World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

Cyber Warfare and Cyber Terrorism: An Analysis of Global Cooperation and Cyber Security Counter Measures

Authors : Mastoor Qubra

Abstract : Cyber-attacks have frequently disrupted the critical infrastructures of the major global states and now, cyber threat has become one of the dire security risks for the states across the globe. Recently, ransomware cyber-attacks, wannacry and petya, have affected hundreds of thousands of computer servers and individuals' private machines in more than hundred countries across Europe, Middle East, Asia, United States and Australia. Although, states are rapidly becoming aware of the destructive nature of this new security threat and counter measures are being taken but states' isolated efforts would be inadequate to deal with this heinous security challenge, rather a global coordination and cooperation is inevitable in order to develop a credible cyber deterrence policy. Hence, the paper focuses that coordinated global approach is required to deter posed cyber threat. This paper intends to analyze the cyber security counter measures in four dimensions i.e. evaluation of prevalent strategies at bilateral level, initiatives and limitations for cooperation at global level, obstacles to combat cyber terrorism and finally, recommendations to deter the threat by applying tools of deterrence theory. Firstly, it focuses on states' efforts to combat the cyber threat and in this regard, US-Australia Cyber Security Dialogue is comprehensively illustrated and investigated. Secondly, global partnerships and strategic and analytic role of multinational organizations, particularly United Nations (UN), to deal with the heinous threat, is critically analyzed and flaws are highlighted, for instance; less significance of cyber laws within international law as compared to other conflict prone issues. In addition to this, there are certain obstacles and limitations at national, regional and global level to implement the cyber terrorism counter strategies which are presented in the third section. Lastly, by underlining the gaps and grey areas in the current cyber security counter measures, it aims to apply tools of deterrence theory, i.e. defense, attribution and retaliation, in the cyber realm to contribute towards formulating a credible cyber deterrence strategy at global level. Thus, this study is significant in understanding and determining the inevitable necessity of counter cyber terrorism strategies.

Keywords : attribution, critical infrastructure, cyber terrorism, global cooperation
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020