A Critical Examination of Whether the National Security of Sri Lanka is Adequately Protected in Cyberspace

DU Jayasinghe[1#] and GD De Silva[1]

[1]Department of Law, University of Peradeniya, Sri Lanka

[#]dulmi.jayasinghe@gmail.com

The 21st Century is the century of Hi-tech and is no stranger to cyberattacks. Even Sri Lanka has undergone many cyberattacks in the past, which have also raised national security concerns. Whilst Sri Lanka has enacted legislation to deal with computer crimes such as the Computer Crime Act No. 24 of 2007, Evidence (special provisions) Act No 1995, Electronic Transactions Act No. 19 of 2006, Payment Devices Frauds Act No 30 of 2006, and the Intellectual Property Rights Act No. 36 of 2003, there are no enacted cybersecurity laws. In fact, the two Bills, namely the Cyber Security Bill and the Defence Cyber Commands Act have still not been passed even though it was proposed in 2018. Consequently, only Section 06 of the Computer Crime Act No. 24 of 2007 mentions computer crime offences committed against national security. Thereby, the research problem of this article is to examine whether the current cyber laws in Sri Lanka are sufficient to adequately protect the country's national security in cyberspace. The research objectives of this research are to examine whether the current cyber laws protect the national security in Sri Lanka (1), to evaluate the implementation process in the criminal justice system in terms of cyber laws (2) and to gain some perspectives on how other countries such as the United Kingdom and the United States of America have formulated legislation to protect their country's national security in the cyberspace. This research is an internet-based desk-based research and concludes that the existing legislation is insufficient to adequately protect the national security in Sri Lanka and that it is imperative to enact the two draft cybersecurity Bills at the earliest.

Keywords: *cyber-attacks, national security, cyber security laws*