation Vula was launched in the 1980s (Henderson 1997) after decades of struggle that failed to de-structure and ultimately dismantle the oppressive white supremacist regime in place since 1948. Operation Vula aimed to put an end to the apartheid regime by bringing covertly in South Africa ANC senior leadership to foster a people's war[3]. Operation Vula, a short for Vulindlela, meaning Open the Road or the Path in Zulu (Henderson 1997), was envisaged at a time when liberation from apartheid seemed beyond reach. The many setbacks the ANC and the Umkhonto weSizwe (MK), the ANC independent military wing, had faced seemed to render the fall of apartheid less and less of a reality. ANC and MK operatives were being killed, arrested, tortured and/or forced into exile.

As the ANC Technical Committee's[4] experimentation with automating encryption seemed promising in supporting the ANC cause, it was deemed worthy to be tried and integrated in Operation Vula. The autonomous encrypted communication network, which evolved in refinement over time had to use heterogeneous forms of technologies and communication devices to adjust to the reality on the ground at a time where the internet as we know it today did not yet exist.

In this article, I will first focus on the South African background to contextualise the reasons why an encrypted communication network was set up. The long history of the ANC in setting up different forms of technological and communication systems to share and distribute information in addition to communicate strategic information across borders is important to understand on a communication and technological continuum. The ANC had used radio broadcasts, newspapers, leaflet-bombs, among others, as a way to inform, trigger activism and keep hope with South Africans who were experiencing oppression on a day to day basis. Moreover, the high level of infiltration within the movement and the burdensome task of hand-written cryptography are two other factors that need to be grasped to understand the future interest of Operation Vula with programming and cryptographic tools. The fact

[2] In 1978, President Carter banned the sale of USA goods to the South African Military and Police including computers, but in 1982 Reagan lifted the ban. Following public and congress pressure Reagan had to reverse his decision. Having said that it is important to understand that the CIA was funding and supporting the South African apartheid regime in their so-called anti-communist quest.

[3] Lin Piao (1965) declaration "Long Live The Victory of People's War" first proposed the concept of a People's War, which was used by many subsequent guerrilla movements. Retrieved from https://www.marxists.org/reference/archive/lin-biao/1965/09/peoples_war/

[4] Exiled in the UK, Ronnie Press started with others the ANC Technical Committee (TC). The TC was to provide technical assistance for the anti-apartheid movement.

that the ANC leadership was in exile (often based in Lusaka, London or elsewhere) made communication difficult. And as surveillance of phone calls, postal mails, leaflets, radio broadcasts was ubiquitous by the apartheid regime whether in South Africa or elsewhere, the ANC could not fully rely on such means of communication to share and exchange strategic information.

In order to understand what I mean by anti-colonial hacking, I will propose and discuss five principles that characterise it using the autonomous encrypted communication network developed during the anti-apartheid struggle as a case study. In an attempt to define anti-colonial hacking these principles will be explored in relation to contemporary forms of crypto-activism impelled by Wikileaks and Edward Snowden's revelation of mass surveillance. The history of cryptography has had until now strong Western and American groundings. While acknowledging the importance of this history to the crypto movement today, I will nonetheless argue that the example of the autonomous encrypted communication network comes to enrich the history of hacking and cryptography by highlighting its anti-colonial nature and the necessary assemblage of technologies (Deleuze & Guattari 1980) to adapt to a specific context and underground situation.

While I believe the concept of anti-colonial hacking might open up a new field of investigation, I still maintain that the practice is inscribed in a continuum of hacking practices. Its sensitivities however are informed by particular political, liberation and resistance contexts and conditions. Such sensitivities brings visibility to a field, hacking, that has long been dominated by a certain form and understanding of practices located particularly in the western world and often from a libertarian perspective (Turner 2006). The set of values that are projected on and about Africa is one that needs redress. The continent of Africa is a site of constant resistance to past and present pillaging by the West (Rodney 2012) in particular and against the (neo) colonial narratives that has legitimised its exploitation (Bowker and Star 2000; Eckstein & Schwarz 2014). It is my hope that by using the term anti-colonial hacking it helps redress in some ways the visible imbalances and the contributions that the practice and the nascent research on the practice has afforded to the continent and its people.

Data and Methodology:

Up to now, there has been nearly no scholarship on this autonomous encrypted communication network. Most of published articles are either in intelligence or counter intelligence journals analysing the

military and political aspects of Operation Vula (Henderson 1997) or have been personal accounts or biographies written by those who have taken part in this project (Braam 1992; Jenkin 1995; Maharaj 2010; O'Malley 2007; Press 1995). One of the only articles inscribed in a more social movement scholarship entitled Revolutionary Secrets: Technology's Role in the South African Anti-Apartheid Movement (Garrett & Edwards 2007) highlights the use of technology for social change, but does not link the autonomous encrypted communication network to the hacker and crypto movements. Therefore, rather than anchoring this research in social movement scholarship, as Garrett and Edwards have done, I rather look at it from a Science and Technology Studies (STS) perspective at the intersection of Anti-Colonial Scholarship to bring new light to an encrypted communication system that Nelson Mandela (O'Malley 2007) referred to as bringing a whole new dimension to the struggle against apartheid.

> *'It extended the boundaries of the struggle, and in doing that, transformed the nature of the struggle itself. For the first time ever, the ANC was able to connect the various tentacles of the struggle.' (p.19)*

The bulk of this research rests on primary and secondary material such as academic articles, biographies, personal accounts, African National Congress archives, and a documentary film about Operation Vula entitled: The Vula Connection. In order to bring to the fore the voices of those who have been instrumental in creating, operating and using the encrypted communication network, I have also conducted interviews to corroborate and enrich the primary and secondary material. I have interviewed Tim Jenkin, the main developer of the encrypted communication system, and kept communication via email to better understand the system he designed with Ronnie Press[5]. I have also interviewed, Janet Love an Operation Vula and MK cadre who used the encrypted communication network while underground in South Africa. Finally, Lucia Raadschelders a Dutch national was interviewed via email as she was the one who received and send encrypted messages from Lusaka, Zambia.

The contribution of this article rests in two primary areas. First, it is at the historical and empirical level and second at the theoretical and political level. This article is part of the history of technology as it attempts to document with available sources, mostly Jenkin's account (1995) of how the system worked. The interviews conducted also helped to have a better sense of the system as a whole. The second contribution is to suggest the concept of anti-colonial hacking as a way to understand a

[5] Ronnie Press passed away in 2010.

phenomenon that has existed at the practical level, but not been theorised yet. Therefore the *raison d'être* of this article is not only to document what has happened, but also to intervene in the discourse of the sociology of technology. Intervening in the discourse is done in two ways. One the one hand, through the demonstration of the politisation of technology. In the case of the encrypted communication network this technology was developed from a particular point of view with clear goals in mind. On the other hand, by using anti-colonial scholarship it allows to formulate a critic of modernity, of technological progress, by suggesting an alternative form of modernity (Anderson 2002, Appadurai 1996, Feenberg 1996; Sahlin 1995). Anti-colonial hacking is a break in the history of technological progress and a departure from western hegemonic narratives about technology generally and hacking more specifically. This brings to the fore new aspects of hacking that inform an anti-colonial posture such as with collectivism, autonomy, the assemblage of technology, digital literacy and women's roles.

Before going further I need to highlight the shortcomings with this research. First, it only focuses on one case study to illustrate the concept of anti-colonial hacking. However, the example taken is so significant in embodying the concept that I hope the shortfall can be somewhat alleviated. Second, I have not been able to communicate with some major figures who were at the heart of Operation Vula, such as Mac Maharaj, Siphiwe Nyanda and others. And finally, all the people I interviewed were white people who dedicated their lives to supporting the anti-apartheid struggle.

Finally, the growing body of literature that pertains to post-colonialism and science and technology is growing. Among them are hacking in the Global South (Chan 2014; Lindtner 2014), post-colonial computing (Irani, L., Vertesi, J., Dourish, P., Philip, K. & Grinter, R. 2010), feminist post-colonial science and technologies studies (Harding 2011, 2008) and post-colonial piracy (Eckstein & Schwarz 2014). All these fields deserve to be more documented.

Background

In the 1960s, the ANC had to revise its strategies after two significant events. The government ban of the ANC[6] and the Sharpeville Massacre of 1960[7] . In response, the ANC founded a radical organization, the Umkhonto we Sizwe (MK or Spear of the Nation) which was described by Joe Slovo as "an

[6] Other parties such as Pan African Congress (PAC) were banned or other entities such as the ANC Women's League (ANCWL) were also banned.

[7] On March 21, 1960, the South African police open fire on unarmed black protesters who were marching to contest a law (the pass law) that made them second class citizen, killing 69. Many of them were killed in the back as they were fleeing. In

independent military body that supported the liberation movement" (Slovo 1986).[8] MK's operatives started with a sabotage campaign which targeted the apartheid economic infrastructure such as pylons, communication and transport infrastructures or the infrastructure that represented oppression such as pass offices and other governmental buildings (Slovo 1986; Davis 2009). Early on, in 1962, Mandela[9] was arrested, but when Rivonia farm, the secret headquarters of the high command of MK, was busted in 1963 documents incriminating Mandela found him and others responsible for the sabotage campaign (Holland 1989). He was sentenced to a life sentence. In his trial statement Mandela said:

> *I do not, however, deny that I planned sabotage. I did not plan it in a spirit of recklessness, nor because I have any love of violence. I planned it as a result of a calm and sober assessment of the political situation that had arisen after many years of tyranny, exploitation, and oppression of my people by the Whites*. (1964)

It is also at Rivonia farm where activist started Freedom Radio or ANC radio (later known as Radio Freedom) a clandestine radio station meant to create a new narrative, a political propaganda around revolution, which in turn it was hoped would support MK's actions. The radio stopped transmitting when authorities busted the farm, but would re-emerge from abroad in subsequent years and carry an important role in broadcasting ANC messages to South Africa (Suttner 2008, Lekgoathi 2010).

The MK-led sabotage campaign was met with state repression coming in the form of new laws, surveillance, arrest, etc. Looking back Slovo highlights that: "In the years immediately after the Rivonia trial, all our attempts to rebuild underground structures failed. The structures of the ANC inside South Africa had been destroyed (1986)." Having no ANC leaders on the ground to propel, organise and strengthen local resistance, would later be recognised as the *raison d'etre* of Operation Vula in order to change this state of affair.

Despite this context, the ANC was nonetheless sending a few well-trained operatives on the ground to make the ANC and its cause visible. One of those operatives was a white late twenty year-old tech-savvy South African named Tim Jenkin. Before his political consciousness was raised which later push him to become involved with the ANC, Jenkin had no idea of the brutality of the apartheid regime despite having grown up in South Africa. In his book Jenkin's (1987) talks about the difficulty for white South African to "break free of the web of privilege and racism " and how through the intellectual route he was able to see the light (p.). After working clandestinely in Cape Town for two years printing and

1966, the United Nations recognised March 21 as the International Day for the Elimination of Racial Discrimination.

[8] Starting the MK and presenting it as Joe Slovo did was and is still is contentious.

[9] Joe Slovo (1986) wrote that the ANC had appointed Mandela and South African Communist Party (SACP) himself to compose the High Command of the MK.

distributing ANC material he was arrested in 1978 and convicted to twelve years in prison under terrorist charges (Jenkin 1987). He was jailed for leaflet bombing[10], a bomb device he was taught to build by the ANC Technical Committee to "wake up" South African to the ANC cause. In a meticulously planned escape[11], using lock picking[12], Jenkin and two others, namely Alex Moumbaris and Stephen Lee escaped from a Pretoria prison for white political prisoners, one year and half after Tim and Stephen had been convicted (Jenkin 1987; North 2012). After taking refuge in London, UK, in the early 80s freedom fighter Tim Jenkin became one of the trainers for underground work and covert operations. At the same time and as part of the Technical Committee Tim Jenkin and Ronnie Press, an exiled South African chemistry professor, started experimenting with programming and cryptography on some of the first affordable computers available in Britain.

Until the beginning of the 1980s, the ANC did not rely a sophisticated and effective communication[13] network. It often used couriers who travelled in and out of the country to bring instructions, banned literature and pamphlets[14] (Suttner 2007) or used Radio Freedom (Davis 2009; Houston and all 2013; Lekgoathi 2010) to convey messages and revolution narratives. The ANC also resorted to plain old hand-written cryptography, but this form of communication was so demanding time-wise that very few operatives underground were using it on a regular basis.

The difficulty in and time required to exchange secure communication changed drastically with Tim's system. Jenkin said in the first ever account of the encrypted communication network:

> "It is astonishing that so few [ANC leaders] were able to see this [the need for a secure communication network], as communications is the most important weapon in any conflict situation […]. The purchase of our first computer led to a revolution in our communications that ultimately made possible operations such as vula". (Jenkin, 1995)

[10] A leaflet bomb was a means to broadcast ANC material and news such as the invasion of Angola by South Africa or to remind South Africans of the "anniversary" of the Sharpville massacre. Leafltboms succeeded in spreading information about events and news that were otherwise not available for ordinary South Africans.
[11] The book *Papillion* by Henri Charrière was a great source of inspiration to plan their escape.
[12] Within about a year, Jenkin and comrades made wooden keys of all the prison locks in the prison wood workshop. Through the assemblage of wooden pieces, they were able to escape passing through 10 locked doors. It is to be said that lock-picking workshops are a regular occurrence at hacker conferences.
[13] It is important to remember that all mails comprising of posters, leaflet, etc. destined to South Africa that was sent from abroad or that was being circulated inside the country were intercepted by the South African police. Snail mail was not a reliable system of communication nor was the phone as telephone communication were bugged. Moreover, the use of hand-written crypto was a very slow process. The use of automated cryptography did allow for the increase speed of conveying strategic information and as it was an underground autonomous encrypted communication network the South African did not know it existed until it was busted in the 1990s.
[14] Women were often doing this kind of work.

To come up with the encrypted communication network, Tim Jenkin and Ronnie Press experimented with a multitude of technologies from paging devices, touch tones, modems, public and landline phones, tape recorders, among others. They also experimented with a small computer available at the time, a PX-1000 which allowed for encrypted communication, but the latter was deemed not appropriate for the task at hand.[15]

How did the system work? (See Drawing 1)[16]

The top level cadres who were sent into South Africa were trained by Tim Jenkin in London and Lusaka. These cadres then trained others in key operations related to the communication system. The laptop computers, encryption programs, essential equipment and key disks were infiltrated by anti-apartheid activist Antoinette, a Dutch flight attendant, who regularly flew from Amsterdam to Johannesburg.

To send a message from South Africa, the user - let's say Janet Love - would type a message on her laptop computer, encipher it and then pass it out through the computer's serial port to an acoustic coupler modem. This converted the digital data to sound and the audio stream was captured on a small cassette tape recorder. She would then take the recorder to a public telephone or anonymous telephone in an office and dial Tim Jenkin's phone number in London, which had a special answering machine attached to it to receive the messages. If Jenkin was travelling, instructions would be given to dial Ronnie Press' backup number, also in London. Jenkin's and Press' flats were connected by a private Bulletin Board System, with a backup radio link. The recording on the tape recorder (the "humming buzz sound") was played into the telephone mouthpiece with a small speaker. The received audio messages were stored on the London 'receive' answering machine. Jenkin (or Press) would then reverse the process by playing the received audio messages back through a similar acoustic modem attached to their computers, to convert it back to digital. The digital data would be deciphered using a matching key disk. The deciphered message would then appear as plaintext on the computer screen and could be

[15] In an email conversation with Tim Jenkin, he explained that a PX-1000 could first only talk to another PX-1000 and second only at the same time and on the same communication line. In anti-apartheid struggle, this was impossible to use he explains as no one could be on the same line at the same time. Second, Jenkin did not trust the encryption on the machine. He suspected that there might be a 'backdoor' that would allow the enemy to crack their messages. Third, he found that the PX-1000 did not work very well between South Africa and Europe. The quality of the lines were never good enough, he said.

[16] I would like to thank Tim Jenkin for is review of this section.

printed for archiving or stored with another encryption program. The London operators would analyse each message to determine which items had to be passed on to Lusaka, which items were for other destinations and which could be dealt with by London.

When there were messages for South Africa from London, the operative who the messages were for would be paged with a code indicating how many messages there were to pick up. The operative would then go to a public telephone and dial a different number in London to access the 'send' answering machine. The messages to be received were played as outgoing messages by the answering machine and recorded by the operative onto the same small cassette tape recorder by placing a special microphone on the earpiece of the telephone. The recorded messages would be taken home where they were played back into the laptop via the acoustic modem, and deciphered as described above.

The initial arrangement in Lusaka worked in much the same way, but without having to use public telephones. Lucia would receive enciphered messages, decipher them and print them out. A courier would pick up the printed messages at Lucia's office and take them to Olivier Tambo, the president of the ANC, and other senior ANC members who were in the know about Operation Vula. Messages for London were likewise left on the separate 'receive' answering machine. Later a more advanced Bulletin Board System was used. A dedicated computer in London was used for both depositing and receiving messages.

The encrypted communication network was fully operational from July/August 1988. When it was discovered in July 1990 by the South African Police, Jenkin quickly changed the keys, which allowed it to continue operating for almost another year. When infiltrated Operation Vula cadres got amnesty in June 1991 and negotiations with the South Africa government were at an advanced stage, the autonomous encrypted communication network slowly wound down. In total about ten top-level cadres used the autonomous encrypted communication network in South Africa, although there were others who performed minor roles such as relaying and receiving messages from public telephones. There were other links to the Netherlands, Canada, Zimbabwe and in the UK.[17]

Drawing 1. Simplified Drawing of How The Encrypted Communication System worked. The drawing shows how to send a message from South Africa to Lusaka via London.

[17]For a complete and exhaustive technical description see Jenkin 1995.

It is through the tinkering with many different technologies that Jenkin and Press slowly built a technological assemblage that would come to compose the autonomous encrypted communication network.[18] Over the years, Jenkin would continue to improve his cryptographic skills refining its algorithm[19] on which the autonomous encrypted communication network would reside. He would end-up conceiving an effective means of encrypted communication despite the local challenging context. His users, the operatives sent in South Africa and those who would be receiving/sending the messages from Lusaka would also play a role in creating the conditions to make the best use of the autonomous encrypted communication network, except however when the communication network was accidently discovered by the South African police in 1990 (to know more see Henderson 1997).

What is significant with this chapter of history is that some historical records show that hand-written cryptography was used by other African liberation struggle such as in Angola (Ribeiro-Kabulu 1996), but it appears that Tim Jenkin and Ronnie Press autonomous encrypted communication network developed in the mid and late 80s, and in full use in the end of the 80s and beginning of the 90s might have been the first of its kind developed by and for an African liberation struggle movement making this example at the heart of what I call anti-colonial hacking.

Anti-Colonial Hacking

What kind of principles and sensitivities inform anti-colonial hacking? Before being able to answer this question properly one needs to understand what hacking is. Hacking can be loosely defined as a prac-

[18] While the WWW as we know today did not exist, FidoNet an early form of the internet that connected computers together did. FidoNet consisted of a few thousand nodes which "move email and e-news over the public telephone network using a unique protocol and data format" (Bush 1993). One of these nodes was WorkNet (today SANGONeT) an organisation set up in 1987 in South Africa at about the time when the encrypted communication system was being tested and implemented. Using FidoNet was considered too dangerous for sharing strategic information. While WorkNet did not connect to Operation Vula, the NGO did share and convey information about human rights in their networks through the Fido system and this network of NGO Fido nodes that composed the Association for Progressive Communication (APC) (Mikelsons 1992).

[19] Jenkin's algorithm was based on the automation of a one time pad. The one time pad encryption method was used during the second World War by the Soviet Union. The way it functioned was that it was based on a one time pad booklet with 100 sheets in the booklet. Each sheets had a unique alphabet (A-Z and 1-9 and a few other characters). On each pages the characters would be different. Once you had written your message in plain text and convert it into its new alphabetical value you would simply had to right the value below and covert it to modular arithmetic (i.e. where you just add two number (e.g. 9+9 = 18 and you throw the 1 so you have 8). As time went on, Jenkin and Press further developed their algorithm using the same idea. Howeber, instead of encrypting at the character level (which would be limited in terms of the length of the message – a message of a 1000 caracter would imply a 1000 keys), they would encrypt at the bytes level. The one time pad became a very long file that would fit on a floppy disk.

tice that involves programming and/or tinkering with technology. In Coleman's (forthcoming 2015) introduction to the term hacker, she defines one "as a technologist with a penchant for computing" and define a hack has "a clever technical solution arrived at through non-obvious means" (p. 1). At the core of today's hackers and tech activists are such concerns as freedom of expression and privacy expressed through their struggle and criticism towards the corporatisation of the internet, mass surveillance, the importance of building tools for anonymity and encryption and Free, Libre and Open Source Software (FLOSS), among others.

To inform the concept of hacking through an anti-colonial perspective, I use anti-colonial scholarship as a way to bring light to the struggle against dispossession and domination from colonial relationships through the practice of hacking. Anti-colonial scholarship is a rich field of research and praxis that Young describes in the following terms:

> "[…] anti-colonialism was a diasporic production, a revolutionary mixture of the indigenous and the cosmopolitan, a complex constellation of situated local knowledge combined with radical, universal political principles, constructed and facilitated through international networks of party cells and organizations, and widespread political contacts between different revolutionary organizations that generated common practical information and material support as well as spreading radical political and intellectual ideas" (2001, p.2).

From this starting point, I refer to anti-colonial hacking in very general and broad terms as a practice that uses technological skills, including programming and crypto skills, as part of a liberation or decolonisation movement that aims to fight colonialism in all its forms, including apartheid. But it also goes further than only the people who are involved in this quest. As it will be demonstrated below, I understand anti-colonial hacking as a way to question the modern narrative of technology that considers technology as neutral. Anti-colonial hacking questions the techno-determinist argument that technology brings about social progress. In fact, anti-colonial hacking is a situated technology. This largely sets them apart from many but not all of today's hacking practices. In other words, anti-colonial hacking is developed from a certain point of view to support very specific outcomes. As we will see below, anti-colonial hacking foregrounds collectivism, autonomy, the assemblage of a set of technology, literacy and the inclusion of women as key values.

The concept of anti-colonial hacking that will be used to discuss the autonomous encrypted communication network is mostly inspired by the work of Frantz Fanon (1952, 1961, 1964, 2011).

While Fanon helps shed light on the decoloniation process through an enabling politics of violence, it is also important to remember that other anti-colonial actors who were first influenced by Ghandi's principles of civil disobedience as with Ghana (Nkrumah 1973), Tanzania (Nyerere 1968) and Zambia (Kaunda 1982), came to the realisation that settler colonialism had to resort to the use of violence to bring to an end such forceful regimes (Cabral 1969, Kaunda 1982, Nkrumah 1973, Young 2001).

In *The Wretch of the Earth,* Fanon (1966) articulates decolonisation as a fierce process that sets out to change the order of the world from the ground up.

> *To tell the truth, the proof of success lies in a whole social structure being changed from the bottom up. The extraordinary importance of this change is that it is willed, called for and demanded. The need for this change exists in its crude state, impetuous and compelling, in the consciousness and in the lives of the men and women who are colonised* (1966, p. 29).

Using such scholarship to propose a particular form of hacking along the lines of anti-colonialism is apt in the context of 1980s apartheid. Moreover, it highlights the importance of such practice at a time where technology and particularly computers were used as a tool for surveillance, control and structured violence that reinforced apartheid. In the case of South Africa under apartheid, not only people were under constant surveillance through different technological regimes such as the passbook (Bowker & Star 2000), but all communication and information outlets whether by radio, tv, newspapers, books, etc. were controlled, and laws were implemented to restrict freedom of the press and the right to communicate (Davis 2009). The state and intelligence apparatus were also monitoring, tracking and surveying underground means of communications. Freedom fighters in exile whether in Great Britain, The Netherlands or elsewhere, were constantly surveilled and spied on. Therefore, the use of encryption was a response to counter the surveillance and repression exercised by the state and its technologies.

Below I propose to examine five principles and sensibilities that comes to underpin the autonomous encrypted communication network developed to fight apartheid. In turn, those traits help to shed light on a conceptualisation of anti-colonial forms of hacking. They also permit to refine what anti-colonial hacking means by showing that the practice as particular components that sometime distinguishes sometime resembles more contemporary hacking practices. Bringing closer together anti-colonial scholarship and hacking practices come to enrich the field of hacking both at a conceptual and practical levels.

Collectivism

First, I posit that the centrality of the autonomous encrypted communication network rests on defending the collective rights of a people. Collective rights here are less understood through a classic contemporary human rights framework of socio, economic and cultural rights (a.k.a second generation rights) and the political and civil rights (a.k.a first generation rights). They are rather understood through a form of collectivism or African communalism that foregrounds mutual aid, solidarity and social justice (Young 2001).

When looking at Fanon's work on the struggle for freedom, the process of collective consciousness raising through action which in turn brings about a collectivism framework is clearly stated:

> *[In the struggle for freedom] Individualism is the first to disappear. The native intellectual had learnt from his master that the individual ought to express himself fully. The colonialist bourgeoisie had hammered into the native's mind the idea of a society of individuals where each person shuts himself up in his own subjectivity, and whose only wealth is individual thought. Now the native who has the opportunity to return to the people during the struggle for freedom will discover the falseness of this theory. (1966, p. 38)*

The grounding of anti-colonial hacking in collectivism is in contrast with the individualism that is particularly present in today's ubiquitous world of social media and to some extent encryption.[20] Indeed, encryption is often understood as revolving around the sanctity of the right to privacy and freedom of expression, two rights that can be categorised as individual rights[21]. Far from wanting to pit individual rights vs. collective rights, civil liberties are fundamental in this ubiquitous world of surveillance, I nonetheless want to highlight the ways in which a particular understanding of individual rights, has been popularised by the libertarian cypherpunk movement[22] where the no rules, no laws, no government ideas prevail.

The cypherpunk movement that was created in the late 80s did not want the USA government to restrict

[20] Ippolita's (2015) most recent publication calls on the link between social networking sites, particularly Facebook, and the propagation of libertarian values and practices (p.53).

[21]While i argue that encryption today is mostly framed through an individual rights perspective, i don't deny that encryption might embody collective rights intention.

[22]The movement is still philosophically influenced by Tim Way "Crypto Anarchist Manifesto" and Eric Hughes "Cypherpunk Manifesto" two political libertarians whose mailing list, the cypherpunk mailing list, was instrumental to the coming together of this movement.

their desire and interest for anonymity whether it be for financial transactions or private communications. The development and use of encryption today seems to largely be influenced by this individualist paradigm. To understand this strong influence, one needs to remember that cryptography was prohibited to be used in the civilian sphere before the late 1990s, making it only available to governmental agencies and later to companies whose algorithms would have to be approved by the National Security Agency (NSA). At that time the USA government was trying to stifle the efforts of academics, mathematicians and activists to have public-key cryptography[23] fall in the civilian sphere and be shared on the internet[24] or through academic papers. In the 1990s a battle was fought on multiple front by programmers, mathematicians and academics to consider strong cryptography outside the categorisation of a weapon or a "munition". In the USA, cryptography was regulated under The Arms Export Control Act and the International Traffic in Arms Regulations. It required anyone who intended to publish their work on cryptography to submit their ideas to the "government for review, to register as an arms dealer, and to apply for and obtain from the government a license to publish their ideas"[25]. Failure to do so would result in civil and criminal sanctions. As a result of this situation and the interest of more and more people towards cryptography, a cryptowar was started and was ultimately won by programmers, mathematicians, academics and amateur cryptographers who succeeded in making cryptography a non-weapon tool (Levy 2002). In the famous *Bernstein v. The Justice Department* case, it was recognised that "source code was speech protected by the First Amendment and that the government's regulations preventing its publication were unconstitutional"[26].

The libertarian and Californian hyper-capitalist stance highlighted in this example foregrounds an understanding of freedom based on free market, on very little to no laws, rules or regulations that prevent individuals to do what they want. This is in contrast with the values that animated and informed the collectivism framework behind the encrypted communication network. In fact, what the encrypted communication network example seems to allow is a strong focus on collective rights and collectivism i.e. the use of crypto in particular, but also the assemblage of different kind of technologies for allowing strategic and tactical information to be exchanged between the ANC leaderships and operatives on the ground with the ultimate aim of liberating a people from oppression.

[23] Public key cryptography or asymmetric cryptography is made out of a public key and a private key. It is based on a one-way function, which means that a message is easy to encrypt, but extremely hard to reverse. That is the strength of a one-way function. For more on one-way function and thus of asymmetric crypto see Levy 2002.
[24] One of the best example of this is with OpenPgP. To know more see Levy 2002.
[25] https://www.eff.org/cases/bernstein-v-us-dept-justice
[26]https://www.eff.org/cases/bernstein-v-us-dept-justice

To exemplify the consciousness that happens in liberation struggles, Fanon illuminates:

> *The mobilisation of the masses, when it arises out of the war of liberation, introduces into each man's consciousness the idea of a common cause, of a national destiny and a collective history. (1966, p. 73)*

Understanding this form of hacking through a collectivism framework also allows for the expansion of the scope and values associated with the use of cryptography. The encrypted communication network's goals were different than the goals and attempt of the cypherpunk movement and of many of today's crypto projects. While the two latter aimed at having crypto useable in the civilian sphere whether for private economic transactions or for private and anonymous communications, the former was to be used only by a few. One of the main reasons to keep the communication network secret was to avoid infiltration, a plight of past ANC and MK work (David 2009). It was also restricted to a few developers and users because the symmetric cryptography system developed required that both the sender and the receiver use the same key disk. Hence the fewer the people who had the disk the better.[27] While the latter might appear as a limitation, it is fundamental to understand that the encrypted communication system fit into the multiple tactics used to bring about liberation. The system built was not separated from a liberation struggle, it was fully embedded in it.

Re-appropriation and Re-purposing:

Another important aspect of the encrypted communication network is the re-appropriation and re-purposing of a technology for the purpose of liberation[28]. In a context where the South African apartheid regime was using computers to automate apartheid (NARMIC/American Friends Service Committee 1982) the re-appropriation and re-purposing aspect of the encrypted communication network was in direct opposition to it. The regime in place had set up a passbook system (Bowker & Star 2000) [29] that according to Edwards and Hecht (2010) "sought to stabilise a specifically racial personal identity around a document coupled to a biometrically indexed database" (p. 625). 30 While the South African

[27]The strength and innovation with the public key cryptography (a.k.a. asymmetric cryptography) is that it allowed to have one's public key public and one private key private. This would enable widespread use of crypto.

[28]While in my article I often use the word liberation to mean either independence or liberation, I do agree with Cabral's differention of the two processes.

[29]To establish the automated passbook the apartheid regime attempted to trackdown and fingerprint every individuals. The aim of the passbook was to control the 'native' movements.

[30]In such a context of "techno apartheid" the black population was however able to forge or "hack" this system in forging the passbook.

government used technology to try to automate apartheid and create a narrative of progress and modernity around their use of technology to set them aside from the rest of the African continent, those resisting the regime in place were creating an assemblage of technology that supported a different epistemological understanding of technology closer to a form of African socialism.

Frantz Fanon (2011) article entitled: *Ici la voix de l'Algérie (*This is the Voice of Algeria*)* is illuminating in this context and is about the re-appropriation and re-purposing of a western technology, the radio, in the case of colonial Algeria. Fanon explains that early on in a coloniser-colonised framework Algerians did not want to own nor listen to the radio. At one level it was argued that it was for morality reasons, but at another level it was believed that the technology had been rejected as a way to resist the colonial state, its propaganda and its technology. Under French colonialism and before the Algerian revolution, radio sets were owned by a majority of white Europeans and the content broadcasted represented the views of the oppressor. But this changed dramatically during the Algerian revolution. The announcement of the creation of the secrete radio *La Voix de l'Algérie Libre et Combattante (*The Voice of Free and Combative Algeria) by the Algerian National Liberation Front (FLN) changed this state of affairs. In less than 20 days Fanon explains, Algerians were listening avidly to the radio to get news and criticisms which were coming from outside the colonial state purview. Fanon demonstrated how radio stopped being perceived as an instrument of colonial propaganda and transformed into a technology of liberation for the Algerian people.

Though the encrypted communication network was not used for propaganda purposes, it was rather used to foster a people's war, that is for an operational goal, Fanon's analysis helps shed light to the fact that technology are not neutral. The encrypted communication system use of computers were subverted by the ANC for the liberation struggle, despite the fact that only a few operatives on the ground were aware of this re-appropriation and re-purposing of technology.

Autonomous Infrastructure

Following Star and Ruhleder I use the term infrastructure to mean that it is "fundamentally and always a relation, not a thing" (1994, p.253). Infrastructure is thus understood as a system of the artifact kind (computer, software, code, algorithm etc.), and as a cultural and historical system. As for autonomy, it is not understood as meaning technology working by itself (such as with autonomous robotics, google cars, etc.) rather it is in the sense that it strives to be as much as possible outside the dominant oppressive system with its own goals and values, in addition to the self-valorisation it creates among

disenfranchised people. Autonomy used here is in the tradition of African socialism a framework that was popular among many leaders in Africa, but which took different forms whether it was an emphasis on self-reliance and small-scale projects in Nyerere Tazania or Nkrumah's contribution to African cultural and intellectual autonomy (Young 2001). From this understanding, I posit that autonomous infrastructures have the power to disrupt systems in place and in certain context to bring destructuration. In the case of the encrypted communication network the infrastructure that was built helped facilitate the destructuration of the apartheid regime and of its understanding and use of technology. They were not only creating a system from the ground up, they were also hacking the dominant epistemic stance of the apartheid understanding of modernity and technology. In a more concrete and matter of fact way, highlighting the people's war objective, it enabled as Tim Jenkin wrote to do the following:

> "Most requests were for money, documents, additional equipment for communications and the like. When the first request for weapons appeared on my screen my eyes stood out on stalks. I had seen the comrades packing some light weaponry when I was in Lusaka in June but now they were asking for an arsenal: AKM automatic rifles, TNT, detonating cord, hand grenades, RPG rocket launchers and rifle silencers, amongst other things."(Jenkin, 1995)

The encrypted communication network rests on the experiences and the mastering of the technological means of production by freedom fighters who are able to re-appropriate and re-purpose technologies for liberation (Noble 1983; Soderberg 2008). This re-appropriation is about creating a space of autonomy with an existing technology and the creation of something new with the assemblage of technologies. In other words, it is about developing one's own autonomous technology or technological infrastructure that does not oppress, but rather aims at liberation.

Autonomy is of course relative and the system developed by Tim Jenkin and Ronnie Press resided on using technology that already existed (such as phones, tape recorders, computers, the international communication system, etc.) and created an assemblage that repurposed the technologies used which in turn opened up new possibilities. This is part of what a clever hack means or what Anne Balsamo (2011) understands as a form of imagination. She writes "the wellspring of technological innovation is the technological imagination, a quality of mind that enables people to think with technology, to transform what is known into what is possible" (p.6). The imagination, curiosity and dedication it takes for transforming an idea into a concrete possibility and a clever hack is a characteristic that many

hackers share and that the crafters of the encrypted communication network embodied.

Autonomy is also related to the non-commercial aspect of the developed technology. In relation to this aspect Tim Jenkin made it clear from the start that this initiative was not intended for commercial use. The ultimate aim was to facilitate the liberation of a people. The technological assemblage that they put together was beyond the simple idea of innovating for innovating or to make profit, it was about facilitating the secure communication of a small group of people to make an Operation, like Vula possible.

The autonomous aspect of the communication system was not based on a commercial algorithm or commercial option to encrypt ones' communications, it was based on an algorithm that had been designed by Jenkin and which embodied the autonomous aspect of the network. When Jenkin developed his algorithm, the Diffie-Hellman (DH) and RSA (Rivest-Shamir-Adelman) algorithms already existed[31], but few outside a very confined crowd knew about these important development in strong crypto (Levy 2002). In addition, these algorithms only fell into the public domain respectively in the year 2000 (for RSA) and 1997 (Diffie-Hellman) (Omura n.d). Both MIT (RSA) and Stanford (DH) had patented the discovery of their mathematicians and both groups had put together companies to sell their products with a profit aim. Before the algorithms fell into the public realm who ever wanted to use them needed to pay for its use.

Compare with the work of the academics and mathematicians who designed the DH and RSA, the goal of Tim Jenkin and his compatriots was not to make money nor to patent the device[32]. The project was not based on scientific curiosity or came from a hobbyist passion. Their goal was specific, they were working around the clock to come up with devices and an assemblage of technologies which would help the ANC cause. Their struggle through technical means permitted a level of agency which was a response against the brutal conditions in which people in South Africa or those in exiled lived. The creation of this encrypted communication network was inscribed in somewhat of a different set of values: to create the conditions for liberating a people's from a white supremacist state. In fact, when the apartheid regime collapsed and was replaced by a democratically elected state, the autonomous

[31]These are the main algorithms for strong crypto that were designed in the 1970 and are still the main algorithm used for public key crypto.

[32] MIT and Stanford both patented the algorithms of their researchers and the RSA MIT mathematicians create a company to sell their algorithm for big bucks to companies. After 20 years, the algorithm patent has fallen in the public domain meaning that activist tech collective for instance can use the algorithm without having to pay the patent.

encrypted communication network stopped being used.

As a response to Garrets and Edwards (2008) view that ponders why Jenkin had reinvented the wheel with the encryption part of the communication network and rather not use the algorithm available commercially at a time, I would rather like to suggest that the feeling of autonomy was crucial to the communication network. In their 2008 paper Garrets and Edwards say:

> *In the mid-1980s, when Jenkin and Press began to contemplate using computers, computer-based encryption was already a well-established field with a robust research literature, national standards, and commercial products. For example, by 1977 the United States had established a national Data Encryption Standard ("Data Encryption Standard Fact Sheet," 1996), and products based on this standard were commercially available ("IBMs Cryptographic Products," 1978).*

The DES was indeed an encryption algorithm that existed and as Levy (2002) argues "would become the no-brainer choice for private industry" (p. 38). Moreover, Levy states that Hellman, one of the two cryptographers behind the Diffie-Hellman algorithm, "knew that his old and trusted colleagues at IBM had been cooking up a system designed to satisfy the government's criteria [...] and learned that the National Security Agency apparently had a hand in its development" (p.39). In other words, the DES had a backdoor. When interviewed about this aspect Jenkin said:

> *They wonder why we reinvented the wheel. They did not get it. Even at that time, we knew that backdoors could exist, but at that time we did not fully understand what it meant. We were just experimenting and we didn't have the knowledge that we have today. But the suspicion was there. The commercial stuff did not answer our needs so we needed to build our own.* (*Tim interview, June 19, 2015*)

This need to build ones' own infrastructure, is also present in today's tech collectives such as Riseup, Nadir, Autistici/Inventati, among others (Milan 2013). Those tech collectives develop their own email service infrastructure even when Gmail, Hotmail and Yahoo services exist. The question of whether such services already exist or not, I would argue, is not the right way to frame the development of the encrypted communication network. It is rather about autonomy. The possibility to control to some extent the means of production, the way a technology is being used and out of the control of the state

and corporation apparatus.

Technological Literacy

As computers and cryptography were largely new in the 1980s, technological literacy and trainings were paramount for the well-functioning of the encrypted communication network as many had never used a computer before. This was embedded in the project from the start. In fact, the only way for Operation Vula, to function was to make its users technologically literate. This aspect goes in perfect line with liberation struggles strong literacy and educational component to their larger endeavour. New ANC and MK recruits for instance who were sent to training camps outside South Africa were being thought how to write and read in addition to anti-colonial thoughts (Cherry 2012).

In talking about the training dimension, Jenkin says:

> *As this was the 1980s very few people had much experience with computers. This made the training quite difficult for some as they had to learn the basics before they could even get to the encryption programs. So the selection* [of users] *was not made on the basis of experience but on the basis of need. Those comrades who were going to be on the 'front line' and who needed to communicate with the ANC leadership were the ones who were required to learn how to operate the comms equipment.* (*Tim interview, June 19, 2015*)

An operative such as Lucia and other users on the ground in South Africa needed to be trained to use the system. The aspect of basic technological literacy could not be taken for granted in the late 1980s where computers were not widely used. Talking about the training she received to operate the system Lucia said:

> *[I was trained] mainly how to use a laptop (first time ever for me), how to connect and use the modem, how and when to use the two encryption programmes, simple trouble shooting, how to use the answering machine, down and uploading of messages, what to be aware of. (Lucia interview, June 9, 2015)*

Moreover, Tim Jenkin who trained most of the users and operatives in using the system talked about the ways in which there was a division of labour with using the system to ensure security.

Some of those trained in the communications were only trained in certain aspects of it, such as taking the tape recorders to the public telephones to send and receive messages. These people did not learn or even know about the computer equipment and encryption programs. (*Tim interview, June 19, 2015)*

Moreover, in a context like Lusaka, Zambia particularly, electricity was not a given, the quality of the telephone lines and the downtime in telephone service among others were all impediment to the well-functioning of the autonomous encrypted communication system. One of the operators of the encrypted communication network Lucia Raadschelders based in Lusaka from 1988 to 1991 said to highlight the difficulties met with handling the system and the ingenuity of those who crafted the system:

There had been a fire in an electricity sub-station and I was without electricity during the day for almost a year. Again this meant going to somebody else's house [to send and receive encrypted messages] but this was not sustainable. Tim & Co configured the IT system to run off a car battery and he came to install. (Lucia interview, June 9, 2015)

Janet Love one of the first person to be brought in South Africa as part of Operation Vula in 1987 and who had already taken computer training talked about the ease of using automated encryption after having used hand-written cryptography for such a long time.

My role involved setting up infrastructure such as printing, distribution, dead letter boxes and safe houses. At that stage, although I had had initial training in using the computer program it had not yet been roll out, so in the very initial days I was based in South Africa we were still using non-electronic encryption, which was extremely laborious, but done nonetheless. When the computer program was roll out which would have been by the end of 87 it was a welcome relief. (Janet Interview, June 12, 2015).

One of the main challenges however experienced by operatives on the ground was about the time it took to send a message via the system. Even if the time was reduced from hand-written crypto to automated crypto, it could often take one hour to send a message. Janet Love recalls

The main challenge was to send encrypted data using normal telecommunication facilities. [...] Firstly it took a hell of a long time. [...] There is a particular sound, I am very bad at mimicry, but there is a particular sound, that the transmission of this data makes when it is finally going through, it is a kind of high pitched signal and to get to that point with the signal to actually go

through, was a sort of an incredible relief because it actually took so long. And part of the problem there was one could not presume to use any phones so I had to set up the possibility to use phones in various offices. Some I was using with the knowledge of the office owners others I had to find ways to get in without the knowledge of the owners. It was quite obtrusive if you can just imagine somebody seating at a phone with this equipment trying to get the data to communicate into the phone and often not happening, and finally having the data go through. That was a huge relief. (Janet Interview, June 12, 2015).

The Role of Women

The role of women in the anti-apartheid struggle has been paramount. "Of all freedom struggles, the longest and the most recently realized, that is South Africa, saw the most active intervention by women [...]" (Young 2001, p. 366). As early as 1920, the ANC had created a women's section and by 1949 an ANC women's league which would become banned in the 1960s. Women's active contribution against the apartheid regime has however been under-acknowledged in the writing of leaders of anti-colonial movement such as Neyrere, Nkrumua and Cabral. Feminist anti-colonial and post-colonial scholars have however been prolific in the past few years brining closer together STS, post-colonial scholarships and feminism (Harding 2011, 2008).

The struggle against apartheid in South Africa saw many women involved in a variety of roles and tasks. While a few numbers were MK commanders, more were involved in courier and communication related work (Cherry 2012, Cock 1993, Suttner 2007), work that was paramount for any operations. In a Dying Colonialism, Fanon (2011) highlights that women were performing tasks that were often impossible for men to perform as they attracted less attention. Though the main leaders of Operation Vula and those who crafted the communication system were men, many women came to operate and use the encrypted communication system and were thus crucial in its functioning.

Within Operation Vula there were more women there is no question about that. Including people who were MK commanders and trainers of units in Operation Vula. So there were more women occupying various roles within the Operation including people who were not from South Africa including people who actually did physical courier work including publication type material, money as well as ornaments. The gender composition in Operation Vula saw quite a number of women. It was less than 50% but there were a number of women in various capacities (Janet Interview, June 12, 2015).

This is reminiscent of the story of the ENIAC Girls who set up and operated the world's first electronic computer. At that time since programing was seen as a low level task it was seen as being perfect for women. In the Computer Boys Take Over, Ensmenger (2010) documents the history of computer programming and argue that at first the field was constituted of a largely feminized labor with a low status such as the ENIAC girls, which evolved as a field perfect for men and advertised as such. That's when and how the "computer boys" took over and the history of the ENIAC girls and their importance in developing the early field of programming got lost in the process. In today's hacking and encrypted context this is particularly informative as few women are involved in hacking and cryptography. As it has been well documented, the recent history of technology and its dominant narrative has been associated with masculine values (Cockburn, 1983, 1985; Wajcman, 1991, 2004). At the material level, this has been seen for instance in the percentage of women in computer science in the western world decreased significantly from 1980s onwards (reference ?). It ought to be mentioned though that in Asia, particularly Malaysia, this is a completely different story where such the work of programming that is happening within the private sphere is perfect for women (Mellström 2009). The latter example exemplifies a western bias with regards to gender and technology. Knowing about this particular feature of the encrypted communication network demonstrate that women were instrumental in its operation and use.

Conclusion

The encrypted communication network that was set up as part of the ANC endeavour to bring about an end to the apartheid regime in South Africa is a corner stone example of the use of hacking in an anti-colonial setting. I have argued that this example is part and parcel of the history of hacking. By shedding light to this history, the article helps to enlarge the goals, aspirations and political nature of cryptography and hacking. It also allow to give credit to a continent of the world, Africa that is often eclipsed from the limelight of technological innovation and hackerdom, but which rightly deserves it place. By shining light to this hidden chapter of history it creates solidarity between movements with different positionalities and contexts without suppressing the significant and important history of each of them.

Moreover, the desire to craft an autonomous and non-commercial encrypted infrastructure to bring about a sense or a feeling of autonomy and self-valorisation to a people is reminiscent of the work of

tech activists such as Riseup, Autistici/Inventati and Nadir tech collectives, among others. The encrypted communication network fits in the history of tech activism and should be recognised as such to open up the possibilities of thinking about the use of crypto and the assemblage of variant forms of technologies for liberation struggles. This is a powerful illustration of what I call anti-colonial hacking.

Bibliography:

Anderson, W. (2002). Introduction: Postcolonial Technoscience. *Social Studies of Science.* 32(5/6), 643-658.

Appadurai, A. (1996) *Modernity at Large: Cultural Dimensions of Globalization.* Minneapolis: U of Minnesota Press.

Bhabha, H. K. (2004). "Forward: Framing Fanon." In The Wretched of the Earth. By Frantz Fanon. Trans. Richard Philcox. New York: Grove Press.

Balsamo, A. (2011). Designing culture: the technological imagination at work. Durham, NC: Duke University Press.

Bowker, G. C. and Star, S. L. (2000). Sorting things Out: Classification and its Consequences. Cambridge, Mass.: The MIT Press.

Braam, C. (2004). Operation Vula. Bellevue, South Africa: Jacana

Bush, R. (1993). FidoNet: Technology, Tools, and History. Communications of the ACM - Special issue on internetworking, Volume 36 Issue 8, 31-35.

Deleuze, G. and Guattari, F. (1980). A Thousand Plateaus: Capitalism and Schizophrenia. Minneapolis, MN: University of Minnesota Press.

Cabral, A. (1969). *Revolution in Guinea: An African People's Struggle*. London, Stage 1.

Chan, A. (2014). Beyond Technological Fundamentalism: Peruvian Hack Labs and "Inter-technological" Education, Journal of Peer Production, 5.

Chatterton, P. (2010). Autonomy: The Struggle for Survival, Self-Management and the Common. Antipode Vol. 42 No. 4, pp 897-908.

Cherry. J (2012). Spear of the Nation: Umknonto weSizwe. Athends: Ohio University Press. Project Muse.

Cock, J. (1993). Women and war in South Africa. Cleveland : Pilgrim Press.

Cockburn, C. (1983). Male Dominance and Technological Change. London, UK: Pluto Press.

Cockburn, C. (1985). Machinery of Dominance: Women, Men and Technical Know-how. London, UK: Pluto Press.

Coleman, E. G. (Forthcoming 2015). Hackers. In *The Johns Hopkins Encyclopedia of Digital Textuality*. Marie-Laure Ryan and Lori Emerson, Benjamin Robertson (eds.). Baltimore: MD, Johns Hopkins University Press.

Coleman, E. G. (2012). Coding Freedom: The Ethics and Aesthetics of Hacking. Princeton University Press.

Coleman, E. G. (2012). Phreaks, Hackers, and Trolls and the Politics of Transgression and Spectacle. In

The Social Media Reader, ed. Michael Mandiberg. New York: NYU Press.

Coleman, E. G. & Golub, A. (2008) Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism. Anthropological Theory 8(3): 255-277.

Davis, S. R. (2009), 'The African National Congress, its Radio, its Allies and Exile', Journal of Southern African Studies , 35: 2, pp. 349–73.

Eckstein, L. and Schwarz, A. (Eds). (2014). Postcolonial Piracy: Media Distribution and Cultural Production in the Global South. London, UK: Bloomsbury Press.

Edmunds, M. (Producer). (2014). The Vula Connection. Documentary film.

Edwards, P. & Hecht, G. (2010) History and the Technopolitics of Identity: The Case of Apartheid South Africa, Journal of Southern African Studies, 36 (3), 619-639.

Fanon, F. (2011). L'an V de la révolution algérienne. La Decouverte Poche / Essais, N°340.

Fanon, F. (1964). Pour la Révolution africaine, Librairie François Maspero, coll. « Cahiers libres ».

Fanon, F. (1961). *Les Damnés de la Terre.* Paris: Éditions La Découverte.

Fanon, F. *(1952). Peau noire, masques blancs.* Paris: Seuil.

Feenberg, A. (1996). Alternative Modernity: The Technical Turn in Philosophy and Social Theory. Berkeley, CA: University of California Press.

Garrett, R. K. & Edwards, P. (2007). Revolutionary Secrets: Technology's Role in the South African Anti-Apartheid Movement. *Social Science Computer Review. 25 (1), 13-26.*

Haraway, D. 1988. 'Situated Knoweldges: The Science Question in Feminism and the Privilege of Partial Perspective' in Feminist Theory Reader: Local and Global Perspectives, 2nd edn, eds C McCann, & S Kim, Routledge, New York, pp.370-383.

Harding, S. (eds.). (2011). *The Postcolonial Science and Technology Studies Reader*. Durham, NC: Duke University Press.

Harding, S. (2008). *Sciences from Below: Feminisms, Postcolonialities, and Modernities***.** Durham, NC: Duke University Press.

Henderson, R. (1997). Operation Vula Against Apartheid. *International Journal of Intelligence and CounterIntelligence, 10(4), 418-455.*

Holland, H. (1989). The Struggle: A History of the African National Congress. London:UK, Grafton

Books.

Houstin and all (2013). The Liberation Struggle and Liberation Heritage Sites in South Africa. Democracy, Governance, and Service Delivery (DGSD) Human Sciences Research Council (HSRC).

Ippolita (2015). In the Facebook Aquarium: The Resistible Rise of Anarcho-Capitalism. Amsterdam, NL: Institute of Network Cultures. Retrieved from http://networkcultures.org/blog/publication/no-15-in-the-facebook-aquarium-the-resistible-rise-of-anarcho-capitalism-ippolita/

Irani, L., Vertesi, J., Dourish, P., Philip, K. and Grinter, R. (2010). *Postcolonial Computing*: A *Lens on Design and Development*. Proc. of CHI'10. ACM.

Jenkin, T. (1995). Talking To Vula: The Story of the Secret Underground Communications Network of Operation Vula. Retrieved from http://www.anc.org.za/show.php?id=4693

Jenkin, T. (1987). Escape from Pretoria, London : Kliptown Books.

Kaunda, K. D. (1982). Kaunda on Violence [1980]. London, Sphere Books.

Lekgoathi, S. P. (2010). The African National Congress's Radio Freedom and its audiences in apartheid South Africa, 1963-1991. *Journal of African Media Studies.* 2 (2), 139-153.

Levy, S. (2002). Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age. Penguin Books.

Lindtner, S. (2014) Hackerspaces and the Internet of Things in China: How makers are reinventing industrial production, innovation, and the self, China Information, 28(2), 145-167.

Mandela, N. (1995) *Long Walk to Freedom.* Back Bay Press.

Mandela, N. (1964). "Statement from the Dock at the Opening of the Defense Case in the Rivonia Trial," Pretoria Supreme Court, South Africa. Retrieved from http://www.anc.org.za/show.php?id=3430

Maharaj, Z. (2010). Dancing to a Different Rhythm: A Memoir. Cape Town, South Africa: Zebra Press.

Mellström, U. (2009). The Intersection of Gender, Race and Cultural Boundaries, or Why is Computer Science in Malaysia Dominated by Women? Social Studies of Science 39(6): 885–907

Mikelsons, A. (1992). Technical Report of the Global Networking Workshop. Retrieved from http://www.africa.upenn.edu/Global_Comm/Global_Networking.html

NARMIC/American Friends Service Committee. (1982). Automating Apartheid: U.S. Computer Exports to South Africa And the Arms Embargo, Philadelphia, Pennsylvania.

Nkrumah, K. (1973). *Revolutionary Path.* London, Panaf Books.

Nyerere, J. (1968). *Ujumaa: Essays on Socialiam*. Dar es Salaam, Oxford University Press.

Milan, S. (2013). Social Movements and Their Technologies: Wiring Social Change. London, UK: Palgrave Macmillan.

North, R. (Producer). (2012). Escape from Pretoria. National Geographic Channel Documentary. Retrieved from https://www.youtube.com/watch?v=0WyeAaYjlxE

Noble, D. F. (1983) "Present Tense Technology", *Democracy*, 3(2), 8-24.

O'Malley, P. (2007). Shades of Difference: Mac Maharaj and the Struggle for South Africa. Penguin Press.

Omura, J. (n.b.). Alternatives to RSA: Using Diffie-Hellman with DSS**.** Retrieved from http://www.di.unisa.it/~ads/corso-security/www/CORSO-9900/keyescrow/Alternatives%20to%20RSA%20Using%20Diffie-Hellman%20with%20DSS.htm

Press, R. (1995). To Change the World! Is reason Enough. Retrieved from

http://www.anc.org.za/show.php?id=11385

Ribeiro-Kabulu, A. (1996). Angola. p.27-30. In Sellström, T. (Ed) Liberation in Southern Africa—

Regional and Swedish Voices:. (2002). Nordiska Afrika institutet, Uppsala. Retrieved from

http://www.liberationafrica.se/publications/91-7106-500-8.pdf

Rodney, W. (2012). How Europe Underdeveloped Africa. Cape Town, SA : Pambazuka Press.

Rouvroy, A. & Berne, T. (2013) Gouvernementalité algorithmique et perspectives d'émancipation: Le disparate comme condition d'individuation par la relation ? Réseaux. 1 (177), 163 – 196.

Sahlins, M. (1995). How "Natives" Think: About Captain Cook, For Example.
Chicago: University of Chicago Press

Slovo, J. (1986).The Sabotage Campaign, Dawn, souvenir issue, p. 24.

Smith, A. (2015). Not Seeing: State Surveillance, Settler Colonialism and Gender Violence. In *Feminist Surveillance Studies.* Dubrofsky, R. and Magnet, S. (Eds.). Duke University Press.

Söderberg, J. (2008). Hacking capitalism : the free and open source software movement. New York, NY : Routledge.

Star, S. L. and Ruhleder, K. (1994). Steps Towards an Ecology of Infrastructure: Complex Problems in Design and Access for Large-Scale Collaborative Systems. In *Proceedings of the 1994 ACM Conference on Computer Supported Cooperative Work*, 253-264. CSCW 1994. New York, NY: ACM.

Suttner, R. (2007). Women in the ANC-led underground In *Women in South African History*, Ed. Gasa, N. Cape-Town, HSRC Press.

Suttner, R. (2008). The ANC Underground in South Africa to 1976: A Social and Historical Study, Johannesburg: Jacana Media.

Turner, F. (2006). From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism. Chicago, Il: The University of Chicago Press.

Young, R. J. C. (2001). Postcolonialism: An Historical Introduction. Oxford: Blackwell Publishing.

Wajcman, J. (1991). Feminism Confronts Technology. London, UK: Polity Press.

Wajcman, J. (2004). Technofeminism. London, UK: Polity Press.