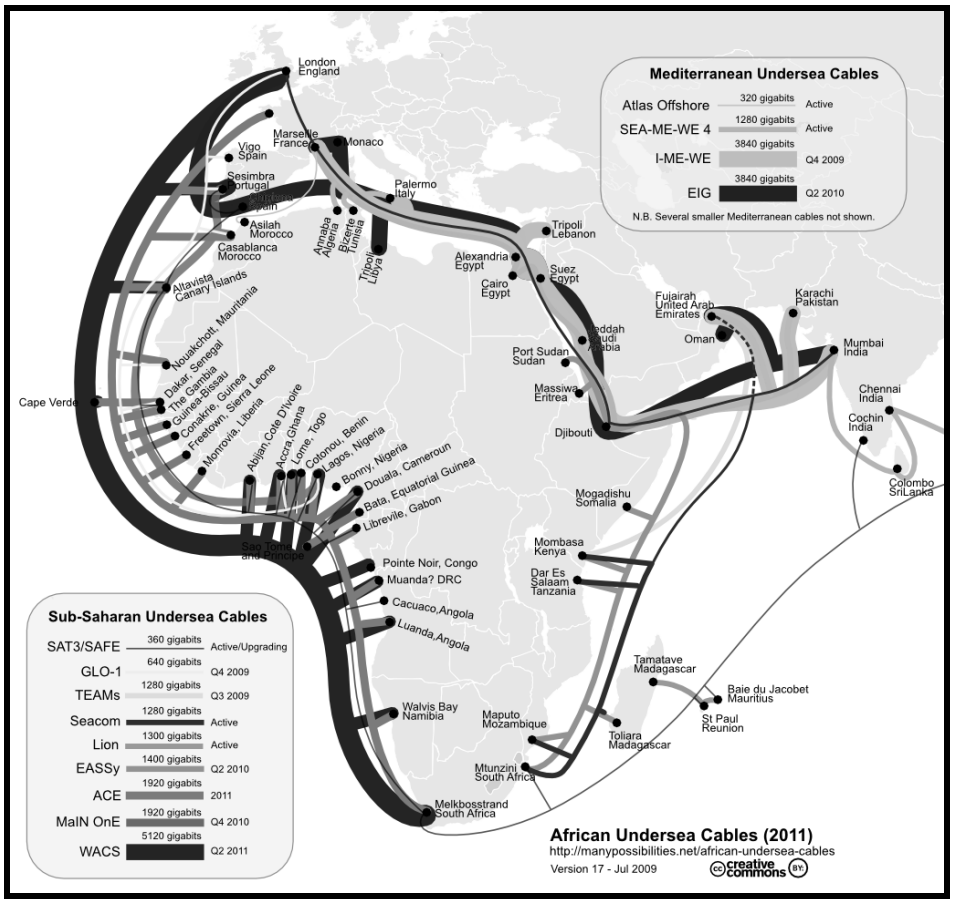

Figure 3. Final African undersea cables [20]

The SEA Cable System, referred to as Seacom, will provide African retail carriers with equal and open access to inexpensive bandwidth. Not only will this remove the international infrastructure bottleneck, but it will also support African economic growth [5], dramatically reduce the cost of bandwidth, reduce the Round Trip Times (RTT) and increase the connection capacity to reduce current congestion. This new cable will contribute to the development of telecommunication networks in Africa.

A. Increased broadband access in Africa

Although the arrival of broadband had a tremendous effect on the world's internet use, the focus currently is on the effect that increased broadband access have on Africa. World Wide Worx predicted that the arrival of the Seacom undersea cable will increase South Africa's maximum international bandwidth 50-fold. "South Africa's Internet population is expected to grow as much in the next five years as it has in the 15 years since the Internet became commercially available in SA".

According to Symantec's annual Internet Security Threat Report, an increase in broadband speeds is directly proportional to a spike in cyber crime [11]. The expectation is thus that Africa will soon see more cyber crime activity in its cyber space.

B. Influence of broadband access on cyber threats and trends

Due to the international nature of cyber space, the effect of cyber crime in Africa cannot be considered in isolation. The effect and influence of broadband access have a wider impact on (global) cyber threats and trends as well.

The increasing broadband usage creates a favorable environment for increased cyber space criminal activities. Not only are there potentially more victims, but the technology is faster, allowing more virus distributions and infections [21]. Currently, South Africa's internet broadband penetration is at two percent, far below the global average of 22.5 percent [22].

Kaspersky Lab's EEMEA Global Research and Analysis Team says: "Experience seems to indicate there is indeed a link between the connectivity of a country and its subjectivity to cyber crime" [11]. To illustrate, in 2003 South Korea was one of the countries most severely affected by the Slammer worm. Since most of the people in South Korea had high-speed Internet links at home, the Slammer worm was easily distributed through networks. These high-speed Internet links only became common to other countries a few years later, in effect preventing a severe Slammer infection. On the other hand, broadband Internet access was banned in North Korea to curb the illegal downloading of Western movies [23].

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

There are different opinions on the potential influence that the increased broadband access may have on cyber crime. Although Sophos reckons that the increase in cyber crime may not be as dramatic due to caps and cost, the South African DoC's broadband policy aims to increase broadband affordability [12]. Should this affordability be realized, Africa might see a dramatic upsurge in cyber crime once faster broadband speeds come to the country, and the prices come down. However, regardless of the cost involved, more Internet connections mean more opportunities to be exploited. Fig. 4 shows the comparable cost of broadband Internet access in countries across the world. Currently, bandwidth in Africa is the most expensive [20].

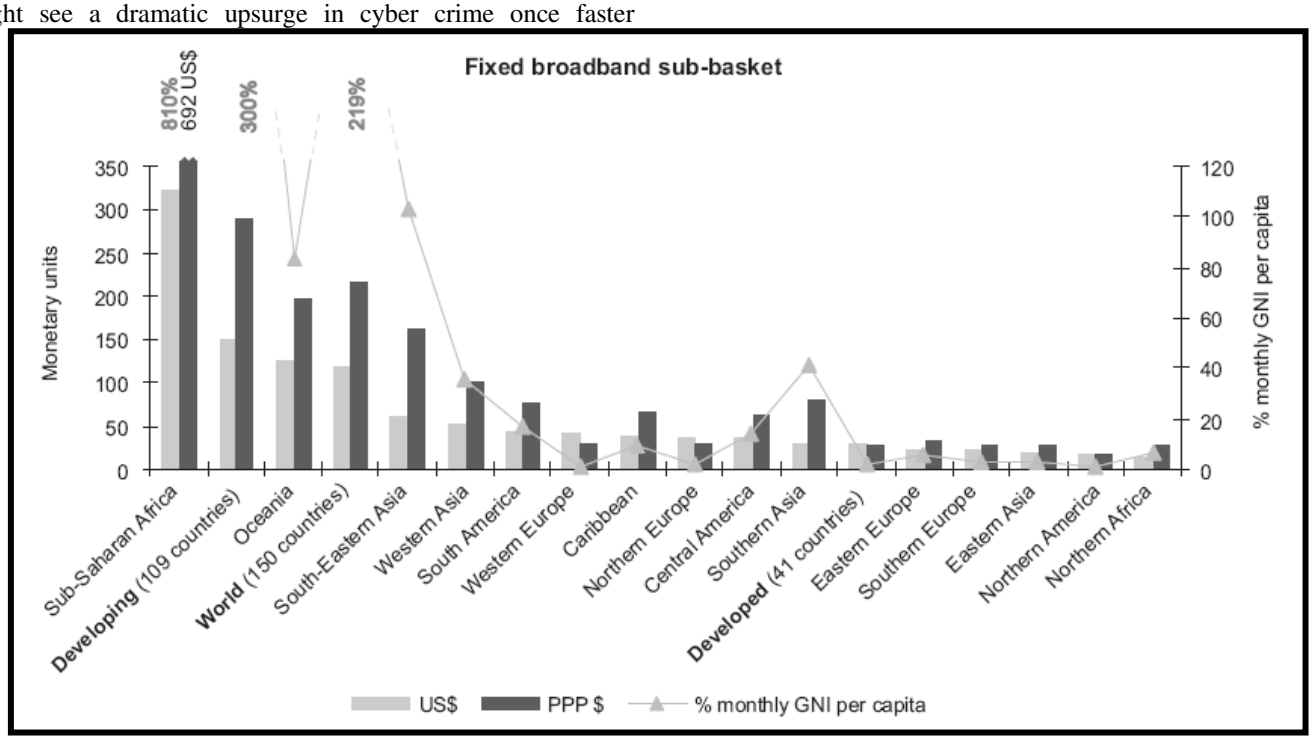

Figure 4. Cost of broadband Internet access in countries of the world [20]

The next sections will look at the influence that increased broadband access may have on the earlier identified primary and secondary cyber space threats and trends.

1) Influence of broadband access on IT education shortage

With the increase in broadband access, millions of new, computer-illiterate users will be able to connect to the Internet through the Seacom cables. Chances are that the devices used to connect may be unprotected, furthering the existent cyber crime statistics. "Newly-connected computers that are unprotected will be rapidly compromised and used to launch attacks on other computer systems across the globe" [11].

An increase in broadband access will give Internet access to more users in Africa. If the increase and distribution of IT education of these users do not match the increase and distribution of the broadband access, the existent lack of IT know-how may be exploited.

IT education should reach both computer users in the rural areas, as well as current computer users in urban areas that are currently risk proofed by slow download times. "Fast increasing broadband penetration such as we are seeing locally can be dangerous, as many South African companies are not security-savvy enough to be able to thwart attacks successfully" [11].

2) Influence of broadband access on absence of African languages

An increase in broadband access will give Internet access to more users speaking an African language. If these users are not educated in the global English language, or more Internet content published in African languages, these users might be vulnerable to cyber attacks due to miscomprehension. The unfortunate reality is that innocent Web surfers can visit a compromised website and unknowingly place their personal and financial information at risk.

The absence of African languages in cyber space has an indirect impact on the amount of crime taking place in cyber space. "… While western countries have partially learned to neutralize the threat of computer viruses, Africa has become a hive of Trojans, worms and exploiters of all stripes. As PC use on the continent has spread in the past decade (in Ethiopia it has gone from 0.01% of the Ethiopian population to 0.45% through 1999-2008), viruses have hitched a ride, wreaking havoc on development efforts, government programmes and fledgling businesses …" [10].

Unfortunately, a vulnerability in the network rarely stays isolated and may put the rest of the African network and internet population at risk of cyber attacks.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

3) Influence of broadband access on OS distribution

An increase in broadband access may not have a direct influence on OS distribution. As the market share leader, Microsoft's Paul Cooke suggests the support of pirated versions of Windows 7 with patches [25]. "… There seems to be a link between the Internet speed and software piracy rate. In countries that are poor and Internet cheap, people can download pirate software from the Internet, together with movies and music. These are between the most successful attack vectors for malware" [11]. Some of the most famous incidents of malicious software infection have come after security updates were publicly available from Microsoft, e.g. Blaster, Conficker and Sasser.

Although the solution suggested by Cooke is ideal from a community perspective, the onus remains solely on Microsoft to provide the necessary support. This will only be a viable solution if Microsoft makes this commitment for all Windows computers, and anti virus organizations such as Symantec and McAfee offer free subscriptions on a project-by-project basis. "If there isn't a global response to this threat before mid-2010, we will all come to regret the consequences, and global corporations who could afford to act and didn't, should be held accountable in the aftermath" [25].

4) Influence of broadband access on lack of standardised procedures

An increase in broadband access may potentially emphasize the current lack of standardized procedures. With more users connected to the Internet, and potentially more occurrences of cyber crime, it will be even more urgent to get consensus on how to handle cyber crime in a court of law. Without standardized procedures, this classification is left to the discretion of the judges and is not applied consistently throughout Africa, let alone the world.

It is necessary for law enforcement agencies and judiciary in the African continent to devise ways of curbing Internet fraud and enhancing their skills in computer security and risk management [26]. This is the only way to counter the current lack of standardized procedures.

5) Influence of broadband access on Trojans, viruses, spam and botnets

An increase in broadband access may potentially increase Trojan, virus, spam and botnet activity in Africa. Not only will more users in Africa be vulnerable to attacks, but with faster Internet access, these users' computers may be used in remote attacks and spam distribution. "South Africa currently has a relatively small Internet population due to the historically high broadband prices, but this is all set to change. Millions of new people and new devices are going to be connecting to the Internet as prices tumble and capacity booms, few of which will be properly prepared for the barrage of Trojans, viruses, worms and hacks." [11].

Africa is home to about 100 million PCs, 80% of which are estimated to be infected with some kind of malware. This malware infestation is partly due to the intense poverty throughout the continent directly contributing to the inability to pay for anti virus protection and the pervasive distribution of pirated software.

Although the high percentage of malware-infected computers is a dire problem, the current situation is that most Internet access occurs via dialup. With the increased broadband access planned for 2010/2011, these unprotected computers will become an easy target for bot herders [25].

IV. COMBATING CYBER SPACE CRIME IN AFRICA

"The worldwide information infrastructure is today increasingly under attack by cyber criminals and terrorists - and the number, cost and sophistication of the attacks are increasing at alarming rates… With annual damage around the world now measured in billions of US dollars, these attacks threaten the substantial and ever-growing reliance of commerce, governments, and the public upon the new technology to conduct business, carry messages, and process information." [27].

Throughout Africa, a lack of understanding, education, training, unclear policies of government, insufficient Information Security and low confidence exhibited in Africa's e-business poses potential problems for cyber space safety and security [26]. With this rising number of cyber crimes, it is imperative to take specific counter measures to address crimes in cyber space. Some of the identified countermeasures include specific cyber space initiatives, Computer Security Incident Response Teams, and cyber security awareness campaigns.

A. Cyber space initiatives

A number of international and Africa specific initiatives address cyber crimes. In her 2008 budget vote speech, Dr. Ivy Matsepe-Casaburri (former South African Minister of Communication) said that the issue of cyber security is high on South Africa's national agenda. Initiatives such as the International Telecommunication Union (ITU) High Level Expert Group (HLEG) aim to develop strategies and guidance to countries in dealing with cyber crime [3]. [More information on this initiative can be found at http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.]

Participants from various African countries attending the 2006 International Conference on Computer Security and Cybercrime in Africa established the African Information Security Association (AISA). This initiative was established with a view to promote knowledge and create awareness about computer security and cyber crime on the continent. AISA aims to promote global best practices in information, computer and Internet security, campaign against cyber crime, conduct annual survey on Information Security, promote legislation and regulations and create linkages and networks in Africa [26]. [More information on this initiative can be found at http://www.jidaw.com/security/aisa/aisa.html.]

Another initiative is Computers for Africa (CFA) that promotes sustainable information and communications technology development in rural African communities. The program is developed by African and USA personnel, and is

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

based on American volunteers refurbishing computers into ready-to-set-up labs. The disadvantage and potential negative influence of this approach is that the consistent importing of old computers into developing countries may turn these countries into dump sites for electronic waste [6]. [More information on this initiative can be found at http://www.computers4africa.org/.]

Another cyber space initiative is One Laptop per Child. This initiative is trying to create educational opportunities for the world's poorest children by providing each child with a rugged, low-cost, low-power, connected laptop with content and specifically designed software [6]. [More information on this initiative can be found at http://laptop.org/en/.] Both the CFA and One Laptop per Child initiatives attempt to minimize the digital divide as a starting point to combating cyber space crime in Africa

B. Computer Security Incident Response Teams

A Computer Security Incident Response Team (CSIRT) is a team of dedicated Information Security specialists that prepares for and responds to Information Security incidents. It is a well-established practice among network security specialists and dates back to the 1980's. South Africa is unfortunately lagging behind the rest of the world in this regard. It currently does not have a national CSIRT. In the whole of Africa only Tunisia, Egypt and Kenya have a CSIRT.

The Internet has become a global network, which gives great opportunities for businesses to create and develop new innovations, business models and services. On the other hand, it also gives opportunities for criminals to use the Internet with malicious intentions and activities. Therefore, the capability for quick incident handling and international incident coordination becomes essential.

Developing countries that do not have proper skills and organizations relating to incident response, are vulnerable and a big risk for other countries as well. These kinds of countries are an easy target for criminal activities in the form of botnets for example. Therefore establishing a national CSIRT capability throughout Africa will have promising crime combating effects.

C. Cyber security awareness campaigns

"Computer security and cyber crime awareness should be created with a view to sensitizing all users of the Internet facility with the emerging indicators of crime and fraud being committed through computer" [26]. To prevent innocent South Africans from becoming victims of internet-related attacks, intensive awareness campaigns need to be developed and launched in South African areas that only recently became connected to the internet.

If these South Africans are not properly educated, their technology devices may remain unprotected. This may leave the South African internet infrastructure vulnerable to attacks, posing a severe threat to national security. The Council for Scientific and Industrial Research has recently launched such a project to educate novice internet and technology users specifically with regard to basic security.

In this specific impact project, national security will be promoted through awareness training focusing on the newly released broadband capability and knowledge transfer within rural communities of Limpopo. The project identified primary schools, secondary schools and community centres that already have computer facilities, but not the necessary cyber skills.

The premise of this project is to provide the necessary basic skills to individuals that have only recently been introduced to computers and the cyber world. The awareness training will assist these individuals in utilizing computers and the internet for their own benefit (e.g. internet banking, eFiling for SARS), whilst protecting both the communities and the larger national state from unnecessary making the network vulnerable through a lack of knowledge. This project can be extended at a later stage to other rural and urban communities within South Africa.

With the importance that information plays in the everyday environment, information and cyber security plays a key role in the maintenance of national security. In this regard, information and cyber security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. By educating individuals and making them aware of the potential dangers that come with the use of broadband, it may help to limit the scope of cyber crime in South Africa.

V. CONCLUSION

The contribution of this paper is in its view of the known, obvious matters in a very specific environment. With the rising number of cyber crimes, it is imperative to take specific counter measures to address crimes in cyber space. An increase in broadband access will give Internet access to more users in Africa. With the increase in broadband access, millions of new, computer-illiterate users will be able to connect to the internet through the Seacom cables, potentially making the entire network more vulnerable to cyber threats and attacks.

There are different opinions on the potential influence that the increased broadband access may have on cyber crime. Although some reckon that the increase in cyber crime may not be as dramatic due to caps and cost, others have the opinion that more users in Africa will be vulnerable to attacks, and with the faster internet access, these users' computers may be used in remote attacks and spam distribution.

To combat cyber space crime in Africa, three routes can be followed: maintaining and supporting specific cyber space initiatives, establishing an operational CSIRT, and educating individuals on the potential dangers of cyber space. At the moment, a thorough and updated understanding of the current and future threats and trends of cyber space crimes is a step towards solving the problem.

REFERENCES

[1] KILLCRECE, G., RUEFLE, R. & ZAJICEK, M. 2003. State of the Practice of Computer Security Incident Response Teams [online]. URL: http://www.educause.edu/Resources/StateofthePracticeofComputerSe/153687 (Accessed 16 October 2009).

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

[2] ZUMA, J.G. 2009. State of the Nation Address by His Excellency, JG Zuma, President of the Republic of South Africa; Joint Sitting of Parliament, Cape Town [online]. URL: http://www.parliament.gov.za/content/SONA3June2009.doc (Accessed 16 October 2009).

[3] CYBER CRIME AFRICA SUMMIT. 2008. Successful strategies to combat, prevent and Investigate Cyber crime in Africa [online]. URL: http://www.oppiweb.com/suid-afrika/index.php?topic=354.0;prev_next=next (Accessed 18 November 2009).

[4] VEERASAMY, N. & TAUTE, B. 2009. An introduction to emerging threats and vulnerabilities to create user awareness. ISSA 2009 Conference, 6-8 July 2009, University of Johannesburg, South Africa.

[5] INTERNET WORLD STATS. 2009. Internet Usage Statistics for Africa (Africa Internet Usage and Population Stats) [online]. URL: http://www.internetworldstats.com/stats1.htm (Accessed 1 April 2010).

[6] MILICEVIC, M. 2008. Cyber space and globalization [online]. URL: http://www.ais.up.ac.za/digi/docs/milicevic_paper.pdf (Accessed 19 October 2009).

[7] FOSSI, M., JOHNSON, E., TURNER, D., MACK, T., BLACKBIRD, J., MCKINNEY, D., LOW, M.K., ADAMS, T., LAUCHT, M.P. & GOUGH, J. 2008. Symantec report on the underground economy. Symantec, 2008.

[8] CHIZOBA, O.M. 2005. Cyber crime [online]. URL: www.takingitglobal.org/action/projects/download.html/4926/CYBER%20CRIME%20ABUJA.doc (Accessed 4 April 2008).

[9] MAIL & GUARDIAN. 2008. Cybercrime syndicate swindles govt out of R199m [online]. URL: http://www.mg.co.za/article/2008-06-10-cybercrime-syndicate-swindles-govt-out-of-r199m (Accessed 18 November 2009).

[10] MICHAEL, C. 2009. Computer viruses slow African expansion. guardian.co.uk [online]. URL: http://www.guardian.co.uk/technology/2009/aug/12/ethiopia-computer-virus (Accessed 5 October 2009).

[11] DOYLE, K. 2009. Could SA lead cyber crime rankings? ITWeb [online]. URL: http://www.itweb.co.za/index.php?option=com_content&view=article&id=27948:could-sa-lead-cyber-crime-rankings (Accessed 17 November 2009).

[12] MYBROADBAND. 2009a. Affordable broadband for all [online]. URL: http://mybroadband.co.za/news/Broadband/9809.html (Accessed 18 November 2009).

[13] MUSINGUZI, B. 2008. African languages absent in cyber space. AllAfrica.com – The Monitor [online]. URL: http://allafrica.com/stories/200804081119.html (Accessed 12 October 2009).

[14] BILLON, M., MARCO, R. & LERA-LOPEZ, F. 2009. Disparities in ICT adoption: A multidimensional approach to study the cross-country digital divide. Telecommunications Policy. 33. Pp 596 – 610.

[15] WITSA. 2000. Cyber crime … and punishment? Archaic Laws Threaten Global Information [online]. URL: http://www.mcconnelli nternational.com/index.php?option=com_content& view=article& id=10&Itemid=6 (Accessed 24 August 2009) p4.

[16] MARKET SHARE. 2009. Operating system market share [online]. URL: http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=8&qptimeframe=Y&qpsp=2009&qpmr=100&qpdt=1&qpct=3 (Accessed 14 August 2009).

[17] PATRIZIO, A. 2007. Report says Windows gets the fastest repairs [online]. URL: http://www.internetnews.com/security/article.php/3667201 (Accessed 18 November 2009).

[18] SOPHOS. 2009. Security threat report: July 2009 update. Sophos: Boston.

[19] CAMBINI, C. & JIANG, Y. 2009. Broadband investment and regulation: A literature review. Telecommunications Policy. 33. Pp 559 – 574.

[20] COTTRELL, R.L. & KALIM, U. 2009. New E. Coast of Africa Fibre [online]. URL: https://confluence.slac.stanford.edu/display/IEPM/New+E.+Coast+of+Africa+Fibre (Accessed 18 November 2009).

[21] HALBHEER, R. 2009. The Africa cable – a chance for Africa! – A threat for the internet? InformationSecurity.com [online]. URL: http://www.infosecurity-us.com/blog/2009/10/7/the-africa-cable--a-chance-for-africa--a-threat-for-the-internet/28.aspx%20- (Accessed 3 October 2009).

[22] MYBROADBAND. 2009b. SA broadband penetration poor: Minister [online]. URL: http://mybroadband.co.za/news/Broadband/10526.html (Accessed 25 November 2009).

[23] RUIZ, M. 2006. Internet law – Kenya, Uganda and Tanzania adopt cyber laws [online]. URL: http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1539 (Accessed 27 November 2009).

[24] SYMANTEC. 2009a. Symantec internet security threat report finds malicious activity continues to grow at a record pace. Press release [online]. URL: http://www.symantec.com/about/news/release/article.jsp?prid=20090413_01 (Accessed 17 November 2009).

[25] INTELLIBRIEFS. 2009. Africa – home of the world's largest cyber pandemic [online]. URL: http://intellibriefs.blogspot.com/2009/10/africa-home-of-worlds-largest-cyber.html (Accessed 8 October 2009).

[26] AKINSANMI, G. 2006. Fight against cybercrime, legislation as rescue [online]. URL: http://www.cipaco.org/spip.php?article716 (Accessed 18 November 2009).

[27] SOFAER, A.D. & SEYMOUR, E.G. 2001. The transnational dimension of cyber crime and terrorism. Stanford, California: Hoover Institution Press.