Cybersecurity Challenges in Developing Nations

Submitted in partial fulfillment of the requirements for

the degree of

Doctor of Philosophy

in

Department Engineering and Public Policy

Adam C. Tagert

B.S.E., Computer Science, Princeton University

Carnegie Mellon University
Pittsburgh, PA

December, 2010

Acknowledgements

Sources of Funding:

- John D. and Catherine T. MacArthur Foundation Grant #05-85273-000-GSS.
- Francis and Christine Tagert
- NSF – STIM Center – Award Number - CNS0433540
- The Department of Engineering and Public Policy
- Benoit Morel’s INI Discretionary Fund

Committee

- Benoit Morel (Chair)
- Archie Andrews
- David Farber
- Seymour Goodman

People

Benoit Morel – Your advice, guidance and support have enabled me to get to the point of having this document. You have always been available for me, which has been wonderful and I appreciate it so much. You have always had faith in me and knew exactly how to guide me in my research. It has been a great adventure in cybersecurity and in our trip to Rwanda. Thank you for reading drafts of my thesis multiple times, even at times before I heavily proofread them, it must have been hard, especially with my unique spellings of satellite and Sahara. I am so fortunate to have you as my advisor. You have been a wonderful positive influence on my development, which I will never forget and will always be grateful.

Archie Andrews – Archie, our meetings have been great. I have learned so much about CERTs from you. Thank you, I felt a connection to the global CERT community. Thank you for taking the time in guiding me towards my dissertation. You have pushed me for excellence and helped me find extra potential. You meticulously read my writings and provided valuable annotations. My thesis as a result is far better than it would have been without your effort and energy. It is still amazing that our first meeting was at the Italian Café by campus just days before it was closed to become another CMU building. If you had not suggested it, I would have never been there before it closed. You have been an inspiration to me and thank you for your input and support.

David Farber – You are a wonderful person. You seem to know everyone that is involved with the Internet and can point me exactly to the right person. I feel grounded to the technical implementation of the Internet with your input. You remind me of my time at working in an ISP and as a network administrator. Your mailing list, IP, has also been a great resource of Internet news. I have learned about many Internet issues from it. In my research you always provided perfect advice, which would eliminate my confusion and make what I needed to do so clear. Whenever I encountered difficulties with my research, you were an amazing problem solver. Thank you so much for your time and agreeing to be on my committee.

Seymour Goodman – Sy, you have been involved in my academic development from before I even was on the topic of cybersecurity in developing nations. You have had such a positive and lasting impact. We began with our workshop at Georgia Tech, which has always influenced my thinking of the international dimensions of cybersecurity. Our time together in Washington with the Rwandans and Tunisians was incredibly influential on me. This dissertation and the concept of CERTs were influenced by our time with the Department of Commerce. In my thesis, you always reminded me that countries are in a spectrum of situations rather than a dichotomy, and I needed to choose words that reflected this reality. You never let me forget that wireless and smartphones are a key issue for the future. I am very grateful for your positive influence on my thesis and my development as a person. Thank you for spending your time on me.

David Mundie – David, I am grateful for your help in my maturity as a writer. You did this by reading my writings and showing me what I was doing to muddle my thoughts. Through you, I learned to connect ideas together instead of bookending ideas together. I also learned how to guide a reader in my thought process rather than allowing it to be an exercise left to the reader. I also appreciate the amount of time and effort that you were willing to spend on me, just because you cared. Thank you so much as your influence will have a permanent effect on me.

Family – Mom and Dad, thank you for so much. I'm dedicating this thesis to you because I would have never completed this thesis without your support, prayers and motivation. You have always had faith in me that I could complete a Ph.D. even before I went to Carnegie Mellon. You two have done far more to help me to get here than could ever be expected. I love you both and will always be grateful. To the rest of my family, thank you for always being there and understanding when I was not. I love you all.

Friends – Thank you to all my friends for your support, encouragement and accommodations. It would have been much harder without you. To Larry and Shirley Streff, thank you for making me part of the family and for all your kindness. To my roommates, Nick, Rob, Jon, Ger and Aaron, you have been great roommates. Jon Kowalski, thanks for being so flexible when it came to housing, filling your house with stuff and my indeterminate moving out date. Royce, it was fun working together in class and facing grad student life together. Jon Fan, thanks for being supportive with your late night phone calls. To everyone else including EPP friends, church friends, and other friends, thank you. And most of all to God who has never left my side.

Abstract

This thesis examines the guidance that is being given to developing nations that are rapidly deploying information and communication technologies. It studied the African countries of Rwanda and Tunisia to draw lessons of the situation and potential methods of improving the situation. The thesis found that developing nations are often recommended to implement a conglomeration of existing rules and regulations found in other countries especially in European countries and in the United States. Developing countries are also recommended to create national CERTs, organizations of cybersecurity experts to coordinate a nation to respond to cyber incidents. The proposed rules and regulations are largely irrelevant for developing nations and the proposed missions of a CERT do not match the needs of those countries. In promoting better guidance, the thesis identifies and discusses several challenges. It finds policy makers in developing nations are aware of the cyber threat, and that the cyber threat is different and often smaller in less ICT developed nations even if they are using similar equipment and software. To help craft better recommendations, the thesis identifies the benefits of ICT especially in agriculture, education and government. These benefits are analyzed to determine whether they would be protected by current guidance and the analysis determines that protecting ICT use in government should be the priority. In crafting future guidance the challenges are that nations have differences in ICT architecture and ICT use, and developing nations have fewer resources but also they have different resources to use. Another such difference is the common lack of a private cybersecurity sector and different expectations of government. This thesis concludes with discussing unexpected results. The first is Rwandan policy makers desire good enough security and have a higher risk tolerance concerning cyber threats than is found in more developed nations. In addition, open source software can be a potential way to reduce the cost of cyberspace defense and this thesis makes an initial investigation. The lesson of the thesis is that cybersecurity strategy is not a one size fits all and so it must be customized for each country.

Table of Contents

Acknowledgements iii

Sources of Funding: iii

Committee iii

People iii

Abstract vii

Table of Contents ix

Introduction 1

Chapter 1 – The Problem, Motivation and the Approach 8

Introduction 8

Defining the Problem 8

Motivation for Solving the Problem 9

Why Rwanda and Tunisia 11

Similar Nations 11

Different stages of ICT maturity 12

Differences of Rwanda and Tunisia 13

Conclusion 14

Chapter 2 – Current Status 16

Introduction 16

Sources of Guidance 16

The Guidance 19

Perception of the situation 20

Awareness 21

Large Cybersecurity Problem 22

Similar ICT infrastructure 25

Complex Government Structure 27

The Common Solution 28

Introduction to CERTs 29

Activities of CERTs 33

Conclusion of CERT Activities 45

Affordability 45

Laws and Enforcement 46

Conclusion 52

Chapter 3 – The Motivation for ICT Adoption and Cyberspace Defense 54
Why Governments Invest in ICT 56
ICT in Education 57
ICT in Agriculture 63
ICT in Government 66
ICT for Economic Growth 73
Information Society 75
Public/Private Investment 82
Conclusion 90
Chapter 4 – Issues to Address to Improve Guidance 92
Prescriptiveness 92
ICT in Agriculture 94
ICT in Education 95
OLPC Security 96
ICT Appliance Security 97
Traditional Desktop and Laptops Computers 97
Agricultural and Educational ICT 97
ICT in Government 98
Weakness of Current Recommendations 99
The Argument for the Existence 99
Differences in ICT use 99
ICT Architecture 102
Limitation of Resources 103
Expectations of Government 110
Conclusion 112
Chapter 5 – Unexpected Findings 113
Introduction 113
Perspective of Cybersecurity 113
Open Source Tools 115
A Concept Model of Security Tool Use 115
Definition of Open Source and Free Tools 117
Staying Current 121
Potential for Market Failures in Open Source 122
2010 Status 125

Conclusion of Open Source Tools ... 126
Conclusion ... 126
Conclusion ... 128
References ... 136

Introduction

The objective of this thesis is to provide ICT policy makers in countries experiencing transformative Internet growth with guidance on creating a national cyberspace defense strategy. Current guidance on implementing cyberspace defense is based on the single model of nations with mature infrastructures and broad adoption of Internet usage. The result is that the available guidance does not directly address the challenges encountered by nations with emerging ICT infrastructures. Policy makers, such as those in Rwanda who viewed current guidance as not implementable, have assessed that a strategy based on existing guidance would not solve their problem, is not reflective of their needs and is not implementable with their national resources. The approach this thesis will take to provide actionable guidance to nations with emerging Internet infrastructures is accomplished by first identifying the important challenges that current guidance has had limited usefulness in meeting. These reasons include affordability, the availability of cybersecurity personnel, and current perceived low susceptibility. However; each nation has its own set of challenges that influence cyber defense guidance.

The challenge of securing the Internet is the consequence from that Internet adoption is enabling a plethora of both beneficial and malicious actions. The beneficial activities include: e-shopping, e-communications, e-business and e-learning. It also has the capability to transform healthcare, education, and government. These transformations are the result of the Internet fostering countless beneficial activities.

Unfortunately, cyber miscreants have realized the potential of the Internet for malicious purposes. They have been honing their skills and capabilities since before the mass adoption of the Internet. Some have become extremely capable and dangerous while the majority is less capable but still often effective especially on soft targets. Many of their attacks presently exploit financially rewarding targets, which has spared the lightly using Internet countries, the recent adopters.

The potential harm from the attacker can raise the threat to a national security issue as cyber-attacks can harm the national interests of all countries. One relevant cyber threat to national interests of an ICT emerging countries is the potential harm to economic growth. While these nations are full of ideas and ways of how they can benefit from the Internet, but they have not yet recognized and dealt with the cyber threat they are facing. It is unlikely that if they continue their current development progress that their cyberspace defenses will continue to meet their increasing cyber vulnerability. This is a troubling proposition. Effective guidance is needed for them to develop and implement a strategy as they are becoming heavy users of the Internet at a time when securing cyberspace is a complicated and difficult field.

The issue of guidance for securing cyberspace including in ICT emerging countries is important to all nations because cyber insecurity has international ramifications. The Internet is a borderless globally connected network that enables cyber attackers to harm other countries by using computer's in countries with poor security to launch attacks, use as proxies to remain anonymous and to add to the global level of cyber insecurity. The openness of the Internet thus requires all nations to have effective cybersecurity policies to have a safe and secure Internet. Having better guidance on building cyberspace defenses in ICT emerging countries is thus an important objective for all countries and not just for the ICT emerging countries bust also those countries that are already online and vulnerable.

The importance of good cyber defense in ICT emerging countries by heavy using countries is illustrated by the outreach programs from organizations such as the U.S. State Department, F.B.I, the U.N. and the ITU. The United Nations produced a resolution mandating the International Telecommunications Union (ITU), a UN agency, to spearhead an effort at spreading a culture of cybersecurity. The ITU acted based on the generally accepted conceptualization of there being one right approach on how to implement cybersecurity. The idea is that there is a universal way to respond to cybersecurity and that this solution fits all nations, a one size fits all approach. It was illustrated clearly in the Johannesburg resolution, which recommended that all nations establish a national CERT to combat the cybersecurity problems of nations.

The strategy within the Johannesburg resolution is to base the strategy on how the current heavy using nations have responded. A quick examination of these countries, such as the United States, finds that the response is not well defined and hardly centralized or government run. Instead, the response is decentralized and has been developing and evolving simultaneously as the attackers have been developing attack methods. The two have in effect developed and evolved together though not in a symbiotic relationship. The defenders, victims, do not benefit from the relationship. The current approach is straining to respond to recent attack methods, which have nearly incapacitated the current defensive approaches, and consequently new original approaches are required. The newly adopting Internet countries face a monstrous challenge in that they cannot follow a similar path of slowly evolving cybersecurity defense as the attackers are already potentially very dangerous. These countries will need a solution that is capable of being built quickly. Transplanting current best approaches is also a challenge as the current approaches are straining to meet the threats in addition to the substantially different conditions on the ground, even if the technical challenges are similar.

While outreach programs have attracted consideration from targeted developing nations, the nations have not closely followed the advice. This thesis documents that this information was based on the natural but faulty assumption that countries like the US were a useful template to duplicate. The central issues among others were CIIP, Critical Information Infrastructure Protection, and building cybersecurity capability in a universal standard way. Of interest to the thesis is that the developing nations, who are actively progressing towards a better cybersecurity situation, are often doing “their own” thing. Tunisia built a CERT from the ground up without international support and Singapore built capacity by outsourcing the majority of its operations to the Singaporean private sector. Rwanda has a team of two individuals to keep abreast of the Rwandan situation. Through the analysis, the thesis finds that the current approaches could be tailored to better fill the needs and goals of developing nations. Rwanda and Tunisia have similar goals in that their cybersecurity priority is to protect their citizens and business from online threats rather than CIIP protection as these countries have yet to build these infrastructures.

The approach chosen in this thesis for improving guidance is to use "case studies" of two countries, Rwanda and Tunisia as data for a study of differences. The study collects information, evaluates it, and then draws lessons from it to reveal the nature of the cybersecurity challenge in ICT emerging nations. Rwanda and Tunisia are good countries to study because they differ in fundamental ways and yet have commonalities. While both are in Africa and experiencing transformative Internet growth, they are culturally different but are still actively exploring ways to cooperate in their cybersecurity policy. Rwanda is one of the poorest countries in the world but has a vision to use information communication technologies (ICT) and the Internet to enable it to develop. Furthermore Rwanda is a small country. It is manageable to build a detail understanding of the interactions within the country. At the beginning of the research, Rwanda was nearly a blank slate in regards to cybersecurity and thus it was possible to monitor how cybersecurity germinated and developed. Tunisia was selected because it is the most proactive country in Africa in regards to building cyber defenses as illustrated by their young but still high quality CERT. From the study of these two countries, through the difference of situations, the thesis is able to identify a wealth of similar constraints they share with most if not all the other Internet emerging countries. This study illuminates the challenge from which guidance can be formed that meets the needs of ICT policy makers.

The thesis built its empirical data set by interacting and building relationships with the government officials that work in telecommunication, development and regulation in these countries, interacting with their private sectors and it also included on the ground research in Rwanda. This enabled the thesis to have an understanding of the challenge of defending cyberspace from a firsthand perspective from a developing nation.

This thesis' goal of more appropriate guidance has several criteria as the result of the nature of the cyber threat in countries experiencing transformation Internet growth. Guidance should efficiently meet nationally important challenges because they contribute significantly to the structure of the cyberspace defense strategy of some nations even though it may not be as important for other nations. An added complexity for a cybersecurity strategy is how other nations respond to their situation because cyber defense is a global interconnected effort and actions within one nation affect all others. This complexity encourages beneficial cooperation among nations. Quality guidance should help nations develop a cyberspace defense strategy to meet short term needs, but still respective of the long term. Finally, guidance should encourage a cybersecurity strategy that is more than a deployment of a set of security tools or making a list of missions to accomplish. It should encourage nations to be prepared to meet a dynamic and ever changing threat to an economy whose reliance on ICT is also evolving. In addition to identifying these important reasons, which make cybersecurity a different challenge for each country, this thesis discusses potential ways to meet the challenge they represent.

The structure of this is the following. Chapter 1 discusses the cybersecurity challenge and the countries of Rwanda and Tunisia. Chapter 2 details what the potential loss of cyber-attacks is by studying the motivations for ICT deployment in developing countries. The third chapter contains the study of differences in Rwanda and Tunisia and identifies the issues for which that current guidance could be improved. The fourth chapter addresses the issues and the final chapter covers the open questions and issues that were not obvious before the research.

The research and analysis in this thesis provides needed guidance on cybersecurity. Presently, governments of ICT emerging nations are left to figure out what to do, because what advice and knowledge exists, does not speak to their situation. Their needs are poorly articulated and often, as this thesis finds, misperceived. This lack of understanding hampers efforts to help developing nations secure their cyberspace as efforts are not precisely targeting the most pressing needs. This thesis rectifies this by using the case studies and a study of differences of situation to gain a better understanding of the situation. This will provide guidance on what are the needs and what others can offer. One such need is a precise and prescriptive structure that is appropriate for a nation experiencing ICT transformation. Many ICT emerging nations earnestly want to have cybersecurity but haven’t found the solution yet.

Chapter 1 – The Problem, Motivation and the Approach

Introduction

The purpose of this chapter is to introduce the aspect of the cybersecurity problem that this thesis is examining. This includes explaining and defining the problem and motivation for addressing it and the methodology used to address the problem. The methodology of this thesis is an empirical study of differences using the countries of Rwanda and Tunisia. This chapter specifies why these countries were selected for the study.

Defining the Problem

The concern of this thesis is those countries that are currently experiencing a transformation in ICT. Often these countries are also developing nations. These countries are adopting ICT and greatly increasing their use of ICT and the Internet. They have high hopes for the positive impact of their investment, but have yet to reap their reward. These countries are emerging ICT nations and their populations are emerging online.

The research in this thesis found that policy makers in these countries need better guidance on how to secure their cyberspace. They view the approach found in current guidance as not fitting their situation. There is a need for a better understanding of the cybersecurity challenges in those nations. The challenges faced need to be better articulated and the situation analyzed for ways to respond to the challenges and where further research is needed.

Motivation for Solving the Problem

The Internet is currently structured as a global and borderless computer network. The ability to communicate easily with any other device has enabled the Internet to have great benefits, but this also enables cybersecurity problems in one part of the globe to easily impact users somewhere else. As a result of this architecture, the cybersecurity situations in all countries are interrelated. For example of the positive benefits and negative consequences from the borderless architecture are illustrated by e-mails and SPAM (unwanted e-mail). People are able to communicate easily as the marginal cost of sending e-mail to any e-mail address is nearly zero. This low cost has also enabled cyber criminals, marketers and con artists to send unsolicited e-mails (SPAM) in bulk and at low cost.

One type of cyber-criminal behavior that has greatly expanded because of the low cost of e-mail is the 419 scam. The details of this scam illustrate the global nature of the Internet and the interdependencies of all countries' cybersecurity. The scam is based on the victim placing unwarranted confidence on the criminal by giving money, or often financial information, in the hope of receiving a greater payout.   Nigeria has gained the reputation of being the source of many 419 scams to targets within other countries and particularly the United States. As a result, the cybersecurity situation in the United States is interrelated with Nigeria and other countries that are sending and receiving 419 scam e-mails. SPAM and 419 scams are just two simple examples of how a country cybersecurity situation is dependent on everyone else. Consequently, it is the global interest to have all countries working to reduce the amount of malicious traffic exiting their country.

ICT emerging nations are the target of this thesis for multiple reasons. There is a perception that these governments are not taking the issue of cybersecurity seriously, because few have created substantial programs to secure cyberspace. This is important because if the cybersecurity situation is poor they will emanate malicious traffic which will harm the global Internet. In addition, because these countries are at the early stages of ICT development, they have an opportunity to structure their ICT infrastructure for cybersecurity in ways that were not done when other nations adopted the Internet. These pressing reasons create a need for better guidance for policy makers. The goal of this thesis is thus to provide research and analysis to help others provide better guidance.

Methodology

The research approach in this thesis is an empirical study of differences. The study studies the cybersecurity situation in countries experiencing transformative Internet growth and in particularly studies the African Countries of Rwanda and Tunisia. These study closely examines the situation to gather clues to what is occurring and why. This enables the study to identify the challenges that current guidance is not meeting sufficiently. The study also enables an analysis and discussion on how to improve guidance to be more useful for these policy makers. Finally, the study identifies open questions that were not obvious before the research.

Why Rwanda and Tunisia

The countries of Rwanda and Tunisia are good countries for this study. They are distinct from each other but share situational commonalities. The commonness of their situation was also recognized by the Rwandans and Tunisians as the Rwanda policy makers have obtained guidance, help and training from the Tunisian cybersecurity team. Some of the basic commonalities are that both countries are geographically small, though Rwanda is smaller, which enables them to share solutions that have scalability problems in larger countries. In terms of population, both are around ten million (CIA World Factbook 2010). These facts make Rwanda the most densely populated country in Africa. The size also enables a study of the country to capture a fuller picture of the situation and motivations. This was especially the case in Rwanda and Tunisia, where we had an incredibly generous amount of access.

Similar Nations

Rwanda and Tunisia share commonalities in regards to cyberspace defense. One relevant resemblance is in government. Both Rwanda and Tunisia are countries with organized and active governments. These governments are actively working towards creating economic prosperity and jobs and they believe that ICT deployment is the way to achieve these goals. These countries are poor and need more well-paying jobs (Beaubien 2005) (Trabelsi 2010) (Yahia 2008). Rwanda's plan is articulated in Vision 2020 (Republic of Rwanda n.d.) and Tunisia's in e-Tunisia (Ouaili 2006). Both governments want to bridge the digital divide and build an information society. They want to be technical hubs for their regions and have ICT access for all their population. These governments have put action behind their vision. Rwanda has a universal access program (RURA 2008) to distribute computers to rural and poor areas and Tunisia has a family PC program (Ouaili 2006) for computer distribution. Both countries are also fostering their objective of ICT jobs by helping information based businesses via Rwanda's Kigali ICT Park (UNIDO n.d.) and Tunisia's Tunis Telecom City (BI-ME staff 2009). The end result is that these governments are integrating ICT with the hope of transforming their countries into a prosperous information society. The governments in both countries want their ICT investment to be secure from cyber threats and are willing to take appropriate actions.

Coordinating appropriate actions in both countries is similar as the number of companies providing ICT services is nearly equal in both countries. Both Tunisia (BuddeComm 2010) and Rwanda have three cellular providers with the latest operator being licensed in 2009 (BuddeComm 2010). These countries also have similar numbers of ISPs; Tunisia has 11 (BuddeComm 2010) while Rwanda has a similar number (RURA 2009). This means in terms of coordinating a cybersecurity solution with the Internet operators that both countries have about the same number of partners and equivalent scalability challenges.

Different stages of ICT maturity

The two countries are not identical in terms of quantity and maturity ICT even though they have similar long range objectives. Tunisia has a more established ICT infrastructure than Rwanda. For example, Tunisia (Flobal Arab Network 2010) began building its national fiber backbone a decade before Rwanda (Kezio-Musoke, Rwanda's national backbone fiber optic cable set for 2009 2008). Internet access is also much more prevalent in Tunisia than Rwanda (Internet World Stats 2010). Tunisia has about a third of its population online while in Rwanda, the penetration is at less than three percent. The greater Internet penetration is partly attributed to geography. Tunisia has access to the sea and is close to Europe, which has enabled Tunisia to use relatively cheap submarine cables for International connections instead of the expensive satellite links that Rwanda had been using.   This reduced cost of international connectivity has led to cheaper Internet access charges and being more affordable to more. As a result of its Internet adoption, Tunisia has been facing Internet threats longer and in greater numbers than Rwanda and therefore has encouraged Tunisians to respond earlier to cybersecurity issues than Rwandans. Tunisia's government thus has a more mature cyber defense operation than Rwanda's, highlighted by Tunisia's young but capable national CERT, tunCERT. This organization is tasked with Tunisia's national cyber defense. The topic of what tunCERT does and what national CERTs do is covered in the third chapter. Another important ICT technology is the cell phone, which are also more prevalent in Tunisia. Tunisia has 80% cell phone penetration (CIA World Factbook 2010) compared to Rwanda's 10% (CIA World Factbook 2010).

Differences of Rwanda and Tunisia

Rwanda and Tunisia have important differences which can enable the study to show that cybersecurity challenges identified are not unique to a particular country.

Instead, the identified challenges are relevant for a breath of countries. In terms of money, Rwanda and Tunisia have GDP per capita that is below the world average, but Rwanda is an order of magnitude less. Tunisia is at $8,000 per capita (CIA World Factbook 2010) while Rwanda is at about $900 (CIA World Factbook 2010). The increase of GDP also contributes to Tunisia's greater Internet and cell phone adoption.

These countries also differ in culture even if both are in Africa. A few ways the cultures are different is first, Tunisia is a North African Arab country while Rwanda is a sub-Sahara country. The second is in religion. Tunisia's official religion is Islam (U.S. State Department n.d.) while Rwanda is predominantly Christian, though it is not recognized by their constitution (U.S. Department of State 2007). These countries also differ in employment. Most Rwandans are subsistence farmers, while Tunisians have diverse employment opportunities. The differences and similarities of these countries make Rwanda and Tunisia good choices to study.

Conclusion

The goal of this thesis is to provide insights on the cybersecurity situation in countries experiencing a transformation from ICT investment. These insights are to help provide better guidance for policy makers in these countries as current guidance is not presently meeting their needs. The approach taken in this thesis is to study Rwanda and Tunisia and use them in a study of differences. These countries were selected because they have commonalities and differences in their situation. The impact of this research is that ICT emerging countries will be able to have better cyberspace defense, which is important as countries with poor cybersecurity negatively impact the Internet as a whole. In the next chapter, the current situation concerning guidance is examined.

Chapter 2 – Current Status

Introduction

This chapter discusses what current guidance on building cybersecurity capacity is, what it reveals on how the situation of the developing countries is perceived and whether these perceptions align with what is actually occurring concerning cybersecurity in ICT emerging nations. The research for this chapter finds that what is alluded to in current guidance is not always the same as what is occurring. To determine what people imagine, assume or perceive, the thesis examines current guidance and past projects to determine what they were trying to fix. There is an assumption that what they were trying to fix is what was believed to be the problem. The research assesses the soundness of the commonly perceived situation. This was done through research in the country and interactions with those governments. Current guidance usually includes the recommendation for ICT emerging nations to establish a national CERT, i.e. a government organization to coordinate the country's response to cyber threats. This proposed institution is modeled on the existing national CERTs.

Sources of Guidance

For a country like Rwanda, there are multiple sources of guidance that are available. The sources fall in the categories of international organizations, governmental agencies, consultants and CERTs. In the category of international organizations, the International Telecommunications Union (ITU) has been the most visible organization promoting cybersecurity. It has produced documents and organized workshops about how to approach the issue. An ITU working group produced a resolution at an October 2008 ITU meeting in Johannesburg, South Africa (ITU-T WTSA-08 2008). This document recognized that developing nations, least developed nations and countries with economies in transition are having an increasing level of computer use and computer dependency at a time where there are increasing attacks and threat on ICT networks. The authors also acknowledge the CERTs in developing countries improve their countries participation in the world cybersecurity efforts. In the light of those facts, the ITU working group resolved to determine the best practices to establish CERTs and identified where CERTs are needed. It would also promote the establishment of CERTs by collaborating with international experts and bodies, by providing support and by facilitating collaborations among national CERTs. Finally, the resolution strongly suggests that member states create a national CERT and to collaborate with other countries. The ITU's participation in international cybersecurity is not limited to producing resolutions. It also hosts workshops and conferences on building cybersecurity capability (International Telecommunication Union 2010). Another multinational organization is the European Network and Information Security Agency (ENISA). This organization was setup by the European Union to work on information security issues. One of its core missions is to be an advice broker (ENISA 2010). ENISA also provides advice to organizations outside the EU including governments of developing nations.

International organizations are not the only source of guidance. Developing nations can learn from U.S. government agencies. Multiple agencies, such as the U.S.

Department of Commerce, are willing to share how they approach cybersecurity. There are also nongovernmental organizations offering guidance. These include consultants and consulting firms such as the SANS institute, which has programs, classes and training intended to help developing nations improve their cyberspace defense (SANS Institute 2008). Another consultant firm is e-Cop. It is a firm that started in Asia and has since branched out to help countries built governmental cybersecurity capabilities. One of its projects is to build a CERT in Oman (e-Cop 2009).

In addition to SANS and e-Cop, there are freelance consultants. Two such consultants produced a report ordered by the World Bank about the needs of cybersecurity in Rwanda (Naidu 2008). This report is one of the main sources for informing the following section on what current guidance is. The report was commissioned by the World Bank as part of an investment of $10 million into the e-Rwanda initiative. This initiative, outlined in Chapter 3, was a program to improve and increase the efficiency of the Rwandan government through ICT. The report was intended to be unbiased so a consultant chosen was one without any ties to Rwanda, the World Bank, or the initiative. The creation of this report was not uneventful. The first consultant visited Rwanda but ran into difficulties in writing the report, which caused a second consultant to be added to help complete the one year overdue report. The report was a long list of things to do, like a laundry list, which could apply to any country, because there was almost nothing specific about Rwanda. It assumes that all countries had exactly the same cybersecurity needs and Rwanda was no exception. The report was received by the Rwandans without enthusiasm. They were unsure of the proposed institutional framework and believed that the proposal recommendations were too complex and too large. Without following the report, the Rwandans have started to build cyberspace defense capabilities. The impact of the report thus has been minimal other than being useful for this thesis in characterizing current perceptions on how cybersecurity threats should be approached.

The last source of guidance are existing CERTs. These organizations specialize in cyberspace defense and one of their common activities is helping others improve in managing cybersecurity issues. They share their experience and hold training classes on how to approach cybersecurity. Rwanda has used information from CERTs especially CERT/CC in Pittsburgh and tunCERT in Tunisia. CERT/CC has built the Qatar national CERT. Other African countries (for example Kenya) have found other CERTs useful such as CERT-FI in Finland, SingCERT in Singapore, AUS-CERT in Australia and CERT-Hungary in Hungary.

The Guidance

It is impractical to report in detail what form the guidance took in each special case. Here the focus is on the common themes. One such theme is that ICT emerging nations should establish a government entity to manage the cybersecurity problem. Often this entity is called CERT (Computer Emergency Response Team) or CSIRT or as the consultant report for Rwanda called it, a National Cyber Security Strategy Council (NCSC). These activities will be detailed later in this chapter and will highlight the activities of the national CERT of Tunisia. In general, guidance recommends that ICT emerging nations establish a CERT with a long list of proposed activities for it.

The themes are not limited to the creation of a CERT. There is also a theme in the type of laws and approaches suggested for countries to adopt. As illustrated by the Rwandan consultant report, guidance is often a global conglomeration of existing laws, regulations and approaches. The report recommended that Rwanda make policies that meet the requirements of ISO Standards, IT Governance Institute Publications, NIST Special Publications, HIPAA, FISMA, European Data Publishing Act, Basel II Accords, Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, etc. (Naidu 2008), things which are utterly irrelevant in Rwanda. This fact was immediately recognized by the Rwandans when they received the report. It is easy to be overwhelmed by the amount of proposed laws and regulations. This report also illustrates the theme that approaches used in ICT developed nations should also be used in ICT emerging nations. It assumes that the situation is similar and can be approached and managed in similar fashions.

Perception of the situation

By studying current guidance, some perceptions are alluded to. These perceptions are often uniformed and generalizations, which fail to capture the diversity situations. Together the beliefs form a narrative of how the cyber problem is understood to be and the logical guidance based on it. This section defines these beliefs and the evidence for the existence of these beliefs. These perceptions are based on how countries are being advised and are not specifically created for the sake of argument. The thesis also compares each perception to the situation in Rwanda. The first belief is that policy makers in developing nations lack awareness of the cyber threat and they are unaware of, another assumption, that there is potentially a large cybersecurity problem in their country. This cybersecurity problem comes from the expectation that the ICT situation has commonalities among all countries in particular because the infrastructure is being built from the same basic equipment. The logical, though incorrect, conclusion from these beliefs is that all countries including ICT emerging nations are facing a common cybersecurity problem and thus the same approach can be used to mitigate it. This conclusion motivates people to recommend approaches used in the most heavy Internet using nations. They assume that these approaches are needed to deal with the expected complex government structures. To deal with the complexities and multiple entities, a CERT is needed. One other theme is that laws and enforcement are an integral part of effective defense. In summation, there is a perception that ICT prevalent nations, such as the United States, can be used as a template for everyone.

Awareness

A common misconception is that the governments and the policy makers are unaware of the cyber threat presented by the Internet. There is a perception that these countries are so unaware of the Internet that the policy makers do not appreciate the threat presented by the Internet. The argument for this belief is that if the policy makers know about the problem, then they would take active steps to deal with it, and thus since they are not perceived to be doing anything then it logically follows that they are unaware. This belief on the lack of awareness is visible in the literature such as in the ITU Cybersecurity Work Program for Developing Countries (International Telecommunications Union 2007). This program has a goal of increasing a country's awareness by providing a toolkit so these countries can self-assess their readiness. The finding of the assessment would make the policy makers aware of their cybersecurity problem.

The research found that Rwanda and Tunisia have ICT policy makers very much aware of the cybersecurity threat. This awareness can be attributed to the efforts to raise awareness and how the threat is becoming readily apparent. There are plenty of anecdotal stories of people being victims of cyber-attacks and these stories raise awareness of the threat. These stories include stories of scams about cars, theft of e-mail account passwords and people losing money from online banking. One commonality is that these attacks all leave visible consequences for all to see, including to those without specialized training. There is less awareness of subtle attacks. There are plenty of people, including government officials, who do not know if and when their computers are infected with malware as it is not visible to them. In Rwanda there is awareness of the fact that there is a cyber-threat, but there is a lacking of a deep understanding of the situation. The evidence suggests that while policy makers are aware that there is a threat, they are poorly informed on the nature and size of the threat. The same happens to policy makers in other countries.

Large Cybersecurity Problem

The cybersecurity problem is often believed to be similar between nations that use ICT heavily and ICT emerging nations because both types of countries deploy similar hardware and software. Some of the commonalities are that all countries use TCP/IP as the protocols for communication, and all are reliant on the same operating Systems

(Windows, UNIX, Linux, and others), software applications (Firefox, Skype, Microsoft Office and many others) and the large router manufactures (Cisco and Juniper). Countries thus do not appear very technologically distinct. The logic is that since the technology is similar then the problems created by the technology are therefore similar. The cybersecurity problem in developed nations, like the United States, has been well documented and it is a large problem. There are a countless number of cybersecurity problems both large and small in the United States. Some problems are related to critical information infrastructure (CIIP), SCADA (supervisory control and data acquisition) systems and government networks, while others are related to the Internet infrastructure and host devices like desktop computers, smart phones, and Internet enabled devices. The implication is that ICT emerging nations must also have a large cybersecurity problem.

The expectation of a similar sized problem is best illustrated by guidance that recommends a similar size response in all countries. Often guiding strategies recommend a large organization to be built with many missions. One example is the NCSC recommended for Rwanda in the World Bank consultant report. The NCSC is a large institution especially in respect to the size of the Rwandan government. Some guidance creates a laundry list of activities needed to be performed by the government. Often this laundry list requires a small font and extra-large paper to fit on a single sheet. The list includes tasks to secure CIIP and SCADA systems, the banking industry, air traffic control, the agriculture sector, the government, the military and many other sectors.

The amount of tasks is sized to a large problem intertwined into many aspects of an ICT connected society such as the United States.

The research found that the cyberspace problem in Rwanda is different than in the United States. Rwanda's threat is smaller and less mature, because among multiple reasons there is less ICT. They still receive the malicious traffic, but there are a limited number of victims to suffer and so there are fewer incidents. For example, there is less ICT in their critical infrastructures and so they are far less integrated into the Internet. As a result, they are not experiencing many CIIP incidents. In addition, the ICT that does exist is mostly fairly new and while Rwanda may have a legacy equipment issue in the future, they presently have minimal levels of legacy equipment. They do not have much ICT that is decades old; almost everything was destroyed in the genocide. Thus, they do not experience attacks that exploit legacy technologies. Another factor that makes Rwanda's potential problem smaller is that the country is in multiple ways smaller than the United States. The population is less, the area is less and the amount of ICT is far less. In addition, the set of activities performed online are different. For example, financial transactions are different. The U.S. uses credit and debit cards, while Rwanda is expanding its cell phone based payment system (money transactions). The best evidence that Rwanda does not have a large cybersecurity problem is that there are fewer incidents even though it is spending far less money and effort on cyberspace defense.

Similar ICT infrastructure

It has already been stated that all countries rely on similar technologies and the expectation that results is that these countries have a similar infrastructure. Some of the commonalities are in the same type of communication infrastructures, the same protocols for wired (Ethernet) and wireless (802.11, GSM, WiMax), the same hardware and software vendors, and in other ways. This concept is also alluded to in guidance because guidance is similar regardless of the country's infrastructure.

The study of Tunisia and Rwanda leads to believing that the infrastructures are not completely similar as there are important differences. First, ICT emerging nations have more wireless, cyber cafés and people are using low powered devices, such as smart phones, as their primary way of accessing content. This change can affect cyberspace defense as fewer users are the primary administrator for their devices. It also changes the software situation. Users often do not have the ability to install software or update software and so they may end up using insecure software. This change introduces a different set of vulnerabilities. Cyber cafés also introduce the threat of multiple people sharing a public computer for potentially private uses. Software can leak information about the previous users. In Uganda, criminals recorded banking from people using cyber café computers. These attackers had physical access to the computer; a difference from typical Internet only cyber attackers. Computer security is usually very poor against attackers with physical access.

Another potential change is in Internet access costs. Unlimited Internet access is not universal. The consequence is that downloads are not free and there is an impact on security. Security updates are usually thought of as free, because they have low cost to the user to download and install. The only cost is the user's time. The patch and the download are both free. In Tunisia, Internet access is paid by the amount of data transmitted and so then there is a cost associated with downloading and installing updates. TunCERT found that many people did not install updates because they did not want to pay to download them. The amount of data needed to download is often significant, as Windows service packs can be hundreds of megabytes. On slower internet connections the download time is also significant, which can become an issue if the electricity supply is unreliable. It could be difficult to keep the computer running and downloading uninterrupted for the hours and possibly days that the download requires to complete. TunCERT's response to these conditions was to distribute free CDs containing the patches. This is just one example of how slight differences in the ICT infrastructure can affect the cybersecurity situation and the appropriate strategy.

The last assumption that is relevant for concluding a similar ICT infrastructure is that the future of the infrastructure is set. This idea does not adequately address the opportunity that ICT emerging nations have. They have the opportunity to build an ICT infrastructure that is different from more developed ICT nations. In building the existing infrastructures, security considerations were largely not considered and presently there are security issues that relate to the intrinsic design of the infrastructure. For example, TCP/IP are the main data communication protocols on the Internet. The IP protocol was designed to get data packets to the destination at best effort while TCP protocol was responsible for reliability. Accountability, the ability to identify the sender of a packet, was not part of the specification and therefore identifying sources of malicious traffic is difficult and usually requires multiple entities cooperating. It would be extremely difficult to migrate the Internet to using protocols other than TCP/IP, but it is an example of how choices made today can have a lasting impact. It is a lesson for ICT emerging nations to carefully consider ICT design decisions as these choices will have effects for a long time. It would be wise to consider the cybersecurity implications of these decisions. While it is unrealistic to recommend that an ICT emerging nation use protocols other than TCP/IP, they can have a strategy that influences infrastructure design choices, which is unavailable to more developed nations. This topic on the potential use of other software will be addressed further in the final chapter, chapter 5.

Complex Government Structure

Many of the challenges that the United States Government faces are the result of a large and complex government. It has many organizations that are responsible for specific activities. For example, one department is responsible for financial regulations while another interacts with electrical power industries. The difficulty stems from that cybersecurity cuts across these traditional boundaries and impacts almost everyone. It cannot be assigned to one organization to manage it. The consequence is that there are many organizations working on various aspects of the cyber problem. It thus becomes difficult to coordinate everyone to work together and not to overlap as there are many competing interests in the U.S. government. Finding a good solution is difficult as many solutions are difficult to scale to the size of an institution like the U.S. government.

Current guidance assumes at times that ICT emerging nations have similar difficulties. This belief can be seen in the guidance that Rwanda received in the consultants reported. There was significant attention devoted to organizing the government and its processes. The NCSC was to have stakeholders from many other parts of the government. There is also a recommendation for security experts to be located throughout the government. Therefore it appears to have an implicit assumption that the government of Rwanda is large and complex.

In reality, Rwanda's government is presently much smaller than the American government. It does not face the same scalability challenges. They still have challenges in cooperating between government entities, but their newness (Rwanda's government is about a decade old) has limited the growth of the challenges. There are fewer challenges from engrained ways of doing things. Cooperation is also easier because there are fewer entities involved. This has enabled a single team from RURA to set regulations for cybersecurity for the entire government and ICT users in the country. For example, RURA has published guidelines (regulations) for Rwandan ISPs. There is no American equivalent to the cybersecurity team in RURA. The implication of smaller and simpler government structure is that solutions that are unworkable in the United States may work there and successful American approaches may not be optimal for Rwanda. Better guidance would understand the Rwandan government structure and find solutions appropriate for them.

The Common Solution

Current guidance often recommends the creation of a national CERT. This was stated as a goal of resolution at an ITU meeting in October 2008 in Johannesburg, South Africa. The national CERT recommendation was developed in response to increasing level of computer use and computer dependency and the increasing attacks and threat on ICT network through computers (ITU-T WTSA-08 2008). This recommendation also is given by university professors, academic papers, U.S. government organizations and other CERTs. This following section details what existing CERTs do and in particular it details tunCERT, the national CERT of Tunisia. This is relevant because this organization is the leading CERT in Africa and could be a role model and resource for other countries.

Introduction to CERTs

CERTs (Computer Emergency Readiness Team) and CSIRTs (Computer Security Incident Response Team) are teams that are often created as a way for an organization to respond to cybersecurity problems. They are found globally in many types of organizations; both public and private. Many teams are responsible for handling cybersecurity within an organization, but a few have national responsibilities. There is an acceptance in current guidance that these special purpose teams are the best approach to responding to the cybersecurity situation.

CERTs and CSIRTs

There is an issue of terminology to clear up before defining CERTs. The distinction between CSIRT and a CERT is not always clear. CERTs and CSIRTs are both types of teams who respond to cybersecurity problems. A CSIRT (Computer Security Incident Response Team) is a generic name for a security team (Killcrece, et al. 2003). CERT is trademarked by CERT/CC who controls the use of the name (CERT/CC 2008). This is done to create some form of brand control by preventing malicious individuals from adopting the name. While the CSIRT acronym implies only incident response, CSIRT organizations have grown beyond that original mission. Due to the ambiguity of the terminology, both terms are commonly used to describe a cybersecurity team. In this thesis, the organization typically described is one that has national responsibility, is capable and able to become a member of the CERT community and for these reasons it will be referred to as a CERT instead of a CSIRT.

National CERT

Some CERTs are specified as national CERTs. These CERTs focus on issues that threaten a nation. National CERTs focus on large threats that impact the economy, critical infrastructure, operations of the government or to national security. A targeted denial of service attack on a nation is a large incident that would be of concern to a national CERT. For example, Estonia experienced in 2007 a denial of service attack on important national websites including banks and government offices (Vamosi 2008). The attack was launched in response to the Estonian government moving the Bronze Solider statue, a Soviet era war memorial. An unimportant compromised webserver would not rise to a national event, as it is unlikely to collapse a national economy. The Estonian national CERT coordinated the response to the attack with help from global experts. Another reason for the Estonian national CERT involvement is that national CERTs are also tasked with protecting the government's ICT resources and the attack targets included government websites including the presidency and parliament (Traynor 2007).

Creation of CERTs

The first CERT was created at Carnegie Mellon University's Software Engineering institute in response to the Morris Worm of 1988. Defeating the worm required administrators in UC Berkeley, MIT and others to figure out how it worked and then how to stop and remove it. In 1988, the Internet was still a research project called ARPANET (Advanced Research Projects Agency Network) and in response to the worm, DARPA (Defense Advanced Research Projects Agency) funded a center to coordinate experts in emergencies. This center is CERT/CC. It was a way to prepare for the next event. The CERT Charter defined CERT's mission to include being a reliable, trusted single point contact for emergencies (CERT/CC 2010). It would have capabilities lined up and working relationships so that a response would not be ad hoc like it was in the Morris worm. It would also be responsible for coordinating and facilitating communications, because any incident would be too large for any single entity. CERT also was to maintain close ties to research activities and conduct research to improve security (CERT/CC 2010). Finally CERT was also to raise awareness of cybersecurity. CERT/CC is not the only security team created in response to an incident. For example, the Danish CERT, DK-CERT, was created in 1991 as a response to the first Danish hacking case.

Not all CERTs are formed in response to a single event. For example, US-CERT (United States Computer Emergency Readiness Team) was formed in 2002 and was located within the U.S. Government's Department of Homeland Security. It wasn't created in response to any particular incident, but rather as a response to the threat of large scale cyber-attacks (US-CERT 2007). Its mission would be to prepare for and respond to incidents that would overwhelm existing systems. It was also created to improve the cybersecurity of U.S. governmental networks. It has a role in national security and more particularly in US cyber protection. It is designated as the national CERT of the United States. The difference between US-CERT and CERT/CC is that CERT/CC provides cyber security technical expertise while US-CERT is to be responsible for securing the nation's information infrastructure (US-CERT 2007). Similar to the motivation for US-CERT, the recognition of the threat also led Brazil to establish a national CERT, CERT.br. It was formed in response to an understanding of the cybersecurity threat and the realization that an organization was needed to respond and to coordinate a response. Similarly, tunCERT in Tunisia was formed because its founder convinced the Tunisian government that the country needed such an organization to manage cyber problems.

Not all CERTs are created by governments as many were created by private entities and universities to deal with their cybersecurity issues. MIT and Stanford are just two examples of universities with CERT teams. In the private sector, Boeing, Bank of America, and Google have created CERTs and CSIRTs for themselves (FIRST.org 2010). In conclusion, CERTs are created as a way of tasking experts to work on cybersecurity issues that benefit the parent organization. CERTs have been created in the private sector, in academia and in government and so it is indicative of the belief that CERTs are needed and a good way to respond to cyber problems. It is thus logical that guidance often encourages ICT emerging nations to establish CERTs.

Activities of CERTs

Many organizations have created CERTs, implying that their CERTs must provide some type of useful service that fills a need. Generally, the services provided by a particular CERT are those that are useful to its clientele. This section characterizes CERT activities to see how and why CERTs are considered so important to cybersecurity defense. This section often uses tunCERT, the national CERT of Tunisia as an example. CERT/CC classifies CERT activities into four categories: reactive services, proactive services, artifact handling and security quality management (CERT/CC 2002).

Proactive Services

CERT services that aim at preventing intrusions or incidents are classified as proactive services. Proactive services demonstrate that one role of CERTs is to help prevent intrusions. These services include: information dissemination, tool development, network monitoring, auditing, penetration testing and regulation development. Each of these services requires further discussion.

Information Dissemination

Information dissemination such as announcements of vulnerabilities and patches is done by many CERTs including US-CERT (United States), tunCERT (Tunisia), AUS-CERT (Australia), JP-Cert (Japan) and many others. CERTs usually disseminate information by posting it on their websites or by e-mail distribution lists. The goal is for the CERT to be a knowledge repository and thus a single trusted point of contact for information, which is beneficial to both Internet users and software vendors. The service facilitates the flow of information so that users and vendors can spend less time and effort communicating cybersecurity information. Users benefit in a second way when a CERT acknowledges information. Users can know that the information is factual because it has been verified by a trusted party. This is better for users as many other online sources of cybersecurity information have dubious trustworthiness. Information dissemination by CERTs enables Internet users to have better information than before. Quality information allows users to take appropriate actions to improve cybersecurity.

Security Audits

Security audits are a method to verify the implementation of best current practices. This approach has no guarantee of improving security; it is just one of multiple activities. The principle behind performing security audits is that cyber-attacks are less likely to be successful if best current practices are followed. Many intrusions are the consequence of not following the best current practices. This approach has been codified into law in Tunisia. Tunisia has a legal requirement for all public organizations and some private to have a yearly security audit (tunCERT 2010). The private entities that are audited are those that handle and automatically process personal data of Tunisian citizens. The audit requirement also applies to the operators of critical telecommunication infrastructures and large organizations with large private networks that could affect the telecommunication infrastructure. The CERT certifies the auditors and creates the audit process. TunCERT provides a model to the auditors for how the audit should be performed. The model requires the evaluations of ICT systems and the reporting of the methods that will be taken to fix the security deficiencies found in the evaluation. The audit process includes a risk based assessment that calculates risk based on the ISO standard 17799. Much of the audit work and reporting is done by the organization itself, but they must be supervised by certified auditors. The goal of the Tunisian audit requirement is to make organizations and administrative staff aware of cybersecurity problems and requires them to take measure to correct the problems. Inspiring the Tunisian law is a similar United States' law, Federal Information Security Management Act of 2002 (FISMA). This law tasks U.S. government agencies and departments to audit their ICT. Auditing is believed to be a way for CERTs to help organizations to be more compliant with best current practices, but there is significant debate on the effectiveness of security audits to achieve these goals. Determining whether security audits should be performed and how is beyond the scope of this thesis.

Penetration Testing

Penetration testing also falls within proactive services and is part of the tunCERT audit model and one of the recommended ways to improve U.S. governmental network security. The tests are a way of verifying the effectiveness of security policies and procedures by using simulated attacks. One of the difficulties is creating tests/attacks that don't actually harm the assessed systems. Tests cannot unleash a malicious virus or worm to see what happens and thus requires skilled experts to perform penetration tests. Performance is measured by comparing anticipated results with the actual results. Penetration testing has drawbacks. First, it only tests for known threats, which are becoming an ever smaller percentage of attacks. Secondly, it is possible for a false negative which can lead to a false sense of security (Munro 2008). The tunCERT audit requires penetration testing done by automated analysis and scanning for known vulnerabilities. There is a body of knowledge that a CERT can draw from to build their penetration capabilities. The National Institute of Standards and Technology (NIST) has published a guide (SP800-115) to help organizations conduct technical testing and examination methods (Scarfone, et al. 2008).   In addition to SP800-115 is the Open Source Security Testing Methodology Manual (OSSTMM). It is a peer-reviewed free document that further contributes to the open body of penetration knowledge (Herzog 2005). There is also training and certifications associated with the OSTMM. Penetration testing is believed an important part of cyber defense because if often shows to the administrator what an attacker might find during a system reconnoiter (Syamntec 2008) (Rubens 2008).

Tool Development

When the Conficker worm was infecting computers, US-CERT released a tool to help users determine if they were infected and in need of reactive services (AFP 2009). The tool was based on Conficker knowledge generated by non US-CERT security researchers. This exchange of knowledge shows that US-CERT relied on collaboration in responding to Conficker.

Not all tools are built for distribution to the public; some enable a CERT to be better. National CERTs are tasked with protecting the government's network and to do so they often need to create network monitoring tools. US-CERT developed the Einstein network monitoring system as a way to find signs of compromised systems and detect new types of attack. TunCERT has developed a set of tools called Saher, which translates to English as "vigilant." The Saher program/tool is capable of: monitoring websites for defacement, detecting denial of service attacks and other Internet infrastructure attacks, and collecting malware in honeypots. The details of Saher will be discussed in the next section on the topic of network monitoring. Tools are in general designed to detect attacks, prevent incidents or increase CERT capability.

Network Monitoring

Network monitoring of government networks is one task assigned to national CERTs like US-CERT. By using Einstein, a tool it developed, US-CERT examines the communications between the federal government's network and the Internet. It is currently a network intrusion detection system (NIDS), but capabilities are being added to allow Einstein to be able to respond to threats it has detected. Einstein examines packet header information and compares packets to malware signatures (Department of Homeland Security 2004) (U.S. Department of homeland Security 2008). Tunisia has tasked their national CERT will similar responsibilities. TunCERT collects information from Internet traffic to have situational awareness of cyber-attacks in its Saher program (El Mir 2008) (tunCERT 2010). The Saher program is an application based on open source tools. It has four major components. It includes the monitoring of over 6,000 websites within .tn domain (Tunisia) for web defacements. It can also detect DoS attacks and deterioration of web access. The defacement process includes multiple methods to reduce false positives. The algorithm compares the current website to a MD5 hash of a previous check and verifying that the website was not supposed to have been modified. The defacement algorithm also checks for keywords that are often associated with defacement. Saher includes a component for monitoring status of

Internet services including e-mail services, routing and DNS service attacks including cache poisoning. It has a NIDS component to detect nationally important, large scale, attacks of DDoS and viruses/worms. The goal is to be able to determine and thus focus on the large threats. Saher is built as a distributed NIDS, multiple sensors, based on open source tool SNORT that attempts to track the spread of malware in Tunisia and to detect and report ongoing attacks. Detection occurs by signature matching for detecting known attacks and an anomaly based detector for attempting to detect new types of attack.

Honeypots

Honeypots are computer systems deliberately setup insecurely to attract and enable the monitoring of attackers. They are designed in such way that no activity is supposed to occur and thus everything that does occur is illicit. The setups vary depending on the type of attack wanting to be detected. Some are configured to attract spammers and thus collect sample spam and others collect malware. The fourth component of tunCERT's Saher is a honeynet, a system of honeypots, to gather attack information. In Brazil, CERT.br participates in the Brazilian Honeypots Alliance. It is a network of honeypots that are used to gather cybersecurity information on Brazil's cyberspace. It can be used for incident detection and statistics generation. In 2007, the alliance had 36 partners with sensors distributed within Brazil (Honeynet.br 2007). The honeynet produces local data about the state of Brazil's cyberspace instead of more general data or data specific to another country that is produced by other projects (Hoepers and Steding-Jessen, Distributed Honeypots Project: How It's Being Useful for

CERT.br 2006) (Hoepers and Steding-Jessen, The Brazilian Honeypots Alliance 2007). It is used to notify Brazilian networks about IPs that are producing malicious traffic. The system is capable of collecting malware samples. The structure is based on OpenBSD and can emulate different OSs and services to collect information. Other CERTs also perform network monitoring. For example, the Korean CERT in collaboration with the ISPs in Korea has built similar capabilities to Saher. They built a system to detect cyber-attacks, by deploying monitoring equipment on the Korean Internet backbone (Carpenter and Allen 2007). A CERT may use honeypots as a way to study cyber-attacks without the privacy concerns associated with monitoring and capturing general Internet traffic.

Regulation

CERT-FI (Finland) performs a proactive service that very few other CERTs do. It is involved in regulating cybersecurity in Finland. The CERT's technical component acts like a traditional CERT while the regulatory half or parent, the Finnish Communications Regulatory Authority (FICORA or Viestintavirasto) acts much like the FCC in the United States. The CERT and the industry work together in developing regulations that are beneficial for cybersecurity. This is a similar process to how the regulators and industry work together in the FERC/NERC cybersecurity regulations.

To be successful, CERT-FI constructed a separation between the enforcement and the CERT or to phrase it another way between the carrot and stick operations. This separation enables the CERT to maintain confidentiality and encourage users to share sensitive information. This arrangement allows for issues to be brought to the CERT without fear of being punished from the regulator. There is a view that getting it fixed is more important than punishing. This separation is not unique to CERT-FI. TunCERT is also separated from enforcement. Legislation prevents them from reporting incidents to law enforcement. This separation enables the CERT to work with sensitive problems. Trusting the CERT to be a partner is important for it to be successful.

Proactive services are very important as if they are successful, attacks fail. Preventing attacks is a better solution than responding to attacks. Proactive services show that a major role of CERTs is to enable others to be more resistant to cyber-attacks.

Reactive Services

Attacks at times are successful. CERTs respond to attacks in two ways. They can focus on solving the technical problem, Vulnerability Management, or the cleanup, Incident Management. Through the use of reactive services, CERTs help reduce the harm that occurs from successful attacks.

Incident Handling

Incident handling is a very common activity, which is responding to cybersecurity events (Carpenter and Allen 2007). National incident response focus on large incidents that impact the economy, critical infrastructure, operations of the government or to national security. A small incident could be responding to a defaced website. Response would include determining how and what was done and stopping the attack and how to prevent it again. It could also involve determining who was involved. National incident handling focuses on big incidents. A compromised webserver alone will not bring a critical infrastructure. A targeted denial of service attack on a nation, such as the one that Estonia experienced, is a large incident. The scale is what determines if an event is a national incident. Incidents that are of national importance are within the scope of a national CERT. Large events usually require some type of coordination as multiple entities are involved.

Incident handling often includes the issuing of alerts and warnings. A task a national CERT often performs is to be a portal to distribute alert bulletins. The CERT can issue bulletins that are appropriate for that country. These information bulletins help administrators have current information. CERT/CC released an advisory alerting the public to the threat from the Slammer worm and recommended that traffic on the UDP Port 1434 be not allowed to enter or exit networks (CERT/CC 2003). This was done in response to the Slammer worm which had been released and was rapidly infecting vulnerable SQL servers. A reactive advisory alert concerns incidents already in progress as compared to proactive advisory alerts which warn of potential issues.

Vulnerability Handling

Reactive services include other services that deal with active threats or issues. A known vulnerability is one type of active problem as developers attempt to remediate it before attackers find and exploit it. CERT/CC has services to help vendors find the security bug in code that is creating the vulnerability (CERT/CC 2009). Some software vendors may not have enough expertise to respond quickly to discovered or exploited vulnerabilities in their code and want to use experts in that field. Vulnerability handling includes developing mitigating techniques before a complete solution is found.

Reactive services are offerings from CERTs that respond to ongoing problems. Incident handling and vulnerability handling are two main types. National CERTs are concerned with those incidents and vulnerabilities that are a threat to a nation.

Artifact Handling

Artifacts are objects or files that are found on systems that could be involved in a probe or attack (CERT/CC 2002). Artifacts include viruses, trojans, worms, etc. A CERT can do a technical examination on the artifact to determine purpose and function. Once it understands it, it can develop a response and then coordinate with other CERTs. Artifact handling is dealing with code of the software or hardware being attacked and artifact handling deals with the code often used or left by the attacker. Malware samples are a type of artifact that CERTs collect and study. TunCERT's Saher team studies artifacts that are collected with its honeypot network (tunCERT 2010). Artifact handling increases the knowledge of cyber-attacks which allows for better defenses.

Security Quality Management Services

Security quality management services are services that CERTs offer to help organizations better prepare for cybersecurity. Providing an advisory to an organization is only beneficial if the organization knows how to respond to it. These services help organizations build better capabilities. These services are a way for a CERT to expand beyond dealing with problems to developing a culture of cybersecurity. Security quality management services are not services that are only offered by CERTs and CSIRTs, but they bring a unique perspective from their experience performing other services. These services include risk analysis, disaster recovery planning, security consulting, education, training, product evaluation and others.

In general, CERTs often offer services like consultants. They can work with an organization to improve their cybersecurity capabilities and defenses. CERT-IPN (Portugal) offers consulting services: penetration tests, assessments, design information security solutions and computer forensics (CERT-IPN n.d.).

Outreach – Awareness, Education and Training

Consulting is not the only type of service. CERTs outreach programs are categorized as security quality management services. These programs are comprised of awareness, education and training. These tasks have been missions of CERTs from the beginning. Raising awareness is laid out as a mission for CERT/CC in its charter. Awareness, education and training differ on who is being educated. Awareness is informing the public. CERT's educational activities help incorporate cybersecurity into school's curriculums for the benefit of students while training is for professionals.

TunCERT (Tunisia) and Q-CERT (Qatar) are active CERTs in educational outreach. TunCERT has partnered with academic institutions in Tunisia to offer master's degrees in ICT security. The CERT helped form the curriculum and the instruction materials to enable the universities to offer the program. They also have a program to educate new high school faculty with some basic cybersecurity knowledge. A goal is to have some cybersecurity as part of the standard curriculum in high school and college (tunCERT 2010). TunCERT is not alone with educational outreach. High school students in Qatar, during a college preview program, had a class from an information scientist from Q-

CERT (Qatar) (Q-CERT 2009). Q-CERT also reaches out to educators to help them understand cybersecurity issues so they can then educate their students (Nagy n.d.). To help them, Q-CERT created materials designed for students at different ages.

Awareness outreach can include students and thus at times it is difficult to distinguish from education. A way to separate is based on the amount of involvement with curriculum. For example, Q-CERT had a competition for students to create art, based on their understanding of cybersecurity (International Telecommunication Union 2009). This program is classified as awareness as it does not target curriculum.

Raising the public awareness of cybersecurity issues helps the public to make sound decisions that concern cybersecurity. The term culture of cybersecurity refers to a population that has a basic understanding of cybersecurity issues. CERTs often promote awareness via guides, pamphlets, websites and e-mail distribution lists; TunCERT even developed a kids cartoon to increase children's awareness of cyber dangers to them. Microsoft and the Indian CERT have collaborated to create a website to help online users be more aware of threats like cybercrime and cyber-attacks and methods to defend (Information Madness 2009). US-CERT has a mailing list on security tips that the public can subscribe to and receive information about protecting oneself (US-CERT 2010).

Awareness outreach focuses on basic cybersecurity knowledge, while training are classes that help professionals learn specific skills and knowledge. Many CERTs provide classes to help individuals to be more competent in cybersecurity. CERT/CC has an extensive set of training classes to help people in topics like building a CSIRT or how to perform incident handling.   CERT/CC also has training to enable others to teach its material. CERT.br participates in the program as it offers several CERT/CC classes. CERT/CC is not the only CERT to offer trainer training. TunCERT, in Tunisia, is building a program that trains certified professionals who can teach cybersecurity training, on topics from basic defense of network perimeter security to incident handling (tunCERT 2010).

Security quality management services especially consulting, education, awareness outreach and training are important activities for a CERT in a developing nation that has few individuals with enough cybersecurity knowledge.

Conclusion of CERT Activities

CERTs provide services that mainly revolve around technical solutions and educating others about cybersecurity. They develop tools, study threats, vulnerabilities, artifacts, networks, etc. They do testing and research. They train and they educate. CERTs have become technical repositories of knowledge and cybersecurity experts. CERTs are useful because they enable a few cybersecurity experts to guide many others to secure cyberspace. This is a type of force multiplier. A security expert in a CERT can do much more than he can do alone.

Affordability

CERTs are an approach that is not cheap to build. Some of the costs are the experts' salaries, training and travel. It is an example of how guidance sometimes recommends expensive solutions. CERTs are not the only issue of affordability. A more mundane example is the use of anti-virus software. While the average American can afford to buy the software, the average Rwandan cannot.

In providing guidance it is important to remember that there is a vast difference of resources between the United States and Rwanda. Rwanda's government is poor as illustrated by many of its large projects being supported by international funds. For example, the fiber backbone is supported by a World Bank grant.[1] Compared to their government, the Rwandan people have even less money. The majority of its people are well below poverty standards. Affordability thus becomes a challenge for developing nations. They need solutions on the cheap. One must develop and recommend solutions to ICT emerging nations, like Rwanda, solutions that are more cost effective than those being recommended. These affordable solutions may be slightly less effective, but at least there is a way to implement them. They are still far better than nothing. As will be address later, open source software may be a solution to this affordability challenge.

Laws and Enforcement

Some ICT emerging nations have cybercrime laws and others do not. There are some that believe law and enforcement are a vital component to reduce cyber threats. This belief is illustrated by the emphasis placed on the all countries signing and ratifying the European Convention on Cybercrime. This convention is an international attempt to harmonize cybercrime laws and so that cyber attackers who are located anywhere can be brought to justice. It is beyond this thesis to determine the relative importance of

[1] This backbone is described in detail in Chapter 3.

cybercrime laws, but the following section argues that laws alone are insufficient, but still important to implement.

Laws are often used to solve problems. If drivers are traveling too fast on a section of road, the response is to place a speed limit, but as seen on American highways, speed limits are only effective when heavy and constant enforcement is involved. The politicians have tried to criminalize cybercrime and as the problems are still present, they have been ineffective.

Cyber laws in many cases have not caught up with cyber-attacks and threats. Looking for a way to punish a spammer, a law against trespass to chattels was used (Eletronic Frontier Foundation 2007). In other countries, especially developing, laws for cybercrimes haven’t been enacted yet (Xinhua 2010). International efforts have been made to standardize the cybercrime laws in many countries. A major effort, the Council of Europe's Convention on Cybercrime helped established baselines for cybercrime: hacking, fraud, virus writing and child pornography (Robel 2006) and cooperation among the signers with standards for investigating (Walker 2006). While the U.S. has signed and ratified it, (The Associated Press 2006) the treaty has not been signed by all large countries on the Internet, much less ratified. China has not signed it yet (Council of Europe 2006) and they have the most Internet users (Internet World Stats 2009). The other consequence of international treaties including the Convention on Cybercrime is they often degenerate to vague statements and become the lowest common denominator between the signatories (Hosein 2001). The problems and challenges that have occurred in creating an international regime to respond to cybercrime, do not imply the effort should be abandoned. The global nature of the Internet necessitates a global response. Developing nations, both large and small and rich and poor, must all criminalize cybercrimes and enforce their laws.

Jurisdiction is a hurdle for cybercrime laws. The perpetrator, the location of the crime and the victim are often in different jurisdictions. It requires cooperation among the multiple jurisdictions, which can be difficult if not impossible if in one jurisdiction the actions were not considered a crime. This is the reason that Marc Rich fled to Switzerland after committing tax fraud in the United States. Switzerland would not turn him over to the United States because what he did in the United States was not considered a criminal offense in Switzerland. To reduce the number of safe countries, extradition treaties are signed. The treaties are attempts to encourage countries to return criminals.

The Internet complicates the issue. An individual in a foreign country can via the Internet violate a cybercrime law without having to be physically in that country. In addition, his country may not have criminalized the action and thus he would not physically be within the jurisdiction of any violated laws. His own country is often uncooperative in the investigation when the incident is not illegal. The individual is for the most part safe from punishment for his crime. The convention addresses the jurisdiction issue by first making the country criminalize the unwanted actions and secondly, to cooperate in the investigation of the crime. The convention attempts to eliminate two obstacles for cybercrime punishing: jurisdiction and being identified. Attribution still remains a difficulty, as it still an unsolved problem, but the convention promotes the idea that cooperation leads to more attribution. It recognizes that without help of the attacker's nation, it is nearly impossible to attribute an attack. The supposed effect is that cybercriminals would be found, when possible, and penalized for their crimes and the deterrence aspect of that would cause cybercrime to reduce.

Part of the convention is a requirement for signatories to provide support for investigating crimes. They are required to create a phone number that can be called 24/7 that can be used to ask for assistance by investigators in other countries. If a developing nation was planning on participating, the CERT is a logical organization to be answering the phone. They will or should have the technical capacity to provide assistance and they should have the 24/7 capacity as cyber threats can occur at any time. The relationship between CERT and law enforcement has to be defined so that the CERT does not unintentionally end up being a punishing authority.

Could a country be successful in cybersecurity defense if it took the approach of only passing cybercrime laws and enforcing them? The country would likely be worse off even with perfect enforcement. First, the attackers would either attack from a country not participating or hide from enforcement. The attacker could send the attack traffic out of the country to an unhelpful country by compromising a computer in that country and then from that computer attack. He would most likely not be found. So as long as some countries are not part of the program, a legal and enforcement approach is insufficient.

Assuming hypothetically that all countries participate in the international cybersecurity regime and that attributing and convicting the criminals is perfect, this approach has weaknesses. The problem is that the response, detection and prosecution are reactive and thus an attacker can still perform the activity. The problem is of deterrence; if the expected penalty is not greater than the expected benefit for the rational attacker, that attack will happen. For example, a terrorist who does not care about the punishment could use the Internet to disrupt and cause chaos. The laws and the punishment do not have a deterrence effect on the terrorist. The country would have justice, but would have failed at protecting its people from the cyber-attack. Though it may be possible to craft laws in such a way to account for attempts so that some law is violated before the actual attack. For laws to work and deter, perfect attribution is required.

A second issue is more technical, attribution with the reality of botnets. Do you punish the owner of the computer who ended up being in a botnet? The Recording Industry Association of America (RIAA) tried to sue every computer owner that was uploading copyrighted material. This approach failed and caused awful public perception of the RIAA. It also failed at having large enough deterrence to end copyright infringement. One problem is that the victims are the same people whose cooperation is needed. If the fear of punishment is so great on an action one believes to have little control of, the individuals may avoid the Internet. There needs to be a simple way to defend ones computer before one is accountable for its actions.

A third issue is cyber activities that are not illegal, but results may be confused with illegal actions. One needs to be careful in constructing laws so that only the malicious actions are punishable. For example, a DDoS attack and flash mob have the same effect, same methods of occurring, but different motivations. The DDoS attack can overwhelm a website with too much traffic. The Slashdot effect swamps websites with real traffic from a news website, Slashdot (Malda 2000). The purpose of the attack is to disable the target. A DDoS on Amazon.com may be an entire botnet visiting the website to in effect overload it and prevent it from being available for actual customers. The flash mob is similar, but the purpose is not to deny service. On Thanksgiving Day, November 23rd, 2006, Amazon.com ran a sale of 1,000 Xboxes for $100 instead of the normal price of $300 (The Associated Press 2006). The rush of traffic to the website brought it down for everyone. The service outage was not the response to an attack but a rush of individuals all doing the same thing. There was no crime in this event, but is easy to confuse with a cyber-attack. The rush of traffic is nearly impossible to determine if it is a DDoS or a flash crowd if the DDoS attack is crafted to look like real traffic.

An underlining problem with international agreements, such as the cybercrime convention, is that the only behaviors that are criminalized are those that all parties agree upon, the lowest common denominator. The net effect is that only the lowest common denominator is outlawed. These differences are often pronounced when comparing countries with different cultures. The United States is a proponent of free speech, but in Thailand it is illegal to insult the king (BBC News 2007). The country banned YouTube over several insulting video clips. It is unlikely to have insulting the Thai King to be an international law that all countries cooperate to find and arrest the insulting individuals. Cooperation is unlikely to find those located within Thailand and it will not happen to those outside the country.

The consequence is that any cyber security strategy must include defense and proactive approaches to the security threats. Securing cyberspace requires a multi approach response. There is no one simple solution to the problem. Criminalization and international standards have a role, defense and offense must be played too.

A developing nation must determine what cybercrimes are valid for them and criminalize them. Without the laws, removing the cybercriminals is nearly impossible. It is frustrating when one cannot stop a cyber-attack. Signing and ratifying The Cybercrime Convention should also be an early step at starting to secure cyberspace. However, laws alone are an insufficient strategy to secure cyberspace in both developed and developing nations.

Conclusion

Policy makers in ICT emerging nations have many sources of guidance to draw from when developing a strategy to respond to the cyber threat. These sources include international organizations, governmental agencies, consultants and CERTs. The common theme of the guidance is the transplantation of approaches, laws, regulations and organizations created in ICT developed nations to respond to their cyber threat. One common recommendation is for the establishment of a national CERT, an organization that specializes in cybersecurity and especially in the aspects that are of national significance. CERT activities often involve coordinating others to cooperatively respond to cybersecurity problems. Their actions can be grouped into four categories: proactive services, reactive services, artifact handling and security quality management.

Current recommendations also imbue some perceptions. The first is that policy makers in ICT emerging nations are unaware of the cyber threat. The research finds that they are very much aware that there is a threat, but do not yet have a great deal of depth. The second is that ICT emerging nations have a large and complex cybersecurity problem that is similar to the one in ICT developed nations. The problem is actually still fairly small as ICT emerging nations have yet to heavily integrate ICT into society. The third identified perception is that all countries have a similar ICT infrastructure. While the technologies are similar, ICT emerging nations are using them in different ways and for different purposes. They are at times leapfrogging over older methods and adopting the latest. There are also different primary access methods such the increase in use of wireless and low powered devices. The fourth assumption is that ICT emerging nations have large and or complex governments. It is not always true. The fifth item is that ICT emerging nations can pay to have a similar solution. The research found the affordability is a significant obstacle for implementation of guidance. Finally, laws and enforcement are an important component, but should not be the entire strategy. In summary, this chapter finds that approaches in ICT developed nations cannot be directly transplanted, but rather requires customization to the needs and the situation of ICT emerging nations. In the next chapter, the benefits of ICT deployment are determined so that guidance can be improved and customized to protect these benefits.

Chapter 3 – The Motivation for ICT Adoption and Cyberspace Defense

Gaining an understanding of how to defend cyberspace in a developing nation needs an understanding of how ICT (information communication technology) is being used and how it is expected to be used in developing nations. Outlining the perceived benefits from ICT deployment helps sets the motivation for implementing cyberspace defense. Protecting these benefits from cyber attackers should be one of the objectives for a national strategy and so it is essential to know what they are. This understanding of the motivation is beneficial because it gives an objective to the cyberspace defense strategy. It defines what is to be protected and thus it is possible to target the defense to particulars instead of generalities. In the future, it will also be a way to evaluate performance by determining if the benefits were protected.

This chapter is organized by first explaining why governments invest in information and communication technologies (ICT). Their motivation is discussed by examining how ICT is used in developing nations and its benefit for education, agriculture and government. These are just parts of a developing nation's overall goal, to grow economically. The research on determining what the benefits of ICT to a nation actually are, has not yet provided a complete and definitive answer, but there is a general acceptance that increase ICT use is beneficial and has positive return on investment. Part of the difficulty is that ICT use has also non-economic benefits, which are difficult if even possible to quantify. For example, how does one quantify the ICT benefit to democracy that results from greater individual participation and involvement in government and politics? The perceived benefits of ICT encourage governments to invest in ICT because the optimal level of ICT is above the level that would only be provided by private investment. This chapter uses Rwanda as an example to illustrate these points. Some developing nations, including Rwanda, believe that benefits are so great that they are attempting to transform their society from an agrarian to an information society. The chapter concludes with a discussion on the four requirements for an information society and how it compares to the ways the Rwandan government is investing.

Why Governments Invest in ICT

The view that technology is good is shared by many, in both developing and developed countries. There are people that view increased ICT as a necessary component for further growth. For example, this view is shared by both mature Internet using countries, like the United States, and the newer adopters, like Rwanda. Both governments are investing to increase Internet use within their countries. The United States Government is investing in rural broadband. In the stimulus of 2009 (The American Recovery and Reinvestment Act of 2009 (Recovery Act)) $9.7 billion were set aside for rural broadband (Federal Communications Commission 2009). Rwanda is building a fiber backbone, connecting the country to the submarine cable infrastructure, to drive down the cost of broadband in Rwanda. The reason that both Rwandan and the American governments are investing in the Internet is that they believe that more Internet use is good for their countries.

An additional motivation exists for developing nations. ICT is seen as a way for a country to stand up and join the world community. Some countries, such as Rwanda, are using ICT to transform a subsistence agricultural economy into a knowledge based economy similar to the United States'. This transformation to knowledge based society is part of Rwandan President Kagame's vision to lead his country away from the causes of the horrors of the 1994 genocide. Some scholars, especially Jared Diamond, have attributed part of the motivation for the genocide to subsistence farming (Diamond 2005). They argue that Rwanda's high birth rate and land scarcity created small family farms (1/7 of acre per person) that were barely able to support the family. Individuals killed in hopes of obtaining more land and improving their family's quality of life. Subsistence farming hardly implies a future genocide, as it is but one of many contributing factors. Improving the quality of life of all Rwandans is nevertheless a priority and President Kagame believes that ICT is the tool to do so. His belief stems from the general expectation that ICT is a benefit to all aspects of society especially: education, agriculture, government, communications, health care, standards of living in urban and rural areas, national unity, and particularly the economy. But the research on the actual macro level return on ICT investment is inconclusive. Education, agriculture and government are three areas in which this thesis will further discuss in further detail the interplay with ICT.

ICT in Education

Technology is being applied to education with the hope that it can be the device to improve the educational system. Integrating technology into education has three main objectives. The first is to increase ICT literacy, 2nd to improve education by learning with it, and finally 3rd to apply learned skills and knowledge.

Beginning with the 2nd point of using the technology to learn with, using ICT can improve education, more precisely can transform education. ICT is viewed as a partner of the student in his or her academic development. It plays a role greater than just as knowledge repository. ICT is used to transform and improve academic education in the United States and other similarly developed countries (Benbunan-Fich 2002) (Stigler and Hiebert 1999) (Twigg 2004). At least it is that belief that motivates developing nations in investing in ICT for education. ICT transforms the classroom from lecturing and textbooks to a student centered classroom. In this new environment, the student works in multiple directions on different activities at the same time and the teacher is a guide. Instead of being an information sponge, the student becomes an active participant. The guiding principle is that an education is more than the ability to regurgitate information. Being an active participant is important because the Internet greatly increases the amount of information available to students and thus forces the student to learn critical thinking skills where they can evaluate information. Another way that ICT improves education is by helping teachers overcome the student complaint of the lack of an apparent connection from the lesson material to the real world. ICT can help make the connection clearer and thus motivate the student to higher achievement. Another transformation is a shift from knowing to knowing how. The old idea with textbooks was focused on the skills of recall and memorization, inert knowledge, instead of the new focus on higher level thinking skills of analysis, using knowledge, metacognition, and thinking with data. Technology is not a requirement for this transformation but it fits well in a student centered classroom.

ICT can improve education in ways other than being used in a student centered classroom. In a poor developing nation, ICT enables students to have access to information that was inaccessible and unaffordable before. The Internet has many free and informative websites, like Wikipedia, that can be used as information sources by students in any location. Wikipedia is a replacement to a printed encyclopedia and it is far cheaper than the encyclopedia volumes. The site is free, and the only costs are the Internet equipment and Internet access. Wikipedia may not be appropriate for citations especially in academic setting or scholarly publications (Wikipedia 2010), but it is beneficial when considering the lack of academic resources that are accessible to students in ICT emerging nations. Wikipedia is not the only informative website online. Universities have started posting high quality content online. For example, Penn State University published many academic papers online and Massachusetts Institute of Technology has posted thousands of courses online via its Open Courseware website (Massachusetts Institute of Technology 2010). Books are also becoming free online. For example, Google and publishers have been posting books, journals and magazines online and Project Guttenberg has been distributing books in the public domain. Conferences also often publish articles and presentations online and some even stream presentations online such as conferences like NANOG, Blackhat and Defcon. There is a general trend toward more and more quality educational materials online. With ICT, Information can be distributed electronically and instead of having maybe one book for the entire class; each student can see the information on his or her own computer screen.

ICT enables students and teachers to be able to do more than just passive reading and knowledge absorption. For example, teleconferencing allows students to have interactive access to other students, teachers, experts and other resources that normally would not be available (Morel and Tagert 2007). These technologies require active participation on the remote end unlike a webpage. Learning and education are more than reading and ICT can help students in developing nations to have opportunities to interact with more people. It enables them to overcome distance issues.

The 3rd goal of using ICT is using technology to apply learned skills. It is reflected in the belief that technology may make learning more fun and thus a student will enjoy the experience and want to continue learning. Computers allow students to use word processors to create reports and other publishing tools to create a variety of other projects such as presentations, construct displays or simulate events. Students can use presentation software to create oral presentations. With the benefit of technology, students are able to do more and create personal projects. A student can do much more with a webcam and video editing software than with pens and paper. The communication technologies allow the student to expand beyond the classroom by communicating with other students and presenting their projects to the Internet community. The desire of a young student to communicate online will force the student to learn reading, writing, sentence construction, grammar and spelling, which reinforces the objective of school, learning skills to accomplish ones desires.   By doing these activities, students learn project design and thinking skills.

Returning to the first point of increasing ICT literacy, the objective is that by using technology and computers in school, it accomplishes the goal of having students become proficient in the use of technology and computers. Computers are technologies that are transforming the world and if a student is incapable of using it, the student will be unprepared to enter the world and be a productive member. Computer kiosks are used for common tasks like check-in at airports, to rent movies, or to even apply for jobs like at Wal-Mart and Lowes. Computers are even more vital to more knowledge based tasks such as college, engineering with CAD software (Computer Aided Design), rapid prototyping and CNC (Computer Numerically Controlled) tools, journalism and accounting. To be a productive member of the information economy one must have computer proficiency and technological literacy skills.

In a nation that is transitioning from an agricultural or perhaps industrial to information economy, ICT skills must be taught somewhere. School is a logical place, as these skills are needed almost as much as reading and writing. Students are not likely to pick up the skills naturally from their environment, as would be the case in developed information based economies. In the United States students aged from eight to eighteen spend about an hour or two per day on the computer and are exposed to different types of technology for an average of eight to twelve hours per day (Foresman 2010). These students are immersed continually in the technologies and often the students have greater computer literacy than teachers and other adults.   This concept has penetrated culture to the point that there are many comics that show parents asking for help from kids including help with parental controls. Education needs to be appropriate to the level of literacy students and society has. Even in actual reading, writing and vocabulary, there are different proficiency levels and schools have adjusted to continually develop the students' abilities. Computers and technology should be no different.

Teachers along with students can benefit from ICT in education. Communication between teacher, student and parents can also be aided by ICT. Traditionally the student is the medium of communication between teacher/school and parents. It is a biased and often unreliable medium with its own interests and goals. ICT, specifically the Internet enables parents to be more aware of the student's current grades and active assignments. An active parent by using ICT can be a much more active participant than before with limited additional burden on faculty. The benefit of this relies more on the parent and ICT is an enabler.

ICT benefits teachers by allowing them to create lesson plans more easily by pulling resources from the Internet. The resources add significantly to what textbooks offer. They include pictures and videos, for example. In total, the computer and the Internet allows a teacher, as it did for a student, to have access to a larger body of knowledge than before. This information can be found more quickly with a computer than by using a set of reference books and the data is likely to be more current. It enables the teacher to be more productive and have greater knowledge depth and breath, which can improve the quality of the instruction.

Teachers who use ICT often need to spend less time on administrative tasks like recording grades. An electronic grade book can calculate midterm and semester averages automatically instead of manually computing each result. It also allows teachers to use a word processor for creating handouts and tests/exams. This staple of ICT can save time during proof reading and revisions and in creation with copy and paste. The software enables teachers to create more polished and professional documents and be able to communicate better. When a word processor is integrated in communication technologies, teachers can share materials and ideas within a school and without. It is possible for teachers to collaborate in creating materials more widely and easily than in handwritten material world (Roblyer and Doering 2010). The ease of revising a digital document may allow teaching materials to be revised when the revisions were not time efficient in the hand written creation process. In general, ICT technology allows a teacher to create better teaching material, as the document creation process is much faster and simpler than without ICT.

The benefits also include the new ways of learning and access to new resources for education. Finally, the benefit of ICT in education is that it allows students to apply their knowledge and skills to projects. Teachers benefit from ICT as it allows them to communicate better, have access to more information and people. ICT transforms education and is not simply an elective.

As education is important for future growth, a cyberspace defense strategy needs to protect ICT so that it is able to be utilized for education. Protecting all these benefits is among other goals, which a good cyberspace defense should accomplish.

ICT in Agriculture

Agriculture is a substantial employer in many developing nations. For example, most Rwandans practice subsistence agriculture. The collection of ICT in agriculture is called e-Agriculture. ICT can be used for information dissemination and communication and decision making. ICT can enable the farmer and family to grow beyond subsistence farming, by informing him of new crops or of ways to increase efficiency and contribute more to the local economy. Even if at first computers and communication technologies may appear as to be of little concern for the farmer; in fact it has the potential to help farming and also to improve the farmer's livelihood.

The ICT projects in agriculture in developed nations are different from developing nations. In the developed nations, farming is a capital intensive operation using sophisticated technologies. With capital, ICT enables precision farming, using GPS controlled auto steering tractors for driving and planting in straight lines (Das 2009). Precision farming can use satellites to build highly detailed maps of fields. The maps enable farmers to apply the exact correct amount of fertilizer, pesticides, irrigation, etc. to one meter resolution instead of field wide averages when combined with GPS auto driving (Heald 1999). However, ICT plays a very different role for rural farmers in developing nations, practicing subsistence agriculture.

Information dissemination is the first component of e-Agriculture. The objective is to provide the rural farmer the knowledge to farm better. A better farmer grows more food and is able to have surplus and make money from selling it and improve the life of not just the farmer and the farmer's family but also the country. Lessons include information on crop rotation, irrigation, pest control and farming techniques. The Bill and Melinda Gates foundation has worked on information dissemination and found that portable DVD players with video lessons were very effective. The foundation held contests with local farmers to find best practices and disseminated the information (Penn 2008). Pakistan has created websites where information can be exchanged between farmers and has expanded to social media like Facebook and Twitter (Pakissan 2010). The list of projects that have done information dissemination is extensive.

A farmer needs more information than just the best techniques and practices. The farmer is highly dependent on the weather. From citrus growers in Florida needing to know if frost and freezing temperatures are coming to rice growers' need for rain, weather plays a vital role in agriculture. ICT has also enabled rural famers to have access to local weather forecasts and long range projections. The weather information enables the farmer to better respond and prepare for upcoming weather. The long range projections are useful for deciding what to plant. The farmer wants to plant crops that are suitable for expected weather conditions.

The best crop to grow based on weather alone may not be the best crop to plant. ICT has enabled farmers to better understand market prices so they can see prices and decide what to plant. With better understanding of how much crops are worth, the farmer can optimize his planting. At harvest time, ICT has enabled a farmer to see market prices without having to travel to the market. The famer can decide which market is best and if it's worth even going. Some farmers sell their crops to middlemen who then take the crop to market. This knowledge of market prices limits the prices that middleman, people who take the crop to market, can charge. The farmer is at a better bargaining position when he knows what the true value of the crop is. One assumption here is that the farmer has other options for selling his production; it is a competitive market. This would not be the case if there was only one middleman with monopolist power. The farmer would still be in a take it or leave it position. The ICT used in learning market prices is often a phone call to a family member who lives near the market. Likewise, when it comes to other products farmers need to buy, they can find the best price and are in a better position to negotiate with middleman (Blommestein, van der Krogt and Lamoureuz 2006).

The main role of agricultural ICT in developing nations is enabling farmers to have better access to information for improving farming techniques. It also provides the farmer with accurate current information so as to enable the farmer to buy and sell goods closer to their actual value. The lesson from agriculture for cyberspace defense is that first the user is a subsistence farmer and the strategy must have realistic expectations of his capabilities in defending his ICT equipment and that keeping the devices operational is a main goal.

ICT in Government

Governments have been the first users of computers. The first computer, the ENIAC, was designed and built to calculate artillery firing tables for ships in World War II (Randall 2006). The United States Census Bureau in 1890 began using technology with mechanical tabulators and punch cards (Census Chronology n.d.). Technology and government use have been closely connected. Developing nations' governments have been much slower to adopt technology than the United States government, but are rapidly deploying e-government initiatives.

E-government, (electronic government,) is the process of governmental functions occurring electronically. This is a very broad definition and thus a vast amount of projects fall within e-government. Often e-government refers to an initiative to build a governmental website, but the term is used more broadly. Many governments have e-government initiatives, offices, departments and/or portals. The United States has an

Office of E-Government & Information Technology in the Office Management and Budget within the White House (Office of Management and Budget n.d.). It is used to post documents related to the budget so the documents are publicly available. This is an example of government to citizen communication. The other types of communication relationships are: government to business, government to government, and government to employee.

The government to citizen relationship characterizes electronic interactions between citizens and the government. Governments can use electronic means to inform, by posting information online for example. The US Census Bureau posts the census results online. The FBI (Federal Bureau of Investigation) posts the top ten wanted fugitives online. It is an electronic version of the posters that are found in post offices and is an example of static content. The government's interactions with its constituents can have different levels of interactivity: static content, online submissions and connected government. The online submission interactive level allows the constituents to submit data to the government while the connected government allows for information to flow from one government entity to another.

Forms are an example of the levels of interaction. The most basic allow for the citizen to print the form, static level of interaction. The more interactive allow the forms to be found online and submitted online. Each increased level of interaction is more complex and thus more difficult to build and maintain and the complexity increases the difficulty to secure. The risk associated with each service is highly dependent on the service. Estonia allows for online voting for elections, a service that must be highly secure and trustworthy. American opinions vary over whether they can achieve that, but it has been secure enough in Estonia (Borland 2007).

The motivations for e-government are varied. To Internet users who are accustomed to online services, the e-government services are something they expect. The government has high expectations to meet, as the private sector has set the bar of expectation with 24/7 accessibility, online services, and rapid response. Government physical services have been traditionally anything but having those properties. The government invests in their online presence to match the online offering from the private sector. A second motivation is that e-government services have the potential to enable the government to be more efficient and be able to respond more quickly much like an online private enterprise.

E-government programs can do more than just offering services online by connecting the various services together. A connected e-government is capable of sharing information in the backend, electronically, between government entities. Backend systems are ICT systems that enable an organization to function like a database. Government agencies often have separate online presences and users must access each and information does not easily travel from one service to another (horizontal); nor does it travel from federal to states and local (vertically). An example of the potential for a connected e-government is illustrated by the process to obtain a photo ID in Pennsylvania for a non U.S. citizen. In Pennsylvania, the state issues identification cards, so in a connected government, an individual would go to the state's department of motor vehicles to obtain an ID through their website and get confirmation to be able to get one’s photo taken; instead of needing to obtain and physically present documents from the Social Security Administration, a Visa if applicable from the Department of State, and proof of residency. The state then verifies the information is correct, by sending papers to other government entities such as the Department of Homeland Security. The system takes weeks for the information to flow and be confirmed. In a connected government the information would electronically flow to any organization that needs to approve or deny the application. Connected government systems enable faster information flows and therefore a more efficient and quicker responding government.

In government to business interactions, an e-government can offer online services appropriate for businesses. Business.gov is the U.S. federal government’s website that offers services and information tailored to business. That includes information on marketing, taxes, laws and regulations, and starting and expanding businesses. The relationship is similar to the government to citizen relationship but customized to the needs of businesses.

In addition, governments have commercial relationships with businesses. They are customers of businesses. Their systems and processes can be designed to interact with the businesses’ systems to improve efficiency and accuracy. In New York State, local governments use the Internet to buy office supplies, saving them 10% of the cost of supplies (Cook, et al. 2002). In Pennsylvania, contractors can bill the government electronically for services performed by using e-mailing excel spreadsheet forms. ICT has enabled these governments to be more efficient and more accurate in their commercial relationships. The growing level of adoption of ICT by the private sector of developing nations should lead to an improvement of the quality of the relation between the private and public sectors in those nations.

Governments are not one homogeneous organization. There are many moving parts and agencies, departments, and ministries that need to be able to communicate with each other. Relationships within government and to other levels of government are characterized as government to government. This describes a vertical relationship, so the City of Pittsburgh, Allegheny County, the Commonwealth of Pennsylvania and the US federal government can share data and can interact with each other. For example, the county electronically interacts via e-mail and databases when providing services that the state pays for. The type of services and interaction levels are similar as before with information and services appropriate for other governmental entities. Governments also need to coordinate and share information horizontally. Horizontal information sharing helps different entities within the same government coordinate. This can be used when a government organization is dependent upon another government organization for some type of service or information. During the Russian and Georgian 2008 South Ossetia War, attackers aimed at the Georgia websites including some used to command and control within the government (Shachtman 2008). The Georgian government was using a website to post orders from the President.

The final type of e-government interactions are between the government and its employees. Employees have different needs than any of the other groups and electronic services can be beneficial for them also. For example, employees could use

ICT to find forms and submit changes for reimbursements or for modifying direct deposit account information.

All interactions between government and citizens, businesses, governments and employees rely on similar technologies, but the content is appropriate for each type. It is about making information and services more accessible and being able respond to electronically submitted requests.

The United Nations surveyed its member nations on their e-government programs and ranked them based on sophistication. The results were conclusive and unsurprising, the nations one would expect to perform well, did, like the United States, Denmark, Sweden, South Korea and Australia (Bertucci 2008). In general, technologically developed nations had governments that were technologically developed.

Governments must also buy and setup ICT. Governments often use those technologies at a large scale, like for example the accounting system being developed in California (Hsu 2009). There are the advance technological purchases and build outs: servers, datacenters, and SQL databases. These are important, but an ICT emerging nation’s early purchases and builds are more mundane, but no less required. They include computers, local networks, e-mail accounts and Internet connections. There is the process of creating digital offices that fully use ICT, such as enabling government personnel to e-mail with each other and with non-governmental people. This type of digital office is being built by a World Bank project to add ICT into the Rwandan government (World Bank 2006). The goal of this project is typical of ICT projects for governments. The objective is to improve efficiency, accountability and capability of government employees. While these types of projects have already been done in developed nations, they are yet to be done or just have been done in developing ones. This type of project cannot be ignored in favor of the more Internet presence services.

The governmental computer systems are an important resource to protect. These systems contain personal and sensitive information and with increase use, they become vital for the operation of the government. Protecting government systems can rise to the level of a national security issue. For example, in Rwanda, the Senate and Parliament operate nearly paperless (Orlale 2006). Each elected official has to carry a government issued laptop and vote electronically. These computer systems contain important government secrets, which have to be protected. It is also important to keep the integrity of the data, i.e. make sure that it hasn't been modified by unauthorized parties. One can easily imagine why outsiders, enemies of the government, neighboring countries, would like to have access and even modify that kind of information to influence or interfere with the government. Another possibility is to cause an outage to hinder timely operation of the government. Computer secrets are not solely the domain of the senate and parliament. Many government agencies have sensitive computer information including the military. One could imagine a hacker introducing to the system fake military orders with devastating consequences. This is important in Rwanda, as there are still rebels against the government based in the democratic republic of Congo (RDC), who could operate more effectively if they knew the military and government secrets. These are just a few examples of how ICT is a national security issue and since the government is a large user of ICT and it should put considerable effort to secure it.

ICT for Economic Growth

ICT for economic growth or development is the main motivation for ICT deployment. The research, papers and reports on this topic are somewhat inconclusive. Still it is generally accepted that education is correlated to personal income as it was seen in 1940 census data that the better educated males earned more (Schultz 2001). So investing in education is not only to improve the quality education, but it is also an investment in the human capital of a nation. Along with the government, Individuals view education as a worthy investment because they pay for education. They do this because they believe it will improve their lives by enabling to hold better paying jobs than they would have without the education (McMahon 1999). Beyond improving the standards of living, governments invest in education as it benefits society as a whole (Psacharopoulos 1998). Educated people provide beneficial externalities to the society. Although these externalities are difficult to quantify, educated people tend to cost less in social programs and they are less likely to be incarcerated (Eichaer n.d.). Whether a statistical correlation can be interpreted as a causal relation is often problematic.

In Africa, there are high expectations from education and especially primary education. There are great benefits from literacy and numeracy as both are needed in modern societies (Castro-Leal, et al. 1999). Higher level education, colleges and universities, have been proven to be important to national productivity, competitiveness and economic growth (Bloom, Canning and Chan 2006). They can help lead to technology leap frogging and faster growth. In other words, education is needed for improving a nation and ICT is a way of improving education.

ICT can benefit the economy through education, but also through its effect on the quality of governments and its services. ICT enabled governments can analyze data and govern better. Communications within a government are greatly increased with ICT as well as between government and other parties. Better government leads to better management of the economy and economic growth; well-chosen tariffs, and precisely target education and health projects to achieve greater returns on the investment (Castro-Leal, et al. 1999). ICT enables governments to be more efficient and to use their resources better.

ICT is a driver of economic growth in more ways than just in education and government. It can drive growth in the economy as ICT products/capital and as value added (Colecchia and Schreyer 2001). During the 1990s, the United States business sector doubled the rate of ICT capital growth to 34% a year. At the same time of growth, the cost of ICT was falling. One third to almost all Gross Domestic Product (GDP) growth can be attributed to ICT capital.

The cheap cost of ICT capital has created a substitution effect between ICT and labor in developed nations with expensive labor. Labor in parts of Africa is still cheaper than ICT capital and thus Africa and developing nations will have a different optimal balance between the use of ICT and the use of human labor. The best approach is still the one with the highest rate of return whether it uses ICT or labor. A common type of labor replaced by ICT is low and unskilled; however unskilled labor in Africa is cheap.

For example, the approach used to lay long distances of fiber is a large group of men digging with hand shovels instead of a few men using heavy equipment. ICT won't replace cheap labor until the labor is no longer cheaper or available.

ICT producing industries are not needed for a country to experience growth due to ICT. For a developing nation, it does not need to have its own ICT industry, to be able to grow due to ICT. ICT is able to diffuse into other industries and create growth. It can use the technology, capital, and improve its industries. ICT enables agriculture to be more productive, as well as manufacturing and transportation industries. The farmer using a cell phone to learn market prices to negotiate a higher price for his crop is an example of how ICT can improve other industries.

ICT is being adopted in developing nations for multiple reasons. First, ICT has been deemed a main driver of economic growth in developed nations (McGibbon 2005). From this fact, developing nations view ICT as a requirement for their growth. Secondly, an advance telecommunication system is needed for foreign investment (Wilson and Wong 2003). Having ICT is now a perceived requirement for a developing nation to be competitive globally and achieve economic growth.

Information Society

For a developing nation to increase the standard of living, one possible model is to try to become an information society. Rwanda is trying to build an information economy that will enable it to become a middle income country. This goal was laid out in the President Kagame's Vision for 2010 (Republic of Rwanda 2008). The motivation of the vision is to improve the lives of all Rwandans. Such a goal is good for Rwanda, even if it appears unrealistic to some. Alternatives to an information economy have significant impediments. For example, if Rwanda wanted to become a manufacturing hub, it would have to overcome serious handicaps. An important requirement for being a manufacturing hub is ease of importing and exporting goods. Rwanda is a land locked country with poor physical transportation infrastructure to the rest of the world. Importing and exporting goods is thus difficult and expensive. This makes manufacturing a challenging proposition. But the other option that Rwanda keeps the same agricultural economy is not desirable either. The population is currently mainly involved in subsistence farming and with much of the population still very young. For a country like Rwanda, which is one of the most densely populated in Africa, this societal structure is unsustainable. Due to the lack of available land, subsistence farming will be unable to expand to provide employment for the children when they become adults. This pressure for land and the resultant small farm size is believed to have been a contributing factor to the 1994 genocide (Diamond 2005). It is important for President Kagame and Rwanda to eradicate the factors that contributed to the genocide and therefore the emphasis for changing the society. The transition to an information society does not raise the same kind of difficulties as a transition to a manufacturing economy or staying the same, and it has the potential to improve the country. As a result, the government is attempting to transform the society from agrarian to an information society. There is hope that the young population can make the transition more easily as traditionally young people can learn new skills faster than older people especially in technology. The present Rwandan government believes that the future for

Rwanda is in becoming an ICT center for sub-Sahara Africa and eventually the world. To become an information society, research has identified four pillars: ICTs and connectivity, usable content, infrastructure and deliverability, and human intellectual capability (Johnson, Ariunaa and Britz 2005).

Rwanda is investing in connectivity, the first pillar. It is replacing its satellite links with fiber connections to the submarine cable infrastructure through Uganda to Kenya (Kisambira 2008). The first connection was to the SEACOM cable in 2009 (Rwandatel 2009). In an effort to expand capacity, lower prices and increased reliability (Wafula 2010), Rwanda has a $24 million program with the World Bank to connect to the other two Indian Ocean submarine cables, EASSy and TEAMS (Malakata 2008). These connections are expected to be operational in 2010. Connecting Rwanda to these submarine cables is challenging, because Rwanda is a landlocked country. It thus requires the cooperation of neighboring countries to create a path. The path is created by both Rwanda and the neighboring country laying fiber lines to meet at the same point on the border. Because the neighboring country may not have a connection to a submarine cable either, the process is repeated until an ocean is reached. This process takes time and capital to complete. For the new connection to submarine cable system TEAMS, the path has been through Uganda to the landing station in Mombasa, Kenya (RNA Reporters in Nairobi and Kigali 2009). The EASSy project will have two distinct fiber paths and be able to utilize the landing stations in Mombasa and in Dar es Salaam, Tanzania (EASSy 2010). To do this, Rwanda is also laying fiber to Tanzania. The new connectivity greatly increases, three times, throughput and capacity and is expected to reduce latency and packet loss. Through these efforts to increase international connectivity, the price for international phone calls and data is expected to greatly decrease, 99% or from $3,000 to $25 per MB/S (Majyambere, Internet costs to reduce by 99 percent 2010), and thus become more affordable for Rwandans.

The second pillar, usable content is more of a challenge than connectivity. Developing nations do not need to depend on themselves to create content. They can leverage the content and services that already exist. They don't need to create a new social network website or a video sharing site. They can leverage the services provided by Facebook or YouTube, for example. The question remains whether the existing content is suitable for the locals. The sites may be designed for the preferences and styles of other countries. Language can be another barrier; Kinyarwanda and Swahili are the dominant languages in Rwanda, yet only Swahili may be used on Facebook while it lacks Kinyarwanda and YouTube lack both. Kinyarwanda does not have a written component, so that is a significant barrier for using it online. There is progress to create Rwanda specific content with an online version of the New Times (Rwanda newspaper). More can be done as the .rw dns registry is still small.

Infrastructure and deliverability is the 3rd pillar. It might sound similar to the first pillar, but the difference lies in that the first pillar is concerned with external connectivity, the connection from the country to the rest of the Internet, while the third pillar is focused on the internal infrastructure, the capability of delivering the Internet to the end users. Rwanda is building out the infrastructure, through both DSL and wireless. It is subsidizing cell phones for rural farmers and has a universal access fund so that the entire country may have some type of access to ICT. The goal of the national fiber backbone is to drive down the cost of broadband Internet connections. Lower prices translate into increased adoption.

Human intellectual capability is the fourth and final pillar needed for an information revolution to occur. A high quality Internet connection with quality content is useless for someone who fails to understand how to use it. There are multiple components that need to be addressed. First, does the end user know how to access content online? This includes the basic operation of an Internet connected device and the ability to browse websites. Secondly, one must be able to understand the content online, the person must be literate or there must be enough content and services available for the illiterate. The Internet is still text heavy, but is gaining increase usability for the illiterate. Another component is whether the human capital has the capability to expand beyond consumers and create content. For example in the case of YouTube, one capability level is to be able to browse, search and view videos but to be able to record, edit and publish videos requires another capability level. The ability to innovate and incorporate ICT in already existing businesses requires still another level of capability. There is skill and knowledge involved in integrating ICT and gaining the efficiency associated with ICT. However, as ICT causes transformation, building in respect to ICT efficiencies might be easier and more successful than modifying an existing organization to adopt ICT. Finally, building the human capital capability is a difficult task as it is not an item one can buy in the same way as the other pillars.

Rwanda is educating its citizens in a variety of ways. As part of their universal access fund, they educate the citizens of the newly connected villages. Technical education is provided through the Kigali Institute of Science and Technology (KIST) and the government is attempting to build centers of excellence that focus on development. Each of these initiatives focuses on different components of building the human intellectual capital.

Transitioning from an agricultural society to an information society is not completely without precedent. Finland did that. This is a complex and protracted process. The arctic weather of Finland may make it appear far removed from sub-Sahara Africa, but Finland has also gone through the transformation that Rwanda now looks towards. Finland was an agricultural economy and relied on its forests. It has now become a high tech education information society (Etta and Elder 2005). It was very poor and not well connected to the global markets and technology. It launched a program to become an information society and Finland has become a high tech society. Linus Torvalds is the Finnish creator of Linux (Linux Online 2007). Finland now has very high cellular phone penetration and scores high on other statistics of information societies. The four pillars were integral parts of Finland's transformation. While it might have taken Finland decades to become an information society, developing nations will be able to develop faster as they leapfrog intermediate technologies. As will be discussed later, Finland's response to the demands of cybersecurity can be an example of how poor and little developing nations can organize.

Cybersecurity and the culture of cybersecurity is lacking in the theory of the four ICT pillars. It can and should be integrated into each one. The growth of Internet capacity will make Rwanda have a larger cybersecurity problem. Rwanda will have more capacity to receive attack traffic and the country will a better target. One reason they are a better target is that the computers within Rwanda will have faster Internet connections and as a result be more useful to botnet operators in tasks such as transferring files and sending SPAM. They are also better targets as more valuable information is put online. Also increasing the size of the cybersecurity problem is the rapid growth of Internet users because there are many more potential victims and more equipment that can be compromised. A future with a larger cybersecurity problem is not inevitable. The infrastructure can be built with security in mind and distributed. Teaching can include a cybersecurity component and content can be both secure and be about security. As no country has done an excellent job at cybersecurity, developing nations on the one hand have no template to follow, on the other hand, they have an opportunity to build from the beginning with security in mind. They can learn from the experiences and mistakes from those who went before and take a better approach than what was done before. When security is implemented it is often viewed by users as a burden and an inconvenience. Perhaps people who are unaccustomed to cybersecurity will not view cybersecurity as a burden but rather the way it is if they are introduced to security from the beginning.

Rwanda is making an effort to install each pillar to be able to transform its economy from subsistence farming into an ICT economy as Finland has done, but the four pillars of an information economy should include security.

Public/Private Investment

There are several reasons why information and communication technologies (ICT) are deployed in countries. The two dominant motivations are private investment with expected private returns, and investment for economic development. The economic development return is economic growth and sustainable job creation (International Telecommunications Union 2009).

Private investments in ICT are common in developed nations. For example, Verizon, a conglomerate of several of the baby bells, invested billions of dollars in a fiber optic network to the home which allows them to offer FIOS (Fiber Optic Systems) services and earn a return on their investment. Investors have debated whether the return on the infrastructure is positive over fifteen years (Hansell 2008). The societal benefits of FIOS aren't directly considered by Verizon or its investors when deciding how to proceed when faced with an obsolete copper infrastructure incapable of handling modern data needs. The decision for Verizon is based on what is best for Verizon, which is to maximize profit. When business interests line up with societal interests, which is the case for FiOS, there is no need for public involvement.

Society has benefited from Verizon's large capital investment. In many locations the new FIOS service has introduced a competitor to the services offered by the cable television company. It can compete and exceed their offerings in maximum Internet speed and in the amount of high definition television channels. The benefit for the consumer from competition is real. Verizon FIOS has offered faster Internet speeds and more high definition channels than had existed before. Verizon's competitive service has pushed the cable companies to invest in their infrastructure to be able to match the offering from Verizon. There is more urgency to upgrade when one is losing customers to a service, which one cannot technologically compete with. Comcast has deployed DOCSIS 3.0 and has been transitioning television channels from analogue to digital to improve its consumer offerings.

The increased speeds of FIOS have enabled consumers to use technologies that were previously impossible under the speeds provided by cable companies and DOCSIS 2.0. One example is streaming HD video from ones house. Other uses for extremely high speed Internet are expected to be invented as high speed Internet access becomes more prevalent.

It is possible to have private investment for ICT infrastructure in areas that have sufficient economic resources and sufficient population density. The population density is an often cited reason of why Japan has much faster Internet access than the United States (Harden 2007). When an infrastructure is being built through private investment, the first regions receiving it are the most profitable and that stops at the point where return on the investment is no longer great enough. In that case there can be market failure requiring some public involvement.

One mechanism of market failure stems from the fact that market private entities, do not include the value of externalities as part of the return of their investment. Externalities include social benefits and social costs. These benefits and costs are external to the private investors and are not considered in their optimization and as a result the societal optimum is not achieved. In the case of Verizon FIOS, the externalities include the lower Internet access prices and pay TV subscription prices (Breibart 2008) from increased competition and the increase of speeds and value of new services available. The amount of investment, area covered, that is optimal for Verizon's return is different from what is best for a community. When Verizon was negotiating franchise agreements, many city councils have pushed for citywide build outs that enable everyone within the city to be able to subscribe. New York City, Philadelphia, Washington and Pittsburgh have all required Verizon to make FIOS available citywide (Neibauer 2009). There is value to the city for a citywide network and that value is an externality. Verizon agreed to these contracts because the return on investment for an entire city is large enough to be attractive. The highly profitable areas effectively subsidize the unprofitable areas instead of being profit for Verizon.

Private investment builds infrastructure in developed locations like New York City, Pittsburgh or affluent suburban neighborhoods. Unprofitable regions are not built with private investment. The broadband Internet is just the latest of series of infrastructures to be built. Each had an underinvestment in unprofitable areas, which are usually rural and poor. In the 1930s, 90% of urban people had electricity but only 10% in rural areas. The rural farmers were too poor to pay for the high cost of electrifying the rural areas as each share would be large due to the large distances and low population density. President Roosevelt created the Rural Electric Administration to bring power to rural regions. He believed it was the government's responsibility to ensure everyone had access to electricity (Benader 2008). The problem with the rural areas reappeared with the telephone, clean water, and now again with broadband. The Department of Agriculture's Rural Utilities Service has programs to further develop rural areas (United States Department of Agriculture n.d.).

One view might be that very little of Africa could financially support new ICT infrastructures as it would appear not to be a profitable investment. However, foreign direct investments have invested heavily in ICT in Africa (International Telecommunications Union 2009). Forty percent of investment in Africa has been foreign direct investment. Much of this investment has been in mobile phones. Each type of investment is private, public or a combination of both. Private investment alone in a developing nation is not optimal for the country and thus the governments had to step in to achieve a more desirable investment level and desired infrastructure. Rwanda has multiple private cellular providers: MTN, Rwandatel and TIGO. These carriers cover much of the country including safari areas (Lacy 2009). MTN is a South African company, TIGO is based in Luxembourg, (Millicom International Celluar S.A. 2007) and Rwandatel's majority shareholder is the investment arm of Libyan government (Butera and Kanyesigye 2010). The TIGO cellular network covers most of the country and many locations not covered, are covered by the Rwandatel network. The quality of service is seen favorably even by visitors from the United States. The services provide not just GSM voice but 3g data also. CDMA EV-DO is also available for data and likewise, WiMax for fixed locations. Cellular service is a profitable business in Rwanda and has drawn investments from multiple international organizations. Rwandatel was bought by the Libyans in 2007 with an agreement that it needed to invest $87 million (Cellular News 2007) and the license for the third carrier had four organizations interested in it before it was awarded to TIGO (Cellular News 2008). A fiber backbone has been built to support the data demands of the wireless subscribers. This capital investment reinforces the profit in the mobile market.

Perhaps the International interest in Rwanda's cellular communication is based on expectation of the market. The percentage of Rwandans with a cell phone is rapidly increasing. By 2012, RURA's (Rwanda Utility Regulatory Agency) target is for six million subscribers or about 50% of the country population from about two million in the beginning of 2010. Rwandatel added 420,000 subscribers in the first six months of 2009, starting at almost zero in the beginning of the year when it launched its new GSM network (Cellular News 2009). Also illustrating the expectations of the market, Rwanda is now home of a mobile handset factory which is a joint project between a Chinese company and RDB, (Rwandan Development Board), a development branch of the government (Cellular News 2008). Contributing to the expectations of a large market are the government's actions. To increase the use of cell phones in rural Rwanda by farmers, the government is subsidizing phones. The government pays 50% of the cost, MTN 25%, and the farmer pays the remaining 25% (Majyambere, Rwandan Gov't Buys 35,000 Phones to Boost e-soko Project 2009). The project's success increases with higher participation rates. Over 53,000 phones have been bought with this program (Cellular News 2008).

Rwanda is also on a major fiber optic cable build-out. Unlike in the United States, the objective is not to create a fiber optic last mile, linking homes to the Internet, but to create a fiber optic backbone. The backbone interconnects the major points within the country and will eventually connect Rwanda to the rest of the world. This is a separate infrastructure from the fiber used to support mobile telephony. The US has had a copper based backbone originally, which has been upgraded to a fiber backbone as the technology matured and in response to demands for increased speed and capacity. The early tests occurred in the mid-1970s with the construction beginning around 1980 and with large amounts being laid in the late 1990s (Hecht 1999).

Rwanda is currently building its fiber backbone in rings for redundancy and following existing roads. The project will lay about 800 miles of fiber for the national backbone. There are two technical objectives with this project. The first is to increase accessibility to broadband and have increased capacity. Most links presently are either wireless microwave links or DSL/ADSL links over copper, data links on conventional phone lines. However, these links are not the main bottleneck in Rwanda. Rwanda is dependent on satellite links to the rest of the world. The backbone will enable Rwanda to have fiber optic links to its neighboring countries and to reach the submarine cables in the Indian Ocean. As Rwanda is a landlocked country, it must connect to its neighbors to reach the ocean.

Developing nations, including Rwanda, must stop relying on satellite links. First, satellite links are technically inferior and secondly much more expensive. The price makes it too expensive to be affordable for the majority of Rwandans. Compared to long distance fiber optic cables, satellite links have higher latency, the time for data packet to reach the other end. The signal must travel from earth to a satellite in geostationary orbit and then return back to earth. The orbit is about 22,000 miles above the equator thus the signal must travel about 44,000 miles (That takes about 250ms). The latency is visible during television broadcast where someone is communicating to someone across a satellite link. There is a delay associated with the response. The latency prevents some interactive applications from working well. A remote desktop session, a connection that allows for the remote administration of computers and servers, would have poor response times due to the long data transit times. Likewise, multiplayer video games would be almost unplayable. VoIP, a telephone conversation, becomes very noticeable when parties are separated by a satellite. The limit for American call centers is 500 milliseconds, which is within the range of 450 to 550 milliseconds latency provided by satellite service (Mitchell 2005).

Satellites also have less capacity for data when compared to optical fiber. The limitation can be attributed to limited frequencies available that can penetrate the atmosphere including clouds and other weather conditions. Satellite users must also share capacity. While it may be possible to purchase a set amount of bandwidth, and have it called dedicated, the total traffic must be less than maximum capacity. If a satellite over Africa has X mbits of capacity, all users must share that X mbits of capacity. How it is divided up, is a different problem.

What satellites do offer is to provide access to unwired locations. To access the Internet, make telephone calls, transmit and receive TV and video from locations without an accessible wired connection in the region are the benefits. Satellite links are great for rural areas where connectivity is important and there is no other available method.

The lack of competition from other services and the ability to operate with little additional infrastructure and the high cost of components make satellite connectivity expensive. The high cost of international connectivity drives up the costs of an Internet connection within the country. The price a subscriber pays for Internet access must include not just the price of the physical connection, but also the price of the subscriber's international bandwidth use. One approach to reduce the price of Internet access is to reduce the price of international bandwidth. The Rwandan connections to the submarine cables are expected to drive down the cost of Internet access in Rwanda by 40% (Kezio-Musoke, Rwanda's national backbone fiber optic cable set for 2009 2008). Lower prices enable more people to be able to afford to connect and use the Internet. Rwanda would not be able to achieve its goal of becoming an ICT center without a fiber backbone and connections to the submarine cable infrastructure.

Rwanda may have had in the past little infrastructure, but its ambition of becoming an ICT hub of Africa has put it on the trajectory of having a modern ICT infrastructure. Rwanda shows that cellular communications are a profitable area for private investment. However, many individuals still cannot afford the equipment or the services and in these cases the government needs to be involved as the country can benefit from increased ICT use. The higher capital cost of infrastructure projects requires much more government involvement as the return on investment is less than in cellular.

Private investment and foreign investment can fund some projects, but others, like the national fiber backbone require the government to pay when the financial realities of the project do not have a sufficient return on investment. The infrastructure is needed to support an information economy and an information economy is needed to pay for the infrastructure, thus one must be created first. The infrastructure can exist without the economy to pay for it if someone, like the Rwandan government, pays for it.

In a developing nation, cell phones and smart phones with data are very likely to be available as even in the incredibly poor Rwanda, foreign investment found it profitable to deploy the infrastructure. Smart phones with data service like blackberries and Apple iPhones (or copies if not the actual) will be present. The infrastructure to support the traditional computing infrastructure of desktop computers, servers and data centers might not actually be built without government funds or at least funds from sources other than private investment.

Conclusion

The allure of the benefits of ICT is so great that governments in developing nations are investing in ICT. These benefits need to be protected from cyber-attacks, as they are important to the country. The governments must invest when the private sector fails at providing the socially optimal level of investment and cyber defense. This occurs because the private sector attempts to maximize their private rate of return and does not value externalities, benefits and costs not captured by them. ICT has externalities that benefit agriculture, education and government and cyber-attacks that have costs. The improvements in these sectors are believed to lead to economic growth. The use of ICT is believed to grow an economy including those economies that do not produce ICT products. The perceived benefits from ICT have encouraged some developing countries to attempt to transform their society into an information society. To be able to transition, four types of ICT are needed. These include having a high quality and affordable communication system within a country and between that country and the rest of the world. This also requires having information technologies that are beneficial to the country and the human capital to be able to use the ICT infrastructure. The question is no longer should a country invest in ICT; it is happening. An effective cyberspace defense strategy is needed in ICT emerging nations to maximize the return on their ICT investments. In the following chapters, this thesis discusses issues that an effective national cybersecurity strategy considers.

Chapter 4 – Issues to Address to Improve Guidance

The previous chapter laid out several ways that ICT can transform a country. This chapter examines how current guidance informs ICT emerging nations on how to protect those expected benefits. The primary field to focus on is ICT use in government, because ICT in agriculture and education are presently not very susceptible and not a specialized situation as the use is a change in content rather than a change in technology. This chapter's objective is to identify weaknesses that contribute to the perception that guidance is not completely appropriate. For each identified weakness, the chapter will argue why it is a weakness and discuss related information.

Prescriptiveness

In analyzing guidance, recommendations and proposed strategies, the issue of prescriptiveness must be addressed. Prescriptiveness is about specifying exactly how something should be. It is about rules and directions. A recipe is a common form of prescriptive directions. The problem with prescriptive recommendations is that they are inflexible and have difficulty in dealing with constantly changing issues. Cybersecurity is one of those constantly changing issues that present a challenge to prescriptive direction. The best practices of today are likely to be different tomorrow. It would also be very difficult to craft prescriptive recommendations robust enough to be correct for a diversity of situations. The approach used in current guidance is not to be so specific, prescriptive, that the guidance becomes obsolete very quickly and is inappropriate for multiple countries, situations and technologies. Instead, it is about describing flexible approaches that can adapt to changing threats and technologies. It thus requires the recipient to make decisions on details.

This lack of specifics in guidance is one of the frustrations expressed by Rwandan policy makers. When trying to secure a technology or system, non-prescriptive guidance is not particularly useful. One challenge for the Rwandan policy makers was determining how to secure the Rwandan DNS country domain, .rw. There are no set of instructions within current guidance on how to secure a DNS domain or how to migrate to the new securer protocol DNSSEC. This example shows the challenge of determining precisely what to do, when one needs the solution today and not after training or researching as cyber attackers are not waiting for countries to build capacity.

Instead of providing a set of instructions, what guidance provides is an organizational structure, a CERT, for Rwandans to build, which would determine the details of how to secure their DNS domain. In effect, guidance is prescriptive about what to have for determining the answer rather than providing the exact answer. Another common approach in being prescriptive is to release toolkits, which are a series of steps to find a solution. It is formulaic and not much thinking is involved as the analysis was done by the toolkit maker. If one inputs values of one’s situation into a toolkit, the output is supposedly a customized solution for one’s situation. Often these approaches also fail at capturing enough situational nuances to produce the intended quality of output.

Dealing with prescriptiveness is a challenge when trying to evaluate the effectiveness of guidance in protecting the ICT benefits outlined in chapter 3. One cannot evaluate the effectiveness of the proposed configuration to secure a technology. Instead, the method used in this chapter is to determine how well guidance leads to the determination of what should be done.

ICT in Agriculture

Protecting the benefits from ICT use in Agriculture should not be the focus because the technologies involved do not presently have a large threat and do not need specialized cyber defense programs. Using ICT for improving agriculture was discussed in the previous chapter. The technologies typically used have low cyber vulnerability. Two discussed examples were the Gates foundation using portable DVD players and Rwanda subsidizing cell phones for farmers. Portable DVD players are not susceptible and basic cell phones are minimally vulnerable. The more susceptible ICT technology in agriculture is websites like those used in Pakistan. Furthermore, using cell phones or websites to improve agriculture does not require additional or special security when compared to generic cell phone and website use and protection. The result is that governments do not need to take special actions to protect these technologies. If the general security programs are sufficient then the agricultural benefits are therefore also protected. This means that the governments should not make protecting ICT in agriculture a priority because current guidance does not need to be tailored in regard to agriculture. Agricultural ICT does not therefore need to be further discussed in this thesis.

ICT in Education

ICT has the potential to transform education, a topic of chapter 3. Like with agriculture, the technologies in education are not presently demanding government attention. The technologies involved are desktop/laptop computers, One Laptop per Child (OLPC) laptops, and ICT appliances. These ICT appliances are technologies that are not computers. In general, appliances are devices with limited functionality and are not general purpose computing devices (Ziltrain 2008). Some categories of ICT appliances are home electronics, game consoles, video conferencing systems and e-readers, and some example products from these categories are TIVOs, Xboxes, Cisco TelePresence and Amazon's Kindle. The second technology is the OLPC. It is a laptop envisioned by Nicholas Negroponte and designed for students in developing nations. OLPC computers are being deployed in about 34 developing countries (OLPC 2009), including Rwanda, which has a program to deploy 120,000 of these low cost computers (OLPC 2010). The third technology is the vanilla laptop and desktop computers that are used globally.

Protecting educational ICT projects in Rwanda is presently a simple task, because very few of these technologies are presently connected to the Internet. For example, due to the lack of Internet connections and electricity, the OLPC program is being deployed without an Internet connection for the computers. Another related issue that limits ICT use is that the majority, 96%, of schools do not even have electricity (OLPC 2010). The consequence of the educational circumstances in Rwanda is that the Rwandan experience does not shed much information of how well current guidance addresses ICT in education. The security implications of each of these technologies will be evaluated next.

OLPC Security

While Rwanda may not presently need to be concerned about securing OLPC computers, their rapid deployment of Internet access and the goal of a national WiFi hotspot, leads to the conclusion that securing OLPC will be an issue in the future. At this future point, will guidance lead Rwandan policy makers to security? In answering this question, a study of present day Tunisia is not informative concerning OLPC because it is not deploying OLPCs. The OLPC is a unique security challenge because it has a different security model than traditional computers. Instead of restricting access to files, the OLPC operating system, Sugar, restricts functionality (Krstic n.d.). This approach is starting to be also used in smart phones such as Android (Android Developers 2010). At the time of writing this thesis, how to secure OLPC computers is unclear (Felten 2007). Instead, what is important is the flexibility to implement security practices when they are developed. This is likely to happen with the current guidance, because the deployment in Rwanda does show that OLPC deployments are done with a close partnership with the OLPC organization, the world’s best experts on the OLPC. This suggests that the current model is sufficient to protect OLPCs, assuming the OLPC organization acts responsibly to secure the devices. It implies that the security of OLPC computers does not presently need to be the focus of the Rwandan government.

ICT Appliance Security

These devices are difficult to attack and difficult to secure. The difficulty comes because the manufacturer decides what programs can run and which cannot. Outside security people have thus limited influence on the appliances. Just about the most one can do is to follow the current best practices from the manufacturer. Current guidance does lead ICT emerging nations to adopt current best practices. It is then likely that current guidance is sufficient for ICT appliances in education. These appliances are also not very common and not a major issue and should not be presently considered a high priority.

Traditional Desktop and Laptops Computers

Traditional computers are found everywhere. In schools and for education are just one potential location and use. Securing these systems is difficult for everyone everywhere. While these systems are used in developed nations, the traditional computer is too expensive (Kinetz 2010) for mass adoption in developing nations. When these computers are deployed, the use for educational purposes does not require a change in approach to secure. If the guidance is effective in other fields then it is likely to be appropriate here. This means that the thesis does not need a present focus on improving guidance to protect the educational benefits from the use of traditional computers.

Agricultural and Educational ICT

Securing technologies used in education and agriculture is currently not a pressing issue to Rwanda. In education, the technologies are usually not connected to the Internet or are not in such numbers to be a large problem. In agriculture, the technologies are not very susceptible to be a major concern. As protecting these benefits is not the most pressing issue, there will be no further analysis and discussion on ICT for education and agriculture in this thesis.

ICT in Government

The protecting of ICT in government is the major issue. The benefits are deliberated in Chapter 3. It is important and should be the focus because governments, including Rwanda's, are rapidly adopting ICT. One example is the often referred $10 million e-Rwanda initiative from the World Bank to deploy ICT into the Rwandan government. In addition, the consequences of a successful compromise are potentially large. For example, Rwanda's parliament and senate are conducting business entirely electronically with government issued laptops. These computers contain sensitive information that should not be released publically. There are also databases with private information that need to remain private and correct. One such database in Rwanda is a database linking a person to an IP address (RURA 2009). Finally, the technologies used are more vulnerable and more difficult to secure. For example, securing a database is more difficult than securing a cell phone for agricultural purposes. The solution that is often proposed is the establishment of a national CERT.[2] The following sections discuss three reasons on how the situation is different and what can potentially be done about it. This is followed by a discussion on recommendations and the role of government.

[2] Guidance and national CERTs are discussed in Chapter 2.

Weakness of Current Recommendations

When considering what advisors recommend for a national CERT to do in ICT emerging nations, three particular issues are not well addressed. The weaknesses are that nations have differences in ICT architecture and ICT use, they have fewer resources but also they have different resources to use. Another such difference is the common lack of a private cybersecurity sector. The first section shows that each of these weaknesses exists from examining how guidance directs Rwanda to secure its government ICT systems. Each weakness is then analyzed for potential responses.

The Argument for the Existence

Differences in ICT use

The fact that there is a difference in ICT use among nations is obvious. These differences in use create a different level of need for effective defense. By examining the Rwandan electricity system, it is clear that the Rwandan government is presently not responsible for cyber security of the electricity system nor should it spend considerable effort in defending it. The evidence suggests that the Rwandan government needs an appropriately sized response, which is far smaller than the responses found in more developed nations.

Some nations are heavily depended on ICT and the Internet, like the United States, and others are barely, like Rwanda. Most nations are somewhere in between these extremes. The recommendations are usually from the more dependent countries and do not fit well with the less dependent countries. For example, considerable effort in the U.S. cybersecurity strategy is dealing with critical infrastructures. The U.S. has identified 17 sectors including water, energy, communications, and information technology (Department of Homeland Security 2010). In a country like Rwanda, recommendations on protecting the critical infrastructures are untimely. Rwanda has not yet gotten to that level of ICT maturity. Their policy makers listen politely, but they are not yet facing that problem in this area. They do not have critical infrastructures that are significantly using the Internet nor would they considerably suffer from the effects of successful cyber-attacks.

In addition, when they do have modern high tech projects, these projects are not being operated by Rwandans, but rather by international companies. ICT security is likely to be part of the responsibility of the operators until Rwandans take over operations or when the operators fail in dealing with cyber threats. One such critical infrastructure is the energy sector, which is a growing sector as Rwanda needs additional domestic electricity production. The largest completed energy project in Rwanda is a new 20 megawatt power plant (Ndikubwayezu 2009). Rwanda is also home of the largest solar energy plant in Africa (Asiimwe 2007) and a 25 megawatt plant is being built that is powered from methane gas captured from the waters of Lake Kivu (ContourGlobal 2009). These plants are being built and operated by international companies. The Lake Kivu plant for example is being developed, built and operated by ContourGlobal a company headquartered in New York City. The solar project was built by Juwi Solar from Colorado and is being financed and operated by Stadtwerke Mainz AG from Germany (Juwi Solar 2007).

The Rwandan government does not need to be responsible for the cybersecurity of the energy sector because it does not build, own or operate the large components in the electricity sector and the present consequences of cyber-attacks are not unbearable. Even though the American electricity grid is also operated by the private sector, it would be incorrect to reach the same conclusion. The major difference is that the American energy infrastructure is extremely vulnerable and the consequences would be significant. The American government needs to be involved because the private sector has not adequately addressed cybersecurity in respect to the large externalities that would result from an outage. There is thus a market failure, which encourages government intervention.

This issue of the consequence of a successful attack needs to be considered. It is a way of defining how large the risk is and how large the response should be. The research found that infrastructure outages are not as consequential in some countries. In the electricity system, the fear from a cyber-attack usually involves a cyber-attacker causing a blackout. The blackout is often considered a terrible consequence because of the expectations of the power grid in countries like the United States. In 2003, a blackout affected 50 million people, in a wide swath of U.S. and Canada, from Michigan to New York (Holguin 2003). The consequence was that people were stuck in elevators, Cleveland's water system was inoperable as vital pumps lost power, airports had to cancel flights, road tunnels were closed, trains and subways stopped running, and the blackout disrupted many other electrical dependent tasks. The cost has been estimated from $4.5 billion to $8.2 billion (Electricity Consumers Resource Council 2004). In a country like Rwanda, the electricity supply is far less reliable. People must plan for outages. Rolling blackouts are even part of the energy management plan as the country's demand outstrips the production capability (Haines 2007). It is not likely the country would suffer much additional harm from an additional blackout. People are prepared for a power outage as blackouts are a fact of life. Improving the reliability of the energy supply is a priority, but until then, the consequence of a cyber-attack on the energy infrastructure appears far less than catastrophic. Using the theory of benefit cost analysis, one can see if the benefit is low, avoiding the cost of a blackout, then one should only spend a low amount to avoid it. At some point in the future when Rwanda is a more developed country, the consequence will demand an extensive response.

The lessons from Rwanda for other countries are that while many of the critical infrastructures are not the responsibility of Rwandans, the government should be just capable enough to be aware of the situation to know when there is a problem and how to start the process of dealing with it, with perhaps the regulatory approach used in more developed countries. This low level is appropriate, because currently there are small consequences from a successful cyber-attack.

ICT Architecture

The architecture of ICT is closely related to the use. Both impact the other. How one would design it is influenced by how one intends to use it and vice versa. In Rwanda and many other previously unwired nations, wireless is the dominant form of last mile connectivity, the connection from the infrastructure to the user. This is the consequence of the fact that wireless technologies are cheaper, easier and faster to deploy than a network of hardwires. The wireless infrastructure has also contributed to the dominant access device, cell phones and smart phones. Current recommendations do not address this situation, but this does not mean there is a failure here. It is an issue of prescriptiveness, as guiding principles should not be centered on how to secure a specific technology. Instead, the question to ask is whether the institutions and recommended approaches will help a country like Rwanda determine what to do. Assuming that a country could follow the recommendations, the answer is yes. The CERT is a team of experts that specialize in cybersecurity and is likely that they could determine an approach to follow. However, as will be discussed, it is unlikely that a country would be able to create such a competent institution at the present.

Limitation of Resources

The study found three resources that are of a different nature which makes it a challenge to build an institution like a CERT. The first is restrictive monetary resources; the second is the difficulty in training personnel; and the third is that many countries do not have a mature private cybersecurity sector. These weaknesses need to be better addressed so ICT emerging nations can have more appropriate advice.

Monetary

The restrictive financial resources have a major role in defining what a country can accomplish. Countries often try to build the most cost effective solution that fits well to their needs. Both Rwanda and Tunisia have followed their own path.

When there is abundant money, a country can follow the approach done by Qatar and hire top level experts from CERT/CC to build a CERT (Software Engineering Institute 2005). Even then, there are challenges, such as dealing with a different culture.

Most other developing nations have less money to spend because they are not an oil rich country like Qatar.

Some of the costs for building a CERT is paying the salaries of the experts and providing their training. These issues in the case of Rwanda become important when one considers the size of proposed organizations. A few experts are affordable, but many are not. Reducing the number has an impact on the amount of work that can be done by a CERT. Instead of providing a long list of activities, it needs to be determined what tasks and capabilities are the most important. In the case of Rwanda, the task that is most important is having someone that is aware of what is going on about cybersecurity and can provide insights, guidance, advice and connections. The research for this thesis found that Rwandans have a need for prescriptive information for their situation. They also have a challenge in determining which issues need outside help and which do not. This person can triage situations and either provides the answer directly, shows a resource that has the appropriate information, or determines whether outside consultants are needed. Rwanda has started to create this team within the Rwanda Development Board, with Charles Mugisha being the first member.

Tunisia is in a different situation. Its CERT, tunCERT, has taken on considerably more responsibility, but it is years older and better funded. The activities it chose to do were based on what it could provide to Tunisia rather than following international recommendations. TunCERT was largely built from domestic resources. Its early focus was on helping Tunisians be safe online. It provided information for children to be safe from online predators; it helped users install security patches by distributing patches on

CD and giving presentations in public; it also provided free malware removal from computers brought to the CERT. The CERT activities were not limited to just keeping individuals safe, but also companies and the government. To do that, the head of tunCERT, Nabil Salhi, drafted a law for requiring auditing and for protecting those who came to the CERT with problems by preventing the CERT from informing law enforcement. Further activities of tunCERT are described in Chapter 2.

Both Tunisia and Rwanda have policy makers that are not initially building large institutions, but rather starting with organizations that are small and cost effective. They try to find solutions that have the highest return on investment. Future guidance could be improved by making recommendations for partial packages.

Training

Training is closely linked to monetary resources, but not completely. There are two challenges for training. The first is finding affordable training and the second is finding training for what is needed. Existing training programs are typically designed for teaching specific skills. Some classes teach how to handle incidents and others how to ethically hack (SANS 2010). Globally the list is extensive and classes are offered by many, including consultants, CERTs, CERT collaboration groups, universities and Internet organizations. However, when trying to find appropriate training for Charles Mugisha from Rwanda, it was a challenge to find a suitable program. Many classes were either too expensive or not on useful topics for him.

The types of classes that they wanted were on topics that are difficult to be self-taught. They also looked for learning skills on which further skills could be built upon.

For example, theory and thinking processes contain tacit knowledge, which is learned from experience. They wanted to learn how to approach a situation or technology. These are generalized skills, which can be applied to multiple situations and are helpful for long term sustainability. On the other hand, training on technical details was far less desired, because those were topics that someone intelligent could figure it out from books and information online.

In identifying a curriculum with these properties, one organization, National Defense University, stood out. It provided classes which were affordable and would teach him useful hands on skills that were tailored to help secure vulnerable high risk systems in the developing world, particularly Africa. However, enrolling at NDU is a bureaucratic challenge as it is funded by the U.S. government. Charles was eventually sent for training in India.

In building tunCERT, training was also a challenge. They ended up becoming self-taught. However, it was easier than it would have been in Rwanda, because tunCERT was able to draw on the Tunisian universities to provide skilled employees. A few of the technical experts in Rwanda have also had university education, but from non-Rwandan universities. The university graduates in Tunisia may not have had the specialized training in cyberspace defense, but they were technically very good. They had the ability to be able to learn the needed skills for beginning tunCERT. Since then, they have continued to develop and have become quite good. In fact, they have helped Rwanda by visiting, providing guidance and training.

Both Rwanda and Tunisia show that there is a difficulty in finding training that is both affordable and useful. They need training that is focused on teaching tacit knowledge and theory.

Private Sector Differences

There are several approaches found in recommendations that rely on the private sector. There is a problem with these recommendations because usually ICT emerging nations do not have a private sector that is cybersecurity capable. This becomes an issue concerning regulatory approaches, auditing, and in providing incident handling.

The regulatory approach concerning cybersecurity deemed to be the best in the United States is the FERC/NERC model (CSIS Commission on Cyberspace for the 44th Presidency 2008). FERC, Federal Energy Regulatory Commission, are energy regulators and NERC, North American Electric Reliability Corporation, is an organization of grid operators (private sector). This approach has the government regulators setting objectives and standards, and then the private sector determines how to meet the specified objectives, which the regulators then review and approve. Implementations are verified by the industry, the government and 3rd parties. The theory behind this approach is that the infrastructures are operated by private entities and those entities are in a much better position to determine how to secure the infrastructure than the government regulators. The private entities, owners and operators, understand the details of the system, how it was built and how it operates. The FERC/NERC regulatory approach requires that the operating entities be in a better position than the regulators at determining how cybersecurity should be done. In Rwanda, this is definitely the case for electricity and telecommunications, because international companies are operating power plants and the telecommunications infrastructure. But it is misguided to apply this type of approach with entities that are not better positioned. For example, it might be tempting to have the domestic companies take appropriate action, but they will need additional help. They will not be able to turn to a domestic company for help, as they do not yet exist and hiring an international consultant is an unaffordable expense. The government will initially have to provide some type of help. TunCERT in Tunisia recognized this fact as they offered service to help clean up malware. In Rwanda, the cybersecurity regulators in RURA are still working out their approach, but it involves RURA issuing guiding rules. The lack of a private security sector shows that if ICT emerging nations desire to regulate cybersecurity defense, then they will need to use a solution in some cases other than the FERC/NERC model.

One of the approaches of regulating is requiring security audits. This is an approach used in Tunisia. The details of the auditing program can be found in chapter 2. To improve the country's cybersecurity, there is a Tunisian law that requires certain organizations, both public and private, to receive a yearly audit. This audit is usually a supervised self-audit. TunCERT needed to train auditors as there were no existing cybersecurity auditors. What this shows is that governments need to support the establishment of the private sector if they are going to be an integral part of a strategy. How to best support its establishment would be useful guidance, but is beyond this thesis.

Auditing and regulating are both preemptive approaches to cybersecurity. However, security breaches do occur and require reactive solutions. These events are called incidents. Dealing with incidents is a major component of CERTs, for details see chapter 2. CERTs often coordinate others to form an organized and coherent response. They tackle challenging aspects of incidents and provide useable information to the technically competent. This structure of coordinating and information sharing is a force multiplier as it allows a small organization to have a larger impact. When a non-technically competent computer user in America needs help such as the removal of a virus, this person turns to the private sector rather than to CERT/CC or US-CERT. Instead, they will seek help from the private sector such as Symantec, Geek Squad or one of the many computer repair businesses. In Tunisia, the CERT had to provide these needed services because their private sector was not filling the need. The Tunisian CERT was required to think differently on the mission of a traditional national CERT and offer a different set of activities. Rwanda reinforces the concept of an inadequate private sector. A Rwandan needing cybersecurity assistance has nowhere to turn. The private sector and the government are not yet providing services. The lesson from this immature private sector is that if a CERT is established, the services provided need to be different than the national CERTs in more advance countries. This is a consequence of the CERT being in a different situation with different requirements concerning cybersecurity.

Expectations of Government

The final adjustment for cyberspace defense strategies is incorporating the diversity of expectations and roles of government. The effect is from changes in what is acceptable government behavior. The consequence of this fact is that other countries will find potentially successful approaches that are not already used.

A short description of what Americans expect from government is needed to show how the American perspective of government is not the only perspective and how it influences recommendations. The American government role is traditionally to be involved in cases of market failure, situations where the private sector fails at researching a socially optimal level. This belief was well articulated in the National Strategy to Secure Cyberspace from 2003 (National Strategy to Secure Cyberspace 2003). The government role was to be the "grease" to enable the private sector to perform better. However, enabling the private sector to be better did not result in good enough cyberspace defense. A new role was formed for the government and it was to be a leader instead of a supporting entity in improving cybersecurity. This new role was a conclusion of President Obama's 60 day review on U.S. cyber activities (Cyberspace Policy Review 2009). Americans view the government sometimes differently than the government views itself. One belief is that the government is a hindrance and the opposition, which prevents one from doing what one believes to be right. President Regan captured the feeling when he described people's opinion of government. "The 10 most dangerous words in the English language are, 'Hi, I'm from the Government, and I'm here to help (Reagan 1988)." This is one of the reasons industries self-regulate; to stave off government regulation attempts (Pitofsky 1998). Americans also dislike the government competing with the private sector. This view was clearly visible in the health care debate of 2009 (The Wasington Times 2009). In general, Americans like individual freedoms and a minimalist government, though there is much debate over what is the minimum.

This view is not global. Some governments especially in Asia are paternalistic (Ha and Kim 2002). It is a view that the government knows best and is trying to protect its people from harm. This type of government would perform tasks and pass laws that would not be acceptable everywhere. For example, in South Korea, the government imposed a six hour curfew to help reduce video game addition in kids (Cain 2010). This also appears when governments try to prevent its people from accessing certain information online. Pakistan banned access to YouTube and Facebook over blasphemous material found on those sites (Haider 2010).

Rwanda's government also has taken strong action on freedom of the press concerning ethnic issues. For some context, the media played a central role in motivating people for the genocide. Rwanda has a law that prevents inciting public to discrimination or divisionism (Waldorf n.d.). They also require license for journalists and newspapers, which can be revoked (Commitee to Protect Journalists 2007). It is clear that different countries have different acceptable behavior for governments.

Different expectations of government have an impact on cybersecurity strategies. For example, the U.S. CERT would not directly offer free malware support, but that service is acceptable in Tunisia. In the U.S., US-CERT would probably have to contract with a private entity or entities to provide that service. RURA is preparing guidelines, regulations, to make many organizations take cybersecurity seriously and defend themselves appropriately. They want to be an advice giver to help others protect themselves online. Similar regulations in the United States would cause uproar. It would be totally unacceptable. For example, a bill that would have given the president powers in an emergency was soundly criticized for giving the government power over private networks (FOXNews.com 2009).

In conclusion, what is appropriate action for a government is different for different countries. Thus in making recommendations for a country, one should not be limited to what is acceptable for the American government.

Conclusion

Countries that are in similar positions to Rwanda do not need to invest significant resources and time into protecting the benefits of using ICT in agriculture and education. This is because in these fields, cyber defense does not need to be customized. For a government's ICT protection, action is needed. The recommendation of a national CERT to specialize in the national cybersecurity interest is good, but its size and missions need to be tailored to the country. This customization is needed because critical infrastructure protection is not as vital, there are limited resources and because there are various roles of government. If guidance reflects these differences and adopts the approaches in this chapter, it will be more useful for policy makers in ICT emerging nations.

Chapter 5 – Unexpected Findings

Introduction

This final chapter details the unexpected findings that were uncovered during the research. This research found that the technical policy makers in Rwanda had an unexpected perspective on cybersecurity in which they were willing to accept a lower level of security. This is because they wanted the best affordable security rather than near perfect security, which would be unaffordable for them. This affordability view impacted the choices of software tools used in dealing with cyber threats. They were willing to use cheaper and potentially less effective tools. One potential way of reducing the cost of needed security tools is to use free open source software. There are important questions regarding the use of open source security tools. The questions are whether open source security tools can be relied upon and what types of tools can be replaced with open source tools and what types cannot. This chapter does an initial investigation into answering these questions. This chapter provides ideas to help guide future research on studying the cybersecurity situation in countries that are experiencing a transformation from the Internet.

Perspective of Cybersecurity

One of the preconceived ideas when starting this research was that the governments of the ICT emerging nations wanted and were trying to achieve the same level of cybersecurity that is found in other countries and in particularly the United States. In America, the common view and objective of cybersecurity policy and programs is to have no successful attacks. It is impossible to ever achieve total security, because software is not perfect, and all defensive methods have diminishing returns. The other factor that makes security difficult is that the defender must prevent all methods of attack, while the attacker must only find one successful way. These factors, combined with the objective of the best possible cyberspace defense, leads to expensive programs. The U.S. government is estimated to spend between $2 billion and $8 billion per year on cybersecurity with a growth rate of 5 percent to 8 percent (Sternstein 2010). If one believed that the best possible security was a shared goal, then the challenge would be how to teach, train and guide a country to get to the same destination.

It was surprising that the Rwandan policy makers stated explicitly that as they could not afford the cybersecurity programs found in the U.S., they were willing to accept a lower level of security (still above their present situation). In other words, they were more risk tolerant concerning cyber threats than Americans. Instead of wanting the best possible security, they desired “good enough” security. Defining what “good enough” security means to them and what is their tolerance to risk, are questions for future research. While these still need to be defined, there are lessons that can be drawn. The first lesson is that if one was thinking about guiding them down a path of cybersecurity enlightenment, not only is the path unknown, the destination is not what was expected and worse, it is also currently unknown. This different objective of cybersecurity policy might change what programs, methods, institutions, and training they need and should receive. It shows that to help these countries, one must not only understand their current situation; one must also understand their desired situation.

The other lesson is that it opens up the question of what is the most cost effective national strategy. Analysis of the most cost effective is usually performed for determining the best strategy to achieve a given risk tolerance rather than finding the point where diminishing returns discourages further investment. In other words, when considering costs, what is the optimal cybersecurity strategy for a nation? To help guide ICT emerging nations more effectively, this analysis needs to be performed to answer these questions.

Open Source Tools

One of the ways to reduce the cost of improving cybersecurity defense is to reduce the cost of cybersecurity tools. These tools are vital in building capabilities. These tools include the basic anti-virus scanner, to the complex malware decompilers. Outside of security tools, open source software has been herald as a key component in helping developing economies to build their information technology infrastructure. This section begins to address the policy question of what extent it is possible to solely rely on open source and free tools for security purposes.

A Concept Model of Security Tool Use

This section outlines the use of several types of security tools. The types are anti-malware, patch management, and intrusion detection.

The type of tool that is nearly universally used is anti-virus, anti-spyware, anti-malware, and anti-rootkits software to scan for various types of malicious code. The anti-virus scanners help protect computers from harmful programs and for someone to run a computer without an anti-virus, is negligent. Often this type of tool is the first and most basic level of security. Many anti-virus programs are commercial, such as Symantec's Norton Anti-virus, but quite a few are free and or open source. The objective of a real time scanner is to detect and possibly prevent malicious code from entering a computer as an e-mail attachment, a file downloaded from the Internet, or in a file from another source. Examples of open source antivirus tools are ClamAV, an open source anti-virus e-mail scanning client and Moon Secure, an open source desktop anti-virus client. A client program is a component of the client server model, in which the servers provide data/computational power etc. to the clients. In this case, the client software does the actual scanning and the servers provide updates to the clients. One method to reduce the probability that a computer be compromised or infected is to insure that it has the latest updates including the anti-virus scanner. Updates could be signatures of newly detected malware that an anti-virus client needs to be able to recognize the latest threats. ClamAV and Moon Secure use the same definitions, which are supported by the open source community. It is unclear whether the open source community can keep up and release updates at a fast enough rate.

Updates are also fixes to bugs, which may have introduced a vulnerability that an attacker could use. Determining whether a computer has all the updates for all the software is actually difficult, and there are tools to help both end users and network administrators. Network administrators have the additional challenge of deploying updates across a network. Microsoft has simplified the update process for its software by providing free tools, but many other vendors do not have such a simple system.

Most users currently manage by only having anti-virus tools and updates, but for critical computers such as those with important data or operations, additional tools are used.

Network scanners, NIDS (Network Intrusion Detection Systems) monitor communications looking for patterns that could signify that either a computer has been infected or that someone is attempting to do something malicious. Snort is the leading IDS (Intrusion Detection System) and is open source. Snort is very useful and it was the founding for the Saher monitoring system built by tunCERT in Tunisia.[3] Being a foundation was helped by the fact that it is open source and thus tunCERT could modify it to meet their needs. The practice for some internet service providers, ISPs, is to use NIDS to detect infected computers and then place infected computers in a "walled garden", allowing them to only communicate with security resources so to encourage the user to clean the infection.

HIDS (Host-based Intrusion Detection Systems) are similar to NIDS, but monitor computers and files instead of the network communications. OSSEC is the foremost open source HIDS. A common approach for a HIDS is to build a hash of all files and then detect when a file is modified. A modified file might indicate an infection. IDS are also particularly suited for network administrators to secure an entire network.

Definition of Open Source and Free Tools

There are some differences between free software and open source software. Free security tools are programs distributed for free, but the source code is not open to

[3] The details of Saher can be found in Chapter 2.

the public. In this case, the term is only referring to free as in monetarily free,[4] but is limited to who can use and distribute. A functioning demo is not a free tool, but a tool supported by advertising would be free if the user does not pay. This definition is from the software category of freeware, which is any permanently fully functional software that the user does not have to pay for. Free tools can have limited features to encourage users to pay for the more full featured programs and thus the equivalent of a demo. Some free tools are provided by corporations to drive customers to their other pay services; as shall be shown, this also occurs with open source tools. In rare instances, free tools are provided as a form of corporate responsibility or charity. One important fact is that free tools are only provided for free because the developer wants the tool to be free to that user, and could at any time stop supporting the tool, begin to charge for the tool, or restrict who can use it.

Open Source tools are free monetarily too,[5] but in addition, the source code is publicly available and there is no way to prevent the user from doing whatever he or she wants to do with it, a major distinction from free tools. Source code is the human readable form of computer programs, which can be compiled, converted, into a machine readable form. Going from machine readable back to human readable is a very difficult process and is often referred to as a type of reverse engineering. The source code is often written in programming languages such as C, C++, C#, Java, and FORTRAN. The result of having the source code is that anyone can modify the program to either fix

[4] Free as in Beer

[5] The actual definition allows for a charge for distribution, but the software itself is free. One could charge $100 for a box, but could not force the buyer from redistributing it for less or even free.

bugs or add new features. The users are not depended on a vendor for updates, fixes, or even for new versions. TunCERT has modified SNORT to better fit their needs as a national CERT. Their version has more capabilities to detect threats to the nation of Tunisia rather than being a monitor for a network.

The development of open source programs comes from volunteers. The volunteers are often individuals who choose to spend their own time and effort on the project, but other volunteers are paid by companies to participate in developing a project. An example of paid volunteering is IBM employees who are hired to contribute to Apache, an open source web server (IBM 2010). Several studies have attempted to understand the rationale of why an unpaid individual volunteers for open source projects. Stephen Weber suggested that it may be because by contributing a bit to the project, the final project is worth more in regards to the volunteer programmer than the cost of participating (Weber 2004). It is the same concept of a potluck dinner, where the total is greater than any of the parts. The analysis is an explanation on the very real phenomenon and the programs created can be used even if the motivations of the volunteers are unclear. The benefit to the users, free riders, is that the cost of development is not and cannot be recaptured by the vendor; therefore the end cost to end users may be less.

Giving away the software may initially suggest that there is no way to earn money from an open source project, but this is false. This helps explain why a company would have employees contributing to open source programs. For example, Sourcefire makes money from open source programs. Sourcefire, the company that owns the open source IDS Snort as well as the open source ClamAV, earns money from selling subscriptions to the latest rules, licensing Snort to be in commercial products, and from Snort t-shirts and other paraphernalia. However, to use Snort one does not need to pay anything to Sourcefire. Anyone can create rules, but for most users the cost of subscribing to the rules is cheaper and easier than creating a personal set. Sourcefire also provides pay commercial support for its open source anti-virus software ClamAV for a fee (SourceFire 2010).

There are other methods for corporations to earn money with open source, such as having a feature missing for paying users, often called commercially crippled software. This was a practice for Bitkeeper, an open source project that helped managed the development of software projects. It was a version control program to help manage a software project. Bitkeepker reported a change log to a public website, the equivalent of publishing the code. Someone who doesn't want to have their changes made public, must pay for a crippled version. Developers using Bitkeeper would pay if they are creating a proprietary or internal application. To enforce payment, the software when modified must pass a regression test to be used and the publishing feature is checked to verify its existence (Weber 2004). BitMover has changed Bitkeeper to a commercial product from an open source product as there had been a falling out between the two communities (McVoy 2002).

Open source projects are not lawless free-for-alls, but structured by the license agreements such as GNU GPL (GNU General Public License), Microsoft Public License and BSD licenses (Berkeley Software Distribution). The BSD license is simple, the program must retain the original copyright and license in a readable form in the source code and documentation, and the names contained within the documentation do not imply an endorsement of any kind. The license allows for a BSD license application to be redistributed and even sold. The Microsoft Public license is similar to BSD license, but prevents the source code from being relicensed. The more restrictive GPL allows anyone to use and modify the source code, but it may only be distributed if it retains the GPL license. A great benefit of these licenses is that once a copy is obtained, it can be modified and installed on as many computers as desired with no monetary considerations.

Staying Current

One potential fear of adopting a policy that incorporates open source tools is whether the tools will innovate in a comparable manner with commercial products. The fear stems from the fact that commercial vendors have an added incentive to develop new methods for software to work. However, innovation has been constantly occurring in the software industry and when a great idea does come about, other vendors and the open source community copy and improve upon it. If there are copyright issues, the various communities have developed around them. In a famous example, Xerox invented the graphical user interface with the mouse and was copied by Apple Computers, and in turn by Microsoft, IBM and the open source community. There are many smart programmers and they can incorporate the latest innovations in the products.

Open source programs do have issues with patents. A current suit from Trend Micro on Barracuda Networks claims that Barracuda is infringing on their patents by including ClamAV in their appliance to scan for viruses at the gateway, which Trend Micro has patented (ExtremeTech Stuff 2008). Open source software licenses are not designed for dealing with patents (Byfield 2008). There are a few take away concepts from the suit. First, as patents are only pertinent in the nation where obtained, a developing nation must determine the best way to structure its patent system and in particularly software patents. Secondly, depending on how patent laws evolve in the United States and Europe, it may affect open source software development. There is great uncertainty on how it will change.

Developing nations are currently mainly consumers of ideas. With increased development, these governments will need to consider the policy implications on innovation as developed nations currently do. At some point they will have an economy that can afford the costs of commercial software if they choose to obtain it. Open source software may also transform the software industry and there would be no need for commercial software.

Potential for Market Failures in Open Source

The benefit for open source software in developing nations is clear, it provides software that is free and with the source code public, no one, individual or group, can deny access. If a company that publishes a software title decides to no longer sell the title, then a user would no longer have access to the title. This is not possible with open source programs. The benefits of open source software to nations with limited resources like developing economies are obvious. It has often been argued that open source and developing economies go hand in hand.

To rely on the open source software model to be a key component for securing cyberspace may appear to be risky without an understanding of the motivations involved. It is assumed that all the actors in the open source development process are rational. The only reason a rational entity would participate is if the personal benefits outweigh the personal costs. The logic applies to both volunteers and to commercial entities. One additional aspect is that entities choose how they participate. The project or projects are selected to work on from all the available open source projects. The selection is rational; perhaps it is selected based on interests of the programmer or company. A programmer then chooses which new feature to program or which problem to debug. Acting rationally, the programmer will choose the feature or the bug that has the greatest rate of return for them personally. The remaining question is why someone would participate since a free rider (non-participant) would gain the same benefits without the cost. A corporation benefits if the involvement allows it to be better able to sell service or derivative/complimentary products. Sourcefire is able to sell more subscriptions to Snort rules if Snort is improved and thus has an incentive for Snort to improve. An individual's volunteering motives are less clear, but have been attributed to a variety of reasons including: fun, ego, reputation, identity, personal/collective accomplishment and personal improvement.

However, this situation may be a case of market failure if the developer contributes to an open source project only when her benefit is greater than her cost.

This prevents projects that do not benefit the developer from getting built. Projects that have high value for many programmers attract many programmers. This can be seen in Linux, Apache and OSSEC. An operating system is vital on a computer and thus Linux benefits many programmers. Likewise, a webserver is extremely useful for those serving content on the Internet. This is also seen in security tools. OSSEC is an HIDS that allows network administrators to look for intrusions on computers running a variety of operating systems.

Market forces may not drive the creation of security tools that completely fulfill the needs of developing economies. In these cases there exists a market failure, which has to be addressed. Further research is needed to determine what types of tools would need to be subsidized. A potential failure would be if there was a feature that would have a benefit to a developing economy, but not so much for the rest of the world. One example could be localization for a region or improving usability for the non-security professional. In the usability example, the volunteer programmers already know how the program operates and thus would not benefit for making it easier. Corporate interests that provide support services would have a disincentive to improve usability as that would reduce their ability to market their services. If a task is quick and easy then there is limited willingness to pay someone else to do it. However, a developing nation would benefit as the training costs would be less. In this case, it is reasonable to suggest a possible market failure.

In general, projects that do not greatly benefit individual programmers or organizations with skilled programmers and with the resources necessary to contribute to an open source program, do not get built. An organization would be mistaken if it believed that all open source projects are successful. Projects do not automatically attract developers; the developers must want to participate. Thus not all applications can be built for free. In this case, someone must step in and solve it as there is a market failure, a problem that governments should solve.

2010 Status

Open source security tools may provide the software needed to secure cyberspace in developing nations in the long term. However, that does not imply that in September 2010, a country can solely rely on these tools. Snort, a NIDS with HIDS features, is already a first class product used in Tunisia to support their Saher program,[6] and may even be the leading NIDS; likewise ClamAV is a good e-mail scanning anti-virus program. The areas that need development and improvement are especially with anti-virus desktop clients, where some required features are not yet present. There are market incentives to add these features. In the case of Sourcefire for example, as they have announced in December 2007, they will provide commercial class support for ClamAV at a price. It is logical to think if there is demand for the missing capabilities, they would be added, which was the case with ClamAV. As of September 2010, there is a build of ClamAV for windows with real time scanning (ClamAV 2010). This feature was missing in 2007 when Sourcefire started offering support. While ClamAV is a good program, open source tools are not yet ready for stopping malware, spyware and rootkits. Evaluating the relative performance among tools including free, pay and open

[6] Saher is described in Chapter 2

source tools is not needed for a policy discussion, as the performance of any particular tool can vary significantly between years and especially since cyber attackers are always becoming more refined, requiring tools to be constantly updated, which has already been discussed that open source tools can adapt for future threats. At this point, in a heterogeneous environment of a developing nation's cyberspace, the open source security tools cannot yet, as of September 2010, provide all the security needed.

Conclusion of Open Source Tools

Open Source security tools can be beneficial for a developing economy for reducing the cost of cyberspace defense. However, propriety software is still needed in some instances as some security needs are not currently provided by open source tools. The current status does not imply that in the future these tools will not exist. There are market forces encouraging development and support. The potential of missing out on the next great advancement because of choosing to use open source software is small and would exist even with a propriety security tool.

Conclusion

Researching into cybersecurity of ICT emerging nations finds unexpected realities. Rwanda's policy makers are trying to build cybersecurity capabilities in their own way and are not just trying to copy. They realize that affordability is an issue for them and as a result, they are willing to be more risk tolerant as they have yet to become highly dependent on ICT and the Internet. They want "good enough" security, which needs to be defined. This means that the goals of other countries for cyber defense may not be the same as Rwanda's. One potential way of reducing costs is to use open source security tools, and the preliminary analysis points that open source can be useful, but it cannot yet provide a complete solution. Further research outside of this thesis is needed into these issues.

Conclusion

The research and analysis within this thesis can influence the creation of a developing nation's cyberspace defense strategy. This thesis found that a common approach and proposed frameworks for developing nations have flaws and it further develops and informs how developing nations could better approach their cyber security problems. It finds that developing nations have been trying to copy what is being done in the developed world, which the thesis concludes is not a good approach. The thesis reached this conclusion by studying the cybersecurity problem and the current theory on how developing nations should approach the problem. It analyzed the theory in regards to the researched conditions in developing nations and the effectiveness of programs that they have established. The analyses lead to the conclusion that a better approach starts by identifying differences between developing nations and developed nations and how these differences impact strategies.

The starting hypothesis of this thesis is that a developing nation's strategy should incorporate the most successful already tried approaches many of which are found implemented in the developed world. Often, this strategy is the establishment of a national CERT by the government. A national CERT is defined as a governmental organization whose mission is to defend nationally important ICT in cyberspace, especially the government's ICT and the country's Internet dependent critical infrastructures. Developing nations are increasingly recognizing that national CERTs are a good way to respond to the ever changing cyber threat as several developing nations have established national CERTs. The typical mission of a national CERT is defined by a laundry list of proposed activities including coordination, information sharing and incident handling. The laundry list of activities is frequently based on the services performed and offered by established and mature CERTs in developed nations. This thesis concluded that developing nations need a governmental team to lead their cyber defense, but calling it a national CERT is problematic because the name often implies a predetermined set of activities. This thesis is questioning if this set of activities is appropriate for a developing nation. For clarity in this thesis, strategy is used to describe what a developing nation should do as strategy includes both the actions of the government and the activities of the government team or agency designated for cyberspace defense.

There are multiple examples of developing nations being advised to establish a national CERT. One such example is a consultant's report commissioned by the World Bank to study the cybersecurity situation in Rwanda and make recommendations to secure the Rwandan government's new ICT infrastructure. The report, which was supposedly a study of Rwanda, contained no Rwandan specific information. The authors gave the impression that the solution is universal and does not require knowing the situation in Rwanda. This idea of a universal solution is strongly believed as it is evident in another example, a guide released by the ITU on building cybersecurity in developing nations. The ITU guide included the concept of a toolkit, which if implemented would result in a secure Internet. Both of these examples reflect multiple assumptions that need to be true to justify their approach. The first assumption originates the idea of the universal approach to securing cyberspace. It assumes that each country must do the same thing as the technical solution is the same, because each country has to secure the same types of hardware and software. It also includes the belief that developing countries have the same types of ICT infrastructures to secure that developed nations have including SCADA infrastructures, desktop computers and smart phones. The second assumption is that the strategy and method of securing cyberspace in developed nations is the best solution or at least a good enough solution. The consequence is that effort is being made to have developing nations implement similar programs found in developed nations. The third important assumption is that developing nations have the same goals and desired penetration difficulty level as developed nations when it comes to cybersecurity. It assumes that like the United States Government, developing nation's governments want and are willing to pay for the best possible cyber defense.

This thesis studied the cybersecurity situation by analyzing the cyber threat, cyber defense approaches and strategies in both developed and developing nations, including direct on the ground research to evaluate the hypothesis. It found evidence that leads to the conclusion that the underlying assumptions are not always true, which signals that the hypothesis is not true and that the same cyberspace defense strategies are not applicable to all countries. The main conclusion on the hypothesis is that while the physical hardware and software may be the same, the circumstances in a developing nation are different, which necessitates a customized solution and strategy. The evidence is that developing nations differ from developed nations on the threat against them and the resultant motivation, economy, expectations of government, resources, technical competency, vulnerability, and the lack of legacy equipment stemming from leapfrogging technologies. Each of these differences is expanded on in this conclusion.

Motivation for defending cyberspace is one area that an understanding of the country is important. This thesis studied how developing nations respond and finds that they respond to the cyber threat that they perceive rather than the one that is present in developed nations. Rwanda's government views cyber security as important, but most of the problems are not applicable for them. Infrastructures, such as electricity, water purification, sewage, agriculture and many others, are not usually dependent on the Internet. In the case of Rwanda they do not have infrastructures that are dependent on the Internet and thus CIIP (Critical Information Infrastructure Protection) is not a strong motivation for a large investment of precious resources. Another challenge for mustering resources is that in many cases it is hard to see infections. Detection of cyber events is often poor as many attackers try to remain hidden. The result is that cybersecurity is hard to justify until there is a large visible incident. Without the effects being visible, it reinforces the opinions that cybersecurity is not very applicable to them at this point in time; it will be different in the future. These factors contribute to the conclusion that the strategy be appropriately sized to the country's need and to the country's willingness to implement. The strategy should also reflect the future needs of the country. While these infrastructures do not exist today, they will in the future if these countries continue their rapid ICT deployment pace. The best strategy is for the developing nation to build cybersecurity capacity at the moment it is needed.

The limitation of resources is evident in the allocation of resources to build cybersecurity but the limitation also influences the shape of the strategy and not just the size. During the thesis analysis, it found that the approaches in developed nations rely on their economies' private sectors and especially the cybersecurity private sector to perform vital cybersecurity work. This sector has the technical competency to provide tools, analysis, training, education and experts that are relied upon in the strategies. The government's role is often as a coordinator or as an information disseminator. For the most part, developing nations do not have an equivalent sector and thus the developing nation's government needs to act differently. The activities that the private sector performs in developed nations, may now be needed to be performed by the government's cybersecurity team, until the private sector exists and is capable of taking over. One such activity is determining how to secure ICT equipment and how to clean up after an infection.

The thesis found that a country's expected role of government, influences that government's cybersecurity strategy. Without considering the role of government in a specific developing nation, the strategy may reflect a dissimilar role and harm the effectiveness of the strategy. For example, because the American government's role relies on its mature cybersecurity private sector, a developing nation's government could be encouraged to have a similar role and rely on its cybersecurity private sector even though it is minimal if it even exists. This would result in an ineffective and inappropriate response to the cyber threat in the developing nation. The thesis concluded that the cybersecurity strategy of a nation should have the government's cybersecurity team performing tasks and filling roles that are appropriate for it and that these roles are not the same among all countries or even among all developing nations.

The importance of the differences is illustrated by the actions of tunCERT in Tunisia. TunCERT is the best CERT or cybersecurity program in Africa. One of its activities is providing malware cleanup on computers for free to Tunisians. The malware clean-up mission of tunCERT reflects the concepts that developing nations have more limited resources, a different shape of their economy and have a different expected role of government. The malware cleanup program of the Tunisian government would be an unacceptable role for the United States government as it would be viewed as the U.S. government performing an activity that is best left to the private sector. The US government does not need to perform this role either, as the private sector is able to afford and is capable of providing malware cleanup. If Tunisia had only modeled its response on the U.S., it would not have created this successful program. This program reflects how differences can lead to different solutions and strategies and reinforces a conclusion of this thesis that the defense against cyber-attacks is not universal.

The details of the structure of the ICT infrastructure is not universal either, because developing nations are leapfrogging old and obsolete ICT. This thesis concluded that leapfrogging should have an effect on their strategy. One major area of where leapfrogging is occurring is in wireless communication.   Developing nations are mainly using wireless for last mile communications and people are rapidly buying and using cell phones including Internet enabled smart phones. One of the reasons is that cellular networks are quicker and cheaper to deploy and smart phones are cheaper for consumers to buy, than the traditional landline and desktop computer model found in developed nations. There are two potential differences with leapfrogging in wireless. The first is security differences of using wireless communication and smart phones. The second is the security consequences of having a higher proportion of wireless devices many of which are low powered compared to wired and full powered computers. By studying these two differences, the thesis concluded that the impact of wireless has yet to be realized and developing and developed nations will discover together the cybersecurity consequences of using wireless and smart phones. The implication for developing nations reinforces the conclusion that the best cyberspace defense strategies are flexible and able to respond to the constantly changing cyber threat.

Finally, technical competence and awareness are thought as pressing issues to achieve cybersecurity in developing nations. These areas are of vital importance, but these are not problems for developing nations alone. Much of this knowledge is tacit and teaching in a class or writing it in a book is difficult. The methods to raise are interrelated with the other aspects of a country such as the relationship with the government and how technicians are trained. There are three areas that training is needed. The first is help for policy makers to build a national strategy. The second is for building capabilities in the national team to secure cyberspace and the third is training for the many computer users and administrators in the country. The thesis found global resources that developing nations could use, but often their curriculums are not tailored to reflect the differences discussed in this thesis and would require the developing nation to adapt the knowledge. Many of these resources were also identified as unaffordable for developing nation's governments, especially as these governments are not presently motivated to spend large amounts on cybersecurity. The private sector has even less resources to spend on cyber security training.

This thesis found the theory that developing nations should establish national CERTs similar to those national CERTs found in developed nations, is not the best course of action for them. While the software and hardware used in developing nations is the same, the situation developing nations are in, requires a different approach. A better strategy reflects the differences between developed and developing nations. These differences include that developing nations have little to presently protect and are only lightly suffering from cyber-attacks. Developing nations also have different and often limited resources from which to build a response. Finally, many of the global security resources are too expensive to be affordable. The thesis concluded that the best course of action for a developing nation is not to assume that their needs are the same as a developed nation and they should identify what their current and expected future cyberspace defense needs are and build to those needs.

References

AFP. *New homeland security tool to detect Conficker worm.* March 30, 2009. http://www.google.com/hostednews/afp/article/ALeqM5gYZcCtEaQfLLQNKGa0uT4BKKgfXw (accessed April 8, 2010).

Android Developers. *Security and Permissions.* September 8, 2010. http://developer.android.com/guide/topics/security/security.html (accessed September 10, 2010).

Asiimwe, Arthur. *Rwanda installs "Africa's biggest" solar plant.* June 8, 2007. http://www.reuters.com/article/idUSL0871691720070608 (accessed September 14, 2010).

BBC News. *BBC News.* April 4, 2007. http://news.bbc.co.uk/2/hi/asia-pacific/6528303.stm (accessed September 8, 2010).

Beaubien, Jason. *Wired Hopes for Rwanda.* August 15, 2005. http://www.npr.org/templates/story/story.php?storyId=4800031 (accessed August 11, 2010).

Benader, Lynn. *Rural Electrication Program.* November 21, 2008. http://reference.cooppower.coop/meeting-area-for-workgroups/for-phil/rural-electrification-program (accessed April 7, 2010).

Benbunan-Fich, Raquel. *Improving education and training with IT.* June 2002. http://portal.acm.org/citation.cfm?id=508448.508454 (accessed August 29, 2010).

Bertucci, Guido. *United Nations e-Government Survey 2008.* New York: United Nations, 2008.

BI-ME staff. *Tunis Telecom City project takes off with US$3 billion investment from UAE.* January 15, 2009. http://www.bi-me.com/main.php?c=3&cg=3&t=1&id=29905 (accessed August 10, 2010).

Blommestein, Nele, Stijn van der Krogt, and Lucie Lamoureuz. *ICTs for Agricultural Livelihoods.* The Hague: International institute for Communication and Development, 2006.

Bloom, David, David Canning, and Kevin Chan. *Higher Education and Economic Development in Africa.* Cambridge: Harvard University, 2006.

Borland, John. *Online Voting Clicks in Estonia.* March 2, 2007. http://www.wired.com/politics/security/news/2007/03/72846 (accessed April 7, 2010).

Breibart, Joshua. *What the Verizon Deal Does -- and Doesn't -- Do.* May 2008. http://www.gothamgazette.com/article/tech/20080530/19/2539 (accessed April 7, 2010).

BuddeComm. *Rwanda - Telecoms, Mobile, Broadband and Forecasts.* May 4, 2010. http://www.budde.com.au/Research/Rwanda-Telecoms-Mobile-Broadband-and-Forecasts.html (accessed August 11, 2010).

—. *Tunisia - Telecoms, Mobile and Broadband.* February 19, 2010. http://www.budde.com.au/Research/Tunisia-Telecoms-Mobile-and-Broadband.html (accessed August 11, 2010).

Butera, Saul, and Frank Kanyesigye. *Libya to Expand Investments.* January 20, 2010. http://allafrica.com/stories/201001200007.html (accessed 4 7, 2010).

Byfield, Bruce. *Software patent case defendant seeks support of FOSS community.* January 29, 2008. http://www.linux.com/feature/125807 (accessed January 31, 2008).

Cain, Geoffrey. *South Korea Cracks Down on Gaming Addiction.* April 20, 2010. http://www.time.com/time/world/article/0,8599,1983234,00.html (accessed September 16, 2010).

Carpenter, Jeff, and Julia Allen. *Tackling Security at the National Level: A Resource for Leaders .* August 7, 2007. http://www.cert.org/podcast/show/20070821carpenter.html (accessed April 8, 2010).

Castro-Leal, Florencia, Julia Dayton, Lionel Demery, and Kalpana Mehra. *Public Social Spending in Africa: Do the Poor Benefit?* Washington D.C.: The World Bank Reserach Observer, 1999.

Cellular News. *Four Companies Interested in Rwanda's 3rd Mobile License.* June 24, 2008. http://www.cellular-news.com/story/32003.php (accessed April 7, 2010).

—. *MTN Rwanda Aims for 2 Million Subscribers by Year-End.* October 25, 2009. http://www.cellular-news.com/story/40252.php (accessed April 7, 2010).

—. *Rwanda Government Sells Telco to Libyan Based Investors.* October 15, 2007. http://www.cellular-news.com/story/26685.php (accessed April 7, 2010).

—. *Rwandan Government Subsidises Rural GSM Handsets.* January 30, 2008. http://www.cellular-news.com/story/28950.php (accessed April 7, 2010).

—. *Rwanda's First Domestic Mobile Phone Factory.* September 1, 2008. http://www.cellular-news.com/story/33373.php (accessed April 7, 2010).

Census Chronology. n.d. http://www.washingtonpost.com/wp-srv/national/includes/census_timeline.htm (accessed April 7, 2010).

CERT/CC. *About CERT.* May 11, 2010. http://www.cert.org/meet_cert/ (accessed August 30, 2010).

—. *CERT: Frequently Asked Questions.* July 30, 2008. http://www.cert.org/faq/cert_faq.html (accessed August 30, 2010).

—. *CERT® Advisory CA-2003-04 MS-SQL Server Worm.* January 27, 2003. http://www.cert.org/advisories/CA-2003-04.html (accessed April 8, 2010).

—. *CSIRT Services.* 2002. http://www.cert.org/csirts/services.html (accessed April 8, 2010).

—. *Vulnerability Analysis.* February 25, 2009. http://www.cert.org/vuls/ (accessed April 8, 2010).

CERT-IPN. *Consulting Services.* n.d. https://www.cert.ipn.pt/en/consulting.html (accessed April 8, 2010).

CIA World Factbook. *Rwanda.* August 2010. https://www.cia.gov/library/publications/the-world-factbook/geos/rw.html (accessed August 11, 2010).

—. *Tunisia.* August 2010. https://www.cia.gov/library/publications/the-world-factbook/geos/ts.html (accessed August 11, 2010).

ClamAV. *ClamAV for Windows.* 2010. http://www.clamav.net/lang/en/about/win32/ (accessed September 24, 2010).

Colecchia, Alessandra, and Paul Schreyer. *ICT Investment and Economic Growth in the 1990s: Is the United States a Unquie Case? A comparative Study of Nine OECD Countries.* New Milford: OECD Publishing, 2001.

Commitee to Protect Journalists. *In Rwanda, government strips new journal's license after first edition* . June 12, 2007. http://cpj.org/2007/06/in-rwanda-government-strips-new-journals-license-a.php (accessed September 16, 2010).

ContourGlobal. *ContourGlobal Signs Agreement With Republic of Rwanda to Develop Lake Kivu.* March 2, 2009. http://www.reuters.com/article/idUS175973+02-Mar-2009+PRN20090302 (accessed September 14, 2010).

Cook, Meghan E, Mark F LaVigne, Christina M Pagano, Sharon S Dawes, and Theresa A Pardo. *Making a Case of Local E-Government.* July 2002. http://www.ctg.albany.edu/publications/guides/making_a_case/making_a_case.pdf (accessed April 26, 2010).

Council of Europe. *Convention on Cybercrime.* September 2, 2006. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=9/2/2006&CL=ENG (accessed April 7, 2010).

CSIS Commission on Cyberspace for the 44th Presidency. *Securing Cyberspace for the 44th Presidency.* December 2008. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf (accessed April 8, 2010).

Cyberspace Policy Review. 2009. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Das, Debasis. *GPS on Tractors for Precision Farming.* September 22, 2009. http://www.brighthub.com/electronics/gps/articles/49812.aspx (accessed April 7, 2010).

Department of Homeland Security. *Critical Infrastructure and Key Resources.* April 5, 2010. http://www.dhs.gov/files/programs/gc_1189168948944.shtm (accessed September 14, 2010).

—. *Privacy Impact Assessment EINSTEIN Program.* September 2004. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf (accessed April 8, 2010).

Diamond, Jared. *Collapse.* 2005. http://www.ditext.com/diamond/10.html (accessed August 29, 2010).

EASSy. *EASSy Maps.* 2010. http://www.eassy.org/map.html (accessed September 3, 2010).

e-Cop. *e-Cop Signs Contract to Establish National CERT for Oman Government.* March 23, 2009. http://www.e-cop.net/Data/1/Folder/news/e-Cop%20signs%20contract%20to%20build%20OmanCERT_23Mar2009_SIN.pdf (accessed September 27, 2010).

Eichaer, Theo. "The Social and External Benefits of Education." *Washington Learns.* n.d. http://www.washingtonlearns.wa.gov/materials/Eicher_presentjune14.pdf (accessed April 7, 2010).

El Mir, Haythem. *Tunisia's Experience in Building an ISAC.* June 2008. http://www.google.com/url?sa=t&source=web&ct=res&cd=2&ved=0CAgQFjAB&url=http%3A%2F%2Fwww.first.org%2Fconference%2F2008%2Fpapers%2Fel-mir-haythem-slides.pdf&rct=j&q=el-mir-haythem-slides&ei=IVy9S_eRCcX7lweu8_2IAg&usg=AFQjCNHI8swOxjktubfbEivkYg0CvdCIiw (accessed April 8, 2010).

Electricity Consumers Resource Council. *THe Economic Impacts of the August 2003 Blackout.* Febrauary 9, 2004. http://www.elcon.org/Documents/EconomicImpactsOfAugust2003Blackout.pdf (accessed September 15, 2010).

Eletronic Frontier Foundation. *Trespass to Chattels.* March 17, 2007. http://ilt.eff.org/index.php/Trespass_to_Chattels (accessed April 7, 2010).

ENISA. *Activities.* 2010. http://www.enisa.europa.eu/about-enisa/activities (accessed August 30, 2010).

Etta, Florence, and Laurent Elder. *AT the Crossroads: ICT Policymaking in East Africa.* Nairobi: East AFrican Educational Publishers, 2005.

ExtremeTech Stuff. *Update: Barracuda Takes on Trend Micro over ClamAV Patents.* January 29, 2008. http http://www.pcmag.com/article2/0,2704,2254006,00.asp (accessed January 31, 2008).

Federal Communications Commission. *FCC: Broadband Opportunities for Rural America: Broadband for Rural America: Recovery Act Funding.* November 27, 2009. http://wireless.fcc.gov/outreach/index.htm?job=recovery (accessed April 7, 2010).

Felten, Ed. *OLPC: Too Much Innovation?* March 19, 2007. http://freedom-to-tinker.com/blog/felten/olpc-too-much-innovation (accessed September 10, 2010).

FIRST.org. *Alphabetical list of FIRST Members.* 2010. http://www.first.org/members/teams/ (accessed August 26, 2010).

Flobal Arab Network. *Communications technologies top priority in Tunisia's development.* May 20, 2010. http://www.africa-investor.com/article.asp?id=6931 (accessed August 11, 2010).

Foresman, Chris. *Kids consume media as a full-time job—many getting overtime.* January 21, 2010. http://arstechnica.com/media/news/2010/01/obvious-report-on-increased-media-use-among-kids-is-obvious.ars (accessed April 7, 2010).

FOXNews.com. *Senate Bill Would Give President Emergency Control of Internet.* August 28, 2009. http://www.foxnews.com/politics/2009/08/28/senate-president-emergency-control-internet/ (accessed September 16, 2010).

Ha, Yong-Chool, and Sangbae Kim. *The Internet Revolution and Korea: A Socio-cultural Interpretation.* December 4, 2002. http://web.rollins.edu/~tlairson/asiabus/koreaicts.pdf (accessed September 16, 2010).

Haider, Kamran. *Pakistan blocks Facebook over caricatures.* May 19, 2010. http://www.reuters.com/article/idUSTRE64I29P20100519?feedType=RSS&feedName=technologyNews&utm_source=feedburner&utm_medium=feed&utm_cam

paign=Feed%3A+reuters%2FtechnologyNews+%28News+%2F+US+%2F+Technology%29 (accessed September 19, 2010).

Haines, Lester. *Rwanda fires up Africa's 'biggest' solar plant.* June 8, 2007. http://www.theregister.co.uk/2007/06/08/rwandan_solar_plant/ (accessed September 15, 2010).

Hansell, Saul. *Verizon's FiOS: A Smart Bet or a Big Mistake?* August 18, 2008. http://www.nytimes.com/2008/08/19/technology/19fios.html?pagewanted=1&_r=2 (accessed April 7, 2010).

Harden, Blaine. *Japan's Warp-Speed Ride to Internet Future.* August 29, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/08/28/AR2007082801990.html (accessed April 7, 2010).

Heald, Aimee. *Farming by Satellite* . October 20, 1999. http://www.research.uky.edu/odyssey/fall99/satellitefarming.html (accessed April 7, 2010).

Hecht, Jeff. *City of Light: The Story of Fiber Optics.* New York: Oxford University Press, 1999.

Herzog, Pete. *OSSTMM 2.2.* December 13, 2005. http://www.isecom.org/mirror/osstmm.en.2.2.zip (accessed April 8, 2010).

Hoepers, Cristine, and Klaus Steding-Jessen. *Distributed Honeypots Project: How It's Being Useful for CERT.br.* July 2006. http://www.google.com/url?sa=t&source=web&ct=res&cd=1&ved=0CAYQFjAA&url=http%3A%2F%2Fwww.cert.org%2Farchive%2Fpdf%2FCERTbr-Honeypots-public.pdf&rct=j&q=hnbr-honeypots-national-csirts-meeting2006&ei=A1u9S8-GKIK8lQeMhqCHAg&usg=AFQjCNEFnrPTFx_4pxn792_BWo--Pa (accessed April 8, 2010).

—. *The Brazilian Honeypots Alliance.* April 15, 2007. http://www.honeynet.org.br/presentations/hnbr-first-qcert2007.pdf (accessed April 8, 2010).

Holguin, Jamie. *Biggest Blackout In U.S. History.* August 15, 2003. http://www.cbsnews.com/stories/2003/08/15/national/main568422.shtml (accessed September 15, 2010).

Honeynet.br. *Status Report: May 2006 -- April 2007.* 2007. http://www.honeynet.org.br/status-report/ (accessed April 8, 2010).

Hosein, Gus. *The Birth and Rise of International Conventions on Cybercrime, the Five-Act Tragi-Comedie.* February 6, 2001. http://personal.lse.ac.uk/HOSEIN/cybercrime/oncoe_acp.html (accessed April 7, 2010).

Hsu, Tiffany. *Aging computer system holds up unemployment checks to 117,000 Californians.* December 9, 2009. http://articles.latimes.com/2009/dec/09/business/la-fi-jobless-benefits9-2009dec09 (accessed May 6, 2010).

IBM. *IBM Support for Apache Geronimo.* 2010. http://www-142.ibm.com/software/dre/ecatalog/detail.wss?locale=en_US&synkey=G970711I08282C77 (accessed September 20, 2010).

Information Madness. *Microsoft CERT Awareness Portal SecureYourPC.in* . April 29, 2009. http://www.informationmadness.com/cms/technology/web-tools/1444-microsoft-cert-awareness-portal-secureyourpcin.html (accessed April 8, 2010).

International Telecommunication Union. *Cybersecurity.* January 19, 2010. http://www.itu.int/ITU-D/cyb/cybersecurity/ (accessed August 30, 2010).

—. *WORLD TELECOMMUNICATION AND INFORMATION SOCIETY DAY – QATAR PROMOTES CYBERSECURITY FOR ITS CHILDREN.* 2009. http://www.itu.int/itunews/manager/display.asp?lang=en&year=2009&issue=05&ipage=37&ext=html (accessed April 8, 2010).

International Telecommunications Union. "Confronting the Crisis: Its Impact on the ICT Industry." *ITU Corporate STrategy Division.* February 2009. http://www.itu.int/osg/csd/emerging_trends/crisis/fc05.html (accessed April 7, 2010).

—. *ITU Connect CIS Summit calls for investment in ICT.* November 27, 2009. http://www.itu.int/newsroom/press_releases/2009/54.html (accessed April 7, 2010).

—. *ITU Cybersecurity Work Programme to Assist Developing Countries 2007 - 2009.* December 2007. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf (accessed August 17, 2010).

Internet World Stats. *Africa.* June 19, 2010. http://www.internetworldstats.com/africa.htm (accessed August 11, 2010).

—. *Internet Usage in Asia.* December 31, 2009. http://www.internetworldstats.com/stats3.htm (accessed April 7, 2010).

ITU-T WTSA-08 . *[166] Draft new Resolution [L] - Encourage the creation of national Computer Emergency Response Teams (CERTs), particularly for Developing countries.* October 28, 2008. http://www.itu.int/md/T05-WTSA08-C-0166/en (accessed August 25, 2010).

Johnson, C. A., L. Ariunaa, and J. J. Britz. *Constructing the Pillars of a Knowledge Society: The Challenge of Providing Access to ICTs in Rural Mongolia.* Germany: Libri, 2005.

Juwi Solar. *juwi and the municipal utiliity of Mainz provindg solar electricity to Africa.* June 10, 2007. http://www.docstoc.com/docs/20103783/solar-electricity-to-Africa (accessed September 14, 2010).

Kezio-Musoke, David. *Rwanda's national backbone fiber optic cable set for 2009.* July 7, 2008. http://www.ugabytes.org/nod/index.php?q=node/351 (accessed August 11, 2010).

—. *Rwanda's national backbone fiber optic cable set for 2009.* July 7, 2008. http://www.ugabytes.org/nod/?q=node/351 (accessed April 7, 2010).

Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. *State of the Practice of Computer Security Incident Response Teams (CSIRTs).* Pittsburgh: Carnegie Mellon University / Software Engineering Institute, 2003.

Kinetz, Erika. *$35 computer introduced in India.* July 23, 2010. http://www.csmonitor.com/From-the-news-wires/2010/0723/35-computer-introduced-in-India (accessed September 10, 2010).

Kisambira, Edris. *Uganda telecom extends fiber to Rwanda border.* April 7, 2008. http://computerworldzambia.com/articles/2008/04/07/uganda-telecom-extends-fiber-rwanda-border (accessed August 30, 2010).

Krstic, Ivan. *The Bitfrost security platform.* n.d. http://dev.laptop.org/git/security/tree/bitfrost.txt (accessed September 10, 2010).

Lacy, Sarah. *How to Cross the Digital Divide, Rwanda-Style.* June 24, 2009. 2010 (accessed April 7, 2010).

Linux Online. *About Linus Torvalds.* September 7, 2007. http://www.linux.org/info/linus.html (accessed April 7, 2010).

Majyambere, Gertrude. *Internet costs to reduce by 99 percent .* September 3, 2010. http://www.newtimes.co.rw/index.php?issue=13691&article=10114 (accessed September 3, 2010).

—. *Rwandan Gov't Buys 35,000 Phones to Boost e-soko Project.* September 17, 2009. http://mobilemoneyafrica.com/archives/682 (accessed April 7, 2010).

Malakata, Michael. *Rwanda Targets Two Fiber Cables for Cheaper Bandwidth.* October 27, 2008. http://www.cio.com/article/457071/Rwanda_Targets_Two_Fiber_Cables_for_Cheaper_Bandwidth (accessed August 30, 2010).

Malda, Rob. *About Slashdot.* June 13, 2000. http://slashdot.org/faq/slashmeta.shtml (accessed September 8, 2010).

Massachusetts Institute of Technology. *Free Online Course Materials.* 2010. http://ocw.mit.edu/index.htm (accessed August 29, 2010).

McGibbon, Stephen. *Growth and Jobs from the European Software Industry.* December 2005. http://www.politech-institute.org/review/articles/MCGIBBON_Stephen_volume_3.pdf (accessed April 26, 2010).

McMahon, Walter W. *Deducation and Development: Measuring the Social Benefits.* New York: Oxford University Press, 1999.

McVoy, Larry. *Re: New BK License Problem?* October 5, 2002. http://marc.info/?l=linux-kernel&m=103384262016750&w=2 (accessed January 31, 2008).

Millicom International Celluar S.A. *Contact.* 2007. http://www.millicom.com/contact/contact.cfm (accessed April 7, 2010).

Mitchell, Austin. *Asian Telecom Outage Leaves Widespread Call Center Damage.* July 11, 2005. http://www.macnewsworld.com/story/44527.html (accessed April 7, 2010).

Morel, Benoit, and Adam Tagert. *Computer Security incident Response Teams.* International Telecommunications Union, 2007.

Munro, Ken. "Beware False Negatives." *Secure Business Intelligence.* August 5, 2008. http://www.scmagazineuk.com/beware-false-negatives/article/113356/ (accessed August 30, 2010).

Nagy, Mina. *Staying Safe in Cyber Space .* n.d. http://www.ict.gov.qa/output/page1206.asp (accessed April 9, 2010).

Naidu, Jayachandran B. *The Sub Plan for National cyber Security Center.* Kigali, Rwanda: Rwanda Information Technology Auhority , 2008.

National Strategy to Secure Cyberspace. February 2003. http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (accessed April 8, 2010).

Ndikubwayezu, Gilbert. *Jabana Power Plant Gets World Bank Thumbs Up.* May 21, 2009. http://allafrica.com/stories/200905210009.html (accessed September 14, 2010).

Neibauer, Michael. *Verizon promises citywide FiOS access within a decade.* November 24, 2009. http://www.washingtonexaminer.com/local/112408_Verizon_promises_citywide_FiOS_access_within_a_decade.html (accessed April 7, 2010).

Office of Management and Budget. *Office of E-Government and Information Technology.* n.d. http://www.whitehouse.gov/omb/e-gov/ (accessed April 7, 2010).

OLPC. *Category: Deployments.* February 10, 2009. http://wiki.laptop.org/go/Category:Deployments (accessed September 10, 2010).

—. *OLPC Rwanda.* August 5, 2010. http://wiki.laptop.org/go/Rwanda (accessed September 10, 2010).

Orlale, Odhiambo. *Kigali : Where MPs debate and vote in a simple click.* October 21, 2006. http://www.cipaco.org/spip.php?article1062 (accessed August 30, 2010).

Ouaili, Montasser. *ICT for development "Towards e-Tunisia".* October 2006. http://www.2006.ict4allforum.tn/plateforme/pdf/presentations/02_Montassar_Ouaili.pdf (accessed August 10, 2010).

Pakissan. *Pakissan.com: connecting Agricultural community for Better Farming.* April 7, 2010. http://www.pakissan.com/ (accessed April 7, 2010).

Penn, Mary Sue. *Bill Gates Ready to fight Malaria and Bring Technology to the Poor .* February 20, 2008. http://www.chicagobooth.edu/news/2008-02-20_gates.aspx (accessed April 7, 2010).

Pitofsky, Robert. *SELF REGULATION AND ANTITRUST.* February 18, 1998. http://www.ftc.gov/speeches/pitofsky/self4.shtm (accessed September 16, 2010).

Psacharopoulos, George. *Returns to Investment in Education: A Global Update.* Washington D.C.: The World Bank, 1998.

Q-CERT. *Summer Class on Information Security.* July 15, 2009. http://www.qcert.org/news/IS_class.html (accessed April 8, 2010).

Randall, Alexander V. *The Eckert Tapes: Computer Pioneer Says ENIAC Team Couldn't Afford to Fail -- and Didn't.* February 20, 2006. http://www.computerworld.com/s/article/108790/The_Eckert_Tapes_Computer_Pioneer_Says_ENIAC_Team_Couldn_t_Afford_to_Fail_and_Didn_t?taxonomyId=012 (accessed April 7, 2010).

Reagan, Ronald. *Remarks to Representatives of the Future Farmers of America.* July 28, 1988. http://www.reagan.utexas.edu/archives/speeches/1988/072888c.htm (accessed Apil 8, 2010).

Republic of Rwanda. *Rwanda Vision 2010.* March 7, 2008. http://www.rwandainvest.com/IMG/pdf/Vision-2020.pdf (accessed May 7, 2010).

—. *Rwanda Vision 2020.* n.d. http://www.rwandainvest.com/IMG/pdf/Vision-2020.pdf (accessed August 10, 2010).

RNA Reporters in Nairobi and Kigali . *High-speed broadband cable switched on in Kenya, Tanzania .* July 23, 2009.

http://www.rnanews.com/index.php?option=com_content&task=view&id=1612&Itemid=27 (accessed September 3, 2010).

Robel, Dan. *International Cybercrime Treaty: Looking Beyond Ratification.* Washington D.C.: SANS Institute, 2006.

Roblyer, M D, and A H Doering. *The Impact of Word Processing in Education.* 2010. http://www.education.com/reference/article/impact-word-processing-education/ (accessed April 7, 2010).

Rubens, Paul. *Bugger Off: The Importance of Penetration Testing.* July 25, 2008. http://www.serverwatch.com/tutorials/article.php/3690836/Bugger-Off-The-Importance-of-Penetration-Testing (accessed August 30, 2010).

RURA. *Guidelines for Internet resources management and allocation in general and .RW domain in particular.* September 2009. http://www.rura.gov.rw/docs/GUIDELINES_4_INTERNET_RESOURCES.pdf (accessed September 13, 2010).

—. *ICT: Licensed Operators* . 2009. http://www.rura.gov.rw/index.php?option=com_content&view=article&id=225&Itemid=64 (accessed August 11, 2010).

—. *Universal Access* . 2008. http://www.rura.gov.rw/index.php?option=com_content&view=article&id=78&Itemid=183 (accessed August 10, 2010).

Rwandatel. *Rwandatel SA Launches Super Fast Internet Speeds with SEACOM's Submarine Fibre Optic Cable.* July 10, 2009. http://www.subtelforum.com/articles/?p=1547 (accessed August 30, 2010).

SANS Institute. *SANS Announces $1 Million Grant to Expand Cyber Security Capacity of Developing Countries "We are All In This Together".* May 20, 2008. http://www.sans.org/press/impact.php (accessed August 30, 2010).

SANS. *Security Training Courses.* 2010. http://www.sans.org/security-training/courses.php (accessed September 15, 2010).

Scarfone, Karen, Murugiah Souppaya, Amanda Cody, and Angela Orebaugh. *Technical Guide to Information Security Testing and Assessment.* September 2008. http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf (accessed April 8, 2010).

Schultz, T. Paul. *Why Governments Should Invest More to Educate Girls.* Hannover: Yale University, 2001.

Shachtman, Noah. *Georgia Under Online Assault.* August 10, 2008. http://www.wired.com/dangerroom/2008/08/georgia-under-o/ (accessed April 7, 2010).

Software Engineering Institute. *CERT Coordination Center Partners With Qatar's Supreme Council to Battle Cyber Risks.* December 15, 2005. http://www.sei.cmu.edu/newsitems/qatarcertrelease.cfm (accessed September 15, 2010).

SourceFire. *Certifed ClamAV Support.* 2010. ttp://www.sourcefire.com/products/clamav/support (accessed April 7, 2010).

Sternstein, Aliya. *Cybersecurity costs climb as market expands.* August 30, 2010. http://www.govexec.com/dailyfed/0810/083010mag2.htm (accessed September 20, 2010).

Stigler, James W., and James Hiebert. *The Teaching Gap.* 1999. http://books.google.com/books?hl=en&lr=&id=F1kKZgIqtfEC&oi=fnd&pg=PR11&dq=computers+improve+education&ots=O2oWC5REBo&sig=sZulBn88zn3CclFBMjoNYfKYG-Y#v=onepage&q&f=false.

Syamntec. *The Importance of Assessment Services and Penetration Testing.* February 20, 2008. http://www.symantec.com/business/resources/articles/article.jsp?aid=20080219_importance_assessment_services_penetration_testing (accessed August 30, 2010).

The Associated Press. *Senate ratifies treaty on cybercrime.* August 4, 2006. http://www.usatoday.com/tech/news/techpolicy/2006-08-04-cybercrimetreaty_x.htm (accessed April 7, 2010).

—. *Xbox Sale Slows Amazon.com.* November 24, 2006. http://www.foxnews.com/wires/2006Nov24/0,4670,AmazonOutage,00.html (accessed September 8, 2010).

The Wasington Times. *EDITORIAL: Unfair government competition.* August 17, 2009. http://www.washingtontimes.com/news/2009/aug/17/unfair-government-competition/ (accessed September 16, 2010).

Trabelsi, Housa. *Unemployment haunts Tunisia college graduates.* July 30, 2010. http://www.magharebia.com/cocoon/awi/xhtml1/en_GB/features/awi/features/2010/07/30/feature-01 (accessed August 11, 2010).

Traynor, Ian. *Russia accused of unleashing cyberwar to disable Estonia.* May 17, 2007. http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (accessed August 26, 2010).

tunCERT. *About Tuncert.* 2010. http://www.ansi.tn/en/about_agency/about_tuncert2.html (accessed April 8, 2010).

—. *About TunCERT.* 2010. http://www.ansi.tn/en/about_agency/about_tuncert.html (accessed April 8, 2010).

—. *About TunCERT.* 2010. http://www.ansi.tn/en/about_agency/about_tuncert2.html (accessed April 8, 2010).

—. *F.A.Q.* 2010. http://www.ansi.tn/fr/audit/faq.html (accessed April 8, 2010).

—. *Services Provided.* 2010. http://www.ansi.tn/en/about_agency/about_tuncert2.html (accessed April 8, 2010).

Twigg, Stephen. *ICT transforms education says Stephen Twigg MP, in support of NCH.* April 20, 2004. http://www.publictechnology.net/content/889 (accessed August 29, 2010).

U.S. Department of homeland Security. *Privacy Impact Assessment for Einstein 2.* May 19, 2008. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf (accessed April 8, 2010).

U.S. Department of State. *Rwanda.* 2007. http://www.state.gov/g/drl/rls/irf/2007/90115.htm (accessed August 11, 2010).

U.S. State Department. *Tunisia.* n.d. http://travel.state.gov/travel/cis_pa_tw/cis/cis_1045.html (accessed August 11, 2010).

UNIDO. *United Nations Industrial Development Organization.* n.d. https://www.unido.org/index.php?id=o56357 (accessed August 10, 2010).

United States Department of Agriculture. *Recent News.* n.d. http://www.usda.gov/rus/ (accessed April 7, 2010).

US-CERT. *Mailing Lists and Feeds.* 2010. http://www.us-cert.gov/cas/signup.html#st (accessed April 8, 2010).

—. "National Cyber Security: Division US-CERT Overview." *US-CERT.* November 29, 2007. http://www.ncs.gov/tpos/esf/mclean/Tab%2013%20-%20US-CERT%20Overview.ppt (accessed August 30, 2010).

Vamosi, Robert. *Newsmaker: Cyberattack in Estonia--what it really means.* March 29, 2008. http://news.cnet.com/Cyberattack-in-Estonia--what-it-really-means/2008-7349_3-6186751.html (accessed August 26, 2010).

Wafula, Walter. *Third internet cable starts operation.* August 11, 2010. http://www.monitor.co.ug/Business/Technology/-/688612/974578/-/uiwarp/-/index.html (accessed August 30, 2010).

Waldorf, Lars. *Censorship and propaganda in post-genocide Rwanda.* n.d. http://www.idrc.ca/fr/ev-108305-201-1-DO_TOPIC.html (accessed September 16, 2010).

Walker, Carolee. *U.S. Senate Votes To Ratify Cybercrime Convention.* August 7, 2006. http://www.america.gov/st/washfile-english/2006/August/20060807133221bcreklaw0.5304834.html (accessed April 7, 2010).

Weber, Stephen. *The Success of Open Source.* 2004.

Wikipedia. *Wikipedia: Citing Wikipedia.* February 12, 2010. http://en.wikipedia.org/wiki/Citing_Wikipedia (accessed April 7, 2010).

Wilson, Ernest .J III, and Kelvin Wong. *African Information Revolution: A Balance Sheet.* London: Elsevier Science Ltd., 2003.

World Bank. *Rwanda Receives Assistance to Modernize Government Systems.* September 13, 2006. http://www.rwandagateway.org/article.php3?id_article=2900 (accessed April 7, 2010).

Xinhua. *India mulls separate laws, specialized agency to fight cyber crime .* February 1, 2010. http://english.peopledaily.com.cn/90001/90777/90851/6883976.html (accessed April 7, 2010).

Yahia, Mona. *Tunisia looks to increase job opportunities for college grads .* December 10, 2008. http://www.magharebia.com/cocoon/awi/xhtml1/en_GB/features/awi/features/2008/10/12/feature-01 (accessed August 11, 2010).

Ziltrain, Jonathan. *The Future of the Internet and How to Stop it.* Penguin Books, 2008.