ADDRESSING THE SPECTRE OF CYBER TERRORISM: A COMPARATIVE PERSPECTIVE

F Cassim[*]

SUMMARY

This article looks at the definition of cyber terrorism and terrorist use of the Internet. The article evaluates cyber terrorist threats facing countries such as the United States of America, the United Kingdom, India and South Africa. The article also examines measures introduced by the respective governments in these countries to counteract cyber terrorist threats. Finally, the article will propose a way forward to counteract such possible threats in the future.

The face of terrorism is changing. The convergence of the physical and virtual worlds has resulted in the creation of a "new threat" called cyber terrorism. Cyber terrorism is one of the recognised cyber crimes. The absence of suitable legal frameworks to address cyber terrorism at national and regional levels, the lack of adequate safeguards, the lack of cyber security strategies and the pre-occupation of countries with internal factors have all contributed to the creation of an environment that can be easily infiltrated by cyber terrorists.

The horrific events of 9/11 provided the impetus for many countries to introduce anti-terrorist legislation. The United States of America, United Kingdom, India and South Africa have introduced legislation to address the threat of cyber terrorism.

KEYWORDS: Cyber space, cyber terrorists, cyber crime, cyber terrorism, hacktivism; legislation, international legislation; anti-terrorist legislation, cyber security, computer networks, critical infrastructure; United States of America, United Kingdom, India, South Africa.

[*]   Fawzia Cassim, BA (UDW) LLB (UN) LLM LLD (UNISA)Associate Professor, Department of Criminal and Procedural Law, UNISA, cassif@unisa.ac.za