Hacking Apartheid

Revolutionary Communication and the South African National Liberation Movement[1]

Sophie Toupin

Abstract

In the 1980s, South African freedom fighters created an encrypted communication system that allowed infiltrated activists on the ground to communicate secretly and transnationally with the senior leadership of the African National Congress (ANC) based in Lusaka, Zambia via London, UK. This encrypted communication system was set up as part of Operation Vula, an operation that aimed to launch a people's war and ultimately liberate South Africa from apartheid. While the successful deployment of an encrypted telematics system was remarkable at a time when the Internet as we know it today did not yet exist, the ANC already had a history of experimenting with and setting up different forms of communication systems. By mapping, documenting and elucidating the ways in which the encrypted communication system worked, this article explores one specific example of mediation via telematics technology in a liberation movement. Finally, I propose to explore this case study through the hacking apartheid concept, and ask how this concept enables us to think through hacking as a political, social and technical practice embedded in a national liberation movement.

Keywords: Hacking, Apartheid, Liberation Movements, Encryption, South Africa

It's early July 1990. The Durban Security Branch has just arrested two Umkhonto we Sizwe (MK)—the ANC's military wing—operatives in Durban, South Africa and found on them floppy disks containing a list of operatives' names, safe house locations and UK phone numbers, among many other things (Garrett & Edwards, 2007; Henderson, 1997; O'Malley, n.d.). By first arresting Mbuso Shabalala and Charles "Francis" Ndaba,[2]

1 I am grateful to Professor Darin Barney, Professor Gabriella Coleman and Professor Carry Rentschler for their generosity in advising me on the larger project associated with this article. This article is indebted to the freedom fighters who participated in Operation Vula and their allies. Finally, I would like to thank the peer reviewers for their feedback.

2 Shabalala and Ndaba were working underground for Operation Vula. After their arrest in

the Security Branch had accidently discovered Operation Vula and an encrypted communication system whose aim was to dismantle the white supremacist regime in place since 1948. The computer diskettes and UK phone numbers were part of a sophisticated encrypted communication network developed by exiled South Africans Tim Jenkin and Ronnie Press[3] who were part of the African National Congress (ANC) Technical Committee (TC). The system had been up and running for two years (Jenkin, 1995) and enabled freedom fighters who were part of Operation Vula to communicate secretly and transnationally mainly between South Africa and Lusaka, Zambia via London, UK. Other links were also set up in Amsterdam (Netherlands), Alberta (Canada), Harare (Zimbabwe) and Paris (France).

This article will focus on the technological communication ingenuity and inventiveness of the South African national liberation movement. Mapping and documenting the prototyping of a variety of communication technologies built in, and for, conditions of oppression and scarcity is significant. It counters the belief that African liberation movements were devoid of early sophisticated technological experimentation and highlights the role played by anti-apartheid freedom fighters—one of whom is associated with the contemporary hacker movement—in bringing about freedom in South Africa. This article attempts to contribute to the history of digital media and communication studies generally and more specifically to the history of revolutionary communication by reflecting upon the South African liberation movement's communication and technological practices. This will involve presenting a brief overview of some of the communication tools experimented with by the national liberation movement including by the African National Congress (ANC), Umkhonto we Sizwe (MK)—the military wing of the ANC—and the South African Communist Party (SACP). Highlighting some of these projects situates the development of the encrypted communication system within a wider history of communication and technological development.

I will then touch on the concept of *hacking apartheid* as a way of understanding the development and use of this encrypted communication system. I will ask how this concept enables us to think through hacking as a political, social and technical practice embedded in a national liberation movement. Finally, I will call for further study of the experimentation, development and/or use of communication and technological systems by liberation movements, particularly in Latin America, Asia and Africa. Because of the nature of underground communication and the danger in

July 1990, they both disappeared. During the Truth and Reconciliation Commission, it was revealed that both operatives had been murdered.

3 Press passed away in 2009.

revealing its existence when in operation, it is usually only in hindsight that such systems can be revealed and that concept work can emerge from empirical projects.

Methodology

This article is based on mixed-methods, including a study of academic articles, published and unpublished autobiographies of South African freedom fighters, South African newspaper clippings of when Operation Vula was discovered in July 1990, published and unpublished messages exchanged through the system, video documentaries, interviews and archival work. One important archive I have examined for this research is the O'Malley archive kept by the Nelson Mandela Centre of Memory. This archive is of particular interest as it contains documents related to Operation Vula and the encrypted communication system (ECS). It was set up by Professor Padraig O'Malley who, between 1985 and 2005, conducted interviews with many key personalities who played an important part in South Africa's political history. The University of the Witwatersrand Historical Papers research archive was also important for this research as it consists of a number of documents and newspaper clips related to Operation Vula. The unpublished autobiographies of both Ronnie Press and Tim Jenkin were relevant sources which shed light on concealment and experimentation practices using heterogeneous communication tools.

Moreover, I have conducted interviews with the former freedom fighters who developed, used or operated the system. I interviewed Tim Jenkin many times (face-to-face and virtually) and kept up regular email contact with him. I also interviewed Lucia Raadschelders who was tasked with receiving and sending messages through the encrypted communication system from Lusaka, Zambia as well as Janet Love who was one of the operatives infiltrated in South Africa and who used the system to convey strategic information back to Zambia via London. I also interviewed Sathyandranath Ragunana 'Mac' Maharaj, Operation Vula's commander, in Durban. It was Mac who requested the ANC TC to find a way for freedom fighters to contact each other safely in urban environments (Jenkin, 1995), initiating further experimentation with encryption and programming that would eventually lead to the encrypted communication system. Additionally, I interviewed Helen and Rob Douglas, a Canadian couple who set up safe houses for Vula and facilitated the ECS operation.

This article draws on a previously published article entitled Gesturing Towards "Anti-Colonial Hacking" and its Infrastructure (Toupin, 2016). Finally, as this article is part of a larger research project, further

interviews are being conducted in South Africa and more archival work is being examined in Cape Town, Durban, Johannesburg, Port Elizabeth and Pretoria.

A brief history of anti-apartheid technological experimentation

Operation Vula was launched in 1986 following decades of struggle that had failed to dismantle the oppressive white supremacist regime in place in South Africa since 1948 (Henderson, 1997; Motumi, 1994; Williams, 2000). The operation aimed to create the conditions for an armed insurrection—what was called a people's war. The aim of the operation was to facilitate direction of the struggle via the physical return of the ANC leadership to the country.

People's war was a frequent strategy among colonized or oppressed countries from the 1950s onwards in places such as Algeria, Cuba and Vietnam. In the context of South Africa, people's war was defined in the Green Book[4] as a "war in which a liberation army becomes rooted among the people who progressively participate actively in the armed struggle both politically and militarily, including the possibility of engaging in partial or general uprising" (O'Malley, 2008, p. 207).

As part of Operation Vula, an encrypted communication system was set up to facilitate secret and transnational communication within a small circle of people who were part of the national liberation movement. Vula—short for Vulindlela, meaning "open the road" in Zulu (Braam, 2004; Henderson, 1997)—was envisaged at a time when South Africa had seen increased levels of violence which many considered a context of near civil war (O'Malley, 2008). Operatives of the ANC, SACP and MK were routinely arrested, forced into exile, tortured and/or killed.

Prior to the setting up of the first functional version of the encrypted communication system as part of Operation Vula, the ANC, MK and SACP had a history of experimentation with different forms of concealment strategies and communication tools. In his unpublished autobiography, Jenkin (1992, p. 3) suggests that it was when the ANC was banned in the 1960 and many South African freedom fighters went into exile that "communication became a subject and practice in its own right." The ANC first set up an underground radio broadcast called Radio Freedom. While this underground radio station broadcast for a short while from South Africa,

4 The Green Book is also known as the Report of the Politico-Military Strategy Commission to the ANC National Executive Committee (ANC, 1979). It is in the Green Book that the concept of a people's war began to be part of ANC literature.

it soon stopped functioning when ANC leaders were arrested in the early 1960s. The radio broadcast resurfaced in 1969 in exile in Tanzania—where the Nyerere government gave it 15 minutes airtime per day—and in Zambia where the exiled ANC leaders were located, and then in other African countries (Mosia, Pinnock & Riddle, 1992).

When the ANC and other political formations were banned, cadres were sent to the Soviet Union and other destinations such as Cuba, East Germany and the Netherlands to learn radio engineering and methods of concealment, codes and cyphers (Jenkin, 1992; Mosia, Pinnock & Riddle, 1992; Naidoo, 2012). When they came back, cadres passed on their knowledge and trained those who needed it. Underground operatives sent to South Africa were soon cut off from the exiled leadership since transnational and secret communication using code books and invisible ink was very slow —it often took more than a month for a message to get through.

A less typical form of broadcasting was leaflet-bombs, which were used as a means to communicate revolutionary messages on printed leaflets—small detonators would launch pamphlets in the air in a crowded area—and were designed to wake South Africans up to the anti-apartheid cause (Edmunds, 2014; Jenkin, 1987). Primarily used in the 1970s, leaflet-bombs were meant to spread ANC material and news in a country where the ANC, MK and SACP and their messages were banned. Tim Jenkin (1987) was one of the main leaflet-bomb operatives, printing leaflets at night and "exploding" them in crowded areas during the day. Small detonations in public areas, and leaflets flying through the air, attracted attention, informed South Africans and defied apartheid censorship. However, after the Soweto uprising in 1976, Jenkin (1992, p.10) wrote that "it was our comms that prevented us from adapting to the new revolutionary situation and made us feel increasingly irrelevant." In referring to his leaflet bomb cell, Jenkin (1992) wrote: "Our incommunicado propaganda cell was like a factory without telephones to take the orders and operating in an environment without railways and roads to move the goods. Our hopelessly inadequate forms of contact were a rein holding us back." (p.10)

In 1978, Jenkin and his comrade were arrested for leaflet-bombs and sent to jail under terrorism charges. Before escaping by lock picking—it took Jenkin and two others one and a half years to craft a set of ten different wooden keys to escape—he returned to the ANC TC in London (Jenkin, 1987).

With his understanding of the challenges in the field, Jenkin joined the ANC technical committee with a mission to improve communications between the field and exiled leaderships. Jenkin and Press read books on programming and encryption, and went to technological trade fairs.

The appeal of using electronic communication technologies can be explained by the distance separating anti-apartheid activists across many countries, the exiled status of the ANC leadership, the high levels of counter-intelligence infiltration within the movement and the burdensome nature of hand-written cryptography. Moreover, another goal of the encrypted communication system was to have Nelson Mandela use it during the negotiations over his liberation in the late 1980s (Edmunds, 2014; O'Malley, 2008; Mandela, 1995). An earlier attempt to make secret contact with Mandela through another device—the radio pen—is described in Ronnie Press's (1995) auto-biography: "[In 1970], I was asked to make a radio receiver that could be smuggled to Nelson Mandela on Robben Island. At that time they were denied all communication with the outside world even newspapers. The idea was to have the receiver in a pen and have one of the Red Cross visitors get it to Nelson. It worked well. The pen was sent down to Lusaka where it was tested. [...] Unfortunately our contact could not pass it to Nelson and the project failed." (p. 27)

The above brief and incomplete overview shows that efforts to design an encrypted communication system were just part of a history of experimentation with different forms of communication devices by the South African national liberation movement. The technical committee and its members were instrumental in crafting communication and technological devices that would foster the anti-apartheid cause. Not only did they experiment with heterogeneous forms of technologies and communication devices to adjust to realities on the ground, but they also read articles and books about technology, and relied on the expertise of other exile South Africans to further develop their skills. I will now turn to explaining how the earlier version of the encrypted communication system worked.

The how to of sending an encrypted message[5]

Documenting how the ECS worked is significant since it reveals how the technical and human infrastructure needed for such a system to operate worked. Top level South African cadres and their allies —many were Dutch and Canadians—were infiltrated on the ground through Operation Vula and used the ECS to communicate secretly (see fig. 1 below). These cadres and their allies were generally trained by Tim Jenkin in London, UK or Lusaka, Zambia. The training covered how to use laptop computers — the first time for many— encryption programmes and basic digital and physical

5 This section describing how the encrypted communication system worked draws heavily on an article I published in 2016 in the open access Journal of Peer Production entitled Gesturing Towards "Anti-colonial Hacking" and Its Infrastructure (Toupin, 2016).

security. Part of the equipment, including the floppy diskettes on which the encrypted system was found, were covertly delivered by a Dutch KLM flight attendant who regularly flew from Amsterdam to Johannesburg and doubled as an anti-apartheid activist (Braam, 2004).

If operatives wanted to send messages using laptop computers in Johannesburg, they first needed to encipher it using the encryption program, and then pass it on through the computer's serial port to an acoustic coupler modem. This converted the digital data into sound, and allowed the audio stream to be captured on a small cassette tape recorder. Operatives then took the tape recorder to either a public telephone or located a telephone in an office building and dialled Tim Jenkin in London. Dialling Jenkin's number automatically recorded the message on his answering machine. If Jenkin was travelling, instructions would be given to dial Ronnie Press's backup number, also in London. Jenkin's and Press's flats were connected by an electronic Bulletin Board System (BBS) with a backup radio link. The tape recording was played through a small speaker into the telephone mouthpiece. Audio messages were stored on the London 'receive' answering machine and Jenkin (or Press) would then reverse the process, playing the received audio messages back through a similar acoustic modem attached to their computers, thus converting it back to a digital file which would be deciphered using a matching floppy diskette. Deciphered messages then appeared as plaintext on the computer screen, and could be printed for archiving, stored via another encryption programme or forwarded. The London operators would analyse each message to determine which items were to be passed on to Lusaka, which were for other destinations and which could be dealt with by ANC operatives based in London.

When messages needed to be sent to South Africa from London, the operatives who the messages were for would be paged by telephone and given a code indicating the number of messages they would be receiving. They would then go to a telephone and dial a different number in London, connected to a 'send' answering machine. The messages to be received were played as outgoing messages by the answering machine and recorded by operatives onto the same small cassette tape recorder by placing a special microphone on the phone earpiece. The recorded messages would then be taken home, where they could be played back into the laptop via the acoustic modem and deciphered as described above.

Initially, the arrangement in Lusaka worked in much the same way—only without the need for public telephones. An operative —Lucia, a Dutch woman, operated the Lusaka station for almost two years —she received enciphered messages, deciphered them, printed them out at her office and couriered them to ANC president Olivier Tambo and other senior

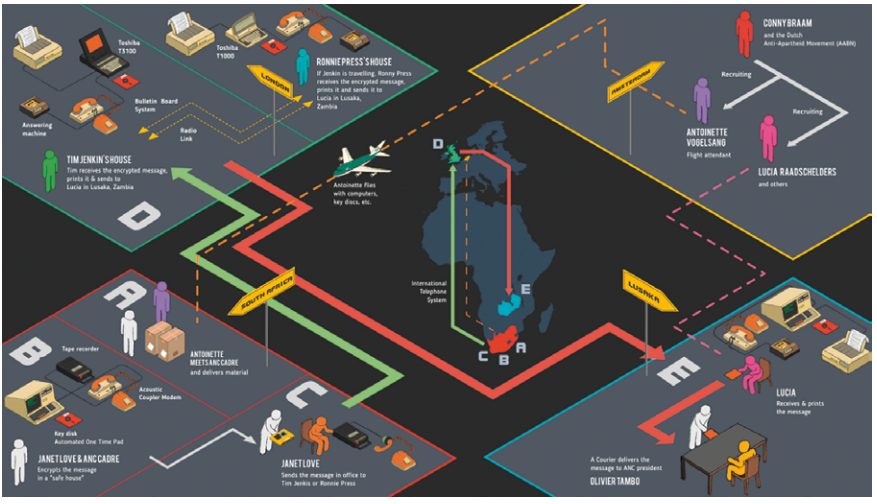

Fig. 1: Infographic: Ariel Acevedo and Sophie Toupin. CC BY-NC-SA. Simplified infographic showing how the encrypted communication system worked.

Operation Vula operatives. Outgoing messages from Zambia were likewise left on the London 'receive' answering machine. Later, a telematic set up in London allowed users to dial into a dedicated computer system used for both depositing and receiving messages.

The ECS was fully operational from July 1988 until June 1991. On the South African end, only a few top-level cadres involved in Operation Vula used the network directly, while other operatives performed more minor roles, such as preparing safe houses or relaying messages over public telephones. Other encrypted communication links facilitated contact with the Netherlands, Canada and other locations in the UK, among others. In July 1990, the ECS was accidentally discovered and, as a result, many of the Vula operatives in South Africa were arrested. This was the moment that the South African authorities became aware of the technological sophistication of the ECS designed by the ANC technical committee. After the bust, Jenkin changed the system's encryption keys—a move that enabled operations to continue for almost another whole year. When the arrested Operation Vula cadres were granted amnesties in June 1991 and negotiations with the South African government were at an advanced stage—Mandela had already been released—the ECS slowly wound down. Operation Vula had largely ceased and secret communication was no longer seen as a priority.

Hacking apartheid

The concept of *hacking apartheid* might help illuminate the practice described above, one which has largely been invisible in the history of hacker movements. In this short section, I will attempt to shed some light on this signifier or category and enquire into the extent to which this concept enables us to think through hacking as a practice in a national liberation movement. Also, I will link up this practice to another form of hacking which took place in South Africa, this time not 'hacking' the apartheid regime via the creation of an alternative infrastructure but attempting to disrupt the first democratic elections in 1994. Finally, I will touch on what this concept of hacking apartheid might accomplish.

In the 1970s and 1980s, the term "hacking" was not well known beyond a very specific circle. This does not mean, however, that the terminology may not be useful with the benefit of hindsight. Hacking can loosely be defined as a practice that involves tinkering shrewdly with a range of technologies. Gabriella Coleman (2014a, p.1) has defined a hacker as "a technologist with a penchant for computing and a hack is a clever technical solution arrived at through non-obvious means." While Tim Jenkin did not see himself as hacking during the Vula years, nor when he lock picked his way out of prison, he now identifies as a hacker, but a good one! Far from fearing technologies, hackers attempt to understand how they work for various purposes be they a hobbyist passion, technical curiosity or, in the case of the encrypted communication system, to evade state surveillance by building an alternative infrastructure and, ultimately, achieve liberation. This practice echoes the book Hacking Europe, where Caroline Nevejan and Alexander Badenoch (2014, p. 199) argue that "[b]y understanding rather than fearing the tools of computers, hackers could subvert the process by appropriating them for their own goals." Moreover, hacking apartheid resonates with the book Resistance, Liberation Technology and Human Rights in the Digital Age (Ziccardi, 2013) where hacking is understood as a form of liberation technology in the contemporary era and across countries. The ECS case study expands the repertoire of hacking as a liberation or revolutionary technology by showing how such practice was implemented in a situation of significant oppression during a struggle for emancipation.

While many politically oriented hackers in the West have tended to use hacking to uphold civil liberties such as free speech, privacy, and access (Coleman, 2014b), freedom fighters in South Africa used politically-oriented hacking practices to dismantle the white supremacist regime. They repurposed various forms of technology to organize transnationally and secretly, thereby attempting to evade the South African regime's surveillance apparatus. What they ended up building was an alternative

communication infrastructure, one of a number of responses to apartheid's technological infrastructure. For some time, the South African apartheid regime had been involved in technological infrastructural political projects designed to oppress, differentiate the country from other African nations and demonstrate its modernity. As a case in point, the regime set up a passbook system (Bowker & Star, 2000) which aimed to track down and fingerprint all non-white individuals. Only in the 1980s was fingerprinting extended to white people following a series of sabotage attacks on oil installations (SASOL plants in particular) by white members of MK (Breckenridge, 2014). The aim of the passbook system was "to stabilise a specifically racial personal identity around a document coupled with a biometrically indexed database" (Edwards & Hecht, 2010, p. 625), to control the movements of the black population. These techno-political projects were presented as examples of "industrial development"—a rhetoric that masked its underlying racial oppression (Hecht, 2012). All the while, the regime was at work developing and using computer systems to automate or computerize apartheid's processes (NARMIC/American Friends Service Committee, 1982; Komitee Zuidelijk Afrika, 1990).

The ANC technical committee's freedom fighters had much in common with social justice oriented hackers. Firstly, they shared a love of science and technology (Press, 1995). The drive to think with technology to find ways of fighting injustice is paramount for social justice oriented hackers. Secondly, the two main developers of the ECS were part of a socially privileged group of actors who were male, white and in exile in London when they developed the system. They used these privileges (whiteness, skills, know-how and access to technologies, among others) in their struggle for a better world. Thirdly, whether in the global North or South, hackers play a geopolitical role (Coleman, 2017). The threat represented at the geopolitical level by hackers is prevalent today. In South Africa, it can be illustrated by a US State Department cable sent from the American embassy in Pretoria to Washington in July 1990 when Operation Vula was discovered. The cable reads: "Despite Mandela's disclaimers, the available evidence shows that an ANC underground structure is operating in South Africa, that it is dominated by communist party members and that it is well-armed and well-organized. It is also computerized" (O'Malley, n.d., p.n.d.).

While a hacker group such as Telecomix[6] has much in common with Operation Vula's ECS, the context and conditions in which hacking was deployed in the anti-apartheid era differs. An apartheid-like situation is Palestinian resistance through hacking, including sabotaging Israeli web-

6 When the Mubarak Regime cut off access to the Internet in 2011, a group of hackers called Telecomix acted together with Egyptians and helped to circumvent the blockage (Dahlberg-Grundberg, 2016).

sites and circumventing censorship (Skare, 2016) which also has similarities with the ECS though it is more about disruption than building an alternative tech infrastructure. Using the concept of hacking apartheid is helpful when considering a communication and technical infrastructural response to the regime's oppression.

Looking at the practice of hacking within the national liberation movement builds on the wider ranging ideas of Jean Comaroff and John Comaroff (2012) in their book Theory for the South: Or, is Euro-America Evolving Toward Africa. In their book, they argue that it is the "Global South that affords privileged insights in the working of the world at large" (Comaroff & Comaroff, 2012, p. 1). Their argument not only shifts our centre of gravity toward the global South and Africa in particular, but also aims to highlight the fact that extreme forms of capitalism and (neo) colonialism have led to both frightening configurations and innovative counter political action.

The above case study highlights a type of hacking for national liberation whereas below I will briefly tell the story of a type of white supremacist hacking, which happened during the first democratic election in South Africa. Peter Harris (2011) documents this instance of hacking in Birth: The Conspiracy to Stop the '94 Election'. In this book, he tells the story of how right-wing hacker(s) attempted to break into the electronic counting system during the 1994 South African election. Before Harris and his team at the election commission discovered it, the hacker(s) successfully broke into the voting system to increase the votes of two white supremacist parties and one fierce ANC opponent— the National Party, the Freedom Front and the Inkatha Freedom Party. However, the election commission discovered the hack when it happened and thereby minimized its impact and ensured a democratic process. What this brief example illustrates is that computer hacking did exist in South Africa in the 80s and 90s, and it was used by people and movements to further their political vision both pro- and anti-colonialism, pro- and anti-fascism, pro- and anti-racism.

The final question I would like briefly to explore is what the concept of hacking apartheid can accomplish? Firstly, it enables us to understand hacking as performative; the setting up of a complex communication system with a clear anti-apartheid stance aiming at freedom and equality. The system configured particular forms of communication devices specifically for the purpose of facilitating emancipation at a time when liberation from apartheid seemed beyond reach. This was in stark contrast with both the right wing form of hacking exemplified above and the apartheid state which had initiated techno-political infrastructural "development" projects (such as mining, nuclear energy, a biometric system and other surveillance mechanisms).

The use of the word performative in this context is inspired by Judith Butler (2004) who, in her book Undoing Gender, gives the example of black South Africans under apartheid who turned up at polling stations to vote even if they did not have the right to do so. They performatively invoked the right to vote with no prior legal authorization (Butler, 2004). This, Butler argues, was an innovative practice of some value as part of a process whose aim was to create a less violent and exclusive future, a future that laid claim to universality and justice just as it sought to counter racism and violence (Butler, 2004).

Secondly, it allows hacking to be viewed as a highly political and intentional practice within a specific white supremacist context. When hackers design systems or disrupt or reinvent existing ones they have aims in mind. Stressing their agency is paramount, especially in view of the fact that the reasons behind their actions were that non-whites had long been denied such agency under apartheid. However, as crafty as hackers might be, we should not underestimate the confederation of human and non-human assemblage (Latour, 1991; Mitchell, 2002). Mitchell (2002, p. 34) reminds us that "human agency and intention are partial and incomplete products." No individuals really master all the elements, technological or otherwise, and the connections between them. This means that to understand how power works holistically, human agency and intentionality in and of themselves are insufficient.

The practice of hacking apartheid was deployed in a context of violence and injustice. It was one of a range of responses to an infrastructure of violence and injustice. Therefore it seems to have been ephemeral, coming and going as needed. While I use the term ephemeral here, I am not situating the practice of hacking apartheid as a heroic moment in the past and therefore ephemeral and vain, but rather considering it as embedded in past and present everyday forms of resistance. This view is informed by Frederick Cooper (2005, p. 25) who shies away from a disillusioned approach which reifies an understanding of an "atemporal modern colonialism." Understanding hacking apartheid in this way enables the concept to be supported and cultivated in the present.

The deployment of hacking apartheid is also different from state or corporate sponsored technologies whose purpose is frequently control, measurement and/or surveillance. In the case of South Africa, both Keith Breckenridge (2014) and Antina von Schnitzler (2016) have demonstrated how state sponsored technologies travelled from and even expanded out of the apartheid era into the democratic era. Both biometric registration systems and pre-paid meters for water or electricity consumption have been implemented. While it has been well documented that these techno-political systems have travelled from one era to the other, I wonder the extent to

which hacking against injustice has also travelled from the apartheid era into the democratic era in South Africa. While such practices do not seem to produce lasting techno-political infrastructures, the extent to which continuities in hacking practices from pre- to post-apartheid eras exists requires examination. At this particular juncture, what needs to be further examined is the relationship between current hacking practices in South Africa and the encrypted communication system developed during the national liberation movement. Are there perhaps forms of continuities (and discontinuities) with past and current hacking practices in South Africa?

Conclusion

This article highlighted some of the inventiveness of the South African national liberation movement from a communication perspective by exploring one main case study of the development and use of an encrypted communication network during the 1980s. It then examined the concept of hacking apartheid as a way with which to understand this system and touch on what this concept might mean.

This article makes a twofold contribution. Firstly, it recognizes that the South African national liberation movement was technologically sophisticated. It experimented with heterogeneous communication devices with the goal of securing and increasing the speed of communication between freedom fighters located across borders. What still needs to be examined, however, is whether this case study was a precursor within national liberation struggles. Or were other case studies of the development of alternative technological infrastructures using computer encrypted communication created by other national liberation movements? More work is needed to answer these questions. Secondly, this article builds on a previously published article (Toupin, 2016) and continues to explore the way in which this practice of designing an alternative technological infrastructure is linked to the history of the hacker movement and hacker practices.

References

African National Congress (1987). Apartheid South Africa: Colonialism of a Special Type. *ANC website*. Retrieved from www.anc.org.za/content/apartheid-south-africa-colonialism-special-type.

ANC (1979). The Green Book: Report of the Politico-Military Strategy Commission to the ANC National Executive Committee. *South African History Online (SAHO)*. Retrieved from www.sahistory.org.za/archive/

green-book-report-politico-military-strategy-commission-anc-national-executive-committee-aug.
Braam, C. (2004). *Operation Vula*. Johannesburg, SA: Jacana Press.
Bowker, G. C., & Star, S. L. (1999). *Sorting Things Out: Classification and its Consequences*. Cambridge, MA: MIT Press.
Breckenridge, K. (2014). *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*. New York, NY: Cambridge University Press.
Butler, J. (2004). *Undoing Gender*. New York, NY: Routledge.
Comaroff, J., & Comaroff, J. (2012). *Theory from the South: Or, How Euro-America is Evolving Toward Africa*. London, UK: Routledge.
Coleman, G. E. (2014a). Hackers. *The Johns Hopkins Encyclopedia of Digital Textuality*. Retrieved from http://gabriellacoleman.org/wp-content/uploads/2013/04/Coleman-Hacker-John-Hopkins-2013-Final.pdf.

Coleman, G. E. (2014b). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. New York, NY: Verso.
Coleman, G. E. (2017). From Internet Farming to Weapons of the Geek, *Current Anthropology* 58 (15), 91-102.
Cooper, F. (2005). *Colonialism in Question: Theory, Knowledge, History*. Berkeley, CA: University of California Press.
Dahlberg-Grundberg, M. (2016). Technology as movement: On hybrid organizational types and the mutual constitution of movement identity and technological infrastructure in digital activism. *Convergence* 22 (5), 524-42.
Edmunds, M. (2014). *The Vula Connection*. Johannesburg, SA: Sabido Production. Retrieved from www.youtube.com/watch?v=29vrvKsKXPI.
Edwards, P. N., & Hecht, G. (2010). History and the Technopolitics of Identity: The Case of Apartheid South Africa. *Journal of Southern African Studies* 36 (3), 619-39.
Garrett, R. K., & Edwards, P. N. (2007). Revolutionary Secrets: Technology's Role in the South African Anti-Apartheid Movement. *Social Science Computer Review* 25 (1), 13-26.
Harris, P. (2011). *Birth: The Conspiracy to Stop the '94 Election'*. Johannesburg, SA: Penguin Random House South Africa.
Hecht, G. (2012). *Being Nuclear: Africans and the Global Uranium Trade*. Cambridge, Mass: MIT Press.
Henderson, R. (1997). Operation Vula Against Apartheid. *International Journal of Intelligence and Counter Intelligence* 10 (4), 418-55.
Jenkin, T. (1987). *Escape from Pretoria*. London, UK: Kliptown Books.
Jenkin, T. (1992). *No Title*. Unpublished manuscript.
Jenkin, T. (1995). Talking To Vula: The Story of the Secret Underground

Communications Network of Operation Vula. *ANC website*. Retrieved from www.anc.org.za/content/talking-vula.

Komitee Zuidelijk Afrika. (1990). *Computerizing Apartheid: Export of Computer Hardware to South Africa*. Translated by Munaf, M., Olofsen, K., & Slob, G. Amsterdam, Netherlands: Holland Committee on Southern Africa.

Latour, B. (1991). *Nous n'avons jamais été moderne: Essai d'anthropologie symétrique*. Paris: La. Découverte, coll. L'armillaire.

Mandela, N. (1995). *Long Walk to Freedom: The Autobiography of Nelson Mandela*. London, UK: Abacus.

Mitchell, T. (2002). *Rule of Expert: Egypt, Techno-Politics, Modernity*. Berkeley, CA: University of California Press.

Mosia, L., Pinnock, D., & Riddle, C. (1992). Warring the Ether. *Review*, July. Retrieved from www.rjr.ru.ac.za/rjrpdf/rjr_no4/the_ether.pdf.

Motumi, T. (1994). Umkhonto We Sizwe: Structure, Training and Force Levels (1984-1994). *African Defence Review* 18. Retrieved from www.sahistory.org.za/archive/umkhonto-we-sizwe-structure-training-and-force-levels-1984-1994-tsepe-motumi.

Naidoo, N. (2012). The 'Indian Chap': Recollections of a South African Underground Trainee in Mao's China. *South African Historical Journal* 64 (3), 707-36.

NARMIC/American Friends Service Committee. (1982). *Automating Apartheid: U. S. Computer Exports to South Africa and the Arms Embargo*. Retrieved from http://psimg.jstor.org/fsi/img/pdf/t0/10.5555/al.sff.document.bmdv3_final.pdf.

Nevejan, C., & Badenoch, A. (2014). How Amsterdam Invented the Internet: European Networks of Significance, 1980-1999. In *Hacking Europe: From Computer Cultures to Demoscenes*. Alberts, G., & Oldenziel, R. (eds.) 179-205. London, UK: Springer.

O'Malley, P. (2008). *Shades of Difference: Mac Maharaj and the Struggle for South Africa*. New York, NY: Penguin Books.

O'Malley, P. (n.d.). The Heart of Hope: South Africa's Transition from Apartheid to Democracy. *Nelson Mandela Foundation's Centre of Memory and Dialogue*. Retrieved from https://omalley.nelsonmandela.org/omalley.

Press, R. (1995). To Change the World! Is Reason Enough ? Retrieved from www.sahistory.org.za/archive/change-world-reason-enough-london-august-1995.

Skare, E. (2016). *Digital Jihad: Palestinian Resistance in the Digital Era*. London, UK: Zed Books.

Toupin, S. (2016). Gesturing Towards 'Anti-Colonial Hacking' and Its Infrastructure. *The Journal of Peer Production*, 9. Retrieved from

http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/anti-colonial-hacking.

von Schnitzler, A. (2016). *Democracy's Infrastructure: Techno-Politics and Protest after Apartheid*. Princeton, NJ: Princeton University Press.

Williams, R. (2000). The Other Armies: A Brief Historical Overview of Umkhonto We Sizwe (MK), 1961-1994. *Military History Journal*, 11 (5), 173-85.

Ziccardi, G. (2013). *Resistance, Liberation Technology and Human Rights in the Digital Age*. New York, NY: Springer.

Sophie Toupin
is a PhD candidate at the Art History and Communication Studies Department at McGill University in Montréal, Quebec, Canada. This research was partly funded by the Social Sciences and Humanities Research Council of Canada. Sophie can be contacted at McGill University, 853 Rue Sherbrooke Ouest, Montréal, QC, H3A 0G5, Canada,
sophie.toupin@mail.mcgill.ca