Understanding Cyber-Crime in Ghana: A View from Below

Jason Warner[1]
Harvard University, USA

Abstract

Cybercrime perpetrated by pockets of citizens in the Global South is increasingly coming to light as a threat to U.S. national and global security; particularly, the West African nation of Ghana has recently come to be recognized as a major hub for cyber-criminal activity. This article argues that although a superficial examination of the process is instructive to a point, in attempting to understand the practice of Ghanaian cybercrime, a more profound investigation of local ground-level realities is necessary. As such, it presents a broad overview of the rise and practice of cybercrime in Ghana, before offering three ground-level case studies (relating to West African geopolitics, the techno-spiritual paradigm of Sakawa, and the justificatory philosophies of social justice) that are necessary for understanding Ghanaian cybercrime yet also largely under-recognized in Western discourses.

Keywords: Cybercrime; Ghana; West Africa; Global security.

Introduction

In January 2011, I purchased a discarded hard drive for $27 in a secondhand computer store on Bantama High Street in Kumasi, Ghana. Upon connecting it to a hard drive reader, I learned a plethora of information about the drive's former owner. Her name is Alice.[2] She lives in Surrey, England, just outside of London, and was a chiropractor. In 2004, she was one year away from becoming a pensioner and getting a free bus pass, a fact that made her nervous. Her Meyers-Briggs personality type is between ISTJ (energetic and analytical) and ISTP (curious and introspective), which might help to explain her regime of daily self-affirmations: "success is a journey, not a destination;" "your attitude determines your altitude." In 2005, she was also helping a family member battle through a bout of alcoholism, and as such, turned turn to the Bible for fortitude. Her favorite verse was Matthew 10:8, "freely you have received, freely give." (Hard drive purchased in Kumasi, Ghana, 2011).

Alice's hard drive, like so many from the United States, Europe, and Japan, are increasingly ending up in locations around the developing world after their owners have discarded their computers. While computer owners are typically assured by receptors of

[1] Ph.D. student in African/African-American Studies and Government at Harvard University, Cambridge, MA 02138, 617.495.1000, United States of America. Email: jasonwarner@fas.harvard.edu

[2] To protect the identity of the owner, her name and certain other details have been altered.

the machines in their home countries that their computers will be dismantled on site, such is not the case. Within the past decade, a trend has arisen that sees these old computers and other electronic devices being "discarded" into the developing world, where they are either repurposed and resold (as was the case with Alice's hard drive) or simply thrown into waste dumps out of the purview of the previous owners. This influx of electronic waste, or "e-waste," has unquestionably deleterious impacts not only on environmental and public health security of those living at importing sites, but also on the assurance of information security for both private citizens and governments from exporting sites (Warner, forthcoming).

Breaches of Western information security thanks to a rise in electronic waste circulation have been particularly pronounced in Ghana, where a certain cadre of citizens has taken to searching out information on Westerners' old hard drives for extortive purposes. To this end, a recent notable case originating from Ghana was one in which U.S. Congressman Robert Wexler (Democrat-Florida) was contacted by a Ghanaian, who attempted to blackmail him with information stolen from one of Wexler's discarded hard drives that had found its way to Ghana's secondhand computer market (Abugri, 2011). In a different case that highlights e-waste's negative impacts on state security, in 2009, an investigative journalism team from the University of British Columbia was able to purchase a second hand hard drive in Ghana that formerly belonged to Northrup Grumman, one of the U.S. military's largest contracting firms. Disturbingly, the drive contained information about some $22 million-worth of top-secret U.S. government contracts related to the Transportation Security Administration, NASA, and other federal agencies. (PBS Frontline, 2010). In yet another recent instance, a second hand hard drive was purchased on e-Bay that contained information on the testing procedures for the U.S. military's Terminal High Altitude Area Defense ground-to-air missile defense system, an Iraq-based operation used to shoot down SCUD missiles aimed at U.S. and ally targets (Abugri, 2011). Other U.S. agency machines that have surfaced in Ghana include those from the U.S. Army, the Washington Metro Transit Authority, the State of Connecticut Mental Heath Facility, and ironically, the U.S. Environmental Protection Agency (Claiborne, 2009). Truly, for Ghanaian cybercriminals, one man's trash is another man's treasure.

Similarly, if Alice could have been an easy target for cybercrime because of the extant information on her hard drive that I purchased in Ghana, the implications for U.S. national security because of the e-waste trade should go without saying. To this end, the United States has recently recognized the perpetration of cybercrimes as an up-and-coming threat to national security. When asked about preeminent threats to the United States in a 2010 interview, Deputy Defense Secretary William J. Lynn replied: "Number one [are] the cyber threat[s]. If we don't maintain our capabilities to defend our networks in the face of an attack, the consequences for our military, and indeed for our whole national security, could be dire." As such, the new U.S. Cyber Command slated to be opened in Fort Meade, Maryland, is but one tangible example of how the U.S. is taking an active role to combat threats from information insecurity (Kruzel, 2010).

But within discussions of how to protect the United States from cyber-insecurity, no one, at least to this author's knowledge, has made the explicit recognition that the recent influx of e-waste has catalyzed Ghana's status as an emerging locus of cybercrime. Indeed, this and myriad other ground-level realities often go unconsidered in discussions of cybercrime, particularly those that focus on the Global South. An investigation of these unconsidered realities serves as the primary consideration of this paper.

This paper argues that as cybersecurity increasingly becomes a focus of U.S. national security, views of cybersecurity from the top-down are insufficient; rather a more profound understanding of the sundry ground-level realities undergirding its practice warrant greater attention. Using Ghana as a case study, it asserts that the praxis of cybercriminality there is enmeshed in a more complex web of geopolitical, religious, and ideological phenomena into which have been embedded local understandings of a decidedly new technological era. To truly understand and mitigate the threat of cybercriminality emerging from the country (and indeed, around the world) the unique processes that underwrite it from a grassroots level need greater attention, which they are given here.

This paper first proceeds by offering a broad overview of Ghanaian cybercrime, focusing on its genesis, the various incarnations of national scams, and further offering a profile of the typical Ghanaian scammer and a discussion of state-level reactions. Having presented a superficial sketch of the phenomenon as seen from above, the second section investigates the process from the bottom-up, presenting three ground-level realities (relating to West African geopolitics, the techno-spiritual paradigm of Sakawa, and justificatory philosophies of justice) necessary for understanding Ghanaian cybercrime that are both unique to the country yet also largely under-considered in Western investigations.

Cybercrime in Ghana: History, Paradigms, Profiles, and Responses

In 2010, Ghana, long viewed as Africa's flawless gem, had its sparkling reputation tarnished. In a report published that year, Ghana gained the unsavory distinction – along with Anglophone African neighbors[3] Nigeria and Cameroon – as one of the top ten cybercrime generating states worldwide (Ghana, Nigeria cited, 2010).[4] In addition to its embarrassing addition to this list, a prior report also revealed that Ghana was the second-most frequently blocked location by U.S. online retailers skeptical of fake orders from Internet scammers (Kwablah, 2009). To better understand just how one of the continent's superlative states fell victim to the practice, this section offers a broad sketch of cybercrime in Ghana. Beginning with a brief history of cybercrime in Ghana, it then details the three

[3] Whether these assertions of Nigerian complicity in underwriting Ghanaian cyber-fraud are true or not, one commonality between the two countries that no doubt contributes to their statuses as the numbers one and two cyber-criminal states in Africa is their official languages: English. English, as many have noted, is the contemporary language of the Internet. Thus unlike citizens of Francophone or Lusophone African countries whose target audience for these crimes is much smaller, one sees that a far broader market of wealthy victims exists in the Anglophone world (from the United States, Canada, the U.K, but also from the billions of English bilinguals in the world). So while the West African region is typically thought of as "*l'Afrique francophonie,*" the few pockets of English speakers in the region are surfacing in Ghana's cybercrime rings, with notable arrests coming not only form Nigeria, but also from the English-speaking parts of Cote d'Ivoire as well as Liberian refugees left over from that country's 1994 civil war. In the rankings of top cyber-criminal countries, South Africa also made the list, highlighting the extent to which the phenomenon of cybercrime – in both Ghana and Nigeria as well – is truly anglicized on the African continent.

[4] It should not go without mention, however, that the leading state involved in cybercrime is the United States, followed by the U.K. Comparatively, U.S. and British national security forces would be wise to exert comparatively more effort mitigating the process domestically as opposed to internationally.

most common scams, offers the profile of a typical scammer, and finally investigates the ways that the Ghanaian state is attempting to manage and mitigate this new development. Ultimately, this section gives a superficial overview of the phenomenon as seen from above; that is, one that might be forwarded without attention to the more profound ground-level realities that underline such operations.

Cybercrime is a relatively new phenomenon in Ghana. According to anonymous sources, cyber-fraud came to rise in the country between 1999 and 2000. But during this period, electronically based crimes were primarily related to credit card fraud, which was initially facilitated by bellhops at international hotel chains who would share Western visitors' credit card information with scammers. In these instances, Ghanaians would steal the numbers of Western credit cards, purchase goods from the Internet, and have them shipped to Ghana. However, since approximately 2004, credit card purchases over the Internet have dropped; instead, newer forms of Internet fraud have begun to take shape (Anonymous employee of the Ghana Criminal Investigations Department, personal communication, 2011).

Sources within the Ghanaian national security apparatus[5] have delineated that three primary types of cyber-fraud are most commonly perpetrated in the country today. The first and most common of these is identity fraud. In this instance, Ghanaians will contact Westerners – often via social networking sites like Facebook, but also via Internet dating sites like Match.com, or eHarmony.com, in which Ghanaians were astonishingly the third most frequenting nationality behind only Americans and Britons (Ghana and Nigeria: Scammers in E-Harmony, 2011) – and communicate under the guise of a false identity. Most common within identity fraud cases are so-called "romance frauds." In short, Ghanaians may either portray themselves accurately (as Ghanaians) or falsely (as Westerners living in Ghana). After making contact and chatting, the fraudsters will eventually begin asking their presumed love interests for financial information and passwords. For instance, one typical case that Ghanaian authorities shared was that of a Ghanaian man who duped a German woman into believing that he was a former U.S. soldier (of Italian descent and New York upbringing) who had been stranded in Ghana with two boxes of gold. Only with her help could he get them out. Especially amongst the more advanced fraudsters, authorities have noted that even before they begin communicating with a potential victim, they will fabricate a range of documents that might be requested by the scammed paramour. Seasoned veterans are able to anticipate the types of identity verification that will be asked of them, and as such, go to great lengths to assuage their victims' fears of being defrauded by creating such sundry fake documents as: birth certificates, passports, visas, marriage licenses, high school and university diplomas, land and house deeds, medical records, airline tickets, bank statements, business letterheads, and lengthy import and export receipts (Anonymous employee of Ghana Criminal Investigations Department, personal communication, 2011).

Relying upon the same tactics of false identification, the second genre of cyber-fraud most frequently perpetrated in Ghana is that of fake gold dealers. Named the "Gold Coast" during its British occupation, Ghana is well known for its abundance of the ore. Today, Ghanaians will contact Westerners to offer them the opportunity to invest in

[5] Various members of the Ghanaian Criminal Investigations Department as well as the U.S. embassy were kind enough to speak with me at length about sundry dimensions of cybercrime manifest in the country today. Nearly universally, these insights were shared on the condition of anonymity.

upstart gold mining corporations based in the country. The fraudulent operation then unfolds as follows: After chatting on the Internet, Westerners will fly to Ghana for the purposes of surveying the investment-potential gold mines. Their would-be Ghanaian business partners will greet them at the airport and lodge them in hotels, which, authorities note, are often in obscure places so as to keep their duplicitous dealings out of the public limelight. Once there, the scammers will show the foreigners bars of gold – mostly real – as well as bags of fake gold shavings. The following day, the scammers will take the Westerners to small, gold-rich villages in the northern parts of the country in order to show them the "location" where their mutual gold mining enterprise will be based. Having already alerted members of the village, one "elder" (usually just a relative or friend of the cyber-thieves) will come out to greet the Westerners in traditional Ghanaian garb, and, evoking hyperbolic parallels to colonial white imaginations, will invite the Westerners to come in and help them mine the gold. Thereafter, the Westerners are typically sufficiently confident to invest. Back at the hotel, having proven the veracity of their Internet claims, the Ghanaians and Westerners will make the collaboration official: the Westerners will make down payments on their new joint business ventures, while the Ghanaians will put bars of gold into safes that they will leave with the Westerners as proof of their trustworthiness. At the last minute, the Ghanaians will switch the gold-filled safes with empty ones and will leave the hotel, assuring their new business partners that they will return the following day to make final arrangements. The Ghanaians will not return (Anonymous employee of the Ghana Criminal Investigations Department, personal communication, 2011).

The third type of prevalent cybercrime in Ghana is that of estate fraud, whose victims are not typically Westerners, but instead, Ghanaians residing in the Diaspora. As it is common for Ghanaians living abroad to return to the country upon retiring, new enterprises have sprung up across the Internet to cater to these wealthy Ghanaians' patrimonial real estate needs. Several cases have been reported wherein Ghanaians create fake construction firms that they then advertise on the Internet that purportedly specialize in retirement housing for their compatriots returning to the country. Boasting websites with pictures of houses that they ostensibly built themselves (but which in reality, are simply random existing houses), the scammers will then "sell" the would-be retirees blueprints for such houses as well as plots of land on which these houses will be built. Later, they will send their clients' receipts for building materials such as cement and tile as proof of construction. After extracting as much money as possible from the distant clients, the "companies" will collapse, disappearing into Internet anonymity (Anonymous employee of the Ghana Criminal Investigations Department, personal communication, 2011).

Though deviations exist, those perpetrating these schemes fit a specific profile. The typical Ghanaian Internet scammer is a male – an estimated 90% are men, though there are exceptions[6] – and he is under 30 years of age (Edith Clarke, personal communication,

[6] Historically, females that have been involved in Ghanaian cybercrimes have tended to be the girlfriends of the scammers themselves, who will often field calls from foreign national males who, although believing that they are corresponding electronically with a Ghanaian woman, are actually talking to the woman's boyfriend pretending to be one. However, more recently, commentators have cited the emergence of a uniquely female incarnation of Sakawa. In this scam, a woman goes to a *juju* priest to bless her with extreme sexual charms (in the cited story, with a potent lip gloss),

2011). He resides in or near an urban center such as Accra or Kumasi where access to Internet cafes is easy, a requisite given that home-based Internet connections are reserved for only the wealthiest in the country. Frequently, he resides in slums such as Nima, Maamobi, Accra New Town, and Mallam Atta (Abugri, 2011). He is typically unemployed or underemployed, and as such, does not normally attend school. Instead, his days are spent lingering around cyber cafés, often with others engaged in the same activities (Issah Yahaya, personal communication, 2011). Such collectives of cybercriminals are commonplace, yet their acephalous nature makes stopping them more difficult since, as one official noted, "When you catch one boy, five others will pop up" (Anonymous employee of the Ghana Criminal Investigations Department, personal communication, 2011).

With the recognition that cybercrime is an increasingly real threat to the country, the government of Ghana – particularly the Ministry of Communications – is beginning to take measures to combat it. Prior to 2008, no laws existed in Ghana specifically in regard to cybercrimes and resultantly, police treated cyber criminals as if they were simple defrauders. However, in 2008 Ghana passed the Electronic Transactions Act (Act 772), which both criminalized computer hacking and resultantly gave police officers more latitude to pursue suspected cybercriminals. Although hopes are high that the law will help to minimize the practice, today the government worries that the future of cybercrimes in the country will not be computer-based, but cell phone based. With 17 million cell phone subscribers and only three million home Internet subscribers, the assumption is that the proliferation of smart phones throughout the country will make tracking Internet activity, especially that of cybercrime, even more difficult in the foreseeable future (Issah Yahaya, personal communication, 2011).

Because of the relative newness of cybercrime and the concurrent dearth of literature devoted to the creation of paradigms within which to analyze it (optimistically ameliorated by this publication), situating Ghanaian cybercrime within a theoretical context is a challenging proposition. Nevertheless, one sees that the "Space Transition Theory" propounded by Jaishankar (2008, pp.283-301) is instructive in that, as in the case of Ghana (Danquah & Longe, 2011), it accurately assesses that "persons…have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space," as well as the fact that, "identity flexibility, dissociative anonymity, and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime." Moreover, one sees that cybercrime in Ghana largely parallels the emergence and proliferation of the phenomenon in other locations throughout the Global South. For instance, Scott Henderson (2007, 101-104) corroborates that some of Ghana's most prevalent types of cyber fraud – such as banking fraud and blackmail – have been common in contemporary Chinese hacking circles, and as will be seen presently, the same trends and operations of Ghanaian cybercrime are also common in Nigeria. Yet despite these similarities, a variety of unique facets about the nature of cybercrime does exist, and are detailed in the next section.

The Hidden Story: Ghanaian Cybercrime as Seen From Below

While marginally useful (and indeed, typical of the types of analyses frequently forwarded) the preceding overview of the rise and nature of Ghanaian cybercrime is far

which helps her to attract extremely wealthy men that she will sleep with and from whom she will later extort money (Female Sakawa hits Accra, 2008).

from fully revelatory. Rather, to understand the full picture of cybercrime in the country, additional factors apart from those just delineated demand consideration. The following section highlights three specific socio-cultural phenomena – including Ghanaians' presumptions of the culpability of Nigerians; the rise of the cyber-thieving theology of Sakawa; and the underlying philosophies of social justice used to justify cyber-fraud – which have thus far, gone unconsidered. While these by no means constitute an exhaustive list of the myriad ground-level realities that are serving to underwrite cybercrime in Ghana, they nevertheless are a useful initial point of investigation.

Beggar Thy Neighbors: The Culpability of Nigerians in Ghanaian Cybercrime

"Nigeria: They are our senior brothers." The comment came with an uneasy laugh and an eye roll from an annoyed Ghanaian (Anonymous employee at the U.S. embassy, personal communication, 2011). The troubled African behemoth Nigeria and its comparably diminutive and more peaceful neighbor Ghana could not be more divergent. The mired political history of the former is often assumed by citizens of the latter to be characteristic of the country's population in general, and as such, the Nigerian immigrant community is often blamed for importing, catalyzing and propagating cybercrime in Ghana. Consequently, the first understudied dimension of contemporary Ghanaian cybercrime is the perception by local populations that, at its core, it is a problem that has primarily been imported by Nigerians.

This presumed culpability is perhaps not surprising: known locally (and increasingly, internationally) as "419 schemes," Nigeria is frequently thought of as the cradle of global cybercrime. 419 schemes, known in their pre-Internet incarnation as "advanced-fee fraud," originated in Nigeria earlier than they did in Ghana, emerging in the 1980s after the collapse of world oil prices left Nigeria's oil-dependent economy shriveled and citizens in need of quick capital (Smith, 2008, p.29). In the 1980s and 1990s, 419 scams were common in Nigeria. Catalyzed by the emergence of business centers offering phone and computer services, an increasingly educated yet unemployed youth demographic, and a generally deep-seated culture of national corruption during the military government eras of Ibrahim Babangida (1985-1993) and Sani Abacha (1993-1998), it was during this period that Nigeria began to garner infamy for its culture of deception (Smith, 2008, p.30).[7] During these two decades, however, Nigerian 419 scams were not Internet-based, but rather, involved credit card fraud; like the predecessor to Internet scams in Ghana, Nigeria's early cyber-fraudulent schemes were "cyber" only in their telecommunicative nature. It was at the dawn of the 21st century, however, that the Nigerian 419 paradigm was to undergo a seismic shift.

After the election of Olusegun Obasanjo in 1999 ushered in civilian rule, the easing of communications restrictions coupled with the emergence of global Internet connectivity gave rise to the Internet-variety of 419 scams in Nigeria for which the country is infamous today. In an anthropological study of Nigerian corruption in the mid-2000s, Brown University Professor Daniel Jordan Smith held a sub-focus on Nigerian 419 Internet

[7] Daniel Jordan Smith notes that during the 1990s, Sani Abacha, in an ostensible effort to stamp out illegal activities related to 419, made a national decree making the operation of small business centers illegal. However, human rights advocates saw the decision not as a move to eliminate corruption – in which Abacha and his cohorts were deeply involved – but instead as a means to stifle communication between the members of the highly discontented Nigerian civil society (Smith, 2008, 31).

scams. After years of research, Smith was able to shockingly assert with authority that, "in an Internet café of twenty to twenty-five terminals, at any one time at least four to five terminals were being used to send scam letters" (Smith, 2008, 25). Today, Nigerian cyber-scammers are best known for sending unsolicited emails from a variety of characters – including Nigerian princesses, wives of former military rulers, and desperate entrepreneurs – who, caught in precarious financial or legal conundrums, require the timely assistance from those possessors of Western capital. Victims are duped into providing bank account numbers to facilitate the transfer of money from these Nigerians' accounts to their own, a process which ultimately and nearly universally sees funds being moved in the opposite direction. The U.S. Secret Service estimated that in the 1990s alone, such Nigerian 419 schemes costed their victims five billion dollars (Smith, 2008, p.32).

When discussions about cybercrime arise in Ghana, Nigerians are the first to be blamed for its genesis in the country. Because of an ECOWAS (Economic Community of West African States) treaty to which both Nigeria and Ghana are signatories, citizens are able to flow freely between the countries so long as they posses a passport from one. As a result, Ghanaians have claimed that Nigerians have streamed into their country in the past decade, bringing with them what are locally known as "formats," or cyber-fraud paradigms or storylines that have proven economically fruitful when employed in the past (Edith Clarke, personal communication, 2011). An official at the Ministry of Communications suggested that cyber-scamming Nigerians were flooding into Ghana both to flee from prosecution from 419 crimes committed in Nigeria, as well as to take advantage of Ghana's comparatively better (and therefore, more profitable) Internet bandwidth (Issah Yahaya, personal communication, 2011). Ghanaians tend to believe that once in the country, these Nigerian expatriates congregate in tight-knit clusters around major urban centers like in the areas of Achiomota and Nima in Accra where they are able to access the Internet in relative secrecy (Edith Clarke, personal communication, 2011).

Ghanaian authorities have taken note of the influx of Nigerians, and have outlined a variety of differences in the *modus operandi* between Nigerian cyber-fraudsters and Ghanaian ones. The first of these differences relates to chosen victims. For Ghanaians, the primary targets for cybercrime tend to be older, divorced or widowed white women, sometimes living in the U.S., but more frequently from the United Kingdom or Germany. In contrast, Nigerians' primary targets tend to be middle-aged male business executives from the U.S. Midwest, particularly, Texas (Anonymous employee of the Ghana Criminal Investigations Department, personal communication, 2011). Two reasons underlie this latter trend. First, Texas has one of the largest populations of Diasporan Nigerians – situated in urban centers such as Houston and Dallas – a minute minority of whom work in clandestine criminal cooperation with their partners based in Nigeria proper. Second, Nigerians frequently target Texas because it is the center of U.S. oil operations. Legitimate cooperation between Texan and Nigerian-based oil companies is common, thus scammers, cognizant of this fact, will often exploit these pre-existing links between Texans and Nigerians for their benefit, duping Texan oil magnates into investing in fake oil ventures based in Nigeria, akin to the fake gold dealers operating in Ghana (Smith, 2008, p.32-33).

"If a Ghanaian has a bowl of *kenke* and fish, he is happy; the Nigerian wants to own his own airline before he is content." This sentiment, expressed by an anonymous Ghanaian official at the U.S. embassy, highlights the perception amongst some Ghanaians that immigrant Nigerians are changing consumption patterns in the country, encouraging

young Ghanaians to live ostentatious lifestyles like them supported through the perpetration of cyber-fraud. For many like this official, young Ghanaians' avarice is a marked turn from ideas about consumption from their own adolescence. The Jerry Rawlings' 1979 left-wing revolution and subsequent two-decade rule imbued within the Ghanaian social psyche an aversion to displays of wealth, leaving Ghanaians feeling self conscious about driving expensive cars for fear that they would be labeled "bourgeois." Now, the tides are beginning to change, with young Ghanaians seeking to emulate international rap stars' lifestyles filled with expensive cars, jewelry and women. So profound is this contemporary desire for lavish living that many of the older generation worry that Ghanaian youth will stop at nothing – even Internet crime – to get what seemingly successful Nigerians have (an Anonymous employee at the U.S. embassy, personal communication, 2011).

Cybercrime as a Religion: The Rise of Sakawa

The second underreported ground-level aspect of Ghanaian cybercrime is the emergence of what is known locally as *Sakawa*, which can be described as an ever-evolving klepto-theological paradigm created to abet in the perpetration of Internet crime. In Ghana, priests and other spiritual leaders of both local and Western religions have taken to performing "Sakawa blessing ceremonies" for youth participating in cybercrime, which are intended to protect cybercriminals from being discovered and ensure their ultimate financial success.

The contemporary ritualized religious aspects of cybercrime in Ghana can be traced back some four decades. Even before the advent of the Internet, young Ghanaian men maintaining international pen pals would go to consult their local priests, who would bless them so that their pen pals would send better gifts along with letters: more photos, small trinkets or amounts of money. With the rise of online correspondence the process took on a digital dimension (Expert calls for national body, 2010).

Because of the abundance of youth that are now involved in Internet scamming and the recognition of the real legal dangers that the enterprise can place them in, Ghanaian youth are now turning to religious leaders known as "malams" to protect them.[8] To gain legal protection and moral fortitude before scamming, youth will go to such *juju* priests, who, upon a prognosis of the situation, will render an appropriate prescription. Writes one blogger in Ghana:

> The Sakawa kid will go to the priest and [the priest] will say, 'you must sleep for a night in a coffin [with a corpse], then sacrifice three chickens, then give me five cedis [approximately $3.33].' If the person does all this, their [sic] fraud will be successful. If not, they [sic] are disregarding the prescription of a *juju* priest, which, as everyone knows, is an unwise thing to do. [The process] usually involves you getting turned into an animal of some kind, or running naked through the market square…There are also rumours [sic] about human sacrifices being made (Taylor, 2009).

[8] The name of such priests derives from what is locally believed to be the first cybercrime priest, "Mallam Isa Kawa" meaning 'Mallam Isa's ring,' which was based in Swedru, some 30 miles from Accra (Taylor, 2009).

According to Kumasi based computer programmer Chris MacQuansah, the ritual aspect of Sakawa has a variety of purposes. Not only does it help keep the hacker's identity anonymous and thus free of prosecution, it further ensures that other members of the community – many, themselves, who are in the business – "forget" that their friend had been involved in such a crime (Chris MacQuansah, personal communication, 2011). The Sakawa scammers claim that the religious aspect of the crime is working, as occasionally, scammed Westerners will refuse to turn perpetrators because of the interpersonal relationships that have formed between them. For Sakawa boys, this legal indemnity is proof of metaphysical providence (Edith Clarke, personal communication, 2011). Said MacQuansah (2011), "if [cybercrime] was just a technical issue, we would have made more headway. But now that there is a ritual and a religious aspect to it, that makes it much harder to stop."

Perhaps unsurprisingly, there is a decidedly dark underbelly to Sakawa. Distressingly, Sakawa rituals have been blamed for numerous deaths and injuries over the last five years. A boy in Cape Coast was paralyzed while performing a Sakawa ritual and lamentably, human sacrifice for the benefit of Internet fraud does appear to be a genuine phenomenon (Sakawa ritual paralyzes student, 2009). In July 2009, two teenage girls – one of whom was pregnant – were brutally murdered and their genitals removed in what authorities believed to be a Sakawa-related ritual (Girls killed for Sakawa, 2009). Another Ghanaian report has mentioned that abductions of children and babies are also part of some Sakawa rituals (The Sakawa menace, 2009). Apart from physical harm, the young, poor and often uneducated Ghanaians who patronize malams are also being exploited in another way, by expending considerable amounts of their already limited resources for such blessings, which, also unsurprisingly, have an unimpressive rate of success.

As is typical in any discussion of cybercrime, Ghanaians view other West Africans, particularly Nigerians, as having some complicity in the rise of the emergence of the religious transformations of Sakawa cybercrimes. Highlighting the fact that religious Sakawa is a larger West African phenomenon that extends beyond just Ghana, a documentary by the Ghanaian Broadcasting Corporation followed Sakawa malams all the way to Benin with their clients for blessings (Issah Yahaya, personal communication, 2011). Yet as always, blame is primarily placed on the shoulders of Nigerians. One Ghanaian mother of three relayed that she believed that Nigerian Nollywood films, which are omnipresent in the country, are indoctrinating the Ghanaian youth to believe that *juju* magic can be used especially in Internet fraud to reap great rewards (Anonymous employee of the U.S. embassy, personal communication, 2011). Mary Adekoya, a scholar of Nigerian cinema, corroborates this potentiality, writing that indeed:

> *Juju* is very pervasive in Nigerian video films and it is often presented…as a way of obtaining wealth and status when all other routes to fulfilling such desires have become impossible. Seeing how *juju* in Nigerian films is typically used to give potency to an endeavor to gain wealth and status, it is not far-fetched to see how a 419 scam artist would turn to *juju* - that is, in a movie (Mary Adekoya, personal communication, 2011).

Adekoya remains skeptical, however, that Ghanaian youths' exposure to Nollywood movies alone is at the root of the Sakawa religious movement, instead conjecturing that the films are "perhaps only one element of a larger occult imagination that Ghanaian scam artists are exposed to in everyday life, that makes them open to the possibility that witchcraft can be a route to material gain" (Mary Adekoya, personal communication,

2011). Whether by cinema or societal pressures, the rise and proliferation of the techno-religious phenomenon of Sakawa is another increasingly embedded, yet underreported, aspect of the practice of Internet fraudulence in Ghana.

Justified Thievery: Philosophies of Domestic and International Social Justice

Internet thieves in Ghana are rarely remorseful about the cybercrimes that they commit. Instead, such Sakawa boys – often poor, uneducated urban dwellers – view themselves as occupying the lowest rungs of the social ladder due not to indolence, but rather, a malevolent trifecta of exploitative social forces that operate around them: the Ghanaian state, the Ghanaian bourgeoisie, and the imperial West. An excerpt from an interview with a Nigerian Internet scammer succinctly highlights these attitudes in the neighboring country. Said the interviewee:

> For me, I am just struggling…Obasanjo and his boys [the state] are stealing so much money while the rest of our society is falling apart. That's the real 419…I would not be here sending these emails looking for rich greedy foreigners [the imperial West] if there were opportunities here in Nigeria. How much do I really get from this anyway? The people getting rich from this are the same people at the top [the local bourgeoisie] who are stealing our money. I am just a struggle-man (Smith, 2008, 38).

Consequently, for them, the perpetration of Internet fraud against the state, wealthy Ghanaians or avaricious Westerners is not a crime, but a sort of redemptive project of social justice. The third understudied aspect of Ghanaian cybercrime then is the constellation of philosophies of domestic and international redistributive justice that percolate within Ghanaian cyber-criminal circles that give justification to their illegal activities.

Within Ghana, Sakawa boys justify their activities as being the only way that they can survive in a country where the state is not doing enough to offer social protections to ensure their livelihoods. It is common knowledge that Sakawa boys turn to the crime to make money that cannot be made in legitimate ways, thus in national policy discussions on how to mitigate cybercrime, finding suitable employment for youth is a frequent topic of conversation (Essel, 2009). Moreover, the youth that are involved in these activities have also come to them as a last resort, having previously had other run-ins with symbols of the state such as the police and the judicial system and penal systems. As such, they retain a healthy skepticism of the state for both forcing them into cybercrime, and simultaneously, attempting to prosecute them for the committing such crimes of necessity. Writes one Sakawa boy:

> Hey, what is all this i am hearing, BLOODMONEY, BLOODMONEY. There is nothing like that, what is going people call it BLOODMONEY is called SAKAWA and this simple means PAY BACK. How about the government, why don't they call it blood money as well. When the police arrest as, then who is going to pay Tax and Vat [Value Added Tax].They should sit down and think before they are. From the begining of this Game, when have you heard anything about armed robbery, Let them think about that well…MOREMONEY MOREMONEY MOREMONEY AMOKODEY [sic] (Kwablah, 2009).

Similarly, Sakawa boys harbor deep resentment for the burgeoning upper class of Ghanaians. Once again, Internet scammers view the rich of Ghana as being bulwarks against their own rise to the top, not least because of their collusion with the aforementioned structures of the state. Yet for Internet scammers, targeting this demographic of Ghanaian society presents unique challenges. On one hand, they are more difficult to scam than Westerners, since, as a cash based society, the Ghanaian bourgeoisie is less likely to use credit cards than their European or U.S. counterparts (Issah Yahaya, personal communication, 2011). On the other hand, elite Ghanaians are increasingly being seen as ideal targets. As an anonymous official noted (2011), Ghanaians are deeply embarrassed about getting scammed, feeling that as members of the society, they should have been more vigilant; consequently, even when duped, Ghanaian elite tend not to come forward to the authorities for fear of embarrassment. For Sakawa boys, the rich and silent make ideal victims.

Internationally, Sakawa boys justify their duping of Westerners by claiming that it is pointed retribution for centuries of historical injustices perpetrated by the West against Africans. Indeed, the histories of the Trans-Atlantic slave trade, combined with the none-too-distant experience of colonialism and a surface-level adherence to the Pan-Africanist ideal of international social justice has combined to form a triumvirate of rationales to excuse the robbery of Westerners via the Internet. As one Sakawa boy relayed on a public website:

> Am a Sakawa boy and all i can say is….Sakawa in Ghana is pay back to the white-men and woman…Have we all forget about what they done to as...Taking our Gold and buy we the same time..By the way i wish one of you know what Sakawa is…..Everyone is saying what he like……Sakawa is not about blood money…All u have to do is to email me and i will tell u what we do before white- men or woman send his money joemilla77@hotmail.com [sic] (Kwablah, 2009).

To be sure, for Ghanaians (and Nigerians), histories of injustice – by the state, elites, and the West – have allowed the commission of contemporary cybercrimes to be rewritten in a vernacular of an ethically permissible retribution.

Conclusion

Internet criminality has recently surfaced as a real concern for law enforcement officials in Ghana, and by proxy, members of the global community at large. Its victims range from Europeans to Ghanaians to U.S. citizens, yet relatively scant attention has been given to gaining an understanding of the ground-level realities underpinning these processes. This article has sought, in its own modest way, to broach the topic in ways that have heretofore been unexamined. It began by giving a standard, top-down overview of the contemporary incarnations of Ghanaian cybercrime, before moving on to investigate three more complex, yet understudied, grassroots realities that must be understood if Internet criminality is to be mitigated. By offering discussions of the presumed guilt of Nigerians, Sakawa religious orders, and justificatory philosophies of justice, this article has sought to broaden the discursive plane on which Ghanaian cybercrime exists today. And if there were any debate as to the need for such a discussion on the mitigation of the Ghanaian Internet crime, there remains only one course of action: go ask Alice.

References

Abugri, S. (2011) Ghana: Internet criminals cashing in on e-waste. *New African*. Retrieved January 24, 2011, from http://www.sydneyabugri.com/Home2/features/217-ghana-Internet-criminals- cash-in-on-e-waste-dumping.html.

Claiborne, R. (2009, August 2). U.S. Electronic Waste Gets Sent to Africa. *Good Morning America.* Retrieved February 23, 2011, from http://abcnews.go.com/GMA/Weekend/story?id=8215714&page=1.

Danquah, P., & Longe, O. B. (2011). An Empirical Test of the Space Transition Theory of Cyber Criminality: The Case of Ghana and Beyond. *African Journal of Computing & ICTs. 4*(2), 37-48. Retrieved October 14, 2011 from http://ajcict.net/uploads/Danquah___Longe_-_An_Empirical_Test_Of_The_Space_Transition_Theory_of_Cyber_Criminality_-_The_Case_of_Ghana_and_Beyond.pdf

Essel, I. (2009, August 12). National Youth Policy to solve Sakawa, homosexuality – Veep. *My Joy Online.* Retrieved February, 23, 2011 from http://news.myjoyonline.com/news/201008/50648.asp.

Expert calls for national body to combat threats. (2010, August 27). *Ghana Business News.* Retrieved February 10, 2011, from http://www.ghanabusinessnews.com/2010/08/27/expert-calls-for-national-body-to-combat-cyber-threats/.

Female Sakawa hits Accra. (2008, November 29). *My Joy Online.* Retrieved February 23, 2011, from http://news.myjoyonline.com/features/200811/23323.asp.

Ghana and Nigeria: Scammers in E-Harmony. (2010). *E-Harmony Blog.com.* Retrieved February 22, 2011, from http://eharmony-blog.com/842.

Ghana, Nigeria cited among top 10 countries in global cybercrime ranking. (2010, December 2). *Ghana Business News.* Retrieved February 24, 2011, from http://www.ghanabusinessnews.com/2010/12/02/ghana-nigeria-cited-among-top-10-countries-in-global-cybercrime-ranking/.

Girls killed for Sakawa. (2009, August 13). *XFM 95.1 NewsCenter.* Retrieved February 22, 2011, from http://ghanavoices.wordpress.com/2009/08/13/girls-killed-for-Sakawa/.

Henderson, S. J. (2007). *The Dark Visitor: Inside the World Of Chinese Hackers.* Leavenworth, KS: Foreign Military Studies Office.

Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. In F. Schmallager, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Kruzel, J. J. (2010, February 4). Cybersecurity Seizes More Attention, Budget Dollars. *American Forces Press Service.* Retrieved February 12, 2011, from http://www.defense.gov/news/newsarticle.aspx?id=57871.

Kwablah, E. (2009, February 17). Cyber crime: Giving a bad name to Ghana. *Ghana Business News.* Retrieved January 23, 2011, from http://www.ghanabusinessnews.com/2009/02/17/cybercrime-giving-a-bad-name-to-ghana/.

PBS Frontline. (2010). *Ghana: Digital Dumping Ground*. Online Documentary. Directed by Peter Klein.

Sakawa ritual paralyzes student. (2009, March 27). *Daily Graphic.* Retrieved February 23, 2011, from http://news.myjoyonline.com/news/200903/28062.asp.

Smith, D. J. (2008). *A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria*. Princeton, NJ: Princeton University Press.

Taylor, L. (2009, July 6.) Sakawa! No, Really! Sakawa! *Linnettaylor's Weblog*. Retrieved February 22, 2011 from http://linnettaylor.wordpress.com/2009/07/06/Sakawa/.

The Sakawa menace. (2009, May 4). *The Ghanaian Journal*. Retrieved February 11, 2011, from http://www.theghanaianjournal.com/2009/05/04/the-Sakawa-menace/.

Warner, J. (Forthcoming). "Everything Means Nothing: The Trouble of Human Security Threats and Electronic Waste in Ghana." (Working paper).