A Conceptual Model for the Development of a National Cybersecurity Index: An Integrated Framework

Full paper

Manal M. Yunis
Lebanese American University
myunis@lau.edu.lb

Kai S. Koong
University of Texas – Pan American
koongk@utpa.edu

Abstract

As ICT and cyberspace become sources of impressive innovation, the reliance of organizations, governments, and people on them will increase. However, with this vast reliance, hazardous vulnerabilities have emerged. These vulnerabilities may be exploited, resulting in information and cybersecurity issues at the national as well as the international levels. Cybersecurity is critical for sustaining resilience in critical infrastructures (CI) as well as information infrastructures (CII). Accordingly, cybersecurity should be incorporated into the economic and national security model of a nation. With this in mind, a cybersecurity index is a necessary tool to compare the performance of nations in terms of cybersecurity initiatives, and in articulating effective cybersecurity policies and strategies. This paper proposes a holistic framework for building a cybersecurity index taking into consideration the technological, legal, economic, cultural, and international relations factors pertinent to countries and paves the way for cybersecurity measures and metrics to be established and tested.

Keywords (Required)


Introduction

With the information and communications technologies (ICT) rapid advancements, cyberspace has become the main stage of operations for almost every human being, industry, and government in the world. Focusing on the role ICTs play in the economic competitiveness of a nation, the analysis will start with a core fact that ICTs are becoming increasingly intertwined in the daily activities of most, if not all, societies. Some of these ICT systems, services, networks and infrastructures form a vital part of economies and societies, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures (CI) (Department of Homeland Security, 2013; European Commission, 2009). They are typically regarded as critical information infrastructures (CIIs) as their disruption or destruction would have a serious impact on vital societal and economic functions.

For example, a hacker attack on the nation’s power grid has the potential for causing blackouts as well as a domino effect of consequent failures in other interdependent systems (Cavelty, 2008). To illustrate such overwhelming effects resulting from cyber-attacks targeting interdependent systems in a nation’s CII, it would be useful to envision the impact on intertwined entities across the economy. Depicted in Figure 1, the illustration visualizes two core points: (DHS and DOE, 2007).

1. Technical innovations and rapid ICT advancements have markedly linked and increased interdependence among the nation’s critical infrastructures. This suggests that harmful attacks directed at a critical asset would have disturbing and possibly amplified effects on the other infrastructures.

2. Infrastructure interdependencies extend beyond the national borders and cross international borders.
Analysis of these two points would lead to the inference of the following:

- Because of the interdependencies among the various CIs within a nation, a cyber-attack on one CI will have a ripple effect on the other CIs. In other words, the attack can create an adverse situation not only in the target CI, but also in the other intertwined CIs. The ripple effect is used here to describe a situation where an attack vector drops into a critical asset in the nation and momentum builds out externally. This is illustrated in Figure 2. As shown, the adverse impact that the attack vector will cause in one CI will also generate disruptions – that are possibly amplified – in the other critical national assets.

Figure 2. The Ripple Effect of Cyber Attacks

- The world is becoming more and more networked, with the connections and information flows now reaching far beyond the conventional borders of organizations and even countries. Given the possibility that certain CIs in different nations are integrated and interdependent (e.g., the integrated energy systems in North America), the impact of a disruption attack will probably go
The importance of information and cybersecurity has never been more significant. This is because the digital key resources and the networked critical infrastructures of a nation are increasingly the backbone of sustainable and prosperous economies, transparent government, and better developed societies (White House, 2011).

The need for this study stems from the fact that CIs, which are mostly underpinned by CII, are now pivotal to economies, especially the industrial and developed ones. These economies are as good as these CIs are. Citizens, governments, and businesses are all increasingly becoming reliant on a massive array of intertwined information and physical infrastructure to accomplish daily tasks, solve problems, and make decisions. It is worth recalling that CI interdependence sometimes extends beyond a nation’s borders and crosses into other nations, as is the case with power transmission, oil, gas, and other power sources, or the Internet. This means that failure to attain and maintain safe, resilient, and robust infrastructure in one nation can generate adverse effects on others.

Today, more than 3 billion people around the world now use the internet via a variety of different devices, with social media use and networking growing exponentially (Kemp, 2015). Innovation in various sectors paved the way for a convergence between telecom, broadcasting, and IT. This has given rise to new and innovative services in the financial, education, government, and healthcare sectors, not only in developed but also in developing countries. Accordingly, the increasing deployment and use of ‘e-enabling’ in various societies has increased the need for securing the channels of communication. In the globalization era, this security – the security of cyberspace - is deemed crucial, not only within a nation but also between and across nations.

Availability, reliability, and security of communications and information services are essential to the functioning and growth of a modern economy (Dalmini et al, 2009). These services are collectively termed critical information infrastructure (CII). The distinguishing feature of a CII is that it encompasses and links all the other CIs together; so if it is removed, many other CIs will be down relatively soon (Westrin, 2001).

This tolls the bells regarding the possible risk of exploiting any vulnerability in this vital infrastructure, rendering all the other intertwined CIs vulnerable to exploitation. Within this realm, the World Economic Forum (WEF) estimated in 2009 that there is a 10 to 20% probability of a major CII breakdown in the next 10 years. This is anticipated to have a global economic cost of approximately $250 billion (World Economic Forum, 2008). In 2011, the same estimation is provided by WEF with a description of the global impact that such a breakdown will bring about (World Economic Forum, 2011).

This renders prudent and vital the establishment of reliable trust frameworks and global cybersecurity cultures (WSIS, 2003). Within such cultures, there could be a supportive environment for setting national level strategies and collaborative international agreements to enforce cybersecurity policies and reduce the occurrence or alleviate the impact of possible cyber threats. The process may start with the formulation of a cybersecurity measure that would give an insight regarding the cybersecurity status of countries as well as their cybersecurity initiatives and strategies. This measure should incorporate factors that are potentially associated to a country’s cybersecurity level.

Previous research has contended that CII are components of CI (Walker, 2008; Lopez et al., 2007; Wilson, 2007; Cukier et al., 2005; and Rinaldi et al., 2001) and are influenced by the same legal framework and regulatory policies. Previous research has also discussed cybersecurity as it applies to an industry (e.g. Taixeira et al, 2010), to supervisory control and data acquisition (SCADA) systems (Farooqui et al, 2014; Ten et al, 2008), or to a specific country (for example, Glantz et al, 2014; Venter, 2014). However, to the best of the author’s knowledge, there’s a lack of research that attempts to define a framework for assessing the cybersecurity initiatives at the country level, taking into consideration country related factors and indicators. The only study that the author is aware of is the cybersecurity index generated by the international Telecommunications Union (ITU) and the ABIresearch joint project (ITU-ABlresearch, 2014).
This paper proposes a holistic framework that is based on the ITU cybersecurity initiatives agenda in order to identify the country level factors that are most likely to be associated to a nation’s cybersecurity level and to pave the way for a quantitative estimation of that level using data pertinent to each country’s strategies--technical, legal, economic, cultural, human development, and international relations.

The remaining of the paper will proceed as follows. The following section will discuss the theoretical framework that the paper draws upon. Next will be a review of the literature pertinent to cybersecurity and the country factors associated to it. Then, the proposed model will be presented and explained. Finally, the study implications and contributions will be stated and discussed.

**Theoretical Framework**

The foundation of this study is a rich theoretical framework that draws its components from the Theory of International Relations (Waltz, 1979) with its National Security and Deterrence components. Cybersecurity is a pivotal factor in national security (DHS, 2010). David Jablonsky (2001) defines national security as that part of government policy whose objective is to create national and international political conditions that are favorable to the protection or the extension of vital national values against existing or potential adversaries. Jablonsky defines national security in terms of the respective elements of the power base of the state and the priorities that are seen as of vital and/or national interest.

Within the growing literature on the topic of cyber security, many authors have addressed technical aspects of this increasingly important concept, providing practical guidance for security experts and infrastructure designers (Lee et al, 2002; Abu Nimeh et al, 2013). Others have focused on deterrence as a governmental organization policy and strategy (Rosenweig, 2010); and still others dealt with the issue from a domestic and international law perspective (Schmitt, 2010). Relatively speaking, few researchers have addressed the cyber security issue using the international relations theory (Waltz, 1979) as a theoretical foundation. Within this framework, strategies like international cooperation (Cavelty, 2008, 2007) and law enforcement (Newmann, 2002) are well implied and considered.

Cyber security literature also includes another derivation from the international law theory; namely, deterrence. Deterrence is commonly thought about in terms of convincing opponents that a particular action would elicit a response resulting in unacceptable damage that would outweigh any likely benefit. Rather than a simple cost/benefits calculation, however, deterrence is more usefully thought of in terms of a dynamic process with provisions for continuous feedback. The process initially involves determining who shall attempt to deter whom from doing what, and by what means. Within this frame of reference, deterrence could be in the form of weaponry, and in the case of cyber space, other forms of cyber-attack deterrence may include legislation, international collaboration, and effectively secured communication lines (Kshetri, 2010; Nickolov, 2006; Shue and Lagesse, 2011; Neumann, 2007).

**Literature Review and Proposed Model**

Cybersecurity is not a recent phenomenon, as computer data breaches have always been a concern (Goodhue and Straub, 1991; Straub and Welke, 1998; Culnan and Williams, 2009). But what is cybersecurity? The International Telecommunications Union, ITU (2005), defines the term as follows:

“Cybersecurity is concerned with making cyberspace safe from threats, namely cyber-threats. The notion of “cyber-threats” is rather vague and implies the malicious use of information and communication technologies (ICT) either as a target or as a tool by a wide range of malevolent actors” (p.3). According to ITU (2005), the term is commonly used to refer to three things:

1. A set of technical and non-technical activities and other measures designed to protect computers, networks, stored and communicated information, as well as the overall cyberspace from all types of threats, including threats to national security;
2. The degree of protection generated by the above activities and measures;
3. The associated professional field, including research work aimed at analyzing, developing, and implementing those activities for a better security quality.

Cybersecurity roots extend back to the Cuckoo’s Egg incident in the mid-1980s (Stoll, 1990). Viruses and worms have been active, infuriating actors on the stage of computing for a long time (de Villiers, 2009). Still, it was only when major cyber-attacks hit an entire nation in spring 2007 that the
issue was propelled to the center of attention. The nation was Estonia, and the sustained cyber-attacks that targeted the country were labeled by observers as cyber warfare, cyber terror, or cybercrime (Wilson, 2008). Shortly preceded by a political event where officials in Estonia took down a statue in Tallinn which had been in place since the Soviet-era, which resulted in a huge backlash in Russia against the Estonians. That attack effectively crippled Estonia’s government websites, newspapers, police, ministries, media and online banking. The attack came in the form of large Distributed Denial of Service (DDoS) attacks where computers and servers were flooded by multitudes of visits and voluminous e-mails, which blocked legitimate users and caused many websites to shut down for some time (Collier, 2007; Tiirmaa-Klaar, 2011).

The attack had a devastating impact on the country’s media, banking sector, and communications systems (Trustwave, 2011). Later, in 2010, the computers at a nuclear plant in Iran were affected by the ‘Stuxnet’ worm virus. According to Trustwave’s Global Security Report (2011), most of the attacks that hit national CIs were DDoS attacks. These are carried out using ‘botnets’ – computer networks that “have been hijacked by remote users, often without the knowledge of their owners” (Trustwave, 2011, p.31).

The use of technology has resulted in more reliable power with a reduced need for manpower and resources. Cyber technology provides everyone with immediate global reach and exponential decreases in the constraints of time, distance, and power required – factors that could be of high benefit to both users with good intentions and those with bad ones. This manifests the double-edge sword that ICT represents (Assante, 2009).

**The Impact of Cybersecurity**

Along with all the benefits that the Internet, a major part of ICT, provides, it nevertheless has a dark side that has been an issue of concern to organizations, ICT designers and developers, policy makers, and researchers for more than two decades (Schneier, 2005). This dark side of ICT is threatening the very critical infrastructures of nations by increasing their vulnerability to cyber threats and attacks. This growing vulnerability led Richard Clarke (2010) to reemphasize the idea of a ‘digital pearl harbor’ especially after the many reported alarming incidents of cyber espionage and cybercrime. Of course, in this time period, it is more cost-effective to manage infrastructure systems remotely within an internet framework using easy-to-use software and network protocols. Nevertheless, this cost effectiveness and better convenience resulting from the use of ICT to manage critical infrastructures (ICT) are embedded with risk that involves the vulnerability resulting from insufficient or non-robust security measures (Geers, 2009).

Secure information systems have become a necessity for modern society. This is attributed to two important reasons: (a) the significant social and economic benefits they provide, and (b) the serious consequences of their malfunctioning (Attwood et al., 2011; Nickolov, 2005). In fact, the information society success is assessed by its pervasiveness and correct functioning. However, a look at critical infrastructures in general, and critical information infrastructures in particular, shows that while they are widespread and ubiquitous, they are strongly susceptible to vulnerabilities (Cukier et al., 2005). Such vulnerabilities may be exploited (Barmin et al, 2011; McConnell & Hamilton, 2002) by hackers, criminals, or other groups, using a variety of cyber threat and attack weapons, such as those listed in Table 1.

The above are a few of the myriad examples that demonstrate the huge vulnerability of critical infrastructures to cyber threats. These threats manifest themselves in a variety of potential exploitations and reported incidents, such as cybercrime and cyber espionage. A list of some of these cyber threats/exploitations is presented in Table 2.
<table>
<thead>
<tr>
<th>Cyber Threat Weapon</th>
<th>Description</th>
<th>Impact Scope</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Stuxnet Malware</td>
<td>A sophisticated software that enhances the potential for cyber espionage and infrastructure attacks.</td>
<td>SCADA</td>
<td>Byres (2011)</td>
</tr>
<tr>
<td>• Zeus</td>
<td>A malware that enables the theft of valuable intellectual property as well as money.</td>
<td>Critical Infrastructure</td>
<td>Binsalleeh et al., (2010)</td>
</tr>
<tr>
<td>• Zero-day</td>
<td>A virus which takes advantage of a security weakness (hole) that has no patch yet. So, zero-day represents the period of time when there’s nothing that could be done to stop the intrusion which took advantage of a security flaw.</td>
<td>Internet Infrastructure</td>
<td>Acohido and Swartz (2008)</td>
</tr>
<tr>
<td>• Botnet</td>
<td>A network of compromised computers used to launch internet crimes, with the computer owners unaware of it. The network, mainly comprised of home-based computers, is used to spread spam, Worms, and viruses.</td>
<td>Critical Infrastructure</td>
<td>APCERT (2011); UNODC (2011); and Wilson (2008)</td>
</tr>
<tr>
<td>• Social Engineering</td>
<td>A technique where the hacker aims at obtaining information that will enable an unauthorized access to valued system information, through the use of clever manipulation of a human nature: the tendency to trust.</td>
<td>SCADA</td>
<td>Granger (2001); Dondossola et al., (2008); Beggs (2010); Parmar (2012).</td>
</tr>
<tr>
<td>• Advanced Persistent Threat</td>
<td>A sophisticated cybercrime category aimed at political and business targets. To be successful, they require a high degree of stealthiness, as well as prolonged time periods. They go beyond immediate financial gain and are based on various avenues of attack.</td>
<td>SCADA</td>
<td>Alperovitch (2011)</td>
</tr>
<tr>
<td>• Mobile Application Exploits</td>
<td>Mobile phones are increasingly becoming a threat vector that could introduce a wide range of attacks. Malware uses root exploits to launch sophisticated attacks on smart phones.</td>
<td>Critical Infrastructure</td>
<td>Schneier (2011)</td>
</tr>
</tbody>
</table>

Table 1. List of some Cyber-attack Weapons against CI: Description and Impact Scope
Cybersecurity Initiatives

International organizations, such as ITU, recognize that information and technology security are critical priorities for the international community. Cyber security generally is in everyone’s best interests and this can only be achieved through a collaborative effort. Cyber threat issues are global and therefore the solutions must be global, also. It is vital that all countries arrive at a common understanding regarding cyber security; namely, providing protection against unauthorized access, manipulation and destruction of critical resources. The ITU believes the strategy for a solution must identify those existing national and regional initiatives in order to work effectively with all relevant players and to identify priorities (ITU, 2010). Following is a description of the measures and factors that may contribute to the understanding of differences in cybersecurity initiatives across countries.

Table 2. A List of Some Cyber Threat / Exploitation Types and Exploitation Method

<table>
<thead>
<tr>
<th>Threat / Exploitation Type</th>
<th>Description</th>
<th>Motivation</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Espionage</td>
<td>An activity which is either foreign sponsored or coordinated intelligence to unlawfully access proprietary economic information (FBI, 1995; Tucker, 1997)</td>
<td>Obtaining economic and political secrets of nations or industries, and stealing intellectual properties (Lewis, 2010).</td>
<td>A nation’s government, corporations, establishments, and individuals (Fraumann, 1997).</td>
</tr>
<tr>
<td>Cyber Crime</td>
<td>This refers to offenses ranging from activity against data to infringement of content and copyright (Krorie, 2005). It also involves fraud, child pornography, unauthorized access, and cyber stalking (United Nations, 2000)</td>
<td>Financial gain or Economic espionage (PWC, 2011)</td>
<td>Individuals, governments, companies (Twomey, 2010).</td>
</tr>
<tr>
<td>Cyber warfare</td>
<td>This refers to the use of exploits in cyberspace as an intentional means to cause harm to economies, people, and assets (Owen, 2008).</td>
<td>Military or political dominance (Twomey, 2010)</td>
<td>Critical infrastructure, economies, military and political targets (Shimeall and Williams, 2002; Chen, 2010; Kelsey, 2008).</td>
</tr>
<tr>
<td>Hacktivism</td>
<td>Known as a convergence of both hacking and activism, the term refers to the pursuit of political ends through the use of digital means and tools (Vamosi, 2011).</td>
<td>Changing political systems or regimes (Denning, 2000)</td>
<td>Corporations, military sites, governments, and law enforcement agencies (Mansfield-Devine, 2011; Vamosi, 2011).</td>
</tr>
<tr>
<td>Cyber Terrorism</td>
<td>This refers to the use of computer network tools by a hostile nation or group to exploit the vulnerabilities of a poorly secured network to disrupt or to stop critical functions (Lewis, 2002).</td>
<td>Changing political/social systems; Defending a specific cause, ideology, or conviction (Wilson, 2008; Singh and Siddiqui, 2011).</td>
<td>Governments, civilian populations, critical infrastructures (Vatis, 2006).</td>
</tr>
</tbody>
</table>
Economic Aspect

The impact that an economy may have on cybersecurity is bi-faceted. On one hand, the developed ICTs and the resulting high level of interconnectedness in developed nations make them more vulnerable to cyber threats as well as amplify the potential adversary impact of an attack (Dogrul, 2011). Developed countries remain highly vulnerable to cyber-attacks against the computer networks that are critical to national and economic security. Nevertheless, the high level of ICT innovation in those countries allows for advanced cybersecurity technology solutions. This susceptibility to incidents drove the governments of developed nations to invest intensively in cybersecurity technologies, organize their information and cybersecurity policies, and formulate certain legal measures. At the same time, developing countries have a higher risk of being the target of cyber-attacks (United Nations, 2011). What increases the risk is the weak surveillance capacity in those countries (United Nations, 2011). Taking the economic aspects of countries into consideration can contribute to the understanding of various cybersecurity ranks and measures across different countries.

National Culture

Previous research suggested that cultural aspects are very important factors influencing non-compliance behavior by employees (Silvius, 2010). At a wider scope, the compliance to national cybersecurity policies may vary widely across developed and developing countries due to differences in values, norms, and beliefs across various communities, countries, and regions.

Legal Measures

The adoption by all countries of appropriate legislation against the misuse of ICTs for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cyber security. In fact, the priorities of a nation are reflected in its policies and laws, and these in turn influence its rate of growth and direction of development. This component measures the impact of a nation’s policies, laws, and regulations, and their implementation for the development and use of ICT (Dutta and Mia, 2007). Moreover, policy programs must remain coherent and manageable (Poel and Bodea, 2008). Accordingly, the role of the government policy in the process of ICT diffusion enhancement cannot be underestimated. For example, the role of institutional systems in enhancing education and regulatory policies is substantial in global Internet diffusion (Zhao et al., 2007).

Technical Measures: Secure Infrastructure

Infrastructure is defined as the level of availability and quality of the key access infrastructure for ICT within a country. A quality ICT-access infrastructure facilitates the adoption, usage, and impact of these technologies, which in turn promotes investment in infrastructure. Infrastructure thus plays a critical role in influencing the networked readiness of a nation (Dutta and Mia, 2007). In fact, one finds this factor is a common element in nearly all the research work that deals with all kinds of ICT adoption and diffusion. In the context of this study, it refers, among other things, to Internet connectivity, high bandwidth for accessing the network, and sufficiency and competence of the national power grid (Mutula and Brakel, 2006).

Moreover, a country's infrastructure includes the telecommunications facilities, Internet access, dial-up access, bandwidth, and broadband access. As a matter of fact, the role of investment in improving a country's technological infrastructure is very important. For example, investment in fiber networks rather than in telephone hubs can make big differences for bandwidth. A relative advantage in such technology is that it can attract a bigger share of the global economy in one country when compared to others (Fuhr and Fociask, 2007).

Institutional Measures

Individuals, organizations and governments are increasingly dependent on globally interconnected networks. In order to protect network infrastructures and address threats, coordinated national action is required to prevent, respond to and recover from incidents. Collaboration at all levels of government and
with the private sector, academia, regional and international organizations, is necessary to raise awareness of potential attacks and take steps toward remediation (ITU, 2010). Effective incident management also requires considerations of funding, human resources, training, technological capability, government and private sector relationships, and legal requirements. Efforts are being made to bring together organizational structures at the national and regional level in order to facilitate communications, information exchange and the recognition of digital credentials across different jurisdictions. However, more needs to be done at the global level and international cooperation between these different structures is indispensable (Dutta and Mia, 2007).

**Human Development**

Successful training effort on implementation and use of new technologies in certain nations will enhance individual cognitions of application knowledge and business context knowledge, and the inter-individual cognitions of collaborative task knowledge (Yetton et al., 1999). Human resource complementarities, like end-user training, will create embedded advantages that explain significant performance variance among organizations in those nations (Powell and Dent-Micallef, 1997). In developing nations, appropriate end-user training will also ensure a coordinated and comprehensive approach to the introduction of new technologies. Investment in mature technology in these countries means that the potential of the newly introduced technology is established. In this environment, training will ensure that the end-users are able to capitalize on the opportunities that the new but established technology offers. This fusion will be a source of process-level business value (ITU, 2010).

**Portrayal of the Conceptual Model**

With the previous literature and theoretical frameworks described above, and with all the sets of hypotheses derived, a conceptual model is proposed that is based on all that has been aforementioned and analyzed so far. The model is depicted in Figure 3. Analyzing the model, one can find that it has three important characteristics:

1. First, it is an integrated socio-technical model. The model synthesizes the majority of the social and technical elements that are mentioned in the literature as being important determinants of ICT and information security systems. While the technical measures, like cryptography (Wang and Lu, 2013; Haraty et al, 2004) and improved secure socket layer (SSL) protocol (Otrok et al, 2006) are important, they are not enough. This is because security is not a product (Schneier, 2014). It is rather a process entailing several factors that interact with the technology component.

2. Second, it is a dynamic model. The technological, legal, human, and international relations specific to a certain nation are envisioned as major catalysts that can shape cybersecurity initiatives of a country.

3. Third, it is potentially a proactive model. Understanding the environmental factors—both domestic and global—along with the available resource endowments, a country’s strategists can affect certain policies or initiate certain agreements that would improve the cyber security levels of a nation.

![Figure 3. Conceptual Model](image)
Research Implications and Contributions

Drawing on the study findings, ITU initiatives (ITU, 2011), and cybersecurity reports generated by the governments of several countries, one can draw several implications at the theoretical and pragmatic levels. Nowadays, cybersecurity analysts, national leaders, and organizations are associating economic security to the security of the critical infrastructures that the economy is based upon. Based on this, cyberspace safety/security can never be an afterthought. It is a major element in any kind of country development strategy or discussion.

At the same level, a major contribution of this study is the introduction of a cybersecurity framework. This cybersecurity formative construct may pave the way for an international and systemic cybersecurity index to be developed. Such an index is believed to help gauge nations’ performance in terms of ICT, innovation, and cybersecurity initiatives. At the same time, it can help guide the policy setting, legislation process, and cybersecurity technology design toward formulating optimal solutions for ensuring optimal levels of cybersecurity for efficient and reliable operations in the cyberspace. Finally, emphasizing the role that human capital plays in cybersecurity initiatives also bears an important contribution to the research streams of information security, and cybersecurity. The framework is a first step towards the formulation of the index. Using country-level data generated by international organizations, and using appropriate methodologies designed for building composite indicators, the conceptual model could be tested and assessed.

On the pragmatic level, the implications can be viewed from both the national and the international perspectives. At the national level, a cybersecurity joint effort bringing together top business, government, and academic experts to frame the key issues for cooperation on cyber threats should be established. At the international level, international cooperation should manifest itself in serious efforts made by governments to establish a common global understanding that cyber weapons are extremely dangerous and have an agreement to not use them. For example, governments may sign a treaty against the use of cyber weapons in the same way as they have done against nuclear, biological and chemical weapons (Ashford, 2013). This implies that there could be an opportunity opened by such agreements to have greater cooperation among the various national intelligence agencies to share information about threats and attackers in cyberspace (The Economist, 2013).

Another implication has to do with ICT laws, i.e., the legal aspect of information technology use and deployment. Cybercriminals are already exploiting vulnerabilities and loopholes in national and regional legislation as they shift their operations to countries where appropriate and enforceable laws are not yet in place, and can, with almost total liberty, even launch attacks on victims in countries that do have laws in place.

Finally, the study has several policy implications- the need for cybersecurity policies that take into consideration the importance of the factor and its effect at the economic and national security levels. Such policies should enhance and be supportive of international cooperation and agreements (ITU, 2012), private-public partnerships, building community awareness, and empowering the human capital to identify cybersecurity problems, participate in designing solutions, and sharing with the other community entities the responsibility for having a safe and a resilient cyber space (CTO, 2010).

Moreover, national efforts to combat cyber threats and attacks have to take into consideration the fact that the vulnerability of modern societies, caused by their dependence on a spectrum of highly interdependent information systems, has global origins and implications. Based on this, international cooperation, ICT law enforcement, along with a secure infrastructure are presented as important elements in all cybersecurity-related policies. Any adequate protection policy that extends to strategically important parts of the information infrastructure will thus require global solutions: global cooperation and joint law enforcement (Cavelty, 2007).

To summarize, a number of initiatives related to cybersecurity and responses to cyber threats could be proposed among the international community participants. These could be envisaged within a model that can integrate the measures taken within an overall integrated and comprehensive framework. Provided that the implications mentioned above are taken into consideration, and a systemic approach that looks at the cyberspace problem in a holistic way is adopted, a country’s strategists, economics and security analysts, and policy makers can start with an analytical framework that encompasses threat assessments,
identifies gaps, determines vulnerabilities, and develops appropriate responses. The responses should take into consideration the results of the cyber threat impact analysis, as well as the criticality of the nation’s assets in terms of critical infrastructures, economic security, and national security.

REFERENCES

De Villiers, M. 2009. “Information Security Standards”, University of New South Wales, Faculty of Law, Research Series, Paper 34.


Silvius, A. G., & Schipper, R. 2010, November.” A maturity model for integrating sustainability in projects and project management”. In 24th World Congress of the International Project Management Association. IPMA Istanbul.

Cybersecurity Index: Integrated Framework


