ABSTRACT

Active e-government is becoming a significant aim for many legislatures around the domain including Sri Lanka. Sri Lankan government initiate distribute many government services through e-channels such as introducing government information center (GIC) and payment gateways e-ticketing and e-procurement service etc.

Cybercrime has exceptionally improved in past few years as an obvious by product of high usage of internet, normally, and current a wide range of criminal act or threats to large business organizations and citizens alike. While cyber offenses (e.g., cyber harassment, Cyberstalking, intellectual property theft and identity theft,) and their address have been observed through various academic disciplines including criminology, sociology, electrical engineering, and information technology , nominal attention has been given to the role of e-government in overcome cybercrime a slightly ironic oversight given the electronic context of both. In Sri Lanka, there have been four main acts which used in prevention of cyber-crime. Content analyzed these acts. In Sri Lanka, there is an encounter in preventing cyber-crimes. Growth of communication based (network) crime has raised problematic issue in respect of proper balance among the requirements of those to carry out investigating and indicting such crime, and the privileges of users of such system networks. In this regard, this study will analysis challenges facing e-government focus on legislation, Regulatory, Institutional arrangements, policies and the current existing law and suggest any amendments if where necessary.

As cybercrime occurrences are on the growth, and it threat to both e-government initiatives of institutions of government, citizens and private own businesses, the focal objective of this research will be to way forward, how prevent and aware public and private sector the fact that about cybercrime which is unseen and that has not been exposed as yet as it relationship to the rate of escalation, effort of attack, incentive of the person who is doing cybercrime and find a way of reducing cybercrime activities at last and it effect on e-commerce or any other businesses to the bare minimum. Where prevention and control or avoid any of cybercrime is not completely probable, this research study will focus on preventive measures like recommending maximum and suitable punishment for offenders. Increasing the awareness about new media literacy is one way to minimize cyber-crime.

Keywords: E-government, cyber-crime, cyber law, digital security