Chapter 3

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION IN THE DEVELOPING WORLD

Ian Ellefsen and Sebastiaan von Solms

Abstract Critical information infrastructure protection (CIIP) has long been an area of concern, from its beginnings with the creation of the Internet to recent high-profile distributed denial-of-service attacks against critical systems. Critical systems rely heavily on information infrastructures; a disruption of the information infrastructure can hinder the operation of critical systems. The developed nations have mature CIIP solutions in place, but these solutions are not always suitable for developing countries, where unique challenges and requirements have to be addressed. Meanwhile, the developing nations are experiencing unprecedented growth of their information infrastructures. However, the lack of national CIIP efforts creates a situation for developing nations to become launch pads for cyber attacks. This paper discusses the need for CIIP in developing nations. It examines the current state and future development of information infrastructures in these nations and outlines a number of CIIP requirements.

Keywords: Critical information infrastructure protection, developing countries

1. Introduction

Critical information infrastructure protection (CIIP) is an area of worldwide concern. Developed and developing countries employ a number of critical systems [9]. These critical systems rely heavily on information infrastructures in order to function.

However, the information infrastructure is a single point of failure, where critical systems can be interrupted, and possibly disabled, by disrupting the underlying information infrastructure. The incidents in Estonia in 2007 [22] and Georgia in 2008 [19] have demonstrated the inability of countries to function effectively in the face of cyber attacks on their information infrastructures.

T. Moore and S. Shenoi (Eds.): Critical Infrastructure Protection IV, IFIP AICT 342, pp. 29–40, 2010.

The interconnected nature of systems brought about by the Internet allows cyber attacks to be conducted from anywhere on the globe. Due to advances in technology and growth of their infrastructures, developing nations are being used to launch these attacks. This problem is compounded by ineffective or nonexistent cyber security policies and CIIP solutions.

The development of CIIP structures in developing nations is an issue of vital importance to protect new information infrastructures and to support critical systems. This paper discusses CIIP as it pertains to the developing world. It examines existing protection models and their relevance to developing nations. The current state of affairs in South Africa is presented to set the stage for formulating CIIP requirements in the developing world.

2. CIIP

Critical information infrastructure protection (CIIP) is an issue of vital important to every nation. Developed countries have long had structures in place to protect their critical information infrastructures. Moteff, *et al.* [20] observe that there are a number of different infrastructures that can be considered to be "critical." They define critical infrastructures as those that are "... so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security."

Critical systems, such as electricity distribution, water distribution and financial systems, are of utmost important to the operation of a country [9]. As critical systems become more complex, there is an ever increasing level of interconnection that is required for their operation. Interconnected critical systems heavily rely on information infrastructures. The interconnecting information infrastructures themselves are classified as critical due to the role they play in the operation of other critical systems.

Critical information infrastructures such as the Internet are designed to be fault resistant; however, they can quite easily be affected by events outside the control of a nation's protection structure. A cyber event of sufficient scale can have a detrimental effect on the global operation of the Internet and, thus, critical systems in countries around the world. This section discusses the vulnerability of information infrastructures to cyber attacks that target a nation's critical systems.

2.1 Cyber Attacks

Critical information infrastructures are particularly vulnerable to cyber attacks. For example, large-scale distributed denial-of-service (DDoS) attacks can be initiated quickly using botnets to prevent national systems from operating at full capacity. Such cyber attacks impact information infrastructures and may have significant physical effects.

Cyber attacks can affect countries directly or indirectly. Attacks on infrastructures within one country can have indirect effects on another country; alternatively, a large-scale cyber attack can have global effects. This is largely

due to the interconnected nature of the Internet. Indeed, the world exists in a state of collective vulnerability because of interconnected infrastructures.

The monitoring and management of critical systems that are heavily reliant on information infrastructures are particularly important to mitigate the impact of cyber attacks. The following sections discuss some major cyber attacks, in particular, the Estonian and Georgian incidents, and the DNS root server attacks. These attacks, which impacted the operation of national critical systems, provide insight into the importance of CIIP at the national, regional and global levels.

The Estonian Incident Beginning on April 27, 2007, a series of DDoS attacks were launched against several key computer systems in Estonia. The attacks, which affected the private and public sectors, were executed during a period of civil unrest and increased tension between Estonia and Russia, due to the Estonian Government's decision to move a World War II war memorial. At the time, Estonia blamed Russia for the attacks [5, 6].

The attacks ranged from generic traffic floods to coordinated botnet attacks [22]. Network traffic from the attacks was measured at 90 Mbps for upwards of 10 hours [22]. This had a devastating effect on web access in Estonia.

Even in 2007, Estonia had an extensive information infrastructure structure and relied heavily on Internet services [23]. The attacks disrupted or disabled access to financial institutions, government services and other critical systems, severely impacting the country's ability to function.

The Georgian Incident During the South Ossetia War between Georgia and Russia in August 2008, a number of Georgian governmental and commercial computer systems came under coordinated cyber attacks [10]. These attacks eliminated the ability of Georgian officials to communicate with the outside world [19]. In order to regain the ability to communicate, Georgian officials contracted hosting companies located in other countries, including the United States [10, 19].

Although the attacks on Georgian assets were similar to those that affected Estonia the previous year, they provide insight into the role of the Internet in CIIP. Korns and Kastenberg [19] report that the transfer of key Georgian websites to U.S.-based Internet hosts resulted in portions of the U.S. information infrastructure being affected by the DDoS attacks.

The interconnected nature of the Internet causes other countries to become indirect targets of cyber attacks. While the cyber attacks discussed above were targeted at individual countries, it is conceivable that attacks against the Internet in general could disrupt operations in almost every country around the world.

DNS Root Server Incidents Cyber attacks are not limited to a single country or geographic region; they can have a global impact. This was demonstrated by two DDoS attacks on the Domain Name System (DNS) root servers

that occurred on October 21, 2002 [26] and February 6, 2007 [16]. Although the effects were limited, the attacks demonstrate the ability of malicious actors to cause global disruption of the Internet.

The core of the DNS includes thirteen root servers, with as many as 200 instances in existence around the globe. The root servers translate human-understandable domain names into machine-based IP addresses. Global DNS server disruption can severely impact the operation of the Internet because many critical systems rely on DNS servers to translate domain names into the associated IP addresses. As it turned out, the 2002 and 2007 DDoS attacks did not cause major disruptions due to the over-provisioning of services.

Nevertheless, cyber attacks can have a major impact on the functioning of critical systems in the public and private sectors. These attacks can be organized rapidly and strike without warning. Every country must implement mechanisms to protect the national and global critical information infrastructures. The next section discusses CIIP with regard to developing nations and its current and future impact on the Internet and associated systems.

2.2 Developing Nations and CIIP

The information infrastructure in developing nations is often used to launch or coordinate cyber attacks [12]. According to a 2009 report by Akamai Technologies [2], much of the attack traffic that targets software and hardware vulnerabilities originates in developing countries. This is not to say that users in these countries are actively involved in attacks, only that their computer systems and networks are being utilized for cyber attacks. Indeed, developing countries are often "staging points" for attacks because of their rapidly growing information infrastructures coupled with the lack of coordinated cyber security measures.

Internet Connectivity Developing nations are becoming increasingly dependent on the Internet for communications, e-commerce and e-government services. They are rapidly provisioning their information infrastructures in order to support these services. Countries such as India or China, in particular, are seeing phenomenal growth in Internet-based technologies to support their critical systems [28].

Broadband penetration and Internet connection speeds in developing countries have historically been low, especially for countries in Sub-Saharan Africa [15]. However, several projects are underway to bring massive amounts of bandwidth to these countries [1]. Figure 1 illustrates the current status and future growth of Internet connectivity and bandwidth in the African continent.

The investment in information infrastructures will advance public and private sector efforts, which are essential to economic and social development. In particular, the new infrastructures will increase the resources available in critical areas such as telecommunications, finance, education, health care and social services. Individuals will also benefit from the new infrastructures, with more people having access to the Internet and Internet-based services. However, the

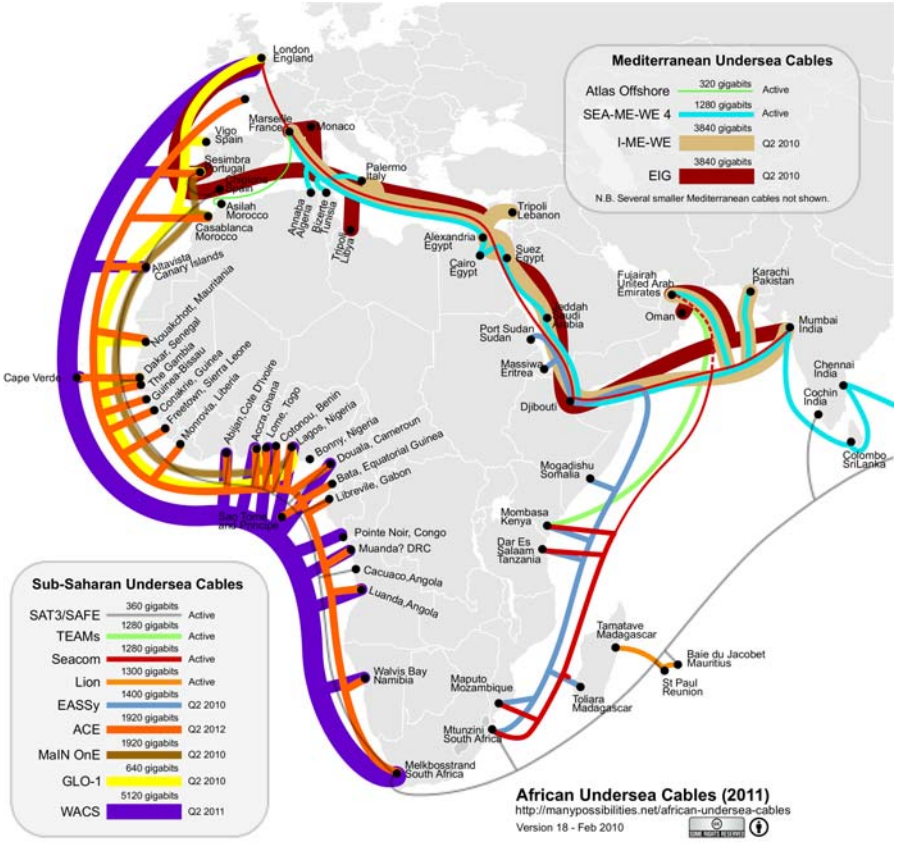

Figure 1. Undersea cables for the African continent (2011 projection) [24].

"always on" Internet culture brings with it its own set of problems such as malware, phishing schemes and botnets.

A 2009 study by Akamai Technologies [2] reveals that a significant percentage of attack traffic originates from developing countries. Table 1 shows that six developing countries or newly industrialized countries (in bold font) are in the top ten list. At the top of the list are Russia and Brazil, most likely due to the prevalence of Conficker-related infections [2].

Table 1 shows an 8% increase in attack traffic from the second quarter to the third quarter of 2009 in the "Other" category, which includes most of the developing countries in the world. This statistic coupled with the growth of their information infrastructures imply that attack traffic from these countries will increase very significantly in the future.

The increased connectivity and bandwidth in developing countries will have the effect of increasing the available pool of users and resources for malware

Table 1. Top ten originators of attack traffic [2].

Rank	Country	2009 Q3	2009 Q2
1	**Russia**	**13.0%**	**1.2%**
2	**Brazil**	**8.6%**	**2.3%**
3	U.S.	6.9%	15.0%
4	**China**	**6.5%**	**31.0%**
5	Italy	5.4%	1.2%
6	Taiwan	5.1%	2.3%
7	Germany	4.8%	1.9%
8	**Argentina**	**3.6%**	**0.8%**
9	**India**	**3.4%**	**0.9%**
10	**Romania**	**3.2%**	**0.6%**
–	Other	39.0%	31.0%

creators and botnet operators. These new pools of users and resources can be leveraged to launch highly destructive DDoS attacks against assets in other countries.

The expansion of the information infrastructure is not limited to investments in fiber optic cables and Internet connectivity. Developing countries are also experiencing unprecedented growth in mobile technologies. According to Cisco Systems [8], developing countries accounted for approximately 75% of the four billion mobile phones in use worldwide in 2009.

Mobile technologies enable developing countries to provide telecommunication services much more effectively than traditional land-based technologies. The MTN Group [21] reported that the "100 million mobile subscriber mark" was attained in developing and emerging markets during the middle of 2009. Mobile devices are being used increasingly as entry points into critical systems, a fact that is often overlooked in existing security policies [4].

The extensive use of mobile technologies also exposes more users to cyber attacks. Cisco Systems [8] predicts that large numbers of users in developing nations will fall victim to cyber attacks that leverage mobile technologies.

The information infrastructures in developing countries must be secured, managed and monitored to prevent them from being used as staging points for attacks. The countries will have to invest in legislation, education and CIIP mechanisms to prevent their new infrastructures from being abused. CIIP will have to be accomplished without limiting the functionality of the infrastructures. This is a particularly challenging aspect of "bridging the digital divide."

Cyber Security Policies Cyber security policies are essential to the management and operation of information infrastructures. Developed countries have created extensive security mechanisms and policies over time, which enables them to identify threats and mitigate the effects of attacks on their critical systems.

Until recently, developing countries have had little need for complex security mechanisms and policies due to their limited infrastructures. The lack of adequate protection for their information infrastructures creates a situation where criminals can utilize them for malicious purposes without fear of attribution or reprisal [7].

Despite the paucity of security mechanisms and policies, most developing countries do have some structures in place to deal with cyber crime. These normally take the form of incident response teams in large companies and government agencies, and digital forensic units in law enforcement agencies [11]. These entities are essential to identifying and prosecuting cyber criminals, but they do not provide monitoring and reporting capabilities for the national information infrastructures.

The next section discusses the structures that are in place for CIIP. These structures are loosely hierarchical in nature and are designed to monitor and report cyber incidents, enabling the relevant parties to react quickly and efficiently to incidents.

3. Protection Structures

Several structures exist for protecting critical information infrastructures. Some of these structures are specifically designed to provide incident handling and monitoring functions. The primary goal is to enable the relevant authorities to take quick, decisive steps to prevent cyber incidents and mitigate their adverse effects.

This section discusses two key structures: (i) computer security incident response teams (CSIRTs) that are used in large organizations; and (ii) warning, advice and reporting points (WARPs) that cater to smaller organizations and individuals.

3.1 CSIRTs

Computer security incident response teams (CSIRTs) (or computer emergency response teams (CERTs)) are commonly used by large corporations and government agencies, as well as for local, regional and national CIIP efforts. CSIRTs provide incident handling services [27], responding to cyber events and providing information and support to their stakeholders. For example, a CSIRT may monitor vulnerability reports from software and security appliance vendors and report information about threats, vulnerabilities and security controls to its stakeholders, enabling them to take the appropriate steps to protect their critical systems.

Organization CSIRTs are normally loosely hierarchical in nature. A tiered approach allows for the coordination of many, possibly diverse, stakeholders. The CSIRT hierarchy typically includes coordinating CSIRTs, regional CSIRTs and private CSIRTs. Each of these CSIRTs operates as a security team that is responsible for a specific constituency [17].

A coordinating CSIRT spearheads national information infrastructure protection efforts. It coordinates regional and private CSIRTs, and communicates with its counterparts in other countries. Its constituency includes regional and private CSIRTs, and other international CSIRTs.

Regional CSIRTs operate in a specific geographic region, providing support to organizations and the general population. They prevent the coordinating CSIRT from becoming overwhelmed by a large constituency. Regional CSIRTs also serve as the regional contact points for CIIP efforts.

Private CSIRTs (or private security teams) are created for large companies, academic institutions, government and law enforcement agencies, and military entities. They are normally responsible for managing incidents directly related to their particular organizations. Private CSIRTs are a vital entity in the CSIRT hierarchy as they experience the direct effects of cyber incidents and serve an first responders in their organizations.

The CSIRT hierarchy is presented in a generic manner. Koivunen [18] observes that each CSIRT and CSIRT hierarchy are unique, depending on the requirements imposed by the organizations and stakeholders, and their operating environments.

Analysis The establishment of a national CSIRT hierarchy is a proven method for implementing CIIP. Killcrece [17] notes that individual CSIRTs serve as trusted points of contact for cyber incidents. The coordinating CSIRT can help establish national best practices for cyber security, and provide advanced support for security incidents. However, Harrison and Townsend [14] argue that a CSIRT hierarchy is expensive to set up and maintain in terms of personnel and technology costs. Moreover, CSIRTs are primarily reactive as opposed to proactive.

3.2 WARPs

CSIRTs are large structures that are not designed to support smaller organizations and individuals. Warning, advice and reporting points (WARPs) fill the gap by serving as informal providers of cyber security information and expertise to small, focused constituencies.

Organization WARPs were first created in the United Kingdom as part of its CIIP efforts [3]. They are informal in nature and are focused on small member communities, to whom they provide computer security advice and limited incident handling services [14]. The members of a WARP typically number between 20 and 50, enabling the WARP to remain community-driven and focused on its member needs. The informal and focused nature of WARPs makes them very cost effective [14].

Analysis WARPs are very effective at providing CSIRT-like services to small communities that may not be adequately served by a larger CSIRT. Their obvious benefit, specifically for developing countries, is their low cost.

WARPs cannot provide adequate protection at the national level and are, therefore, not a replacement for CSIRTs. However, WAPRs can operate very effectively in conjunction with traditional CSIRTs.

4. South African Case Study

The creation and implementation of effective cyber security policies in developing countries are vitally important to national, regional and international CIIP efforts. Many of these countries are using hastily-created policies to cope with the dramatic expansion of their information infrastructures and the associated vulnerabilities in their critical systems. But these policies are only adequate for the short term; sustained efforts are necessary to provide long-term CIIP solutions.

In February 2010, the South African Department of Communications released a draft cyber security policy for South Africa [25]. This document outlines various structures for protecting the South African information infrastructure and associated critical systems.

The document notes that South Africa neither has a coordinated cyber security effort nor a broad legal framework for dealing with cyber crime. It goes on to stress that these technological and legal deficiencies must be addressed. The document also highlights the need for international cooperation in the area of CIIP. However, South Africa does not currently have adequate international relationships for effective information infrastructure protection.

The document makes a number of recommendations regarding the development of a CIIP framework. The recommendations are aimed at securing South African cyber space as well as reducing threats and vulnerabilities.

A key recommendation is the creation of a National Cybersecurity Advisory Council (NCAC). The NCAC will be responsible for advising governmental entities on issues related to cyber security. It will also be responsible for coordinating cyber security across the South African Government.

The document also recommends the creation of a CSIRT structure for managing threats and vulnerabilities, and to serve as point of contact for cyber security information. The proposed structure will consist of a national CSIRT, a governmental CSIRT and a number of sector-specific CSIRTs. Finally, the document highlights the need for local and international partnerships for effective CIIP.

5. CIIP Requirements for the Developing World

In order for developing nations to implement effective CIIP solutions, there are a number of requirements that should be satisfied. These requirements are diverse and depend on the goals mandated by governmental policies.

The nature of a CIIP solution would clearly depend on the specific country and infrastructure that needs to be protected. However, any solution that is developed will have to be cost effective.

Because developing nations are experiencing phenomenal growth in their information infrastructures, CIIP solutions have to be extensible to support future development without incurring excessive costs.

CIIP solutions in developing countries will require the support of international entities. To this end, the CIIP structures must support information exchange and knowledge transfer, both locally and internationally.

Special care must be taken with regard to mobile technologies. The growth of mobile technologies in the developing world enables millions of individuals to access information and services that were previously unavailable. However, mobile technologies dramatically increase the size of the user pool for exploitation by malicious actors. CIIP solutions in developing countries must take this into consideration.

Developing countries will have to embrace technology in order to supplement traditional methods of communication. This will allow vital information to be communicated in the event that traditional modes are unavailable. For instance, should communication via email not be possible, information could be exchanged via SMS messages or fax.

Finally, developing nations have to invest in broad-based awareness programs to ensure that new users are aware of the risks associated with their activities in cyber space. Such programs benefit users as well as the nation as a whole. Critical systems are connected by the same networks that are used by the general public; reducing threats and vulnerabilities at the user end helps protect critical systems as well as the underlying information infrastructure.

6. Conclusions

Modern critical systems rely heavily on information infrastructures in order to operate efficiently; this is true for developed countries as well as developing countries. However, due to the lack of adequate CIIP structures and security policies, developing countries are often used as launch pads for cyber attack. Much of the world's attack traffic already originates in these countries and the proportion of attack traffic will only increase with the dramatic growth of their information infrastructures.

Traditional CIIP solutions, such as CSIRTs and WARPs, support the monitoring and reporting of cyber incidents. Such solutions hold promise for the developing world, but issues such as cost-effectiveness, information exchange and international cooperation must be addressed.

Our future research will investigate a number of models that will satisfy CIIP requirements for developing countries. It will also examine the relationships between successful CIIP solutions across the developing world, and articulate best practices for national and regional CIIP efforts.

References

[1] Akamai Technologies, State of the Internet, vol. 2(2), Cambridge, Massachusetts (www.akamai.com/stateoftheinternet), 2009.

[2] Akamai Technologies, State of the Internet, vol. 2(3), Cambridge, Massachusetts (www.akamai.com/stateoftheinternet), 2009.

[3] B. Askwith, WARP case study – Experience setting up a WARP, Center for the Protection of the National Infrastructure, London, United Kingdom (www.warp.gov.uk/Index/indexarticles.htm), 2006.

[4] S. Baker, S. Waterman and G. Ivanov, In the Crossfire: Critical Infrastructure in the Age of Cyber War, Technical Report, McAfee, Santa Clara, California, 2010.

[5] BBC News, The cyber raiders hitting Estonia, London, United Kingdom (news.bbc.co.uk/2/hi/europe/6665195.stm), May 17, 2007.

[6] BBC News, Estonia fines man for "cyber war," London, United Kingdom (news.bbc.co.uk/2/hi/technology/7208511.stm), January 25, 2008.

[7] BBC News, What makes a cyber criminal? London, United Kingdom (news.bbc.co.uk/2/hi/americas/7403472.stm), May 19, 2008.

[8] Cisco Systems, Cisco 2009 Annual Security Report, San Jose, California (www.cisco.com/en/US/prod/collateral/vpndevc/cisco_2009_asr.pdf), 2009.

[9] R. Dacey, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, Testimony before the Subcommittee on Technology Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform, GAO-04-628T, General Accounting Office, Washington, DC (www.gao.gov/new.items/d04628t.pdf), 2004.

[10] D. Danchev, Coordinated Russia vs Georgia cyber attack in progress, ZDNet, San Francisco, California (blogs.zdnet.com/security/?p=1670), August 11, 2008.

[11] J. Fick, Cyber Crime in South Africa: Investigating and Prosecuting Cyber Crime and the Benefits of Public-Private Partnerships, Technical Report, PriceWaterhouseCoopers, Sunninghill, South Africa (www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079if09pres_JaquiFick_report.pdf), 2009.

[12] Georgia Tech Information Security Center, Emerging Cyber Threats Report for 2009, Georgia Institute of Technology, Atlanta, Georgia (www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf), 2008.

[13] M. Handley and E. Rescorla, Internet Denial-of-Service Considerations, RFC 4732, Internet Engineering Task Force, Fremont, California (www.ietf.org/rfc/rfc4732.txt), 2006.

[14] J. Harrison and K. Townsend, An update on WARPs, *ENISA Quarterly Review*, vol. 4(4), pp. 13–15, 2008.

[15] R. Heacock, Internet filtering in Sub-Saharan Africa, Technical Report, OpenNet Initiative, Harvard University, Cambridge, Massachusetts (opennet.net/sites/opennet.net/files/ONI_SSAfrica_2009.pdf), 2009.

[16] ICANN, Factsheet: Root server attack on 6 February 2007, Marina del Rey, California (www.icann.org/announcements/factsheet-dns-attack-08mar 07.pdf), 2007.

[17] G. Killcrece, Steps for Creating National CSIRTs, CERT Coordination Center, Carnegie Mellon University, Pittsburgh, Pennsylvania (www.cert .org/archive/pdf/NationalCSIRTs.pdf), 2004.

[18] E. Koivunen, Survey on Certain European CSIRT Teams' Administration, Operations, Cooperation and Communications, Technical Report, CERT-FI, Helsinki, Finland, 2009.

[19] S. Korns and J. Kastenberg, Georgia's cyber left hook, *Parameters*, vol. XXXVIII, pp. 60–76, 2008.

[20] J. Moteff, C. Copeland and J. Fischer, Critical Infrastructures: What Makes an Infrastructure Critical? Report for Congress RL31556, Congressional Research Service, Library of Congress, Washington, DC (www.fas .org/irp/crs/RL31556.pdf), 2003.

[21] MTN Group, MTN reaches the 100 million subscriber milestone, Press Release, Johannesburg, South Africa (www.mtn.com/media/overviewdetail .aspx?pk=381), May 2009.

[22] J. Nazario, Estonian DDoS attacks – A summary to date, Arbor Networks, Chelmsford, Massachusetts (asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date), May 17, 2007.

[23] J. Richards, Denial-of-service: The Estonian cyberwar and its implications for U.S. national security, *International Affairs Review*, vol. XVIII(1) (www.iar-gwu.org/node/65), 2009.

[24] S. Song, African undersea cables, Many Possibilities, Durbanville, South Africa (manypossibilities.net/african-undersea-cables), 2010.

[25] South African Department of Communications, Draft Cybersecurity Policy of South Africa, Government Gazette No. 32963, Pretoria, South Africa, 2010.

[26] P. Vixie, G. Sneeringer and M. Schleifer, Events of 21-Oct-2002 (c.root-servers.org/october21.txt), November 24, 2002.

[27] M. West-Brown, D. Stikvoort, K. Kossakowski, G. Killcrece, R. Ruefle and M. Zajicek, Handbook for Computer Security Response Teams (CSIRTs), Handbook CMU/SEI-2003-HB-002, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, 2003.

[28] P. Wolcott, The provision of Internet services in India, in *Information Systems in Developing Countries: Theory and Practice*, R. Davison, R. Harris, S. Qureshi, D. Vogel and G. de Vreede (Eds.), City University of Hong Kong Press, Hong Kong, China, pp. 253–267, 2005.