## ABSTRAKSI

Pesatnya perkembangan teknologi berdampak pada kejahatan yang berbabis pada teknologi juga, seperti halnya *cybercrime*.Kini, hampir semua kejahatan dapat dilakukan menggunakan *cyberspace*, salah satunya adalah kejahatan terorisme.Terorisme sendiri merupakan kejahatan yang tidak luput dari perhatian masyarakat internasional, dimana terorisme dianggap sebagai suatu kejahatan luar biasa (*extra ordinary crime*).Oleh karena itu, fenomena kejahatan terorisme berbasis internet atau yang lebih dikenal dengan *cyber terrorism*, merupakan suatu ancaman serius bagi kemanan dunia. Serangan *ransomeware WannaCry* merupakan salah satu serangan *cyber* yang massif, dengan korban mencapai 150 negara di dunia, menyerang sejumlah kantor pemerintahan, layanan rumah sakit, sistem transportasi umum dan masih banyak lagi. Serangan terhadap jaringan komputer ini kemudian dianggap sebagai suatu serangan terror yang berbabis internet.

Penelitian ini disusun dengan metode penelitian yuridis normatif, yaitu penelitian yang difokuskan untuk mengkaji bahan pustaka atau data sekunder seperti perjanjian-perjanjian internasional, hasil penelitian, hasil karya dari kalangan hukum dengan menggunakan spesifikasi penelitian deskriptif-analitis, dan dikaji menggunakan metode Analisa data kualitatif.

Dari hasil penelitian ini, bahwasanya serangan terhadap suatu jaringan komputer dapat dikualifikasikan sebagai suatu bentuk kejahatan *cyber terrorism* apabila didasarkan pada unsur-unsur dalam kejahatan terorisme.Dimana suatu serangan siber tersebut dapat diklasifikasikan dalam bentuk *cyber terrorism* murni.Pada dasarnya, bentuk dari serangan *cyber* ini berupa *hacking*, *cracking*, DOS, *carding*, *unauthorized acces*, *cyber espionage*, *sabotage*, dan *extortion*.Dalam kasus serangan *ransomeware WannaCry* pada tahun 2017 silam, serangan *cyber* terjadi secara massif dan bersamaan di sekitar 150 negara di dunia.Serangan *cyber* secara massif ini kemudian dapat dikatakan sebagai suatu *cyber terrorism* dan merupakan suatu kejahatan transnasional yang teroganisir.


**Kata Kunci: *cyber terrorism*, hukum pidana internasional, jaringan komputer**

## ABSTRACT

*The rapid development of technology has made an impact technology-based-crimes, or better known as cybercrimes. These days, most of crimes can be done on cyberspace, for example terrorism. Terrorism itself caught the attention of the international community, and also considered as an extraordinary crime. Therefore, the internet-based-terrorism-act phenomenon (cyber terrorism) is a threat to world security and peace. The WannaCry Ransomeware attack, was the world most massive cyber attack. Spread to almost 150 contries across the world. It attacked government offices, hospital services, public transportation systems, etc. This cyberattack was considered as an internet-based-terrorist attack.*

*This research is conducted with a normative legal research which is defined as a scientific research done through literature study, by studying the various international regulations, literature, research, and papers related, with descriptive-analytical research spesifications, and qualitative data analysis method.*

*From this methods, it can be concluded that cyber terrorism can be formed as an attack on the computer network, if its has a terrorism background. Whereas, the attack can be qualified as pure cyber terrorism. Basically, the froms of cyberattack used by the terrorist are hacking, cracking, DOS, carding, unauthorized access,cyber espionage, sabotage and extortion. The WannaCry Ransomeware attack in 2017 was a massive cyber attack, claimed to be an act of cyber terrorism and also an organized transnational crime.*


***Kaywords: cyber terrorism, international criminal law, computer system***