Global Political Studies Journal
Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

Kerjasama Pemerintah Indonesia Dan Pemerintah Kerajaan Inggris Dalam Bidang Keamanan Siber

Monica Romauly Weu[1]
[1]Program Studi Ilmu Hubungan Internasional, Universitas Komputer Indonesia
Jl. Dipati Ukur No.112-116, Bandung, Indonesia
e-mail: **monicaromauly@mahasiswa.unikom.ac.id**

Abstract

The development of increasingly advanced technology provides many conveniences that are obtained. However, technological advances not only have a positive impact, but also have a negative impact. The high number of cyber crimes is one form of negative impact from the development of information and communication technology. Indonesia and the UK are countries that cannot escape cyber threats and attacks. Thus, the two countries need to strengthen cyber resilience and security. This study aims to determine the cooperation carried out by Indonesia and the UK in the cybersecurity sector. From this research shows that the implementation of cyber security cooperation is implemented in the form of a cyber dialogue forum that discusses Capacity Development, meanwhile the cooperation carried out is not only limited to improving defense and cybersecurity in each country, but there are other interests that want obtained through this collaboration. In the implementation of this cyber security cooperation there are obstacles faced by the two countries, but the two countries have an optimistic view that this cooperation will have a positive impact on the sustainability of relations between the two countries.

Keywords— *Indonesia, UK, Cybersecurity Cooperation, National Interests.*

Abstrak

Perkembangan teknologi yang semakin maju memberikan banyak kemudahan yang diperoleh. Namun, dengan kemajuan teknologi tidak hanya memberikan dampak positif, tetapi juga memberikan dampak negatif. Tingginya angka kejahatan siber merupakan salah satu bentuk dampak negatif dari perkembangan teknologi informasi dan komunikasi. Indonesia dan Inggris merupakan negara-negara yang tidak dapat trhindar dari ancaman dan serangan siber. Sehingga, kedua negara perlu memperkuat ketahanan dan keamanan siber. Penelitian ini bertujuan untuk mengetahui kerjasama yag dilaksanakan oleh Indonesia dan Inggris dalam bidang keamanan siber. Dari penelitian ini menunjukkan bahwa pelaksanaan kerjasama keamanan siber ini diterapkan dalam bentuk cyber dialog forum yang membahas mengenai Pengembangan Kapasitas, sementara itu kerjasama yang dilakukan tidak hanya sebatas pada meningkatkan pertahanan dan keamanan siber di masing-masing negara, namun adanya kepentingan-kepentingan lain yang ingin diperoleh melalui kerjasama ini. Dalam pelaksanaan kerjasama keamanan siber ini terdapat kendala-kendala yang dihadapi oleh kedua negara, namun kedua negara memiliki pandangan yang optimis bahwa kerjasama ini akan berdampak positif bagi keberlangsungan hubungan kedua negara.

Kata kunci— Indonesia, Inggris, Kerjasama Keamanan Siber, Kepentingan Nasional.

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

1. 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 kehadiran internet. Kehadiran internet telah menciptakan dunia baru bagi umat manusia yang berbasis komputer dengan menawarkan realitas yang baru dalam kehidupan manusia dengan realitas virtual atau maya. Kelebihan dari Internet yakni 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).

Namun, 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 bidang, seperti data perbankan, jaringan militer, bahkan sistem pertahanan negara.

Hal ini dikarenakan sifat *Cyberspace* yang bersifat global menyebabkan *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. 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. 2016. Strategi Keamanan Cyber Amerika Serikat. Diakses darihttps://search.unikom.ac.id/index.php/jipsi/article/view/239).

Di Indonesia, serangan siber yag dilakukan oleh pelaku tindak kejahatan siber dilaporkan sesuai dengan hasil 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 (Laporan Tahunan Honeynet Project BSSN IHP, 2018, diakses melalui https://bssn.go.id/wp-content/uploads/2019/02/Laporan-Tahunan-Honeynet-Project-BSSN_IHP-2018.pdf).

Dari tindakan penyerangan tersebut, menimbulkan dampak yang buruk bagi Indonesia terutama pada sektor perekonomian. 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 (diakses melalui https://news.microsoft.com/id-id/2018/05/24/ancaman-keamanan-siber-menyebabkan-kerugian-ekonomi-bagi-

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

organisasi-di-indonesia-sebesar-us34-2-miliar/).

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 (diakses dari https://www.cnbc.com/2017/01/11/ pada 14 Mei 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.

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. 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.

Dengan 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 secara terus-menerus dalam meningkatkan sistem pertahanan dan keamanan siber, dan peningkatan akan kemampuan kapasitas dan kuantitas dari sisi teknologi informasi dan juga komunikasi serta sumber daya manusia.

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 tahun 2016-2021 yakni bersedia bekerjasama secara internasional dalam menjaga keamanan siber internasional, dengan tujuan Inggris yakni untuk menjadi negara yang aman di dunia maya untuk melakukan bisnis dan mengamankan kepentingan Inggris yang berada di luar yuridksi negara Inggris yang berdampak secara langsung pada keamanan nasional Inggris.

Dengan demikian, melihat permasalahan siber yang dialami oleh Indonesia dan juga untuk mencapai tujuan strategi nasional Inggris tahun 2016-2021, maka Pemerintah Inggris menginisiasi kerjasama secara langsung dengan Pemerintah Indonesia di bidang keamanan siber.

1.2 Rumusan Masalah

Dari uraian latar belakang tersebut, maka peneliti merumuskan rumusan masalah sebagai berikut:

a) Bagaimana penerapan kerjasama antara Indonesia dan Inggris dalam bidang keamanan siber berdasarkan MoU yang telah disepakati?
b) Apa yang menjadi kepentingan Indonesia dan Inggris dalam melakukan kerjasama dalam bidang keamanan siber?
c) Apa yang menjadi kendala terhadap pelaksanaan kerja sama dalam bidang keamanan siber?
d) Bagaimana prospek kerjasama yang dilakukan oleh Indonesia dan Inggris dalam keamanan siber?

2. Kajian Pustaka dan Kerangka Pemikiran

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

a) Hubungan Internasional

Pada dasarnya Hubungan Internasional merupakan suatu ilmu yang mempelajari hubungan antar negara. Istilah hubungan internasional mempunyai beberapa macam arti yakn sebagai berikut; Suatu bidang spesialisasi yang meliputi aspek-aspek internasional dari beberapa cabang ilmu pengetahuan; Sejarah baru dari politik internasional; Semua aspek internasional dari kehidupan sosial manusia dalam arti bahwa semua tingkah laku manusia yang terjadi atau berasal di suatu negara dan dapat mempengaruhi tingkah laku negara lain; Suatu cabang ilmu yang berdiri sendiri (Darmayadi.2015: 22).

Berdasarkan sejarahnya, hubungan internasional lahir pasca era Perang Dunia Pertama dengan tujuan agar dunia mampu menghindari konflik besar di masa yang akan datang serta bertujuan untuk memastikan interaksi negara-negara di dunia berjalan secara damai, sehingga diharapkan bahwa melalui studi hubungan internasional ini mampu melahirkan pendekatan-pendekatan ataupun pemikiran-pemikiran terkait solusi perdamaian untuk dunia (Triwahyuni.2015:51).

Hubungan internasional saat ini berada pada masa transisi dimana faktor-faktor dalam hubungan internasional tidak mengalami perubahan, namu suasana atau lingkungan internasional yang berubah dan masih terus mengalami perubahan. Perubahan ini disebabkan oleh perubahan sistem ketatanegaraan, perkembangan teknologi dan informasi yang begitu cepat, pernanan yang makin bertambah penting dari negara-negara yang bukan negara Barat, dan *revolution of rising expectations* yang terdapat pada negara-negara yang sedang berkembang (Darmayadi. 2015: 25).

Hubungan internasional saat ini tidak hanya sebatas mengenai politik, tetapi mencakup semua unsur-unsur yang terlibat dalam interaksi baik berupa ekonomi, sosial-budaya, ideologi, hukum, pertahanan dan keamanan yang melintasi atau melewati batas nasional negara antara aktor-aktor ataupun kondisi yang terlibat dalam interaksi tersebut. Wujud dari interaksi yang ditimbulkan dapat berupa kerjasama, perang, pembentukan aliansi, konflik, serta interaksi dalam suatu organisasi internasional.

Dengan demikian, maka hubungan internasional kontemporer dapat diartikan sebagai suatu interaksi yang melibatkan fenomena sosial yang berupa aspek ideologi, politik, hukum, ekonomi, sosial-budaya, dan pertahanan keamanan yang melintasi batas nasional suatu negara antara aktor-aktor baik yang bersifat pemerintah maupun non-pemerintah, termasuk kajian-kajian yang relevan yang mengitari aksi tersebut (Perwira dan Yani, 2017: 8).

Hubungan internasional sangat penting bagi suatu negara dalam memenuhi kebutuhan nasionalnya, maka sangat jelas bahwa suatu negara membutuhkan negara lain sehingga tujuan negara dapat tercapai.

b) Kerjasama Internasional

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

Kerjasama internasional merupakan suatu bentuk hubungan yang dilakukan oleh suatu negara dengan negara

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

lainnya dalam rangka memenuhi kebutuhan dalam negeri. Kerjasama yang dilakukan meliputi aspek ekonomi, sosial, budaya, dan keamanan yang berdasarkan pada politik luar negeri dari masing-masing negara.

Isu utama dari kerjasama internasional dapat dilihat dari sejauhmana keuntungan yang dapat diperoleh secara bersama melalui kerjasama, serta mendukung konsepsi dari kepentingan tindakan yang unilateral dan kompetitif (Perwita dan Yani, 2017: 34).

Terbentuknya kerjasama internasional dikarenakan kehidupan internasional yang beraneka ragam seperti politik, sosial, budaya, ekonomi, lingkungan hidup, pertahanan, kemanan dan ideologi, dan juga adanya kelebihan-kelebihan yang dimiliki oleh negara lain yang mana kelebihan-kelebihan tersebut tidak semuanya dimiliki oleh negara di dunia. Dengan demikian hal ini akan menimbulkan hubungan saling kebergantungan antara negara yang satu dengan negara yang lain, dimana hubungan saling membutuhkan ini dilatarbelakangi oleh kepentingan nasional suatu negara.

Untuk memenuhi kebutuhan-kebutuhan tersebut, maka suatu negara akan menjalin hubungan dengan negara lain yang kemudian akan dilanjutkan dengan manjalin suatu hubungan kerjasama antar negara dalam bentuk Memorandum of Understanding atau dikukuhkan dalam bentuk lainnya.

c) Kepentingan Nasional

Konsep kepentingan nasional sangat diperlukan dalam menjelaskan sikap yang diambil oleh suatu negara dalam sistem internasional. Kepentingan nasional menjadi kunci utama dalam merumuskan kebijakan luar negeri. Kepentingan nasional dapat diartikan sebagai tujuan fundamental dan faktor penentu akhir yang mengarahkan para pembuat keputusan dari suatu negara dalam merumuskan kebijakan luar negerinya (Perwita dan Yani, 2017: 35).

Kepentingan nasional negara merupakan kebutuhan penting negara seperti ekonomi, militer, keamanan, pertahanan. Keberadaan suatu negara tetap berlanjut apabila tercapainya kepentingan-kepentingan negara. Kepentingan yang dimaksudkan adalah suatu hal yang menguntungkan, sehingga kepentingan nasional ini dapat pula diartikan sebagai hal yang menguntungkan bagi bangsa. Kepentingan nasional suatu negara bersifat vital sehingga yang menjadi priotitas utama adalah mewujudnyatakan kepentingan tersebut.

Konsep kepentingan nasional yang dikemukakan oleh Hans J. Morgenthau dirangkum dalam tiga bagian yakni: pertama, perlindungan terhadap identitas fisik yang dalam arti bahwa negara dapat mempertahankan integritas wilayahnya; kedua, perlindungan terhadap identitas politik yang diartikan dengan mempertahankan rezim politik dan ekonominya; ketiga, terhadap kulturnya, dalam arti mampu mempertahankan linguistik dan sejarahnya (Yani, Montratama dan Wahyudin, 2017: 17).

Dalam kepentingan nasional terdapat juga aspek-aspek yang menjadi identitas negara. Hal ini dapat ditinjau dari fokus negara untuk mewujudkan pencapaian kepentingannya dalam menjaga kelangsungan bangsanya. Dari berbagai kepentingan-kepentingan tersebut dapat dirumuskan dalam perencanaan jangka pendek, menengah, dan perencanaan dalam jangka panjang.

d) Konsep Keamanan

Suatu hubungan yang terus berlangsung dalam proses perubahan baik pada tingkat domestik, regional, maupun

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

global akan membentuk suatu lingkup ancaman dan gangguan keamanan nasional suatu negara yang bersifat kompleks. Menurut Buzan, keamanan berkaitan dengan masalah kelangsungan hidup (survival), sehingga perlu adanya suatu tindakan yang memprioritaskan isu tersebut agar dapat ditangani sesegara mungkin dengan menggunakan sarana-sarana yang ada dalam menangani masalah tersebut (Perwita, A.A.B. dan Yani, Y.M : 2005).

Dalam konsepsi klasik, keamanan lebih diartikan sebagai usaha untuk menjaga keutuhan teritorial negara dari ancaman yang muncul dari luar. Pasca berakhirnya perang dingin, membuka era baru dalam sudut pandang masyarakat akan keamanan. Keamanan tidak lagi diartikan secara sempit sebagai hubungan konflik militer saja, tetapi keamanan pada hari ini berpusat pada keamanan masyarakat atau dikenal dengan istilah kemanan non-tradisional. Keamanan non-tradisional berfokus kepada *Human Security*.

Beberapa contoh keamanan non-tradisonal membahas mengenai kejahatan transnasional seperti terorisme, penyelundupan manusia, senjata, kejahatan lingkungan, kejahatan hak asasi manusia, penyelundupan manusia, teknologi dan kesehatan.

Sebuah keadaan yang dapat membahayakan keamanan nasional merupakan perpaduan dari ancaman dan kerawanan. Keduanya berhubungan erat serta berhubungan dengan keamanan baik nasional maupun internasional. Yang dapat dilakukan sebuah negara untuk menangkal hal ini adalah dengan membuat kebijakan keamanan nasional yang difokuskan pada negara itu sendiri, sebagai upaya untuk meredam keamanan dalam negeri, sekaligus dengan tidak melupakan kebijakan luar negeri untuk mengurangi ancaman dari luar.

e) Keamanan Siber

Tindak kejahatan dunia maya atau yang dikenal dengan istilah cyber crime yang bersifat tidak mengenal batas merupakan suatu bentuk tindakan ancaman terhadap keamanan individu hingga global. Oleh karena itu, ruang siber perlu mendapatkan perlindungan yang layak guna menghindari potensi yang dapat merugikan pribadi,organisasi bahkan negara.

Istilah pertahanan siber muncul sebagai upaya untuk melindungi diri dari ancaman dan gangguan tersebut (https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf).

Cyber security merupakan tindakan untuk melindungi operasi sistem komputer atau integrasi data di dalamnya dari aksi-aksi kejahatan. 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 (Yani, Montratama, dan Mahyudin, 2017: 73).

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 terhindarkan ancaman terhadapnya dengan semakin kompleksnya berbagai aktor yang terlibat dalam aktivitas yang terkoneksi melalui internet (Octa Putri, 2015: 137).

Ancaman-ancaman tersebut dapat berupa pencurian identitas, gambar pelecehan seksual, penyebaran virus, penipuan lelang internet, spionase, dan juga

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

kejahatan teroris untuk penghasutan radikalisme yang menimbulkan ancaman serius bagi keamanan nasional dan internasional. Ancaman-ancaman ini dapat disebabkan oleh kelemahan dalam mendesain internet, kelamahan dalam perangkat keras dan lunak serta langkah dalam penempatan sistem yang disebut sebagai more critical dalam dunia maya atau virtual (Octa Putri, 2015: 137).

Serangan siber merujuk kepada penggunaan kode komputer untuk mengganggu fungsi dari sistem komputer untuk tujuan politik ataupun strategi tertentu. Karakteristik penyerangan ini sesuai dengan tujuan dan kepentingan yang ingin diperoleh dari penyerangan siber tersebut.

Tujuan dari penyerangan tersebut tidak hanya sekedar menghancurkan sistem komputer, namun juga kepada aspek-aspek ekonomi, sosial atau terhadap pemerintahan. Penyerangan siber ini tidak bergantung pada letak geografis, perangkat komputer tidak berpengaruh kepada jarak geografis ataupun letak suatu wilayah, hal ini yang menjadikan potensi serangan siber lebih luas dan lebih banyak dari serangan konvensional.

3. Metode Penelitian

Dalam meneliti penelitian ini, penulis menggunakan metode penelitian kualitatif. Penelitian ini menggunakan teknik pengumpulan data melalui studi pustaka, penelusuran data online, dokumentasi, wawancara. Untuk metode wawancara, teknik penentuan informan yang peneliti gunakan adalah teknik purposive sampling. Dalam penelitian kualitatif ini, peneliti menganalisis data dengan menggunakan teknik reduksi data.

4. Hasil dan Pembahasan

4.1. Penerapan Kerjasama Antara Indonesia dan Inggris Dalam Bidang Keamanan Siber

Kerjasama antara Indonesia dan Pemeritah Kerajaan Inggris dalam bidang keamanan siber merupakan suatu kerjasama yang baru terlaksana. 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.

Peserta yang menjadi perwakilan dari Republik Indonesia diwakili oleh Badan Sandi dan Siber Negara dan untuk Kerajaan Inggris Raya diwakili oleh Kementerian Luar Negeri dan Persemakmuran. Namun, kerjasama ini tidak hanya mutlak diikuti oleh Badan Sandi dan Siber Negara dan juga Kementerian Luar Negeri dan Persemakmuran, tetapi juga dapat diikuti oleh instansi pemerintahan yang lain tergantung pada konteks pembahasan dan juga tergantung pada jumlah porsi yang dibutuhkan pada pembahasan dalam *cyber dialog forum*.

Pada *cyber dialog forum* topik 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. Pelaksanaan Peningkatan Kapasitas di tahun 2019 diawali dengan 2 program pembahasan

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

yakni *Cyber Law* dan *Cybersecurity Awareness*.

Pada pembahasan *cyber law*, kedua peserta membahas terkait *United Nations Group of Governmental Experts* (UN GGE) dimana Indoensiad dan Inggris dipilih sebagai 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, (diakses dari https://www.un.org/disarmament/).

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 (diakses dari https://www.un.org/).

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 hukum internasional yang dapat diberlakukan dalam operasi serangan siber. Pada konteks ini, Pemerintah Inggris berusaha untuk menggambarkan Tallinn Manual 2.0 yang menjadi pedoman yang komprehensif dalam mengatur operasi siber.

Hal ini menjadi pembahasan pada kerjasama siber yang dilakukan oleh Indonesia dan Inggris, karena sejauh ini Tallinn Manual 2.0 belum menjadi bahan pertimbangan pemerintah Indonesia dalam membuat kebijakan keaman siber. Karena, Indonesia tidak terlibat dalam perumusannya, sehingga tidak diketahui apakah kepentingan nasional Indonesia bisa tercakup di dalamnya atau tidak. Sehingga, Tallin Manual 2.0 masih menjadi kajian bagi Indonesia untuk mengetahui apakah Tallin Manual 2.0 dapat menjadi jembatan bagi Indonesia untuk memenuhi kepentingan Indonesia terutama pada sektor keamanan siber.

Pembahasan berikutnya yakni terkait *Cybersecurity 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 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

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

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.

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

4.2.1. Kepentingan Indonesia

Pemerintah Indonesia memahami bahwa ancaman dunia siber merupakan suatu tantangan yang akan berdampak pada perekonomian serta keamanan negara yang dapat mengganggu kedaulatan Indonesia, sebab pelaku tindak kejahatan siber akan terus berusaha untuk mengganggu, menyelidiki bahkan menyerang sektor pemerintahan, swasta, perusahaan dan individu. Sehingga perlu adanya penguatan dalam sumber daya manusia serta kapasitas peningkatan 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. 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, 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.

Hal ini bertujuan untuk meningkatkan kualitas dan skala penelitian keamanan siber akademik dan pelatihan pascasarjana; memudahkan bagi para akademisi dalam melakukan proses identifikasi penelitian terhadap keamanan di dunia maya dan pelatihan terbaik pada program pascasarjana yang ditawarkan oleh Pemerintah Inggris terkait dunia siber.

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

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 negara negara Inggris untuk lebih memahami bagaimana cara dalam melindungi diri pada ruang dunia maya, serta membantu pemerintah dan industry dalam melakukan pengembangan terhadap teknologi baru yang berfungsi untuk melindungi infrastruktur kritis nasional Inggris.

Di Inggris, terdapat 19 universitas yang berkualitas dan berkualifikasi yang sangat bagus di bidang keamanan siber. Ke-19 universitas ini memiliki jurusan terkait siber dan keamanan siber yang diakui oleh Pusat Keunggulan Akademik dalam Riset Keamanan Siber. Kedudukan Pusat Keunggulan Akademik dalam Riset Keamanan Siber tidak perlu diragukan lagi, dikarenakan lembaga ini telah diakui secara resmi oleh *Engineering and Physical Sciences Research Council* (EPSRC) dan *Government Communications Headquarters* (GCHQ) dalam memimpin dan menilai skema untuk mengakui kedudukan Pusat Keunggulan Akademik Inggris dalam Penelitian Keamanan Cyber (ACEs-CSR).

Inggris yang memiliki beberapa pemikir terbaik di bidang keamanan siber dan memiliki kualifikasi yang bagus dibidang pendidikan, akan memberikan peluang dan kesempatan bagi Indonesia untuk menerapkan hal tersebut di Indonesia. Di Indonesia, sudah ada pusat penelitian terkait keamanan siber, namun belum ditingkat secara intensif dan efektif terkhususnya pada bidang akademik untuk jenjang universitas.

Pemerintah Indonesia baru menempatkan pelajaran-pelajaran seputar Ilmu Komputer, Rekayasa Komputer, Sistem Informasi, Teknolgi Informasi serta mempelajari tentang Internet di kurikulum pendidikan. Pada tingkat universitas, Indoensia belum memiliki jurusan secara khusus terkait keamanan siber.

Melalui kerjasama ini, maka 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, kerjasama ini dapat memberikan informasi, pengetahuan secara pemahaman yang lebih mendalam bagi Pemerintah Indonesia khususnya pihak pemerintah terkhususnya pihak Badan Siber dan Sandi Negara akan menciptakan dan mengatur strategi keamanan siber nasional Indonesia. Namun, untuk mendukung penguatan di sektor ini, tentu saja hal ini membutuhkan dukungan serta pendekatan dari semua multistakeholder.

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 mengelola keamanan siber di sektor pemerintahan. Pada sektor pemerintahan, *Government Communications Headquarters* (GCHQ) akan berusaha untuk mengidentifikasi ancaman-ancaman yang menyerang dan

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

akan memainkan peran utama yang berkolaborasi dengan pemerintah untuk melindungi Inggris dari ancaman-ancaman tersebut.

Dari kerjasama ini Pemerintah Indonesia terkhusus CSIRT Sektoral Pemerintah (Gov-CSIRT Indonesia) akan berkolaborasi dengan CSIRT Organisasi di Instansi Pusat (baik Kementerian maupun Lembaga Pemerintah Non Kementerian), Pemerintah Daerah tingkat Provinsi, dan Pemerintah Daerah tingkat Kabupaten/Kota dalam mengelola keamanan siber Indonesia di sektor pemerintahan.

Diharapkan bahwa setiap sektor 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.

Penggunaan akan teknologi informasi dan komunikasi merupakan hal yang sangat penting dan menjadi suatu kebutuhan dalam pemanfataan terhadap Infrastruktur Kritis Nasional, 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 sektor keuangan dan perbankan, transportasi, energi, pertahanan, intelijen dan keamanan, telekomunikasi, kesehatan, e-governance, industri kritis. Sektor-sektor infrastruktur kritis nasional yang saling terhubung dengan internet atau terkoneksi dengan *cyberspace* akan memberikan dampak yang berbahaya apabila tidak diimbangi dengan perlindungan terhadap infrastruktur nasional.

Melalui kerjasama ini, Indonesia dapat belajar dari Inggris terkait hal untuk memberikan perlindungan dan mengamankan Infrastruktur Nasional Krtitis Inggris. 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 mengeluarkan kebijakan pada seluruh bidang pemerintahan dan infrastruktur nasional harus termasuk dan melalui proses pemeriksaan dasar, selain itu Proteksi Infrastruktur Nasional Inggris berkolaborasi dengan HMG dalam mengeluarkan panduan dan membuat saran untuk perlindungan terhadap infrastruktur kritis nasional Inggris.

4.2.2. Kepentingan Inggris

Kerjasama dalam bidang keamana 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.

Bagi pemerintahan Inggris, kemakmuran ekonomi dan kesejahteraan sosial merupakan salah satu hal yang bergantung pada keterbukaan dan keamanan jaringan, sehingga sangat penting bagi pemerintahan Inggris untuk bekerjasama secara internasional yang dapat dilaksanakan melalui kerjasama secara bilateral maupun multilateral atau bahkan mendukung organisasi internasional untuk memastikan keamanan

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

siber ataupun keamanan dunia maya yang berdampak secara langsung pada perekonomian dan kesejahteraan Inggris.

Pemerintah Inggris menyadari bhawa salah satu faktor tingginya serangan siber yang menyerang Inggris tidak hanya berasal dalam lingkup internal namun juga berasal dari lingkup eksternal yang menyerang. 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.

Salah satu 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 bekerjasama secara internasional untuk terus memastikan bahwa keamanan dan kemakmuran Inggris di masa yang akan datang melalui aturan-aturan yang telah 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. 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. Namun selain itu, adanya kepentingan Inggris untuk mengumpulkan data-data penting yang berdampak pada keberlangsungan negaranya.

Selain beberapa kepentingan tersebut, kepentingan lain Inggris dalam menjaga keamanan nasionalnya yang dapat dilakukan di luar teritorial Inggris yakni mengumpulkan dan menyediakan informasi dan data-data yang dibutuhkan bagi Pemerintah Inggris terkait perkembangan suatu negara yang dilakukan oleh intelijen Inggris (diakses dari https://www.bbc.co.uk/academy/id pada 15 Agustus 2020).

Data-data yang dibutuhkan tersebut berhubungan dengan pengambilan keputusan ataupun kebijakan suatu negara terkait politik, ekonomi, peta kekuatan

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

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* (GCHQ), sehingga Pemerintah Inggris dapat dengan mudah untuk menentukan arah kebijakan luar negeri. Selain itu, badan intelijen Inggris akan semakin memperketat keamanan dan kerahasisaan datanya dimana intelijen dari negara lain tidak mampu untuk meretas sistem informasi data 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 sistem 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, selain itu Pemerintah Inggris berusaha untuk memperoleh informasi secara langsung yang akan digunakan untuk keperluan negosiasi dan diplomasi.

4.3. Kendala Terhadap Pelaksanaan Kerjasama Dalam Bidang Keamanan Siber

Dalam proses pelaksanaan kerjasama bidang keamanan siber antara Indonesia dan Inggris mengalami kendala sehingga tidak banyak pelaksanaan kesepakatan kerjasama yang dilakukan. Pada 24 Mei 2019, terjadi pergantian pemimpin Badan Sandi dan Siber Negara Mayjen TNI (Purn.) Djoko Setiadi digantikan oleh Letjen TNI (Purn.) Hinsa Siburian, maka kesepakatan pelaksanaan kerjasama yang sebelumnya sudah ditetapkan harus dijadwalkan kembali sekaligus menyesuaikan waktu antara Badan Sandi dan Siber Negara dengan Pemerintah Kerajaan Inggris.

Selain itu, di masa Pandemi Covid-19, pertemuan antara pihak Badan Sandi dan Siber Negara Indonesia dan Organisasi Cybersecurity Inggris menjadi tertahan. Pelaksanaan cyber dialog forum melalui via online tidak disepakati oleh kedua pihak karena ada beberapa hal yang sensitive yang perlu dibicarakan secara langsung. Kendala lainnya adalah pembahasan terkait poin-poin kerjasama siber yang harus dilaksanakan pada forum resmi dan tidak dapat dilaksanakan pada forum informal.

4.4. Prospek Kerjasama Yang Dilakukan Oleh Indonesia dan Inggris Dalam Keamanan Siber

Pemerintah Indonesia melalui kerjasama dengan Pemerintah Kerajaan dalam bidang keamanan siber akan mendapatkan peluang dalam menyusun undang-undang khusus keamanan siber. Selain itu, walaupun manfaat dari kerjasama ini belum dapat dirasakan secara efektif, namun dari kerjasama ini dapat membuka peluang-peluang baru bagi keamanan siber. Kerjasama ini akan memberikan interaksi yang rutin antara

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

Indoensia dan Inggris mengenai perkembangan ancaman-ancaman siber sehingga kedua negara dapat memitigasi serangan siber.

Prospek lain dari kerjasama ini adalah dibangunnya information sharing dengan tujuan agar Pemerintah Indonesia dan Pemerintah Kerajaan Inggris dapat saling bertukar informasi ketika terjadi serangan siber yang akan berdampak pada Indonesia ataupun Inggris, sehingga kedua negara dapat melakukan antisipasi dan semakin memperkuat pertahanan keamanan siber di masing-masing negara dan juga kedua negara dapat saling belajar bagaimana mengatasi serangan siber yang telah terjadi di antara kedua negara ini.

5. Kesimpulan dan Rekomendasi

a) Kesimpulan

Kerjasama yang dilaksanakan oleh Pemerintah Indonesia dan Pemerintah Kerajaan Inggris merupakan suatu bentuk kerjasama dalam bidang keamanan siber dengan tujuan untuk saling memperkuat ketahanan siber di masing-masing negara. Pemerintah Indonesia dan Pemerintah Kerajaan Inggris menandatangani nota kesepahaman kerjasama dalam bidang keamanan siber pada 14 Agustus 2018 di Jakarta. Bentuk penerapan kerjasama dalam bidang keamanan siber diterapkan dalam bentuk cyber dialog forum. Dari ke-5 poin kerjasama yang disepakati bersama, Pemerintah Indonesia dan Pemerintah Kerajaan Inggris lebih terfokus kepada Peningkatan Kapasitas. Pada Peningkatan Kapasitas, Pemerintah Indonesia dan Pemerintah Inggris membahas 2 hal yakni Cyber Law dan Cybersecurity Awareness.

Inti dari pembahasan terkait Peningkatan Kapasitas adalah bagaimana kedua peserta saling berbagi informasi dalam membantu dan mengembangkan pemahaman organisasi ataupun suatu instansi terkait keamanan siber pada saat melakukan pengelolaan data, sistem, aset termasuk sumber daya manusia. Adanya sumber daya yang mendukung dan mumpuni, sehingga akan mampu untuk 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. Pada Kapasitas Pengembangan ini juga membantu kedua peserta dalam membuat kerangka kerja keamanan siber, sehingga akan lebih mempermudah organisasi ataupun instansi pemerintah dalam mengambil keputusan ataupun menentukan manajemen risiko keamanan siber.

Dalam kerjasama tersebut dapat dikatakan bahwa baik Indonesia dan Inggris sama-sama memiliki kepentingan nasional yang ingin dipenuhi melalui kerjasama dalam bidang keamanan siber. Melalui kerjasama ini, Pemerintah Indonesia dapat mengatur ulang kembali strategi keamanan siber serta dapat memberdayakan secara efektif sektor-sektor pemerintahan, akademisi serta industi dalam menjalankan strategi keamanan siber nasional Indonesia. Sementara Pemerintah Kerajaan Inggris memiliki kepentingan yaitu mewujudkan salah satu National Strategy 2016-2021 yakni bersedia bekerjasama secara internasional untuk menjadi negara yang aman di dunia maya untuk melakukan bisnis, melalui kerjasama internasional hal ini bertujuan untuk mempromosikan Inggris sebagai negara yang aman untuk melakukan bisnis ataupun berinvestasi secara digital.

Pelaksanaan terhadap kerjasama dalam bidang keamanan siber mengalami kendala yang harus dihadapi oleh kedua

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

negara yakni penyesuaian waktu pimpinan dalam melaksanakan cyber dialog forum, pertukaran informasi oleh kedua negara terkait siber harus dilaksanakan pada forum resmi dan tidak pada forum informal, kendala lainnya adalah cyber dialog forum harus dilaksanakan pada high level sebelum dilaksanakan pada low level.

Walaupun terdapat berbagai kendala dalam melaksanakan kerjasama keamanan siber, serta dampak yang dirasakan dari hasil kerjsama ini belum dapat dirasakan secara signifikant dan berjalan secara efektif. Hal ini dikarenakan bentuk pelaksanaan yang dilaksanakan masih dalam bentuk pembahasan, dan belum ada tindakan secara nyata seperti pelaksanaan pelatihan bagi sumber daya manusia untuk kedua negara dalam mengelola teknologi ataupun pelatihan dalam teknik mengatasi ancaman siber seperti penyerangan yang dilakukan melalui virus.

Diharapkan bahwa, kerjasama kedua negara ini dapat terus ditingkatkan dan berlangsung efektif, sehingga dampak dari kerjasama ini dapat dirasakan oleh seluruh elemen.

b) Saran

Sebagai masyarakat internasional kita harus dapat memahami terkait perkembangan dan kemajuan teknologi informasi dan komunikasi, sehingga kita dituntut untuk semakin sadar serta melindungi keamanan data seperti menjaga kerahasiaan data, melindungi akurasi serta kelengkapan data dan informasi dari dampak negatif yang ditimbulkan dari kemajuan teknologi informasi dan komunikasi terutama penggunaan fasilitas dan infrastruktur dari internet.

Kondisi keamanan siber yang lemah bagi suatu negara akan sangat berpengaruh kepada negara lain yang dikarenakan sifat internet yang tidak memandang batas negara, sehingga perlu adanya kerjasama baik secara bilateral maupun mulitilateral atau antar lembaga keamanan informasi antar negara sehingga dapat memperkuat keamanan informasi dan mampu mengimbangi hal-hal yang sama dengan negara lain dalam konteks keamanan siber.

Untuk meminimalisir penyalahgunaan tindakan dalam menjaga keamanan informasi, maka perlu dilakukan tindakan dalam pegamanan personil. Maksudnya adalah perlu adanya tanggungjawab dari karyawan ataupun para pemanggu kepentingan yang menjalankann suatu perusahaan, organisasi ataupun instansi pemerintah terutama pada bagian pemrosesan informasi data yang dapat dilakukan dengan menandatangani surat perjanjian kerahasiaan informasi data.

Selain itu, perlu dilakukannya sosialisasi atau promosi kesadaran keamanan informasi yang dapat dilakukan secara berkala sehingga para pengguna ataupun pemangku kepentingan semakin sadar akan pentingnya keamanan informasi dan data.

Selain itu, dapat dikatakan bahwa kerjasama ini belum secara efektif dilaksanakan oleh kedua negara. Belum adanya penerapan secara langsung yang dapat dirasakan oleh multistakeholder pada bidang keamanan siber, sehingga semoga kedepannya kerjasama ini dapat berjala sesuai dengan apa yang diharapkan bersama.

Pemerintah Indonesia juga dpat menggerakan sektor pendidikan untuk melakukan kerjasama atau bertukar informasi dengan universitas di Inggris yang memiliki kapasitas dan kualifikasi dalam bidang keamanan siber sehingga dapat dikembangkan di Indonesia terkhusus di bidang pendidikan.

Daftar Pustaka

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.vxix

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

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

Biro Hukum dan Humas BSSN. Mengenali Serangan Siber Global dan Nasional Melalui Laporan Tahunan Honeynet Project BSSN-IHP Tahun 2018. Diakses dari https://bssn.go.id/mengenali-serangan-siber-global-dan-nasional-melalui-laporan-tahunan-honeynet-project-bssn-ihp-tahun-2018/

Direktorat Deteksi Ancaman Siber. Laporan Tahunan 2018 Honeynet Project Badan Sandi Dan Siber Negara-Indonesia Honeynet Project Volume 1, diakses dari https://bssn.go.id/wp-content/uploads/2019/02/Laporan-Tahunan-Honeynet-Project-BSSN_IHP-2018.pdf

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-siber-menyebabkan-kerugian-ekonomi-bagi-organisasi-di-indonesia-sebesar-us34-2-miliar/

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-times-each-by-cyber-attacks-in-2016-says-internet-service-provider.html.

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

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

Kementerian Pertahanan Republik Indonesia. 2014. Pedoman Pertahanan Siber. Diakses dari https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf

Putri Sylvia Octa, Mengenal Studi Hubungan Internasional. Bandung: Zavara.

Group of Governmental Experts https://www.un.org/disarmament/group-of-governmental-experts/

https://www.bbc.co.uk/academy/id/articles/art20160205075210754