Cyber Capacity without Cyber Security: A Case Study of Nigeria’s National Policy for Information Technology (NPFIT)

Roseline Obada Moses-Okè*

* Legal Practitioner, Solicitor and Advocate of the Supreme Court of Nigeria

Abstract
Prior to the year 2001, the phenomenon of Internet criminal fraud was not globally associated with Nigeria. Since then, however, the country had acquired a world-wide notoriety in criminal activities, especially financial scams, facilitated through the use of the Internet. This is not to say that computer-related crimes were alien to the country. It is, however, remarkable that the perpetration of cyber crimes involving Nigerians and traceable to Nigeria became so rampant that questions might be legitimately raised as to why the problem became so pronounced from around that year. It is further remarkable that the attempt to launch Nigeria into the digital age coincided with the unprecedented rise in computer-related financial crimes in the country. In this paper, it is argued that the problem arose as a direct consequence of the lapses in the 2001 National Policy for Information Technology (NPFIT). The argument is based on an analysis of the various provisions of the Policy, with specific focus on the lack of proactive security provisions in it and in its subsequent implementation, in the wider context of global experiences of, and efforts to deal with, cyber security breaches as at the time of the formulation and implementation of the NPFIT.

Keywords: Nigeria; Cyber-criminality; NPFIT; the Internet; capacity; security.

Introduction
The oxymoronic nature of the Internet is one of its unforeseen attributes; at its inception, no one, perhaps, could have clearly foreseen that, and how, the Internet would someday become a veritable platform for globalized criminal activities. As has been copiously remarked, the benefits of the Internet have so often been tainted by its versatility for virtual criminal activities that have vastly devastating physical and social impacts. As noted by I-vission International, “cybercriminality, a phenomenon which is gaining grounds in almost all the continents today, has caused enormous loss and setbacks in the public and private sectors.”¹ According to Stephanie Perrin, for instance, “The rapidly expanding capabilities of information and communication technologies (ICT) have created new crimes and new ways to commit old ones.”² And, as noted by the International Development Research Centre, “The ICT revolution has fundamentally changed society. All sectors are affected by the dramatic diffusion of these technologies
that bring with them both positive and negative effects."³ This vulnerability of the Internet had made itself manifest as far back as 1970⁴, while developments in Information and Communications Technologies have, almost naturally, opened the cyber space to further abuse by criminally minded users of the Internet on a frightening global scale that has long become a matter of serious global public concern.⁵ Yet, the world now seems incapable of any activity without the Internet, and computer-based equipments. The realization of this dilemmatic situation has led the pioneers and early joiners of the Internet age to have been devoting colossal amounts of resources to the multi-structural sanitization of the Internet.⁶ In other words, those who have been long involved in the use of the Internet clearly and openly acknowledge its characteristic shortcomings and openness to abuse, and so have always strived, as much as is possible, to forestall chances of new abuses and to minimize the adverse effects of existing ones that cannot yet be eliminated. In other words, still, the older users of the Internet are acutely Internet security conscious and pragmatically committed to the safety of the facility for all its users.⁷ The world has thus, for a long time now, at least as at 2001, come to the settled realization that in order to maximize the benefits of the Internet, cyber capacity must be simultaneously accompanied, toe to toe, with cyber security.⁸ It is within this context of global awareness of, and war against, Internet insecurity and risk that the recent entry of Nigeria into the digital age is here being examined through the nation’s policy on information technology.

The paper is of the view that in a knowledge-powered world, every individual or collective activity, including policy designs and implementations, should be guided by all the available relevant information. As such, the paper seeks to see how much Nigeria's entry into the world of the Internet, via the National Policy for Information Technology⁹, has been guided by the available relevant information as at 2001, and how this has impacted on the country’s presence in cyber space since then, with a view to providing some insight into the ultimate cause of cyber crime in Nigeria, and consequently, how best to address the situation.

The honest intention of the Federal Government of Nigeria in making the policy for information technology in 2001 must have been to empower Nigerians to join the rest of the developed world to benefit from the multiple advantages of the Internet in a variety of positive ways. It could, therefore, not have been the intention of either the government or the authors of the policy that it should become an instrument for committing crimes. That is to say that it cannot be fairly claimed that the objective of the policy, from the onset, was to empower Nigerians for the commission of Internet crimes. However, it will not stop to appear curious that the introduction of the Policy was quickly followed by the then new phenomenon of online fraud of various kinds, most pernicious of which are those popularly known as ‘419’ or ‘Nigerian cyber-scams’¹⁰, etc., and software piracy, which have adversely affected the economy and profile of the nation. According to the authoritative account of Nuhu Ribadu, former Executive Chairman of Nigeria's Economic and Financial Crimes Commission, (EFCC), the country became fully aware of “this pattern of crime in 2002.”¹¹
Like its concurrent policy on telecommunication, the policy on information technology was overtly intended to open up the nation’s information and communication space to the generality of Nigerians, with the aim of giving them a greater and freer access to both local and global content. The policy also intended that such access would help to narrow the digital divide between Nigeria and the technologically more advanced countries, and impact on education, health, industry, entertainment, social life, and commerce. These are undoubtedly laudable intentions, especially given the parlous state of the country’s telecommunications, transportation, and other social infrastructures prior to and up to 1999 when the country returned to civil democratic rule after decades of military rule. The understandable vision of the authors of the Policy and the government must have been that its implementation would free the people from the inefficiency of the nation’s public telecommunications and postal services, reduce the high carnage on the roads owing to the necessity of travelling on the roads to attend to every little social and business engagement, and fast-track the country’s technological development.

Moreover, and apart from the quantifiable benefits of the Policy, the government had other social-political motives for it. It was regarded as a dividend of democracy and a show of the country’s development and modernization in tune with what obtained in the advanced countries of the world. The government, therefore, did not have any reservations to accept and implement the Policy as was presented. The government believed it was adding value to the lives of the populace and enhancing the status of the country in the comity of the world’s civilized nations. Like the mobile telephone service, the government quickly liberalized the Internet service provision business. Rightly, the liberalization of these services created unprecedented multiplier effects in the economic sector as millions of hitherto unemployed and under-employed citizens became gainfully employed and self-employed in the ICT sector. In particular, cyber cafes quickly became a ubiquitous phenomenon all over the country. An expected consequence of this situation was that the high crime rate allegedly due to high youth and graduate unemployment and the attendant crushing poverty would be drastically reduced.

To a very large extent, the promises of the Policy were substantially fulfilled, albeit, in a negative way in certain instances. The fulfilment of General Objective (xv) of the Policy is a particularly pertinent case in support of this view. The ‘youths’ were indeed empowered with IT skills, but many of them quickly turned their newly acquired skills into tools for online criminal activities. These criminal activities, also negatively, created wealth for the ‘youths’; negatively because such wealth was illegitimate, being proceeds of fraud, and detrimental to the economy and the external image of the country. There is no evidence that the skills so acquired were substantially used for the advancement of software development or other IT engineering tools and techniques, or credible economically viable and lawful online products. Moreover, if the empowered ‘youths’ became globally competitive with their peers, it was largely in the area of online offenses, as it yet remains to be noticed what positive contributions they have made to the global ICT environment.
Thus, as an African (Yorùbá) adage translates, ‘the canine teeth spoilt the dog’s dentition’ (kôkôrô beyiń ajá jê). Naturally, the dog’s canine teeth are evolutionarily purposive and functionally positive. The ‘canine tooth’ of the NPFIT is the pool of cyber-criminality that it engendered, albeit unintentionally, but perhaps, deliberately. Since this ‘canine tooth’ is neither naturally purposive nor functionally positive nor socially desirable, its development and existence require an analytical retrospective understanding, with a view to forestalling such avoidable policy errors in other cases. The question, then, is ‘how did the National Policy for Information Technology facilitate cyber-criminality in Nigeria?’ Towards getting a plausible answer to this question, the Policy will be dissected to see how any of its provisions could have contributed to the cyber crime phenomenon in the country.

A Section-by-section Analysis of the Policy
On the Nigerian scene, the activities of cyber criminals have become a worldwide ugly phenomenon. The government of the Federation in 2001 commissioned a body of experts to design a National Policy on Information Technology. The policy was expected to deal with all emerging issues in the information and communication technology fields. It is however to be noted that the resultant policy does not offer much for the understanding, prevention and eradication of criminal activities in cyberspace. In effect, the policy has not shown a sufficient commitment on the part of government to deal with the problem of cyber-criminality in the country. In particular, the task of the ‘IT Task Force’ that was recommended in the Policy is not specified, while no financial allocation was provided for the Task Force in the spending profile of the policy for combating crimes on the Internet. This observation is without prejudice to the correct perception of the Policy that

Information Technology (IT) is the bedrock for national survival and development in a rapidly changing global environment, and challenges us to devise bold and courageous initiatives to address a host of vital socio-economic issues such as reliable infrastructure, skilled human resources, open government and other essential issues of capacity building.

A close study of the Policy’s ‘General Objectives’ reveals the Policy’s weakness in dealing with the menace of cyber-criminality. The sections of the Policy that pertain directly or in some indirect way to cyber-criminality are discussed below. General Objectives section “(vii): To improve judicial procedures and enhance the dispensation of justice…” “(xv) to empower the youths with IT skills and prepare them for global competitiveness…” and “(xvii) To create IT awareness and ensure universal access in order to promote IT diffusion in all sectors of our national life…”

Considering the high incidence of cyber-criminality in Nigeria today, the three objectives above rather than forestall or address the issues of cyber-criminality appear to be contributory to the commission of cyber crimes. The improvements of judicial procedures and enhanced dispensation of justice, on their own, do not address the
commission or prevention of crimes as such. On the other hand, the empowerment of the youths with IT skills and the diffusion of IT have exposed the youths to the possibilities and ease of committing financially lucrative and hard-to-detect criminal activities on the Internet.

The objective (xxi) of enhancing “national security and law enforcement” appears to be vacuous with respect to cyber-criminality. The Policy also has an objective (xxiii) of promoting “legislation (Bills and Acts) for the protection of on-line business transactions, privacy and security.” This appears to be the most pertinently framed objective of the policy. However, this objective appears to be no more than a gratuitous inclusion in the Policy as shown in the failure of the government to enact the Cyber Crime Bill that had been in the National Assembly since 2004. Moreover, to date, the country does not have any cyber crime-specific law that had been enacted since the advent of the NPFIT and its attendant cyber-criminality.

In further clarifying its objectives, the policy defines ‘Information Technology’ to mean “computers, ancillary equipment, software and firmware (Hardware) and similar procedures, services (including support services) and related resources.” The term ‘IT’ is also defined to include “any equipment or interconnected system or sub-system of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information.” This comprehensive definition captures well all imaginable uses, and abuses, of the cyberspace. Further relevant to cyber-criminality and explanatory of the policy are its chapters 9, 12, 13, 14, 16 and Appendix B.

Chapter 9 section 9.3 (‘Strategies’) states: “(i) Provide a sound responsible and efficient regulatory environment.” At (4), it states: “providing legal safeguards for the privacy of individuals and the confidentiality of transactions against misuse.” In Chapter 12 (“National Security and Law Enforcement”), the pertinent issues are in Section 12.3 (“strategies”) of the NPFIT. These are (i) to use IT “to combat contemporary and emerging security threats and challenges that are being re-defined by Information Technology”; and (ii) to promote “the awareness and education of all those engaged in National Security and law enforcement duties on the use, benefit and risks of new IT environment.” The policy also proposed (iii) to inform and protect Nigerians, the government, infrastructure and assets “from illegal and destructive activities found in the global environment” in order to boost the confidence of Nigerians and the international community in the country. In (iv) the policy says: “Government … will frame appropriate legislation.” Chapter 13 of the IT policy, on legislation, reiterates the proposition (iv) in Chapter 12.3. It states: “The nation shall promote and guarantee freedom and rights to information and its use, protect individual privacy and secure justice for all by passing relevant Bills and Acts.”

The objectives of legislation, as stated in the policy, are to facilitate e-governance, e-commerce, secure e-fund transfer and electronic payment system, and protection of government’s digitalized records and information. Other objectives include establishing and enforcing ‘cyber laws’ to deal with ‘computer crime’. Cyber legislation, according to
To realize the foregoing legislative objectives, the strategies of the IT policy are stated as follows. The National Information Technology Development Agency (NITDA) and the Federal Ministry of Justice are to work out Bills and Acts that would bring about free access and rights to information, and other on-line transactions, with due protection, security and property rights, for individuals as well as for groups. The policy would also seek to introduce the necessary machinery for verifying and admitting in evidence electronically generated records and digital evidence in the event of administrative and legal proceedings, which will be digitalized as much as possible. Also very important in the policy is the plan to review relevant existing laws to make the implementation of the IT policy unhindered. The policy will, in addition, see to the passage of 'Computer Crime and Cyber Laws (CCCL)'. In chapter 16, ("policy implementation"), the policy at 16.2 (xxi) restates that it will see to the enactment of "Bills and Acts to stimulate and protect the right of users and developers including intellectual property rights."

Towards realizing the above objectives, the policy, in Appendix B (Details on the Legal Areas that must be addressed"), states inter alia:

Government through the Federal Ministry of Justice, after due deliberation with IT and sectoral experts, will frame appropriate legislation, using technology-neutral statutory definitions. The legal mechanisms so framed are to apply in the following areas: computer crimes, information technology law, and amendment of non-specific provisions in existing laws. Other areas of application are personal privacy and digital signature.

Significant as the IT policy is, it is noteworthy that the Nigerian state did not take any definite regulatory step on it until 2003, whereas the ICT media proposed in the Policy had become widely available since 2001. It was not until a murder incident at a Nigerian embassy in 2003, which was connected to an Internet crime, that the Federal Government was moved to constitute a cyber crime working group, the Nigeria Cybercrime Working Group (NCWG), to examine all associated problems of cyber-criminality as related to Nigeria and make appropriate submissions to government on how to nip them in the bud. This body was formally launched on 31st March 2004 (by which time the menace of crime on the Internet had become firmly entrenched among a large segment of Nigerian ICT buffs), sequel to the recommendations of the Presidential Committee on Illegal On-line activities led by the National Security Adviser to Ex-President Olusegun Obasanjo (1999-2007).

The NCWG was a high powered Inter-Agency group. Its members were drawn from all the critical law enforcement, security, intelligence, and ICT agencies of the government. The group also had major organized private ICT sector stakeholders as members.
Specifically, the Group had as co-chairpersons the Attorney-General of the Federation and Minister of Justice, and the Minister of Science and Technology. The Inspector General of Police, the Chairperson of the Economic and Financial Crimes Commission (EFCC), the Director-General of the State Security Services (SSS) and the Director-General of the National Intelligence Agency (NIA) were also members of the group. Other members were the Executive Vice-Chairman of National Information Technology Development Agency (NITDA), the President of the Nigerian Computer Society, the President of the Nigerian Internet Group, and the President of the Internet Service Providers Association of Nigeria. The effort of the working group resulted in a draft Cybercrime Bill that is before the National Assembly. This is the draft bill that the National Assembly has not been able to pass into law since 2004.

The commissioning of the policy could be seen as a manifestation of the Nigerian government’s awareness of the pivotal role of information and communication technologies in the contemporary world. This awareness of government was well captured in the Policy thus: “Information Technology (IT) is the bedrock for national survival and development in a rapidly changing global environment.” Cognate to this governmental awareness, the IT policy focused on some areas that should be covered by appropriate laws. Of particular relevance here is the section of the IT policy on Information Technology Law. This section purposes to:

Criminalize the use of computers and related technologies for the commission of crimes or to facilitate criminal behaviour, wrongful access, and deceitful usage; and criminalize the targeting of computers and the data contained within them through an authorized access, unlawful copying of information, damage or tampering with such information, and/or depriving the legitimate owner of data of the benefit of such data.

Wide-ranging in its coverage of cybercrimes as this aim of government was, nothing was done towards enacting either an Information Technology Law or a Computer Crime Law until 2004 when the NCWG was created. The NCWG, a unit of the National Information Technology Development Agency (NITDA), worked out a foundation for a cybercrime law for Nigeria. As proposed, the envisaged law would include a substantive law that would criminalize the following kinds of conduct: (i) Conducts against information and communication technology (ICT) system, (ii) Conducts using ICT systems as tools for committing crime, and (iii) Legally prohibited conducts that have essential ICT infrastructures as targets. It will also contain some procedural provisions that deal with investigation of crime, collection of evidence relating to cybercrime as well as procedures for searches, seizures and interception of digital communication. The third component of the proposed law is an array of options on infrastructure and institutional arrangement. The details of this component are: (i) promote and develop specialized units to deal specifically with ICT offences, as units of existing law enforcement formations, (ii) facilitate cooperation between industry and law enforcement agencies, (iii) create an advanced ICT centre to collect, collate, analyze, and circulate relevant technical information to and for other relevant Agencies, and (iv) if
need be, create an entirely new cybercrime and cyber security agency at par with other specialized agencies like EFCC, ICPC, NDLEA, NAPTIP, NACA and NAFDAC.  

The NCWG had a correct perception and apprehension of the enormity of the problem of cybercriminal as reflected in the conclusion of its report as follows.

Enforcing cybercrime (sic) in Nigeria is a necessary compliment (sic) to the great strides the Nigerian Government has made towards transforming Nigeria into an ICT–driven economy. To leave our systems and networks unprotected is to deliberately endanger the same infrastructures we worked so hard and invested so much to build.  

The lofty ideal encapsulated in this statement is in the right direction and in accordance with what obtains in the highly more technologically and economically advanced countries. However, the government has not shown an enthusiasm for the required urgency to midwife the cybercrime law. This, it is concluded, is a further reinforcement of the negative impact of the 2001 IT Policy in engendering and facilitating cyber-criminality in Nigeria over the past decade.

Conclusion
In the light of the foregoing analysis and in juxtaposition with the Nigerian experience of cyber-criminality, it is to be noted that the NPFIT is a regrettable case of developing cyber capacity without cyber security. The Policy had focused on only the projected possible benefits of ICT, without being critically sensitive to the possibility of IT abuse, and thus failing to be pro-active against IT abuses that were already been experienced and being combated in other places.

Whereas cyber capacity and cyber security ought to be concurrent, the Policy really created a wide time-lag between the two aspects. This gap between IT empowerment and IT security enabled many creative minds to implement the ‘wealth-creation’ objective of the Policy in a non-legal way to their own selfish advantage. This continues to be in the form of Internet scams of various types for which Nigeria is very well known worldwide, and which were previously un-associated with, and generally unknown in, Nigeria before the advent of the NPFIT and the consequent uncontrolled availability of the Internet in the country. Those willing to become rich through fraud learnt very fast how to exploit the weaknesses inherent in the features of the Internet that the Policy did not provide safeguards against.

Although other countries, including the most ICT-advanced countries, also have cyber security challenges, Nigeria, being a latecomer into the technology, ought to have started right in the formulation of a Policy that benefited from the experiences of others whilst still planning to enter into the global cyber community. Failure to do this has resulted in the unstoppable life of cyber crime that some Nigerians have chosen as a profession.
The NPFIT, as experience has shown, is a classical example of uncritical policy design, being not based on adequate research and thus being unmindful of clearly foreseeable social consequences. Whatever moves are now being made, or planned to be made, are no more than panic measures, which only further highlight the error of the Policy. It is to be hoped, therefore that policy makers will always consult widely and undertake detailed critical credible research into all relevant aspects of their terms of reference, and refrain from rushing to produce populist political policies that end up injuring, rather than benefitting, the society.

Finally, that the security deficiency of the NPFIT is ultimately responsible for the explosion of cyber criminality in Nigeria may not be obvious or self-evident, especially as attempts have not been lacking to give some other causal explanations for the cyber crime phenomenon for which the country has become sadly associated world-wide. Hence, critical attention needs to be given to the outlined pertinent linkages between the Policy and cyber crime in Nigeria. To recap, prior to 2001, when the Policy came into effect, Nigerians in Nigeria only heard and fantasised about the Internet and associated communications technologies, such as the mobile phone. Personal computers were also, pre-2001, not a common sight, both in offices and in homes. Hence, although economic and financial crimes were being committed in conventional 'manual' ways, the opportunity for cyber or Internet-facilitated crimes, especially financial scams, was incontrovertibly absent within the shores of the country. The concepts of Internet activities (lawful and criminal), Internet law and associated procedures – crime-detection, investigation, prosecution, and conviction – were unknown to the citizenry, including judiciary and law-enforcement personnel. In effect, prior to 2001 and the National ICT Policy, Nigerians were practically unaware of the Internet and its fullness as attested by the global history of cyber criminality.

As has been recognised over and over again, and as again recently reiterated, a successful ICT programme requires very careful planning and implementation. For instance, as noted at an NICI (National Information and Communication Infrastructure) workshop that was facilitated by many international development agencies, including the Economic Commission for Africa (ECA) and the United Nations Development Program (UNDP), which was held at Abuja, Nigeria in March 2010, “Careful planning leads African nations in the proper direction. The successful implementation of a national ICT plan…requires a great deal of planning on the part of the government.” It is surprising, therefore, that in spite of the reported apparently elaborate plans leading to the formulation of the NPFIT, adequate proactive cyber security plans against cyber attacks were not included in the Policy.

The argument of this paper is further strengthened when the NPFIT is compared with other sub-Saharan national ICT Policies of about the same period (around 2000 – 2003), such as those of Uganda, South Africa, Ghana, and Zambia that have clearly integrated cyber security and regulatory provisions from the outset, which have been followed with comprehensive cyber crime laws, and consequently, those other countries have far lower records of cyber crimes than Nigeria. The continuing failure of Nigeria’s National Assembly to enact a single cyber crime law or a cyber security law
since 2004 and 2008, respectively, in spite of the country’s unenviable high cyber crime profile, is a further indication of the NPFIT’s inadequacy to provide the required environment for cyber security in Nigeria. In particular, the Policy lacks an incorporation of lessons learned from other nations and global experiences. The Policy is also bereft of a concern for promoting best practices with respect to safety and security of Internet users, content and infrastructure. While these security gaps are now proving more difficult to plug in the country’s ICT environment than ordinarily would have been, as rightly acknowledged by the Computer Professionals of Nigeria (CPN), among others, cyber criminals in the country continue with their nefarious activities with impunity.

It is submitted, therefore, that the failure of the NPFIT to make explicit proactive provisions for cyber security measures, prior to, concomitant with, or immediately after its implementation (even though copious relevant information on the need for such security provisions was at the time freely available) is the root cause of the emergence and prevalence of cybercrime in Nigeria. The implementation of the Policy in 2001 facilitated a proliferation of cyber cafes and mobile electronic devices, and an army of “youths and thousands of unemployed but highly knowledgeable ones who are computer savvy”, who have now acquired sophisticated IT skills in an unregulated cyber environment. The immediate consequence of this was, according to Ribadu, the emergence of a new pattern of criminal behavior that had as early as 2002 become so pervasive and so conspicuous in the form of a “myriad offences under its omnibus cybercrime definition that straddle matters of data interference, system interference, illegal interception, illegal access and the misuse of devices in the very typology derived from the characterization of the Council of Europe.” Hence, had the Policy not been implemented, or had it been implemented with all the necessary security and legal provisions that it should have contained (based on global experiences from other IT advanced parts of the world), the undesirable cybercrime situation in Nigeria could either not have existed or not have been as bad as it has been since 2002.

About the Author
Mrs. Roseline Obada Moses-Ôkè received her BA (Philosophy), LLB, and LLM from the Obafemi Awolowo University, Ile-Ife, Nigeria, and was called to the Nigerian Bar in 2008. She is currently pursuing a Doctor of Laws (LLD) degree at the Faculty of Law, North West University, South Africa. The author can be contacted at rosenhillmoke@yahoo.co.uk.

References


15. NPFIT, 2001: ii


25. Ibid, Appendix B; 47.
29. Ibid, 10 & 16.
30. Ibid, 18.
31. This consists mainly of crimes of persuasion, with financial gain as the sole motive and objective. See: Nuhu Ribadu, above; also, http://www.crimes-of-persuasion.com/Nigerian/scammer, (accessed on 26 June, 2011).
35. Nigeria has remained consistently ranked in the third position in global ratings of cyber crime countries after the USA and the UK.
37. Among such IT and cyber security-specific information available before the advent of the Policy are the following:


Stein Schjolberg, Computers and Penal Legislation – A Study of the Politics of a new Technology, Complex 3/86, Universitetsforlaget (1986);

Ulrich Sieber, (ed), Information Technology and Crime – National Legislations and International Initiatives, Cad Verlag KG (1994);


United Nations, *Combating the Criminal Misuse of Information Technologies*, United Nations General Assembly (UNGA) Resolutions 55/63 (2000);

United States Government, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*, March 2000, see: www.cybercrime.gov, (accessed on 13 April, 2009); and


39. Ibid.