ID 114

Equilibrium of Cybersecurity and Data Privacy: Analysing Cyber Terrorism in International Context

SCTS Fernando[1#], WMRK Wijesundara[1] and DNY Welaratne[1]

[1]Faculty of Law, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka

[#]fernandoclare7@gmail.com

Abstract

Since the dawn of information technology, terrorists have used cyberspace as a weapon to carry out their intentions. At the moment, cyber technology provides cyber terrorists with a comprehensive and complicated set of information and instruments with which to continue their attacks on governments. The usage of tools and the motivations of cyber terrorism has an impact on cyber security and data protection both directly and indirectly. This study identifies the effect of cyber terrorism on cyber security and data protection and focuses on the relevant cases that have arisen out of cyber terrorism and legal frameworks that have been established in addressing cyber terrorism, cyber security, and data protection. The study analyses the new trends of cyber security risks arising through cyber terrorism and examines how data breaches affect privacy and lead to cyber-terrorism. This primary research is evident almost at every stage of cyber-attack it affects cyber security and data protection as a subsidiary result. This study has identified the insufficiency of laws addressing cyber terrorism. This qualitative research is primarily supported by case laws, journal articles and statutes. Primarily it is evident the necessity of separate direct laws as well as Penal Code recognition for cyber terrorism and amendments should be taken place to address cyber terrorism, cyber security, and data protection from time to time depending on the innovations of cyber technology, for the perception of minimizing the terrorist attacks and negative impacts on it.

Keywords: *Information Technology, Cyber Terrorism, Cyber Security, Data Protection, Cyber Space*