# KERJASAMA INDONESIA-INGGRIS DALAM MENGATASI KEJAHATAN SIBER DI INDONESIA TAHUN 2018-2020

**Rizky Pratama** [1]

***Abstract:*** *Indonesia is a country with the most internet users, because of this makes Indonesia have various problems in cyber security, to solve these problems Indonesia has made various efforts divided into domestic and foreign efforts, on domestic efforts Indonesia making a laws and a national organisation with the name is Badan Siber dan Sandi Negara (BSSN), on foreign efforts Indonesia's are collaborating with countries that have capabilities in cyber security, one of this collaborations is with the United Kingdom in improving cybersecurity in Indonesia which is also the focus of this research. In this collaboration United Kingdom helping Indonesia to improve cybersecurity through the implementation and development of a national cybersecurity strategy, seminar and training in the field of cybersecurity and the development of cyber security capacity in Indonesia in guarding against cyber crime.*

***Keywords: Cooperation, Indonesia and United Kingdom, Cyber Crime.***

## Pendahuluan

Kemajuan teknologi informasi dan komunikasi khususnya yang berbasis pada internet telah mempengaruhi hampir semua orang untuk memanfaatkan dan menggunakannya. Perpaduan teknologi telekomunikasi, internet, dan penyiaran saat ini telah membuat berbagai aktifitas masyarakat semakin mudah, membuat masyarakat semakin dekat dan banyak terlibat dalam perkembangan teknologi. Perkembangan teknologi ini tidak hanya menimbulkan manfaat bagi masyarakat, namun perkembangan teknologi juga menimbulkan ancaman-ancaman kejahatan baru yang terjadi di ruang siber. Hal ini menjadi pendorong perlunya perlindungan terhadap sarana dan prasarana infrastruktur negara dalam pemanfaatan teknologi informatika.

Pada awal abad ke-21, ancaman berbasis siber menambahkan dimensi baru dalam memahami ancaman keamanan dari abad sebelumnya. Kejahatan siber adalah suatu tindakan ilegal yang dilakukan melalui sistem komputer atau jaringan internet untuk mendapatkan keuntungan dengan cara merugikan pihak lain. Kejahatan dunia maya ini bisa dilakukan dengan berbagai macam cara dan tujuan yang beragam. Pada umumnya, kejahatan tersebut dilakukan oleh orang-orang yang mengerti dan menguasai bidang teknologi informasi (Putra, 2019).

Seiring berkembangnya teknologi, semakin banyak pula jenis kejahatan yang terjadi. Namun, secara umum jenis-jenis kejahatan dunia maya dibagi menjadi beberapa tindakan, seperti: *Unauthorized Access to Computer System and Service, llegal Contents, Data Forgery, Cyber Espionage, Cyber Sabotage and Extortion, Offense against Intellectual Property, infringements of Privacy, Cracking, Carding* (bapenda.jabarprov.go.id. 2017).

Ancaman keamanan siber tidak lagi dipandang sebagai masalah teknis keamanan komputer semata, melainkan mencakup aspek ideologi, politik, ekonomi, sosial, budaya

[1] Mahasiswa Program S1 Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik Universitas Mulawarman. Email: rizkyconankudo@gmail.com

dan keamanan nasional (Chotimah, 2017). Sementara di tingkat internasional, baik negara maupun masyarakat internasional harus mengembangkan strategi kooperatif dalam menanggapi perkembangan di dunia maya yang meluas secara global (Coucri dan Goldsmith, 2012).

Dalam *Global Cybersecurity Index* (GCI) tahun 2019 yang dirilis oleh *International Telecommunication Union* (ITU), Indonesia menempati peringkat ke-41 dari total 175 negara. Peringkat Indonesia naik, dimana pada tahun 2017 Indonesia berada di peringkat ke-70 dari 164 negara dan pada saat itu Indonesia belum mendirikan instansi pemerintah yaitu Badan Siber dan Sandi Negara (BSSN). ITU merupakan badan PBB yang bertujuan mengkoordinasikan operasi dan layanan telekomunikasi di seluruh dunia sementara GCI merupakan inisiasi ITU untuk mengukur komitmen, kepedulian, dan usaha suatu negara terhadap pengelolaan keamanan siber. GCI kini menjadi rujukan bagi seluruh negara di dunia untuk membandingkan komitmen dan usaha dalam menjaga dan meningkatkan keamanan siber (inforial.tempo.co. 2017).

Menurut data dari **Badan Siber dan Sandi Negara** (BSSN) Indonesia menjadi negara kedua dengan kasus serangan siber terbanyak di dunia pada tahun 2018 dengan jumlah serangan sebanyak 225,9 juta dan 40% di antaranya merupakan serangan *malware* (cnnindonesia.com. 2019). Negara yang sering mengalami serangan siber pertama adalah China dan mengikuti dibelakang nya adalah Indonesia, ada beberapa contoh jenis serangan siber maupun perang siber yang pernah terjadi di Indonesia dengan pihak lain, yaitu;

Pertama, *Unauthorized Access to Computer System and Service*, yaitu pada tahun 1998 dimana terjadi kerusuhan di Indonesia yang melibatkan Etnis Tionghoa, yang membuat situs dan database Indonesia diserang para peretas yang diduga berasal dari Cina dan Taiwan.

Kedua, *Cracking and Cyber Sabotage and Extortion,* Berdasarkan penelitian dari Symantec, yaitu produsen Antivirus Norton, pada Agustus 2010 Indonesia berada di urutan kedua setelah Iran di antara 10 negara yang mengalami serangan *worm Stuxnet*. *Stuxnet* adalah *worm* atau virus yang khusus menyerang komputer berbasis operasi *Windows* (industri.kontan.co.id. 2011).

Ketiga, *Cyber Espionage dan infringements of Privacy* Liputan6 pernah melaporkan pada 31 Oktober 2013 bahwa Intelijen Australia telah melakukan penyadapan terhadap sinyal radio, telekomunikasi, dan lalu lintas internet pemerintah Indonesia melalui gedung perwakilan diplomatiknya di Jakarta (liputan6.com. 2014). Direktorat Sinyal Pertahanan Australia telah mengoperasikan fasilitas program *stateroom* di kedutaannya di Jakarta, *stateroom* adalah nama sandi program penyadapan sinyal radio, telekomunikasi, dan lalu lintas internet (Sa'diyah dan Vinata, 2016).

Keempat, *Cyber Sabotage and Extortion Cracking* Pada Mei tahun 2017 lalu, terjadi serangan siber yang disebabkan oleh sebuah virus berjenis *Ransomware* dengan nama *Wannacry.* Ada dua rumah sakit yang terkena serangan tersebut yaitu RS Harapan Kita dan RS Dharmais. Sistem komputernya diserang virus ransomware WannaCry, dari 600 komputer yang ada di Rumah Sakit Dharmais terdapat sekitar 60 unit komputer yang terkena. Pihak rumah sakit harus mengeluarkan uang hingga 17 ribu dollar atau sekitar Rp 226 juta yang dikirim melalui Bitcoin demi menebus data yang disandera penyerang. Mantan Menteri Komunikasi dan Informatika Rudiantara menyatakan rumah sakit menjadi sasaran yang mudah diserang, karena sebagian besar masih menggunakan sistem operasi Windows lama versi 2008 ke bawah. Program jahat

*ransomware WannaCry* menyerang komputer berbasis Windows yang memiliki kelemahan terkait fungsi *Server Message Block.*

Pihak Microsoft menjelaskan salah satu penyebab serangan siber sering terjadi di Indonesia berupa peretasan, penyebaran berita hoax, pencemaran nama baik melalui media sosial dan bentuk serangan siber lainnya adalah penggunaan software bajakan. *Software Asset Management Microsoft* mencontohkan pengunduhan aplikasi mobile dari sumber meragukan di internet yang sering disusupi malware (inet.detik.com. 2016).

Untuk mengatasi kasus-kasus kejahatan siber tersebut, Indonesia membuat Undang-Undang Nomor 19 Tahun 2016 (UU ITE) disahkan pada tanggal 21 April 2008 dan menjadi *cyber law* pertama di Indonesia. Secara umum, materi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dibagi menjadi dua bagian besar, yaitu pengaturan mengenai informasi dan transaksi elektronik dan pengaturan mengenai perbuatan yang dilarang (inet.detik.com. 2016).

Selain upaya internal melalui pemberlakuan undang-undang ITE, Indonesia juga melakukan upaya eksternal yang diwujudkan melalui kerja sama tulisan nya dengan negara-negara lain untuk meningkatkan kekuatan keamanan siber, salah satunya Inggris. Sejak terjalinnya hubungan *diplomatic* antara Indonesia dan Inggris 70 tahun yang lalu kerjasama dalam berbagai bidang diantara kedua negara semakin terjalin erat termasuk dalam bidang keamanan siber. Kerjasama antara Indonesia dan Inggris ini diawali dari kunjungan menteri muda Inggris urusan Asia Pasifik, Mark Field ke Indonesia, membahas seputar hubungan kerja sama kedua negara serta penandatanganan *Memorandum of Understanding* (MoU) terkait keamanan siber oleh Kepala Badan Siber dan Sandi Negara (BSSN) Republik Indonesia yaitu Dr.Djoko Setiadi,M.Si. dan Menteri Muda Inggris Urusan Asia Pasifik yaitu The Rt. Hon. Mark Field, MP, dalam penandatanganan ini juga disaksikan oleh wakil mentri luar negeri Indonesia Abdurrahman Mohammad Fachir dan Duta Besar Inggris untuk Indonesia Moazzam Tufail Malik (Humas, BSSN. 2018).

Inggris merupakan sebuah negara yang sangat maju, unggul dan sangat baik terutama perkembangan teknologinya, dalam peringkat GCI Inggris menempati peringkat pertama dalam 5 besar negara dengan keamanan siber terkuat, ini merupakan satu keuntungan bagi Indonesia, selain itu Inggris juga dikenal memiliki banyak perusahaan keamanan siber dengan reputasi yang baik serta memiliki sekolah dengan memiliki fokus terhadap keamanan siber dan juga Inggris merupakan negara yang terus melakukan pembaruan terhadap keamanan siber nya (great.gov.uk. 2017), dan kerjasama ini juga memberikan keuntungan bagi Inggris karena dapat berbagi pengalaman mengenai keasadaran keamanan informasi untuk masyarakat. Isi MoU dari kerja sama antara Indonesia dengan Inggris tersebut adalah: (menpan.go.id. 2017)

1. Pengembangan dan Implementasi Strategi Keamanan Siber Nasional
2. Manajemen Insiden
3. Kejahatan Siber
4. Promosi Kesadaran dan Pelatihan di Bidang Keamanan Siber
5. Pengembangan Kapasitas

Kerjasama ini menunjukkan bahwa pemerintah Indonesia dan pemerintah Inggris **berkomitmen kuat untuk membangun kapasitas keamanan pada ranah siber di kedua negara.** Mengingat saat ini ranah siber telah menjadi salah satu bidang yang mempengaruhi penyelenggaraan negara dan pemerintahan, dan tentunya dapat berdampak pada ekonomi sosial masyarakatnya (bssn.go.id. 2018).

## Kerangka Teori

### Keamanan Siber

Pada dekade kedua abad kedua puluh satu, prefix *cyber* telah melekat pada konsep-konsep seperti *cyberculture*, *cybersex*, dan *cyberwar*, yang semuanya terkait dengan ranah media digital, virtual reality, dan internet. Dalam budaya populer, awalan dan imbuan berbagai kata terlihat samar-samar, seperti halnya dengan gerakan sastra *cyberpunk*. Demikian pula sejak munculnya internet, kata *network* telah menjadi metafora menonjol dan telah mengambil perhatian di hampir setiap disiplin ilmu kontemporer dan institusi besar. Seperti pada tahun 1948, prefix *cyber* ditemukan dalam istilah *cybernetics* yang digambarkan sebagai "studi tentang pesan sebagai sarana yang mengendalikan mesin dan masyarakat".

Namun pada dasarnya, tujuan *cybernetics* adalah untuk mengembangkan bahasa dan teknik menyerang terkait dengan masalah kontrol dan komunikasi pada umumnya dan kemudian menjadi dasar untuk komputasi setelah Perang Dunia II.Seperti halnya istilah *cyber*, istilah *network* sejak pertengahan abad kedua puluh juga telah ada, dan dalam era globalisasi di mana orang di seluruh dunia saling berhubungan melalui infrastruktur transportasi dan komunikasi, *network* atau jaringan merupakan sebuah material dan realitas metafora.

Sejarah *cyber security* sebagai konsep sekuritisasi dimulai dengan disiplin Ilmu Komputer dan Informasi di mana yang pertama kali menggunakan *cyber security* adalah dalam laporan *Computer Science and Telecommunications Board* (CSTB) pada tahun 1991. Di mana keamanan di era informasi dalam istilah *security* didefinisikan 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 *cyber security* tidak hanya diakibatkan oleh agen atau aktor tertentu tetapi juga oleh sistem itu sendiri sehingga kemudian muncul istilah *computer security*. Nissenbaum menunjukkan bahwa mayoritas ilmuwan komputer mengadopsi wacana teknis yang difokuskan pada pengembangan program yang baik dengan sejumlah bug dan sistem yang sulit ditembus oleh peretas sehingga *computer security* bergeser ke *cyber security* di mana *cyber security* dapat dilihat sebagai keamanan komputer dan sekuritisasi.

Konsep *cyber security* ini kemudian berkembang di mana menurut Saco dan Deibert, ancaman dari *cybercrime* juga telah melanggar batas-batas negara sehingga mengancam secara internasional. Hal ini disebabkan oleh, adanya interaksi masyarakat melalui dunia maya yang semakin tinggi akibat kemajuan teknologi dan era informasi.Berbeda halnya pendapat dari Deibert yang menjelaskan bahwa *cyber security* didasari melalui empat wacana terpisah dengan beda rujukan, ancaman, pilihan kebijakan, dan perintah yang berbeda yaitu mencakup keamanan nasional, keamanan negara (terdiri ancaman eksternal terhadap kedaulatan negara serta ancaman internal terhadap keamanan rezim), keamanan swasta, dan keamanan jaringan.

Pendapat tersebut didukung oleh Hansen dan Nissenbaum di mana dalam kasus *cybercrime* mencakup hubungan antara "jaringan" dan "individu" serta objek referen kolektif manusia sehingga tidak ada wacana tentang keamanan swasta yang merupakan keamanan individu sebagai objek rujukan, melainkan bahwa wacana keamanan individu terkait dengan rujukan sosial dan politik.

**Konsep Kerjasama Bilateral**

Konsep kerjasama bilateral lahir dari teori kerajamasa 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. Suatu kerjasama internasional didorong oleh beberapa faktor:

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

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.

## Metode Penelitian

Jenis data yang digunakan dalam penelitian adalah data sekunder yaitu data yang penulis dapatkan berasal dari telaah pustaka yaitu buku – buku, jurnal ilmiah, dokumen, akses internet dan artikel melalui media internet. Teknik pengumpulan data yang dilakukan adalah studi pustaka dari buku, artikel ilmiah, berita, dan sumber kredibel lainnya seperti berita dan jurnal dari internet yang terkait dengan topik penelitian. Teknik analisis data yang penulis gunakan adakah teknik analisis kualitatif yang menjelaskan dan menganalisis data hasil penelitian mengenai kerjasama Indonesia-Inggris dalam mengatasi kejahatan siber di indonesia tahun 2018-2020 dan menyajikan hasil dari penelitian tersebut kedalam sebuah skripsi.

## Hasil dan Pembahasan

Kejahatan siber pertama kali terjadi pada tahun 1870, kejahatan ini dilakukan oleh beberapa remaja dan merusak sistem telepon baru negara dengan merubah otoritas jaringan negara tersebut. Kejahatan siber selanjutnya terjadi pada awal tahun 1960 yang terjadi pada fasilitas komputer di laboratorium sebuah universitas dengan kerangka utama komputer yang besar, dengan kecerdasan buatan atau juga dikenal dengan sebutan *artificial intelligence* (Nahak, 2017).

Berkembangnya kejahatan siber di dunia membuat munculnya klasifikasi kejahatan siber menjadi beberapa bagian seperti *Carding, Skimming, Cracking, Phising, Malware, Cybersquatting,* Pornografi dan judi online, serta *Transnational Crime* yang diungkapkan oleh Peter Stephenson, dia mengatakan bahwa kejahatan siber merupakan jenis kejahatan yang memanfaatkan sebuah teknologi informasi tanpa batas serta

memiliki karakterisktik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan pada tingkat keamanan yang tinggi dan kredibilitas sebuah informasi yang disampaikan dan diakses melalui internet (siber) (Stephenson, 2000).

Kejahatan siber terjadi disetiap negara salah satunya adalah Indonesia, kejahatan siber pertama kali terjadi pada tahun 1997 yang terjadi kepada Departemen Luar Negeri dan Tentara Nasional Indonesia (TNI) yang diretas oleh *cracker porto* yang merupakan *hacker* dari Portugis yang pro-kemerdekaan, dan kejahatan siber terus terjadi di Indonesia seperti sistem pemilihan di Indonesia yang diretas pada tahun 2005 dan pembajakan e-mail yang dialami oleh Wakil Ketua MPR, Lukman Hakim Saifuddin, yang terjadi pada tahun 2013 (Aisyah, 2019). Selain itu kejahatan siber di Indonesia terus mengalami peningkatan, menurut ID-SIRTII (*Indonesia Security Incident Response Team on Internet and Infrastructure)* yang melakukan perhitungan mengenai jumlah kejahatan siber yang terjadi di Indonesia, mengatakan bahwa jumlah serangan siber di Indonesia semakin meningkat, dari 28,430,843 pada tahun 2015 meningkat menjadi 135.672.984 pada tahun 2016 dan 47% dari keseluruhan kasus yang terjadi merupakan serangan malware, 44% merupakan penipuan, sedangkan sisanya berbentuk kejahatan siber lainnya, seperti *website defacement*, dan aktivitas manipulasi data dan kebocoran data. Tren peningkatan kejahatan siber dalam bentuk penyebaran konten ilegal, *hate speech* dan sejenisnya (wantiknas.go.id, 2018). Ditambah dengan pengguna internet di Indonesia yang mencapai 132.700.000 hal ini yang kemudian membuat pemerintah Indonesia mulai memperhatikan permasalahan kejahatan siber (internetworldstats.com, 2016).

Pemerintah telah berupaya dalam meningkatkan keamanan sibernya, upaya ini kemudian dibagi menjadi dua yaitu upaya dalam negeri pemerintah Indonesia dalam meningkatkan keamanan siber nya adalah dengan mengeluarkan beberapa peraturan No.26/PER/M.KOMINFO/5/2007 yang berisikan mengenai pengamanan, pemanfaatan, jaringan telekomunikasi berbasis protokol internet yang kemudian direvisi dengan peraturan menteri komunikasi dan informatika No. 16/PER/M.KOMINFO/10/2010 dan kemudian diperbarui lagi dengan peraturan menteri komunikasi dan informatika No. 29/PER/M.KOMINFO/12/2010, selanjutnya pemerintah Indonesia mengeluarkan kebijakan keamanan siber dengan mengeluarkan peraturan mengenai penggunaan ISO/IEC 27001 yang diterbitkan pada tahun 2009 dan merupakan Standar Nasional Indonesia (SNI) untuk standarisasi Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Managemen System* (ISMS) yang memberikan gambaran mengenai yang harus dilakukan oleh sebuah organisasi atau enterprise dalam upaya pengimplementasian konsep keamanan informasi (Mahendra, 2017).

Upaya luar negeri yang berupa kerjasama yang dilakukan oleh pemerintah Indonesia dengan berbagai negara dengan sistem keamanan terbaik di dunia salah satunya adalah bekerjasama dengan pemerintah Inggris yang memiliki sistem keamanan tertinggi di dunia (news.itu.int, 2019), kerjasama ini kemudian ditandatangani pada 14 Agustus 2018 di Kantor Kementerian Luar Negeri, Jakarta Pusat, dalam penandatangan tersebut disepakati; Implementasi dan Pengembangan Strategi Keamanan Siber Nasional, Pengelolaan Insiden Siber, Kejahatan Siber, Pelatihan dan Seminar Kesadaran Keamanan Siber dan Peningkatan Kapasitas (bssn.go.id, 2018).

Namun sejak tahun 2018 sampai dengan tahun 2020 kerjasama yang disepakati antara Indonesia telah berjalan, namun dari 5 program yang disepakati hanya 3 program yang berhasil dijalankan hingga pada tahun 2020, dalam kerjasama ini kemudian dilakukan oleh BSSN yang dibantu oleh *The National Cyber Security Centre* Inggris

berperan dalam mendukung dengan melakukan operasionalisasi arah kebijakan serta memberikan pelatihan dalam melaksanakan setiap rencana yang dikeluarkan oleh BSSN, sehingga serangkaian strategi dapat diimplementasikan secara optimal, poin-poin strategi ini kemudian masuk dalam poin kerjasama yang ada dalam MoU, yaitu: (bssn.go.id, 2018)

Implementasi dan Pengembangan Strategi Keamanan Siber Nasional

Dalam kerjasama ini dilakukan oleh Badan Siber dan Sandi Nasional dibantu dengan Inggris melalui *The National Cyber Security Centre* (NCSC) yang dalam pelaksanaannya terbagi atas dua program yaitu satu program teknis yaitu Program Pengembangan Siber dan Sandi Negara serta satu program generik yaitu Program Dukungan Manajemen dan Pelaksanaan Tugas Teknis Lainnya BSSN, dalam kerjasama teknis ini:

a. Mendukung arah kebijakan Penguatan Payung Hukum dalam pelaksanaan tugas BSSN, maka NCSC membantu dalam mendiskusikan strategi yang akan dikembangkan oleh BSSN untuk melakukan analisis bersama mengenai kebutuhan regulasi yang diperlukan untuk menunjang kewenangan dan optimalisasi kinerja BSSN dan melakukan tindak lanjut atas hasil analisisi tersebut.
b. Mendukung arah kebijakan Pengembangan Roadmap dan Pedoman/Standar Keamanan Siber, dalam strategi ini Inggris menyiapkan kebutuhan pedoman/standar dan roadmap yang merupakan alur dalam mendukung pelaksanaan tugas BSSN. Roadmap ini diawali dengan diskusi bersama membicarakan mengenai keamanan siber dan kejahatan siber yang terjadi di Indonesia, dan selanjutnya dari hasil diskusi tersebut disusun roadmap dan pedoman/standar yang komprehensif dan mampu memberikan arahan yang jelas bagi peningkatan kinerja BSSN di masa mendatang, pada strategi dilaksakan pada konferensi Cyber Security pada tahun 2019 yang dilakukan di Jakarta *Convention Center* (JCC).
c. Mendukung arah kebijakan Pengembangan Sarana, Prasarana dan Teknologi Keamanan Siber, dalam strategi ini mencakup pengadaan, pemeliharaan dan pengembangan prasarana, sarana, dan teknologi yang sangat dibutuhkan bagi keamanan siber dan sandi nasional, dalam hal ini pihak BSSN dan *The National Cyber Security Centre* (NCSC) masih masih melakukan perencanaan untuk melakukan *Transfer of Technology* (ToT) seperti penguatan sistem keamanan di Indonesia.
d. Mendukung arah kebijakan Pengembangan SDM yang Kompeten dalam Keamanan Siber, maka strategi yang dikembangkan adalah secara terus menerus melakukan program pendidikan, pelatihan, pengembangan mutu dan peningkatan kompetensi SDM, dalam hal ini pemerintah inggris membantu dengan memberikan pelatihan kepada pihak-pihak terkait tersebut, seperti yang dilakukan pada tahun 2020, melalui lembaga yayasan InfraDigital, pemerintah Inggris beserta BSSN mulai melakukan pelatihan terhadap 6.000 siswa SMK dari kalangan prasejahtera di Jawa Barat yang kemudian para siswa tersebut diberikan sertifikasi cyber security dan terhubung dengan industri terkait pada bidang pengamanan siber dalam negeri dan luar negeri, program ini berjalan bertahap selama 3 tahun hingga 2022.

Setiap strategi dan program tersebut terbentuk sesuai dengan pertemuan atau seminar yang dilakukan oleh BSSN bersama dengan NCSC.

Seminar dan Pelatihan di Bidang Keamanan Siber

Dalam MoU kedua negara yaitu Indonesia dan Inggris bersepakat untuk mengkampanyekan kesadaran keamanan informasi dan siber untuk masyarakat, serta mengedukasi masyarakat tentang nilai infomasi dan dampak penyalahgunaannya. Sedangkan dalam hal pelatihan, BSSN menjalin kerjasama teknis dengan kementrian dalam negeri untuk meningkatkan keterampilan dan keahlian SDM siber untuk mencapai ketahanan ranah siber Indonesia yang kuat.

Dalam kerjasama ini Indonesia melakukan Pelatihan Teknis Keamanan Siber bersama dengan NCSC yang dibuka langsung oleh Deputi IV Bidang Pemantauan dan Pengendalian BSSN Mayjen TNI (Mar) Dr. Suharyanto, S.E., M.M. Pelatihan tersebut di laksanakan di ruang serbaguna pusat pendidikan dan pelatihan (Pusdiklat) BSSN pada hari Rabu, 7 Oktober 2019. Pelatihan Teknis Keamanan Siber diikuti oleh para pegawai dilingkungan pemerintah daerah di Indonesia. Peserta yang mengikuti kegiatan pelatihan teknis keamanan siber berjumlah 27 orang peserta.

Pelatihan yang diberikan kepada peserta ini berupa kompetensi di bidang Keamanan Jaringan; Pertahanan dan Serangan Siber; Pengelolaan Ancaman; Kriptografi, Manajemen Risiko dan Penanggulangannya; serta keahlian mendasar pada pengaturan kebijakan Sistem Operasi Windows dan Linux (pusdiklat.bssn.go.id, 2019).

Selain itu NCSC membantu BSSN melakukan pameran pada tahun 2019 yaitu pameran "*Cybersecurity Indonesia* (CSI) 2019" yang berlangsung selama 3 hari dari tanggal 6 – 8 November 2019 di Assembly Hall, Jakarta Convention Center, dan terbuka untuk umum, hal ini dilakukan agar masyarakat Indonesia dapat mengetahui keamanan siber yang dimiliki oleh Indonesia serta juga menunjukan kehebatan dari keamanan siber negara lain termasuk Inggris yang membantu dalam pameran tersebut, pameran ini resmi dibuka oleh Letnan Jenderal TNI (Purn.) Hinsa Siburian, Kepala Badan Siber dan Sandi Negara (BSSN) didampingi oleh Marsekal Muda Rus Nurhadi Sutedjo, Deputi Bidang Koordinasi Komunikasi, Informasi dan Aparatur Kementerian Koordinator Bidang Politik Hukum dan Keamanan Republik Indonesia, serta duta besa Inggris Moazzam Malik dan perwakilan dari NCSC dalam acara ini juga diikuti oleh negara lain yaitu Singapore, Polandia, Hungaria, Amerika, Russia, dan Korea.

Pengembangan Kapasitas

Bersama Inggris, pemerintah Indonesia membuat *Computer Security Incident Response Team* (CSIRT) yang dibentuk untuk tujuan menangani insiden serangan siber, BSSN akan bertanggung jawab untuk menerima, meninjau dan menanggapi laporan dan aktivitas insiden keamanan siber CSIRT ini yang dibentuk pada tanggal 20 Desember 2018, yang terus disempurnakan melalui bantuan dari NCSC agar terciptanya keamanan siber di Indonesia.

Pembentukan CSIRT di lakukan di instansi pemerintahan di setiap wilayah Indonesia yang dalam pembentukannya dilakukan antara pemerintah pusat dan daerah/kota. Selain itu dalam program ini NCSC melakukan pengembangan terhadap SDM di Indonesia yang juga menjadi salah satu prioritas BSSN, hal ini dikarenakan perkembangan teknologi yang semakin meningkat menjadikan diperlukannya peningkatakan SDM untuk dapat memahami perkembangan teknologi tersebut.

Dalam pengembangan kapabilitas SDM yang dilakukan adalah dengan memberikan tugas kepada setiap Deputi untuk bertanggung jawab dalam pemberian target capaian oleh setiap bagian yaitu:

a. Pendayagunaan Kapabilitas Identifikasi dan Deteksi yang andal dengan 2 (dua) Indikator yang pertama adalah Tingkat Cakupan Penilaian Risiko Keamanan Siber Nasional dan yang kedua adalah Tingkat Cakupan Potensi Ancaman Siber yang Berhasil Dideteksi. Pencapaian ini menjadi tanggung jawab Deputi Bidang Identifikasi dan Deteksi di BSSN.
b. Pengembangan Kapabilitas Proteksi yang optimal dengan Indikator yaitu Tingkat Penerapan Proteksi Keamanan Siber. Pencapaian ini menjadi tanggung jawab Deputi Bidang Proteksi BSSN.
c. Pendayagunaan Kapabilitas Penanggulangan dan Pemulihan yang Kapabel yaitu Tingkat Kesiapan Stakeholder terhadap Insiden Keamanan Siber Nasional. Pencapaian menjadi tanggung jawab Deputi Bidang Penanggulangan dan Pemulihan BSSN.
e. Pendayagunaan Kapabilitas Pemantauan dan Pengendalian yang Profesional dengan Indeks Persepsi Publik Terhadap Reputasi Pemerintah (BSSN) dalam Ranah Siber. Pencapaian menjadi tanggung jawab Deputi Bidang Pemantauan dan Pengendalian BSSN.

Pada poin kerjasama ini BSSN dan NCSC selalu melakukan kontak serta berhubungan dengan baik agar strategi dalam pengembang kapasitas ini terus berkelanjutan. Namun dalam kerjasama yang disepakati ada beberapa program yang tidak berjalan yaitu program pengelolaan manajemen insiden, padahal program ini berisikan mengenai pembentukan dan pengelolaan titik kontak mengenai manajemen insiden nasional dan mengidentifikasi mekanisme komukinaksi yang sesuai, dalam manajemen ini berfokus pada analisis dampak insiden, mitigasi pasca insiden, penanggulangan insiden, dan pemulihan pasca insiden di bidang keamanan siber, mengkonsultasikan dan mengkoordinasikan dalam menanggapi insiden keamanan siber terutama ketika informasi tersebut terkait dengan kedua negara, hal ini disepakati agar kedua negara dapat menjaga keamanan dalam negaranya masing-masing dan dapat saling berhubungan atas kekurangan dalam manajemen yang dilakukan, mempromosikan pentingnya koordinasi dan manajemen insiden yang efektif, pada bagian ini memerlukan kedua bagian diatas sehingga dapat berjalan dengan baik dalam promosi keamanan siber yang dilakukan.

Program pengelolaan manajemen insiden tidak berjalan karena masih masuk dalam strategi nasional Indonesia dan NCSC belum melakukan tindakan lebih lanjut mengenai poin kerjasama ini. Selain itu terdapat program kerjasama kejahatan siber yang juga belum berjalan namun sudah direncanakan berjalan pada tahun 2020. Beberapa alasan yang menjadi tertundanya berjalannya program kerjasama ini adalah:

1. Indonesia melalui BSSN masih melakukan perencanaan kedepan untuk keamanan nasional.
2. Belum adanya kesempatan bagi pemerintah Indonesia untuk mengirimkan delegasinya untuk mengikuti *join exercise* dalam upaya penguatan kapasitas di bidang cyber forensics dan kemampuan investigasi barang bukti digital.
3. Munculnya virus Corona atau juga dikenal dengan Covid-19 ini juga menjadi salah satu kendala dalam menjalankan point kerjasama ini.

Kedua hal inilah kemudian yang menjadi hambatan pemerintah Indonesia dalam penjalanan program kerja "kejahatan siber" yang sudah tertulis dalam MoU.

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 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.

Kerjasama yang dilakukan ini juga memiliki kepentingan sendiri bagi pemerintah Inggris, bagi Mark Field yang merupakan menteri muda Inggris urusan Asia Pasifik, 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 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 keaman siber.

Kerjasama antara Indonesia dan Inggris dalam keamanan 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.

Selain itu, kedua negara juga sepakat untuk meningkatkan nilai perdagangan yang dalam lima tahun terakhir berada di bawah potensi dengan nilai hanya mencapai 2,4 hingga 2,5 miliar dolar Amerika Serikat (AS). Kedua negara sepakat mencari cara-cara kreatif guna meningkatkan kerjasama perdagangan tersebut, selanjutnya Indonesia dan Inggris juga sepakat untuk membuat kembali partnership forum, yang merupakan forum pertemuan antara menteri dari kedua negara dalam upaya meninjau berbagai kerjasama karena mekanisme kerjasama bilateral yang banyak dan berada di berbagai bidang.

## Kesimpulan

Dalam kerjasama yang dilakukan oleh Indonesia melalui BSSN dengan Inggris melalui NCSC berhasil meningkatkan keamanan siber di Indonesia, namun yang berjalan dan ada peran NCSC didalam nya hanya tiga poin yaitu;

1. Implementasi dan Pengembangan Strategi Keamanan Siber Nasional, dalam implementasi ini berisikan berbagai program strategi BSSN yang dibantu oleh NCSC agar strategi dapat berjalan sesuai dengan kebutuhan negara Indonesia, seperti penguatan kebijakan hukum keamanan siber, strategi pengembangan SDM, perencanaan ToT dan juga melakukan pameran.

2. Seminar dan Pelatihan di Bidang Keamanan Siber, yang dijalankan melalui Pelatihan Teknis Keamanan Siber dan juga pameran Keamanan Siber yang dilakukan bersama NCSC.
3. Pengembangan Kapasitas, dalam poin ini BSSN dan NCSC berfokus untuk meningkatkan kapasitas keamanan sibernya melalui Computer Security Incident Response Team (CSIRT) dan peningkatan SDM berkelanjutan

**Daftar Pustaka**

225 juta serangan siber masuk indonesia sepanjang 2018, https://www.cnnindonesia.com/ teknologi/20190207210646-185-367347/225-juta-serangan-siber-masuk -indo nesia-sepanjang-2018

Akamai cyberattack country-list.jpg, https://cms.dailysocial.id/wp-content/uploads/2013/07/akamai_cyberattack_ country-list.jpg

BSSN Luncurkan Government – Computer Security Incident Response Team (Gov-CSIRT) Indonesia, https://bssn.go.id/bssn-luncurkan-government-computer-security-incident-response-team-gov-csirt-indonesia/

BSSN Tandatangani Nota Kesepahaman Kerjasama di Bidang Keamanan Siber D engan Pemerintah Inggris, https://bssn.go.id/bssn-tandatangani-nota-kesepahaman-kerjasama-di-bidang-keamanan-siber-dengan-pemerintah-inggris-raya/

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

Charles W.L. Hill, Chow-Hou Wee, Krishna Udayasankar, Bisnis Internasional,2014, hal 210

Cyber crime di Indonesia masuk 10 besar dunia, https://industri.kontan.co.id/news /duh-cyber-crime-di-indonesia-masuk-10-besar-dunia

Diskusi Publik Peningkatan Kapasitas Keamanan Siber Indonesia https://bssn.go.id/diskusi-publik-peningkatan-kapasitas-keamanan-siber-indonesia

Hidayat Chusnul Chotimah (Politica Vol. 10 No. 2 November 2019) Ilmu Hubungan Internasional, Universitas Teknologi Yogyakarta. Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara.

Hidayat Chusnul Chotimah, (2019) "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara." http://jurnal.dpr.go.id/index.php/politica/article/download/1447/756

Hidayat Chusnul Chotimah, "Membangun Pertahanan dan Keamanan Nasional dari Ancaman Cyber di Indonesia," Jurnal Diplomasi, Volume 7 No. 4, :109, http: //jurnal.dpr.go.id/index.php/politica/article/download/1447/756

http://www.wantiknas.go.id/wantiknasstorage/file/img/kajian/POLICY%20PAPER%204%20-%20Cyber%20Security.pdf

Indeks keamanan siber indonesia naik 29 tingkat, https://inforial.tempo.co/info/1001099/indeks-keamanan-siber-indone sia-naik-29-tingkat

Indonesia-Inggris sepakat kerjasama keamanan siber, https://www.menpan.go.id/site/berita-terkini/berita-daerah/indonesia-inggris-sepakat-kerja-sama-keamanan-siber

Jenis cybercrime berdasarkan motif dan aktivitasnya, https://bapenda.jabarprov.go.id/2017/11/10/jenis-cybercrime-berdasarkan-motif-dan-aktivitasnya

Jumlah Laporan Polisi yang dibuat masyarakat, https://patrolisiber.id/statistic

Kiyono, K. (1969). A Study on the Concept of The National Interest of Hans J.Morgenthau:as The Standard of American Foreign Policy.

Lene Hansen and Helen Nissenbaum, "Digital Disaster, cybersecurity, and the Copenhagen School", International Studies Quarterly, Vol. 53, No. 4 (2009): 1160.

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.

Nur Khalimatus Sa'diyah dan Ria Tri Vinata, "Rekonstruksi Pembentukan National Cyber Defense sebagai Upaya Mempertahankan Kedaulatan Negara," Perspektif, Volume XXI No. 3 : 169.

Patrick Jagoda, "Speculative Security", Dalam Reveron, Derek S., Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World (eds), (Washington, D.C.: Georgetown University Press, 2012), 22.

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