PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan zaman, peradaban akan teknologi informasi dan komunikasi terus mengalami kemajuan. Salah satu kemajuan dari teknologi informasi dan komunikasi yakni internet. Kehadiran internet telah menciptakan dunia baru bagi umat manusia yang berbasis komputer dengan menawarkan realitas baru dalam kehidupan manusia dengan realitas virtual atau maya. Internet mampu mengirimkan atau meneruskan segala bentuk data informasi dengan tepat, cepat, dan efisien serta efektif yang dilakukan secara elektronik. Dengan memanfaatkan internet, para pengguna internet dapat dengan bebas menjelajahi *cyberspace* tanpa dihalangi oleh batas-batas kedaulatan suatu negara. Menurut Howard Rheingold bahwa *cyberspace* merupakan sebuah ruang imajiner atau maya yang bersifat artifisial, dimana setiap orang melakukan aktivitas ataupun kegiatan yang biasa dilakukan dalam kehidupan sosial sehari-hari dengan cara yang baru (Wahid dan Labib: 2005).

Pada perkembangannya, internet tidak hanya memberikan dampak positif namun juga membawa dampak yang negatif. Para pengguna internet harus berhadapan dengan potensi ancaman keamanan dalam hal pengelolaan baik dalam bentuk penyimpanan maupun penggunaannya. Kejahatan yang lahir sebagai dampak negatif dari internet disebut sebagai *cyber crime. Cyber Crime* merupakan suatu bentuk tindakan kriminal dengan menggunakan komputer sebagai alat kejahatan utama yang memanfaatkan kecanggihan teknologi internet

Menurut Kepolisian Inggris, *cyber crime* merupakan segala bentuk tindakan penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi (Wahid dan Labib: 2005).

Ruang siber dalam kaitannya dengan hubungan internasional dapat menjadi sumber berbagai potensi ancaman, kerentanan, dan ketidakamanan pada tatanan internasional. Pemanfaatan ruang siber yang tidak mengenal batas-batas wilayah negara, membuat penggunaan siber oleh suatu pihak yang dapat mengakibatkan kerugian bagi pihak lain dapat dilakukan oleh aktor Negara (*state actor*) maupun aktor bukan negara (*non-state actor*).

Aktor Negara sebagai aktor dalam hubungan internasional merupakan subyek interaksi antar negara-negara yang berdaulat. Selain negara sebagai aktor, terdapat aktor-aktor lain yang bukan negara, yang melalui tindakan ataupun sikapnya dapat menimbulkan pengaruh terhadap kehidupan negara maupun bangsa. Aktor-aktor yang dimaksudkan diantaranya adalah *Intergovernmental Organizations*, *International Non-Governmental Organizations, Non-Governmental Organizations* dan *Multinational Coporations* (Perwita dan Yani, 2017).

Siber dapat menjadi 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, seperti data perbankan, jaringan militer, bahkan sistem pertahanan negara. *Cyberspace* yang bersifat global, menjadikan *cyber crime* sulit untuk ditentukan yuridiksinya, sebab *locus delicti* atau tindak pidana kejahatan 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.

Bentuk serangan yang beragam terdiri dari penyerangan melalui virus, terhadap situs-situs resmi, hacker dan tindakan lainnya yang merupakan ancaman sekaligus tantangan yang harus dihadapi oleh lembaga pertahanan ataupun yang berwenang dalam menjaga keamanan siber nasional (Triwahyuni dan Wulandari. *Strategi Keamanan Cyber Amerika Serikat*. 2016).

John Perry Barlo menyatakan bahwa secara alamiah internet bersifat ekstra-nasional dan anti kedaulatan, sehingga kedaulatan suatu negara tidak dapat diberlakukan pada ruang maya (Adianto dan Nohara: 2010). Hal ini berarti bahwa *Cyberspace* merupakan tempat yang memiliki kedaulatan sendiri secara elektronik dimana para pengguna internet berada di luar batas yuridiksi suatu negara, dimana kedaulatan suatu negara tidak dapat mengendalikan aktivitas para pengguna internet di *cyberspace* karena pada hakekatnya internet sebagai jaringan elektronik tidak dapat dibatasi oleh tempat.

Ruang siber yang tidak mengenal adanya batas negara membuat beberapa serangan siber juga pernah terjadi di Indonesia. Penyebab serangan siber yang dilancarkan ke Indonesia dikarenakan Indonesia merpakan 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. Perkembangan teknologi yang amat pesat

telah membuat teknik perang siber menjadi lebih kompleks dan lebih canggih. Kemampuan intelijen siber negara Indonesia tidak hanya dimanfaatkan ketika terjadinya perang siber, namun juga menjadi pertaruhan besar kemajuan bangsa ke depan.

Dalam hal ini, *The Global Cybersecurity Index (GCI)* Tahun 2017 yang dirilis oleh *The UN International Telecommunication Union (ITU)* melaporkan bahwa Indonesia tergolong negara dengan tingkat keamanan siber yang masih lemah. Dari 195 negara, Indonesia menempati peringkat ke-70 dengan skor 0,424. Catatan *Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII)* menunjukkan, sejak Januari hingga Juli 2017 terdapat 177,3 juta serangan siber masuk ke Indonesia. Ini berarti setiap hari terjadi 836.200 serangan siber, umumnya dilancarkan dalam bentuk peretasan, virus, dan perangkat perusak lainnya seperti malware (Rencana Strategis Badan Sandi Dan Siber Negara Tahun 2018-2019 pada 13 Maret 2020).

Selain itu, Badan Siber Dan Sandi Negara yang melakukan kerjasama dengan Indonesia Honeynet Project yang dibentuk pada tahun 2018, yang mengeluarkan Honeynet Project. Didalam pengembangan *Honeynet Project*, menggunakan perangkat *Honeypot* yang mampu mendeteksi dan merekam identitas serta teknik serangan yang dilakukan oleh penyerang, sehingga dapat menampilkan peta dunia yang menggambarkan intensitas serangan dari negara lain ke Indonesia.

Menurut Laporan Honeynet Project Tahun 2018, melaporkan bahwa sumber serangan *malware* paling banyak dilakukan oleh negara Rusia dengan jumlah

serangan 2.597.256, Cina dengan jumlah serangan sebanyak 1.871.363, sementara Amerika Serikat sebesar 1.428.440, dan Singapura melakukan serangan sejumlah 1.030.769. Pada Laporan Tahunan Honeynet Project dijelaskan bahwa pada tahun 2018, jumlah total serangan sebanyak 12.895.554 dengan jumlah total serangan *malware* 513.863. 3 (tiga) *malware* terbanyak menyerang Indonesia terdiri dari 3 jenis *Worm Conficker* yang berbeda (diakses dari Laporan Tahunan Honeynet Project BSSN IHP. 2018 pada 13 Maret 2020).

Walaupun demikian belum berarti serangan yang dilakukan merupakan serangan langsung dari Rusia maupun negara lainnya. Sebab yang dideteksi adalah nomor *Internet Protocol* (IP), bisa jadi Rusia hanya digunakan sebagai *proxy* oleh penyerang, sehingga belum dikatakan bahwa Rusia maupun negara lainnya sebagai dalang dalam penyerangan siber ke Indonesia.

Tindakan kejahatan yang dilakukan oleh pelaku tindak kejahatan siber dapat mengakibatkan dampak yang buruk bagi Indonesia. Menurut penelitian yang dilakukan oleh Frost & Sullivan yang diprakarsai oleh Microsoft mengatakan bahwa tindak kejahatan siber di Indonesia dapat menimbulkan kerugian mencapai US$34,2 miliar atau setara Rp 478,8 triliun (asumsi US$1 = Rp 14.000). Angka ini setara dengan 3,7% dari total PDB Indonesia. Selain menimbulkan kerugian finansial, kejahatan siber mengurangi kemampuan berbagai organisasi di Indonesia untuk memanfaatkan peluang-peluang yang ada di era ekonomi digital saat ini, dengan tiga dari lima (61%) responden menyatakan bahwa perusahaan mereka telah menunda upaya transformasi digital karena khawatir terhadap risiko-risiko siber. Lebih lanjut

studi yang dilakukan oleh Microsoft dan Frost & Sullivan (https://news.microsoft.com/id-id/2018/05/24/ diakses pada 14 Maret 2020) mengungkapkan bahwa:

1. *Organisasi berskala besar di Indonesia kemungkinan dapat mengalami kerugian ekonomi sebesar US$16,3 juta, 200 kali lebih besar dari kerugian ekonomi rata-rata sebuah organisasi skala menengah.*
2. *Kekhawatiran tentang keamanan siber menghambat rencana Transformasi Digital, yang semakin vital bagi perusahaan dengan diumumkannya rencana kerja "Making Indonesia 4.0" oleh Presiden Joko Widodo dan Kementerian Perindustrian.*
3. *Serangan keamanan siber telah mengakibatkan hilangnya pekerjaan di hampir tujuh dari sepuluh (69%) organisasi pada tahun lalu.*
4. *Berbagai organisasi semakin banyak memanfaatkan teknologi Artificial Intelligence untuk memperkuat strategi keamanan sibernya.*

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. 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.

Tindak kejahatan dalam dunia siber, tidak hanya dialami oleh Indonesia, namun juga Inggris 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 (diakses dari https://www.cnbc.com/2017/01/11/ pada 23 Maret 2020). 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.

Aktivitas bisnis Inggris yang terhubung secara langsung terhubung pada *internet of things* memberikan jalan masuk bagi penyerang siber untuk melancarkan serangan pada perusahaan bisnis Inggris. Tindakan kejahatan ini berdampak pada perekonomian Inggris, sehingga Pemerintah Inggris menginvestasikan biaya yang tinggi untuk perlindungan, pertahanan dan keamanan ketahanan siber bagi bagi kepentingan bisnis Inggris maupun keamanan nasional Inggris.

Dengan kapasitas kemampuan dan didukung dengan adanya kemajuan teknologi informasi dan komunikasi yang dimiliki oleh negara Inggris, 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 bekerjasama secara internasional dalam menjaga keamanan siber internasional dan tujuan Inggris yakni untuk menjadi negara yang aman di dunia maya untuk melakukan bisnis. Dengan demikian, melihat permasalahan siber yang dialami oleh Indonesia, maka Pemerintah Inggris menginisiasi kerjasama dengan Indonesia di bidang keamanan siber.

Sebelum terjalinnya hubungan kerjasama antara Inggris dan Indonesia di bidang keamanan siber, hubungan diplomatik antara Pemerintah Indonesia dan Pemerintah Kerajaan Inggris telah terjalin semenjak Desember 1949. Untuk mempererat hubungan kedua negara, maka Indonesia dan Inggris memiliki forum bilateral diantaranya adalah *Partnership Forum; Annual Trade Talks; Energy Dialogue; Joint Working Group on Education; Joint Working Group on Creative Industries; Navy to Navy Strategic Meeting; Joint Defence Cooperation Dialogue* (diakses dari https://indonesianembassy.org.uk/hubungan-ri-inggris pada 2 April 2020).

Selain pada forum-forum tersebut, hubungan diplomatik antara Indonesia dan Inggris terlihat pada forum kemitraan antara Pemerintah Indonesia dan Pemerintah Inggris yang dilaksanakan pada Resepsi Diplomatik KBRI London dalam memperingati Hari Ulang Tahun ke-74 Kemerdekaan Republik Indonesia dan Hari Ulang Tahun ke-74 Tentara Nasional Indonesia. Di sela resepsi tersebut, Dr Rizal Sukma selaku Duta Besar RI untuk Inggris Raya, Irlandia dan Organisasi Maritim Internasional dan Richard Graham MP sebagai Utusan Khusus Perdana Menteri

Inggris untuk urusan Perdagangan dengan Indonesia dan Masyarakat Ekonomi ASEAN, yang bertindak sebagai Tamu Kehormatan, melakukan pembahasan mengenai hubungan antara Indonesia dan Inggris dalam memperkuat kerjasama bilateral pada berbagai sektor. Terdapat 7 karakter kerjasama antara Indonesia dan Inggris yakni: Kemitraan ekonomi guna memberikan kesejahteraan bagi rakyat kedua negara secara berkesinambungan; Kemitraan global untuk menciptakan tatanan internasional berbasis aturan; Kemitraan dalam bidang maritim guna memastikan laut terbuka untuk semua negara; Kemitraan berbasis norma guna mengawal demokrasi, keberagaman dan toleransi sebagai pedoman bagi setiap negara; Kemitraan bidang politik untuk menciptakan pemerintahan yang baik, terbuka dan akuntabel; Kemitraan bidang pertahanan guna menjaga stabilitas dan keamanan dunia; Kemitraan bidang kebudayaan untuk menciptakan saling pengertian dan mendekatkan hubungan masyarakat antar Indonesia dan Inggris (PRESS RELEASE No. 033/PR.PEN/XI/LONDON/2019 pada 2 April 2020).

Terkhusus pada bidang keamanan siber, kerjasama Indonesia dan Inggris pada keamanan siber merupakan hubungan kerjasama yang baru terbentuk. Dengan adanya hubungan kerjasama 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.

Dengan demikian, kerjasama dalam bidang keamanan siber antara Indonesia dan Pemerintah Kerajaan Inggris telah diresmikan melalui penandatanganan Memorandum Of Understanding pada 14 Agustus 2018. Penandatanganan MoU keamanan siber itu dilakukan oleh Kepala Badan Siber dan Sandi Negara (BSSN) RI, Djoko Setiadi dan Menteri Muda Urusan Asia Pasifik Kemlu Inggris, Mark Field, di Kementerian Luar Negeri RI di Jakarta. Terdapat 5 poin yang melingkupi kerjasama di bidang keamanan siber yakni sebagai berikut (diakses dari https://treaty.kemlu.go.id pada 2 April 2020).

1. Pengembangan Dan Implementasi Strategi Keamanan Siber Nasional

   Pertukaran praktik terbaik dan pengalaman di bidang keamanan nasional.

2. Manajemen Insiden

   a. Membentuk dan mengelola titik kontak mengenai manajemen insiden nasional dan mengidentifikasi mekanisme komunikasi yang sesuai;

   b. Mengonsultasikan dan mengoordinasikan dalam menanggapi insiden keamanan siber terutama ketika informasi tersebut terkait dengan para peserta;

   c. Mempromosikan pentingnya koordinasi dan manajemen insiden yang efektif;

3. Kejahatan Siber

   Mempromosikan kemampuan investigasi dan forensic di bidang siber yang lebih kuat, termasuk melalui pertukaran kesempatan pelatihan.

4. Promosi Kesadaran dan Pelatihan di Bidang Keamanan Siber

a. Pertukaran praktik terbaik dalam peningkatan kesadaran publikndan kampanye perubahan perilaku dibidang keamanan siber;
b. Pertukaran contoh dan pengalaman dalam pengembangan pesan teknis dan pelatihan keamanan siber dalam Pemerintahan, termasuk mitra penegak hukum.

5. Pengembangan Kapasitas
   a. Pertukaran pengetahuan dan praktik yang baik pada bidang tersebut di atas;
   b. Bekerjasama untuk emmfasilitasi hubungan kerja antarinstitusi Indonesia dan Inggris Raya dalam bidang keamanan siber, dalam bentuk Peraturan Pelaksana di bawah MSP ini.

Kerjasama ini menunjukkan bahwa pemerintah Indonesia dan pemerintah Inggris berkomitmen kuat untuk membangun kapasitas ranah siber di kedua negara. Sebagai media untuk berkoordinasi dan bertukar pikiran dalam pengimplementasian substansi kerjasama MoU, pelaksanaan MoU ini diterapkan dalam bentuk *cyber dialogue* yang dilaksanakan dalam setiap tahun. Peserta utama dari kerjasama ini adalah Badan Sandi dan Siber Negara dan Kemterian Luar Negeri dan Persemakmuran, namun dari kerjasama ini juga dapat mengundang entitas-entitas siber yang terkait sesuai dengan isu yang akan diangkat.

Inggris menempatkan serangan siber sebagai kejahatan siber yang berskala besar sebagai salah satu risiko keamanan nasional tertinggi, dengan mempertimbangkan kemungkinan dan dampak serangan yang mungkin terjadi.

Strategi Keamanan Nasional Inggris pada tahun 2010 mengakui serangan dunia maya sebagai salah satu ancaman utama terhadap keamanan nasional Inggris bersama dengan terorisme internasional. Strategi keamanan nasional Inggris menggarisbawahi bahwa pengaruh ancaman siber dapat berpangruh pada kehidupan sehari-hari pemerintah, warga negara dan perorangan, dikarenakan akses internet sudah dianggap sebagai suatu jalinan yang masuk kedalam masyarakat dan suatu hak yang melebihi hak istimewa.

Pemerintah Inggris telah merilis National Cyber Security Strategy 2016-2021 yang baru. Menyadari bahwa serangan siber di Inggris adalah ancaman utama terhadap keamanan ekonomi dan nasional Inggris, strategi ini menguraikan visi dan tujuan untuk menciptakan Inggris yang aman dan tahan terhadap ancaman siber, serta makmur dan percaya diri di dunia digital. Inggris selalu berada di garis depan kegiatan keamanan siber, dan strategi barunya adalah kontribusi penting dan model bagi upaya global.

Oleh karena itu, penandatangan MoU yang dilakukan oleh Pemerintah Indonesia dan Pemerintah Inggris dalam bidang keamanan siber merupakan langkah yang tepat bagi pemerintah Indonesia dan Pemerintah Kerajaan Inggris dalam melakukan keamanan siber. Kerjasama ini menunjukkan bahwa pemerintah Indonesia dan pemerintah Inggris Raya memiliki komitmen yang kuat dalam membangun dan mengembangkan kapasitas siber pada kedua negara. Mengingat bahwa pada saat ini ranah siber telah menjadi bidang yang dapat mempengaruhi penyelanggaraan negara dan pemerintahan, serta dapat berpengaruh pada perekonomian sosial masyarakat.

Dalam upaya memudahkan peneliti dalam mengakaji Kerjasama Indonesia dan Inggris dalam bidang keamanan siber. Peneliti menggunakan beberapa penelitian terdahulu dijadikan sebagai acuan diantaranya yakni penelitian pertama mengenai *Kerjasama Indonesia – Korea Selatan dalam mengimplementasikan keamanan cyber studi kasus Cyberporn* yang ditulis oleh Elin Konstantia Novel. Dalam penelitian ini dijelaskan bahwa Pornografi telah menjadi salah satu masalah rumit dalam penegakan hukum. Itu karena penyebarannya yang begitu masif, sehingga sulit untuk diatasi. Pornografi, bersama dengan keberadaan internet, adalah tantangan lain bagi pemegang hukum untuk menghilangkannya sebagai kejahatan cyber pornografi (Pornografi di internet) yang memberikan dampak besar. Dalam konteks kejahatan, cyber porn dapat dikategorikan sebagai salah satu cyber crime. Hasil penelitian ini menunjukkan proses kerjasama yang dilakukan melalui kerjasama antara Korea International Cooperation Agency (KOICA) dan Pemerintah Indonesia dalam pengembangan keamanan cyber yaitu mencetak Sumber Daya Manusia (SDM) dalam keamanan cyber, keamanan terhadap malware dan pertukaran informasi antara kedua negara dalam mencegah terjadinya ancaman siber.

Penelitian berikutnya ditulis oleh Hegar Krisnaduta yang berjudul *Kerjasama Indonesia-Australia di Bidang Keamanan dalam Mengatasi Cyber Crime di Indonesia melalui Program Cyber Policy Dialogue* 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.

Pada penelitian yang dilakukan oleh 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*.

Selanjutnya yakni penelitian yang berjudul *Latar Belakang Kerjasama Keamanan Siber Pemerintah Indonesia Dengan Inggris Tahun 2015 - 2018* yang diteliti oleh Iqbal Fadhil. Dalam penelitiannya dijelaskan bahwa saat ini Indonesia mendapat ancaman yang nyata melalui ruang siber karena setiap bulan terjadi puluhan juta serangan. Indonesia tidak dapat bergerak sendiri, kerja sama dari berbagai pihak sdan transfer teknologi dari negara yang mumpuni sangat dibutuhkan Indonesia untuk dapat memberi keamanan di ruang siber.

Kesamaan dengan penelitian-penelitian sebelumnya yakni sama-sama membahas kerjasama yang dilakukan oleh Indonesia dalam menangangi cybercrime. Perbedaan terdapat pada pengkajian masalah dimana pada penelitian sebelumnya hanya membahas mengenai latar belakang kerjasama keamanan siber antara Indonesia dan Inggris tahun 2015-2018, sedangkan peneliti tidak hanya membahas latar belakang kerjasama keamanan siber antara Indonesia dan Inggris namun juga perkembangan dan prospek kerjasama yang dilakukan oleh Pemerintah Indonesia dan Pemerintah Kerajaan Inggris dalam bidang keamanan siber tahun 2018-2020.

Berdasarkan uraian diatas penelitian ini akan membahas tentang **"Kerjasama Permintahan Republik Indonesia Dan Pemerintahan Kerajaan Inggris Dalam Bidang Keamanan Siber"**

Ketertarikan peneliti terhadap penelitian ini didukung oleh beberapa mata kuliah Ilmu Hubungan Internasional, yaitu antara lain:

1. Diplomasi dan Negosiasi

   Matakuliah ini membantu peneliti dalam memahami strategi suatu negara dalam melakukan diplomasi dan negosiasi dalam mencapai kepentingannya. Dalam hal ini adalah upaya Indonesia dan Inggris dalam kerjasama keamanan siber.

2. Studi Keamanan Internasional

   Matakuliah ini membicarakan keamanan di suatu negara, keamanan merupakan faktor paling terpenting dalam suatu negara dan dimana teknologi dan informasi berperan di dalamnya. Melalui matakuliah ini membantu peneliti dalam menganalisa kemanan non tradisional dalam bidang keamanan siber pada suatu negara.

3. Informasi dan Komunikasi Internasional

   Matakuliah ini membantu peneliti dalam memahami bagaimana interaksi dan komunikasi yang baik yang melewati batas negara.

4. Keamanan Siber

   Matakuliah ini membantu peneliti dalam memahami bahwa kegagalan dalam melindungi keamanan siber dapat menimbulkan dampak ataupun masalah yang sangat besar.

1.2 Rumusan Masalah

1.2.1 Masalah Mayor

Pada penelitian ini, penulis mengajukan rumusan masalah mayor sebagai berikut *Bagaimana Kerjasama yang dilakukan oleh Pemerintah RI dan Pemerintah Kerjaaan Inggris Dalam bidang keamanan siber?*

1.2.2 Masalah Minor

Dari uraian latar belakang di atas, maka peneliti menarik rumusan masalah minor sebagai berikut:

1. Bagaimana penerapan kerjasama antara Indonesia dan Inggris dalam bidang keamanan siber berdasarkan MoU yang telah disepakati?
2. Apa yang menjadi kepentingan Indonesia dan Inggris dalam melakukan kerjasama dalam bidang keamanan siber?
3. Apa yang menjadi kendala terhadap pelaksanaan kerja sama dalam bidang keamanan siber?
4. Bagaimana prospek kerjasama yang dilakukan oleh Indonesia dan Inggris dalam keamanan siber?

1.2.3 Pembatasan Masalah

Pada penelitian ini, peneliti membatasi masalah penelitian dari tahun 2018-2019. Dikarenakan pada tahun 2018 lebih tepatnya pada 14 Agustus 2018 terjadi penandatangan MoU Kerjasama antara pihak Pemerintah Indonesia yang diwakili oleh Badan Sandi Dan Siber Negara dengan Pemerintah Kerajaan Inggris dalam bidang keamanan siber, dan pada tahun 2019 karena peneliti ingin mengetahui hal-hal apa saja yang telah dilakukan dalam mengimplementasikan MoU, hal-hal yang menjadi kepentingan Indonesia

dan kendala yang dihadapi sekaligus prosepek kerjasama antara Indonesia dan Inggris dalam pengembangan kerjasama dalam bidang keamanan siber.

1.3 Maksud dan Tujuan Penelitian

1.3.1 Maksud Penelitian

Maksud dari penelitian ini adalah untuk mengetahui dan memahami bagaimana kerjasama yang dilakukan oleh Pemerintah Republik Indonesia dan Pemerintah Kerajaan Inggris dalam bidang keamanan siber.

1.3.2 Tujuan Penelitian

1. Mengetahui penerapan kerja sama yang disepakati Indonesia dan Inggris dalam bidang keamanan berdasarkan MoU yang telah disepakati.
2. Mengetahui dan memahami hal-hal yang menjadi kepentingan Indonesia dalam melakukan kerja sama dengan Inggris dalam bidang keamanan siber.
3. Mengetahui kendala yang dialami oleh Indonesia dan Inggris dalam melakukan kerja sama terutama pada bidang keamanan siber.
4. Mengetahui prospek kerja sama yang dilakukan oleh Pemerintah Republik Indonesia dan Pemerintah Kerajaan Inggris dalam pengembangan bidang keamanan siber.
5. Memahami dan menilai efektivitas kerjasama antara Indonesia dan Inggris dalam bidang keamanan siber.

1.4 Kegunaan Penelitian

1.4.1 Kegunaan Teoritis

Secara teoritis, hasil dari penelitian ini dapat menjadi sumber atau referensi pengetahuan terkait perkembangan kerjasama Indonesia dan Inggris dalam bidang keamanan siber untuk mengatasi masalah tindak kejahatan lintas negara yaitu cybercrime yang berada dikedua negara, serta dapat menambah keilmuan mengenai mengenai Keamanan Internasional tentang langkah-langkah yang dapat dilaksanakan oleh negara-negara untuk menjaga keamanan di wilayah regionalnya.

1.4.2 Kegunaan Praktis

1. Bagi peneliti yaitu dapat menambahkan wawasan yang lebih luas bagi penulis tentang dunia siber.
2. Bagi para pembaca yaitu sebagai bahan referensi khususnya jurusan Ilmu Hubungan Internasional.
3. Bagi peneliti berikutnya yaitu sebagai bahan pertimbangan atau bahan yang dapat di kembangkan lebih lanjut, serta referensi terhadap penelitian yang sejenis.