Chapter 38
Big Data and National Cyber Security Intelligence

A. G. Rekha
Indian Institute of Management Kozhikode, India

ABSTRACT

With the availability of large volumes of data and with the introduction of new tools and techniques for analysis, the security analytics landscape has changed drastically. To face the challenges posed by cyber-terrorism, espionage, cyber frauds etc. Government and law enforcing agencies need to enhance the security and intelligence analysis systems with big data technologies. Intelligence and security insight can be improved considerably by analyzing the under-leveraged data like the data from social media, emails, web logs etc. This Chapter provides an overview of the opportunities presented by Big Data to provide timely and reliable intelligence in properly addressing terrorism, crime and other threats to public security. This chapter also discusses the threats posed by Big Data to public safety and the challenges faced in implementing Big Data security solutions. Finally some of the existing initiatives by national governments using Big Data technologies to address major national challenges has been discussed.

1. INTRODUCTION

With the availability of large volumes of structured and unstructured data and with the introduction of new tools and techniques for analysis, the security analytics landscape has changed drastically. To face the challenges posed by cyber-terrorism, espionage, cyber frauds etc. Government and law enforcing agencies need to enhance the security and intelligence analysis systems with big data technologies. There are two different approaches regarding security in the big data context. One is leveraging Big Data for enhancing the national security systems and second is to secure the national data itself. Intelligence and security insight can be improved considerably by analyzing the under-leveraged data like the data from social media, emails, telecommunication systems, web logs etc. By providing timely and reliable intelligence, big data analytics can help in properly addressing terrorism, crime and other threats to public security.

Nowadays more volume of significant data is available with the security officials as well as with the criminals and hence big data provides both opportunities and threats for national security and critical

DOI: 10.4018/978-1-4666-9840-6.ch038

infrastructures. Security systems need to be able to make use of information from a wide variety of sources including human and software applications in order to exploit the big data and to get value out of it. At the same time data ownership and privacy concerns are also to be taken into account. In light of the growing number of incidents of cyber terrorism and cases of threats to public security, in this chapter we will explore the national security implications of Big Data including opportunities, threats and challenges. The rest of the chapter is organized as follows: Section 1 will discuss Big Data opportunities for national cyber intelligence, section 2 will discuss threats of Big Data to National Security environment. Section3 will cover challenges in exploiting Big Data for national security. In section 4 we will discuss the role of Big Data Analytics for Critical Infrastructure Protection (CIP). Section 5 will discuss some of the tools and techniques available in the big data context and section 6 will discuss about some of the major initiatives taken by governments for national security. Section 7 concludes this chapter.

2. BIG DATA OPPORTUNITIES FOR NATIONAL CYBER INTELLIGENCE

This section will give an overview of how Big Data technologies can complement cyber security solutions. Law enforcement agencies can utilizes Big Data to ensure public safety by capturing and mining huge amounts of data from multiple sources. For example, there are systems which collect data related to travel, immigration, suspicious financial transactions etc. Linking previously unconnected datasets can remove anonymity of individuals and analyzing this data can reveal patterns of connections among persons, places or events. These patterns could then be used for proactive policy making to ensuring public safety. Big Data tools can provide actionable security intelligence by reducing the time for correlating, consolidating, and contextualizing information, and also correlate long-term historical data for forensic purposes. For instance, the WINE platform and Bot-Cloud allow the use of MapReduce to efficiently process data for security analysis. (Ardenas, 2013). Now we will discuss some of the opportunities of Big Data in the security landscape.

2.1. Efficient Resource Management to Set a Holistic Strategy

By integrating and analyzing huge amounts of structured and unstructured data from various sources we can have efficient security assessment and thereby support national security agencies to set a holistic strategy for public safety. Leveraging all sources of available data can present great opportunities for a more efficient resource management and thereby provide new insights and intelligence. Using big data logs from multiple sources could be consolidated and analysed. This provides a better security intelligence compared to analyzing in isolation.

2.2. Crime Prediction and Mitigation

Discovering hidden relationships and detecting patterns from data gathered from sources such as internet, mobile devices, transactions, email, social media etc. can reveal evidence of criminal activity. For example by correlating real time and historical user activity we can uncover abnormal user behavior and fraudulent transactions.