Chapter 83
Filtration of Terrorism-Related Texts in the E-Government Environment

Rasim M. Alguliyev
Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan

Ramiz M. Aliguliyev
https://orcid.org/0000-0001-9795-1694
Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan

Gunay Y. Niftaliyeva
Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan

ABSTRACT

E-government expresses the process of utilizing advanced information and communication technologies (ICT) to automate internal activities of government agencies and their external relations with citizens and businesses. All these interactions provide better, faster and more secure public services. In this article, a method for the detection of terrorism-related activities in the e-government environment has been suggested. In the proposed method, terrorism-related activities are defined based on the similarity between the users' opinions and the vocabulary database created linked to terrorism.

1. INTRODUCTION

E-government is accepted as a tool for changing of public administration. E-government has a strong institutional capacity to improve governance by providing better services to citizens and businesses, increasing transparency and social control (Spalevic et al., 2016; DoJ, 2007). In a successful e-government program, the following issues should be considered: economic development; combination (joining) and integration of state systems; advancing democratic principles; developing service to citizens and other constituencies. E-government should allow any user that enters the website to communicate with the

DOI: 10.4018/978-1-7998-2466-4.ch083

company's employees via the internet (audio-video, graphical user interface) (Fang, 2002; Gronlund & Horan, 2004). New technologies should be used to improve website access and state service transmission. Information exchange between state agencies is one of the most important issues for the development of national e-government architecture. The information exchange allows the government agencies to predict the security risks and attacks, including the terrorist threat similar to the September 11 attacks on America. Network relationships between state agencies provide accelerated data exchange. To receive information about terrorist activity simultaneously is very important for various government agencies. Employees of the state enterprise may use this information to protect their country, government, and citizens from traditional and cyber-terrorist attacks. While traditional terrorist attacks, police may rely on information collected (gathered) from previous terrorist activities and biometric documents to track suspects and prevent attacks. Also, a mobile phone can be used to track individuals, locations, and conversations. The use of the global internet network by many government agencies has resulted in the cyber-terrorism activity becoming more serious and complicated threat. Cyber-terrorism means the complete coverage of threats, risks, and technological issues (Weimann, 2004). The initial term of cyber-terrorism is, the national and critical infrastructural activities becoming more dependent on computer networks and the establishment of new shortcomings. Cyber-terrorism and terrorist activity on the Internet are monitored by relevant government agencies (Lemos, 2002).

To determine what drives people to the terrorism is not easy. Monitoring of the users that use critical websites considered to be the property of terrorist can lead to useful information. In order to avoid attacks from various terrorist organizations, government agencies should exchange and collaborate with relevant information. In the references, the detection, monitoring, and blocking of terrorist websites and social network profiles are considered to be the most important activity in fighting terrorism (TSC, 2015; Vighne et al., 2016). Taking on these facts into account an approach to define terrorism-related activities based on user comments in the e-government environment has been suggested in this paper. Detailed information about this approach is provided in the following sections. The paper is structured as follows. Section 2 gives information about terrorism and the Internet, Section 3 provides a brief overview of the terrorism and e-government, and Section 4 describes terrorism and big data analytics. The proposed method is explained in Section 5. A conclusion is provided in Section 6.

2. TERRORISM AND THE INTERNET

Due to the increased use of the Internet, a large number of new technologies are appearing on different dynamic platforms, which makes the use of it possible for malicious people on damaging society and people. Therefore, if the internet is accepted as a large digital library, we can observe billions of pages accessible information available here, and many of them are in the interest of terrorist groups. For example, terrorists can get information about vehicles, nuclear power plants, public buildings, airports and ports, and even anti-terrorism measures from the Internet.

The use of online platforms by terrorists is not novel. After the September 11 attacks and the anti-terrorism operations, a large number of terrorist groups passed in the cyberspace, establishing thousands of websites promoting their messages and activities. Many terrorist websites were targeted by intelligence and law enforcement agencies, and anti-terrorist services.

The usage of social media by terrorists has a number of reasons. The first is that these channels are popular in their coverage and allow terrorism to be part of the essence community. Secondly, social