Chapter 17
A Strategic Framework for a Secure Cyberspace in Developing Countries with Special Emphasis on the Risk of Cyber Warfare

Victor Jaquire
University of Johannesburg, South Africa

Basie von Solms
University of Johannesburg, South Africa

ABSTRACT

The objective of this paper is to provide a strategic framework for a secure cyberspace in developing countries, taking cognisance of the realities and constraints within a developing milieu; and to discuss if the risk of cyber warfare and related techniques against developing countries should be addressed within 'The Framework'. Cybersecurity policies and related strategies are required for developing countries in order to effectively safeguard against cyber related threats (the same as for developed countries). These policies and strategies for developing countries will differ from those of developed countries due to the unique realities within a developing world. Africa in specific is presently seen as a hotbed for cybercrime, and one of the reasons is that many African countries do not have a proper framework, policies and procedures to properly protect cyberspace. Experience has also shown that a pure adoption by developing countries of the cyber frameworks of developed nations will not always be effective, especially due to the unique requirements and realities within developing worlds, such as limited resources, infrastructure, technologies, skills and experience. It is also necessary when talking about a strategic framework to secure cyberspace, to discuss cyber warfare, its general application and its possible utilisation as part of the strategy to protect national critical information infrastructure. This, as part of a developing country's national security strategy in addition to traditional cybersecurity defence measures. The approach taken for the research program, and discussed in this paper, is based on a comprehensive literature study on several existing cybersecurity policies and strategies from both

DOI: 10.4018/978-1-5225-7912-0.ch017

developed and developing countries. From this the drivers / elements for national cybersecurity policies and strategies were identified. These drivers were than adapted to specifically relate to the requirements of developing countries, and then, utilising the identified and adapted drivers, our strategic framework for developing countries to secure their cyberspace was developed. This document will be very useful for those African countries venturing into defining relevant policies and procedures.

1. INTRODUCTION

The continuous development of the internet in the last few decades together with the resulting growth, innovation and capital investment in related technologies, compel developing nations to establish and mature its cybersecurity environment in order to mitigate the threats that accompany the vast capabilities that these innovations provide. The growing access of developing countries to cyberspace, requires that all such countries should have a proper plan to help secure their cyberspace. Although some documents for this purpose do exist, they are usually long and complex and do not provide simple and clear cut guidance on where to start securing cyberspace. Developing countries, because of financial and expertise constraints, cannot do everything at the same time – so a more basic document is needed with clear steps on how to start.

What is therefore needed is a strategic framework for developing countries to secure cyberspace (in the rest of the paper referred to as 'The Framework'), to provide a starting point for developing countries when implementing its cybersecurity strategy. Such a framework can then be utilised as best practice or a blueprint by developing countries as a starting point in designing their own framework and strategy.

The purpose of this paper is to present such a framework in order to establish a guidance based on relevant factors and to encourage developing countries to address the securing of cyberspace in a comprehensively approach, instead of just focussing on a narrow scope of activities (Fischer, 2005).

Similar to the approach that ENISA followed in drafting an evaluation framework for national cyber security strategies, during which it analysed, among other, existing EU and non EU national cyber security strategies (ENISA, 2014); the approach taken in this research project is to study a number of relevant cybersecurity documents from a number of countries (developed and developing) and regional bodies. From these documents, the core elements which are common to all documents, are identified and extracted to determine the real important elements of such a strategic framework.

These identified elements are then evaluated in terms of the problems experienced by developing countries (DCs), and those ones which can add the quickest value to DCs – the quick wins – were used as the basis for the final framework. This approach ensures that DCs who want to venture along this path, has a framework document which provides clear direction on where to start and what to implement first – within the limitations of a DC.

The paper is structured as follows:

- Section 2 will briefly review the documents which were studied, while section 3 will list the priority elements which were identified;
- In section 4 the need for cyber warfare and the utilisation of related techniques within a developing country is discussed, with a deliberation on its inclusion within the strategic framework in line with the effort to secure cyberspace;