UPAYA SEKURITISASI PEMERINTAH INGGRIS DALAM KEBIJAKAN KEJAHATAN CYBER WANNACRY TAHUN 2017

SKRIPSI

Oleh:

ALMA SYAFIRA

17323047

PROGRAM STUDI HUBUNGAN INTERNASIONAL

FAKULTAS PSIKOLOGI DAN ILMU SOSIAL BUDAYA

UNIVERSITAS ISLAM INDONESIA

2020

UPAYA SEKURITISASI PEMERINTAH INGGRIS DALAM KEBIJAKAN KEJAHATAN CYBER WANNACRY TAHUN 2017

SKRIPSI

Diajukan Kepada Program Studi Hubungan Internasional

Fakultas Psikologi dan Ilmu Sosial Budaya Universitas Islam Indonesia

Untuk Memenuhi Sebagian Dari Syarat Guna Memperoleh

Derajat Sarjana S1 Hubungan Internasional

Oleh:

ALMA SYAFIRA

17323047

PROGRAM STUDI HUBUNGAN INTERNASIONAL
FAKULTAS PSIKOLOGI DAN ILMU SOSIAL BUDAYA
UNIVERSITAS ISLAM INDONESIA
2020

HALAMAN PENGESAHAN

Skripsi dengan Judul:

UPAYA SEKURITISASI PEMERINTAH INGGRIS DALAM KEBIJAKAN KEJAHATAN CYBER WANNACRY TAHUN 2017

Dipertahankan di depan Dewan Penguji Skripsi Prodi Hubungan Internasional

Fakultas Psikologi dan Ilmu Sosial Budaya

Universitas Islam Indonesia

Untuk Memenuhi Sebagian Dari Syarat – Syarat

Guna Memperoleh Derajat Sarjana S1 Hubungan Internasional

Pada Tanggal

22 Desember 2020

Mengesahkan

Program Studi Hubungan Internasional

Fakultas Psikologi dan Ilmu Sosial Budaya

Universitas Islam Indonesia

Ketua Program Studi

(Hangga Fathana, S.I.P., B.Int.St., M.A)

Dewan Penguji: Tanda Tangan

1. Hangga Fathana, S.IP., B.Int.St., M.A
2. Hadza Min Fadhli Robby, S.IP., M.Sc.
3. Willi Ashadi, S.HI., M.A.

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini, saya:

Nama : Alma Syafira

No. Mahasiswa : 17323047

Program Studi : Hubungan Internasional

Judul Skripsi : Upaya Sekuritisasi Pemerintah Inggris Dalam Kebijakan Kejahatan Cyber WannaCry Tahun 2017

Melalui surat ini saya menyatakan bahwa:

1. Selama melakukan penelitian dan pembuatan laporan penelitian skripsi saya tidak melakukan tindakan pelanggaran etika akademik dalam bentuk apapun, seperti penjiplakan, pembuatan skripsi oleh orang lain, atau pelanggaran lain yang bertentangan dengan etika akademik yang dijunjung Universitas Islam Indonesia. Karena itu, skripsi yang saya buat merupakan karya ilmiah saya sebagai peneliti, bukan karya jiplakan atau karya orang lain.
2. Apabila dalam ujian skripsi saya terbukti melanggar etika akademik, maka saya siap menerima sanksi sebagaimana aturan yang berlaku di Universitas Islam Indonesia.
3. Apabila di kemudian hari, setelah saya lulus dari Fakultas Psikologi dan Ilmu Sosial Budaya, Universitas Islam Indonesia ditemukan bukti secara meyakinkan bahwa skripsi ini adalah karya jiplakan atau karya orang lain, maka saya bersedia menerima sanksi akademis yang ditetapkan Universitas Islam Indonesia.

Yogyakarta, 22 Desember 2020

Yang menyatakan,

Alma Syafira

HALAMAN PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Alhamdullillahirabbil'alamin

Rasa syukur tiada henti diucapkan oleh penulis atas keberhasilannya dalam melewati proses penelitian yang menghasilkan karya sederhana ini sebagai tanda bakti, hormat, dan terima kasih tiada tara yang saya persembahkan kepada:

Ayah dan Ibu

Terimakasih teruntuk ayah dan ibu yang selalu mengiringi dengan doa dan dukungan yang tak pernah putus. Berkat do'a yang diberikan setiap langkah terasa ditunjukkan pada jalan terbaik dalam menghadapi segala tantangan sehingga berhasil membawa diri ini menyelesaikan studi dengan baik. Terimakasih atas segala kasih sayang yang terus memotivasi diri ini sebagai diri yang terus mengedepankan usaha dan menciptakan kepribadian yang mandiri. Semoga ini menjadi langkah awal untuk berjuang, dan membentuk masa depan yang dapat memberikan rasa nyaman pada ayah dan ibu saat hari tua.

Kakak dan Keluarga Besar

Terimakasih atas segala dukungan, motivasi, dan do'a yang selalu berhasil dalam mengembalikan rasa semangat pada proses penyusunan peneliatian ini.

HALAMAN MOTTO

"Don't say you don't have enough time. You have exactly the same number of hours per day that were given to Helen Keller, Pasteur, Michelangelo, Mother Teresa, Leonardo da Vinci, Thomas Jefferson, and Albert Einstein."

– H. Jackson Brown Jr –

"The secret of your future is hidden in your daily routine."

– Mike Murdock –

"I've never wanted to be a lady who lunches;
I've always wanted to be a woman who works."

– Meghan Markle –

"Do anything, but let it produce joy."

– Walt Whitman, Leaves of Grass –

KATA PENGANTAR

Segala puji bagi Allah Subhanahu wa ta'ala, Tuhan semesta alam, yang Maha Pengasih lagi Maha Pemurah serta sholawat dan salam kepada Rasulullah Shallallahu 'alaihi wasallam. Berkat limpahan rahmat-Nya penulis mampu menyelesaikan skripsi ini dengan baik yang mana merupakan persyaratan guna memperoleh gelar Sarjana Hubungan Internasional pada Universitas Islam Indonesia. Penulis menyadari bahwa dalam proses pengerjaan skripsi ini tidak bisa lepas dari bimbingan, dorongan, nasehat dan bantuan baik materil maupun spiritual dari berbagai pihak. Oleh karena itu pada kesempatan ini penulis ingin menyampaikan rasa terimakasih yang sebesar-besarnya kepada:

1. Allah SWT, yang tanpa henti mengaliri rahmat-Nya kepada penulis.
2. Kedua orang tua, kakak, serta keluarga besar atas segala kasih sayang, do'a dan dukungan yang begitu memotivasi penulis untuk dapat terus berjuang dan melawan rasa malas untuk mempersiapkan masa depan yang baik. Segala jasa yang diberikan sungguh tak dapat di deskripsikan dengan kata betapa bersyukurnya saya berada pada lingkungan keluarga yang suportif dan menjadikan diri ini untuk terus berusaha mencapai apapun dengan baik. Semoga keluargaku, sebagai orang pertama yang selalu saya cintai, selalu dibawah lindungan Allah SWT.
3. Bapak Dr. H. Fuad Nashori, S.Psi., MA.g., Psikolog selaku Dekan Fakultas Psikologi dan Ilmu Sosial Budaya Universitas Islam Indonesia
4. Bapak Hangga Fathana, S.IP., B.Int.St., M.A. selaku Dosen Pembimbing Skripsi (DPS) yang telah menjadi peran besar dalam meraih capaian ini dapat terjadi. Sungguh syukur tidak pernah henti saya

ucapkan atas segala jasa yang bapak berikan. Terimakasih atas segala bentuk motivasi, ilmu dan saran yang bapak sampaikan sehingga membuat diri ini merasa semakin percaya diri terhadap kemampuan yang dimiliki. Setiap bimbingan selalu memberikan semangat besar tanpa adanya tekanan yang kemudian menjadi dorongan utama dalam menyelesaikan skripsi ini. Saya juga ingin mengucapkan terimakasih atas segala waktu yang sudah diluangkan untuk memeriksa skripsi saya yang mungkin seharusnya digunakan untuk istirahat, saya memohon maaf apabila ada salah sikap yang pernah saya buat. Semoga segala kebaikan yang telah bapak berikan akan dibalas dengan kebaikan yang berlipat ganda oleh Allah SWT. Aamiin

5. Bapak Enggar Furi Herdianto, S.I.P., M.A. selaku Dosen Pembimbing Akademik (DPA). Terimakasih atas bimbingan, dampingan, dan saran yang telah diberikan selama studi saya di HI UII. Tidak pernah sekalipun saya merasa tersesat dikarenakan bapak senantiasa memberikan informasi yang bermanfaat bagi kami. Saya begitu senang melakukan interaksi dengan bapak disaat ada hal yang perlu saya tanyakan atau diskusikan sehingga tidak sekalipun saya berada pada posisi yang membingungkan. Terimakasih banyak Pak, semoga bapak selalu bertemu dengan orang-orang baik dan kebaikan bapak akan dibalas dengan kebaikan yang berlipat ganda oleh Allah SWT. Aamiin.
6. Segenap tim penguji skripsi, Bapak Hadza Min Fadhli Robby, S.IP., M.Sc. dan Bapak Willi Ashadi, S.HI., M.A. yang telah menguji,

mengoreksi, mengkritik dan memberikan saran kepada penulis, sehingga skripsi ini bisa lebih bermakna dan berguna.

7. Seluruh dosen dan civitas akademika Hubungan Internasional Fakultas Psikologi dan Ilmu Sosial Budaya Universitas Islam Indonesia. Berkat pengorbanan, ketulusan, kebaikan, dan ilmu pengetahuan yang Bapak dan Ibu berikan, kami bisa menjadi pribadi yang lebih baik dan berguna. Tak lupa juga saya ucapkan kepada Mbak Mardiatul Hasanah selaku staff prodi HI UII yang selalu membantu kami dengan kesabaran, baik dalam urusan-urusan akademik dan juga membantu dalam masalah penyelesaian skripsi ini. Semoga program studi HI UII akan selalu sukses dan membanggakan dari segi kualitas pendidikan yang diberikan.
8. Chieka Cartadila Jasmin, selaku kakak tingkat yang awalnya saya kenali sebagai partner kerja pada organisasi KOMAHI UII divisi media dan informasi. Terimakasih telah menjadi seseorang yang memiliki kepribadian yang memberikan nyaman pada orang-orang disekitarnya. Terimakasih telah menjadi seseorang yang selalu menerima segala bentuk cerita, memberikan saran, dan juga memberikan ilmu tak terkecuali pada hal media. Berkat Kak Chieka juga lah skripsi ini dapat diselesaikan dengan baik, terimakasih sudah mau direpotkan dan tetap bersedia untuk membantu walau terkadang saya datang pada waktu yang mungkin merupakan jam *nonton film-nya.*
9. Malinda Hestiyana, selaku kakak tingkat yang saya kenali melalui organisasi KOMAHI divisi media dan informasi yang selalu

memberikan bimbingan disaat ber-organisasi, hal akademik, dan juga membuat diri ini menjadi lebih terbuka disaat sesi bercerita. Tak lupa juga kepada M Aditya Dwi Sukmara, yang juga banyak memberikan bimbingan dalam hal berorganisasi, kepanitiaan, hal akademik. Terimakasih telah datang secara tiba-tiba dengan membawa informasi yang sangat mendetail untuk membantu sidang skripsi saya. Segala bentuk dukungan sangat memperlancar sidang saya pada hari H.

10. Dara Sonya, Annisa Nur Hidayati, Jifa Malika, Dewi Permatasari, dan Faqi Rawni selaku teman saya dari masa awal perkuliahan hingga saat ini. Terimakasih telah menjadi teman saya baik dalam hal akademik/non akademik serta menghiasi hari perkuliahan menjadi sangat menyenangkan dengan banyak canda tawa.
11. Santika Iza Hanifah, dan Agus Dzuriana Poetra selaku teman yang selalu bersedia untuk diajak pada hal yang berfokuskan pada masa depan yang lebih baik. Terimakasih telah menjadi teman yang sangat mendukung pada bidang ini meskipun tidak jarang Agus membagikan lelucon yang cukup membuat Santika dan Alma *geleng kepala.*
12. Annisa Wulandari, Nadia Firdaus, Santika Iza Hanifah, Sylva Fahri N., Fitria Trihandayani, Deo Fitra Amaldi, Yoma Nugraha, dan Dovan Patrioza selaku teman-teman kelas A yang masih memiliki ikatan erat dan menjadi alasan masa perkuliahan ini menjadi sangat menyenangkan serta berharga.
13. Teman-teman yang saya kenal melalui organisasi KOMAHI UII khususnya divisi Media dan Informasi (Periode 2018 – 2019) dan juga

Board of Executive (Periode 2019 – 2020) terlebih untuk Triokta Pela (Bang Rio) yang sudah memberikan kepercayaan pada saya sebagai salah satu anggota divisinya pada dua periode. Banyak sekali pelajaran serta pengalaman baru yang didapatkan melalui proses berkembang dengan kegiatan berorganisasi. Terimakasih telah menjadi saksi mata atas perkembangan saya dalam bekerjasama dengan team, serta membawakan saya pada lingkungan teman yang begitu suportif dalam membangun diri ini menjadi lebih baik.

14. FPCI UII periode 2018 – 2019 dan periode 2019 – 2020, terimakasih telah menjadi organisasi yang memperluas wawasan saya pada bidang HI, terimakasih atas segala pengalaman yang begitu membekas dan tidak akan pernah terlupakan. Kalian semua adalah orang-orang hebat.
15. Seluruh pihak yang telah hadir dan memberikan perubahan baik pada diri saya. Terimakasih telah datang dan memberikan dukungan dengan berbagai cara, semoga Allah SWT selalu membalas kebaikan kalian dengan berlipat ganda.

Atas segala bantuan yang telah diberikan, semoga mendapat imbalan yang setimpal oleh Allah SWT. Penulis juga berharap semoga skripsi ini dapat bermanfaat bagi pembaca.

Yogyakarta, 22 Desember 2020

Alma Syafira

DAFTAR ISI

DAFTAR TABEL

DAFTAR BAGAN

DAFTAR FIGUR

DAFTAR SINGKATAN

NHS	: *National Health Service*
NCSC	: *National Cyber Security Centre*
NCA	: *National Crime Agency*
GCHQ	: *Government Communications Headquarters*
OS	: *Operating System*
EPRR	: *Emergency Preparedness, Resilience and Response*
CNI	: *Critical National Infrastructure*
ACD	: *Active Cyber Defence*
CSP	: *Communications Service Providers*
NOCP	: *National Offensive Cyber Programme*
SGG	: *Strategic Governance Group*
CareCERT	: *Care Computer Emergency Response Team*

ABSTRAK

Kini penyerangan siber merupakan isu yang telah menjadi studi hubungan internasional. Ruang dunia siber atau ruang dunia maya akan terus berkembang dan akan semakin berkaitan dengan berbagai kegiatan masyarakat. Melihat dari besarnya aktifitas yang dapat dilakukan di dunia maya, tidak menutup kemungkinan untuk dapat memunculkan berbagai ancaman baru yang dapat sekaligus memberikan pengaruh besar pada negara. Saat ini negara dunia telah menyadari akan pentingnya meningkatkan keamanan siber sebagai salah satu prioritas. Kejadian penyerangan siber WannaCry pada tahun 2017 menjadi peringatan bagi negara seluruh dunia dikarenakan virus ini cukup untuk menyoroti kelemahan keamanan siber pada suatu negara. Melalui penelitian ini penulis akan menganalisis mengenai tindakan sekuritisasi yang dilakukan oleh Inggris sebagai salah satu korban yang terdampak besar pada kejadian penyerangan siber WannaCry tahun 2017.

Kata Kunci: *Penyerangan siber, keamanan siber, WannaCry, National Health Service, Sekuritisasi.*

ABSTRACT

Cyber attack has become an issue that has been around taking International Relation study's attention. The cyberspace will continue to grow and will increasingly be associated with various human activities. Judging from the large amount of activities that can be carried out in cyberspace, it is possible to create various new threats that can simultaneously have a big impact on the country. Currently, the world's countries have realized the importance of increasing cybersecurity as a priority. The WannaCry cyber attack incident in 2017 is an alert to countries around the world because this virus is enough to highlight the cyber security weaknesses in a country. Through this research, the writer will analyze UK's securitizing moves due to the fact that UK is one of the victims who were greatly affected by the WannaCry cyber attack in 2017.

Keywords: *Cyber Attacks, Cyber Security, WannaCry, National Health Service, Securitization.*

BAB I

PENDAHULUAN

1.1. Latar Belakang

Kemajuan pesat pada perkembangan ilmu pengetahuan dan teknologi membawa dunia saat ini tengah berada dalam era digital. Internet sebagai bagian dari *new media* pada era ini menjadi salah satu faktor perubahan gaya hidup pada masyarakat luas. Seiring dengan adanya revolusi industri, saat ini para pengembang teknologi digital meningkatkan fasilitas pada berbagai aspek kehidupan yang memudahkan kegiatan sehari-hari masyarakat. Internet adalah platform multimedia yang memberikan wadah bagi aneka ragam bentuk seperti komunikasi, informasi, dan transaksi (McQuail, 1983, p. 313). Internet memiliki peranan penting yang tidak dimiliki media konvensional. Kehadiran internet memberikan ruang pada dunia baru, atau sering disebut dengan dunia maya (*cyberspace*) yang menyempitkan waktu, ruang, dan jarak sehingga memudahkan komunikasi satu sama lain (Jati, 2016, p. 26).

Penetrasi internet pada masyarakat internasional selalu berkembang setiap tahunnya. “Semenjak dikenalnya pola komunikasi melalui dunia maya atau internet, batas-batas konvensional yang dahulu dianut dan dipatuhi oleh konsensus internasional menjadi semu” (Soewardi, 2013). Peluang bagi para ahli teknologi digital untuk terus melakukan inovasi pada sistem semakin terbuka lebar, keamanan pada penggunaan internet secara bertahap juga menjadi krusial. Banyak dari masyarakat yang kini telah menaruh sebagian besar data pribadi hingga data penting pada suatu perangkat dan juga memanfaatkan fitur penyimpanan data online. Negara juga memanfaatkan penggunaan teknologi dan jaringan untuk

memudahkan memberikan layanan bagi masyarakat, tetapi hal tersebut dapat menjadi sebuah ancaman yang meluas apabila negara tidak mempersiapkan pertahanan dan keamanan sebagai bentuk kewaspadaan. Penyerangan siber (*cyber-attack*) menjadi suatu hal yang membahayakan mengingat penyerangan dapat dilakukan secara anonim dan mampu melampaui batas suatu negara.

Dampak negatif dari pengembangan dunia maya tidak hanya berdampak pada individu tetapi juga memicu ketegangan antar negara yang memberikan dampak pada perdamaian dunia (Soewardi, 2013). Terdapat dua bentuk kejahatan dunia maya: 1) Komputer sebagai alat dalam melakukan kejahatan, seperti adanya pelecehan melalui sosial media, penipuan, propaganda yang melanggar hukum, pornografi, intimidasi, dan sebagainya. 2) Komputer sebagai sasaran kejahatan, seperti munculnya ancaman yang merusak atau mengganggu sistem komputer melalui malware, botnet, pencurian identitas, dan lainnya (Tabansky, 2012, p. 119). Bentuk ancaman yang menjadikan komputer sebagai sasaran memberikan kerugian yang sangat besar. Kerugian peretasan yang mengakibatkan hilangnya data dan ambil alih kontrol terhadap teknologi, merupakan suatu hal yang tidak sederhana apabila terjadi pada institusi besar. Penyerangan siber berpotensi merugikan negara di tingkat strategis atau politik. Estonia merupakan salah satu negara yang mengalami awal munculnya penyerangan siber yang sangat besar. Pada tahun 2007, sekitar 3 minggu kehidupan internet negara Estonia telah terganggu. Penyerangan tersebut mengakibatkan terganggunya akses pada portal pemerintahan, kementerian, bank-bank besar, bisnis toko online masyarakat, dan lainnya. Akibatnya, sebagian besar berdampak pada aktivitas ekonomi masyarakat dan

menciptakan keresahan bagi seluruh Uni Eropa. Penyerangan ini dimulai tanpa adanya peringatan dan persenjataan. (NATO Stratcom, n.d., p. 52 & 56)

Penyerangan siber kemudian semakin meluas pada berbagai sektor dan dapat dilakukan untuk kepentingan individu secara anonim. Pada tahun 2013 di Kiev, Ukraina, seseorang berhasil meretas jaringan komputer administrasi bank dan mengalami kerugian lebih dari 300 juta dollar. Pencuri telah berhasil melakukan pemindahan uang melalui ATM yang telah di retas dan dikirimkan ke rekening palsu mereka. Peretasan ini dimulai dengan mengirim email sebagai umpan kepada karyawan bank, kemudian secara tidak sengaja kode berbahaya telah terunduh. Peretas mulai mengamati jaringan bank sampai mereka menemukan karyawan yang bertugas mengelola sistem transfer tunai (ATM) yang terhubung dari jarak jauh. Melalui berita tersebut diketahui banyak negara lain yang juga mengalami hal yang serupa dalam rentang waktu yang bersamaan. Walaupun kejadian ini tidak diungkapkan pada masyarakat secara menyeluruh, tetapi kejadian tersebut menjadi sebuah peringatan untuk meningkatkan keamanan siber bagi seluruh negara dunia (Satter, 2015).

Sesuai dengan perkembangan teknologi, model serangan yang ada semakin kompleks dan turut berkembang seiring pengembangan ilmu pengetahuan manusia. Motif kejahatan siber secara garis besar dilakukan dengan pemerasan. Setiap tahunnya angka total biaya yang diakibatkan oleh penyerangan siber selalu meningkat, total biaya dari dampak kejahatan dunia maya meningkat dari US$ 11,7 juta pada tahun 2017 menjadi US$ 13,0 juta pada tahun 2018 artinya terdapat kenaikan 12 persen (Bissell & Ponemon, 2019, p. 11). Pelaku tidak hanya menyerang pada industri perbankan, tetapi juga pada sektor kesehatan, sektor

teknologi informasi, dan lainnya. Seiring adanya revolusi industri, berbagai sektor penting negara semakin bergantung pada sistem dan jaringan komputer, oleh karena itu pengembangan berkelanjutan masalah penyerangan siber menjadi bagian dari masalah keamanan baik nasional dan internasional. Permasalahan siber memiliki posisi penting bagi setiap negara dunia untuk dilakukannya pembangunan keamanan yang akan mencegah ancaman masuk.

UK telah menjadikan keamanan siber sebagai salah satu dari empat prioritas terpenting oleh keamanan nasional sejak tahun 2010 (House of Parliament, 2011, p. 1). Dalam menjalani strateginya, menurut *Global Cyber Security Index 2018*, United Kingdom (UK) telah berhasil menduduki posisi urutan pertama dunia pada pengembangan keamanan siber tahun 2018 (ITUPublications, 2019, p. 62). Kehidupan masyarakat yang semakin modern, menjadikan salah satu faktor UK memanfaatkan kegunaan teknologi untuk mendorong sektor bisnisnya sehingga cakupan dan kegunaan pada dunia siber semakin luas. Keterlibatan penggunaan teknologi digital yang semakin dibutuhkan dapat memiliki dampak besar baik positif maupun negatif. Seperti yang dialami oleh beberapa negara dunia dan institusi besar, UK juga telah menjadi sasaran terhadap penyerangan siber. Ransomware merupakan salah satu dari jenis *malicious software* (malware) yang melakukan alih kendali suatu perangkat dengan mengunci data atau file-file untuk mendapatkan tebusan. Penyebarannya dapat menyebar tanpa melihat batas negara. Motif dari penyerangan ini, pelaku melakukan penguncian data menggunakan enkripsi serta memberikan ancaman akan menghapus data secara permanen apabila korban tidak melakukan pembayaran. Serangan ransomware ini dinamakan

serangan siber WannaCry yang terjadi pada tahun 2017 dan merupakan kejadian penyerangan malware terbesar dari yang sudah ada.

Munculnya WannaCry pada tanggal 12 Mei 2017 lalu memberikan pengaruh pada setidaknya 100 negara di dunia dan meretas lebih dari 200.000 perangkat (NAO Report, 2018, p. 4). Untuk mendapatkan filenya kembali, pelaku menginginkan tebusan yang dibayarkan melalui bitcoin. Beberapa korban yang telah membayar tebusan tidak sepenuhnya mendapatkan jaminan datanya akan kembali. Di China, korban WannaCry di dominasi oleh pelajar. Banyak dari mereka yang kehilangan data seperti tugas sehari-hari hingga tugas akhir yang mengakibatkan tertundanya kelulusan (Soo, Ng, & Chen, 2017). Selain China, Amerika Serikat juga menjadi korban besar dalam penyerangan ini. Ransomware menginfeksi industri besar, FedEx, yang kemudian juga menjadi dampak ransomware NotPetya. Dalam mengatasi masalah ini FedEx mengalami dampak kerugian besar pada masalah finansial (Palmer, NotPetya cyber attack on TNT Express cost FedEx $300m, 2017). Hal ini juga terjadi di UK, tidak pada pelajar tetapi WannaCry menginfeksi sebanyak 81 *National Health Service* (NHS) yang mengakibatkan sejumlah rumah sakit harus melakukan pemindahan pasien darurat ke rumah sakit lainnya dan beberapa perangkat seperti MRI tidak bisa di operasikan (NAO Report, 2018, p. 11). Penyerangan WannaCry diketahui menyerang komputer yang tidak melakukan *patch* sistem keamanan terbaru yang diluncurkan oleh perusahaan Microsoft pada satu bulan sebelumnya. Virus ini kemudian menyebar dengan cepat antar komputer yang terhubung dengan satu jaringan. *National Health Service* (NHS) merupakan layanan perawatan medis dan kesehatan yang didanai pemerintah untuk semua orang yang tinggal di UK. NHS menjadi

layanan kesehatan yang terpercaya dan tersebar di banyak daerah. Hal ini menjadi krusial karena memberikan dampak bagi keberlangsungan masyarakat yang membutuhkan pelayanan kesehatan baik secara darurat dan yang sudah terjadwalkan.

Penyerangan siber pada perangkat komputer merupakan hal yang penting diperhatikan dan menarik untuk diteliti. Seiring dengan kemajuan ilmu pengetahuan saat ini, serangan berupa malware juga berkembang semakin kompleks dan tidak mudah diatasi. Kecanggihan teknologi meningkatkan kesadaran negara untuk meningkatkan keamanan siber (*cyber security*) sebagai keamanan negara. Penelitian mengenai siber dalam konteks keamanan nasional sudah banyak dilakukan oleh para peneliti terdahulu, tetapi pada penelitian ini penulis akan lebih meneliti mengenai tindakan sekuritisasi Inggris disaat terjadinya penyerangan siber WannaCry yang memberikan dampak besar pada organisasi pelayanan kesehatan NHS di Inggris.

1.2. Rumusan Masalah

1. Bagaimana analisis sekuritisasi pemerintah Inggris dalam kebijakan siber terkait insiden WannaCry pada tahun 2017?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

a. Mengetahui pentingnya melakukan keamanan siber sebagai bagian dari prioritas negara dalam mengamankan kepentingan di ruang maya yang memiliki pengaruh pada dunia nyata.
b. Mengetahui kebijakan perlindungan keamanan siber yang dimiliki oleh Inggris dan tindakan sekuritisasi pada saat kejadian penyerangan WannaCry.
c. Mengetahui dampak penyerangan siber WannaCry bagi *National Health Service* (NHS) di Inggris yang mempengaruhi keamanan negara bagi masyarakat.

1.4. Signifikansi

Signifikansi dari penelitian ini adalah:

Ketergantungan negara yang sangat besar terhadap jaringan sistem informasi telah memberikan perubahan signifikan pada sistem keamanan dunia. Hingga sekarang ini, penyerangan siber terus meningkatkan kerugian finansial dan meluas pada banyak sektor industri. Penyerangan siber WannaCry pada tahun 2017, membuktikan dengan terancamnya sektor pelayanan kesehatan memberikan peluang menjadi sasaran baru yang berpotensi menciptakan keadaan rasa tidak aman yang meluas bagi masyarakat. Penyerangan ini tidak menargetkan NHS sebagai target utama, tetapi dengan terjadinya penyerangan ini cukup membuka adanya kerentanan terhadap keamanan siber negara Inggris. Hasil penelitian ini diharapkan dapat melengkapi penelitian terdahulu mengenai peningkatan

keamanan siber untuk keamanan negara dengan memperkaya kajian terkait pentingnya peningkatan keamanan siber, terlebih perlunya peningkatan upaya keamana siber pada sektor pelayanan kesehatan sebagai bentuk perlindungan masyarakat. Penelitian terdahulu secara umum meneliti mengenai analisis baru mengenai arti keamanan dan mengkaji peran penting meningkatkan keamanan siber di sektor perlayanan kesehatan. Pada penelitian ini penulis akan lebih membahas mengenai tindakan sekuritisasi Inggris menggunakan tiga unit variabel berdasarkan teori sekuritisasi untuk menganalisis tindakan Inggris dalam mengatasi masalah penyerangan siber WannaCry yang sebagian besar berdampak pada *National Health Service* (NHS) di Inggris pada tahun 2017.

1.5. Cakupan Penelitian

Adapun cakupan penelitian ini adalah:

Penelitian ini akan fokus pada keselarasan dengan komitmen pemerintah UK yang telah dibangun pada tahun 2016, untuk menjadikan UK sebagai tempat paling aman untuk tinggal dan berbisnis secara online (Martin, 2016). Hal yang mendasari penulis untuk mengambil penelitian ini, karena adanya penyerangan WannaCry sebagai serangan siber terbesar yang mempengaruhi *National Health Service* (NHS) di Inggris pada tahun 2017. Dalam hal ini penulis akan melakukan pengumpulan data dari penelitian terdahulu, mulai dari tahun 2016 sebagai tahun pertama pada periode strategi keamanan siber UK yang diterapkan untuk lima tahun kedepan, hingga tahun 2020 yaitu tiga tahun setelah kejadian penyerangan WannaCry sehingga diperolehnya informasi dari berbagai sumber mengenai pasca kejadian. Penelitian ini juga akan lebih membahas mengenai kebijakan keamanan

siber serta respons Inggris terhadap penyerangan siber. Dampak terhadap penyerangan WannaCry dialami oleh ratusan negara lainnya, tetapi penelitian ini hanya berfokus pada negara Inggris dan *National Health Service* (NHS) sebagai salah satu sasaran yang merasakan dampak besar yang diakibatkan oleh penyerangan WannaCry.

1.6. Tinjauan Pustaka

Kesadaran atas pentingnya keamanan siber Inggris telah menetapkan keamanan siber sebagai salah satu empat prioritas utamanya sejak tahun 2010 lalu. Melalui jurnal yang ditulis oleh Savita Mohurle & Manisha Patil menjelaskan pentingnya kesadaran atas keamanan siber, dengan menganalisis apa yang dimaksud dengan ransomware, efeknya, dan beberapa tindakan pencegahan karena bentuk serangan yang merujuk mulai dari skala kecil seperti ancaman melalui surel hingga serangan skala besar yang dapat mempengaruhi politik dan perekonomian negara. (Mohurle & Patil, 2017)

Mengenai kondisi penyerangan siber yang terjadi pada NHS Inggris tahun 2017 lalu, sebuah jurnal penelitian yang ditulis oleh Maxwell Mago, Farai Fransisco Madyira memaparkan prespektifnya dari sudut pandang pendidikan teknologi terhadap penyerangan tersebut. Dalam jurnalnya menuliskan bahwa, serangan siber WannaCry telah menginfeksi lebih dari 230.000 dari 150 negara di dunia. Ia berargumen bahwa serangan ransomware merupakan fenomena yang mengkhawatirkan dan dapat mengifeksi ratusan ribu komputer diseluruh dunia, yang juga berdampak pada keamanan sistem teknologi jaringan individu dan bisnis.

Hal ini dapat terjadi akibat kurangnya perhatian individu dalam memperbarui sistem operasi perangkat komputer dan kurangnya edukasi terhadap pengguna atas bahaya mengunduh lampiran surel dan tautan dari pengirim tidak jelas dalam email yang mereka terima. (Mago & Madyira, 2018)

Selanjutnya dalam artikel yang disusun oleh Kristoffer Kjærgaard Christensen & Tobias Liebetrau menjelaskan mengenai sebuah serangan ransomware yang mengubah "dari situasi krusial yang ditangani oleh para pakar keamanan, menjadi simbol betapa pentingnya perlindungan keamanan siber secara mendasar dan gambaran yang sebenarnya dari yang dapat terjadi apabila sistem dan perangkat tidak memiliki pertahanan kuat". Kemudian ia juga menjelaskan, insiden penyerangan siber sudah tidak sepenuhnya selaras dengan politik dan demokrasi keamanan nasional tradisional, hal ini menunjukkan perlunya memperhatikan pembuatan keamanan publik karena tidak ditentukan melalui kewarganegaraan nasional sendiri tetapi juga dibentuk melalui interaksi dengan TIK dan perusahaan swasta. (Christensen & Liebetrau, 2019)

Kemudian dalam sebuah penelitian yang dilakukan oleh Ward Priestman, Tony Anstis, Isabel G Sebire, Shankar Sridharan dan Neil J Sebire, bahwa penyedia pelayanan kesehatan seringkali menerima surel yang dianggap mencurigakan yang akan menjadi sebuah ancaman. Data pasien memiliki nilai yang signifikan dan merupakan target potensial bagi para peretas pada baru-baru ini. Namun, pendidikan dan pelatihan staf layanan kesehatan terhadap kemanan siber dalam menghadapi ancaman penyerangan siber berbasis *phishing* dinilai masih kurang, hal ini menunjukkan membutuhkan penyebaran pengetahuan dan evaluasi yang berkelanjutan. (Priestman, Anstis, Sebire, Sridharan, & Sebire, 2019)

Artikel selanjutnya disusun oleh Dewi Triwahyuni dan Tine Agustin Wulandari, yang dalam penelitiannya menjelaskan upaya yang diambil oleh Amerika Serikat menanggapi kejadian penyerangan siber di Estonia tahun 2007. Melalui kejadian tersebut semakin mengokohkan kepentingan utama Amerika Serikat dalam membangun konsep strategi keamanan siber yang aman bagi masyarakat dan terjaganya keamanan komunikasi antar pemerintahan. Dengan beberapa upaya yang diambil oleh Amerika Serikat menunjukkan bahwa permasalahan penyerangan siber juga mejadi ancaman bagi komunikasi dan informasi antar pemerintahan sehingga membawa pengaruh pada pentingnya meningkatkan keamanan siber dinegara belahan dunia lainnya. (Triwahyuni & Wuladari, 2016)

Beberapa hasil penelitian di atas telah disampaikan mengenai keamanan siber di Inggris. Bebeda dengan tulisan-tulisan yang telah dipaparkan dalam tinjauan pustaka diatas, analisis dalam penelitian ini akan lebih membahas mengenai tindakan sekuritisasi Inggris dalam mengatasi permasalahan keamanan siber terhadap serangan siber WannaCry yang sebagian besar berdampak pada *National Health Service* (NHS) di Inggris tahun 2017.

1.7 Landasan Teori/Konsep/Model

Sesuai dengan masalah penyerangan siber yang terjadi di Inggris pada tahun 2017, penulis akan menggunakan teori sekuritisasi sebagai landasan teori yang akan menunjukkan upaya peningkatan keamanan dalam dunia siber di Inggris. Teori ini merupakan bagian dari *Copenhagen School* oleh Barry Buzan, Ole Wæver, dan

Jaap de Wilde (Stritzel, 2014, p. 11). Sekuritisasi dalam teori ini memiliki arti adanya ancaman isu eksistensial yang dijadikannya sebagai agenda keamanan. "Keamanan" merupakan suatu langkah yang dapat membawa politik melampaui aturan permainan secara umum dan dapat dilihat sebagai versi politisasi yang lebih ekstrem. (Buzan, Waever, & Wilde, Security: A new Framework for Analysis, 1998, p. 23). Keberhasilan tindakan sekuritisasi ini ditentukan oleh kemampuan sang aktor dalam mendapatkan persetujuan *audience* bahwa suatu tindakan sekuritisasi tersebut perlu dilakukan. (Buzan, Waever, & Wilde, Security: A new Framework for Analysis, 1998, p. 25)

Menurut Barry Buzan, Ole Wæver, dan Jaap de Wilde, dalam melakukan analisa terhadap studi keamanan tertadapat tiga tipe unit:

1. *Referent Objects*, sesuatu yang dilihat sebagai objek yang terancam dan mendapatkan klaim yang sah untuk mendapatkan perlindungan.
2. *Securitizing Actors*, merupakan aktor yang melakukan tindakan sekuritisasi terhadap suatu isu yang terancam keamanannya.
3. *Functional Actors*, aktor yang tidak harus bertindak seperti *Referent Objects* dan *Securitizing Actors* tetapi dapat mempengaruhi dinamika suatu sektor keamanan. (Buzan, Waever, & Wilde, Security: A new Framework for Analysis, 1998, p. 36)

Dalam penelitian ini, berdasarkan pemaparan di atas pihak organisasi dan individu merupakan *Referent Objects* atau sebagai pihak yang terancam, kemudian Pemerintah Inggris merupakan *Securitizing Actor* yang melakukan tindakan

sekuritisasi, dan pakar-pakar dalam bidang teknologi sebagai *Functional Actors* yang turut memberikan pengaruh pada sektor keamanan.

1.8. Metode Penelitian

1.8.1. Jenis Penelitian

Metode yang akan dilakukan dalam penelitian ini menggunakan metode penelitian kualitatif, dimana akan menggunakan susunan deskriptif analisis melalui data-data yang diolah dari referensi ilmiah, tinjauan literatur dan penelitian sejenis guna memberikan pemahaman yang mendalam terhadap proses penelitian serhingga akan menghasilkan hasil penelitian yang dapat dipahami dan relevan.

1.8.2. Subjek dan Objek Penelitian

Penulis akan menjadikan pemerintah Inggris sebagai subjek dari penelitian. Hal ini dikarenakan pemerintah Inggris merupakan aktor yang melakukan keamanan terhadap penyerangan WannaCry. Kemudian penulis akan menggunakan strategi dalam peningkatan keamanan siber yang dilakukan oleh Inggris menjadi objek penelitian. Hal ini dikarenakan Inggris merupakan negara yang memiliki peningkatan yang sangat signifikan dan dibuktikan sebagai urutan pertama dalam keamanan siber pasca terjadinya serangan siber WannaCry.

1.8.3. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan yaitu data sekunder. Data sekunder merupakan data yang diperoleh melalui berita isu yang sejenis, buku ilmu hubungan internasional, jurnal penelitian terdahulu, pernyataan resmi dari pemerintah, serta laporan berupa fakta dan literatur lainnya yang dapat digunakan

guna menunjang penelitian ini serta memberikan proses pemahaman yang mendalam. Sumber-sumber tersebut didapatkan melalui proses selektif melalui akses data pada alamat situs internet yang kredibilitasnya dapat dipercaya (Sugiyono, 2009).

1.8.4. Proses Penelitian

Proses pengumpulan data akan dilakukan dengan cara analisa dari sumber-sumber yang telah didapat baik website, jurnal atau kajian literatur yang didapati melalui proses seleksi dari sumber yang memiliki kredibilitas terpercaya. Penulis akan mendalami penelitian terdahulu untuk membantu menganalisa data yang dibutuhkan saat mengidentifikasi permasalahan. Kemudian hasil pemahaman dalam mengidentifikasi masalah dikelola untuk menghasilkan sebuah kesimpulan yang menjawab rumusan masalah penelitian.

BAB II

RESPONS DAN KEBIJAKAN PEMERINTAH INGGRIS DALAM KEAMANAN SIBER

Bab ini menjelaskan mengenai tindakan pemerintah Inggris dalam menangani kejadian serangan siber serta perkembangannya dalam meningkatkan keamanan sibernya setelah kejadian serangan ransomware WannaCry. Sub bab pertama akan membahas mengenai kebijakan Inggris dalam mengambil tindakan untuk memastikan keamanan dan perlindungan dalam dunia siber untuk melawan ancaman yang berpotensi mengganggu keamanan negara pada keamanan politik, ekonomi, dan militer. Sub bab kedua akan membahas mengenai respons secara umum oleh pemerintah Inggris dalam menangani kejadian serangan siber yang berkaitan dengan aplikasi dari pendekatan *"Four Ps"*. Sub bab ketiga akan membahas mengenai respons pemerintah Inggris terhadap serangan WannaCry yang mana kejadian tersebut memberikan dampak kerugian yang sangat besar dalam kurun waktu yang tidak cukup lama. Berangkat dari peristiwa tersebut, penyebab terjadinya NHS sebagai salah satu korban besar dari serangan siber WannaCry juga akan dibahas dalam sub bab ketiga ini.

2.1 Kebijakan Keamanan Siber Inggris

Peningkatan pesat pada bidang jaringan komputer, menjadikan keamanan siber sebagai salah satu prioritas seluruh negara dunia. Seiring dengan jumlah pengguna internet yang terus bertambah, serangan siber terus berkembang semakin luas dan membahayakan. Dalam mencapai tujuan dalam meningkatkan

keamanannya, Inggris memiliki visi untuk menjadi tempat yang aman dan tangguh terhadap ancaman dunia maya serta makmur dan percaya diri di dunia digital. Untuk mewujudkan visi tersebut makalah kebijakan telah diunggah melalui website resmi negara yang mencakup informasi terhadap strategi Inggris dalam keamanan siber melalui tiga tahapan, yaitu *Defend, Deter and Develop* sebagai strategi yang akan dilaksanakan pada periode 2016 - 2021 (HM Government, 2016).

2.1.1 Pertahanan (*Defend*)

Strategi pertama yang dilakukan ialah, *Defend*. Pada tahapan ini pemerintah melakukan pertahanan dengan cara bekerjasama dengan berbagai aktor. Mulai dari melakukan pertahanan bersama masyarakat, akademisi, pebisnis, lembaga pemerintah lainnya dan juga bekerja sama dengan negara lain sehingga dapat menciptakan lingkungan dunia siber yang lebih sejahtera. Pemerintah akan menyediakan langkah-langkah terbaik untuk masyarakat individu, bisnis, organisasi dan lembaga sektor publik maupun swasta agar dapat mengakses informasi yang tepat dalam melakukan pertahanan siber secara mandiri sekaligus sebagai langkah pemerintah untuk mempromosikan saran dan standar perlindungan keamanan siber (HM Government, 2016, p. 33).

Terdapat tiga bagian fokus dalam *Defend*. Pertama, yaitu fokus memperkuat jaringan melalui program *Active Cyber Defence* (ACD) dan membangun dunia siber yang lebih aman. Program ini mengacu pada analisis keamanan siber untuk mengembangkan pemahaman tentang ancaman terhadap jaringan, sehingga dapat merancang dan menegakkan prinsip langkah-langkah keamanan untuk mempersiapkan sistem yang lebih kuat terhadap serangan. Pendeketannya antara lain, pemerintah akan menjadi aktor utama dan juga memaksimalkan

perkembangan badan yang bersangkutan yaitu GCHQ, *Ministry of Defence,* dan NCA sekaligus bekerjasama pada industri khususnya *Communications Service Providers* (CSPs) yang memiliki pelayanan sangat berkaitan dalam membantu mengurangi kemungkinan serangan siber, seperti menangani *phising*, memblokir domain dan alamat IP yang berpotensi menyerang. Melalui program ini, pemerintah bertujuan untuk mempertebal keamanan dan menjadikan Inggris sebagai sasaran serangan siber yang tidak mudah untuk diretas. Dalam mencapai hal tersebut, Symantec menyatakan sektor – sektor besar memegang pengaruh besar pada individu, perekonomian dan masyarakat luas. Sehingga diperlukannya perlindungan lebih yang ditujukan keapada sektor tersebut untuk mengurangi resiko terjadinya bahaya yang mengancam negara. Hal ini juga mendukung bagaimana Inggris ingin menjadikan masa depan negaranya merupakan tempat yang sudah aman secara default dalam beraktifitas online (HM Government, 2016, pp. 33-34).

Kedua, yaitu melindungi pemerintah, infrastruktur kritikal nasional (CNI), dan sektor penting lainnya. Serangan dunia maya memberikan dampak yang dapat begitu mempengaruhi keamanan nasional suatu negara. Inggris memberikan fasilitas pelayanan online bagi masyarakat, dalam arti lain Inggris perlu menyediakan juga keamanan bagi data warga negara yang sudah tersimpan secara online. Penyerangan pada infrastruktur dan sektor penting lainnya memainkan peran kuat pada pengaruh terhadap stabilitas, perekonomian, dan reputasi Inggris di mata dunia internasional. Semakin berinovasinya teknologi, keamanan siber semakin menentukan bagaimana kemampuan suatu negara untuk dapat mengatasi permasalahan yang rumit. Maka dari itu, pendekatan yang dilakukan adalah peran

aktif pemerintah dalam memberikan pemahaman, saran, dan informasi terhadap ancaman sehingga para penerima mengetahui langkah untuk melindungi sistemnya secara mandiri pada saat waktu darurat. Pemerintah menyatakan bahwa permasalahan ini terjadi umumnya karena kecerobohan manusia, sehingga pemerintah akan memerhatikan langkah perkembangan peningkatan kesadaran atas pentingnya keterampilan dasar teknologi pada masyarakat (HM Government, 2016, p. 41).

Ketiga, yaitu pemerintah melakukan peningkatan kesadaran dalam perilaku publik dan bisnis serta mempelajari insiden dan ancaman yang sudah terjadi. Pembekalan terhadap kesadaran pentingnya keamanan siber pada publik menjadi salah satu dari cara yang optimal untuk mengurangi penyebaran resiko pernyerangan siber. Pada bisnis sendiri, pemerintah akan bekerja melalui organisasi yang dapat memberikan pengaruh terhadap perusahaan untuk memastikan mereka mengetahui dengan jelas terhadap berapa besar kerugian yang didapatkan apabila tidak mengelola keamanan dunia maya dengan baik. Di sisi lain, jumlah insiden dunia maya terus meningkat. Pengumpulan dan penyebaran informasi perlu dilakukan dengan dilengkapi pendekatan holistik terhadap insiden. Dalam hal ini kerjasama antara mitra sangat membantu dalam memberikan wawasan pada satu sama lain termasuk juga dalam membagi teknik mitigasi. (HM Government, 2016, p. 42 & 44)

2.1.2 Cegah (*Deter*)

Strategi kedua, yaitu *Deter*. Pada tahapan ini merupakan tahapan yang krusial mengingat semakin besarnya aktivitas pada dunia siber mengartikan perlunya keamanan yang sama pentingnya seperti di dunia nyata. Inggris berupaya

untuk meningkatkan keamanannya sehingga Inggris dapat menjadi salah satu negara yang paling sulit untuk dijadikan target penyerangan siber. Pengumpulan data di dunia siber dinilai lebih hemat biaya dari cara tradisional tetapi volume kemungkinan data tersebut dicuri juga sangat besar (CPNI, n.d.). Ketertarikan aktor luar yang ingin menyerang Inggris masih terus berlanjut, salah satu contohnya seperti kegiatan spionase yang kini sudah banyak dilakukan melalui dunia siber. Sehingga sebelum masuknya keadaan yang berpotensi sangat merusak, tahapan *deter* menjadi strategi yang begitu penting bagi Inggris dalam berupaya untuk meminimalkan kelemahan.

Dengan ini, Inggris mengejar pendekatan nasional yang komprehensif baik dalam menanggapi masalah yang terkecil hingga rumit dengan cara meningkatkan kemampuannya untuk mengidentifikasi lawan dan memiliki tindakan yang mampu menghalangi mereka (HM Government, 2016, p. 47). Penyampaian strategi pada makalah kebijakan ini juga sebagai salah satu sarana untuk memberi tahukan kepada pembaca bahwa Inggris memiliki kemampuan dan keseriusan dalam mengejar pelaku penyerangan yang terus menargetkan Inggris. Pemerintah bekerja sama secara khusus dengan lembaga penegak hukum untuk mengaplikasikan peran penting dalam mengejar pelaku yang melakukan penyerangan pada warga negara dan mengganggu jalannya kegiatan bisnis di Inggris. Intervensi dini juga dilakukan dengan cara memerhatikan pergerakan baik pada *deep web* dan mengawasi domain yang mencurigakan untuk mencegah munculnya bibit kriminalitas dan terorisme sehingga Inggris dapat memastikan angka ancaman dari dua golongan tersebut akan terus rendah untuk jangka waktu yang panjang. (HM Government, 2016, p. 48).

Pelaku yang tertangkap akan dilakukan identifikasi untuk membantu Inggris dalam membangun pemahaman mengenai model bisnis kejahatan di dunia maya dan negara akan bertindak untuk memastikan penyerangan tidak dapat dilakukan kembali oleh pihak tersebut. Pencegahan ini antara lain juga akan mengulik mengenai jaringan infrastruktur dan keuangan mereka sehingga akan membantu pemerintah menentukan langkah intervensi terbaik untuk mengganggu perkembangan pergerakan kelompok sejenis. Melalui *National Offensive Cyber Programme* (NOCP) akan dikembangkan kemampuan khusus untuk mendukung tindakan siber ofensif untuk meminimalkan peluang musuh melakukan penyerangan. Siber ofensif ini juga menjadi kemampuan yang dikembangkan pada kelompok angkatan bersenjata sebagai bagian dari operasi yang terintegrasi. Disisi lain, untuk melakukan pencegahan adanya informasi yang dicuri, negara juga menggunakan kemampuan kriptografi untuk melindungi informasi penting negara agar tetap aman disaat dikirimkan kepada pihak sekutu (HM Government, 2016, p. 51).

2.1.3 Kembangkan (*Develop*)

Strategi ketiga, yaitu *Develop*. Tahapan ini berfokuskan pada pengembangan kapabilitas sebagai salah satu fondasi pada strategi keamanan siber. Semenjak masuknya dunia pada era digital hingga masa yang akan datang, ahli pada bidang keamanan siber akan sangat dibutuhkan. Dunia siber yang terus berkembang dan berinovatif menghadirkan keadaan manusia yang semakin bergantung pada teknologi. Negara juga mengambil kesempatan untuk memanfaatkan teknologi untuk mempermudah berbagai pekerjaan. Dalam arti lain, dunia siber perlu dijaga keamanan dan kestabilannya. Inggris dalam menyusun langkahnya kedepan,

membangun pilar "*develop*" untuk memperkokoh keamanan siber dimasa yang akan datang.

Dalam strategi keamanan siber pada tahun 2016-2021, Inggris menyediakan berbagai fasilitas berupa pendidikan dan pelatihan untuk meningkatkan keterampilan tenaga kerja pada bidang keamanan siber. Program ini membuka peluang bagi siapapun yang ingin memulai dan memiliki ketertarikan pada bidang siber termasuk mencari bakat mulai dari anak-anak usia muda. Kegiatannya dapat berupa beasiswa, pelatihan melalui kursus yang dibimbing langsung oleh mentor, *summer-school,* dan lain sebagainya. Penawaran atas program ini sudah disediakan bagi anak-anak berusia 11 tahun. Fasilitas tersebut memiliki tujuan untuk dapat mempersiapkan generasi selanjutnya sebagai generasi yang ahli pada bidang ini. Pemerintah juga mendukung bagi para universitas yang memiliki pilihan jurusan keamanan siber dengan mengidentifikasi silabus untuk menghindari adanya kesenjangan sehingga dapat menciptakan lulusan ahli yang berkualitas dengan keterampilan yang holistik. Untuk memastikan dan mempertahankan kualitas, lowongan tenaga kerja pada bidang keamanan siber juga perlu ditingkatkan. Pemerintah akan mendorong pertumbuhan dibidang keamanan siber dengan meyakinkan bahwa Inggris merupakan penyedia keamanan siber dengan kualitas yang tinggi. Dalam mendukung perkembangan, pemerintah akan mempromosikan penelitian yang terus dilakukan untuk meningkatkan teknologi dan mengundang para ahli dengan kualitas pendidikan terbaik untuk dapat bergabung. Disisi lain untuk memperkokoh jalannya strategi, pemerintah akan melakukan perkembangan melalui *horizon scanning* yaitu menjelajahi rencana terhadap potensi yang akan datang pada masa depan yang sangat dimungkinkan memiliki keadaan yang

berbeda pada saat ini. Baik dalam peluang ataupun ancaman. (HM Government, 2016, pp. 55-61).

2.2 Respons Pemerintah Inggris Terhadap Serangan Siber

Bentuk serangan siber dapat terjadi dalam berbagai bentuk, seperti *malware, ransomware, phishing,* dan lain sebagainya. Setiap tahunnya *the UK Office for National Statistics* (ONS) merilis data serangan siber yang terjadi di Inggris. Pasca kejadian serangan WannaCry tahun 2017, Inggris berhasil mengalami penurunan angka serangan siber hingga 31% pada tahun 2018 (Henshaw, 2019). Seringkali motivasi dari penyerangan siber didasari dengan tujuan untuk meraih keuntungan finansial. Perkembangan Inggris dalam menggunakan siber sebagai bagian dalam membangun perekonomian negara, penting untuk memastikan pencegahan dan tindakan dalam menanggulangi segala bentuk penyerangan siber. Pelaku penyerangan siber tidak selalu dapat ditemukan dan dituntut dikarenakan mereka memiliki keahlian untuk menyembunyikan identitas. Bentuk penyerangan siber yang beragam dan jumlah terus meningkat, menjadi tantangan bagi penegakan hukum untuk menyediakan segala solusi. NCSC sebagai badan keamanan siber di Inggris bertanggung jawab untuk menyediakan strategi penindakan penyerangan siber. Secara umum, tindakan Inggris dalam menindaki penyerangan siber membutuhkan aplikasi dari pendekatan *"Four Ps"* yaitu, *Prevent, Pursue, Protect,* dan *Prepare* (Saunders, 2017, p. 2).

Penyerangan siber mengakibatkan kerugian yang variatif dan dapat terjadi kapan saja. Dalam tahap *prevent* atau pencegahan, pertemuan bilateral dan multilateral termasuk *Europol Joint Cybercrime Action Taskforce* (J-CAT), dan

Budapest Cybercrime Convention, setiap negara dunia secara sadar memiliki perhatian untuk mengetahui apa yang harus dilakukan untuk menangani kejahatan dunia maya di negaranya. Inggris berupaya untuk meningkatkan mitra kerjasama dan melakukan kolaborasi untuk pembangunan keamanan siber (Saunders, 2017, p. 8). Memiliki mitra kerjasama sangat membantu dalam menyusun materi penelitian terhadap insiden penyerangan siber yang kemudian akan sangat dibutuhkan untuk mendukung penelitian baru. Selain peningkatan dalam mitra, Inggris secara aktif melakukan identifikasi dan melakukan pencegahan dengan menyelidiki beberapa motif yang dinilai berpotensi sebagai bibit kegiatan eksperimental. Hal ini seringkali dilakukan oleh mereka yang masih berada diumur muda (Saunders, 2017, p. 6). Inggris menyadari perlunya kesadaran masyarakat atas bahayanya bentuk serangan siber perlu disampaikan dengan mengedukasi masyarakat secara menyeluruh. Dengan kesadaran masyarakat yang tinggi pendekatan yang terpenuhi tidak sekedar mencegah, melainkan memotivasi untuk menghasilkan para ilmuwan baru (*to prepare*). Pemerintah Inggris memfasilitasi bagi siapapun yang ingin memperdalami ilmu dalam bidang ini melalui penawaran pendidikan yang dapat dijumpai dibanyak universitas.

Dengan fondasi keamanan siber yang kuat, insiden akan tetap terjadi. Penyerangan siber dapat dialami oleh siapa saja, baik perusahaan besar, kecil, dan juga individu. Pendekatan kedua, *Pursue* atau mengejar, yaitu pelaku perlu ditindak dan dituntut sesuai hukum yang berlaku. Negara berperan dalam memimpin, dan mengoordinasi tindakan dalam upaya menyelesaikan penyerangan siber melalui *Strategic Governance Group* (SGG). Pengejaran pelaku serangan siber yang paling serius akan dilakukan dengan prioritas tertinggi dan dilakukan oleh spesialis

investigasi (NCA, 2015, p. 17). Setiap pengaduan yang masuk akan dipantau dan dibantu dengan mengindentifikasi pelaku.

Dari banyak kasus penyerangan siber di Inggris, dalam tahap *protect* atau melindungi, secara umum tahap pertama yang dilakukan ialah memberikan saran langkah mitigasi yang sesuai saat kejadian berlangsung. Contoh kasus terjadi pada pelanggaran yang dilakukan oleh Uber pada tahun 2016-2017 lalu, perusahaan aplikasi transportasi online, Uber terkena sanksi karena tuduhan pelanggaran data yang bocor. Informasi pribadi 57 juta pelanggan, termasuk nama, nomor telepon, nomor SIM (bagi pengemudi) dan informasi surel berhasil dicuri. Pemerintah Inggris menghimbau masyarakat untuk segera melaporkan apabila telah menjadi korban kejahatan dunia maya sehingga akan turut mendukung untuk mencegah bertambahnya korban. Selain itu, Inggris memberikan langkah mitigasi seperti hal yang harus dilakukan apabila menerima panggilan atau pesan yang masuk pada nomor telepon dan surel (NCSC, 2017). NCSC mendukung tindak lanjut terhadap investigasi secara transparan dan mengandalkan hubungan baik dengan industri maupun mitra pemerintah. Respons yang diberikan bagi perusahaan dalam rangka mencegah terjadinya penyerangan siber, NCSC memberikan peranan untuk mendukung setiap sektor publik dan privat dalam meningkatkan keamanan pelindungnya.

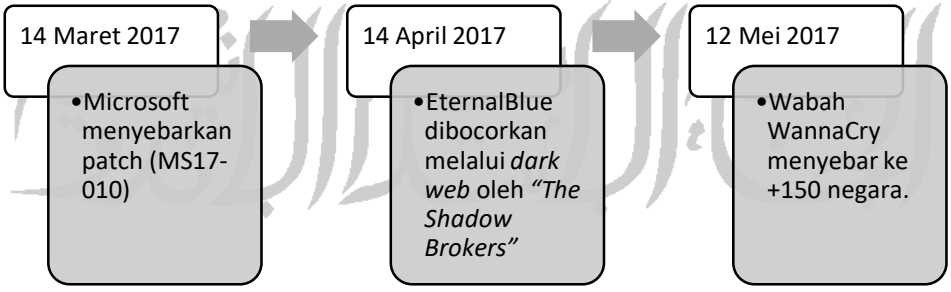
Tahap terakhir, yaitu *prepare,* Inggris menyebarkan keterampilan khusus dan mempersiapkan generasi yang profesional pada dunia maya melalui program unggulan yang disediakan oleh NCSC. Program yang disediakan dapat diikuti mulai dari anak-anak berusia 11 tahun melalui program yang bernamakan

CyberFirst. Program ini merupakan program beasiswa dengan kompetisi yang menarik sehingga dapat memberikan kesempatan bagi anak berusia 11-17 tahun untuk mengeksplorasi minat mereka terhadap teknologi dengan memperkenalkan dunia keamanan siber yang bergerak dengan cepat (NCSC, n.d.). NCSC menyediakan informasi lengkap melalui program yang ditawarkan untuk berbagai jenjang melalui websitenya. Selain itu, pemerintah berperan aktif untuk meningkatkan kesadaran siber melalui informasi yang disebarkan melalui website resmi. Informasi tersebut ditujukan mulai dari penggunaan individu, bisnis kecil, panduan belanja secara online dengan aman, dan panduan untuk melapor apabila menemukan pesan yang mengandung *phishing*.

2.3 Respons Pemerintah Inggris Terhadap Serangan WannaCry

Penyebaran virus pada dunia siber dapat melampaui batas negara dengan mudah. Virus WannaCry merupakan salah satu virus berbentuk ransomware yang mengunci data pada suatu perangkat dalam maksud untuk mendapatkan tebusan dari korban.

Bagan 1. Timeline kejadian*:*



(ENISA, 2017)

Dua bulan sebelum terjadinya penyerangan siber WannaCry, Windows telah menyebarkan pembaruan keamanan MS17-101 dikarenakan sudah terdeteksinya ada kebocoran EternalBlue, yaitu eksploit kit yang dikembangkan oleh NSA. Patch ini memperbaiki kerentanan atas resiko yang disebabkan oleh EternalBlue, tetapi pembaruan keamanan ini tidak segera diinstal pada sebagian besar perangkat komputer di NHS. Selain itu, pembaruan ini sudah tidak ditujukan lagi kepada sistem operasi Windows XP dan Windows 3000 dikarenakan masa *support* yang sudah berakhir. Sudah semenjak 8 April 2014 perusahaan windows merilis status masa pakai Windows XP sudah diberhentikan (Davey, 2020). Namun, di sisi lain sistem operasi Windows XP masih digunakan pada komputer di beberapa cabang NHS Inggris. *The Secretary of State for Health* telah memberikan peringatan untuk melakukan review terhadap keamanan siber untuk NHS sejak tahun 2016, tetapi belum ada tanggapan formal hingga Juli 2017 (NAO, 2018, p. 5).

Kemudian pada tanggal 12 Mei 2017, penyebaran virus ini telah berputar dengan cepat dan mempengaruhi 150 negara didunia. Inggris merupakan salah satu negara yang menerima dampak paling besar terhadap penyerangan ransomware WannaCry pada tahun 2017. Setidaknya terdapat 80 dari 236 NHS Inggris terinfeksi dan mengakibatkan situasi yang cukup darurat di saat kejadian berlangsung. Serangan ini tidak menargetkan NHS secara khusus, tetapi keadaan dari terdapatnya 88 NHS yang tidak lulus standar keamanan siber memberikan dampak NHS menjadi salah satu korban dalam skala besar (BBC, 2017).

Serangan ini secara langsung mempengaruhi akses pada data pasien dan juga beberapa fasilitas seperti MRI tidak dapat digunakan. Pada akhirnya pasien

darurat harus dipindahkan ke rumah sakit alternatif, kemudian terdapat 6.912 jadwal temu pasien termasuk jadwal operasi telah dibatalkan dan sekitar 19.000 jadwal lainnya juga terkena pengaruh akibat serangan ini (NAO, 2018, p. 8). Statistik keuangan menyatakan bahwa kejadian ini menyebabkan kerugian moneter NHS sekitar £20 juta. Selain itu setelah berhasil membersihkan ransomware ini dari server, NHS memerlukan £72 juta untuk melakukan peningkatan keamanan pada sistem teknologi informasinya (Goud, n.d.). Kejadian penyerangan ransomware ini menyerang siapa saja dengan kerugian yang setara, pemerintah melihat kejadian ini merupakan keadaan yang mendesak dan membutuhkan langkah keamanan.

Respons pemerintah Inggris saat kejadian mengambil langkah untuk segera merilis informasi resmi dan himbauan kepada setiap korban untuk tidak membayar tebusan tersebut. Hal ini dikarenakan tidak menjamin data akan kembali secara keseluruhan, di sisi lain, membayar tebusan sama saja dengan membiayai aktivitas kelompok kriminal (NCSC, 2017). Pemerintah juga memberikan himbauan kepada siapapun untuk melindungi keamanan perangkatnya dengan memperbarui sistem operasi atau windows yang digunakan, kemudian jalankan antivirus pada perangkat dan melakukan pindai file secara keseluruhan. Apabila perangkat tersebut sudah terlanjur terkena virus ransomware, saran awal yang diberikan ialah melakukan pemutusan jaringan pada internet sehingga virus tidak menyebar kepada perangkat yang terhubung dibawah satu jaringan. Untuk melindungi korban dari kemungkinan munculnya penipuan, NCSC menyarankan untuk tidak mencoba membawa perangkat ke ahli servis untuk melakukan dekripsi data yang sudah dienkripsi, dikarenakan hal tersebut hanya dapat dilakukan oleh pelaku penyerangan. NCSC bekerjasama dengan NHS Digital dan *National Crime Agency* (NCA) untuk

melakukan investigasi, dibantu juga dengan mitra internasional dan sektor komersial untuk memperhatikan kembali terhadap solusi dalam mengatasi ancaman seperti ini pada masa yang akan datang (NCSC, 2017).

Respons lainnya yang dilakukan semenjak kejadian adalah menyusun laporan "*Cyber Handbook*" yang diharapkan dapat membantu dalam mengambil tindakan terhadap kejadian serupa di masa yang akan datang. Laporan ini berisikan informasi terkait pendekatan dan tindakan yang diambil oleh NHS selama kejadian ini berlangsung. Beberapa pelatihan juga telah dilakukan untuk mempersiapkan para pekerja dan melengkapi skenario pada kemungkinan terjadinya serangan dengan tingkatan yang lebih rumit, seperti terjadinya beberapa kejadian di waktu bersamaan. Sebagai contoh, bom teroris dan serangan siber di waktu yang sama. Selama melakukan latihan tersebut, seluruh pelajaran didokumentasikan dan akan direvisi untuk proses *emergency preparedness, resilience and response* (EPRR) (NAO, 2018, p. 32).

Pentingnya peranan keamanan siber pada sektor pelayanan kesehatan menjadikan NHS England, NHS *Improvement*, dan NHS Digital semakin memperkuat hubungan dengan CareCERT yaitu layanan yang akan membantu memberikan saran dan panduan proaktif tentang ancaman digital pada seluruh organisasi kesehatan dan juga pada pekerja, mulai dari dokter, perawat garis depan hingga kepala eksekutif (UKAuthority, 2016). Dalam mempersiapkan keamanan pada masa yang akan mendatang, pemerintah juga memberikan perhatian pada pekerja untuk mengenal pentingnya keamanan siber termasuk dalam memberikan pelatihan dan pengembangan keterampilan (NAO, 2018, p. 29). Berbagai respon pemerintah dalam menangani serangan ransomware WannaCry membawa Inggris

semakin memformulasikan rencana yang signifikan dalam mendukung misinya pada peningkatan keamanan siber di Inggris.

BAB III

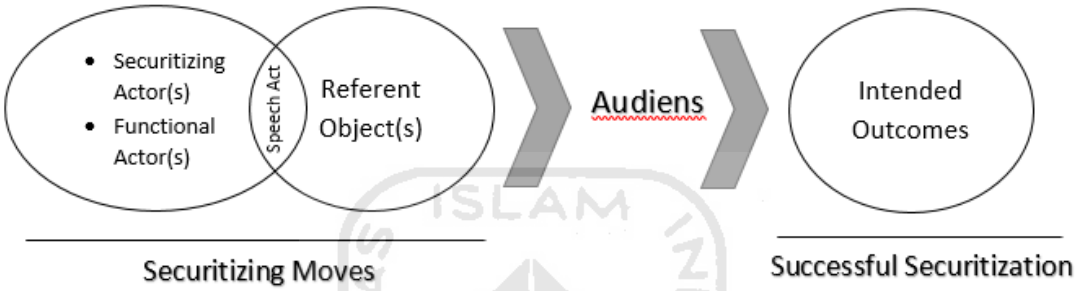
APLIKASI TEORI SEKURITISASI

Pada bab tiga ini, penulis akan memaparkan analisis mengenai pengambilan langkah sekuritisasi yang dilakukan oleh negara Inggris pada kasus penyerangan siber dengan menggunakan teori sekuritisasi yang merupakan bagian dari *Copenhagen School* oleh Barry Buzan, Ole Wæver, dan Jaap de Wilde. Bab sebelumnya telah menjelaskan mengenai strategi Inggris dalam membangun keamanan dunia siber di negaranya. Telah dipaparkan juga respons terhadap penyerangan siber secara umum maupun respons terhadap penyerangan siber WannaCry yaitu kasus yang memberikan dampak besar pada Inggris tahun 2017. Selanjutnya pada bab ini akan lebih menjelaskan mengenai aplikasi dari variabel yang terdapat pada teori sekuritisasi yaitu, untuk mengetahui sesuatu yang menjadi target ancaman *(referent objects)*, kemudian mengidentifikasi aktor yang mengambil langkah pada sekuritisasi *(securitizing actors)*, dan juga untuk mengetahui aktor diluar pemerintah yang juga berperan dalam memberikan pengaruh terhadap keamanan *(functional actors)*.

Dalam menjelaskan kaitan tiga variabel di atas dengan proses sekuritisasi, Barry Buzan, Ole Wæver, dan Jaap de Wilde menjelaskan mengenai peran aktor berupa *securitizing actors* dan *functional actors* yang sangat penting untuk mengidentifikasi dan mengamankan adanya *referent objects* atau masalah yang mengancam sebagai ancaman eksistensial. Tiga variabel tersebut membantu untuk melancarkan tindakan sekuritisasi dengan menyampaikan kepada audiens agar suatu masalah dapat dilihat sebagai masalah yang perlu tindakan keamanan. Kemudian setelah mendapatkan perhatian audiens, akan membantu untuk

masuknya ke tahap desekuritisasi, yakni keadaan yang sudah kembali normal dengan tercapainya keadaan hasil yang diinginkan (Buzan, Wæver, & de Wilde, Security: A new framework for analysis, 1998, pp. 24-26). Proses sekuritisasi dapat dilihat melalui bagan dibawah ini:

Bagan 2. Proses Sekuritisasi



Sumber: (Collins, 2005, p. 570)

Maka dari itu penjelasan lebih lanjut mengenai aplikasi dari variabel teori sekuritisasi akan dijabarkan pada tiga sub bab. Sub bab pertama akan membahas *referent objects* yaitu yang menjelaskan analisis untuk mengidentifikasi objek yang terancam dan memiliki legitimasi untuk dilindungi pada saat penyerangan siber WannaCry di Inggris. Pada sub bab kedua akan membahas mengenai *securitizing actors* yaitu aktor yang membuat tindakan terhadap sekuritisasi sehingga adanya peningkatan pada keamanan dan kesadaran masyarakat terhadap penyerangan siber. Kemudian pada sub bab ketiga akan membahas mengenai *functional actors*, yaitu menganalisis adanya aktor bukan pemerintah yang ahli pada bidang terkait dan bersedia bekerjasama dengan pemerintah dalam meningkatkan keamanan siber.

3.1 Referent Objects

Dalam teori sekuritisasi, mengidentifikasi *referent objects* merupakan salah satu hal penting dalam melakukan analisis terkait masalah keamanan. Perlunya mencari objek pada suatu masalah menjadi tahap awal untuk aktor dapat mengambil langkah keamanan terhadap suatu masalah. Secara definisi, *referent objects* adalah sesuatu yang berada dalam keadaan yang terancam dan memiliki klaim yang sah untuk mendapatkan perlindungan (Buzan, Wæver, & de Wilde, Security: A new framework for analysis, 1998). Dalam arti lain, untuk mengidentifikasi *referent objects* adalah keadaan yang merujuk pada pertanyaan *"security for whom?"* yang umumnya dapat berbentuk individu, negara, dan sistem internasional (Baldwin, 1997, p. 13). Spektrum *referent object* dapat dilihat secara lebih spesifik walaupun memang seringkali penyerangan sangat berkaitan erat dengan memberikan dampak pada kedaulatan negara, tetapi ancaman tidak selalu menjadikan negara sebagai target utama. Saat ini masalah siber telah menjadi isu dengan prioritas tinggi dikarenakan masalah siber dapat memberikan dampak yang sangat kompleks, antara lain dapat berdampak langsung pada sektor politik, ekonomi, militer, dan juga kemasyarakatan. Maka dari itu, *referent objects* memiliki jarak pandang yang luas sehingga perlu disesuaikan secara teliti dengan permasalahan yang terjadi.

Sesuatu yang dapat disebut sebagai *referent objects* adalah suatu masalah yang sangat berkaitan dengan komponen yang berasal dari kebutuhan dasar manusia dan memberikan pengaruh politik sehingga perlu dilakukannya tahapan keamanan. Dalam mengidentifikasikan *referent objects*, umumnnya dapat diketahui melalui pernyataan resmi yang dikeluarkan oleh pemerintah mengenai

permasalahan yang sedang terjadi. Walaupun begitu, identifikasi pada *referent objects* tidak selalu mudah untuk ditentukan. Pada kasus studi penyerangan siber, bentuk ancaman memberikan dampak yang beragam dan memiliki sifat yang konstelasi atau berhubungan (Hansen & Nissenbaum, 2009). Apabila pada umumnya *referent object* ditujukan pada negara, bangsa dan sistem internasional, di kasus penyerangan siber pemilihan *referent objecs* lebih ditujukan kepada wacana keamanan yang menyangkut ke keamanan privasi, keamanan publik, keamanan nasional dan daya saing perekonomian dikarenakan seringkali penyerangan siber mengancam *Critical National Infrastructure* (CNI) (Fouad, 2019, p. 636)

Keadaan yang menimpa organisasi NHS di Inggris disaat terjadinya penyerangan ransomware WannaCry menghadirkan hambatan bagi masyarakat dalam meng-akses layanan kesehatan memunculkan permasalahan yang juga berdampak pada masalah keuangan dan data privasi masyarakat yang terancam bocor. Melalui keadaan yang telah disebutkan diatas, pemerintah mengeluarkan pernyataan seperti dibawah ini:

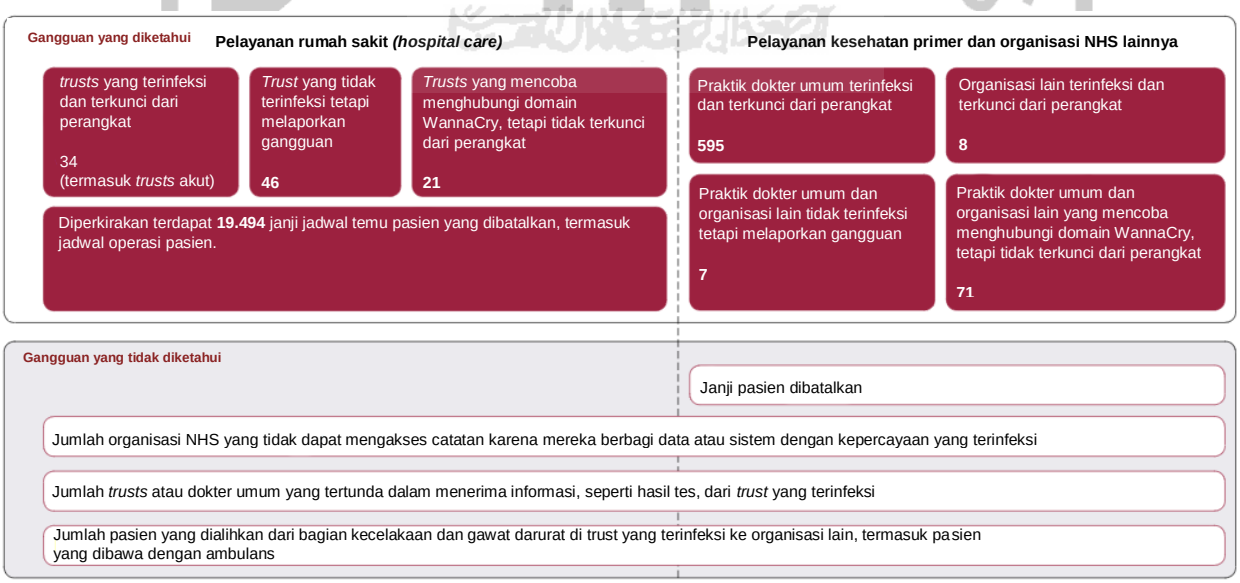
> "Today we have seen a set of global cyber-attacks against thousands of organisations and individuals in dozens of countries. [..] We are very aware that attacks on critical services such as the NHS have a massive impact on individuals and their families, and we are doing everything in our power to help them restore these vital services." – Ciaran Martin (NCSC, 2017)

Pernyataan di atas menjadi sarana penyampaian kepada masyarakat bahwa pemerintah sedang melakukan cara terbaik untuk melakukan tindakan keamanan

terhadap organisasi pelayanan penting masyarakat seperti NHS dan sebagian individu masyarakat. Penyerangan ransomware berpotensi menimbulkan kepanikan pada masyarakat akibat penguncian data yang tidak terjamin data-data tersebut akan kembali setelah adanya proses pemulihan. Hal tersebut cukup memberikan pengaruh politik yang mengganggu kesejahteraan masyarakat.

Dampak yang dirasakan oleh NHS memiliki pengaruh dan permasalahan yang lebih rumit. Penyerangan ini menyebar begitu cepat pada berbagai cabang NHS dan mengakibatkan masalah yang sangat berkaitkan dengan pemenuhan kebutuhan masyarakat luas. Hal ini menunjukkan permasalahan yang juga sudah menyentuh bagian perekonomian negara. Sehingga pemerintah menaruh perhatian khusus pada NHS. Dengan ini pemerintah merilis laporan investigasi yang menjelaskan dampak yang diterima NHS. Data tersebut dapat dilihat sebagai berikut:

Figur 1. Dampak WannaCry bagi NHS



Sumber: (NAO Report, 2018, p. 7)

Data yang tercantum pada Figur 1 membuktikan keadaan yang mendukung NHS sebagai salah satu organisasi yang dijadikan sebagai *referent object* pada penelitian ini. Hasil investigasi tersebut mengkategorikan gangguan yang berhasil diketahui dan gangguan yang tidak diketahui. Pada gangguan yang diketahui, bagian dari pelayanan rumah sakit mencatat terdapat ribuan pasien yang terhambat dalam mendapatkan pelayanan kesehatan, dari laporan investigasi tersebut juga menambahkan beberapa pasien darurat harus dipindahkan ke rumah sakit yang lebih jauh. Kemudian, pada bagian pelayanan kesehatan primer, ratusan dokter umum perangkatnya terkunci dan menghasilkan kendala baik pada mengakses data yang dibutuhkan seperti riwayat penyakit dan juga pembagian data yang dilakukan pada sistem. Disisi lain, infeksi penyerangan ransomware juga memberikan pengaruh besar pada departemen radiologi dan patologi sehingga tidak dapat beraktivitas secara normal. Hal ini dikarenakan penggunaan teknologi medis seperti penguji sampel darah dan pemeriksaan MRI tidak bisa digunakan dikarenakan perlu untuk dinonaktifkan sementara sebagai langkah awal untuk mencegah penyebaran virus ransomware tersebut (National Audit Office, 2018, p. 11). Langkah pencegahan dengan cara menonaktifkan beberapa perangkat pada sementara waktu, berpengaruh pada hasil pemeriksaan pasien yang prosesnya didapatkan melalui perangkat digital dan membutuhkan proses pembagian data melalui jaringan. Proses mitigasi penyerangan sangat berpengaruh pada aktivitas beberapa cabang pelayanan kesehatan NHS, dan memberikan pengaruh pada kelangsungan pasien.

Seperti yang disebutkan pada permasalahan di atas, masyarakat merasakan dampak langsung dari akibat terganggunya jalan pengobatan dan menghasilkan pembatalan janji temu. Walaupun data jumlah pasien yang dibatalkan dan data

lainnya yang tercantum pada figur 1 menunjukkan termasuk dalam kategori yang tidak diketahui, tetapi NHS tetap memiliki fokus pada upaya dan mempelajari hal yang telah terjadi untuk mengatasi masalah kedepannya.

Menanggapi kejadian ini, pemerintah telah mengumumkan klaim yang sah adanya perlindungan yang ditujukan untuk organisasi dan individu dikarenakan telah menjadi korban dan menerima dampak serius. Pada pernyataannya, individu juga menjadi *referent object* dikarenakan persebaran pada permasalahan penyerangan siber ini terjadi melalui jaringan internet sehingga menandakan bentuk ancaman yang dapat menyerang siapa saja. Penggunaan internet sangat beragam, begitu juga dengan dampak yang dihasilkan dapat memberikan masalah yang lebih besar dari perkiraan. Perhatian ini perlu disampaikan kepada audiens bahwa penyerangan WannaCry memberikan permasalahan serius dan mengancam baik individu dan organisasi, sehingga diperlukannya langkah sekuritisasi untuk memberhentikan laju penyebaran virus. Teknologi akan selalu berinovasi dan mengisi kekosongan untuk mempermudah berbagai aktivitas manusia, dalam arti lain aktivitas pada dunia siber memiliki kehidupan dan ancaman yang sama penting untuk diperhatikan seperti dunia nyata. Dengan ini kesadaran akan pentingnya menjaga keamanan dunia siber juga perlu ditingkatkan.

Penggunaan variabel *referent objects* pada penelitian akan memudahkan langkah *securitizing actors* untuk melakukan tindakan sekuritisasi baik dalam memberhentikan laju penyebaran virus, langkah mitigasi disaat terdampak, dan juga langkah pencegahan agar tidak terjadi kembali. Melihat dari dampak yang dialami oleh *referent objects*, analisa tersebut cukup menjelaskan mengenai

kejadian yang dialami sehingga memberikan lingkaran fokus pada langkah keamanan yang perlu dilakukan. Apabila masalah tidak diatasi secara efektif, maka akan memberikan celah bagi kelompok kriminal atau pelaku penyerangan untuk merumuskan rencana penyerangan dengan dampak yang lebih besar. Penyerangan siber dapat ditujukan kepada siapa saja, baik individu, pebisnis, dan negara. Namun, masalah penyerangan siber yang besar pasti akan mempengaruhi kesejahteraan negara, mengingat masyarakat pada saat ini sudah hidup secara beriringan dengan teknologi. Permasalahan pada insiden ini, menjadi awal pada catatan sejarah bahwa ransomware dapat mencakup penyerangan wilayah yang luas dan mengakibatkan implikasi serius baik pada individual dan organisasi. Dalam merumuskan penelitian terkait sekuritisasi, *referent object* membantu *securitizing actors* dalam menunjukkan langkah jelas mengenai siapa yang harus diamankan.

3.2 Securitizing Actors

Proses sekuritisasi membutuhkan kesadaran dan perhatian audiens atau masyarakat luas untuk membenarkan adanya ancaman sehingga dapat turut berpartisipasi untuk mengatasi ancaman tersebut. Dalam membantu penyampaian *speech act* kepada masyarakat dapat disampaikan melalui *securitizing actors* yang juga berperan sebagai aktor yang mendeklarasikan adanya isu keamanan dan merumuskan langkah perlindungan. Mengidentifikasi *securitizing actors* dapat diketahui melalui tindakannya yang merujuk pada *"It has to survive, therefore it is necessary to...."* atau dalam arti lain dapat dilihat melalui "siapa" yang mengumumkan adanya isu dan menjelaskan adanya tindakan untuk menyelesaikan masalah ini. Umumnya mereka adalah individu atau kelompok yang memiliki peran

besar pada negara, antara lain seperti pemimpin politik, birokrasi, pemerintah, dan lain-lain (Buzan, Wæver, & de Wilde, Security: A new framework for analysis, 1998, p. 36 & 40).

Pada permasalahan penyerangan WannaCry telah disinggung pada sub bab sebelumnya, pemerintah merupakan aktor yang mengeluarkan pernyataan terhadap adanya suatu isu yang mengancam keamanan dan juga mengumumkan bahwa pemerintah sedang melakukan tindakan untuk mengatasi penyerangan ini. Permasalahan penyerangan siber menjadi isu negara dan pemerintah merupakan aktor yang berbicara untuk kepentingan bangsa (Buzan, Wæver, & de Wilde, Security: A new framework for analysis, 1998, p. 41). Penyampaian ini dilakukan melalui organisasi pemerintah yang bekerja khusus menangani permasalahan siber, yaitu *National Cyber Security Centre* (NCSC). Ciaran Martin yaitu CEO dari NCSC mengeluarkan pernyataan resminya terkait isu penyerangan WannaCry dan menyampaikan tindakan keamanan sebagai perwakilan dari *Cabinet Office*. Mereka memberikan fasilitas berupa saran dan informasi bagi individu dan kelompok organisasi yang terdampak. Siapapun yang menjadi korban dapat melaporkan terkait kendalanya saat mengatasi masalah ini.

Dalam melakukan langkah keamanan, pemerintah Inggris melibatkan beberapa badan nasional dan lokal untuk berbagi tanggung jawab dan memperlancar tindakan dalam menyelesaikan kasus ini. Badan yang terlibat dapat dilihat melalui tabel dibawah ini.

Tabel 1. Tindakan Sekuritisasi yang Dilakukan oleh Badan Nasional

Badan Nasional		Tindakan Sekuritisasi
Cabinet Office	GCHQ	*Key guidance* diterbitkan oleh *National Cyber Security Service* (NCSC)
	NCSC	
	NCA	*National Crime Agency* (NCA) mendukung NCSC dalam memimpin tanggapan terhadap insiden keamanan siber besar di UK, termasuk penyelidikan kriminal.
	Home Office	

Sumber: (National Audit Office, 2018, p. 22)

Table 2. Tindakan Sekuritisasi yang Dilakukan oleh Badan Lokal

Badan Lokal		Tindakan Sekuritisasi
Department of Health	NHS England	Menghubungkan NHS dengan *department of health* terhadap informasi terkait keamanan siber dan bertanggung jawab untuk menanamkan standar keamanan siber di sektor pelayanan kesehatan.
	NHS Digital	Memiliki hubungan erat dengan NCSC untuk membantu para pekerja pelayanan kesehatan untuk memahami dan memberikan nasihat tentang persyaratan keamanan dunia siber terlebih dalam menanggapi insiden dunia maya.
	NHS Improvement	Mengawasi seluruh cabang NHS untuk mencapai kepastian telah melakukan peningkatan keamanan siber. NHS Improvement berkoordinasi dengan NHS England selama insiden penyerangan siber.
	Care Quality Comission	Memperhatikan keamanan data dan mengatur serta menilai keamanan perawatan pasien untuk menjamin kualitas layanan perawatan.

Sumber: (National Audit Office, 2018, p. 22 & 23)

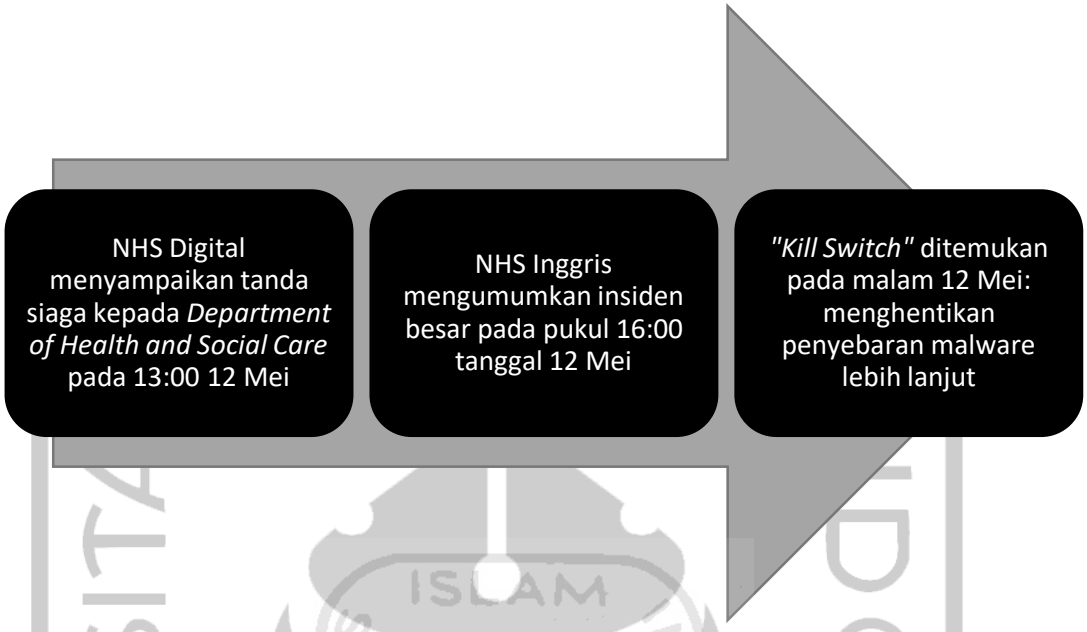
Dalam upaya pemerintah untuk meningkatkan keamanan siber dan mengatasi insiden penyerangan WannaCry, pemerintah memerlukan pembagian tanggung jawab yang diarahkan kepada badan nasional dan badan lokal yang bertujuan agar permasalahan dapat diatasi dengan efektif sesuai dengan cakupan lingkup masing-masing. *Cabinet Office* memiliki peran untuk memimpin kebijakan dan prinsip terhadap langkah penanganan yang dilakukan oleh badan yang terlibat melalui organisasi dibawah GCHQ yaitu NCSC badan yang khusus menangani masalah pada dunia siber. NCSC berperan untuk menerbitkan kunci petunjuk terhadap insiden dan memelihara keadaan dengan kebijakan *deter, defend, develop* yang merupakan langkah pemerintah pada strategi keamanan siber nasional 2016-2021 yang telah dirumuskan oleh pemerintah Inggris.

Adapun respons pemerintah yang telah dipaparkan sebelumnya pada bab dua, bahwa pada analisis ini tindakan sekuritisasi pemerintah juga menerapkan aplikasi dari pendekatan *Four Ps*. Penerapannya yakni, pada tahap *prevent* pemerintah merilis pernyataan resmi terkait adanya penyerangan virus WannaCry yang memberikan implikasi serius bagi NHS. Penyebaran informasi juga ditujukan pada organisasi NHS di seluruh cabang Britania Raya sehingga dapat mengambil langkah darurat untuk meminimalkan dampak serangan akibat WannaCry (Palmer, Hospitals across the UK hit by WannaCrypt ransomware cyberattack, systems knocked offline, 2017). Selanjutnya, pada tahap *protect* pemerintah segera merilis petunjuk bagi pengguna individu / rumahan, pebisnis kecil, organisasi besar, dan administrasi perusahaan berupa saran mitigasi tahap perlindungan mandiri disaat menghadapi insiden ini. Pemerintah sangat membuka laporan informasi dari siapapun terkait permasalahan, sehingga pada langkah *prepare* pemerintah

bekerjasama dengan badan terkait (termasuk non-pemerintah) untuk menyediakan langkah mitigasi terbaik kepada pihak-pihak yang mengalami kendala lebih besar dan juga untuk keamanan siber kedepannya (MalwareTech, 2017). Pada laporan investigasi yang dirilis oleh *National Audit Office* (NAO), lembaga NCSC berkerjasama dengan *National Crime Agency* (NCA) untuk mencari pelaku dibalik penyerangan ini. Pada tahap *pursue*, NCA melakukan pengumpulan data mengenai perangkat NHS yang terinfeksi dengan menyelidiki IP Address dan juga lalu lintas jaringan. Kemudian pada tanggal 27 oktober, menteri pertahanan Inggris, Ben Wallace menyatakan secara terbuka bahwa Korea Utara memiliki peran yang terlibat dalam insiden ini. Namun melalui pertimbangan serius pemerintah tidak memutuskan untuk melakukan langkah serangan balik melainkan memutuskan untuk meningkatkan keamanan sebagai langkah yang lebih aman bagi keselamatan warga negara Inggris (Withnall, 2017).

Kemudian *department of health* memiliki peran yang lebih memfokuskan untuk memimpin badan organisasi pelayanan kesehatan (badan lokal) dan menjadi penghubung kepada pihak pemerintahan. Kejadian ini memberikan pengaruh besar bagi sektor pelayanan kesehatan dikarenakan adanya celah sistem keamanan siber yang belum sesuai dengan standar keamanan. Kejadian pada hari pertama dapat dijelaskan sebagai berikut:

Bagan 2. Insiden Kronologi Hari Pertama



(Smart, 2018, p. 11)

Bagan ini menunjukkan kejadian yang terjadi selama kurang dari satu hari cukup memberikan pengaruh serius bagi organisasi NHS. Pergerakan dari jam 13.00 hingga 16.00 meningkatkan jumlah 16 organisasi (*trusts*) yang terinfeksi. Mereka segera melakukan konferensi EPRR nasional, dan merilis siber buletin pada seluruh NHS beserta penjelasan teknis mengenai ransomware dan saran tindakan terhadap insiden ini. Di hari yang sama, penyebaran malware berhasil diberhentikan tetapi kejadian ini cukup memberikan dampak pada aktivitas NHS hingga satu minggu kedepannya. Pemerintah berupaya agar sistem keamanan siber pada pelayanan kesehatan dapat ditingkatkan sehingga dapat meminimalisir dan mengatasi kejadian penyerangan siber yang akan datang. Selain itu, pemerintah akan membekali tenaga kerja pada keterampilan keamanan siber sehingga para pekerja dapat melakukan tindakan dengan bijak dalam melakukan mitigasi awal disaat terjadinya insiden penyerangan siber. Pembagian tanggung jawab pada badan

nasional dan badan lokal membantu pemerintah mencapai hasil yang diinginkan dalam tindakan sekuritisasi. Langkah di atas kemudian menjadikan pemerintah sebagai *securitizing actor*, yaitu aktor yang melakukan tindakan dengan tujuan untuk mengamankan *referent object* serta cukup dalam menarik perhatian audiens terhadap isu keamanan ini.

3.3 Functional Actors

Pada sub bab di atas telah dijabarkan adanya peran aktor yang melakukannya tindakan sekuritisasi. Dalam variabel ini, kompleksitas dalam menganalisis suatu isu keamanan akan dibantu dengan mendalami fokus aktor diluar *securitizing actors* yang perannya juga dapat mempengaruhi dinamika bidang keamanan. Aktornya dapat berupa organisasi non-pemerintah, akademisi, media, dan para ahli lainnya yang memiliki keterkaitan pada bidang yang dikaji (Eroukhmanoff, 2018). Peran *functional actors* tidak memiliki kekuatan yang sama seperti peran *securitizing actors* dalam mempengaruhi ranah politik, tetapi secara tidak langsung *functional actors* juga memiliki peran yang sama penting pada proses mengatasi masalah isu keamanan. Umumnya mereka tidak berniat untuk melakukan kegiatan yang bersifat politis ataupun menjadi penggerak dalam keamanan, tetapi kegiatan yang mereka lakukan memberikan pengaruh yang signifikan pada keputusan di bidang keamanan (Buzan, Wæver, & de Wilde, Security: A new framework for analysis, 1998, p. 36). Sehingga untuk melakukan identifikasi variabel ini, diperlukan untuk mendalami pengaruh aktor terkait dengan isu yang sedang dikaji.

Pada bidang keamanan siber, masalah penyerangan siber merupakan masalah yang luas dan tidak mudah untuk mengetahui penyebab serta pelaku yang melakukannya. Begitu juga dengan hal meningkatkan keamanan pada dunia siber, para ahli teknologi semakin berlomba-lomba dalam melakukan inovasi sehingga menghasilkan teknologi dan dunia siber sebagai sesuatu yang tidak bisa lepas dari masyarakat. Bertambahnya jumlah para ahli di bidang IT tidak menjadikan inovasi teknologi sebagai satu-satunya tujuan, tetapi juga menghadirkan pelaku berbahaya yang memiliki motif kejahatan. Badan pemerintah sebagai aktor utama membutuhkan berbagai data dan rancangan penelitian untuk melakukan tindakan sekuritisasi. Hal ini digunakan untuk mengukur probabilitas yang dapat membahayakan negara melalui serangan pada dunia siber dan juga menjadikan cara ini sebagai langkah yang mendukung pemerintah dalam merumuskan tindakan keamanan.

Melihat sejarah terjadinya penyerangan ransomware, virus WannaCry menjadi serangan yang paling memberikan dampak skala besar dan menyebar sangat cepat melalui jaringan yang terhubung. Terdapat 150 negara yang menjadi korban terhadap penyerangan ini, walaupun setiap negara mencoba yang terbaik untuk memberhentikan penyebaran virus tetapi keadaan aman dalam satu negara tidak mengartikan virus ini telah berhenti secara keseluruhan. Inggris sebagai salah satu dari negara yang memiliki peningkatan keamanan siber terbaik, tetap memiliki celah kelemahan dan ransomware mulai menginfeksi organisasi pelayanan publik kesehatan NHS di negaranya. Menyebarnya WannaCry ke sebagian besar cabang NHS, antara lain dikarenakan sistem operasi komputer yang masih menggunakan Windows 7. Satu bulan sebelum kejadian pihak perusahaan Microsoft telah

mendeteksi dan mengeluarkan buletin keamanan serta *patch* yang akan terunduh pada masing-masing perangkat disaat melakukan pembaruan sistem (Microsoft, 2017). Namun perangkat komputer pada sebagian besar organisasi NHS belum melakukan pembaharuan OS sehingga *patch* yang telah dirilis belum terinstall pada komputer sebagian besar NHS. NHS yakni organisasi pelayanan kesehatan yang tersebar di wilayah Britania Raya kemudian menjadi sasaran yang menerima dampak terbesar. Terdapat 80 dari 236 cabang NHS di Inggris mengalami hambatan melayani pasien. Masalah ini menjadi permasalah yang sangat serius dikarenakan sudah berada di tahap menghambat fasilitas pelayanan publik dan juga mempengaruhi perekonomian negara. Menanggapi kejadian tersebut, aktor-aktor yang terlibat tidak hanya berasal dari badan pemerintahan, melainkan mendatangkan *functional actors* yang juga memberikan pengaruh pada langkah sekuritisasi.

Marcus Hutchins, seorang peneliti keamanan komputer berwarga negara Inggris tidak sengaja menemukan kode *kill switch* pada ransomware ini. Diawali tanpa intensi untuk mengatasi permasalahan, perhatiannya semakin meningkat disaat mengetahui virus ini menyebar dengan cepat. Memiliki kesesuaian dengan bidang pekerjaannya, Marcus menunjukkan keberhasilannya dalam mengatasi masalah ini. Secara tidak langsung, aktor utama yang memberhentikan kejadian ini secara keseluruhan bukan dari badan pemerintah, melainkan seorang ahli dalam bidang penelitian keamanan komputer. Pemerintah mengakui kemampuan Marcus dalam menyelesaikan penyerangan besar ini. NCSC kemudian bekerja sama dengan Malware Tech, yaitu nama lain dari Marcus Hutchins untuk melengkapi data kronologi yang mana akan berguna pada langkah pemerintah untuk memperkuat

keamanan dan memberikan saran pada organisasi serta masyarakat luas dalam menyikapi insiden ini.

Pasca berhentinya penyebaran virus Wannacry, pemerintah menunjukkan keseriusannya dalam meningkatkan keamanan siber pada sektor pelayanan publik. Mereka mengambil langkah kesepakatan untuk bekerjasama antara *Department of Health* dengan perusahaan Microsoft untuk meningkatkan keamanan dengan memasang sistem operasi windows terbaru, yakni Windows 10 yang sudah memiliki tingkat keamanan yang jauh lebih baik (Microsoft Reporter, 2018). Melalui kejadian tersebut membuktikan bahwa pemerintah memerlukan perhatian lebih terhadap sektor publik maupun swasta mengenai keamanan sibernya. Penelitian dan kerjasama dengan berbagai ahli bidang IT merupakan hal yang perlu dilakukan untuk merumuskan kebijakan yang dapat membantu sektor publik dan swasta baik dalam mengatasi insiden serupa dan memperkokoh jaringan keamanannya. *Functional actors* pada bidang keamanan siber tidak dapat dipisahkan, masalah dunia siber merupakan masalah yang luas dan terus berinovasi dengan cepat sehingga peran *functional actors* sangat diperlukan baik dalam mendukung tindakan sekuritisasi dan untuk memperluas jangkauan penelitian.

BAB IV

KESIMPULAN DAN SARAN

4.1 Kesimpulan

Penyerangan siber WannaCry merupakan penyerangan yang menghasilkan sejarah baru bagi ancaman virus ransomware pada dunia siber. Penyebaran yang terjadi sangat cepat memberikan dampak pada 150 negara di dunia menjadi korban dari penyerangan ini. Inggris diketahui merupakan sebagai salah satu negara yang memiliki peningkatan keamanan siber dengan cepat dan telah menjadikan keamanan siber sebagai prioritas utama sejak tahun 2010, tetapi keadaan tersebut belum menjadikan Inggris sebagai negara yang aman terhadap penyerangan ini. Organisasi pelayanan kesehatan NHS yang tersebar di seluruh negara Britania Raya termasuk Inggris, menjadi korban yang menerima dampak terbesar dari penyerangan WannaCry. Penguncian data pada perangkat melumpuhkan beberapa aktivitas medis yang kegiatannya membutuhkan perangkat digital, terdapat 80 dari 236 NHS di Inggris berakibat tidak dapat menerima pasien darurat dan melakukan perubahan jadwal pada beberapa pasien. Penyebaran ransomware diketahui dapat di berhentikan pada hari yang sama disaat kejadian berlangsung, tetapi kejadian tersebut cukup memberikan dampak pada kegiatan NHS hingga satu minggu kedepan. Hal tersebut kemudian membawa penulis untuk mencari tahu lebih lanjut dan melakukan analisis terkait sekuritisasi yang dilakukan pemerintah Inggris dalam kebijakan siber terkait insiden penyerangan WannaCry 2017.

Dalam melakukan analisis pada topik ini, penulis telah mencantumkan data berupa respons pemerintah Inggris dalam keamanan siber yang tertulis pada BAB II. Kemudian untuk menjawab dari hasil penelitian tersebut, telah dipaparkan pada

BAB III mengenai bagaimana tindakan sekuritisasi yang dilakukan oleh Inggris dengan berlandaskan pada teori sekuritisasi. Menurut Buzan, Waever, & Wilde teori sekuritisasi memiliki arti adanya ancaman isu eksistensial yang dijadikannya sebagai agenda keamanan. Keadaan dunia siber saat ini sangat berkaitan dengan masyarakat dunia. Penyerangan yang terjadi pada dunia siber dapat memberikan dampak pada dunia nyata, sehingga penyerangan siber dapat menjadi masalah yang sangat rumit. Dalam menjelaskan tindakan sekuritisasi Inggris terhadap kejadian, penelitian ini terjawab melalui tiga aplikasi variabel dari *referent objects, securitizing actors* dan *functional actors.*

Pada kejadian ini, langkah awal dalam melakukan tindakan sekuritisasi pihak individu dan organisasi telah diidentifikasi sebagai *referent objects*. Pemerintah melalui pernyataan resmi telah mengumumkan klaim yang sah bahwa individu dan organisasi membutuhkan tindakan perlindungan. Ancaman penyerangan WannaCry tidak menargetkan pihak spesifik tetapi secara tidak langsung individu dan organisasi yang memiliki keamanan siber yang lemah menjadi target dalam penyerangan ini. Penyerangan yang terjadi tanpa melihat batas negara, menjadikan perhatian bersama bahwa kejadian ini dapat memberikan dampak yang lebih besar apabila tidak diatasi secara efektif.

Mengidentifikasi *referent objects* menjadi langkah penting bagi *securitizing actors* untuk melakukan tindakan sekuritisasi. Pernyataan resmi yang dikeluarkan pemerintah, menjadikan pemerintah sekaligus sebagai *securitizing actors* dikarenakan dalam pernyataannya menunjukkan ia sebagai aktor yang melakukan tindakan sekuritisasi. Pemerintah melibatkan badan nasional dan badan lokal agar dapat mengatasi permasalahan secara efektif melalui cakupan yang sesuai pada

bidang masing-masing. Penjelasan tindakan sekuritisasi yang dilakukan oleh badan lokal dan badan nasional dapat dilihat di **Tabel 1 & Tabel 2.** Tindakan tersebut memiliki kesesuaian dengan kebijakan *Defend, Deter, Develop* yang telah dirumuskan oleh pemerintah Inggris sebagai strategi yang akan dilakukan pada tahun 2016-2021.

Penyerangan siber merupakan masalah yang luas, sehingga untuk mencapai tindakan sekuritisasi yang efektif *functional actors* juga turut memberikan kontribusi dalam mempengaruhi tindakan sekuritisasi. Aplikasi dari variabel ini menunjukkan, Marcus Hutchins dan perusahaan Microsoft merupakan aktor non-pemerintah yang membantu jalannya sekuritisasi. Kontribusi Marcus dalam menemukan *"kill switch"* menjadikannya pahlawan yang memberhentikan penyebaran virus di seluruh dunia. Pemerintah sebagai *securitizing actors* kemudian menekan kerjasama dengan Marcus untuk mendiskusikan hal terkait insiden ini. Selain itu, penggunaan sistem operasi Windows pada perangkat organisasi NHS yang diluncurkan oleh Microsoft, menjadikan perusahaan Microsoft juga sebagai *functional actors*. Mempelajari dari insiden ini, pemerintah juga menekan kerjasama dengan Microsoft untuk meningkatkan keamanan siber pada organisasi pelayanan kesehatan NHS. Langkah keamanan yang akan dilakukan oleh Microsoft adalah dengan melakukan instalasi OS Windows versi terbaru yang memiliki tingkat keamanan lebih tinggi.

Permasalahan keamanan siber saat ini sangat memberikan keterkaitan erat dengan keadaan di dunia nyata. Dalam arti lain keamanan dunia siber perlu dijadikan prioritas dan permasalahan yang terjadi perlu diatasi dengan efektif. Sehingga melalui analisis dari aplikasi tiga variabel teori sekuritisasi membantu

penulis dalam menjawab rumusan masalah terkait tindakan yang dilakukan Inggris terhadap insiden penyerangan WannaCry 2017.

4.2 Rekomendasi/Saran

Hasil dari riset yang telah dilakukan penulis tentunya masih memiliki keterbatasan, adanya saran dan rekomendasi diharapkan dapat membantu penelitian selanjutnya untuk memperkaya terkait kajian tema serupa. Penelitian ini memiliki fokus pada langkah sekuritisasi Inggris terhadap kejadian WannaCry. Penulis sempat menyinggung bahwa tahap *pursue* yang dilakukan sebagai respons dari pemerintah Inggris ia menemukan Korea Utara merupakan pihak yang berada di balik penyerangan ini. Britania Raya dengan Amerika Serikat telah mengumumkan secara terbuka tetapi Korea Utara tampak membantah pernyataan tersebut. Kemudian ini meningkatkan perhatian Inggris terhadap ancaman dari tindakan Korea Utara dan menghubungkan dengan penyerangan WannaCry. Sehingga apabila dikaji lebih lanjut, pembahasan yang berfokuskan pada analisis penggunaan penyerangan siber untuk menekan ancaman pada negara lain *(cyber warfare)* dapat menjadi topik pembahasan yang menarik, mengingat melalui kejadian penyerangan WannaCry pelaku cukup berhasil menyoroti kerentanan keamanan siber Inggris di beberapa bidang. Pada penelitian selanjutnya dapat meneliti kasus WannaCry lebih dalam sehingga dapat menemukan dampak yang juga dirasakan pada negara selain Inggris sebagai contoh penyerangan ransomware yang memberikan dampak skala besar pada *Critical National Infrastructure* (CNI) suatu negara.

DAFTAR PUSTAKA

Baldwin, D. (1997). The concept of security. *Review of International Studies (1997), 23.*, 5–26.

BBC. (2017, October 27). *NHS 'could have prevented' WannaCry ransomware attack*. Retrieved from BBC News: https://www.bbc.com/news/technology-41753022#:~:text=More%20than%20a%20third%20of,and%20praised%20the%20staff%20response.

Bissell, K., & Ponemon, L. (2019). *The Cost of Cyber Crime. NINTH ANNUAL COST OF CYBERCRIME STUDY: UNLOCKING THE VALUE OF IMPROVED CYBERSECURITY PROTECTION.* USA: Accenture Security.

Burchil, S. (2005). *Theory of International Relations.* Houndmills: MACMILLAN.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis.* Covent Garden, London: Lynne Rienner Publishers, Inc.

Capling, A. (2008). *Twenty Years Australia Engagement with Asia.* Australia: The Pacific Review.

Christensen, K. K., & Liebetrau, T. (2019). A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry,. *Intelligence and National Security*, 396.

Church, P. (2009). *History of Southeast Asia.* Singapore: John Willey & Sons (Asia) Pte Ltd.

Collins, A. (2005). Securitization, Frankenstein's Monsterand Malaysian education. *The Pacific Review,Vol. 18 No. 4 December 2005*, 570.

CPNI. (n.d.). *Espionage*. Retrieved from Cenre for the Protection of National Infrastructure: https://www.cpni.gov.uk/espionage

Davey, W. (2020, September 30). *Are old operating systems putting the NHS at risk in 2020?* Retrieved from Digital Health: https://www.digitalhealth.net/2020/09/are-old-operating-systems-putting-the-nhs-at-risk-in-2020/

ENISA. (2017, May 15). *WannaCry Ransomware Outburst*. Retrieved from European Union Agency for Cybersecurity (ENISA) : https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

Eroukhmanoff, C. (2018, January 14). *Securitisation Theory: An Introduction*. Retrieved from E-International Relations: https://www.e-ir.info/2018/01/14/securitisation-theory-an-introduction/

Fouad, N. S. (2019). The Peculiarities of Securitising Cyberspace: A Multi-Actor Analysis of the Construction of Cyber Threats in the US (2003-2016). *University of Sussex, Brighton, UK*, 633-640.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly, Vol. 53, No. 4 (Dec., 2009), pp. 1155-1175*, 1163.

Haris, H. (2010). *Metodologi Penelitian Kualitatif untuk Ilmu-Ilmu Sosial.* Jakarta: Salemba Humanika.

Henshaw, S. (2019, Desember 30). *Cybercrime Statistics 2020: An In Depth Look at UK Figures and Trends*. Retrieved from Tiger Mobiles: https://www.tigermobiles.com/blog/cybercrime-statistics/

HM Government. (2016). *NATIONAL CYBER SECURITY STRATEGY 2016-2021.* United Kingdom: HM Government.

House of Parliament. (2011, September). *Post Note: Cyber Security in the UK.* Retrieved from House of Parliament. Parliamentary of Science and Technology: https://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf

ITUPublications. (2019). *Global Cyberscurity Index 2018*. Retrieved from International Telecommunication Union (ITU): https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

Jati, W. R. (2016). CYBERSPACE, INTERNET, DAN RUANG PUBLIK BARU: AKTIVISME ONLINE POLITIK KELAS MENENGAH INDONESIA. *Jurnal Pemikiran Sosiologi Vol. 3 No. 1 Januari 2016*, 2.

Kardaş, T., & Balci, A. (2012, April 1). *The Changing Dynamics of Turkey's Relations with Israel: An Analysis of 'Securitization'.* Retrieved from Insight Turkey: https://www.insightturkey.com/articles/the-changing-dynamics-of-turkeys-relations-with-israel-an-analysis-of-securitization

Lyke, B. (2016). *Does Trade Openess Matter for Economics Growth in CEE Countries?* Muenchen: Deakin University.

Mago, M., & Madyira, F. F. (2018). Ransomware Software: Case of WannaCry. *International Research Journal of Advanced Engineering and Science*, 260.

MalwareTech. (2017, May 13). *Finding the kill switch to stop the spread of ransomware*. Retrieved from National Cyber Security Centre: https://www.ncsc.gov.uk/blog-post/finding-kill-switch-stop-spread-ransomware-0

McQuail, D. (1983). *Mass Communication Theory.* Retrieved from http://docshare04.docshare.tips/files/28943/289430369.pdf

Microsoft. (2017, Maret 15). *MS17-010: Security update for Windows SMB Server: March 14, 2017*. Retrieved from Microsoft Support: https://support.microsoft.com/en-us/help/4013389/title

Microsoft Reporter. (2018, April 28). *Department of Health agrees Windows 10 security deal with Microsoft*. Retrieved from Microsoft News Centre UK: https://news.microsoft.com/en-gb/2018/04/28/department-of-health-and-social-care-agrees-windows-10-security-deal-with-microsoft/

Mohurle, S., & Patil, M. (2017, May-June). A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*, Volume 8, No. 5. Retrieved from International Journal of Advanced Research in Computer Science.

National Audit Office. (2018). *Investigation: WannaCry cyber attack and the NHS .* London: the Comptroller and Auditor General.

NATO Stratcom. (n.d.). *2007 Cyber Attacks on Estonia*. Retrieved from NATO Strategic Communications Centre of Excellence on Messenger: https://www.stratcomcoe.org/download/file/fid/80772

NCA. (2015, August). *The NCA Commitment to Working in Partnership with UK Operational Partners.* Retrieved from National Crime Agency: www.nationalcrimeagency.gov.uk

NCSC. (2017, May 13). *Latest Statement on International Ransomware Cyber Attack*. Retrieved from National Cyber Security Centre: https://www.ncsc.gov.uk/news/latest-statement-international-ransomware-cyber-attack-0

NCSC. (2017, november 23). *National Cyber Security Centre - News*. Retrieved from NCSC response to Uber data breach: https://www.ncsc.gov.uk/news/ncsc-response-uber-data-breach

NCSC. (2017, May 16). *Ransomware: 'WannaCry' guidance for home users and small businesses*. Retrieved from NCSC: https://www.ncsc.gov.uk/guidance/WannaCry-guidance-for-home-users-and-small-businesses

NCSC. (n.d.). *Education & Skills.* Retrieved from 11 - 19 years old (CyberFirst): https://www.ncsc.gov.uk/section/education-skills/11-19-year-olds

Palmer, D. (2017, May 12). *Hospitals across the UK hit by WannaCrypt ransomware cyberattack, systems knocked offline*. Retrieved from ZDNet: https://www.zdnet.com/article/hospitals-across-england-hit-by-cyber-attack-systems-knocked-offline/

Palmer, D. (2017, September 20). *NotPetya cyber attack on TNT Express cost FedEx $300m*. Retrieved from ZDNet: https://www.zdnet.com/article/notpetya-cyber-attack-on-tnt-express-cost-fedex-300m/

Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: threats, mitigation and approaches. *BMJ Health & Care Informatics Journal*.

Sadiaa M., J. R. (2014). *The Oxford Handbook of The International Relations of Asia.* London: Oxford University Press.

Satter, R. (2015, February 24). *Bank Hackers Steal Millions via Malware*. Retrieved from The New York Times: https://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html

Saunders, J. (2017). Tackling cybercrime – the UK response. *Journal ofCyber Policy*, 2.

Smart, W. (2018). *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: February.

Soewardi, B. A. (2013, Maret). *Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia.* Retrieved from Ditjen Pothan Kemhan: https://www.kemhan.go.id/pothan/wp-content/uploads/migrasi/admin/Cyber%20Defence.pdf

Soo, Z., Ng, N., & Chen, S. (2017, May` 15). *Tens of thousands of Chinese firms, institutes affected in WannaCry global cyberattack*. Retrieved from South China Morning Post: https://www.scmp.com/news/china/policies-politics/article/2094377/tens-thousands-chinese-firms-institutes-affected

Stritzel, H. (2014). *Securitization Theory and the Copenhagen School.* London: Palgrave Macmillan.

Sugiyono. (2009). *Metode Penelitian Kuantitatif, Kualitatif dan R&D. .* Bandung: CV Alfabeta.

Tabansky, L. (2012). Cybercrime: A National Security Issue? *Military and Strategic Affairs*, 119.

Triwahyuni, D., & Wuladari, T. A. (2016). STRATEGI KEAMANAN CYBER AMERIKA SERIKAT. *Jurnal Ilmu Politik dan Komunikasi*.

UKAuthority. (2016, September 09). *NHS Digital expands CareCERT cyber security services.* Retrieved from UK Authority: https://www.ukauthority.com/articles/nhs-digital-expands-carecert-cyber-security-services/

Wang, V. W.-C. (2006). China Economic Statecraft Toward Southeast Asia Free Trade Agreement and "Peacefull Rise". *American Journal of Chinese Studies*, 5-34.

Withnall, A. (2017, October 27). *British security minister says North Korea was behind WannaCry hack on NHS*. Retrieved from INDEPENDENT: https://www.independent.co.uk/news/uk/home-news/wannacry-malware-hack-nhs-report-cybercrime-north-korea-uk-ben-wallace-a8022491.html