

THE GLASS FORTRESS: ZIMBABWE'S CYBER-GUERRILLA WARFARE

Clapperton Mavhunga

Contrary to the gun battles we are accustomed to, we now have cyber-warfares fought from one's comfort zone, be it bedroom, office, swimming pool, etc., but with deadly effects.

—Dr. Olivier Muchena, Zimbabwe African National Union–Patriotic Front,
Secretary for Science and Technology¹

The Maxim gun and the Martini-Henry rifle ushered anglophone Africa into 20th century colonialism. The Cold War, in turn, presented a moment for black political elites to acquire weapons (the AK-47 in particular) with which to define and present themselves as African nationalists fighting—with all the material ramifications of this word—to end colonial rule. Could information technology—specifically radio, the Internet and cell phones—be the Martini-Henry, Maxim and AK-47 of the 21st century?

Zimbabwe offers an example of the way ordinary citizens in Africa are using these information technologies to express and demand genuine individual freedoms. Words and information are a kinetic process. To control words is to control mobility; when mobility is frozen, so too is information. This essay examines the technologies that enable and transform the mobility of words into weapons of resistance—by the state against its own citizens and by citizens against the state.

Using the lens of mobility of words (specifically those that contest state versions of truth and falsehood), this essay traverses the last ten years of newspaper, radio, computer, Internet, telephone and cellular technology in Zimbabwe. These technologies have enabled people to fortify their right to freedom of expression, to both minimize and maximize the value of their movements in search of better politics and to assemble resources and personnel to challenge the state. The state has responded with control mechanisms like surveillance, interception, physical

violence and propaganda. Twenty-first century information technology has enabled individual citizens to become cyber-guerrillas, using their smart phones, laptops, and desktops to perforate the fortress of a ruler still caught up in the 20th century from their own homes, vehicles, rural villages, in the country or in the Zimbabwean diaspora.

Technologies have enabled people to fortify the freedom of expression, to adjust movements in search of better politics and to assemble resources and personnel to challenge the state.

Zimbabwean users have designed a new use for technologies of communication:

to address the question of liberation and the tension between national freedom and personal freedom. The Internet, e-mail and radio waves have become instruments to challenge the late 20th century metanarrative of the so-called father figure who built the nation—that big man of courage who liberated his people—that anchors the dominant state-centric idea of Africa.² This status entitles him to rule the people permanently and rapaciously, whether they want him to or not—hence Zimbabwean President Robert Mugabe’s proprietary (as opposed to patriotic) declaration that “Zimbabwe is mine.”³ It gives the fullest meaning to his rebuff to then British Prime Minister Tony Blair: “Keep your England and let me keep my Zimbabwe.”⁴

According to Giorgio Agamben, the “fighting” and “loss of blood,” the stuff that “liberating” is made of, was supposed to be a process of profanation—sacrificing or spilling blood to cleanse the country of the demon of white privilege so that the ordinary black person could decide on his or her government. Guns were supposed to clear the path to allow the pen or ballot to govern. Instead, the opposite happened in many African countries, including Zimbabwe. Many leaders of liberation struggles, once in power, used the sacrifice of spilled blood to elevate themselves to the status of gods.⁵ The media—television, radio and newspapers—was used as a personal, party and state instrument for this transformation. In many states, a strict censorship system was installed to barricade any counternarrative—to filter what was heard, silence what might be said, and if necessary, shut the ears of those who might hear.

Interestingly, the pervasive power of the Internet and its use as an instrument of profanation—as an instrument to challenge the metanarrative of leaders who sacrifice their citizens and exploit the history of liberation for self-deification—mimics the dual capacity of the AK-47 to both install and challenge power. Yet there is one problem for these self-anointed gods: They cannot suppress the reality that the “liberated” people they dominate are not free.

While some Pan-Africanist scholars were busy using Mugabe to write a race-based narrative of liberation, the Zimbabwean people were writing their own narratives of liberation through their experience of the hardness of life. From the standpoint of these two “social imaginaries,” Mugabe, Zimbabwe and liberation did not look, let alone feel, the same.⁶ Yet the state and its defenders insist on one version of truth.

TRUTH AS FALSEHOOD AND FALSEHOOD AS TRUTH

Mugabe adopted heavy-handed Cold War tactics to confront the new challenges of the 21st century mobility of words. He lived in a rhetorical world where African countries could only be pro-West or pro-Soviet. The irony is that his lifestyle and lifetime mimicked that of the West—his eloquence in the English language, his designer suits, his wife’s love for shopping, the Mercedes-Benz luxury cars and the colonial-era festivities for the opening of Parliament. Mugabe detested only one thing about the West: calls for democratic governance. Otherwise the West was his quiver, carrying a deadly rhetorical arrow—the much fabled but ultimately false claim that it was the British who postponed the resolution of the land question.

For Mugabe, the so-called truth (in Shona, *chokwadi*) was not merely “If I am right, you are lying,” but something that must not be false or someone will die. Supposed falsehood (*manyepo*) was something that was ontologically true, but which must be false or else. To kill the mobility of falsehoods or dangerous information, the state sealed off the countryside using roadblocks and militia bases. To open what was sealed was called “terrorism.” Reporting, or criticism, became aggressive combat.⁷ The witnessing and feeling of violence by the Zimbabwe African National Union-Patriotic Front (ZANU-PF) transformed the fight of the main opposition party, the Movement for Democratic Change (MDC), into a battle for liberation.

The state broadcaster Zimbabwe Broadcasting Corporation (ZBC), and the state newspaper stable Zimbabwe Newspapers (Zimpapers), specifically the *Herald* and *Sunday Mail*, were trusted with ensuring that only approved information was filtered to the public. Photographs became instruments for distortion and amplification of the state’s supposed truth. The state photographer and editor skillfully juggled the zoom lens, producing close-up pictures to capture the odd white person or so in a sea of black faces. Through this process, MDC leader Morgan Tsvangirai’s big rallies appeared as no more than a meeting of a handful of aggrieved, racist white farmers and confused black puppets—possibly the white farmer’s workers who feared losing their jobs if they did not follow their boss.⁸ On other occasions, Tsvangirai simply looked as if he was talking to himself. By contrast, ZBC cameras shot ZANU-PF and Mugabe’s rallies from a distance so

that the small crowd filled the lens, creating the impression of a multitude spread over a large area.

The state also sought to control the production and mobility of information. So-called independent newspapers with ZANU-PF sympathies mushroomed, publishing “thinly-disguised political puff-pieces.”⁹ Something similar happened in South Africa during the apartheid era; in Russia this is common as well. The state even wanted to control “regional truth” about Zimbabwe and defeat what it considered the reactionary falsehoods of South African weeklies like the *Sunday Times* and *Mail & Guardian*.¹⁰

MOBILITY: A DEMOCRATIC OPTION

Many Africans do not think that Mugabe’s longevity in power lies in his own strength or calculations. These critics see the *absence of physical confrontation* as evidence that Mugabe is not resisted. They believe that either Zimbabweans are docile, or they are cowards expecting the world to come and liberate them while they do nothing.¹¹

My interest lies in the subtle resistance of exercising democracy within an undemocratic space. Specifically, I examine the option of voting with one’s feet when the ballot has failed. This process involves using mobility to recuse one’s body and mind from an environment of political abuse and relocate it to a place that respects one’s right to exist. This is a case where some would choose to relocate and keep up with the 21st century rather than follow Mugabe on his determined retreat into the Stone Age.¹²

Emigration has been a crippling brain drain on Zimbabwe. Unwilling to critique itself as the culpable brain-drainer, the state accused the Anglophone West—principally the UK, the United States, Canada, Australia and New Zealand—of skill theft. This conceited, self-important register of entitlement located the emigrating body within a larger scheme of the UK’s other alleged thefts, such as land. The mobile body carried no mind or self-interest, only the state’s need.

Migrating out of reach was a function of the mobility of words. Most emigrants discovered, enquired about and secured opportunities via the Internet, telephone and fax, and traveled by foot, automobile and airplane to claim them. In 2001, overseas companies realized the man-made implosion in Zimbabwe offered an opportunity to scavenge for unappreciated skill. Headhunters descended from the anglophone West looking for nurses, doctors, artisans, teachers and lawyers.¹³ Mostly, though, citizens themselves sought and pursued their own opportunities. Zimbabweans could now travel overseas where their ancestors could not through two mobilities: transportation and communication. The co-construction of technological capabilities and human agency is worth probing.

WEAPONIZING THE AIRWAVES

On 4 October 2000, Mugabe issued a decree setting up the Broadcasting Authority of Zimbabwe (BAZ). This body was charged with the power to license or de-register journalists and broadcast media houses and to regulate the airwaves for six months. Before the decree expired, Information Minister Jonathan Moyo pushed the Broadcasting Services Act into law, backdating its effect to cover the period of the decree. This act also turned the BAZ into a legal body. Shortly afterward, in 2001, the act was passed, creating the state-controlled broadcaster, the Zimbabwe Broadcasting Corporation, which gained a monopoly over the airwaves. The station was unbundled into two successor companies so that the broadcasting and signal transmission services would be able to compete—against nobody. This 2001 act also mandated that only citizens of Zimbabwe permanently resident in the country could broadcast or fund broadcasting stations. If any Zimbabwean received even a penny from outside of the country, he would disqualify himself as a broadcaster. Freedom of association had been limited as well. Because resources for free expression might be derived from associating with people who have financial means, the act also curtailed freedom of expression.¹⁴

The act also mandated that 70 to 80 percent of a station's programming contain local content.¹⁵ The few programs that made pretensions towards objective coverage were closed down. The most balanced of these were "Talk to the Nation" and "Spotlight," which were both banned after allowing the public to freely air their views.¹⁶ When Zimbabwe Broadcasting Corporation (ZBC) journalists disagreed with the party line, or did not display their enthusiasm more loudly, they were kicked out. One of them was Geraldine Jackson, fired for taking irate phone calls from the public protesting the violent crushing of the 1997 food riots.¹⁷ Determined to continue giving such voices of dissonance a platform, she set up an independent station called Capital Radio. It was promptly shut down, despite having secured a broadcasting license. In 2001, Jackson established SW Radio Africa in London with a few of her former ZBC colleagues.¹⁸

It had an inauspicious start in a cramped radio studio in the London suburb of Borehamwood. It was the sort of place to find a new guerrilla that used the microphone as a weapon, with airwaves for bullets and hitting its target by outflanking and sneaking into the state frequency monopoly via short wave. London was the perfect place to locate SW Radio because of kinship networks, easy air transport and asylum privileges, all a material legacy of British colonial geographies. An estimated half-million Zimbabweans lived in the UK, over half of them illegally. SW Radio Africa started broadcasting on 19 December 2001 via short-wave and on the Internet. Banning the journalists from entering Zimbabwe made no difference—their voices were entering the country at will every night and engaging in conversa-

tion with individual homes through the Internet and shortwave.

SW Radio's *modus operandi* was smart. Listeners based inside Zimbabwe e-mailed in their phone numbers or called and asked the station to call back for one-on-one or conference calls. It relieved listeners of the financial burden of calling the station and transformed ordinary people in the war zone into journalists. The exact location of the station remained secret for security reasons and pseudonyms became the camouflage uniform of the airwave for callers afraid to reveal their identities.¹⁹ The government of Zimbabwe vehemently protested what it claimed was British-sponsored pirate radio.²⁰ London dismissed the claims, maintaining that Zimbabweans resident in the UK were operating the station independently.²¹

The city of Harare's defense lay in blocking the SW Radio's signal. In early March 2005, the station announced that its broadcasts into Zimbabwe had been jammed.²² BBC Monitoring confirmed "the presence of deliberate jamming on all three broadcasts."²³ Some media reports claimed that the interfering signals had originated from Chinese-made equipment.²⁴ Others claimed that the state had invested more than \$50 million in the installation of two Chinese-built transmitters at Gweru-Thornhill Air Base to block their broadcasts into Zimbabwe.²⁵

The strategy of alternating between three frequencies failed in the face of this attack. It was time for an expensive plan: The station's Web site announced that SW Radio would simultaneously broadcast on three short-wave frequencies, as well as a medium-wave frequency.²⁶ This innovative tactic to overcome the government's two jamming devices came at a high price.²⁷ In May 2005, SW Radio announced that it was in deep financial crisis and was ceasing airing on short-wave, leaving the station with just its Web cast and a medium-wave broadcast.²⁸

The stakes were high: If SW Radio closed, a vital hub of political discourse would be eliminated. The station was host to a convergence of multiple communication modes—Internet, cell phones, fixed lines and shortwave—that connected the diaspora and those at home in one political conversation. In June 2005, the station announced it was no longer closing, thanks to a generous cash injection that would enable transmission for at least twelve more months.²⁹ SW Radio grew in strength in subsequent months.³⁰

Jamming SW Radio transmission was only one form of defense for Mugabe's government. In the summer of 2008, the government embarked on another form of interception: denying listeners the means to receive the signal. As suburbanites turned to satellite television signals to outflank ZBC-TV propaganda, the state undertook *Operation Dzikisai Madhishi* (Take Down Dishes).³¹ Yet Zimbabweans still found ways to listen to these programs.

Acknowledging the futility of physically stopping signals, the state joined in to send its own. This was the genesis of the "Voice of Zimbabwe" a 24-hour short-

wave service to export the government's message to the diaspora and to counter the signal from outside. In May 2007, however, reports surfaced that plans to begin broadcasting that month had been cancelled.³² Mugabe's regime also struck a deal with a Canadian broadcasting firm, JumpTV, to stream its ZBC-TV mouth-piece live on the Internet beginning 22 June 2007. Initially, the station offered the service free to registered users, but began charging a monthly fee as of 15 July.³³

CYBER-GUERRILLAS

SW Radio and Voice of America broadcast only for a few hours each day on short-wave and medium wave, streaming podcasts to stay within their budgets. These constraints led to the innovation of Internet radio. The defining moment for these technological convergences was September 2004, when a group of disc jockeys, many of them purged from Zimbabwean stations and living in exile in the UK, started a twenty-four hour Internet radio station in London. Afro-Sounds FM's mission was to "entertain and inform," to fill the void the closure of the independent print and electronic media had left in Zimbabwe.³⁴ Only this was no longer just entertainment; broadcasting—streaming—was now a cyber-weapon, enabling the physical bodies dispersed by the Zimbabwean government to remain safely behind the firewall of exile while their minds and voices went back through the medium of the Internet and airwave to insist on challenging the official so-called truth.

Once the idea of Internet radio and online newspapers caught fire, the flames raged out of control. That same year another station called Zimnet Radio began twenty-four-hour, seven-days-a-week live streaming, with volunteer DJs located in private homes in North America, the UK, Egypt and South Africa working in shifts so that audiences located in different time zones could make live phone-in and musical requests. Listeners tuned in via the Zim Daily Web site, clicked the Zimnet Radio link, and upon reaching it logged into the chat room and discussion forums to meet the cyber-family. Over time Zimnet Radio has become perhaps the most popular live phone-in, music and news combination online.

Exiled musicians whose music was banned on ZBC also took Internet radio in new directions, hooking their guitars and microphones into their computers and turning them into a potent combination of cyber-assault weaponry against the Mugabe regime. For example, on 18 April 2008 Canadian-based music critic Viomak created Voices of the Oppressed (VOTO), a radio station dedicated to protest music, messages and news. There is nothing new here—guerrillas who fought with a microphone were a decisive factor in mobilizing the morale of the guerrillas fighting with AK-47s in the 1970s.³⁵ All one needs is a computer, Internet, software, a Web site and a headset. It is both bone-chilling and liberating.

E-NEWSPAPERS: FUSIONS OF PRINT AND ELECTRONIC

Strive Masiyiwa was the man who brought the Internet to Zimbabwe. A British-educated, former employee of the state-owned Posts and Telecommunications Corporation (PTC), Masiyiwa established Econet Wireless (Pvt) Ltd. in 1994. The state initially refused to grant him a license, but in 1997 the Supreme Court cleared the way for the company to provide wireless service, and it began operating in July 1998.³⁶

Masiyiwa would become the majority shareholder in Associated Newspapers of Zimbabwe (ANZ), publisher of post-independence Zimbabwe's most successful independent paper, the *Daily News*.³⁷ Masiyiwa was also rumored to be one of the chief financiers of Zimbabwe's main opposition party, the Movement for Democratic Change (MDC), led by Morgan Tsvangirai. His association with two projects of rhetorically and materially undoing the "truth of liberation" made Masiyiwa an obvious target for the government.³⁸

On material value alone, the cell phone (and, increasingly, the type of cell phone) and Internet became the credentials of one's modernity. That fueled Econet's expansion. The wireless network recycled old buses and abandoned trailers into public phone, fax and Internet cafés. It offered trendy new services like local news, CNN and BBC World News Service reports through mobile phones. In a 2002 partnership with its Internet arm Ecoweb, Econet offered the first mobile information service in Zimbabwe. Thanks to these innovations, Econet out-competed its adversaries, Telecel and state-owned Net One.³⁹

The fusion of the Internet and newspapers came with Econet. For most of its history before Zimbabwean authorities ordered the newspaper closed in September 2003, the *Daily News* Web site was based in Zimbabwe. In June 2003, it relocated out of the country to a new home in South Africa hosted by Ecoweb International, the global Internet arm of Masiyiwa's Econet.⁴⁰ As the newspaper's editors in exile wrote that those who drafted the country's media laws had not considered "the technological advancement that enable[d] publishers to reach their audiences from beyond the physical boundaries of Zimbabwe."⁴¹ That was the kind of camouflage the cyber-guerrillas needed.

To be fair, the *Daily News* was not the first Zimbabwean online newspaper—that is to say, a newspaper based primarily in cyberspace, rather than a print publication with a Web site. This genre had already begun in March 2000, when displaced white farmers established cellular hotlines and then Internet listservs to monitor the movements of land invaders and look out for each other as the violence spread.⁴² One such website was ZWNews.com, itself an amalgamation of sites including the farmers' information network ZimNews, established in May 2001. The new site would be a "one-stop shop" for extensive news coverage and a daily

e-mail service with news alerts.⁴³

In July 2004, several exiled journalists and non-media professionals teamed up to start an independent political Web site called Zimdaily.com. The owners hid behind the firewall of anonymity to attack the regime without fear of physical retribution. The paper was edited in Canada, published in England and hosted on a Web site owned and run by WorldOnCall Corporation, a company owned by expatriate Zimbabweans. Within its first two weeks the site claimed to have received 100,000 hits.⁴⁴ Zimdaily is best known for Fair Deal, an online project started in April 2007 to identify children (and spouses) of ZANU-PF officials living abroad and get them deported from Western countries.

Additional online news sources include New Zimbabwe.com and the *Zimbabwe Times*. New Zimbabwe.com was the brainchild of ex-*Daily News* reporter Mduduzi Mathuthu, who was arrested in Zimbabwe on at least three occasions before deciding to migrate out of reach.⁴⁵ Arriving in UK, he filed for the *Daily News* while plotting the establishment of his own online paper. In 2004, Mathuthu started New Zimbabwe.com. Similarly, in October 2006, Geoffrey Nyarota, former editor-in-chief of the *Daily News*, established the *Zimbabwe Times* targeting the diaspora and people in Zimbabwe with Internet access. Although the paper's material status might have changed, The *Daily News*' principle of telling it like it is remained a major selling point. Over time, Nyarota's new news outlet attracted serious public intellectuals not necessarily aligned to the MDC, but committed to freedom, plurality and a belief that democracy is only as good as people's participation.

In all their various shades, online newspapers have distinguished themselves as a cyber-reconfiguration of what Jürgen Habermas called "the public sphere."⁴⁶ Of course, the state could not—and would not—just watch in astonishment.

SNOOPING

As early as 2000, the MDC's Manchester (UK) branch reported that state security agents using diplomatic passports were entering the UK to force exiles into silence by wiretapping phone calls, faxes and e-mails going to and from Zimbabwe. At least two police stations recorded complaints about surveillance.⁴⁷ The surveillance of communications between home and the diaspora also took place at Zimpost, the state postal service, where state security personnel reportedly intercepted international mail and cargo destined for Harare.⁴⁸

E-mail also became a vehicle to deliver viral payload to enemies of the state. In late July 2001, a computer virus struck hundreds of unsuspecting e-mail subscribers, including many at the *Daily News*. The paper's e-mail address was flooded with hundreds of messages infected with a bug that stole or destroyed documents on user hard drives. Subscribers' mail and private information were stolen and

circulated, with the victims as varied as businesses and academic institutions. The Internet service provider (ISP) Zimbabwe Online (ZOL) reported that its anti-virus software was intercepting seven viruses per minute.⁴⁹ While ISPs tried to assuage fears of snooping, there was no way for them to stop the state's interference. Sections 98 and 103 of the Postal and Telecommunications Act (PTA) of 2000 mandated that ISPs allow government intervention. To escape the interceptors, NGOs were switching to international e-mail platforms or limiting the kind of information that they passed through e-mail. ISPs were under no obligation to divulge to subscribers whether or not they had received a state directive to intercept. They went about this work quietly while denying any knowledge of monitoring e-mail for political or criminal reasons.⁵⁰ Not long afterwards, state media reported that police arrested fourteen people for "circulating a subversive e-mail inciting the public to oust President Mugabe from office." The e-mail in question allegedly referred to violent demonstrations to remove the president. The suspects were later freed on bail.⁵¹ It was now common knowledge that the state had been snooping on people's communication.

In February 2006, the Interception of Communications Bill, first introduced as an amendment to the PTA, was modified and re-tabled to legalize the snooping.⁵² The bill was meant to set up an interception center and designate technical experts to operate it. The chief of defense intelligence, director-general of the Central Intelligence Organization, the police and the commissioner-general of the Zimbabwe Revenue Authority would be empowered to authorize these investigations. The minister would issue a three-year "interception warrant to authorized persons" if he found reasonable grounds of any offense or "threat to safety or national security." The warrant would specify the name and address of the target of interception. The impounded information would be disclosed on a need-to-know basis and would be acceptable as evidence in a court of law.⁵³

The ISPs would "install hardware and software facilities and devices to enable interception of communications" and the creation of a data bank of "communication-related information" at their own cost. The terms of reimbursement for aiding the state in snooping were very vague: The ISPs would be "assisted or compensated for the assistance...to the Authority or the monitoring centre."⁵⁴

The bill vested the disclosure of intercepted information only in the authorized persons, who would "destroy [it] as soon as possible after use." The authorized person had power to seize any postal article at his discretion. The aggrieved could appeal to the minister to "confirm, vary or set aside the decision." If unsatisfied, he or she was free to appeal to the Administrative Court. The minister also had power to make regulations to implement the interception law "in his opinion."⁵⁵

The power of the interception bill lay in its capacity to obscure. It was ambig-

uous which agency was authorized to snoop and which facility would be used. The minister did not need to ascertain, independently or through further explanation, that the interception would aid the investigation, prove or prevent the said crime. The law gave the minister carte blanche to act in the name of “national security.” The bill rendered ISPs complicit in the state’s infringement of the Bill of Rights. They were required to spy on their own customers, and pass incriminating information along to the secret service. They would also be compensated for sacrificing the privacy of their clients—who were, quite literally, paying to be spied upon.⁵⁶ Moreover, mechanisms intended to preserve people’s right to privacy became the very keys which the state now used to violate it. The bill required holders of encryption keys to decipher not just intercepts, but any information the “authorized person” deemed to be “in the interests of national security or the economic interests of Zimbabwe, or to prevent or detect a serious offence.” The key-holder would be paid for disclosing such information.⁵⁷

In June 2007, ZANU-PF used its parliamentary majority to pass the bill into law, leaving only the small issue of Mugabe’s signature. Even before the ink had dried on Mugabe’s signature on the Interception of Communications Act in August 2007, there were unconfirmed reports that Chinese-trained technical experts had deployed at Mazoe Earth Satellite station, the country’s gateway to Intelsat, the world’s largest commercial satellite communications services provider. It was there that some believed the government was planning to set up a telecommunications monitoring station, as envisaged by the legislation. While the effectiveness of such a facility was open to question, the real intention was to instill and rule by fear.⁵⁸

HACKTIVISM

Hacktivism is a term used to denote activism by hacking. In September 2001, hackers got into the Reserve Bank of Zimbabwe (RBZ) Web site and diverted some of its links to pornographic material. In early August 2002, they got in again, this time leaving a message calling for the liberation of Palestine on the site. Information technology experts warned that the security of the country’s financial system was too lax.⁵⁹

In 2005, hackers vandalized the government Web site. A person claiming to be one of the hackers later contacted the staff of New Zimbabwe.com, based in Leicester, England, to tell them about the breach: “The idea was to hack into the site and replace everything there with slogans like ‘Robert Mugabe is a tyrant’.... We were about to achieve our goal when the whole thing crashed.... We will keep trying—the security is clearly lax.”⁶⁰ The hacker found it ironic that the regime had used public funds to install cyber-offensive weaponry, while leaving its own databases virtually defenseless against counter-attack.

On 10 May 2008, a hacker using the name r4b00f gained access to the state-owned *Herald* website for three days. Only the next Monday did staffers formally admit the intrusion. The hacker had replaced all headlines with the word *Gukurahundi*—the name of a bloody campaign ordered by Mugabe, which left 20,000 supporters of his rival, Joshua Nkomo, dead.⁶¹

Five days after the *Herald* hacking, r4b00f attacked the *Financial Gazette* Web site using the same tactics, this time posting the words “Mugabe Must Go! Free Zim” and redirecting visitors to the Web site of the civic action group Sokwanele. *IT Business Edge* magazine summed up r4b00f’s *modus operandi* as “just another example of *hacktivism*.”⁶²


The hacker’s most important advantage was the ability to attack without being seen. The hacker knew where the government could be found, yet the government could not find the hacker. Nevertheless, the opposition was itself not immune from cyber-attacks. On 9 June, malicious software was found on the MDC Web site. A Google search of the words “Movement for Democratic Change” returned a warning that the Web site was a suspicious site and could harm one’s computer.⁶³ The malicious software disabled visitors’ computers by forcing them to run multiple programs at once. The malicious code had only been tagged onto one of the Web site’s sixty-three pages and was actually hosted on the Chinese-based servers killpp.cn and nihaol12.com. An analysis of the site suggested that this was the work of hackers.⁶⁴

The *Zimbabwe Times* site was next. On Tuesday, 15 July 2008, it came under severe Denial of Service (DOS) attacks. After yet another cyber-attack, the site took extra measures to fortify its security, telling readers it believed that the hackers’ aim had been to disrupt news and information distribution and comments from readers.⁶⁵

CONCLUSION: CYBER-CONUNDRUMS

Cyber-guerrillas have proved elusive, communicating via secure e-mail and free platforms like Hushmail, S-Mail.com and KeptPrivate.com. Government monitoring equipment has affected public Internet cafés that use unsecured e-mail, but guerrillas have taken cover by installing anonymizing software to shield their identity from snooping.⁶⁶ These electronic insurgents have switched to platforms like Yahoo, Hotmail and Gmail since they use remote servers in the UK or the United States.⁶⁷ They have bypassed the filters using proxies capable of hiding their actual IP address. They visit Web sites that are not blocked, and from there leapfrog onto blocked ones, or they send instant messages with Skype, MSN or Yahoo Messenger, which the state’s filters cannot read without the user’s password.⁶⁸

With the Internet, the state now lives in a glass fortress, behind a weak

firewall permeable to hackers. The cyber-guerrillas can see the state clearly; the state cannot see them. Those who live in glass fortress cannot throw stones, not just because they have no armor, but because they cannot find their enemies. Such mobilities, manipulations of space and weaponizations of the Internet and airwaves into unobvious weapons of democracy should force us to think deeply about the implications of these instruments once the purpose of ending Mugabe's absolute powers is achieved. To what purpose will they be reassigned? On a global scale, they must prompt us to think ahead about this new century that is set to be dominated by virtual communication technologies. 

NOTES

* This article is a revised and expanded version of a piece published in the Association of Concerned Africa Scholars Bulletin No. 80 Special Issue on Zimbabwe 2 (Winter 2008).

¹ Lance Guma, "Mugabe regime draws up list of blacklisted websites," SW Radio, 10 August 2007.

² For a "big man" version of Africa, see John Iliffe, *Honour in African History* (New York: Cambridge University Press, 2004). For a refreshing critique that challenges the hegemonic narrative of masculinity, see Kizito Muchemwa and Robert Muponde, eds., *Manning the Nation: Father Figures in Zimbabwean Literature and Society* (Harare: Weaver Press, 2007).

³ "Zimbabwe is Mine," *Zimbabwe Metro.com*, 20 December 2008.

⁴ "Mugabe: 'Let Me Keep My Zimbabwe,'" *Telegraph*, 2 September 2002.

⁵ Giorgio Agamben, *Profanations* Translated by Jeff Fort. (New York: Zone Books, 2007), 74.

⁶ Charles Taylor, *Modern Social Imaginaries* (Durham: Duke University Press, 2004).

⁷ "Zimbabwe declares war on press," *The Star* (SA), 11 December 2001.

⁸ Staff Reporter, "State media ups propaganda," *Financial Gazette*, 7 March 2002.

⁹ Dumisani Muleya, "Who funds pro-government papers?" *Zim Independent*, 19 October 2002; Dumisani Muleya, "CIO takes over private media," *Zim Independent*, 13 August 2005; "Zim newspapers in CIO funding row," *Zim Online*, 16 August 2005.

¹⁰ The government launched at least one such venture, a joint Zimbabwean-Namibian newspaper. "Zimnam paper faces bleak times," www.journalism.co.za, 18 October 2005.

¹¹ Taungana Ndoro, "Docility is our greatest weakness," *Financial Gazette*, 15 August 2002.

¹² Muckraker, "State media fuels further brain drain," *Zim Independent*, 14 September 2002; "Zimbabwe's tense election aftermath has raised fears of a middle-class exodus," *Newsweek* 15 March 2002.

¹³ "Educated citizens flee Mugabe's rule for South Africa: An exile's story defines Zimbabwe woes," *Boston Globe*, 15 January 2001.

¹⁴ Broadcasting Services Act 2001, <http://www.kubatana.net/docs/legisl/broadcastact010404.pdf>; "Analysis of the Broadcasting Services Amendment Bill 2002 & ZBC Commercialisation Act 2001," (report, Media Institute of Southern Africa - Zimbabwe (MISA-Zimbabwe)), May 2002, <http://www.kubatana.net/html/archive/media/020530misaz1.asp>.

¹⁵ Ibid.

¹⁶ "Zimbabwe bans another talk show," *Times of India*, 13 July 2001.

¹⁷ Banning Eyre, "Playing with Fire: Fear and Self-Censorship in Zimbabwean Music," (report no. 03/2001, Freemuse, Denmark, 2001).

- ¹⁸ Columbus Mavhunga, "Top ZBC presenters, DJs among 435 axed," *Daily News*, 6 June 2002; "Lawyer accuses AG's office of delaying hearing of ZBC case," *Daily News*, 31 May 2002.
- ¹⁹ Paul Harris and Andrew Meldrum, "Zimbabwe's defiant exiles cry freedom over the airwaves," *The Observer* (UK), 6 January 2002.
- ²⁰ "Zimbabwean government wants radio broadcasts stopped," *Media Institute of Southern Africa* (MISA), 15 January 2002.
- ²¹ "UK rejects allegations of funding broadcasts," *Business Day* (SA), 17 January 2002; "Mbeki reveals anti-Mugabe broadcasts," *Business Day* (SA), 20 January 2002.
- ²² "Zimbabwe private radio 'jammed,'" *BBC*, 14 March 2005.
- ²³ BBC Monitoring research, 1900 gmt 16 March 2005.
- ²⁴ "Zim 'jamming' SW radio," *News24*, 19 March 2005.
- ²⁵ Rita Bhebhe, "SW Radio Africa should be saved," *New Zimbabwe*, 27 May 2005.
- ²⁶ "State jamming radio signals from UK," *Daily News*, 14 March 2005.
- ²⁷ Steve Holland, "Radio Free Zimbabwe," *Hendon and Finchley Times*, 9 July 2005.
- ²⁸ "SW broadcasts end," *ZWNNews.com*, 1 June 2005.
- ²⁹ "SW Radio Africa saved from closure," *New Zimbabwe*, 26 June 2005.
- ³⁰ The stories of SW Radio and of Voice of America's Studio 7 are currently the subject of research for a book by the author.
- ³¹ "Is Zimbabwe on the verge of cyber war?" *Zimbabwe Times*, 18 June 2008.
- ³² "Zimbabwe: Launch of 24-hour news station 'postponed indefinitely,'" *BBC Monitoring*, 25 May 2007.
- ³³ Lebo Nkatanzo, "ZBC TV goes live on the internet," *New Zimbabwe.com*, 17 July 2007.
- ³⁴ "Zimbabwe radio station goes live on internet," *New Zimbabwe.Com*, 1 October 2004.
- ³⁵ Harriet Chigege, "Protest musician launched internet radio on Zimbabwe Independence Day," *kubatana.net*, 7 May 2008, <http://www.kubatana.net/html/archive/artcul/080507hc.asp>.
- ³⁶ Simon Robinson, "Strive Masiyiwa: Founder of Econet Wireless," *Time* online, 2002, <http://www.time.com/time/2002/globalinfluentials/gbimasiyiwa.html>.
- ³⁷ Guthrie Munyuki and MISA-Zimbabwe, "Media Ownership in Zimbabwe," *kubatana.net*, November 2007. http://www.kubatana.net/docs/media/misaz_media_ownership_zim_051130.pdf.
- ³⁸ "Moyo orders blackout on Econet," *Daily News* online edition, 10 November 2004.
- ³⁹ "Zimbabwe mobile market swims against the tide," *ZimbabweSituation.com*, 21 March 2002, http://www.zimbabwesituation.com/mar22b_2002.html#link2.
- ⁴⁰ Jemima Kiss, "Zimbabwe's Daily News battles on—online," *Journalism.co.uk*, 28 September 2003, <http://www.journalism.co.uk/2/articles/5727.php>.
- ⁴¹ Associated Newspapers of Zimbabwe (Pvt.), Ltd. Press Release, 9 October 2003.
- ⁴² These situation reports and e-mails are found on *The Zimbabwe Situation*, an online database that started publishing online much of the violence in March 2000. See index on <http://www.zimbabwesituation.com>.
- ⁴³ ZimNews Press Release, *ZimbabweSituation.com*, 24 April 2001, www.zimbabwesituation.com/apr25_2001.html#link2.
- ⁴⁴ Gift Phiri, "Independent news websites mushroom," *Zimbabwe Independent*, 29 October 2004.
- ⁴⁵ Mduduzi Mathuthu, "Shaken and bruised, Daily News' journalist Mathuthu fears for his life," *Daily News*, 27 November 2001.
- ⁴⁶ These and other online newspapers are the subject of a book being researched by the author; Jürgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Translated by Thomas Burger and Frederick Lawrence. (Cambridge, MA: MIT Press, 1991).

- ⁴⁷ “CIO agents deployed to UK,” *Daily News*, 18 December 2000.
- ⁴⁸ Collin Chiwanza, “Zimpost admits rampant mail theft,” *Daily News*, 4 October 2001.
- ⁴⁹ Thomas Deve, “Virus unleashed on Daily News,” *Daily News*, 26 July 2001.
- ⁵⁰ “Missing e-mails raise eyebrows,” *Financial Gazette*, 26 September 2002.
- ⁵¹ Cris Chinaka, “Zimbabwe extends crackdown to anti-Mugabe e-mail,” Reuters, 21 November 2003.
- ⁵² Tererai Karimakwenda, “Government to legalise interception of private communications,” *SW Radio*, 20 March 2006.
- ⁵³ Interception of Communications Bill, 2006, Memorandum and Part III, <http://client.cyberplexaf-rica.co.zw/parliament/cms/Bills/InterceptBill.pdf>.
- ⁵⁴ *Ibid.*, Part III.
- ⁵⁵ *Ibid.*, Part IV.
- ⁵⁶ B.D. Crozier, “Interception Of Communications Bill, 2006 (HB 4, 2006),” *kubatana.net*, 28 June 2006, 3.
- ⁵⁷ *Ibid.*
- ⁵⁸ Lance Guma, “Too much to monitor for snooping squads,” *SW Radio*, 7 August 2007; Lance Guma, “Experts says ‘don’t panic’ as snooping equipment is installed,” *SW Radio*, 6 September 2007.
- ⁵⁹ Staff Reporter, “Hackers Infiltrate RBZ Website,” *Financial Gazette* (Harare), 22 August 2002.
- ⁶⁰ “Hackers break into Zimbabwe government website,” *New Zimbabwe.com*, 1 February 2005.
- ⁶¹ Traian Teglet, “Hackers Take Down Zimbabwe’s Herald,” *Softpedia Hacking News*, 13 May 2008, <http://news.softpedia.com/news/Hacker-Takes-Down-Zimbabwe-039-s-Herald-85463.shtml>; and Staff Reporter, “Financial Gazette second Zimbabwe paper to be hit by hackers,” *ZWNNews.com*, 15 May 2008.
- ⁶² “Hackers Target the Financial Gazette Website,” *Zimbabwe Guardian* (London), 15 May 2008.
- ⁶³ Search engines usually do this to sites they have analyzed and found to contain viruses installed by third parties to discredit the site.
- ⁶⁴ “Is Zimbabwe on the verge of cyber war?” *Zimbabwe Times*, 18 June 2008.
- ⁶⁵ “The Zimbabwe Times under attack,” *Zimbabwe Times*, 16 July 2008.
- ⁶⁶ Lance Guma, “Mugabe snooping law exposes increased repression,” *SW Radio*, 6 August 2007.
- ⁶⁷ Lance Guma, “Experts says ‘don’t panic’ as snooping equipment is installed,” *SW Radio*, 6 September 2007.
- ⁶⁸ Lance Guma, “Mugabe regime draws up list of blacklisted websites,” *SW Radio*, 10 August 2007.