Logic Tester for the Classification of Cyberterrorism Attacks

N. Veerasamy, Council for Scientific and Industrial Research, Johannesburg, South Africa

M.M. Grobler, University of Johannesburg, Johannesburg, South Africa

ABSTRACT

The merging of terrorism with the cyber domain introduces the potential for using computers and networked technologies in cyberspace to carry out extremist activities. Despite the current debate on whether cyberterrorism can be regarded as a real threat, this research will propose a method for classifying incidents as either cyberterrorism or cyber attacks. Although there have been no reported cases of Information Communication Technologies causing life-threatening situations or death, this research aims to show that cyberterrorism is not a negligible threat but instead a dangerous risk that should not be overlooked. This research will investigate the merging of terrorism with the cyber domain and present a multi-layered definition for cyberterrorism. This proposed definition is founded on the definition for traditional terrorism and incorporates elements of the international understanding of cyberterrorism. The research future presents a Logic Tester that uses Boolean logic to test the application of the multi-layered definition for cyberterrorism in terms of past international cyber incidents. The merit of the Logic Tester is presented through its application on a number of potential cyberterrorism scenarios, using the definition to classify these as either cyberterrorism or cyber attacks.

Keywords: *Classification, Cyber Incident, Cyberterrorism, Definition, Logic Tester, Terrorism*

INTRODUCTION

The idea of cyberterrorism merges the worlds of creating havoc and panic in the abstract realm of cyberspace. Cyberterrorism introduces the potential for using computers and networked technologies in cyberspace to carry out extremist activities that support political, religious and social viewpoints. Many argue that cyberterrorism is not a real threat as there are no known or reported cases of Information Communication Technologies causing life-threatening situations or death. However, this research aims to show that cyberterrorism is not a negligible threat but instead a dangerous risk that should not be overlooked.

Already in 2004, Prof Goodman from Georgia Tech (Elrom, 2007) emphasised the importance of taking cyberterrorism seriously as it could become a stronger threat later on. Furthermore, Denning (Elrom, 2007) also stated that terrorists may come to realise the enormous potential

DOI: 10.4018/IJCWT.2015010103

that cyberterrorism offers. She explained that the new generation of terrorists are operating in a digital world in which hacking tools provide for much more power, ease and accessibility.

In the past, terrorism was synonymous with physical attacks such as bombs, hijacking, plane explosions and nuclear attacks. However, due to the growth of digital dependence, cyberspace has also emerged as a prime battlefield. Colarik (2006) mentions that detonating a bomb may result in huge uproar and a high cost in terms of creation and delivery thereof. If a digital attack is executed, the effect can be just as disruptive but with reduced costs compared to a bomb. Terrorists who now wish to promote a political, social, ideological or religious viewpoint have identified computers and cyberspace as a crucial target on which they can unleash their attacks on. This research will investigate the merging of terrorism with the cyber domain and present a multi-layered definition for cyberterrorism, based on the definition for traditional terrorism and the international understanding of cyberterrorism. The research future presents a Logic Tester that uses Boolean logic to test the application of the multi-layered definition for cyberterrorism in terms of past international cyber incidents. The merit of the Logic Tester is presented through its application on a number of potential cyberterrorism scenarios, using the definition to classify these as either cyberterrorism or cyber attacks. The next section will address the merging of the traditional terrorism domain with that of the cyber domain.

BACKGROUND

The 9/11 United States terrorist attacks in 2001 left behind a legacy of effects. Death, destruction and devastation flowed from these terrorist attacks. The associated bloodbath and damage to critical infrastructure resulted in policy decisions around the world with the aim of preventing a similar onslaught in the future. Security at airports was heightened to new levels of control - additional security checks and carryon allowances were introduced. After the 9/11 attacks occurred, there was an outpouring of help from the emergency sector. Their efforts to save the injured and retrieve the dead were commendable. Tirelessly working through rubble and extreme conditions, the emergency services personnel consisting of police, firemen paramedics rushed in to help those trapped without considering the risks to their own lives. This tragic event brought a spotlight to the horror of terrorism. The implications of future attacks became a noteworthy issue.

Colarik (2006) mentions that information and communication infrastructure plays a role in the advancement of the technological capabilities of terrorists. The technological advancement could serve as support to cyberterrorism, as well as being the target of attacks. Borchgrave, Sanderson and Harned (2007) discuss the Internet being used to support terrorism with functions like training, organisation, networking, recruitment and funding. Alternatively terrorists could also be targeting critical networked infrastructure as damage to such targets would have a huge impact. Such infrastructure, according to the United States Army Training and Doctrine Command (2006) supports everyday activities. Critical infrastructure supports critical services and interfering with such life dependant services can have a devastating impact on the defence and economic structure of a country.

Many debate that cyberterrorism is not a realistic threat as cyber attacks do not result in casualties. Desouza and Hensgen (2003) show that one side argues that cyberterrorism has not hurt anyone while others argue that the threat is realistic and raises the issue of the economic losses that result after a virus is unleashed. The effect of the financial losses, productivity effects and damage to reputation and inconvenience should not be overlooked. The camp that argues that cyberterrorism is not a real threat, focuses on the supportive role that the Internet plays in recruiting members and planning operations. They feel that the Internet is not a prime target for