ABSTRACT

Strategies on present warfare is dramatically change from asymmetric warfare to hybrid warfare whereas states and non-state actors paving with more opportunities to penetrates the nation states. In that dilemma offender would be fought in cyber domainand it is essential to formulate strategies to face the traditional and non-traditional threats as defender. Rapid technological developments in the information sector and its growing today's, make accessibility and has enabled its infiltrationto all sector of society. Rationally, then, protecting that upon which we depend should be front of mind for administration, business and industry, academia and every individual. The objectives of this study are to study whether Sri Lanka Armed forces is prepared to face future threats of information age that could penetrate the nation through the cyber sphere and to demonstrate strategies that Armed forces prerequisites to overcome those threats to national security and human security interests. The methodology undertakenfor this research is mix methods, with paper is developed from a positivist philosophy, treating the use of statistical, experimental and other numerical data, to describe the actions and phenomena observed, and the correlations and interactions between them. It is also uses the deductive approach to test the theory and correlations of variables. Secondary data such as newspaper articles, web articles, journal articles and statistics from the Department of Census and Statistics, Sri Lanka and the International Telecommunication Union too were utilised for this research.Internal consistency reliability test was satisfied with fairly high value of Cronbach's Alpha and sample adequacy was strengthen by KMO and Bartlett's Test with higher value of KMO. In conclusion, Sri Lanka civil sector and military sector should expand its capabilities in relation to cyber security. Moreover, implement the international treaties in to legal sector, as well as, empower its Armed Forces with national intelligence bureau so that they are more effective in nature to evaluating threats in the cyber domain and neutralize in initial stage. Furthermore, the country which is in the process of drafting a cyber-security policy for the country, whereas military sector needs to initiate cyber doctrine to pave with the future threats.

Key Words: CyberWarfare, Human Security, National Security,and Cyber security.