Cyber terrorism and Counter it on the Dark Web

Ala Berzinji
PhD Student
Supervisor: Prof. Oliver Popov
Department of Computer and System Science - Stockholm University
Computer Science Department - University of Sulaimani
Alabe@dsv.su.se

Abstract

Everyone uses Internet on a daily base, and subject their privacy to vulnerability with each access. Internet has three layers, the first layer is Surface Web which is commonly used across the globe and constitutes only a small portion of the Internet. The second layer is called Deep Web, which is estimated to be used 1000 to 5000 times more than surface Web. Deep Web isn't used only for bad deals, most of the email servers are using Deep Web too that can be only accessed via direct links, and undetectable by search engines. The third layer is part of the Deep Web called " Dark Web". This layer is regarded as the most alarming part of Internet in which millions of dollars are circulating between its users every day without being controlled or tracked by any country. Deals done through Dark Web include assassinations (hiring a hit man), human trafficking, organ trafficking, buying and selling drugs, weapons and illegal software's used to hack visa cards; and its also currently used in cyber terrorism. Cyber security currently faces numerous threats and the most dangerous threat is the Dark Web. This study is highlighting the Dark Web, its usage and reviews the works of previous researchers aimed at counter cyber terrorism in the Dark Web. This study also demonstrates attempts and researches done in this field using Digital Trust Models, which would be a good guide for researchers willing to work on this subject.