Implementing Critical Information Infrastructure Protection Structures in Developing Countries

Ian Ellefsen, Sebastiaan Von Solms

Chapter 2

IMPLEMENTING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION STRUCTURES IN DEVELOPING COUNTRIES

Ian Ellefsen and Sebastiaan von Solms

Abstract The development of a national critical information infrastructure protection (CIIP) structure is essential to safeguard critical systems from cyber attacks and other threats. As developing nations leverage Internet technologies, it is imperative that they develop their own national CIIP structures to ensure reliable operations, incident response and resilience in the face of attacks. This paper presents a framework designed to enable developing countries to define a set of clear deliverables that can be used to realize a national CIIP structure.

Keywords: Critical information infrastructure protection, developing countries

1. Introduction

Technologically advanced countries have implemented a variety of critical information infrastructure protection (CIIP) structures to safeguard their national information infrastructures and critical systems from cyber attacks and other threats. Historically, developing nations have had poor access to Internet-based technologies [1], which has limited their need to develop effective CIIP structures such as computer security incident response teams (CSIRTs) [12].

However, this situation is changing. Many developing nations are experiencing massive growth in Internet capacity and the use of Internet-based technologies. Attacks on the information infrastructure can severely affect the ability of a country to function effectively [16]. If commercial entities were to lose Internet services for a prolonged period, the economic effects would be significant. The impact of large-scale cyber attacks on national critical systems would be much more devastating. It is clear that developing countries are finding them-

selves in the situation where they have to implement national CIIP structures to safeguard their information infrastructure assets [2].

This paper presents a framework that is intended to be used by developing countries to implement CIIP structures. To this end, the paper investigates the role of traditional CIIP mechanisms such as CSIRTs and related protection structures. The generic framework outlines a set of deliverables that allow for the establishment of a national CIIP structure.

2. Background

Developing countries are making massive investments in Internet and communications technologies. Many large-scale infrastructure assets used for electricity distribution, water supply, and banking and finance are utilizing these technologies to improve their ability to deliver services. The resulting information infrastructure is transforming the manner in which governments interact with citizens, companies transact business, and individuals access vital information and services.

Despite their reliance on the information infrastructure, developing countries rarely implement a nationally-coordinated protection structure to protect their vital information assets [5]. Cyber attacks, such as distributed denial of service (DDoS) attacks, can severely affect all the infrastructure sectors [3]. Cyber attacks differ greatly from traditional types of attacks. Historically, the ability to wage war has been the domain of governments. However, cyber attacks can potentially be initiated by any person with relatively little expenditure and without the need for a high degree of technical proficiency [15], and these attacks can have a direct effect on all sections of society.

In the United States, 85% of all critical systems are owned and operated by private entities [18]. The situation is quite different in most developing countries, where the majority of infrastructure assets are in the public sector. But regardless of the extent of government ownership, there should be a transition from centralized information infrastructure protection structures to public structures that safeguard commercial and individual interests. This is not to suggest that there is no place for governmental structures, only that they should operate in tandem with public protection structures.

3. Protection Structures

There are a number of protection structures that can form the basis of a national CIIP structure. The structures, which are intended to provide a coordinated platform for dealing with cyber incidents, are geared towards the specific environments in which they are deployed. However, despite their differences, protection structures take one of two forms, a top-down structure or bottom-up structure. We discuss a computer security incident response team (CSIRT) as an example of a top-down structure, and a community-oriented security, warning and advice (C-SAW) team as an example of a bottom-up structure.

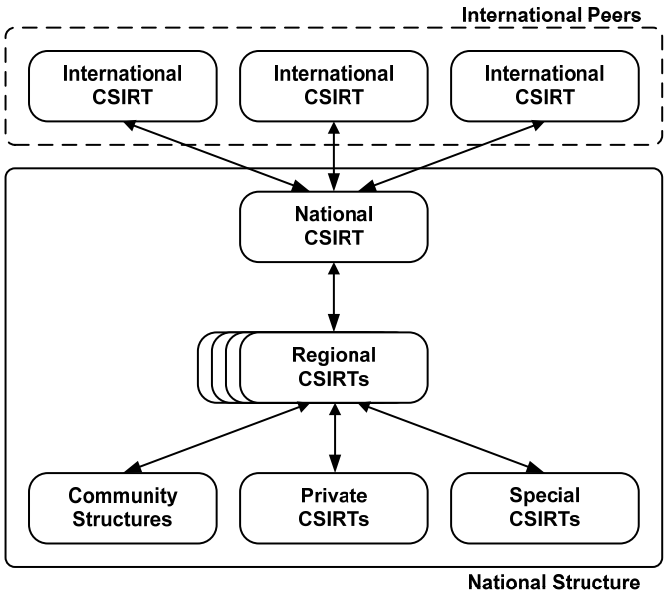

Figure 1. High-level CSIRT model.

Computer Security Incident Response Team. A CSIRT is a national entity that coordinates proactive and reactive efforts focused on managing cyber security incidents [8]. Figure 1 presents the different components of a CSIRT structure, which provide incident handling support to various constituencies.

The CSIRT itself follows a top-down model, where coordination is provided at the national level, with a number of regional CSIRTs that provide support to smaller constituencies [14]. Each CSIRT is structured to suit the environment in which it is deployed [19].

The primary service provided by a CSIRT is incident response. Incident response covers a number of services that seek to identify, manage and mitigate cyber security threats [4, 19].

A CSIRT is national in its scope and, as such, maintains relationships with international peers, governments and large organizations. However, the needs of individuals and small organizations cannot be overlooked in a national CIIP structure. The needs of these segments of the population are addressed by computer security, advisory and warning (C-SAW) teams.

Community-Oriented Security, Advisory and Warning Teams. Small businesses and individual households make up a large percentage of computer users. Often these users have to fend for themselves when dealing with cyber security threats and incidents.

A community-oriented structure is required to enable these smaller stakeholders to receive cyber security support. This structure is a "bottom-up" model, where security support is provided in a loosely-coupled manner from within a community.

Community-oriented security, advisory and warning (C-SAW) teams are an example of a community-oriented model that could be deployed within a national CIIP structure. These teams provide CSIRT-like services to a smaller, less informed community of members [6, 7].

A C-SAW team can also serve as an intermediary between a larger national CIIP structure and the smaller stakeholders, with a direct focus on providing cyber security support to its community. A C-SAW team should be community driven and operated by members of the community it services [7]. The services provided by a team, which typically involve vulnerability tracking and incident response, are largely dictated by the needs of its community.

C-SAW teams should operate independently of the larger national CIIP structure. Nevertheless, a C-SAW team should maintain good communication channels with other teams as well as the national CIIP structure.

C-SAW teams are important to national CIIP efforts because small businesses and individuals may not have the technical expertise available to manage CIIP threats and incidents. These smaller stakeholders should not be ignored because incidents that affect large numbers of these users can severely affect critical infrastructure operations [6]. Other community-based structures serve a similar role as a C-SAW team. The common aspect is that they are community-driven and focus on providing support to their communities.

Overall Structure. The CSIRT and C-SAW teams should operate together to provide the front-end for a national CIIP structure. The design and operation of these teams are vital to ensure that CIIP efforts pervade all sections of society. However, the mere deployment of protection structures is not sufficient to establish a successful national CIIP structure. Indeed, a national CIIP structure typically goes through a number of developmental stages before it can provide adequate protection for a nation's information infrastructure.

4. CIIP Framework for Developing Nations

The International Telecommunications Union (ITU) has produced a number of documents related to the development of CIIP structures in developing countries. One of the key documents is the *ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009* [13], which highlights the need to establish effective CIIP structures in developing nations because of the potential impact that they have on the global economy. This section builds on the ITU effort by describing a framework for developing effective national CIIP structures in developing countries.

Cyber security structures in developed nations have their roots in the early years of the Internet, when the U.S. Defense Advanced Research Projects Agency (DARPA) funded the development of the initial Computer Emergency

Response Team (CERT) in response to the Morris worm [14]. These structures have evolved with the Internet to meet new and expanding requirements.

Developing nations, on the other hand, have historically had limited Internet access and poor provisioning of information and telecommunications infrastructures. However, the introduction of a number of high capacity fiber optic cables – especially in Sub-Saharan Africa [17] – has created a situation where the establishment of effective CIIP structures is a necessity. When designing and implementing these CIIP structures, developing nations have the advantage of being able to leverage the lessons learned from the efforts undertaken by developed countries.

Developing countries have unique challenges that should be addressed by CIIP structures. In particular, Harris [10] has identified the following key challenges:

- Rapid development of information infrastructures.
- High-levels of cyber security illiteracy.
- Significant use of mobile technologies.
- High demand to adopt and provision web services.
- Inadequate legislation addressing cyber security.
- Inadequate policy documentation addressing cyber security.

All these challenges must be addressed in a national cyber security policy. Of course, the scope with which the challenges are addressed would depend on the conditions and needs of the country in question.

It is also important that the CIIP structure provides support to all sections of society. Furthermore, it is necessary to consider the needs of the private sector that may own and operate a significant portion of the critical infrastructure, as well as small businesses and individuals that make up a large segment of computer users within a developing country [9].

5. Two-Factor Development

A national CIIP structure must provide cyber security support to two primary societal groups. The first group is served by a traditional CSIRT structure, and the second by community-based structures. Each group exhibits different cyber security needs, and the overall CIIP structure should be able to address these needs. Ideally, the development of a national CIIP structure should follow a "two-factor development" strategy, where protection for each societal group is developed in parallel, with the holistic structure developing over time.

Figure 2 shows the society groups and the CIIP structures that are responsible for providing cyber security support and managing incidents. We now discuss the roles of the CSIRT and C-SAW teams.

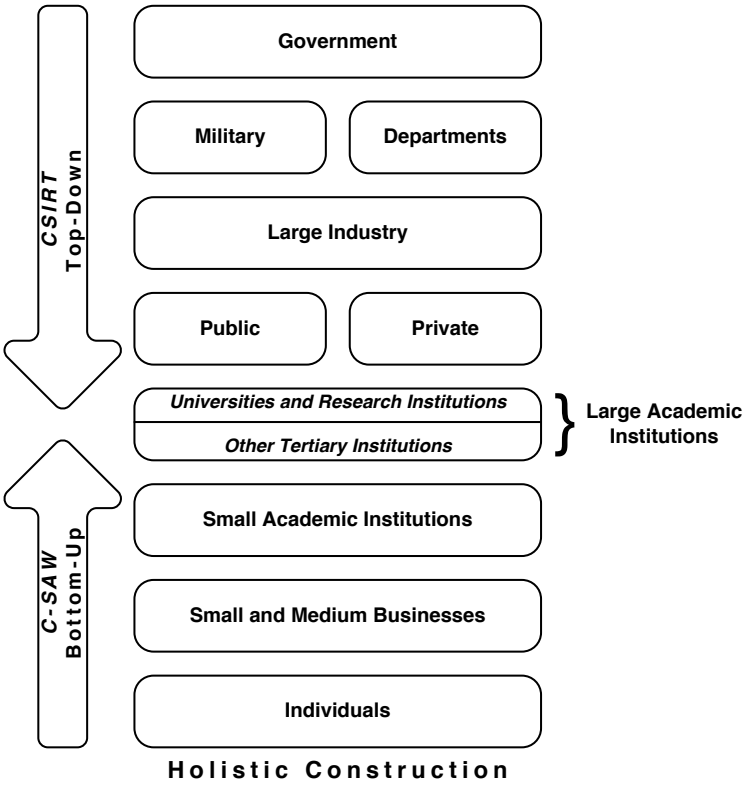

Figure 2. Organizations in a holistic CIIP structure.

CSIRT Role. The CSIRT is the lead entity in a national CIIP structure implemented according to the top-down model. The CSIRT coordinates the national cyber security policy, develops cyber security strategies and provides oversight and management for security related incidents in diverse operating environments. Figure 2 lists the specific organizations that fall under the direct management of a CSIRT structure. The organizations are:

- **Government Entities:** Governmental departments, military entities, and other government-sponsored utilities.
- **Large Industry Entities:** Financial institutions, telecommunication, manufacturing, electrical power, water distribution, sewage treatment and other large industries that provide services at a national level.
- **Large Academic Entities:** Large tertiary academic institutions and national research institutions.

The management of these organizations is delegated to a CSIRT because the organizations have large numbers of users and substantial computing resources. Also, the organizations may control critical infrastructure assets and may require considerable computing resources and network bandwidth. An additional benefit of assigning these entities to an emerging CSIRT structure is that they often have internal security structures and policies in place, which can be utilized to aid in the development of the CSIRT.

C-SAW Team Role. C-SAW teams are responsible for managing and coordinating cyber security efforts for smaller entities. These entities include:

- **Small Academic Entities:** Primary and secondary academic institutions.
- **Small Industry Entities:** Small and medium-sized businesses.
- **Individuals:** Private citizens.

These entities may be smaller than those managed by a CSIRT and they are often overlooked [11], but they are, nevertheless, vital to a national infrastructure. Early CIIP structures primarily focused on large industry entities. However, due to the abundance of individual users and small businesses and their potential to serve as breeding grounds for malware, these entities can have a serious impact on critical national systems.

Following the bottom-up paradigm, the services provided by a C-SAW team are driven by community needs. C-SAW teams play a vital role in educating their communities and helping secure their assets [6]. The teams also provide a bridge between their communities and the national CIIP structure.

6. CIIP Framework Development

The development of a national CIIP framework occurs in an incremental manner. The parallel development of top-down and bottom-up structures over the evolution of the national framework results in a holistic CIIP structure.

6.1 Stages of Development

A national CIIP structure progresses through several phases of development before it can be fully operational. Previous work related to the development of national CIIP structures (see, e.g., [14, 19]) does not translate well into the context of developing nations. This is largely due to the constraints imposed by the environment in developing countries. Therefore, it is necessary to conduct a rigorous assessment of the environment in which the CIIP structure will be deployed.

The following three phases of CIIP structure development are geared towards developing nations:

- **Initial Development:** Environmental assessments are conducted, legislation is evaluated, technological aspects are assessed and basic structures

are put in place. This phase sets the groundwork for the later stages of development.

- **Intermediate Development:** CIIP structures are developed to support growing needs. Community-based structures are expanded and public awareness schemes are initiated.

- **Mature Development:** CIIP structures are fully able to handle cyber security incidents.

6.2 Initial Development

The initial development phase is primarily concerned with laying the groundwork for the national CIIP structure. Many assessments are conducted during this phase, with the goal of deploying a functional CSIRT. The assessments are aimed at understanding the environment that must be protected, and identifying the strengths and weaknesses of existing systems.

Environmental Assessment. The goal of this assessment is to understanding the key components of the environment. Areas addressed in the environmental assessment include:

- **Critical Systems:** Identification of the set of nationally critical systems. The set of systems could be derived from assessments conducted in developed countries. These systems would eventually fall under the jurisdiction of the CSIRT.

- **Stakeholders:** Identification of the stakeholders in the CIIP structure. These are role players who have a vested interest in the stability of national systems. The stakeholders include government departments, large companies and international partners. The degree of interest of each stakeholder must also be gauged.

- **Legislation:** Identification of existing legislation related to cyber security and projected changes to the legislation.

- **Expertise:** Identification of the expertise required to develop the CIIP structure. This helps provide recommendations on whether a country has the local capacity to develop an effective national cyber security structure.

The role of the environmental assessment is to understand the environment where the CIIP structure will be deployed. The assessment is not limited to the components listed above. Indeed, due to the unique nature of each deployment environment, a number of other factors may have to be considered during the assessment.

Legislative Assessment. The legislative assessment is concerned with identifying the legal environment in which the CIIP structure is to be deployed.

As is often the case in developing countries, the legal system may not make provisions for current and future developments in technology. Despite the fact that legal frameworks are complex and diverse, the legislative assessment can be broken down into two basic components:

- **Current Legislation:** Evaluation of the current set of legislation that addresses cyber security, national cyber security policy, physical information infrastructure and compliance with international best practices.
- **Possible Amendments:** Identification of the areas of legislation that may have to be amended to allow for the effective deployment of a national CIIP structure. This component should consider the assignment of legal powers to the various entities in a CIIP structure to enable them to operate effectively.

Once again, these are not the only tasks that to be performed. Further analysis should be conducted during this phase to identify other legal issues.

Technology and Vulnerability Assessment. A technology and vulnerability assessment is conducted in order to gain an understanding of the operating environment. This assessment should identify technological components and their vulnerabilities that could potentially impact the national CIIP structure. The assessment should cover the following aspects:

- **Current and Future Bandwidth:** Investigations of the amount of available bandwidth, and well as future projections.
- **New Technologies:** Investigations of new technologies that could impact information infrastructure security. This would also include investigations of mobile technologies.
- **Current Systems:** Investigations of the current state of computer-based systems and their impact on overall cyber security. The analysis should also cover legacy systems.

In addition to helping understand the current operating environment, the technology and vulnerability assessment enables the national CIIP structure to accommodate longer-term projections.

International Peer and Partner Assessment. The role of international partnerships in CIIP cannot be overlooked. Partnerships with international CIIP structures can provide valuable assistance in creating effective local structures in developing countries. The partnerships are also important during the later phases of development. Due to the international nature of the Internet, these partnerships cannot be ignored. Incident information must be shared freely between international peers to identify and mitigate the effects of security incidents.

Local entities are a valuable resource during the initial phase of CIIP structure development. These entities include multinational companies and large local companies that already have cyber security structures in place.

A key component is fostering trust between international and local partners. Active participation in international organizations such as the Forum of Incident Response and Security Teams (FIRST) can help build trust.

Small-Scale Deployment. After the deployment environment has been assessed, a small-scale deployment of a CIIP structure (CSIRT or C-SAW team) should be attempted to identify any oversights in the initial assessments. The trial deployment lays the groundwork for future development of the CIIP structure and provides valuable insight into the operational environment. The deployment need not focus on incident response; it is beneficial to also concentrate on developing local and international relationships, which are vital during the later phases of CIIP structure development.

6.3 Intermediate Development

After the operational environment has been assessed, the development of the national CIIP structure transitions into the intermediate phase. The intermediate phase focuses on the development of the national protection structures, especially the CSIRT and C-SAW teams.

CSIRT Development. The development of the CSIRT is crucial during the intermediate phase. The lessons learned during the initial phase and the small-scale deployment are applied when creating the CSIRT. The principal goals are to strengthen local and international relationships, and define the roles and responsibilities of the CSIRT. The CSIRT should also initiate its operations, and begin to monitor and respond to cyber incidents.

C-SAW Team Deployment. After the CSIRT structure is operational and has the ability to respond to incidents (even in a limited capacity), the C-SAW teams can be integrated into the national structure. This enables small businesses and individuals to gain the benefits of the national CIIP structure.

The C-SAW teams should work with the CSIRT to raise awareness and educate users about threats, vulnerabilities and mitigation strategies. The C-SAW teams should actively grow their constituencies and work within their communities to drive cyber security programs at the grassroots level.

6.4 Mature Development

During this stage of development, the national CIIP structure is fully operational. The CSIRT and C-SAW teams can communicate effectively with their stakeholders and manage incidents. Also, relationships with international peers and industry partners are well established.

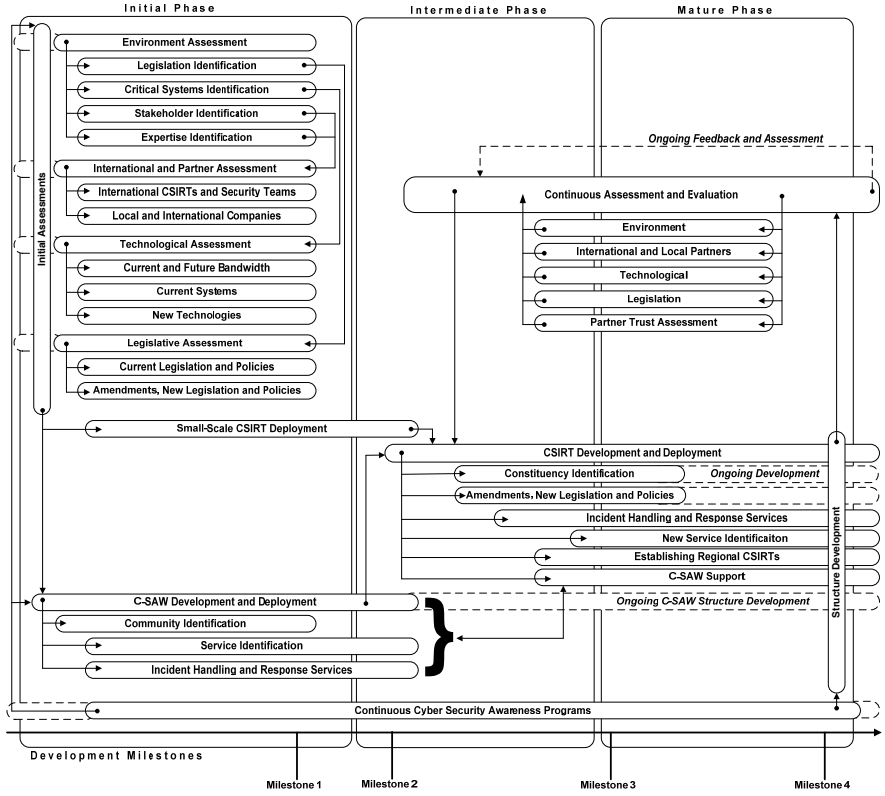

Figure 3. Timeline for deploying a national CIIP structure.

The mature phase does not signify the end of the development cycle. Rather, the national CIIP structure should continuously monitor and adapt to the ever changing environment. Also, CSIRT and C-SAW teams should continue to educate their user bases and ensure that a strong cyber security culture develops over time.

Figure 3 illustrates the CIIP deployment timeline. The timeline spans the four developmental phases, culminating with a mature and robust national CIIP structure.

7. Conclusions

Developing countries have traditionally had poor access to the Internet, and as such have not felt the need to develop national CIIP structures. However, as these countries leverage Internet-based technologies, it is imperative that they develop their own national CIIP structures to ensure reliable operations, incident response and resilience in the face of attacks.

The CIIP framework described in this paper establishes a clear set of phases, goals and outcomes that developing countries can use to establish effective national CIIP structures. Of course, every operational environment is unique. Therefore, it is important that the national CIIP structures accommodate the pertinent features of their environments and continuously evolve with the changing technological and threat landscapes.

Every country must take strong steps to protect its information infrastructure and critical systems. To this end, every national CIIP structure should aim to be all encompassing, open, transparent and publicly available.

References

[1] Akamai Technologies, State of the Internet, vol. 1(4), Cambridge, Massachusetts (`www.akamai.com/stateoftheinternet`), 2008.

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

[3] 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.

[4] N. Brownlee and E. Guttman, RFC2350: Expectations for Computer Security Incident Response, 1998.

[5] I. Ellefsen and S. von Solms, Critical information infrastructure protection in the developing world, in *Critical Infrastructure Protection IV*, T. Moore and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 29–40, 2010.

[6] I. Ellefsen and S. von Solms, C-SAW: Critical information infrastructure protection through simplification, in *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience*, J. Berleur, M. Hercheui and L. Hilty (Eds.), Springer, Boston, Massachusetts, pp. 315–325, 2010.

[7] I. Ellefsen and S. von Solms, The community-oriented computer security, advisory and warning team, *Proceedings of the IST-Africa Conference*, 2010.

[8] European Network and Information Security Agency, Baseline Capabilities for National/Governmental CERTs, Heraklion, Crete, Greece (`www.enisa.europa.eu/act/cert/support/baseline-capabilities`), 2009.

[9] European Network and Information Security Agency, EISAS – European Information Sharing and Alert System for Citizens and SMEs, Heraklion, Crete, Greece (`www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap/at_download/fullReport`), 2011.

[10] L. Harris, CIOs drive expansion into Africa, *ITWeb Brainstorm*, November 11, 2011.

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

[12] 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.

[13] International Telecommunication Union, ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009, Geneva, Switzerland (www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf), 2007.

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

[15] H. Lipson, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Special Report CMU/SEI-2002-SR-009, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania (www.cert.org/archive/pdf/02sr009.pdf), 2002.

[16] President's Information Technology Advisory Committee, Cyber Security: A Crisis of Prioritization, Report to the President, National Coordination Office for Information Technology Research and Development, Arlington, Virginia (www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf), 2005.

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

[18] United States Government Accountability Office, Technology Assessment: Cybersecurity for Critical Infrastructure Protection, GAO-04-321, Washington, DC (www.gao.gov/new.items/d04321.pdf), 2004.

[19] 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 (www.cert.org/archive/pdf/csirt-handbook.pdf), 2003.