Chapter 6
Adaptation of the JDL Model for Multi-Sensor National Cyber Security Data Fusion

Ignatius Swart
CSIR, South Africa

Barry Irwin
Rhodes University, South Africa

Marthie M. Grobler
CSIR, South Africa

ABSTRACT

The potential attack surface of a nation is large and no single source of cyber security data provides all the required information to accurately describe the cyber security readiness of a nation. There are a variety of specialised data sources available to assess the state of a nation in key areas such as botnets, spam servers and incorrectly configured hosts. By applying data fusion principles, the potential exists to provide a representative view of all combined data sources. This research will examine a variety of currently available Internet data sources and apply it to an adapted Joint Directors of Laboratories (JDL) data fusion model in order to illustrate the potential gains and current limitations. The JDL model has been adapted to suit national level cyber sensor data fusion with the aim to formally define and reduce data ambiguity and enhance fusion capability in a real world system. A case study highlights the results of applying available open source security information against the model to relate to the current South African cyber landscape.

INTRODUCTION

As many as 35 nations around the world have published national cyber security policies since 2009 (Luiijf, Besseling, & De Graaf, 2013). The published cyber defence policies seek to address the growing concern that Governments, organisations and individuals have regarding their safety on the Internet. The

DOI: 10.4018/978-1-5225-7912-0.ch006

proposed implementations will involve not only Government or individual organisations but will have to be implemented at a 'whole of nation' or 'whole of Government' level. This is due to the way that the Internet is structured with no single entity controlling all the required infrastructure. These policies were tallied and used as an indicator of cyber readiness (Hathaway, 2013) to set the stage for more technical analysis of nation state cyber readiness to be obtained on a measureable level.

Obtaining a more quantifiable measurement than just taking policy publication into account is no trivial task however. A variety of factors such as available attack surfaces, national information sources, Internet penetration and general population education can play a significant role in such an assessment. While data is available for these additional factors to act as additional information sensors, it is not often considered in cyber security research literature at present. In order to use a variety of data sources, knowledge must be drawn from the field of data fusion since direct integration of all sources is highly improbable. Making use of data fusion principles will allow the information from multiple sensors to be used in such a manner to provide increased situational awareness on a national level. Cyber data fusion has not been extensively implemented, and literature regarding this topic is only recently becoming more readily available. The purpose of this research was to examine the potential use of public data sources for use in information fusion applications that focus on a national level. The data sources selected was evaluated and applied to an adapted Joint Directors of Laboratories (JDL) data fusion model. The results of the experimental system based on the adapted JDL fusion model will be presented in order to allow further evaluation of the model.

In order to achieve a cyber defence system that is applicable on a national level, concepts such as the national Internet domain and how a nation's attack surface could potentially be defined has to be discussed. The first two sections of this paper will introduce the concepts that was used the set the boundaries for this experiment with regard to national domain and measurable attack surface.

RESPONSIBILITY AND DEMARCATION OF A NATION'S INTERNET DOMAIN

Current cyber defence policies published by nations contain lists of key national capabilities that they are striving for. Various frameworks, models and standards are being used to assess the current state and to move forward to a more secure state such as the guide from NIST (National Institute of Standards and Technology (NIST) & United States of America, 2014). The problem is however that once the cyber defence policies of Governments are studied it becomes visible that no clear definition is available of what exactly will be protected (Cavelty, 2014). A recent study (de Souza, 2014) of United States cyber defence policies has revealed that Government is responsible for the safety of the Internet but current implementations focus on only protecting .gov websites. In South Africa legislation exists, and responsibility for each sector is defined in the National Cyber Security Policy Framework. In the policy, there is a clear indication of the responsibility that Government has towards Internet enabled infrastructure. Reinforcing the intent other legislation such as the Electronic Communication and Transactions Act of 2002 (South African Government Gazette, 2003) mandated that the .co.za domain be placed under the control of the Government (Naidoo, Singh, & Levine, 2013).

The question then is, what exactly constitutes the Internet domain of a country? Does liability stop when the IP address of a device is external to the IP address block assigned to the country? Or does geographic location play an important role in the determination of responsibility? The implications of unclear definitions can lead to unnecessary expenditure, misallocation of resources and insufficiently protected