ABSTRAK

Cybersecurity adalah ilmu yang menetapkan sebuah kebijakan terbaik untuk melindungi perangkat dari segala bentuk serangan siber (*cyberattack*). Dalam dekade terakhir, NHS diserang oleh WannaCry dan mempengaruhi sebagian besar arsitektur sistem siber NHS. Penelitian dengan judul "Kebijakan *Cybersecurity United Kingdom National Health Service* (NHS) Pasca *The Ransomware Wannacry Attack* Tahun 2017" memiliki rumusan masalah yaitu bagaimana Kebijakan *Cybersecurity United Kingdom National Health Service* (NHS) Pasca *The Ransomware Wannacry Attack* Tahun 2017. Tujuan penelitian ini adalah untuk mengetahui kebijakan *cybersecurity* yang dilakukan oleh NHS pasca serangan *WannaCry* pada tahun 2017. Penelitian ini menggunakan metode *library research* atau studi kepustakaan. Adapun sumber data yang digunakan adalah data sekunder dari sumber buku-buku, jurnal ilmiah terkait, serta laporan-laporan mengenai informasi kebijakan *cybersecurity* NHS pasca serangan *WannaCry*. Data akan dianalisis dengan teknik analisis kualitatif. Kerangka pemikiran yang digunakan adalah teori sekuritisasi.

Berdasarkan analisis data yang dilakukan, diperoleh kesimpulan bahwa Sekuritisasi NHS mencakup teori sekuritisasi oleh Barry Buzan serta pengembangan sekuritisasi dalam mengkaji *cybersecurity* oleh Hansen dan Nissenbaum yaitu *hypersecuritization*, *everyday security practice* dan *technification*. Aktivitas model sekuritisasi pertama yaitu *hypersecuritzation* dideskripsikan dengan pembentukan NHSX atau *National Health Service User Experience*. Model sekuritisasi kedua, *everyday security practice* di NHS direpresentasikan dengan membentuk *Data Protection Policy* sesuai dengan The EU General Data Protection Regulation (GDPR) tahun 2018. Model terakhir yaitu *technification* hadir dalam bentuk *Cyber Security Operations Centre* (CSOC) dan penggunaan program canggih dari kemitraan Microsoft yaitu *Advanced Threat Protection* (ATP).

Kata Kunci: *United Kingdom National Health Service* (NHS), *Cybersecurity*, Sekuritisasi dan Keamanan Internasional.

ABSTRACT

Cyber security is the science that establishes a best policy to protect devices from all forms of cyber attacks. In the last decade, NHS system was attacked by WannaCry and affected a large part of the NHS cyber system architecture. The study entitled "United Kingdom National Health Service (NHS) Cyber security Policy Post The Ransomware Wannacry Attack in 2017" has a problem formulation that is how the United Kingdom National Health Service (NHS) Cyber security Policy Post The Ransomware Wannacry Attack in 2017. The purpose of this study was to determine the cybersecurity policies which is conducted by the NHS after the WannaCry attack in 2017. This research used library research method. The data sources used were secondary data from books, related scientific journals and reports on NHS cyber security policy information after the WannaCry attack. The data will be analyzed with qualitative analysis techniques. The framework used is securitization theory.

Based on the data analysis, it was concluded that NHS Securitization includes the theory of securitization by Barry Buzan and the development of securitization in reviewing cyber security by Hansen and Nissenbaum that is hyper securitization, everyday security practice and technification. The activity of the first securitization model, that is hyper securitization, was described by the establishment of the NHSX or National Health Service User Experience. The second securitization model, everyday security practice in the NHS was represented by establishing a Data Protection Policy in accordance with The EU General Data Protection Regulation (GDPR) in 2018. The last model, technification, came in the form of the Cyber Security Operations Center (CSOC) and the use of advanced programs from the Microsoft partnership, namely Advanced Threat Protection (ATP).

Keywords: United Kingdom National Health Service (NHS), Cyber security, Securitization and International Security.