Chapter 12
Fostering Public-Private Partnership: Between Governments and Technologists in Developing National Cybersecurity Framework

Vasaki Ponnusamy
Universiti Tunku Abdul Rahman, Malaysia

N. Z. Jhanjhi
https://orcid.org/0000-0001-8116-4733
Taylor's University, Malaysia

Mamoona Humayun
College of Computer and Information Sciences, Jouf University, Saudi Arabia

ABSTRACT

This chapter intends to provide a review of cooperation between public and private sectors towards cybersecurity governance. With the partnership, government can have confidence towards the safety and protection of their national critical digital infrastructure. The goal of this chapter is achieved by analyzing some of the cybersecurity frameworks adopted by the developed and developing nations. The analysis is further carried out by investigating the public-private policy initiatives in their national cybersecurity framework. The chapter also investigates the effectiveness of the National Institute of Standards and Technology Cybersecurity Framework (NIST) adopted by the US government.

DOI: 10.4018/978-1-7998-1851-9.ch012

INTRODUCTION

This Survey starts with brief discussion of some existing structures for Internet governance from the cyber security point of view. The survey will further embark on how different nations and states are responding to cyber security governance by studying the framework that they adopt and synergy between different nations. Among the many governing bodies of the Internet, Internet Corporation for Assigning Names and Number (ICANN) and Internet Engineering Task Force (IETF) play important roles in terms of setting up policies and protocols (Becker, 2019; Bradshaw & DeNardis, 2018). ICANN is dedicated to creating and distributing domains whereas the IETF is more on the technical aspects of the Internet protocols and computer codes (Handley, Bonaventure, & catholique de Louvain, 2013; Veillette, van der Stok, Pelov, & Bierman, 2018) . Although some pieces of the domain of the Internet could be owned by private sectors and the government owners, the Internet by itself is not owned by anyone. The IETF actually sets rules on how the Internet domain works, and in other words, this is an "open international community of network designers, operators, vendors and researchers concerned with the evolution of Internet architectures and smooth operation of the Internet" (Fidler, 2013; Rosenzweig, 2012).

As far as cyber security is concerned, one of the attempts made by IETF is the adoption of Domain Name System Security Extension (DNSSEC). The IETF has proposed some add on a suite of security functionalities that will become part of the Internet Protocol. Under this suite, the user should be able to authenticate the origin of the DNS data, to authenticate the domain name existence and to ensure the integrity of the DNS (Devarapalli & Joshi, 2013). This protocol suite is integrated to ensure that users actually access the legitimate domain name instead of some fake domain names. Without this effort, there is a high tendency for man-in-the-middle attack in which an intruder can intercept the communication between the sender and receiver to perform malicious activities. As far as DNSSEC is concerned, it acts as a synergy between IETF and ICANN. IETF provides the protocol whereas ICANN plays a role in terms of domain name authentication (Devarapalli & Joshi, 2013; Mundy, 2011; Satola & Judy, 2010). In order to authenticate any domain names, a chain of trust has to be established in which a root certification body can provide authentication to any domain names and websites. To trust these root certification bodies, a trust anchor has to be established into the chain of trusts. This trust anchor is provided by ICANN, although some people are not in favor of ICANN since it is an American company and they believe that it is of American interest (Lever et al., 2016).

Establishing trust and providing neutrality is of great challenge and currently, IETF sets the technical standards whereas ICANN is in charge of the creation of new domain names. These two nonprofit organizations are the current role players in international governance (O'Mahony, 2005; Shackelford & Craig, 2014). Although it has become standard practice, the trend is changing at the nation level whereby some countries are trying to alienate themselves from the Internet or even trying to sensor traffics coming to their borders, China a good example of this. While some countries have greater restrictions on Internet use, some countries have even much greater restrictions like the use of domestic Internet domains for all uses of entrepreneurial online services. Some countries have even proposed to impose restrictions on Internet contents as well as to have greater control over the Internet operation. A greater concern for countries like China and Russia is to have their own cyberspace control and to perform censorship on the Internet at the domestic level (Kalathil & Boas, 2010; Taubman, 1998). This is the new trend seen in the new initiative of state leaders to have their own cyberspace borders. This cyberspace territorial sovereignty is not only seen in major key players like China and the United States but also rampant in other countries that are developing in its cyberspace (Heintschel von Heinegg, 2013; von Heinegg, 2012).