Chapter 30
Modeling a Cyber Defense Business Ecosystem of Ecosystems:
Nurturing Brazilian Cyber Defense Resources

Edison Ishikawa
University of Brasília, Brazil

Eduardo Wallier Vianna
https://orcid.org/0000-0003-3914-7352
University of Brasília, Brazil

João Mello da Silva
University of Brasília, Brazil

Jorge Henrique Cabral Fernandes
University of Brasília, Brazil

Paulo Roberto de Lira Gondim
University of Brasília, Brazil

Ricardo Zelenovsky
University of Brasília, Brazil

ABSTRACT

Providing cyber defense in a country is complex. It involves ensuring the security of various products and services that are part of a global supply chain. In this complex scenario, the challenge is the development of a cyber defense business ecosystem that, reaching a minimum level of maturity, guarantees the security of products and services in cyberspace. This work proposes a cyber defense business ecosystem of ecosystems (BEoE) model with two ecosystems that must be created or fostered, the human resources training ecosystem and the product and service homologation and certification ecosystem. These two cyber defense ecosystems are key to the sustainable growth of an entire chain of production and sourcing of cyber defense goods and services. The proposed model allows the Cyber Defense BEoE to evolve, so that different actors (companies and government agencies) with different levels of maturity in defense and cybersecurity may emerge. In this way, a country's Cyber Defense BEoE may be able to provide products and services at different levels of security for its defense system.

DOI: 10.4018/978-1-6684-3698-1.ch030

Copyright © 2022, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

We live in a world that is increasingly dependent upon information and communication technology (ICTs), in which electro-digital controls are embedded in diverse products, services and systems that we use in our everyday lives. This technology and its controls contain known and unknown vulnerabilities, which put people, businesses, societies, and states at risk. In other words, ICTs are a fundamental need in order to maintain our way of life and our wellbeing. Knowledge of the vulnerabilities, and how to manage them, is essential to survival in cyberspace (FERNANDES; MEIRA, 1998).

Brazil faces an elevated dependence upon technology as compared to industrialized countries, in basically every ICT area, from electrical energy systems, through nanomaterial, semiconductors, memory, microprocessors, network and transceiver wiring, modems, switches, routers, firewalls, filmware, software, operational systems, programming language and even cryptographic algorithms (FERNANDES, 2013a). We also depend upon standards, use doctrines, operation, maintenance, and evolution of ICT systems that are not entirely matched to our conditions.

All future scenarios projected for Brazil indicate the intensification of ICT use in society, industry and government. Thus, in the absence of policies that reduce technological dependence, the country will surely lose sovereignty (FERNANDES, 2013c). In other words, the control of the chain of production, operation, maintenance and evolution of ICTs is directly related to National Development and Defense.

If the automation of information and communication is the foundation for industrial development and national defense, and if the country is tending to become less independent and less sovereign, public policies should be created to revert this situation (FERNANDES, 2013c).

Within this context, the following question should be asked: Is the cyber defense of a State tied to the success of the National Productive/Economic Cyber Defense Sector that it sustains?

This article seeks to build and test a Business Ecosystem of Ecosystems (BEoE) model to be applied to a productive/economic sector, that of cyber defense. The text explores a new approach by adapting the concept of Business Ecosystems, which is normally applied within a company in order to launch economic development of a sector with the participation of government, the productive sector, academia, and society. It is worth noting that that which is taking form is not just a game of connecting mismatched parts, but rather a joint construction involving all interested parties with the goal of creating space for consensus, which can then be followed by the erection of institutions, relations and functions of a productive/economic sector to be called the Cyber Defense Sector (FERNANDES, 2012b).

The concept of a productive/economic sector as "BEoE of Brazilian Cyber Defense" comprised of various Business Ecosystems allows comprehension of the context in which Brazilian Cyber Defense is embedded, facilitating recognition of possible connections with diverse actors and chains of production that: either exist or should be created or should be fostered within the Ecosystem.

In order to understand the construction of this model so that a space for consensus may be created between all institutional spheres involved, the chapter suggests the following route: section 2 is a bibliographical inventory on Business Ecosystems; followed by section 3 which presents the work method; next, section 4 proposes a BEoE model applied to a productive/economic sector; section 5 maps the Cyber Defense BEoE according to the model proposed in section 4; and finally, section 6 presents a few final considerations.

25 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/modeling-a-cyber-defense-business-ecosystem-of-ecosystems/288701

Related Content

IoTP an Efficient Privacy Preserving Scheme for Internet of Things Environment
Shelendra Kumar Jainand Nishtha Kesswani (2020). *International Journal of Information Security and Privacy (pp. 116-142).*
www.irma-international.org/article/iotp-an-efficient-privacy-preserving-scheme-for-internet-of-things-environment/247430

A National Information Infrastructure Model for Information Warfare Defence
Vernon Staggand Matthew Warren (2003). *Current Security Management & Ethical Issues of Information Technology (pp. 97-110).*
www.irma-international.org/chapter/national-information-infrastructure-model-information/7386

GARCH Risk Assessment of Inflation and Industrial Production Factors on Pakistan Stocks
Shehla Akhtarand Benish Javed (2012). *International Journal of Risk and Contingency Management (pp. 28-43).*
www.irma-international.org/article/garch-risk-assessment-inflation-industrial/74751

A Trust-Integrated RPL Protocol to Detect Blackhole Attack in Internet of Things
Anshuman Pateland Devesh Jinwala (2021). *International Journal of Information Security and Privacy (pp. 1-17).*
www.irma-international.org/article/a-trust-integrated-rpl-protocol-to-detect-blackhole-attack-in-internet-of-things/289817

Advanced Security Incident Analysis with Sensor Correlation
Ciza Thomasand N. Balakrishnan (2012). *Situational Awareness in Computer Network Defense: Principles, Methods and Applications (pp. 302-319).*
www.irma-international.org/chapter/advanced-security-incident-analysis-sensor/62388