SKRIPSI

KERJA SAMA INDONESIA DAN INGGRIS DALAM BIDANG KEAMANAN SIBER (2018)

MUHAMMAD SYAHRUL ENDY BAHARSYAH
1710521014

PROGRAM STUDI ILMU HUBUNGAN INTERNASIONAL
FAKULTAS EKONOMI DAN ILMU-ILMU SOSIAL
UNIVERSITAS FAJAR
MAKASSAR
2022

SKRIPSI

KERJA SAMA INDONESIA DAN INGGRIS DALAM BIDANG KEAMANAN SIBER (2018)

MUHAMMAD SYAHRUL ENDY BAHARSYAH
1710521014

PROGRAM STUDI ILMU HUBUNGAN INTERNASIONAL
FAKULTAS EKONOMI DAN ILMU-ILMU SOSIAL
UNIVERSITAS FAJAR
MAKASSAR
2022

SKRIPSI

KERJASAMA INDONESIA DAN INGGRIS DALAM BIDANG KEAMANAN SIBER (2018)

disusun dan diajukan oleh

MUHAMMAD SYAHRUL ENDY BAHARSYAH
1710521014

telah dipertahankan dalam sidang ujian skripsi
pada tanggal **17 Februari 2022** dan
dinyatakan telah memenuhi syarat kelulusan

Menyetujui,
Dewan Penguji,

No.	Nama Penguji	Jabatan	Tanda Tangan
1.	Andi Meganingratna, S.IP., M.Si. NIDN: 0931108002	Ketua	1.
2.	Achmad, S.IP., M.Si. NIDN: 0919047402	Sekretaris	2.
3.	Kardina, S.IP., M.A. NIDN: 0922068103	Anggota	3.
4.	Dr. Syamsul Asri, S.IP., M.Fil.I. NIDN: 0926028502	Anggota	4.

Ketua Program Studi Ilmu Hubungan Internasional
Fakultas Ekonomi dan Ilmu-ilmu Sosial
Universitas Fajar

Andi Meganingratna, S.IP., M.Si.
NIDN: 0931108002

PERNYATAAN KEASLIAN

Saya yang bertanda tangan di bawah ini :

Nama : Muhammad Syahrul Endy Baharsyah

NIM : 1710521014

Program Studi : Ilmu Hubungan Internasional

Dengan ini menyatakan yang sebenar-benarnya bahwa skripsi yang berjudul **"KERJA SAMA INDONESIA DAN INGGRIS DALAM BIDANG KEAMANAN SIBER (2018)"** adalah karya ilmiah saya sendiri dan sepenjang pengetahuan saya di dalam naskah skripsi ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila dikemudian hari ternyata didalam naskah skripsi ini dapat dibuktikan terdapat unsur-unsur plagiasi, saya bersedia menerima sanksi atas perbuatan tersebut dan diproses sesuai dengan peraturan perundang-undangan yang berlaku (UU. No. 20 Tahun 2003, pasal 25 ayat 2 dan pasal 70)

Makassar, 05 Mei 2023

Yang membuat pernyataan,

Muhammad Syahrul Endy Baharsyah

PRAKATA

Puji syukur penulis panjatkan kepada Allah SWT yang telah melimpahkan rahmat, hidayah serta karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini. Penyusunan skripsi ini bertujuan untuk memenuhi sebagian persyaratan guna memperoleh gelar Sarjana Ilmu Hubungan Internasional.

Penulis menyadari bahwa dalam penyusunan skripsi ini tidak lepas dari adanya kerjasama dan bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini perkenankanlah penulis mengucapkan terima kasih kepada :

1. Dr. Muliyadi Hamid, S.E., M.Si selaku Rektor Universitas Fajar Makassar.
2. Dr. Yusmanizar, S.Sos., M.I.Kom selaku Dekan Fakultas Ekonomi dan Ilmu-ilmu Sosial.
3. Ibu Andi Meganingratna, S.IP., M.Si selaku Ketua Program Studi Ilmu Hubungan Internasional Universitas Fajar sekaligus penasihat akademik penulis dan pembimbing skripsi yang selalu memberikan banyak masukan, mendukung, memberikan semangat dan afirmasi positif serta sabar menghadapi penulis dengan segala spekulasi penundaan revisi.
4. Dosen-dosen Program Studi Ilmu Hubungan Internasional Universitas Fajar; Bapak Achmad, S.IP., M.Si, Bapak Dede Rohman, S.IP., M.Si, Ibu Kardina, S.IP., M.A., Ibu Adelita Lubis, S.Sos., M.A., dan seluruh dosen yang tak bisa penulis sebutkan satu persatu. Terima kasih Bapak dan Ibu atas ilmu berharga yang telah diberikan selama 8 semester ini.

Terima Kasih pula untuk :

1. Orang tua penulis atas cinta dan semangat yang diberikan kepada penulis. Tak henti-hentinya selalu mendukung secara materi maupun non materi setiap keinginan yang dilakukan penulis dan mendoakan setiap langkah penulis. Walaupun tak seatap, kasih sayang kalian tak pernah putus. Untuk Mami yang sangat sabar dan kuat terima kasih telah mengajarkan arti kehidupan yang sebenarnya. Untuk Ayah yang sangat tegas terima kasih selalu berusaha memenuhi kebutuhan penulis. Skripsi ini untuk kalian berdua yang merupakan usaha awal penulis untuk membahagiakan kalian berdua
2. Keluarga lainnya dikala berkesempatan berkunjung ke Makassar tak lupa memberi pesangon buat tambah uang jajan.
3. Saudara-saudaraku yang juga selalu mendukung penulis untuk segera menyelesaikan kuliahnya.
4. Sahabatku semasa sekolah Salsabila dan Fadil walaupun dengan kesibukan masing-masing, tidak pernah lupa untuk menyempatkan berkumpul dadakan sambil bergibah hehehe.
5. Sodaraku Fio leko, semasa penulis di awal semester, satu-satunya teman yang 1x24 jam bersama, satu-satunya teman yang bisa diandalkan dikala butuh pertolongan. Satu-satunya teman yang tahu dan paham betul bagaimana proses jatuh dan bangkitnya kehidupan penulis.

6. Sahabat penulis yang dipersatukan sejak semester 2 sejalan dengan visi misi berproses di organisasi. Yuda dengan sapaannya
7. Haidir, teman penulis tapi serasa bapak. Rumahnya menjadi rumah kedua penulis. Pribadinya yang pembawaannya memang lebih dewasa dan memperlakukan penulis dengan hal-hal baik dan manis wkwk. Paling berterima kasih karena selalu saling menemani ketika lagi gabut diajak jalan-jalan, liburan, makan, nonton.
8. Teman-teman angkatan POS17IVISM sedari awal semester hingga semester akhir berjuang bersama-sama. Terkhusus Lutfi Nurdin terima kasih pengalaman perjalanan mudik pulang kampung naik motor yang wacana dari tahun 2018 baru terealisasi di tahun 2021. Tim Nusantara; Asrul Achmad, Indah Permatasari, Muhammad Yamin Usman, partner vibes positif yang sekali dua kali seminggu ke kafe ngerjain skripsi sampai kafenya tutup. See you on top guys☺
9. HIMAHI UNIFA; tempat penulis berproses menjadi pribadi yang memanusiakan manusia. Terima kasih telah menjadi naungan pertama sejak penulis masuk di kampus. Terkhusus kanda-kanda yang menemani penulis berproses terima kasih pembelajaran dan waktu kebersamaan yang berkesannya terutama Kak Wahyu, Kak Nelfan, Kak Wandi.
10. Teman-Teman KKN, thank you for drawing my black and white mind for almost 3 Month.

Thank you, life, for being such a roller coaster.

Thank you for being my greatest teacher.

ABSTRAK

KERJA SAMA INDONESIA DAN INGGRIS DALAM BIDANG KEAMANAN SIBER (2018)

Muhammad Syahrul Endy Baharsyah
Andi Meganingratna

Perkembangan teknologi yang semakin maju memberikan banyak kemudahan yang diperoleh. Kemajuan teknologi tidak hanya memberikan dampak positif, juga dampak negatif. Indonesia dan Inggris merupakan negara-negara yang tidak dapat terhindar dari ancaman dan serangan siber sehingga kedua negara perlu memperkuat ketahanan dan keamanan siber. Penelitian ini membahas bagaimana bentuk kerja sama indonesia dan Inggris 2018 dalam bidang kemanan siber. Untuk itu penelitian ini menggunakan konsep kerja sama bilateral dan kemanan siber. Untuk mencapai tujuan tersebut, penulis menganalisa data menggunakan metode penelitian kualitatif deskrptif yang dengan teknik *literature research.* Hasil penelitian ini menunjukkan bahwa ada beberapa bentuk kerja sama yang dilakukan yaitu, implementasi dan pengembangan strategi keamanan siber, pengelolahan insiden siber, kejahatan siber, pelatihan kesadaran kemanan siber, dan pengembangan kapasitas. Hasil yang ditemukan adalah kerja sama dalam bidang keamanan siber belum memberikan hasil yang maksimal karena jumlah serangan siber di indonesia masih terus meningkat.

Kata Kunci: *Kerjasama Bilateral, Indonesia, Inggris, Bidang keamanan Siber.*

ABSTRACT

INDONESIA AND ENGLAND AGREEMENTS IN CYBER SECURITY SECTOR (2018)

Muhammad Syahrul Endy Baharsyah
Andi Meganingratna

Technology Development which is more advanced, gives plenty obtained convenience. Technology advancement apart from giving positive effect, it also gives negative effect. Indonesia and England are countries those are inevitable from cyber-attack and cyber-threat thus both countries need to strengthen cyber security and protection. This research discussed on how the form of Indonesia and England agreements 2018 in cyber security sector is. Therefore this research used cyber security and bilateral agreements concept. In order to find the results, the researcher analyzed the data using descriptive qualitative method along with literature research technique. This research results showed that there are several conducted agreements forms which are, implementation and cyber security strategy development, cyber incident management, cyber-crime, cyber security awareness training, and capacity development. The obtained result is the agreements in cyber security sector had not given maximum results because cyber-attack number in Indonesia is still increasing.

Keywords*: Bilateral Agreements, Indonesia, England, Cyber Security Sector*

DAFTAR ISI

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era sekarang ini seluruh bidang dan aspek kehidupan sebuah negara mengalami berbagai macam perubahan dan pengembangan. Hal ini tentunya di iringi pula dengan kecanggihan teknologi yang semakin mempermudah kehidupan manusia. Kemajuan teknologi informasi dan komunikasi khususnya yang berbasis pada internet telah mempengaruhi hampir semua orang untuk memanfaatkan dan menggunakannya.

Pada perkembangannya, internet tidak hanya memberikan dampak positif namun juga membawa dampak yang negatif[1]. Dampak negatifnya munculnya kejahatan baru sebagai akibat dari perkembangan arus teknologi di dunia melalui globalisasi juga berkembang pesat seperti pesatnya perkembangan teknologi itu sendiri, diantaranya kejahatan manipulasi data, *Data Forgery, Cyber Espionage, Illegal Contents,* dan berbagai macamnya. Bahkan pemerintah belum punya kemampuan yang cukup untuk mengimbangi kejahatan melalui internet ini sehingga sulit untuk mengendalikannya[2].

[1]Anggoro Dwi Listyanto, Sudji Munadi. 2012. Pengaruh Pemanfaatan Internet, Lingkungan Dan Motivasi Belajar Terhadap Prestasi Belajar Siswa SMK. Jurnal Pendidikan Vokasi, h.34
[2]Budi Suhariyanto. 2012. *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: PT Raja Grafindo Persada, h.22

Sedangkan dampak positifnya yaitu mencegah terjadinya serangan-serangan dari pihak-pihak yang ingin memecah kesatuan Indonesia dan memecah belah yang menjadi perbedaan dalam kehidupan bernegara dengan media informasi, Teknologi informasi dapat mempercepat penyampaian informasi sehingga dapat mempercepat pengambilan keputusan, penggunaan program kecerdasan buatan untuk mensimulasikan formasi dan kekuatan musuh memungkinkan serangan menjadi efektif dengan tingkat keberhasilan yang cukup tinggi dan berbagai macamnya. Para pengguna internet harus berhadapan dengan potensi ancaman keamanan dalam hal pengelolaan baik dalam bentuk penyimpanan maupun penggunaannya.

Fenomena terkait *cyber security* telah menjadi isu prioritas seluruh negara di dunia semenjak teknologi informasi dan komunikasi dimanfaatkan dalam berbagai aspek kehidupan, baik dalam aspek sosial, ekonomi, hukum, organisasi, keamanan, pertahanan, dan lain sebagainya. Berbanding lurus dengan tingginya tingkat pemanfaatan teknologi informasi dan komunikasi tersebut, tingkat risiko dan ancaman penyalahgunaan teknologi informasi dan komunikasi juga semakin tinggi dan semakin kompleks. Sehingga diperlukan untuk menyusun strategi keamanan siber dalam bentuk kerjasama antara Indonesia dengan Inggris.

Ancaman siber adalah tindakan yang mungkin muncul namun berpotensi menyebabkan masalah serius terhadap jaringan atau sistem

komputer dan semua orang bisa terkena dampaknya. Dalam ranah negara misalnya, komponen yang terkomputerisasi adalah bagian dari infrastruktur penting pemerintah dan rentan terhadap peretas dan menjadi target serangan siber. Gangguan minor terhadap kinerja sistem bisa menyebabkan kerugian ekonomi yang cukup signifikan. Untuk pengusaha, pencurian kekayaan intelektual serta pelanggaran keamanan dan data menjadi ancaman umum yang perlu diatasi. Sementara itu, dalam ranah individu, perlu disadari adanya risiko terkait pencurian data dan penyebaran perangkat lunak dan virus yang berbahaya[3]. Kejahatan siber merupakan suatu bentuk tindakan kriminal dengan menggunakan komputer sebagai alat kejahatan utama yang memanfaatkan kecanggihan teknologi internet.[4]

Semakin pesatnya perkembangan teknologi informasi berdampak pada resiko ancaman di ruang siber yang mendorong negara untuk menata ulang kebijakan keamanan dalam merespon ancaman siber yang semakin nyata. Pencapaian kekuatan siber bergantung pada strategi dan kebijakan suatu negara dalam mengembangkan keamanan siber. Indonesia belum memiliki kebijakan

[3]Noor Halimah Anjani. 2020. Ringkasan Kebijakan | Perlindungan Keamanan Siber di Indonesia. https://id.cips-indonesia.org/post/ringkasan-kebijakan-perlindungan-keamanan-siber-di-indonesia (diakses pada tanggal 20 Oktober 2021).
[4]Abdul Wahid, Mohammad Labib. 2005. Kejahatan Mayantara *(Cyber Crime*). Bandung: Refika Aditama, h.6

khusus untuk mengelola dan menangani keamanan siber secara terintegrasi[5].

Siber dijadikan salah satu faktor ancaman bagi negara disebabkan ruang lingkupnya yang dapat dimanfaatkan untuk mencuri informasi, penyebaran ide yang bersifat destruktif, maupun serangan terhadap sistem informasi di berbagai bidang. Contohnya seperti data perbankan, jaringan militer, bahkan sistem pertahanan negara. *Cyberspace* yang bersifat global[6], menjadikan kejahatan siber sulit untuk ditentukan yuridiksinya, sebab *locus delicti* yang dilakukan berada dalam dunia maya, dan dunia maya ini bersifat melewati batas-batas teritorial ataupun kedaulatan wilayah. Selain itu, bentuk serangan siber yang dilakukan terdiri dari berbagai jenis[7].

Penyebab serangan siber yang dilancarkan ke Indonesia dikarenakan Indonesia merupakan negara dengan jumlah penduduk yang besar dan memiliki potensi sumber daya alam yang melimpah. Hal ini dapat menjadi faktor utama dimana Indonesia menjadi sasaran *spionase* asing dengan berbagai bentuk tindak kejahatan siber.

[5]Prayudi, Ahmad Budiman, Aryojati Ardipandanto, Aulia Fitri. 2018. Keamanan Siber dan Pembangunan Demokrasi di Indonesia. Jakarta Pusat: Pusat Penelitian Badan Keahlian DPR RI Gedung Nusantara, h.23

[6]Dwidja Priyatno, *Bunga Rampai Pembaharuan Hukum Pidana Indonesia*, (Bandung: Pustaka Reka Cipta, 2018), hal. 13.

[7]M. Arsyad Sanusi. 2005. Hukum Teknologi dan Informasi. Bandung: Tim Kemas Buku, h.45

Perkembangan teknologi yang amat pesat telah membuat teknik perang siber menjadi lebih kompleks dan lebih canggih[8].

Indonesia menjadi Negara dengan tingkat keamanan siber yang rendah karena Indonesia masih rendah dalam hal teknologi siber. Ancaman serangan siber semakin tinggi seiring dengan meningkatnya kebutuhan terhadap teknologi informasi. Sehingga dibutuhkan strategi keamanan siber nasional yang kuat untuk mencegah dan menanggulangi serangan siber tersebut[9].

Berdasarkan dampak tersebut, maka perlu adanya perlindungan terhadap infrastruktur siber dari serangan-serangan yang mungkin terjadi. Keamanan siber menjadi hal yang penting sehingga infrastruktur siber terus dapat berjalan walaupun terdapat serangan siber[10]. *Cyber-security* atau keamanan siber mempunyai fungsi atau peran untuk menemukan, memperbaiki, ataupun mengurangi tingkat risiko terjadinya ancaman siber *(cyber threat)* dan serangan siber *(cyber attack)* serta semua aktivitas yang berpotensi mengancam keamanan seluruh komponen sistem siber itu sendiri yang meliputi *hardware, software*, data/informasi maupun infrastruktur[11]. Roxana Radu

[8]Vishnum. 2018. Ancaman Keamanan Siber Menyebabkan Kerugian Ekonomi bagi Organisasi di Indonesia Sebesar US$34.2 Miliar, h.7
[9]Vishnum. 2018. Ancaman Keamanan Siber Menyebabkan Kerugian Ekonomi bagi Organisasi di Indonesia Sebesar US$34.2 Miliar, h.6
[10]Nazli Coucri dan Daniel Goldsmith, “Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security”, Buletin of the Atomic Scientists 68, No. 2 (2012):72
[11]L. Siagian, A. Budiarto. 2017*. P. Strategi, P. Udara, and U. Pertahanan,* “the Role of Cyber Security in Overcome Negative Contents To. h.33.

memaparkan bahwa *cyber security* merupakan seperangkat kebijakan, alat, instrumen, manajemen risiko dalam mencegah ancaman yang datang dari dunia maya[12].

Maraknya kasus kejahatan siber yang terjadi di Indonesia yang disebabkan karena adanya keterbatasan terkait sarana dan prasarana dalam teknologi dan kemampuan dalam menghadapi serangan siber, sehingga dalam hal ini seluruh elemen pertahanan keamanan kedaulatan Indonesia harus terus menerus meningkatkan sistem pertahanan dan keamanan siber serta peningkatan akan kemampuan kapasitas dan kuantitas dari sisi teknologi informasi dan komunikasi serta sumber daya manusia.[13]

Sebelumnya Indonesia berada pada titik dimana lingkungan strategis semakin tidak pasti dan tidak dapat diprediksi. Oleh karenanya, pemerintah Indonesia perlu menerapkan strategi yang mampu beradaptasi dan meningkatkan peran diplomasi yang dilakukan dalam mencegah konflik yang dapat mengganggu stabilitas kawasan serta kepentingan nasional. Oleh karenanya upaya dalam membangun keamanan siber, bukanlah sesuatu yang dapat diperjuangkan sendirian oleh suatu Negara, namun diperlukan berbagai dukungan dan kerjasama serta keselarasan dari berbagai pihak dalam pembangunan

[12]Radu, Roxana. 2014. *Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace dalam Jan Frederik Kremer & Benedikt Muller* (ed), Cybersp.
[13]Vishnum, Op.Cit.

keamanan siber.[14] Pemerintah Indonesia sangat menyadari gagasan bahwa lingkungan keamanan siber tidak dapat dibangun seorang diri melainkan lebih efektif apabila dilakukan secara bersama-sama. Sehingga Indonesia berinisiatif melakukan kerjasama dengan Inggris.

Berdasarkan fenomena negara yang terjadi antara Indonesia dan Inggris dimana dengan maraknya berbagai kasus kejahatan siber yang dapat berdampak pada kepentingan kedua negara tersebut baik kepentingan nasional maupun kepentingan Inggris yang berada di luar negeri. Kedua negara tersebut saling membutuhkan bantuan dari negara lain untuk mengatasi kejahatan siber dan Indonesia memilih Inggris dikarenakan memiliki kualitas, kuantitas serta kapabilitas yang membuat kerjasama ini terjalin[15].Sejak terjalinnya hubungan *diplomatic* antara Indonesia dan Inggris dalam berbagai bidang diantara kedua negara semakin terjalin erat termasuk dalam bidang keamanan siber[16]. Sebab itu Indonesia perlu melakukan kerjasama dengan Inggris dalam bidang keamanan *cyber*.

Sedangkan Inggris memiliki salah satu tujuan strategis yakni bersedia bekerjasama secara internasional dalam menjaga keamanan siber internasional dan tujuan Inggris yakni untuk menjadi negara yang

[14]Setyawan, David Putra & Arwin Datumaya Wahyudi Sumari. 2016. Jurnal Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui Asean Regional Forum On Cybersecurity Initiatives. Universitas Pertahanan Indonesia, h.49.
[15]Rizky Pratama. *Kerjasama Indonesia-Inggris Dalam Mengatasi Kejahatan Siber Di Indonesia Tahun 2018-2020.* Journal Ilmu Hubungan Internasional, Vol. 8 No. 4, 2020.
[16]Subagyo, A. . *Teori Hubungan Internasional: Teori-teori National Interest.* (Cimahi: FISIP HI-UNJANI), h.23.

aman di dunia maya untuk melakukan bisnis[17]. Mengapa inggris memiliki Tujuan strategis tersebut, karena Inggris ingin mengembangkan bidang keamanan siber. Sehingga Indonesia diharapkan dapat mengambil hal positif dari kemajuan teknologi Inggris terutama di bidang keamanan siber[18]. Dengan demikian, melihat permasalahan siber yang dialami oleh Indonesia, maka Pemerintah Inggris menginisiasi kerjasama dengan Indonesia di bidang keamanan siber. Sehingga Indonesia dan Inggris menandatangani nota kesepahaman terkait keamanan siber dan Pemerintah Indonesia dan Inggris sepakat untuk menjalin kerja sama dalam bidang keamanan siber[19]

Kerjasama yang dilakukan ini memiliki kepentingan sendiri bagi pemerintah Inggris, hubungan bilateral antara Indonesia dan Inggris merupakan hal yang krusial dan penting, hal ini dikarenakan kerjasama ini akan membuat kedua negara memiliki kesempatan untuk mendiskusikan sejumlah isu internasional, terlebih setelah terpilihnya Indonesia menjadi anggota tidak tetap Dewan Keamanan Perserikatan Bangsa-Bangsa (DK PBB) untuk dua tahun mendatang, dengan

[17]David Putra Setyawan dan Arwin Datumaya Wahyudi Sumari, *"Diplomasi Pertahanan Indonesia dalam Pencapaian Cybersecurity melalui ASEAN Regional Forum on Cybersecurity Initiatives",* Jurnal Penelitian Politik, Volume 13 No. 1 (Juni 2016), h.2.
[18]Elizabeth Longworth. 2000. *The Possibilities for legal framework for cyberspace- Including New Zealand Perspective, Theresa Fuentes et.al (editor), The International Dimesions of Cyberspace Law: Law of Cyberspace Series,* Vol.1, Aldershot: Ashgate Publishing Limited.
[19]Islami, M.J. 2017. *Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index.* Jurnal Masyarakat Telematika dan Informasi Vol. 8 No. 2 (Oktober-Desember 2017), h.137-144.

masuknya Indonesia ke dalam anggota DK PBB membuat Indonesia dan Inggris dapat lebih mendiskusikan pelestarian nilai-nilai demokrasi internasional kerjasama yang dilakukan Indonesia dan Inggris tidak hanya dalam bidang keamanan siber. Kerjasama antara Indonesia dan Inggris dalam bidang keamanan bidang siber juga bertujuan untuk menjaga sektor ekonomi dan perdagangan antara kedua negara agar aman dan tidak terancam dengan peretasan atau kejahatan siber lainnya, hal ini dikarenakan Inggris merupakan salah satu investor terbesar di Indonesia (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*)[20].

Kerjasama antara Indonesia dan Inggris dalam bidang keamanan siber merupakan suatu kerjasama yang terlaksana ditahun 2018. Dimana kerjasama dalam bidang keamanan siber ini diinisiasi langsung oleh Pemerintah Kerajaan Inggris ke Badan Sandi dan Siber Negara Indonesia pada bulan Agustus 2018. Untuk menyepakati dan mengukuhkan kerjasama dalam bidang keamanan siber, maka pada 14 Agustus 2018 penandatanganan Memorandum Saling Pengertian Antara Pemerintah Republik Indonesia dan Pemerintah Kerajaan Inggris dalam bidang keamanan siber pada 14 Agustus 2018[21].

[20]Edmon Makarim, Indonesian Legal Framework for Cybersecurity http://www.nisc.go.jp/security-site/campaign/ ajsympo/pdf/lecture2.pdf
[21] Triwahyuni Dewi. Wulandari TA. 2016. *Strategi Keamanan Cyber Amerika Serikat.* Diakses dari https://search.unikom.ac.id/index.p hp/jipsi/article/view/239

Berdasarkan penjelasan di atas diharapkan kerja sama Indonesia dan Inggris dalam bidang keamanan siber mengembangkan kerjasamanya dan membawa aspek yang positif.

1.2 Fokus Penelitian dan Rumusan Masalah

Penelitian ini untuk membahas bagaimana kerja sama indonesia dan inggris dalam bidang keamanan siber.

Berdasarkan hal tersebut maka penulis maka penulis merumuskan permasalhan yanag diangkat penulis yaitu bagaimana bentuk kerjasama dengan Indonesia dengan Inggris dalam bidang keamanan siber dan apa yang menjadi kepentingan Indonesia dan Inggris dalam melakukan kerjasama dalam bidang keamanan siber.

1.3. Tujuan Penelitian

1.3.1 Mengetahui bagaimana kerja sama Indonesia dan Inggris dalam bidang keamanan siber.

1.3.2 Mengetahui apa yang menjadi kepentingan Indonesia dan Inggris dalam melakukan kerjasama dalam bidang keamanan siber.

1.4. Kegunaan Penelitian

1.4.1 Kegunaan Teoritis

Secara teoritis maupun akademis, penelitian ini diharapkan dapat memberikan pandangan, informasi dan data yang akurat di dalam Program Studi Hubungan Internasional tentang keamanan siber

indonesia dan bentuk kerja sama indonesia dalam di bidang kemanan siber.

1.4.2. Kegunaan Praktis

Hasil penelitian ini diharapkan dapat memberikan informasi mengenai kerja sama Indonesia dan Inggris dalam bidang keamanan siber. Penelitian ini diharapkan dapat menjadi acuan bagi penyusunan skripsi khususnya yang berminat mengangkat topik yang berkaitan dengan bidang keamanan siber.

BAB II

TINJAUAN PUSTAKA

2.1. Landasan Konseptual

Setiap penelitian membutuhkan kerangka berfikir yang berfungsi untuk mengarahkan penelitian yang diangkat dan menarik benang merah dari hubungan antara variabel penelitian dan penerapan konsep atau teori yang diangkat ke dalam masalah penelitian.

2.1.1. Keamanan Siber

Cyber-security berasal dari dua kata yaitu *cyber* dan *security.* Cyber berarti dunia maya atau dunia internet dan Security berarti keamanan, sehingga pengertian sederhana dari *cyber-security* adalah keamanan siber. *Cyber-security* atau keamanan siber mempunyai fungsi atau peran untuk menemukan, memperbaiki, ataupun mengurangi tingkat risiko terjadinya ancaman siber *(cyber threat)* dan serangan siber *(cyber attack)* serta semua aktivitas yang berpotensi mengancam keamanan seluruh komponen sistem siber itu sendiri yang meliputi hardware, software, data/informasi maupun infrastruktur[22].

Roxana Radu memaparkan bahwa *cyber security* merupakan seperangkat kebijakan, alat, instrumen, manajemen risiko dalam

[22]L. Siagian, A. Budiarto. 2017*. P. Strategi, P. Udara, and U. Pertahanan,* "the Role of Cyber Security in Overcome Negative Contents To. h.33.

mencegah ancaman yang datang dari dunia maya[23]. Adapun Madeline Carr menjelaskan dalam jurnalnya yang berjudul *Crossed Wires: International Cooperation on Cyber Security* bahwa keamanan cyber merupakan permasalahan post-state. Artinya adalah keamanan cyber merupakan bentuk ancaman yang tidak bisa ditangani menggunakan paradigma Westphalia yaitu mengatasi ancaman melalui instrumen negara seperti militer. Carr menegaskan bahwa ancaman yang datang dari dunia maya bersifat tanpa batas dan tidak terlihat namun dampaknya sangat terasa[24].

Cyber-security merupakan upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan cyber. Tujuan keamanan umum terdiri dari ketersediaan; Integritas termasuk didalamnya keaslian dan kemungkinan upaya mengurangi terjadinya penolakan serta terakhir kerahasiaan. Organisasi dan aset pengguna dalam *cyber-security* termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya.

---

[23]Radu, Roxana. 2014. *Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace dalam Jan Frederik Kremer & Benedikt Muller* (ed), Cybersp.

[24]Carr, Madeline. 2015. *Crossed Wires: International Cooperation on Cyber Security dalam Interstate Journal of International Affairs,* 2015/2016, Vol.2.Issue II.

Keamanan siber dapat dikatakan sebagai sebuah rangkaian aktifitas ataupun pengukuran yang dimaksudkan untuk melindungi dari disrupsi, serangan, atau ancaman yang lainnya melalui elemen-elemen *cyberspace* baik *software, hardware, computer network.*[25]

Cyber-security merupakan tindakan pencegahan kerusakan, perlindungan, dan pemulihan komputer, sistem komunikasi elektronik, layanan komunikasi elektronik, komunikasi kawat, dan komunikasi elektronik termasuk informasi yang terkandung di dalamnya untuk memastikan ketersediaan, integritas, otentikasi, kerahasiaan, dan non-penolakan[26].

Dapat dikatakan bahwa keamanan siber merupakan segala upaya yang dilakukan baik perorangan atau kelompok secara mandiri ataupun kolektif dengan melakukan tindakan-tindakan atau upaya untuk mengamankan, menjaga, mengantisipasi ataupun meminimalisir dampak-dampak yang berkaitan dengan ruang siber. Diketahui bahwa ruang lingkup *cyber-security* dimulai dari install, harden atau keamanan terkait dengan perangkat keras yang digunakan dalam mengoperasikan internet, monitor, yang menyebabkan terjadinya insiden atau kejadian dan insiden itu dapat pula berasal dari serangan atau *cyber attact* yang membutuhkan penangganan terhadap insiden tersebut dengan

[25]Fischer, E. A. 2009. *Creating a National Framework for Cybersecurity: an Analysis of Issues and Options.* New York: Nova Science Publishers, Inc, h.32
[26]Fischer, E. A., Ave, I., & Washington, S. E. 2005. *Creating a National Framework for Cybersecurity : An Analysis of,* h.20.

melakukan uji forensik sebagai pembuktian dalam penegakan hukum terhadap terjadinya *cyber crime.*

Menurut Solms & Nieker menjelaskan penting dalam sistem keamanan siber yaitu faktor manusia. Dalam konteks keamanan siber bahwa faktor manusia sangat terkait dengan peran yang dimainkan sebagai pengguna dalam proses keamanan dan dapat berdampak positif atau negatif terhadap proses keamanan siber[27].

Cyber-security lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (*confidentiality), integritas (integrity),* dan ketersediaan *(availability)* informasi. Mekanisme ini harus bisa melindungi informasi baik dari serangan fisik maupun dari serangan dunia maya.

Cyber security juga dapat diartikan sebagai melindungi hilangnya kemampuan pemilik komputer (pihak yang berwenang atas pengendalian komputer miliknya) untuk mengendalikan sistem komputer sehingga tidak berfungsi sebagaimana mestinya yang diakibatkan oleh adanya serangan penyusup yang masuk ke dalam sistem komputer atau melalui malware[28]. Konsep *cyber security* merujuk kepada persepsi ancaman yang dihadapi mengingat aktivitas yang terhubung melalui internet adalah borderless, namun ketika arus informasi dengan cepat maka tidak

[27]Von Solms, R., & Van Niekerk, J. 2013. *From information security to cyber security. Computers and Security, 38, 97–102*. https://doi.org/10.1016/j.cose.2013.04.004
[28]Yani Y.M, Ian Montrama, Emil Wahyudin. 2017. *Pengantar Studi Keamanan*. (Malang: Intrans Publishing), h.73.

terhindarkan ancaman terhadapnya dengan semakin kompleksnya berbagai aktor yang terlibat dalam aktivitas yang terkoneksi melalui internet[29].

Cyber-security merupakan upaya untuk melindungi informasi dari adanya serangan dunia maya, adapun elemen pokok *cyber-security* adalah:

1) Dokumen *security policy* merupakan dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi.
2) *Information infrastructure* merupakan media yang berperan dalam kelangsungan operasi informasi meliputi hardware dan software. Contohnya adalah *router, switch, server, sistem operasi, database, dan website.*
3) *Network Monitoring* System merupakan media yang berperan untuk memonitor kelayakan, utilisasi, dan *performance* infrastruktur informasi.
4) *System Information and Event Management* merupakan media yang berperan dalam memonitor berbagai kejadian di jaringan termasuk kejadian terkait pada insiden keamanan.
5) *Network Security Assessment* merupakan elemen *cyber-security* yang berperan sebagai mekanisme kontrol dan memberikan *measurement* level keamanan informasi.

[29]Putri Sylvia Octa. 2015. *Mengenal Studi Hubungan Internasional.* (Bandung: Zavara), h.137.

6) *Human resource dan security awareness* berkaitan dengan sumber daya manusia dan *awareness-nya* pada keamanan informasi. Selain *cyber-security* kelangsungan operasi informasi juga bergantung pada physical security yang tentunya berkaitan dengan semua elemen fisikal misalnya bangunan data *center, disaster recovery system,* dan media transmisi[30].

Jenis keamanan yang menjadi konsep dasar dari *cyber security* yaitu[31]:

1. Kerahasiaan (*Confidentiality)*

Pada dasarnya, c*onfidentiality* adalah suatu upaya dalam merahasiakan dan juga menyimpan data. Dalam pelaksanaannya berupa tindakan mengontrol setiap akses data dengan tujuan menghindari adanya pencurian data ataupun kebocoran data. Caranya adalah dengan memberikan batas wewenang akses pada pihak yang tidak memiliki kepentingan. Misalnya seperti memberikan akses ke database penggajian perusahaan pada mereka yang hanya berada pada penggajian saja. Mereka yang bukan termasuk pada bagian penggajian hanya mampu melihat struktur perusahaan saja. *Confidentiality* ini juga bisa dikerjakan dengan *two factor authentication* atau 2FA. Dengan

[30]Edmon Makarim, Indonesian Legal Framework for Cybersecurity http://www.nisc.go.jp/security-site/campaign/ ajsympo/pdf/lecture2.pdf diakses Kamis, 28 Oktober 2021.

[31] Reid, R., & Van Niekerk, J. 2014. *From information security to cyber security cultures. 2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference,* (August 2015). https://doi.org/10.1109/ISSA.2014.6950492

menerapkan 2FA, maka Anda harus bisa melewati dua tahap otentikasi diri sebelum bisa mengakses suatu data. Tahap pertama adalah dengan mengisi password secara tepat, dan tahap kedua adalah dengan kode tertentu yang dikirim ke perangkat ataupun email Anda.

2. Integritas (*Integrity*)

Integrity yang terdapat di dalam teknologi informasi adalah suatu upaya dalam memberikan data secara akurat, konsisten dan juga terpercaya. Sebagai contoh. Dalam kasus yang sama, Anda juga harus bisa terus menjaga data setiap pelanggan dengan baik. Hindari adanya kebocoran data yang mampu merugikan para pelanggan Anda.

Beberapa cara yang bisa dilakukan untuk bisa menjaga integritas adalah dengan enkripsi, tanda tangan digital, sampai *certificate authority* (CA) digital. CA adalah suatu sertifikat seperti SSL atau TLS yang berfungsi dalam menjaga verifikasi identitas setiap pengguna situs Anda.

3. Ketersediaan (*Availability)*

Komponen terakhir yang terdapat di dalam CIA Triad adalah *availability.* Komponen ini mengacu pada bentuk ketersediaan data Anda. Dalam dunia bisnis, ketersediaan suatu sistem, aplikasi dan juga data yang mampu diakses oleh para pelanggan adalah suatu kewajiban[32].

[32]https://accurate.id/teknologi/cyber-security-adalah/ (diakses pada tanggal 27 Oktober 2021).

Salah satu usaha untuk mengatasi ancaman siber yaitu dengan melalui kemanan siber atau *Cyber-security. Cyber-security* adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna[33].

Fungsi dari keamanan siber sendiri dapat dijabarkan sebagai berikut.[34]

1. Menjamin tercapainya sinergi kebijakan pertahanan siber.
2. Membangun organisasi dan tata kelola sistem penanganan keamanan siber.
3. Membangun sistem yang menjamin ketersediaan informasi dalam konteks pertahanan siber.
4. Membangun sistem penangkalan, penindakan dan pemulihan terhadap serangan siber.
5. Mewujudkan kesadaran keamanan siber
6. Meningkatkan keamanan sistem siber sektor pertahanan.
7. Mewujudkan riset dan pengembangan untuk mendukung pembinaan dan pengembangan kemampuan Pertahanan Siber.

[33]Handrini Ardiyant. Cyber-Security Dan Tantangan Pengembangannya Di Indonesia, (diakses pada tanggal 20 Oktober 2021).
[34]KEMENHAN 2014. RI. Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun Tentang Pedoman Siber. Kementrian Pertahanan, h.5.

8. Menyelenggarakan kerjasama nasional dan internasional guna pembinaan dan pengembangan kemampuan Pertahanan Siber.

Keamanan siber sangat diperlukan untuk menjaga dan mengantisipasi ancaman-ancaman yang berasal dari ruang siber. Keamanan siber semestinya adalah sebuah ekosistem dimana hukum *(laws),* organisasi *(organizations),* kemampuan *(skills),* kerjasama *(cooperation),* dan *technical implementation* berjalan secara selaras untuk dapat menjadi efektif.[35] *International Telecommunication Union* (ITU) melakukan survey dalam mengukur komitmen negara-negara anggota terhadap keamanan siber melalui *Global Cybersecurity Index* (GCI). *Global cyber security indexs* atau indeks keamanan siber dunia berguna supaya negara dapat melakukan proyeksi dan peninjauan kembali pada bidang keamanan siber masing-masing negara.

Beragam cara dapat dilakukan dalam meningkatkan atau membangun kemanan siber oleh suatu negara seperti peningkatan kapasitas siber dalam negeri, kerjasama dengan negara lain atau bahkan organisasi-organisasi internasional. Di Indonesia sendiri tentunya telah digalakkan berbagai kebijakan dan usaha-usaha dalam membangun kemanan siber. Salah satu bentuk peningkatan kapasitas siber dalam negeri ialah adanya Keamanan Siber Nasional *(National Cyber Security)* oleh Kemenhan. *National Cyber Security* merupakan segala upaya dalam

[35]ITU. 2017. *Global Cybersecurity Index 2017.* (International Telecommunication Unit), h.8

rangka menjaga kerahasiaan, keutuhan dan ketersediaan informasi serta seluruh sarana pendukungnya di tingkat nasional dan bersifat lintas sector. Kemhan/TNI juga telah merancang pedoman pertahanan siber berdasarkan Permenhan No.82 Tahun 2014 tentang Pedoman Pertahanan Siber. Salah satu bentuk kerja sama dalam upaya peningkatan keamanan siber melalui lingkungan eksternal ialah melalui ASEAN Regional Forum (ARF).[36]

Dampak dari adanya serangan *cyber* menimbulkan dampak yang buruk bagi Indonesia dan Inggris, terutama pada sektor perekonomian. *Cyber* dapat menjadi salah satu faktor ancaman bagi ruang lingkup dari siber yang dapat dimanfaatkan untuk mencuri informasi, penyebaran ide yang bersifat destruktif, maupun serangan terhadap system informasi di berbagai bidang. Dampak serangan lainnya seperti penyerangan melalui virus terhadap situs-situs dan tindakan lainnya yang merupakan ancaman sekaligus tantangan yang harus dihadapi oleh Indonesia dan Inggris dalam menjaga keamanan *cyber*. Pemerintah Inggris menginvestasikan biaya tinggi untuk perlindungan pertahanan dan keamanan *cyber* bagi kepentingan bisnis Ingrris. Sedangkan Indonesia kemampuannya dalam menghadapi serangan siber, dalam hal ini seluruh elemen pertahanan keamanan kedaulatan Indonesia harus secara terus-menerus dalam meningkatkan sistem pertahanan dan keamanan siber, dan peningkatan

[36]KEMENHAN 2014. RI. *Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun Tentang Pedoman Siber*. (Kementrian Pertahanan), h.5.

akan kemampuan kapasitas dan kuantitas dari sisi teknologi informasi dan juga komunikasi serta sumber daya manusia[37].

Dengan maraknya kasus kejahatan siber yang juga dapat berdampak pada kepentingan Inggris dan Indonesia baik kepentingan nasional maupun kepentingan Inggris yang berada di luar negeri, maka kedua Negara tersebut bersedia bekerjasama secara internasional dalam menjaga keamanan *cyber* dengan tujuan yakni untuk menjadi negara yang aman di dunia maya untuk melakukan bisnis dan mengamankan kepentingan yang berada di luar yuridksi negara Inggris dan Indonesia yang berdampak secara langsung pada keamanan nasional Inggris dan Indonesia.

Dalam penulisan penelitian ini penulis meninjau penelitian sebelumnya yaitu pertama bersumber dari artikel yang ditulis oleh Hidayat Chusnul Khotima yang berjudul “Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara”**.** Dalam tulisan tersebut dikatakan sebagai perlindungan terhadap pengungkapan yang tidak diinginkan, modifikasi, atau kerusakan data dalam suatu sistem dan juga untuk pengamanan sistem itu sendiri. Dalam hal ini ancaman dalam cybersecurity tidak hanya diakibatkan oleh agen

[37]Triwahyuni Dewi. Wulandari TA. 2016. *Strategi Keamanan Cyber Amerika Serikat.* Diakses dari https://search.unikom.ac.id/index.p hp/jipsi/article/view/239

atau aktor tertentu tetapi juga oleh sistem itu sendiri sehingga kemudian muncul istilah *“cyber security”*[38]

Rujukan pustaka lainnya bersumber dari artikel yang ditulis oleh Dwi Rezki Sri Astarin dan Muhammad Syaroni Rofii yang berjudul “Keamanan Siber Intelejen Nasional.” Penelitian tersebut menekankan bagaiamana Peningkatan perlindungan terhadap informasi dan sistem terhadap akses yang tidak sah melalui kerahasiaan, integritas, ketersediaan informasi, dan otentikasi guna menghindari serangan siber. Termasuk menyediakan pemulihan sistem informasi dengan menggabungkan kemampuan mendeteksi, melindungi, dan merespon. Tata kelola keamanan siber di Indonesia masih bersifat parsial dan sektoral sehingga menyebabkan penanganan permasalahan keamanan siber belum terintegrasi dan belum terpadu. Hal tersebut menjadikan ancaman siber semakin nyata, terutama bila dikaitkan dengan ancaman ketahanan dan keamanan siber bagi pemerintah sebagai penyelenggara layanan publik sektor Infrastruktur Informasi Kritikal Nasional (IIKN).[39]

2.1.2.Kejahatan Siber

Cybercrime atau kejahatan siber didefinisikan sebagai sebuah kejahatan di dunia maya dengan memanfaatkan terhubungnya internet

[38] Hidayat chusnul ‘Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara’, Jurnal politica, (2019) <dpr.go.id/index.php/politica/article/view/1447>

[39] Dewi Sri Rezky dan Muhammad Syaroni ‘Keamanan Siber Intelejen Nasional’ Sekolah Kajian Strategik dan Global Universitas Indonesia (2020)

dan teknologi siber atau teknologi informasi bisa berupa komputer, telepon genggam, dan lain-lain, yang disalahgunakan untuk menyerang komputer lain yang terhubung juga ke dalam internet dan menyebabkan kerugian kepada korban yang terkena kejahatan tersebut[40]. *Cybercrime* atau kejahatan berbasis komputer, adalah kejahatan yang melibatkan komputer dan jaringan (network)[41]. *Cybercrime* yaitu pelanggaran yang dilakukan terhadap perorangan atau sekelompok individu dengan motif kriminal untuk secara sengaja menyakiti reputasi korban atau menyebabkan kerugian fisik atau mental atau kerugian kepada korban baik secara langsung maupun tidak langsung, menggunakan jaringan telekomunikasi modern seperti Internet[42]. *Cybercrime* sangat dapat mengancam suatu keamanan negara terutama negara Indonesia dan Inggris[43].

Di Indonesia, masalah dari *cyber crime* juga bisa dikatakan mulai diperhatikan sebagai suatu masalah yang serius. Dengan masuknya Indonesia kedalam era globalisasi, khususnya dalam hal hubungannya dengan dunia cyber, berbagai bidang kehidupan masyarakat Indonesia mulai mendapatkan pengaruh dari dunia cyber tersebut. Oleh karenanya tidaklah mengherankan bila mulai bermunculan kasus-kasus kejahatan yang berhubungan pula dengan dunia cyber tersebut.

---

[40]Dista Amalia Arifah, *"Kasus Cybercrime Di Indonesia Indonesia's Cybercrime Case," J. Bisnis dan Ekon.*, vol. 18, no. 2, pp. 185–195, 2011.
[41]Moore, R. 2005. "*Cyber crime: Investigating High-Technology Computer Crime,"* Cleveland, Mississippi: Anderson Publishing, h.8.
[42]Halder, D., & Jaishankar, K. 2011. *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations.* Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
[43]Steve Morgan (January 17, 2016*). "Cyber Crime Costs Projected To Reach $2 Trillion by 2019".* Forbes. Retrieved September 22, 2016.

Dengan munculnya beberapa kasus kejatan siber (cyber crime) di Indonesia telah menjadi ancaman stabilitas keamanan dan ketertiban nasional dengan eskalatif yang cukup tinggi[44]. Maraknya kasus kejahatan siber yang terjadi di Indonesia yang disebabkan karena adanya keterbatasan terkait sarana dan prasarana dalam teknologi dan kemampuan dalam menghadapi serangan siber, sehingga dalam hal ini seluruh elemen pertahanan keamanan kedaulatan Indonesia harus terus menerus meningkatkan sistem pertahanan dan keamanan siber serta peningkatan akan kemampuan kapasitas dan kuantitas dari sisi teknologi informasi dan komunikasi serta sumber daya manusia.[45]

Tindak kejahatan dalam dunia siber, tidak hanya dialami oleh Indonesia, namun, Inggris turut menjadi salah satu negara sasaran serangan siber. Dilaporkan bahwa ditahun 2017, aktvitas bisnis di Inggris mengalami serangan siber dengan rata-rata serangan sebanyak 230.000 serangan siber. Teknik serangan yang dilakukan pada aktivitas bisnis Inggris sebagian besar menggunakan teknik *malware, virus, spyware,* yang mencari kelemahan web sehingga dapat menemukan jalan masuk pada akses komputer perusahaan bisnis Inggris. Inggris yang hampir secara keseluruhan aktivitas bisnisnya terhubung secara langsung pada *internet of thing,* memberikan akses masuk bagi pelaku tindak kejahatan siber untuk melancarkan serangan pada perusahaan bisnis Inggris.

Cybercrime sebagai suatu jenis kejahatan merupakan suatu tindakan yang dilakukan di dalam dunia yang tidak mengenal batas

[44]Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime*), (Jakarta: Refika Aditama, [t.th]), h.131.
[45]Vishnum, Op.Cit.

wilayah hukum dan kejahatan tersebut dapat terjadi tanpa perlu adanya suatu interaksi langsung antara pelaku dengan korbannya. Sehingga dapat dikatakan, bahwa ketika suatu kejahatan cyber terjadi, maka semua orang dari berbagai negara yang dapat masuk ke dalam dunia cyber dapat terlibat di dalamnya, entah itu sebagai pelaku (secara langsung atau tidak langsung), korban, ataupun hanya sebagai saksi[46].

Cybercrime memiliki karakteristik unik yaitu :

1. Ruang lingkup kejahatan
2. Sifat kejahatan
3. Pelaku kejahatan
4. Modus kejahatan
5. Jenis kerugian yang ditimbulkan.

Dari karakteristik diatas, untuk mempermudah penanganannya maka *cybercrime* diklasifikasikan :

1. *Cyberpiracy :* Penggunaan teknologi computer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer.
2. C*ybertrespass* : Penggunaan teknologi computer untuk meningkatkan akses pada system computer suatu organisasi atau individu.

[46]Bima Guntara, Legitimasi Penyebaran Informasi Yang Memiliki Muatan Penghinaan Dan/Atau Pencemaran Nama Baik Dalam Pasal 310 Kuhp Dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan, Volume 4 Nomor 2 Desember 2017, h. 242.

3. *Cybervandalism :* Penggunaan teknologi computer untuk membuat program yang menganggu proses transmisi elektronik, dan menghancurkan data dikomputer.
4. Perkiraan perkembangan *cyber crime* di masa depan dapat diperkirakan perkembangan kejahatan cyber kedepan akan semakin meningkat seiring dengan perkembangan teknologi atau globalisasi dibidang teknologi informasi dan komunikasi[47].

2.1.3. Kerjasama Bilateral

Konsep kerjasama bilateral lahir dari teori kerjasama internasional yang dilakukan untuk mendukung perjuangan melawan segala bentuk pelanggaran nilai-nilai kemanusiaan, kerjasama internasional juga dapat mengatasi segala bentuk agresi atau ancaman kedaulatan nasional, persatuan nasional atau integrasi torotorial, dan penolakan terhadap hak rakyat untuk menentukan nasib sendiri dan hak setiap orang untuk melaksanakan kedaulatan sepenuhnya atas kekayaan dan sumber daya nasional[48].

Kerjasama Internasional adalah hubungan antara negara yang memiliki tujuan berlandaskan kepentingan antar negara. Kerjasama Internasional terdiri dari, seperangkat aturan, prinsip-prinsip, norma-norma, dan prosedur pembuat keputusan yang mengatur jalannya rezim

[47]Bima Guntara, op.cit, h.243
[48]Anne W. 1986. *Brascomb, Toward A Law of Global Communication Network.* USA: Longman, h.15

interasional. Selain itu, negara-negara yang melakukan kerjasama internaisonal mempunyai tujuan bersama atau kepentingan bersama karena, ketidak beradaan kepentingan bersama di dalam kerjasama, merupakan sesuatu hal yang mustahil. Kerjasama internasional adalah ketergantungan antar actor akan membuat mereka melakukan kerjasama untuk mengahadapi ancaman yang akan membahayakan kepentingan internasional[49].

Menurut Yanyan Mochamad Yani, Kerjasama internasional merupakan suatu hubungan kerjasama yang dilakukan oleh 2 negara atau lebih untuk mencapai tujuan-tujuan tertentu. Tujuan dari Kerjasama internasional yaitu mencukupi kebutuhan masyarakat masing-masing Negara, mencegah atau menghindari konflik yang mungkin terjadi, memperoleh pengakuan sebagai negara merdeka dan mempererat hubungan antar Negara.[50]

Sama halnya Indonesia dengan Inggris, mereka melakukan kerjasama di bidang keamanan siber. Indonesia melakukan kerjasama dengan Inggris karena Inggris merupakan negara yang maju, Inggris memiliki perkembangan tekonologi yang baik dan elemen penyelenggara pertahanan siber Inggris mampu mengidentifikasi, mendeteksi, dan

[49]Bobby Firdaus Usman. *Faktor-Faktor Yang Melatar Belakangi Kerjasama Indonesia Dengan Inggris Dibidang Keamanan Siber Tahun 2018*. (Mjir) Moestopo Journal International Relations, Volume 1, No. 2, September 2021.
[50]Anak Agung Banyu Perwita & Yanyan Mochamad Yani. 2006. *Pengantar Ilmu Hubungan Internasional*. Bandung: Remaja Rosdakarya, 66.

menganalisa serangan siber. Selain itu, dengan maraknya kasus kejahatan siber yang juga dapat berdampak pada kepentingan Inggris baik kepentingan nasional maupun kepentingan Inggris yang berada di luar negeri, maka salah satu tujuan strategis negara Inggris yakni bersedia bekerjasama secara internasional dalam menjaga keamanan siber internasional dan tujuan Inggris yakni untuk menjadi negara yang aman di dunia maya untuk melakukan bisnis. Sehingga Indonesia diharapkan dapat mengambil hal positif dari kemajuan teknologi Inggris terutama di bidang keamanan siber.

Dengan demikian, melihat permasalahan siber yang dialami oleh Indonesia, maka Pemerintah Inggris menginisiasi kerjasama dengan Indonesia di bidang keamanan siber. Sehingga Indonesia dan Inggris menandatangani nota kesepahaman terkait keamanan siber dan Pemerintah Indonesia dan Inggris sepakat untuk menjalin kerja sama dalam bidang keamanan siber. Suatu kerjasama internasional didorong oleh beberapa faktor[51]:

1. Kemajuan dibidang teknologi yang menyebabkan semakin mudahnya hubungan yang dapat dilakukan negara sehingga meningkatkan ketergantungan satu dengan yang lainnya.

[51]Vitashya Wowor. 2008. *Peranan United Nations Children's Fund (UNICEF) Dalam Meningkatkan Kesejahteraan Pangan Dan Gizi Anak Di Indonesia* (2006-2008). (Universitas Komputer Indonesia), h. 34.

2. Kemajuan dan perkembangan ekonomi mempengaruhi kesejahteraan bangsa dan negara. Kesejahteraan suatu negara dapat mempengaruhi kesejahteraan bangsa-bangsa.
3. Perubahan sifat peperangan dimana terdapat suatu keinginan bersama untuk saling melindungi dan membela diri dalam bentuk kerjasama internasional.
4. Adanya kesadaran dan keinginan untuk bernegosiasi, salah satu metode kerjasama internasional yang dilandasi atas dasar bahwa dengan bernegosiasi akan memudahkan dalam pemecahan masalah yang dihadapi.

Beberapa faktor dalam kerjasama internasionak ini kemudian memunculkan berbagai hubungan internasional yang kebanyakan merupakan hubungan dalam kerjasama antar negara (bilateral) yang menjadikan hubungan ini sebagai pertemuan untuk menunjukan beragam kepentingan internasional dari beberapa negara yang sifatnya tidak dapat dipenuhi oleh bangsanya sendiri. Menurut T. May. Rudy: “Setelah kerjasama yang terbentuk dari berbagai komitmen individu untuk mendapatkan kesejahteraan secara kolektif yang merupakan hasil dari adanya persamaan kepentingan.” Terciptanya kerjasama bilateral juga tidak terlepas dari tercapainya beberapa kesepahaman antara dua negara yang melakukan kerjasama serta dalam kepentingan nasionalnya yang menjadi usaha untuk menyelenggarakan politik luar negerinya. Dengan tujuan nasional yang ingin dicapai oleh suatu negara dapat

terlihat dari apa kepentingan nasional yang dirumuskan oleh pemerintahan negara tersebu[52].

Terjalinnya hubungan internasional merupakan suatu keharusan sebagai akibat adanya saling ketergantungan dan bertambahnya kompleks kehidupan manusia dalam masyarakat internasional sehingga interdepedensi tidak memungkinkan adanya suatu negara yang menutup dirinya terhadap dunia luar[53]. Sebagaimana yang dikemukakan oleh Plano dan Olton bahwa: “Hubungan kerjasama yang terjadi antara dua negara didunia ini pada dasarnya tidak terlepas dari kepentingan nasional masing-masing negara. Kepentingan nasional merupakan unsur yang sangat vital yang mencakup kelangsungan hidup bangsa dan negara, kemerdekaan, keutuhan wilayah, keamanan, militer, dan kesejahteraan ekonomi.”

Selanjutnya, dalam kerjasama bilateral yang dimaksud adalah kerjasama dibidang ideologi, politik, ekonomi, hukum, keamanan. Adapun menurut Holsty dalam terjemahan Azhary tentang variabel-variabel yang harus diperhitungkan dalam kerjasama bilateral adalah:

1. Kualitas dan kuantitas kapabilitas yang dimiliki suatu negara.
2. Keterampilan mengerahkan kapabilitas tersebut untuk mendukung berbagai tujuan.

[52]Nye, Joseph S. 2011. *The Future of Power.* USA: Perseus Book Group.
[53]Perwita, A.A.B. dan Yani, Y.M. 2017. *Pengantar Ilmu Hubungan Internasional* . Cetakan Kelima. (Bandung: PT Remaja Rosdakarya), h.3.

3. K*redibilitas* ancaman serta gangguan.
4. Derajat kebutuhan dan ketergantungan.
5. *Responivitas* di kalangan pembuat keputusan.

Hubungan akan terjalin sesuai dengan tujuan-tujuan spesifik serta bidang-bidang khusus yang dijadikan tolak ukur bagi suatu negara dalam melakukan hubungan dengan negara lain. Sebagian besar transaksi dan interaksi antar negara dalam sistem internasional sekarang bersifat rutin dan hampir bebas dari konflik. Berbagai jenis masalah nasional, regional, atau global yang bermunculan memerlukan perhatian lebih dari satu negara. Dalam kebanyakan kasus yang terjadi, pemerintah saling berhubungan dengan mengajukan alternative pemecahan, perundingan, atau pembicaraan mengenai masalah yang dihadapi, mengemukakan berbagai teknis untuk menopang pemecahan masalah tertentu dan mengakhiri perundingan dengan suatu perjanjian atau saling pengertian yang memuaskan semua pihak.

Perjanjian bilateral bersifat khusus *(treaty contract)* karena hanya mengatur hal-hal yang menyangkut kepentingan kedua negara saja. Oleh karena itu, perjanjian bilateral bersifat tertutup artinya tertutup kemungkinan bagi negara lain untuk turut serta dalam perjanjian tersebut.

Dalam konsep kerjasama bilateral, kerjasama yang dilakukan oleh pemerintah Indonesia dengan Inggris ini merupakan kerjasama yang terjalin akibat dari perkembangan teknologi yang terjadi sehingga perkembangan hubungan antara keduanya ikut meningkat agar dapat

saling melindungi dan membela diri terhadap berbagai ancaman yang terjadi melalui perkembangan teknologi, kerjasama ini juga memberikan hasil positif bagi Indonesia, dimana serangan siber yang terjadi berkurang dan meningkatnya peringkat Indonesia *dalam Global Cybersecurity Index* (GCI) yang dikeluarkan oleh *International Telecommunication Union* (ITU), peningkatan peringkat ini dari 70 pada tahun 2017 menjadi peringkat ke-41 pada tahun 2019.

Selain itu menurut sebuah riset yang dilakukan oleh *Comparitech,* keamanan siber Indonesia mengalami peningkatan dari tahun 2017 yang menempatkan Indonesia pada urutan 74 dari 76 negara, namun pada bulan September tahun 2020 Indonesia mengalami peningkatan dan menempati peringkat ke 21 dari 76 negara, hal ini dikarenakan Indonesia dapat mengatasi segala ancaman dan kejahatan yang terjadi seperti infeksi *malware* yang dapat mengacaukan perangkat seperti komputer dan *handphone,* selain itu pada riset ini juga menilai negara dari kebijakan mengenai keamanan siber serta kesiapan SDM dalam menghadapi perkembangan serangan siber[54].

Dampak yang mungkin dialami akibat dari serangan siber ialah berupa: Penyalahgunaan informasi, pengendalian sistem secara remote, kerusuhan, ketakutan, kekerasan, kekacauan, konflik, gangguan fungsional ataupun kondisi merugikan lain nya, hingga mungkin dapat

[54]Vishnum. 2018. Ancaman Keamanan Siber Menyebabkan Kerugian Ekonomi bagi Organisasi di Indonesia Sebesar US$34.2 Miliar.

mengakibatkan kehancuran[55].Ancaman-ancaman yang berasal ruang siber sangatlah berbahaya karena mengintai di segala penjuru serta setiap celah yang mampu dimanfaatkan untuk melakukan kejahatan. Kejahatan siber memiliki cangkupan yang luas serta dampak yang luas pula pada suatu negara, kawasan bahkan dunia. Kerjasama dalam rangka di bidang keamanan siber yang telah dilakukan Indonesia dan Inggris, dimana melakukan kerja sama bilateral di bidang keamanan siber dengan Inggris dengan tujuan untuk menciptakan strategi dan solusi untuk meningkatkan kepercayaan dan keamanan di tengah masyarakat informasi.[56]

Selanjutnya, dalam konsep kerjasama bilateral ini kerjasama antara Indonesia dengan Inggris terjalin karena Indonesia membutuhkan bantuan dari negara lain untuk mengatasi kejahatan siber dan dipilihnya Inggris dikarenakan memiliki kualitas, kuantitas serta kapabilitas yang membuat kerjasama ini terjalin[57]. Karena suatu negara pasti akan membutuhkan negara lain untuk memenuhi kebutuhan dalam negerinya.

Untuk mencapai kebutuhan nasional tersebut, maka salah satu cara yang dapat ditempuh yakni dengan membangun suatu hubungan

---

[55]KEMENHAN 2014. RI, Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun Tentang Pedoman Siber. Kementrian Pertahanan.

[56]Menteri Kominfo Pada “High Level Segment ITU Council 2008” Yang Membahas Cyber security, http://www.postel. go.id/info_view_c_26_p_814.htm diakses Selasa, 05 Oktober 2021.

[57]Rizky Pratama. *Kerjasama Indonesia-Inggris Dalam Mengatasi Kejahatan Siber Di Indonesia Tahun 2018-2020.* eJournal Ilmu Hubungan Internasional, Vol. 8 No. 4, 2020.

kerjasama dengan negara lain yang bersifat bilateral maupun multilateral. Pada umumnya kerjasama ini disebut sebagai kerjasama internasional.

Dalam penelitian ini penulis meninjau penelitian sebelumnya yang membahas tentang Kerja Sama Indonesia Dan Inggris Dalam Bidang Keamanan Siber. Sumber dari penelitian yang penulis gunakan adalah kepustakaan yaitu terdiri dari beberapa referensi. Dimana referensi tersebut dijadikan sebagai bahan acuan yang berhubungan dengan skripsi yang ingin penulis teliti, adapun peneliti yang pernah meneliti sebelumnya yaitu sebagai berikut:

1. Penelitian oleh Hegar Krisnaduta yang berjudul Kerjasama Indonesia-Australia di Bidang Keamanan dalam Mengatasi *Cyber Crime* di Indonesia melalui *Program Cyber Policy Dialogue.* Penelitian ini menjelaskan bahwa kerjasama Indonesia-Australia di bidang *cyber security* menjadi nilai positif bagi Indonesia. Pada tahun 2018, Badan Sandi dan Siber Indonesia mencatat bahwa Indonesia menempati posisi ke-9 dengan *nilai Global Cyber Security Index* 0,77 dengan skala (0-1) dikawasan Asia Pasifik. Nilai terendah terdapat pada indikator dengan point social engagement, yaitu kepedulian masyarakat terhadap isu-isu cyber dan pemanfaatan internet secara optimal untuk meningkatkan ekonomi digital.bahwa peningkatan pengguna internet Indonesia belum sebanding dengan meningkatnya risiko keamanan yang akan terjadi, sehingga *cyber*

security harus menjadi isu prioritas untuk mengelola risiko-risiko keamanan tersebut[58].

2. Penelitian yang dilakukan oleh Ina Sayang Tanjuang dalam skripsinya yang berjudul Kerjasama Korea *International Cooperation Agency* (KOICA) Dan Pemerintahan Indonesia Dalam Pengembangan *Cyber Security,* menunjukkan proses kerjasama yang dilakukan melalui kerjasama antara Korea *International Coorporation Agency (*KOICA) dan Pemerintahan Indonesia dalam pengembangan *cyber security* yaitu mencetak Sumber Daya Manusia (SDM) dalam *cyber security*, keamanan terhadap malware dan pertukaran informasi antara kedua negara dalam mencegah terjadinya *cyber threats*[59].

Gambar 2.1.4 Jenis Ancaman Siber

Cybercrime	*Cyber attack*	*Cyber Terrorism*
Cybercrime adalah kejahatanyang menyasar sistem komputer. Pelaku melakukan akses ilegal, transmisi ilegal atau manipulasi data untuk tujuan tertentu. Di antaranya menciptakan gangguan dan mencari keuntungan finansial.	Target *cyber attack* biasanya melibatkan kepentingan politik. Aktivitas ini berusaha mengumpulkan informasi, mencuri data, hingga mengambil alih sistem targetnya.	*Cyber Terrorism* mengacu pada usaha mengancam, provokasi atau intimidasi lewat sistem komputer. Aktivitas cyber ini sangat berbahaya karena menyebabkan kepanikan dan ketakutan skala besar.

Sumber : diperoleh resmi BSSN[1]

[58]Hegar Krisnaduta. 2019. *Kerjasama Indonesia-Australia Di Bidang Keamanan Dalam Mengatasi Cyber Crime Di Indonesia Melalui Program Cyber Policy Dialogue.* Fakultas Ilmu Sosial Dan Ilmu Politik Universitas Pasundan Bandung, h.1

[59]Ina Sayang Tanjung. 2017. *Kerjasama Korea International Cooperation Agency (Koica) Dan Pemerintahan Indonesia Dalam Pengembangan Cyber Security*. Program Studi Ilmu Hubungan Internasional Fakultas Ilmu Sosial Dan Ilmu Politik Universitas Komputer Indonesia Bandung, h.1

BAB III

METODE PENELITIAN

3.1. Rancangan Penelitian

Salah satu bagian penting dalam kegiatan penelitian adalah menyusun rancangan mengenai penelitian yang akan dilakukan. Metode penelitian merupakan bagian yang sangat penting karena sangat menentukan sukses atau tidaknya suatu penelitian. Metode penelitian adalah cara-cara yang digunakan oleh peneliti dalam merancang, melaksanakan, pengolah data, dan menarik kesimpulan berkenaan dengan masalah penelitian tertentu.[60]

Pada penelitian ini, penulis ini menggunakan pendekatan kualitatif yang mengacu pada makna, konsep, definisi, karakteristik, metafora, simbol, dan deskripsi dari suatu hal.[61] Metode penelitian kualitatif yang berarti pengumpulan datanya menggunakan literatur atau penelitian-penelitian terdahulu, berita, dan sumber tertulis lainnya. Penelitian ini tidak menggunakan teknik perhitungan murni tetapi lebih memanfaatkan informasi dari sumber-sumber yang telah ada sebelumnya. Metode ini digunakan sesuai dengan tujuan Penulis, yaitu

[60]Sukmadinata, *Metode Penelitian Pendidikan* (Bandung: Remaja Rosdakarya, 2008), h.317.

[61]B.L. Berg, H. Lune, *Qualitative Research Methods For The Social Sciences, Ninth Edition,* (England, Essex: Pearson Education Limited, 2017), h.12.

untuk menjelaskan bagaimana kerja sama indonesia dan inggris dalam bidang keamanan siber.

3.2. Kehadiran Peneliti

Pada penelitian ini, Peneliti bertindak sebagai instrumen dan pengumpul data. Data yang digunakan merupakan data yang dikumpulkan dari sumber-sumber yang telah ada, seperti penelitian terdahulu yang berkaitan dengan penelitian yang Penulis kerjakan, literatur, buku dan jurnal. Data-data yang dikumpulkan berkaitan dengan bidang keamanan siber. Kehadiran Peneliti sangat dibutuhkan, mengingat peran Peneliti sebagai instrumen dan pengumpul data yang diperoleh dari berbagai literatur.

3.3. Lokasi Penelitian

Untuk kebutuhan literatur dan informasi, Penulis memanfaatkan teknologi untuk pengumpulan data, sebagai berikut:

a. Perpustakaan Universitas Fajar.
b. Perpustakaan *online* dari beberapa universitas di Indonesia.
c. Website resmi Lembaga Ketahanan Nasional (LEMHANAS) dan Badan Siber dan Sandi Negara (BSSN).
d. Berbagai sumber lainnya yang didapat secara online.

3.4. Sumber Data dan Teknik Pengumpulan Data

Penelitian ini menggunakan teknik pengumpulan data dengan pendekatan studi pustaka atau *literature research* dimana Peneliti menggunakan data sekunder atau data yang telah ada sebelumnya. Teknik *library research* merupakan suatu teknik yang digunakan karena

pada dasarnya setiap penelitian memerlukan bahan yang bersumber dari perpustakaan.[62]

Teknik pengumpulan data melalui studi kepustakaan merupakan suatu telaah terhadap buku-buku, literatur serta laporan-laporan yang relevan dengan topik yang diteliti. Sumber data yang digunakan adalah data sekunder, dimana data-data yang diperlukan diperoleh dari hasil penelitian yang telah ada sebelumnya atau dari literatur-literatur yang berkaitan dengan topik penelitian.[63] Sumber data sekunder adalah data yang diperoleh oleh orang lain, bukan oleh Peneliti itu sendiri. Data yang digunakan Penulis bersumber dari buku, *e-journal*, *e-book*, internet hingga *website* resmi pemerintah Republik Indonesia.

3.5. Teknik Analisis Data

Untuk dapat menganalisa serta mendeskripsikan Kerja Sama Indonesia Dan Inggris Dalam Bidang Keamanan Siber. Penulis menggunakan metode analisis isi (*content analysis*) yaitu seorang peneliti melakukan pembahasan terhadap isi satu informasi tertulis atau tercetak pada media massa.

---

[62]S. Nasution, *Metode Research: Penelitian Ilmiah* (Jakarta: Bumi Aksara, 2007), h.145.
[63]Abd Rahman Hamid, Muhammad Saleh Madjid, *Pengantar Ilmu Sejarah* (Cet.IV; Yogyakarta: Ombak, 2015), h.44-45.

Adapun teknik analisis data ini menggunakan teknik studi pustaka, interpretasi, induksi-deduksi, komparasi.[64] Penelitian dimulai dengan mengumpulkan data kepustakaan terkait penelitian tersebut kemudian peneliti akan menjelaskan terjadinya kerjasama antara Indonesia dan Inggris. Kemudian dilanjutkan dengan interpretasi yaitu peneliti mencoba memahami pengaruh kerja sama Indonesia dan Inggris dalam bidang keamanan siber sehingga dapat mencari titik fokus dari pemikiran yang dibutuhkan untuk pembahasan.

Selanjutnya peneliti melakukan analisa induksi-induksi. Sehingga peneliti turut memikirkan dan memahami proses terjadinya kerja sama Indonesia dan Inggris dalam bidang keamanan siber tanpa kehilangan objektivitasnya. Dilanjutkan kembali dengan metode komparasi yang simetris sehingga dapat diperbandingkan hal-hal yang memiliki persamaan maupun perbedaan sampai dengan dasar pemikirannya. Kemudian akan dilakukan deskripsi. Dari sini, peneliti akan menguraikan secara teratur yang menjadi bahan pembahasan dalam penelitian dengan jernih dan tepat setelah itu mereduksi data yang dilakukan dengan membuat abtraksi.[65] Abtraksi merupakan usaha membuat rangkuman tentang masalah ini.

---

[64]Lexy J. Maleong, *Metodologi Penelitian Kualitatif* (Bandung: Remaja Rosdakarya, 1999), h. 60

[65] Ibid.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Kondisi Keamanan Siber di Indonesia

Pemerintah Indonesia sangat menyadari gagasan bahwa lingkungan keamanan siber tidak dapat dibangun seorang diri melainkan lebih efektif apabila dilakukan secara bersama-sama. Sehingga Indonesia berinisiatif melakukan kerjasama dengan Inggris.

Indonesia melakukan kerjasama dengan berbagai negara dalam bidang keamanan siber, salah satunya dengan negara Inggris. Indonesia melakukan kerjasama baik dan elemen penyelenggara pertahanan siber Inggris, mampu mengidentifikasi, mendeteksi dan menganalisa serangan siber. Selain itu, dengan maraknya kasus kejahatan siber yang juga dapat berdampak pada kepentingan Inggris baik kepentingan nasional maupun kepentingan Inggris yang berada di luar negeri, maka salah satu tujuan strategis negara Inggris yakni bersedia bekerjsama secara internasional dalam menjaga keamanan siber internasional dan tujuan Inggris yakni untuk menjadi negara yang aman di dunia maya untuk melakukan bisnis. Mengapa inggris memiliki tujuan strategis tersebut, karena Inggris ingin mengembangkan bidang keamanan siber. Sehingga Indonesia diharapkan dapat mengambil hal

positif dari kemajuan teknologi Inggris terutama di bidang keamanan siber[66].

Konsep keamanan siber merujuk kepada persepsi ancaman yang dihadapi mengingat aktivitas yang terhubung melalui internet adalah borderless, namun ketika arus informasi dengan cepat maka tidak terhindarkan ancaman terhadapnya dengan semakin kompleksnya berbagai aktor yang terlibat dalam aktivitas yang terkoneksi melalui internet[67].

Keamanan Siber meliputi praktik, tindakan, dan upaya yang melindungi ekosistem dari aset-aset wadah dan Perusahaan dan pengguna serangan jahat untuk mengganggu kerahasiaan, integritas dan ketersediaan informasi atau data. Aset yang dimaksud meliputi tetapi tidak terbatas pada perangkat komputasi yang saling berhubungan, infrastruktur penting, server, jaringan dan informasi yang disimpan atau ditransmisikan dalam sistem *cybercosystem.* Mengingat interaksi di dunia Siber berdasarkan ketersediaan, integritas dan kerahasiaan informasi, perlindungan informasi dan instalasi dan infrastruktur digital menjadi semakin penting.

Badan Siber dan Sandi Negara (BSSN) melaporkan 189.957.542 juta kasus serangan siber pada Januari hingga Agustus 2020. Angka ini

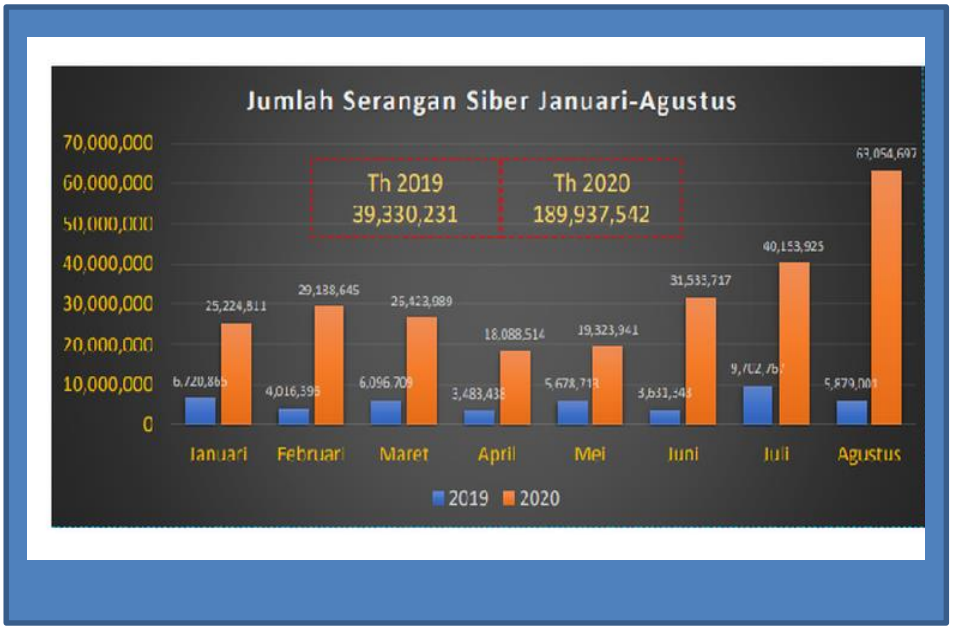
---

[66] Islami, M.J. 2017. *Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index.* Jurnal Masyarakat Telematika dan Informasi Vol. 8 No. 2 (Oktober-Desember 2017) hal. 137-144.

[67] Putri Sylvia Octa. *Mengenal Studi Hubungan Internasional*. Bandung: Zavara, 2015), h.137.

telah meningkat pesat dibandingkan dengan 39 juta kasus tahun sebelumnya. Adapun Republik Indonesia, Badan Investigasi Kriminal Polisi Nasional (Barskrim), yang mengalami peningkatan laporan kejahatan dunia maya.

Gambar 4.1 Indeks Serangan Siber di Indonesia



Sumber : Pusat keamanan siber melalui website BSSN[68]

Serangan siber merupakan serangan pada sistem komputer atau jaringan komputer untuk mendapatkan kontrol atau akses tanpa izin dari sistem komputer yang ditargetkan. Meskipun kejahatan Siber adalah kegiatan ilegal yang menggunakan dan menargetkan sistem komputer atau jaringan untuk menyebabkan kerugian material atautidak material terhadap porsi target. Semua serangan pada si pouties tidak didefinisikan

[68] Pusat Keamanan Siber <https://honeynet.ui.ac.id/badan-siber-dan-sandi-negara-bssn/>

sebagai kejahatan, tetapi serangan batang dan kejahatan dunia maya dianggap sebagai ancaman siber[69].

Kerugian dari kejahatan siber tergantung pada karakteristik korban. Untuk korban korporat, serangan siber dan kejahatan dunia maya menyebabkan kerugian ekonomi dalam bentuk pengurangan manfaat, kerugian nilai pasar, penuntutan, dan kerusakan pada reputasi. Untuk korban individu, kerugian dari serangan siber dan *cybercrime* menyebabkan dampak stres dan psikologis, pencurian identitas dan kerugian finansial. Microsoft and Frost & Sullivan (2018) melaporkan bahwa pada tahun 2017 insiden keamanan siber menyebabkan kerugian ekonomi sekitar US$ 34,2 miliar di Indonesia. Penghitungan tersebut termasuk kerugian yang bersifat: langsung-kerugian finansial dari kerugian produktivitas, denda, dan biaya perbaikan; tidak langsung-hilangnya kesempatan karena perusahaan harus membangun kembali hubungan dengan konsumen setelah reputasinya rusak dan keamanan Siber memiliki dampak mempengaruhi ekonomi dan ekosistem dalam arti luas, menghasilkan penurunan jumlah konsumen dan pendapatan[70].

Adapun Kebijakan *cyber security* di Indonesia :

[69]ITU. 2012. *Global Cybersecurity Index 2017.* International Telecommunication Unit, h.6

[70]Islami, M.J. 2017. *Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index.* Jurnal Masyarakat Telematika dan Informasi Vol. 8 No. 2 (Oktober-Desember 2017) h. 137-144.

1. Kepastian Hukum

Kebijakan *cyber-security* secara khusus di Indonesia telah diinisiasi sejak tahun 2007 dengan dikeluarkannya Peraturan Menteri Komunikasi dan Informatika No.26/ PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet yang kemudian direvisi dengan Peraturan Menteri Komunikasi dan Informatika No.16/PER/M.KOMINFO/10/2010 yang kemudian diperbaharui lagi dengan Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMINFO/12/2010. Salah satu yang diatur dalam peraturan tersebut adalah pembentukan ID-SIRTII, yang merupakan kepanjangan dari Indonesia *Security Incident Response Team on Internet Infrastructure* adalah Tim yang ditugaskan Menteri Komunikasi dan Informatika (Kominfo) untuk membantu pengawasan keamanan jaringan telekomunikasi berbasis protokol internet. Tugas dan fungsi dari ID-SIRTII diantaranya melakukan pemantauan, pendeteksian dini, peringatan dini terhadap ancaman dan gangguan pada jaringan[71].

Menurut Hasyim Gautama, kerangka hukum *cyber-security* di Indonesia saat ini dibangun diantaranya berdasarkan atas dasar UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan

[71] Pasal 9 Peraturan Menteri Komunikasi dan Informatika No. 29/PER/M.KOMINFO/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012 serta surat edaran menteri dan peraturan menteri. Terkait dengan upaya menjamin kepastian hukum dalam pengembangan *cyber-security* telah dilakukan antara lain dengan melaksanakan serangkaian program yang sudah mulai berjalan diantaranya: menginisiasi peraturan perundangundangan yang terkait dengan *cyber-security* seperti UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012, menyusun kerangka nasional *cyber-security.* Namun demikian, legalitas penanganan kejahatan di dunia cyber masih lemah karena meski telah ada peraturan perundangundangan yang melarang bentuk penyerangan atau perusakan sistem elektronik dalam UU Informasi dan Transaksi Elektronik No.11 Tahun 2008 namun belum terdapat peraturan perundang-undangan yang mengatur secara khusus *cyber crime* dan penanganan *cyber crime* padahal dilain sisi bentuk kejahatan dunia cyber semakin meningkat dan pola kejadiannya sangat cepat sehingga sulit untuk ditangani oleh aparat penegak hokum.

2. Teknis Dan Tindakan Prosedural

3. Secara nasional, menurut Hasyim Gautama terdapat sejumlah permasalah terkait dengan pembangunan *cyber-security* yang tangguh di antaranya:

a. Lemahnya pemahaman penyelenggara negara atau security terkait dengan dunia *cyber* yang memerlukan pembatasan pengunaan layanan yang servernya berada di luar negeri dan diperlukan adanya pengunaan *secured system.*
b. Legalitas penanganan penyerangan di dunia *cyber.*
c. Pola kejadian *cyber crime* sangat cepat sehingga sulit ditangani.
d. Tata kelola kelembagaan *cyber-security* nasional.
e. Rendahnya *awareness* atau kesadaran akan adanya ancaman *cyber attack* internasional yang dapat melumpuhkan infrastruktur vital suatu negara.
f. Masih lemahnya industri kita dalam memproduksi dan mengembangkan perangkat keras atau *hardware* terkait dengan teknologi informasi yang merupakan celah yang dapat memperkuat maupun memperlemah pertahanan dalam dunia cyber.

Penangganan kejahatan *cyber* yang masih parsial dan tersebar serta tidak adanya koordinasi yang baku dalam penanganan masalah *cyber security.* Rendahnya *awarenees* atau kesadaran akan adanya ancaman *cyber attack* yang berdampak melumpuhkan infrastruktur vital.

Contohnya adalah sistem radar penerbangan di bandara internasional Soekarno Hatta yang beberapa kali mengalami gangguan. Tidak menutup kemungkinan *cyber attack* menyerang infrastruktur vital negara seperti itu. Terkait dengan kebijakan *cyber-security* di Indonesia perlu diatur sebuah kebijakan yang mengatur tentang berbagai elemen yang terkait dengan *cyber-security* dalam berbagai kebijakan yang mengatur tentang sistem teknologi informasi komunikasi yang digunakan yang meliputi pengaturan perlu adanya dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait dengan keamanan informasi, standar infrastruktur yang wajib dipenuhi yang sesuai dengan standar internasional dalam menghadapi *cyber war* termasuk didalamnya adanya perimeter defense yang memadai, adanya *network monitoring system,* system information and event management yang berfungsi memonitor berbagai kejadian di jaringan terkait dengan insiden keamanan, *network security assement* yang berperan sebagai *control* dan *measurement* keamanan.

4. Struktur Organisasi

Permasalahan lainnya adalah penanganan *cyber-security* dalam kerangka pertahanan negara hingga saat ini masih bersifat sektoral dan belum terkoodinasi serta belum terpadu. Sebagai contoh seperti dijelaskan Eris Herryanto bahwa selama ini konsep *cyber*

defence yang dilaksanakan Kemhan dan TNI masih bersifat sektoral, belum menyeluruh sebagai satu kesatuan. Guna mengatasi *cyber crime,* kebijakan yang telah dilaksanakan kementerian pertahanan keamanan adalah dengan membentuk Tim Kerja Pusat Operasi Dunia Maya *(Cyber Defence Operation Centre)* yang bertujuan menjaga keamanan dan perlindungan internal (Kemhan) maupun keamanan dan perlindungan eksternal (nasional) dalam dunia *cyber. Cyber Defence Operation Centre* dalam tataran kebijakan *cybersecurity* nasional pembentukannya ditujukan untuk membangun sistem pertahanan semesta yang melibatkan seluruh warga negara, wilayah dan sumber daya nasional lainnya untuk menegakkan kedaulatan negara, keutuhan wilayah dan keselamatan segenap bangsa dari ancaman cyber. Guna menyikapi *cyber crime* yang sudah mencapai tahap memprihatinkan tersebut maka salah satu alternatif kebijakannya adalah dengan menempatkan *S* dalam kontek pertahanan. Berbagai kebijakan yang telah dilakukan terkait dengan *cyber-security* dalam konteks pertahanan di tingkat nacional antara lain, pada tahun 2010, Kementerian Pertahanan (Kemhan) memulai program penanggulangan terhadap *cyber attack* dengan membentuk Tim Kerja Pusat Operasi Dunia Maya *(Cyber Defence*

Operation Centre) yang telah menyusun rencana pembentukan Tim Penanganan Insiden Keamanan Informasi[72].

5. *Capacity Building*

   Program pelatihan dan peningkatan keahlian *cyber-security* dilakukan dalam koordinasi Tim Kerja Pusat Operasi Dunia Maya *(Cyber Defence Operation Centre).* Selain itu diperlukan pembinaan SDM tentang arti pentingnya *cyber-security* guna meningkatkan pemahaman langkah-langkah preventif dalam menangkal segala tindak *cyber crime.* Guna pengembangan kapasitas SDM dalam penangganan *cyber-security,* dalam tubuh TNI telah melakukan kerjasama dengan stakeholder yang memiliki kemampuan di bidang Informasi Teknologi diantaranya seperti kerjasama yang dilakukan oleh TNI AD dengan Institut Teknologi Del (IT Del), Sumatera Utara. Kerjasama ini direncanakan berlangsung selama tiga tahun, dari tahun 2014 sampai 2017 dalam tiga program. Ketiga program itu antara lain: penyiapan model perang *cyber,* seminar *military cyber intelligence and cyber operation, serta cyber camp atau pekan cyber.*

6. Kerjasama Internasional

[72]Eris Herryanto Pada Seminar Nasional Keamanan Infrastuktur Internet Yang Diselenggarakan Indonesia Security Incident Response Team On Internet Infrastruktur (ID-SIRTI) Di Universitas Pertahanan Di Tahun 2011.

Langkah lainnya yang dilakukan adalah dengan melakukan kerjasama internasional dengan organisasi regional maupun internasional dalam rangka penanggulangan *cyber crime.* Kerjasama dalam rangka penanggulangan *cyber crime* yang telah dilakukan Indonesia di antaranya dengan menjadi anggota ASEAN *Network Security Action Council,* menjadi anggota *International Telecommunication Union* (ITU), menjadi *steering committee Asia Pacific Computer Emergency Response Team* (APCERT), anggota dari *Forum of Incident Response and Security* (FIRST), melakukan kerja sama bilateral di *bidang cyber-security* dengan Jepang, Inggris serta beberapa negara lainnya. Terkait dengan kerjasama internasional dalam bidang *cyber-security,* Indonesia juga ikut berperan aktif dalam program *Global Cyber security Agenda* (GSA) yang diluncurkan pada *World Telecommunication and Information Society Day* 2007 yang merupakan program kerjasama internasional yang bertujuan untuk menciptakan strategi dan solusi untuk meningkatkan kepercayaan dan keamanan di tengah masyarakat informasi[73].

Dapat disimpulkan bahwa kebijakan *cyber security* di Indonesia ada 5 yaitu kepastian hukum, teknis dan tindakan prosedural, struktur organisasi, c*apacity building* dan kerjasama internasional.

[73]Menteri *Kominfo Pada "High Level Segment ITU Council 2008" Yang Membahas Cyber* security, http://www.postel. go.id/info_view_c_26_p_814.htm diakses Sabtu, 29 Januari 2022.

4.2 Bentuk Kerjasama Antara Indonesia Dengan Inggris Dalam Bidang Keamanan Siber

Pada dasarnya setiap negara berupaya untuk memenuhi kebutuhannya. Kebutuhan ini akan mendorong negara-negara ini untuk bekerja sama agar dapat memenuhi kebutuhan dan kepentingan negara-negara untuk bertahan di dunia internasional kerjasama antar negara akan terus tumbuh sesuai dengan kebutuhan milik negara, seperti masalah keamanan[74].

Keamanan siber merupakan tindakan untuk melindungi operasi sistem komputer atau integrasi data di dalamnya dari aksi-aksi kejahatan dan merupakan teknologi, proses, dan praktik yang dirancang untuk melindungi jaringan, komputer, program dan data dari serangan, kerusakan, atau akses yang tidak sah[75]. *Cyber security* juga dapat diartikan sebagai melindungi hilangnya kemampuan pemilik computer. Hal ini merupakan upaya dalam melindungi data ataupun informasi dari serangan siber[76].

Disatu sisi dengan kelebihan yang didapat dengan memanfaatkan internet di dunia siber, siber dapat juga menjadi salah satu faktor ancaman bagi keamanan ataupun kedauluatan bagi suatu negara yang disebabkan karena ruang lingkup dari siber yang dapat dimanfaatkan untuk mencuri informasi, penyebaran ide yang bersifat destruktif, maupun serangan terhadap sistem informasi di berbagai

[74]Frame, J. D. 2006. *International Business and Global Technology.* Maryland: Lexington Books,h.7
[75]Hardana, Isputra Radian Ferrari. 2019. *Membuat Aplikasi IoT: Internt of Things.* Yogyakarta: Lokomedia, h.37.
[76]Yani Y.M, Ian Montrama, Emil Wahyudin. 2017. *Pengantar Studi Keamanan.* Malang: Intrans Publishing, h.73.

bidang, seperti data perbankan, jaringan militer, bahkan sistem pertahanan Negara.

Contoh kasus yang pernah terjadi di Indonesia seperti kasus *Cybercrime. Cybercrime* atau kejahatan berbasis komputer, adalah kejahatan yang melibatkan komputer dan jaringan (network)[77]. *Cybercrime* yaitu pelanggaran yang dilakukan terhadap perorangan atau sekelompok individu dengan motif kriminal untuk secara sengaja menyakiti reputasi korban atau menyebabkan kerugian fisik atau mental atau kerugian kepada korban baik secara langsung maupun tidak langsung, menggunakan jaringan telekomunikasi modern seperti Internet[78].

Cybercrime sangat dapat mengancam suatu keamanan negara terutama negara Indonesia[79]. Di Indonesia, masalah dari *cyber crime* juga bisa dikatakan mulai diperhatikan sebagai suatu masalah yang serius. Dengan masuknya Indonesia kedalam era globalisasi, khususnya dalam hal hubungannya dengan dunia cyber, berbagai bidang kehidupan masyarakat Indonesia mulai mendapatkan pengaruh dari dunia cyber tersebut. Oleh karenanya tidaklah mengherankan bila mulai bermunculan kasus-kasus kejahatan yang berhubungan pula dengan dunia cyber tersebut.

Contoh kasusnya yaitu Dunia perbankan dalam negeri juga digegerkan dengan ulah Steven Haryanto, yang membuat situs asli tetapi

---

[77]Moore, R. 2005. "*Cyber crime: Investigating High-Technology Computer Crime,"* Cleveland, Mississippi: Anderson Publishing.
[78]Halder, D., & Jaishankar, K. 2011. *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations.* Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
[79]Steve Morgan (January 17, 2016*). "Cyber Crime Costs Projected To Reach $2 Trillion by 2019".* Forbes. Retrieved September 22, 2016.

palsu layanan perbankan lewat Internet BCA. Lewat situs-situs “Aspal”, jika nasabah salah mengetik situs asli dan masuk ke situssitus tersebut, identitas pengguna (user ID) dan nomor identifikasi personal (PIN) dapat ditangkap. Tercatat 130 nasabah tercuri data-datanya, namun menurut pengakuan Steven pada situs Master Web Indonesia, tujuannya membuat situs plesetan adalah agar publik memberi perhatian pada kesalahan pengetikan alamat situs, bukan mengeruk keuntungan.

Persoalan tidak berhenti di situ. Pasalnya, banyak nasabah BCA yang merasa kehilangan uangnya untuk transaksi yang tidak dilakukan. Ditengarai, para nasabah itu kebobolan karena menggunakan fasilitas Internet banking lewat situs atau alamat lain yang membuka link ke Klik BCA, sehingga memungkinkan user ID dan PIN pengguna diketahui. Namun ada juga modus lainnya, seperti tipuan nasabah telah memenangkan undian dan harus mentransfer sejumlah dana lewat Internet dengan cara yang telah ditentukan penipu ataupun saat kartu ATM masih di dalam mesin tiba-tiba ada orang lain menekan tombol yang ternyata mendaftarkan nasabah ikut fasilitas Internet banking, sehingga user ID dan password diketahui orang tersebut. Modus kejahatan ini adalah penyalahgunaan user_ID dan password oleh seorang yang tidak punya hak. Motif kegiatan dari kasus ini termasuk ke dalam *cybercrime* sebagai kejahatan “abu-abu”. Kasus *cybercrime* ini merupakan jenis *cybercrime uncauthorized access* dan *hacking-cracking.* Sasaran dari kasus ini termasuk ke dalam jenis *cybercrime* menyerang hak milik

(*against property).* Sasaran dari kasus kejahatan ini adalah *cybercrime* menyerang pribadi *(against person)*[80].

Dengan munculnya beberapa kasus kejahatan siber *(cyber crime)* di Indonesia telah menjadi ancaman stabilitas keamanan dan ketertiban nasional dengan eskalatif yang cukup tinggi[81]. Maraknya kasus kejahatan siber yang terjadi di Indonesia yang disebabkan karena adanya keterbatasan terkait sarana dan prasarana dalam teknologi dan kemampuan dalam menghadapi serangan siber, sehingga dalam hal ini seluruh elemen pertahanan keamanan kedaulatan Indonesia harus terus menerus meningkatkan sistem pertahanan dan keamanan siber serta peningkatan akan kemampuan kapasitas dan kuantitas dari sisi teknologi informasi dan komunikasi serta sumber daya manusia.[82]

Tindak kejahatan dalam dunia siber, tidak hanya dialami oleh Indonesia, namun, Inggris turut menjadi salah satu negara sasaran serangan siber. Dilaporkan bahwa ditahun 2017, aktvitas bisnis di Inggris mengalami serangan siber dengan rata-rata serangan sebanyak 230.000 serangan siber Teknik serangan yang dilakukan pada aktivitas bisnis Inggris sebagian besar menggunakan teknik *malware, virus, spyware,* yang mencari kelemahan web sehingga dapat menemukan jalan masuk pada akses komputer perusahaan bisnis Inggris. Inggris yang hampir secara keseluruhan aktivitas bisnisnya terhubung secara langsung pada *internet of thing,* memberikan akses masuk bagi pelaku tindak kejahatan siber untuk melancarkan serangan pada perusahaan bisnis Inggris.

---

[80]Bima Guntara Op cit, h. 243.
[81]Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime*), (Jakarta: Refika Aditama, [t.th]), h.131.
[82]Vishnum, Op.Cit.

Contoh kasus yang pernah terjadi di Inggris seperti kasus *Cybercrime. Cybercrime* sebagai suatu jenis kejahatan merupakan suatu tindakan yang dilakukan di dalam dunia yang tidak mengenal batas wilayah hukum dan kejahatan tersebut dapat terjadi tanpa perlu adanya suatu interaksi langsung antara pelaku dengan korbannya. Sehingga dapat dikatakan, bahwa ketika suatu kejahatan cyber terjadi, maka semua orang dari berbagai negara yang dapat masuk ke dalam dunia cyber dapat terlibat di dalamnya, entah itu sebagai pelaku (secara langsung atau tidak langsung), korban, ataupun hanya sebagai saksi[83].

Contoh kasusnya yaitu *cybercrime,* terjadi pertama kali di Amerika Serikat pada tahun 1960-an[84]. Pada tahun 1970 di Amerika Serikat terjadi kasus manipulasi data nilai akademik mahasiswa di Brooklyn College New York, kasus penyalahgunaan komputer perusahaan untuk kepentingan karyawan, kasus pengkopian data untuk sarana kejahatan penyelundupan narkotika, kasus penipuan melalui kartu kredit. Selain itu terjadi pula kasus akses tidak sah terhadap database security pacific national bank yang mengakibatkan kerugian sebesar $10.2 juta US pada tahun 1978. Selanjutnya kejahatan serupa terjadi pula disejumlah negara antara lain Jerman, Australia, Inggris, Finlandia, Swedia, Austria, Jepang, Kanada, Belanda, dan Indonesia.

---

[83]Bima Guntara, Legitimasi Penyebaran Informasi Yang Memiliki Muatan Penghinaan Dan/Atau Pencemaran Nama Baik Dalam Pasal 310 Kuhp Dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan, Volume 4 Nomor 2 Desember 2017, hal. 242.

[84]Edy Junaedi Karnasudirja, 1993, Jurisprudensi Kejahatan Komputer, (Jakarta: Tanjung Agung, 1993), hal. 3. Sebagaimana dikutip oleh Hj Sri Sumarwani, Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif, Jurnal Pembaharuan Hukum Volume I. No. 3.

Kejahatan tersebut menyerang terhadap harta kekayaan, kehormatan sisitem dan jaringan komputer[85].

Tindakan kejahatan ini berdampak pada perekonomian Inggris, sehingga Pemerintah Inggris menginvestasikan biaya yang tinggi untuk perlindungan, pertahanan dan keamanan ketahanan siber bagi kepentingan bisnis Inggris maupun keamanan nasional Inggris lainnya.

Indonesia dan di Inggris terdapat serangan siber yang dilakukan oleh pelaku tindak kejahatan siber. Dari tindakan serangan siber tersebut, akan menimbulkan dampak yang buruk bagi kedua negara tersebut, terutama pada perekonomian.

Tindak kejahatan siber di Indonesia dan di Inggris dapat menimbulkan kerugian. Namun dengan maraknya kasus kejahatan siber yang terjadi di Indonesia dan Inggris yang disebabkan karena adanya keterbatasan terkait sarana dan prasarana dalam teknologi dan kemampuan dalam menghadapi serangan siber, sehingga dalam hal ini seluruh elemen pertahanan keamanan kedaulatan Indonesia dan Inggris harus secara terus-menerus dalam meningkatkan sistem pertahanan dan keamanan siber[86]. Keunggulan keamanan cyber Inggris yaitu adanya sumber daya yang mendukung sehingga akan mampu mengidentifikasi, mendeteksi, memberikan perlindungan dan pertahanan, serta mampu menanggapi atau menentukan sikap dalam mengambil tindakan saat sebelum dan terjadi serangan pada dunia maya serta mampu dalam

[85]Alexander Pattipeilohi, “Di Balik Kecanggihan Sebuah Teknologi”. “Majalah Komputer dan Elektronika, 1985, hal. 42. Sebagaimana dikutip oleh Hj Sri Sumarwani, Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif, Jurnal Pembaharuan Hukum Volume I. No. 3.

[86]Ghernaouti-Hélie, S. (2009). *Cybersecurity Guide for Developing Countries (Enlarged Edition ed.).* Geneva: International Telecommunication Union.

mendukung pemulihan serangan siber sehingga mampu meminimalisir dampak yang diakibatkan dari serangan siber yang dilakukan dan Inggris menawarkan sejumlah teknologi serta bantuan pendanaan pembaunan kapasistas kepada Indonesia.

Sehingga dari permasalahan tersebut, itulah alasan mengapa Indonesia dan Inggris melakukan kerjasama dalam bidang keamanan siber. Kerjasama dalam bidang keamana siber yang diinisiasi secara langsung oleh Inggris merupakan salah satu kepentingan negara Inggris untuk mewujudkan salah satu *national strategy* yakni bersedia bekerjasama secara internasional untuk menjadi negara yang aman di dunia maya untuk melakukan bisnis.

Kerjasama antara Indonesia dan Inggris dalam bidang keamanan siber merupakan suatu kerjasama yang terlaksana ditahun 2018. Dimana kerjasama dalam bidang keamanan siber ini diinisiasi langsung oleh Pemerintah Kerajaan Inggris ke Badan Sandi dan Siber Negara Indonesia pada bulan Agustus 2018. Untuk menyepakati dan mengukuhkan kerjasama dalam bidang keamanan siber, maka pada 14 Agustus 2018 penandatanganan Memorandum Saling Pengertian Antara Pemerintah Republik Indonesia dan Pemerintah Kerajaan Inggris dalam bidang keamanan siber pada 14 Agustus 2018[87].

Kepala Badan Siber dan Sandi Negara, Dr.Djoko Setiadi, M.Si. baru saja melaporkan nota kesepahaman (memorandum pemahaman) dengan pemerintah Inggris dalam hal kerjasama di sektor keselamatan Siber (keamanan *cyber*). Momen bersejarah ini berlangsung pada acara

[87]Triwahyuni Dewi. Wulandari TA. 2016. *Strategi Keamanan Cyber Amerika Serikat.* Diakses dari https://search.unikom.ac.id/index.p hp/jipsi/article/view/239

pertemuan Wamenlu Abdurrahman Mohammad Fachir dengan Menteri Muda Urusan Asia dan Pasifik Kementerian Luar Negeri Inggris Raya yaitu The Rt. Hon. Mark Field, MP, pada hari Selasa 14 Agustus 2018 di Kantor Kementerian Luar Negeri, Jakarta Pusat. Dalam kegiatan tersebut, Kepala BSSN bertemu dengan The Rt. Hon. Mark Field, MP menandatangani kerjasama di bidang keamanan siber yang meliputi[88]:

4.2.1 **Implementasi dan Pengembangan Strategi Keamanan Siber Nasional**

Indonesia dan Inggris sepakat untuk mengatur pertukaran informasi dalam persiapan kebijakan keamanan nasional Siber dan permintaannya. Kolaborasi ini harus berkontribusi pada persiapan standar terutama pada pengembangan strategi kemanan siber khsusunya peningkatan kapasitas SDM keamanan siber terutama bagian ITE. Talent Pool Born to control: Gladiator Cyber Security Indonesia (GCSI). Peningkatan kemampuan keamanan siber dengan target penjaringan 10.000 kandidat untuk peningkatan kapasitas keamanan siber yang lebih terarah. Kemudian pada Bimbingan teknis keamanan informasi kepada Lembaga terkait Edukasi Publik, konten berkualitas, pemahaman kebhinekaan, dan anti terorisme. Kemudian diterapkan di media sosial dengan target pengguna twitter dan isntagram di Indonesia.[89]

---

[88] Ibid.

[89] Fitratun komariah 'RI-Inggris Perkuat Kolaborasi dalam Bidang Keamanan Siber' Rri.id. 2019 <https://rri.co.id/internasional/1257177/ri-inggris-perkuat-kolaborasi-di-bidang-siber-dan-keamanan> (diakses 26 Maret 2022)

Keuda negara juga berkolaborasi dalam mengidentifikasi area yang harus diperbaiki dalam serangan siber, dan meningkatkan tingkat komitmen keseluruhan terhadap keamanan siber di kedua negara. Pengembangan strategi kemanan siber indonesia dan inggris melakukan peltihan profesional kemanan siber khsususnya bagi lembaga BSSN terutama yang mengelola ITE kemudian membuat edukasi publik mengenai pentingnya kemanan siber melalui media sosial.

Berdasarkan implementasi tersebut program yang dilakukan kedua negara masih belum maksimal karena strategi kemanan siber masih yang jarang di ketahui oleh masyarakat umum, kemudian edukasi melalui media sosial kurang menarik bagi masyarakat indonesia karena kurna tidak dapat dirasakan langsung contohnya seperti BSSN turun ke Sekolah menengah atas, kampus dan masyarakat umum kemudian menjelsakan secara langsung kepada audience.

4.2.2 **Pengelolaan Insiden Siber**

Substansi kerja sama ini dikhususkan untuk pengambilan tindakan tindakan dalam memanipulasi insiden Siber, salah satunya adalah menukar titik kontak masing-masing negara sebagai pintu koordinasi awal. Pertukaran Poin Kontak berfungsi sebagai mekanisme untuk berkonsultasi dan berkoordinasi ketika insiden siber adalah global atau di negara masing-masing untuk mengetahui bentuk-bentuk serangan masing-masing, ini dapat memfasilitasi kompilasi solusi bersama.

Memberikan layanan reaktif dengan melaksanakan koordinasi insiden, triase insiden, dan resolusi insiden; Kedua, memberikan

layanan proaktif yakni dengan mempublikasikan informasi kerawanan, keamanan, dan tren teknologi; Dan ketiga, memberikan layanan peningkatan kualitas keamanan berupa konsultasi, *cyber drill*, pelatihan, dan *workshop*. Terutama dalam melakukan penanggulangan dan pemulihan.

Dengan demikian Indonesia dapat memiliki visibilitas yang menyeluruh terhadap aset siber guna melakukan aksi respon yang lebih cepat, sehingga waktu respon dan pemulihan terhadap insiden siber menjadi lebih efektif dan efisien.[90]

Secara kelembagaan berdasarkan kerja sama ini khususnya pengelolan siber sudah cukup lengkap karena dari segi pencegahan serangan siber kedua negara bertukan kontak titik kordinasi serangan untuk mengetahui titik atau poin pada serangan global maupun serangan ke negara masing-masing, pengelolaan siber juga berdampak pada peningkatan pelayanan yang bersifat konsultasi, dan *cyber drill.*

4.2.3 **Kejahatan Siber**

Cybercrime atau kejahatan siber didefinisikan sebagai sebuah kejahatan di dunia maya dengan memanfaatkan terhubungnya internet dan teknologi siber atau teknologi informasi bisa berupa komputer, telepon genggam yang disalahgunakan untuk menyerang komputer lain yang terhubung juga ke dalam internet dan menyebabkan kerugian kepada korban. Bidang *cybercrime* dan penegakan hukum saat ini di Kepolisian Nasional Republik

[90]<https://bssn.go.id/cegah-insiden-siber-di-parlemen-bssn-dan-dpr-luncurkan-csirt-dpr/> (diakses 26 Maret 2022)

Indonesia. Namun, poin inti kerjasama ini adalah *join exercise* dalam upaya penguatan kapasitas di bidang *cyber forensics* dan kemampuan investigasi barang bukti digital sehingga cepat mendat jejak digital dari para pengguna komputer maupu telepon genggam di mana tugas ini diemban oleh salah satu Deputi di BSSN.

Cybercrime diklasifikasikan penggunaan teknologi komputer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer maka dalam kerja sama ini seluruh elemen pertahanan keamanan kedaulatan Indonesia harus terus menerus meningkatkan sistem pertahanan dan keamanan siber serta peningkatan akan kemampuan kapasitas dan kuantitas dari sisi teknologi informasi dan komunikasi serta sumber daya manusia.

Berdasarkan poin terhadap kejahatan siber indonesia berusaha meningkatkan peningkatan kapasitas siber forensik untuk melihat jejak digital yang dilakukan kepada korban, karena kejahatan siber ini dilakukan menggunakan teknologi berbasis komputer, laptop dan *handphone.* Semua yang berhubngan dengan teknologi pasti memiliki jejak digital dan bisa dilacak kembali tergantung tingkat kemanan yang dimiliki oleh pelaku.

4.2.5 **Peningkatan/pengembangan Kapasitas**

Bekerja sama dengan Inggris Pemerintah Indonesia akan melakukan penelitian dengan akademisi di kedua negara untuk mendukung pengembangan penelitian di negara ini, terutama sektor keamanan Siber. Selain itu, melalui titik kerja sama ini, pemerintah Indonesia dengan Inggris dapat menjalin kerja sama dalam industri Siber, yang tentu saja dikonsolidasikan oleh BSSN.

Pada *cyber dialog forum* topic utama yang menjadi pembahasan adalah Pengembangan Kapasitas. Pelaksanaan Pengembangan Kapasitas dilakukan oleh Kedutaan Besar Inggris. Dikarenakan sudah adanya payung MoU dengan Badan Sandi dan Siber Negara, maka pelaksanaan Peningkatan Kapasitas melibatkan Badan Sandi dan Siber Negara.

Peningkatan Kapasitas ini dicoba dengan 2 program pembahasan yakni *Cyber Law* dan *Cybersecurity Awareness.* Pada pembahasan *cyber law*, kemudian membahas terkait *United Nations Group of Governmental Experts* (UN GGE). Yang mana Indoensia dan Inggris menjadi Anggota Kelompok Ahli Pemerintahan yang dibentuk oleh Perserikatan Bangsa-Bangsa (PBB) yang bertujuan untuk meningkatkan dan memajukan perilaku negara untuk bertanggungjawab di dunia siber dalam rangka menjaga keamanan internasional.

Berdasarkan kolaborasi ini menunjukkan bahwa indonesia inggris sangat berkomitmen dalam peningkatan dan pengembangan kapasitas melalui cyber law dan cyber security awarness. Program ini juga bisa meanambah pengetahuan secara

berkala tidak monoton menganai srangan siber, pencegahan siber melainkan belajar mengenai tentang hukum siber dan peningkatan kesadaran kemanan siber.

Fokus perhatian pada pembahasan terkait *United Nations Group of Governmental Experts* (UN GGE) adalah peningkatan kapasitas, norma-norma yang mengikat terkait perilaku suatu Negara dalam dunia siber, peningkatan kepercayaan antar negara dalam melakukan kerjasama keamanan siber baik bersifat bilateral maupun multilateral Selain diskusi terkait *United Nations Group of Governmental Experts* (UN GGE), poin yang turut dibahas adalah Tallin Manual 2.0. Tallin Manual 2.0 berfokus pada operasi siber yang dilakukan oleh negara dan mengkaji kerangka hokum internasional yang dapat diberlakukan dalam operasi serangan siber.

Pada konteks ini, pemerintah Inggris berusaha untuk menggambarkan Tallinn Manual 2.0 (buku yang membahas mengenai opresi siber) yang menjadi pedoman yang komprehensif dalam mengatur operasi siber. Ini adalah diskusi tentang kerjasama dalam bentuk Siber yang dilakukan oleh Indonesia dan Inggris, karena sejauh ini, Tallinn Manual 2.0 belum diperhitungkan pemerintah Indonesia dalam mengambil kebijakan keamanan Siber. Karena, Indonesia tidak terlibat dalam perumusannya, sehingga tidak diketahui apakah kepentingan nasional Indonesia bisa tercakup di dalamnya atau tidak. Jadi, Tallin

Manual 2.0 masih merupakan studi bagi Indonesia untuk melihat apakah manual Tallin 2.0 dapat menjadi jembatan bagi Indonesia untuk memenuhi kepentingan Indonesia, terutama di bidang keamanan siber[91].

Pembahasan berikutnya yakni terkait *Cyber security Awarenes*. Pembahasan pada poin ini mengarah pada peningkatan pemahaman keamanan siber seperti berita hoaks, pengamanan informasi pribadi serta isu privasi, selain itu cakupan yang menjadi pembahasan dalam *cybersecurity awareness* yakni teknik menganalisis dan menginvestigasi malware, memahami strategi dan juga taktik dalam menemukan gangguan dan kerentanan serta *incident hadling* yang dapat dikatakan sebagai tindakan pertama yang perlu dilakukan apabila terjadi serangan siber maka pemerintah atau instansi terkait dapat menangani baik berupa mendeteksi serangan, menangani ataupun memberikan respon serta mempelajari insiden yang terjadi pada keamanan siber.

Dialog kerjasama ini menegaskan komitmen kedua negara untuk terus meningkatkan hubungan kerjasama antara Indonesia dan Inggris dalam bidang keamanan siber dan memiliki kesepahaman terkait isu-isu siber, selain itu kedua peserta juga mengungkapkan keprihatinan terkait meningkatnya angka serangan siber serta dampak yang ditimbulkan. Kedua Negara mengakui bahwa sangat penting kolaborasi antar semua

[91] Monica Romauly Weu. *Kerjasama Pemerintah Indonesia Dan Pemerintah Kerajaan Inggris Dalam Bidang Keamanan Siber.* Global Political Studies Journal Volume 4 Nomor 2 Edisi Oktober 2020 P-ISSN 2301-749X E-ISSN 2686-2905, h.161.

pihak dalam menangani kejahatan siber. Pada akhir dialog tersebut, delegasi Inggris berterimakasih kepada Indonesia karena sudah menjadi tuan rumah untuk penyelenggaraan *cyber dialog* forum.

Kerjasama ini masih dalam bentuk pembahasan dan belum diimplementasikan kedalam suatu tindakan yang nyata seperti pelatihan bersama. Namun dengan kerjasama ini kedua peserta dapat saling berbagi informasi dalam membantu dan mengembangkan pemahaman organisasi ataupun instansi terkait keamanan siber pada saat melakukan pengelolaan data, sistem, aset termasuk sumber daya manusia.

Adanya sumber daya yang mendukung dan mumpuni, sehingga akan mampun mengidentifikasi, mendeteksi, memberikan perlindungan dan pertahanan,serta mampu menanggapi atau menentukan sikap dalam mengambil tindakan saat sebelum dan terjadi serangan pada dunia maya serta mampu dalam mendukung pemulihan serangan siber sehingga mampu meminimalisir dampak yang diakibatkan dari serangan siber yang dilakukan[92].

Dapat di anilisis bahwa bentuk kerjasama antara Indonesia dengan Inggris dalam bidang keamanan siber, meliputi Implementasi dan Pengembangan Strategi Keamanan Siber Nasional, pengelolaan insiden siber, kejahatan siber, pelatihan/Kampanye Kesadaran Keamanan Siber dan pengembangan kapasitas. Dengan adanya hubungan kerjasama

[92] Ibid.,162.

Indonesia dan Inggris pada bidang keamanan siber, kerjasama ini akan membuka peluang-peluang baru bagi kedua negara, mempererat hubungan persahabatan kedua negara, dan membangun komitmen yang kuat untuk kedua negara dalam menjaga keamanan siber di masing-masing negara dan juga keamanan internasional.

Adanya kesamaan tujuan atau kepentingan bersama merupakan hal yang wajib dalam kerjasama. Tidak dipungkiri bahwa dalam kerja sama selalu terdapat benturan kepentingan masing-masing negara, namun selama tujuan bersama dapat disepakati, sejauh itu pula kerjasama dapat terus berjalan.

4.3. Kepentingan Indonesia dan Inggris Dalam Melakukan Kerjasama Dalam Bidang Keamanan Siber

4.3.1. Kepentingan Indonesia

Ancaman siber ataupun serangan siber seringkali mengincar objek-objek vital suatu negara sehingga menyebabkan kerugian besar yang harus ditanggung oleh berbagai pihak. Pemerintah Indonesia memahami bahwa ancaman dunia Siber adalah tantangan yang akan berdampak pada ekonomi dan keamanan negara yang dapat mengganggu kedaulatan Indonesia, karena penulis *cybercrime* akan terus berjuang dari mengganggu, bahkan Investigasi sektor pemerintah, swasta, perusahaan dan individu. Oleh karena itu perlu untuk

memperkuat sumber daya manusia dan kemampuan untuk meningkatkan keamanan siber.

Namun, perlu juga dibutuhkannya kerjasama internasional untuk memerangi kejahatan siber yang bersifat internasional, sebab kejahatan siber tidak hanya berasal dalam internal suatu negara tetapi juga berasal dari luar negara. Sehingga, Indonesia perlu menguatkan strategi keamanan siber nasional Indonesia lebih efektif, sehingga dapat dijalankan dan dimaksimalkan dengan baik.

Dengan adanya peningkatan keamanan siber melalui kerja sama negara internasional ataupun pemanfaatan organisasi internasional sebagai wadahnya. Maka Indonesia telah menunjukan eksistensinya dalam berkomitmen, serta menunjukan kemampuan negara dalam menyelesaikan sebuah isu permasalahan. Kerja sama seperti ini juga menjadi media dalam memperlihatkan kontribusi atau sumbangsih Indonesia dalam menjaga dan mempertahankan kedamaian dunia[93].

Namun, pada strategi keamanan siber Indonesia, terdapat beberapa sektor yang belum dapat diberdayakan secara maksimal yakni Sektor Pemerintah yang mencakup Kementerian Negara dan Lembaga Pemerintah, Sektor Usaha atau Bisnis yang mencakup Perbankan dan *e-commerce*, Sektor Akademisi yang mencakup Perguruan Tinggi dan Praktisi, Sektor Komunitas seperti Hacker. Dapat disimpulkan bahwa,

[93]Jackson, R., & Sorensen, G. 2013. *Introduction to International Relations*. United Kingdom: Oxford University Press, h.55.

beberapa faktor tersebut merupakan salah satu dari sekian kepentingan Indonesia dalam keamanan siber yang dapat dipenuhi ketika bekerjasama dengan Inggris, berikut kepentingan Indonesia dalam melaksanakan kerjasama siber dengan Inggris:

a. Penguatan pemahaman dan keterampilan keamanan siber di bidang pendidikan.

Strategi Keamanan Siber Nasional Pemerintah Inggris adalah melindungi dan mempromosikan Inggris dalam dunia digital, strategi ini menjelaskan bahwa pemerintah akan bekerjasama dengan pihak industri dan juga para akademisi untuk membuat Inggris lebih tahan terhadap serangan dunia maya. Sehingga, Pemerintah Inggris semakin menguatkan pemahaman dan keterampilan keamanan siber di bidang pendidikan. Ini bertujuan untuk meningkatkan kualitas dan tingkat penelitian tentang pelatihan pascasarjana; memudahkan bagi para akademisi dalam melakukan proses identifikasi, Memfasilitasi akademisi dalam proses mengidentifikasi penelitian keselamatan di dunia maya dan pelatihan terbaik pada program pascasarjana yang ditawarkan oleh Pemerintah Inggris terkait dunia siber. Dengan mengoptimalkan kemampuan para akademisi terkhususnya bidang keamanan siber, akan memberikan kemudaham bagi pemerintah Inggris dalam mengembangkan visi dan tujuan bersama di antara komunitas penelitian keamanan siber Inggris baik di dalam dan di luar akademisi, dan membantu warga Inggris lebih memahami bagaimana

melindungi diri di dunia maya dan membantu pemerintah dan industri untuk mengembangkan teknologi baru yang bekerja untuk melindungi infrastruktur kritis Inggris[94].

Indonesia bisa belajar dari Inggris, bagaimana cara mengembangkan, dan memaksimalkan kemampuan para akademisi terlebih pada bidang keamanan siber untuk mampu berkolaborasi dengan Pemerintah, Industri, dan kelompok komunitas masyarakat dalam melakukan pendekatan-pedekatan tertutama pada masyarakat awam dalam memberikan pemahaman dan pengetahuan bahkan memberikan langkah-langkah terkait keamanan siber yang dapat dilakukan secara berkesinambungan. Dengan demikian, kolaborasi ini dapat memberikan informasi, pengetahuan dalam pemahaman terdalam tentang pemerintah Indonesia, khususnya pemerintah, partisi Siber dan kata sandi negara akan membuat dan mengatur strategi keamanan Siber Nasional. Indonesia. Namun, untuk mendukung penguatan sektor ini, ini tentu saja membutuhkan dukungan dan pendekatan untuk semua media multi-partisioner.

b. Memperkuat kerjasama Pertahanan Siber di sektor pemerintahan

Pemerintah Indonesia menilai bahwa melalui kerjasama ini Indonesia dapat belajar dari Pemerintah Inggris khususnya *Government Communications Headquarters* (GCHQ) dalam

[94]Monica Romauly Weu, Loc. Cit.

mengelola keamanan siber di sektor pemerintahan. Pada sektor pemerintahan, *Government Communications Headquarters* (GCHQ) akan berusaha untuk mengidentifikasi ancaman-ancaman yang menyerang dan akan memainkan peran utama yang berkolaborasi dengan pemerintah untuk melindungi Inggris dari ancaman-ancaman tersebut.

Diharapkan bahwa setiap sector pemerintahan dapat bekerjasama dengan baik dalam mengatur dan mengelola keamanan siber, terkhususnya pihak Badan Siber dan Sandi Negara Indonesia sebagai kontak utama untuk mampu bersinergi secara efektif dengan instansi pemerintahan yang lain dalam menciptakan kondisi keamanan siber yang kondusif untuk menjaga keamanan siber Indonesia.

c. Meningkatkan keamanan siber infrastruktur kritis Indonesia

Infrastruktur Kritis adalah aset, jaringan, atapun sistem yang sangat penting, dan jika mengalami gangguan akan berdampak langsung pada kestabilan perekonomian negara, keamanan, dan keselamatan warga masyarakat. Indonesia memiliki infrakstruktur kritis nasional seperti sector keuangan dan perbankan, transportasi, energi, pertahanan, intelijen dan keamanan, telekomunikasi, kesehatan, *e-governance,* industri kritis.

Sektor-sektor infrastruktur kritis nasional yang saling berhubungan atau terhubung dengan *cyberspace* akan memiliki dampak berbahaya jika tidak diimbangi dengan perlindungan terhadap infrastruktur

nasional. Melalui kolaborasi ini, Indonesia dapat belajar dari Inggris sehubungan dengan privasi dan mengamankan infrastruktur Inggris Krtitis United. Keamanan infrastruktur nasional kritis Inggris dikelola oleh *Her Majesty's Government* (HMG), dimana *Her Majesty's Government* (HMG) akan melakukan kontrol keamanan personil minimum dan melakukan pemeriksaan keamanan nasional. HMG telah menerbitkan kebijakan di semua bidang pemerintah dan infrastruktur nasional harus mencakup dan melalui proses inspeksi dasar, serta perlindungan infrastruktur nasional[95] Inggris berkolaborasi dengan HMG dalam menerbitkan pedoman dan pembuatan pedoman. Saran untuk perlindungan terhadap infrastruktur kritis nasional Inggris. Dihadapkan pada kepentingan nasional tersebut, sangat perlu untuk mengukur, mengantisipasi, memahami, mengkaji, dan menyiapkan tindakan yang dibutuhkan dalam menangani kondisi-kondisi di bidang siber. Oleh karena itu diperlukan penyusunan suatu pedoman pertahanan siber sebagai acuan yang digunakan untuk persiapan, pembangunan, pengembangan dan penerapan pertahanan siber.

4.3.2. Kepentingan Inggris

Bagi pemerintahan Inggris, kemakmuran ekonomi dan kesejahteraan sosial merupakan salah satu hal yang bergantung pada keterbukaan dan keamanan jaringan, sehingga sangat penting bagi

[95]Monica Romauly Weu, Op. Cit,.163.

pemerintahan Inggris untuk bekerjasama secara internasional yang dapat dilaksanakan melalui kerjasama secara bilateral maupun multilateral atau bahkan mendukung organisasi internasional untuk memastikan keamanan siber ataupun keamanan dunia maya yang berdampak secara langsung pada perekonomian dan kesejahteraan Inggris.

Pemerintah Inggris menyadari bahwa, salah satu faktor tinggi dari serangan Siber yang menyerang Inggris tidak hanya dalam lingkup internal, tetapi juga berasal dari ruang lingkup eksternal *attaceptant*. Sehingga untuk melindungi kepentingan nasional Inggris baik yang berasal dari dalam negara maupun kepentingan Inggris yang berasal dari luar negara, maka Inggris akan terus memastikan keberlangsungan hukum internasional di dunia maya, berlakunya hak asasi manusia secara online, kesepakatan para pemangku pentingan dalam mengelola dan mengoperasikan pengaturan internet.

Kerjasama dalam bidang keamanan siber yang diinisiasi secara langsung oleh Inggris merupakan salah satu kepentingan negara Inggris untuk mewujudkan salah satu National Strategy 2016-2021 yakni bersedia bekerjasama secara internasional untuk menjadi negara yang aman di dunia maya untuk melakukan bisnis.

Adapun tujuan Inggris yakni menjaga keamanan dunia siber yang bebas, terbuka, damai, dan aman serta mendorong pertumbuhan ekonomi dan mendukung keamanan nasional Inggris. Dengaan

demikian, Inggris bekerjasama secara internasional dengan memperoleh berbagai sumber informasi terkait ancaman dan praktik penyerangan yang terus berkembang saat ini dan masa mendatang, maka Inggris bekerjasama secara internasional dengan melakukan latihan dan mengembangkan standar keamanan siber, memberikan pendanaan bagi Negara lain yang menjadi rekan kerjasama Inggris, dan bekerjasama dalam menegakkan hukum internasional terkhusus pada keamanan siber. Dalam hal ini, Inggris akan terus bekerja sama secara internasional untuk terus memastikan keamanan dan kemakmuran Inggris di masa depan melalui aturan yang disepakati secara internasional.

Untuk mencapai tujuan-tujuan tersebut, Inggris menginisiasi secara langsung kerjasama internasional secara bilateral dengan pihak Indonesia. Hal ini dikarenakan tingginya angka serangan siber di Indonesia, dan masih terbatasnya kapasitas keamanan siber Indonesia. Dalam kerjasama ini, Inggris menawarkan sejumlah teknologi serta bantuan pendanaan pembaunan kapasistas kepada Indonesia, namun hal ini tidak secara langsung diterima oleh pihak Indonesia dikarenakan perlu adanya pembahasan lebih lanjut serta persetujuan terkait bantuan yang diberikan tersebut. Selain itu, kerjasama siber dengan Indonesia,

akan menjadi kesempatan bagi Inggris untuk melihat peluang-peluang yang ada pada dunia siber di wilayah Indonesia[96].

Tujuannya adalah untuk membangkitkan perekonomian pasar digital sekaligus membuka peluang bisnis Inggris secara internasional. Pemerintah Inggris melihat peluang dan juga potensi yang ada pada Indonesia yang dapat dijadikan suatu keuntungan bagi Inggris terutama bagi perusahaan Inggris yang bergerak pada bidang penyedia layanan yang berkaiatan dengan keamanan siber dan juga teknologi informasi dan komunikasi. Tetapi selain itu, kepentingan Inggris untuk mengumpulkan data penting yang mempengaruhi keberlanjutan negara mereka dan menyediakan informasi dan data-data yang dibutuhkan bagi Pemerintah Inggris terkait perkembangan suatu negara yang dilakukan oleh intelijen Inggris[97]. Data-data yang dibutuhkan tersebut berhubungan dengan pengambilan keputusan ataupun kebijakan suatu Negara terkait politik, ekonomi, peta kekuatan dibidang pertahanan dan keamanan seperti informasi terkait angkatan bersenjata bahkan keamanan siber serta hukum.

Badan intelijen Inggris yang ditempatkan diluar dari wilayah kedaulatan nasional Inggris akan bertanggungjawab secara langsung kepada Kementerian Luar Negeri Inggris seperti *Secret Intelligence Service* (SIS-MI 6), dan *Government Communications Headquaters*

[96] Ibid,. 164.
[97]Ibid,. 165.

(GCHQ), sehingga Pemerintah Inggris dapat dengan mudah untuk menentukan arah kebijakan luar negeri. Selain itu, Badan Intelijen Inggris akan meningkatkan keselamatan dan demonstrasi data di mana kecerdasan negara lain tidak dapat meretas sistem informasi data dan bahkan komunikasi yang dilakukan oleh Pemerintah Inggris walau secara elektronik. Semua data yang diperoleh berasal dari persebaran anggota intelijen Inggris yang kemudian dilaporkan atau diolah melalui pemantauan dari semua system teknologi informasi dan komunikasi yang bersifat elektronik seperti internet. Sehingga jelas bahwa, Inggris menawarkan kerjasama keamanan siber dengan Indonesia tidak hanya sebatas untuk mengurangi tindak kejahatan siber, namun juga untuk memperoleh keamanan dan kerahasian data yang dimiliki oleh Indonesia. Data-data serta informasi tersebut akan sangat berguna bagi Pemerintah Inggris untuk mampu memetakan kekuatan keamanan siber Indonesia, Inggris mampu mengetahui adanya tindakan penyerangan ataupun ancaman terhadap keamanan nasional Inggris sehingga mampu mencari solusi dan melakukan tindakan pencegahan apabila terjadi penyerangan[98], selain itu Pemerintah Inggris berusaha untuk memperoleh informasi secara langsung yang akan digunakan untuk keperluan negosiasi dan diplomasi.

[98]Ibid, 166.

BAB V

PENUTUP

5.1 Kesimpulan

Globalisasi membawa dampak perubahahan yang pesat khsusunya 3 dalam bidang teknologi khsususnya dalam kejahatan digital atau kejahatan siber maraknya media sosial menjadi tantangan bagi semua bangsa dalam berhati-hati dalam melakukan aktivitas karena segalanya dapat di publish dan akan menjadi kosnsumsi publik.

Masalah kemanan siber menjadi masalah yang serius dan tidak mudah dihadapi dengan negara indonesia karena tindakan kriminal siber tidak mengenal batas wilayah hukum dan kejahatan ini bisa terjadi tanpa perlu adanya suatu interaksi langsung antar pelaku dengan korbannya. , terlebih serangan siber ke indonesia dari luar negeri sehinnga sangat sulit untuk mendeteksi tapi tidak sedikit juga serangan dalam negeri, serangan dalam negeri biasa dipicu oleh perbedaan dukungan politik dan kelompok sehingga membuat berita hoax. Keamanan siber mempunyai fungsi atau peran untuk menemukan, memperbaiki, ataupun mengurangi tingkat risiko terjadinya ancaman siber dan serangan siber serta semua aktivitas yang berpotensi mengancam keamanan seluruh komponen sistem siber itu sendiri.

Adanya kerja sama ini dengan bertujuan memperkuat kelembagaan keamanan siber dalam wujud pusat keamanan siber nasional sebagai rujukan utama dalam penanganan ancaman keamanan siber. Lemabaga yang bertugas dalam kemanan siber dalam hal ini BSSn berusaha untuk

melindungi dan mencegah serangan siber dengan melakukan kerja sama bidang kemanaan siber dengan inggris untuk memajukan teknologi, kapabilitas sumber daya manusia dengan kerja sama ini indonesia bisa mempelajari teknologi yang didapatkan dari inggris dan dapat dikembangkan. Kerja sama ini dibutuhkan karena kasus serangan siber di indonesia yang begitu tnggi walaupun selama kerja sama kasus serangan siber indonesia meningkat sehingga belum kelihatan efektivitasnya setidaknya dapat teknologi dalam kerja sama ini dapat dikembangkan karena inggris termasuk dalam tiga besar negara tingkat kemanan siber yang tinggi.

5.3Saran

Melihat Kondisi serangan siber yang ada di indonesia masih terus meningkat,dan efektivitasnya kurang maksimal sehingga indonesia sebaiknya melakukan hal diantaranya:

1. mengajak multistakeholder pada bidang keamanan siber, sehingga jangkaunya lebih luas dan dampaknya bisa dirasakan oleh orang banyak efeknya juga bisa mempermudah kampanye mengenai kesdaran keamanan siber kepada masyarakat.
2. Membuat regulasi khsusus mengenai tentang kemanan siber khsususnya di media sosial dalam memfilter segala berita hoax dengan memberikan dukungan penuh kelembagaan keamanan siber dalam wujud pusat keamanan siber nasional sebagai rujukan utama dalam penanganan ancaman keamanan siber.

3. Memperbanyak kerjasama dan peran aktif dalam peningkatan keamanan siber melalui kerjasama bilateral, multilateral, dan public-private partnership, termasuk kerjasama di tingkat nasional untuk mengembangkan kemanan siber intelejen.

DAFTAR PUSTAKA

Buku

Abdul Wahid, Mohammad Labib. 2005. *Kejahatan Mayantara* (Cyber Crime). Bandung: Refika Aditama.

Abd Rahman Hamid, Muhammad Saleh Madjid. 2015. *Pengantar Ilmu Sejarah.* Cet.IV; Yogyakarta: Ombak.

Anak Agung Banyu Perwita & Yanyan Mochamad Yani. 2006. *Pengantar Ilmu Hubungan Internasional.* Bandung: Remaja Rosdakarya.

Anne W. 1986. Brascomb, Toward A Law of Global Communication Network. USA: Longman.

B.L. Berg, H. Lune*, Qualitative Research Methods For The Social Sciences, Ninth Edition,* (England, Essex: Pearson Education Limited, 2017).

Budi Suhariyanto. 2012. *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*. Jakarta : PT Raja Grafindo Persada.

Dwidja Priyatno. 2018. *Bunga Rampai Pembaharuan Hukum Pidana Indonesia*. Bandung: Pustaka Reka Cipta.

Fischer, E. A. 2009. *Creating a National Framework for Cybersecurity: an Analysis of Issues and Options*. New York: Nova Science Publishers, Inc.

Fischer, E. A., Ave, I., & Washington, S. E. 2005. *Creating a National Framework for Cybersecurity : An Analysis of.*

Frame, J. D. 2006. *International Business and Global Technology.* Maryland: Lexington Books.

Ghernaouti-Hélie, S. 2009. *Cybersecurity Guide for Developing Countries (Enlarged Edition ed).* Geneva: International Telecommunication Union.

Hardana, Isputra Radian Ferrari. 2019. *Membuat Aplikasi IoT: Internt of Things.* Yogyakarta: Lokomedia.

ITU. 2017. *Global Cybersecurity Index 2017.* International Telecommunication Unit.

ITU. 2012. *Global Cybersecurity Index 2017.* International Telecommunication Unit.

Jackson, R., & Sorensen, G. 2013. *Introduction to International Relations*. United Kingdom: Oxford University Press.

L. Siagian, A. Budiarto. 2017. *P. Strategi, P. Udara, and U. Pertahanan,* "the Role of Cyber Security in Overcome Negative Contents To.

Lexy J. Maleong. 1999. *Metodologi Penelitian Kualitatif.* Bandung: Remaja Rosdakarya.

M. Arsyad Sanusi. 2005. *Hukum Teknologi dan Informasi.* Bandung: Tim Kemas Buku.

Moore, R. 2005*. "Cyber crime: Investigating High-Technology Computer Crime,"*. Cleveland, Mississippi: Anderson Publishing.

Nye, Joseph S. 2011. *The Future of Power.* USA: Perseus Book Group.

Perwita, A.A.B. dan Yani, Y.M. 2017. *Pengantar Ilmu Hubungan Internasional* Cetakan Kelima. Bandung: PT Remaja Rosdakarya.

Prayudi, Ahmad Budiman, Aryojati Ardipandanto, Aulia Fitri. 2018. *Keamanan Siber dan Pembangunan Demokrasi di Indonesia.* Jakarta Pusat: Pusat Penelitian Badan Keahlian DPR RI Gedung Nusantara.

Putri Sylvia Octa. 2015. *Mengenal Studi Hubungan Internasional.* Bandung: Zavara.

Subagyo, A. 2011. *Teori Hubungan Internasional: Teori-teori National Interest.* Cimahi: FISIP HI-UNJANI.

S. Nasution*.* 2007. *Metode Research: Penelitian Ilmiah.* Jakarta: Bumi Aksara.

Sukmadinata. 2008. *Metode Penelitian Pendidikan.* Bandung: Remaja Rosdakarya.

Yani Y.M, Ian Montrama, Emil Wahyudin. 2017. *Pengantar Studi Keamanan*. Malang: Intrans Publishing.

Internet

Anmar Frangoul. 2017. UK businesses were hit 230,000 times each by cyber attacks in 2016, says internet service provider. Diakses dari https://www.cnbc.com/2017/01/11/uk-businesses-were-hit-230000 timeseach-bycyber-attacks-in-2016-says-internet-service-provider.html

Badan Sandi Dan Siber Negara. Rencana Strategis Badan Sandi Dan Siber Negara Tahun 2018-2019. Diakses dari https://bssn.go.id/wp content/uploads/2019/05/3.-Rencana-Srategis-BSSN-Tahun-2018 2019.pdf

Barrinha A, Renard T. Cyber-diplomacy: the making of an International society in the digital age. Global Affairs; (2017): 1-12. https://doi.org/10.1080/23340460.201 7.1414924, Retrieved from http://www.tandfonline.

BSSN tandatangani nota kesepahaman kerjasama dibidang keamanan siber dengan pemerintah Inggris, https://bssn.go.id/bssn-tandatangani nota-kesepahaman - kerjasama-di-bidang-keamanan-siber-dengan pemerintah-inggris-raya/

Carmen Elena CÎRNU, " – Addressing the Gap in Strategic Cyber Policy", No. 17(May-Jun, 2019), http://www.themarketforideas.com/ cyber diplomacy addressing-the-gap-in-strategic-cyberpolicy-a388/.

Edmon Makarim, Indonesian Legal Framework for Cybersecurity http://www.nisc.go.jp/security-site/campaign/ ajsympo/pdf/lecture2.pdf diakses Kamis, 28 Oktober 2021.

Eris Herryanto pada seminar nasional keamanan Infrastuktur Internet yang diselenggarakan Indonesia Security Incident Response Team on Internet Infrastruktur (ID-SIRTI) di Universitas Pertahanan di tahun 2011.

Handrini Ardiyant. Cyber-Security Dan Tantangan Pengembangannya Di Indonesia, file:///C:/Users/Windows/Downloads/336-652-1 SM%20(4).pdf (diakses pada tanggal 20 Oktober 2021).

KEMENHAN 2014. RI, Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun Tentang Pedoman Siber. Kementrian Pertahanan.

Kementerian Luar Negeri Republik Indonesia. Memorandum Saling Pengertian Antara Pemerintah Republik Indonesia Dan Pemerintah Kerajaan Inggris Raya Tentang Kerja Sama Bidang Keamanan Siber. Diakses dari https://treaty.kemlu.go.id/apisearch/pdf?filename=GBR-2018-0068.pdf.

Menteri Kominfo Pada "High Level Segment ITU Council 2008" Yang Membahas Cyber security, http://www.postel. go.id/info_view_c_26_p_814.htm

Menteri Kominfo Pada "High Level Segment ITU Council 2008" Yang Membahas Cyber security, http://www.postel. go.id/info_view_c_26_p_814.htm diakses Sabtu, 29 Januari 2022.

Noor Halimah Anjani. 2020. Ringkasan Kebijakan | Perlindungan Keamanan Siber di Indonesia. https://id.cips-indonesia.org/post/ringkasan kebijakan perlindungan keamanan-siber-di-indonesia (diakses pada tanggal 20 Oktober 2021).

Pasal 9 Peraturan Menteri Komunikasi dan Informatika No. 29/PER/M.KOMINFO/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

Reid, R., & Van Niekerk, J. 2014. *From information security to cyber security cultures. 2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference,* (August 2015). https://doi.org/10.1109/ISSA.2014.6950492.

Triwahyuni Dewi. Wulandari TA. 2016. *Strategi Keamanan Cyber Amerika Serikat.* Diakses dari https://search.unikom.ac.id/index.p hp/jipsi/article/view/239.

Von Solms, R., & Van Niekerk, J. 2013. *From information security to cyber security. Computers and Security, 38, 97–102*. https://doi.org/10.1016/j.cose.2013.04.004

Vishnum. 2018. Ancaman Keamanan Siber Menyebabkan Kerugian Ekonomi bagi Organisasi di Indonesia Sebesar US$34.2 Miliar. Diakses dari https://news.microsoft.com/id-id/2018/05/24/ancaman-keamanan

sibermenyebabkan-kerugian-ekonomi-bagi-organisasi-di-indonesia sebesarus34-2-miliar.

Jurnal

Anggoro Dwi Listyanto, Sudji Munadi. 2012. *Pengaruh Pemanfaatan Internet, Lingkungan Dan Motivasi Belajar Terhadap Prestasi Belajar Siswa SMK.* Jurnal Pendidikan Vokasi.

Alexander Pattipeilohi, “Di Balik Kecanggihan Sebuah Teknologi”. “Majalah Komputer dan Elektronika, 1985, hal. 42. Sebagaimana dikutip oleh Hj Sri Sumarwani, Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif, Jurnal Pembaharuan Hukum Volume I No. 3 September- Desember 2014.”

Bima Guntara, Legitimasi Penyebaran Informasi Yang Memiliki Muatan Penghinaan Dan/Atau Pencemaran Nama Baik Dalam Pasal 310 Kuhp Dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan, Volume 4 Nomor 2 Desember 2017, hal. 242.

Bobby Firdaus Usman. 2021. *Faktor-Faktor Yang Melatar Belakangi Kerjasama Indonesia Dengan Inggris Dibidang Keamanan Siber Tahun 2018*. (Mjir) Moestopo Journal International Relations, Volume 1, No. 2,

Carr, Madeline. 2015. *Crossed Wires: International Cooperation on Cyber Security dalam Interstate Journal of International Affairs,* 2015/2016, Issue II.

David Putra Setyawan dan Arwin Datumaya Wahyudi Sumari. 2016. *Diplomasi Pertahanan Indonesia dalam Pencapaian Cybersecurity melalui ASEAN Regional Forum on Cybersecurity Initiatives.* Jurnal Penelitian Politik, Volume 13 No. 1.

D Triwahyuni, TA Wulandari. 2016*. Strategi Keamanan Cyber Amerika Serikat.* Bandung: Jurnal Ilmu Politik dan Komunikasi. Volume VI No. 1, Juni 2016

Dista Amalia Arifah, *“Kasus Cybercrime Di Indonesia Indonesia’s Cybercrime Case,” J. Bisnis dan Ekon.*, vol. 18, no. 2, pp. 185–195, 2011.

Edy Junaedi Karnasudirja, 1993, Jurisprudensi Kejahatan Komputer, (Jakarta: Tanjung Agung, 1993), hal. 3. Sebagaimana dikutip oleh Hj Sri

Sumarwani, Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif, Jurnal Pembaharuan Hukum Volume I. No. 3.

Elizabeth Longworth. 2000. The Possibilities for legal framework for cyberspace Including New Zealand Perspective, Theresa Fuentes et.al (editor), The International Dimesions of Cyberspace Law: Law of Cyberspace Series, Vol.1, Aldershot: Ashgate Publishing Limited.

Hegar Krisnaduta. 2019. *Kerjasama Indonesia-Australia Di Bidang Keamanan Dalam Mengatasi Cyber Crime Di Indonesia Melalui Program Cyber Policy Dialogue.* Fakultas Ilmu Sosial Dan Ilmu Politik Universitas Pasundan Bandung.

Halder, D., & Jaishankar, K. 2011. *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations.* Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

Ina Sayang Tanjung. 2017. *Kerjasama Korea International Cooperation Agency (Koica) Dan Pemerintahan Indonesia Dalam Pengembangan Cyber Security*. Program Studi Ilmu Hubungan Internasional Fakultas Ilmu Sosial Dan Ilmu Politik Universitas Komputer Indonesia Bandung.

Islami, M.J. 2017. *Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index.* Jurnal Masyarakat Telematika dan Informasi Vol. 8 No. 2 (Oktober-Desember 2017)

Maulia, Jayantina Islami. 2017. *Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index Jurnal Masyarakat Telematika dan Informasi.* Volume: 8 No. 2.

Monica Romauly Weu. *Kerjasama Pemerintah Indonesia Dan Pemerintah Kerajaan Inggris Dalam Bidang Keamanan Siber.* Global Political Studies Journal Volume 4 Nomor 2 Edisi Oktober 2020 P-ISSN 2301 749X E-ISSN 2686-2905.

Nazli Coucri dan Daniel Goldsmith. 2012. *Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security.* Buletin of the Atomic Scientists 68, No. 2.

Radu, Roxana. 2014. *Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace dalam Jan Frederik Kremer & Benedikt Muller (ed),* Cybersp.

Rizky Pratama. *Kerjasama Indonesia-Inggris Dalam Mengatasi Kejahatan Siber Di Indonesia Tahun 2018-2020.* eJournal Ilmu Hubungan Internasional, Vol. 8 No. 4, 2020.

Setyawan, David Putra & Arwin Datumaya Wahyudi Sumari. 2016. *Jurnal Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui Asean Regional Forum On Cybersecurity Initiatives. Universitas Pertahanan Indonesia.*

Steve Morgan. 2016*. "Cyber Crime Costs Projected To Reach $2 Trillion by 2019".* Forbes. Retrieved September 22.

Vitashya Wowor. 2008. *Peranan United Nations Children's Fund (UNICEF) Dalam Meningkatkan Kesejahteraan Pangan Dan Gizi Anak di Indonesia* (2006-2008). (Universitas Komputer Indonesia).