

Kerjasama Indonesia-Inggris Dalam Pengembangan Keamanan Siber Nasional Melalui *Cyber Diplomacy*

Indonesia-UK Cooperation in Developing National Cyber Security Through Cyber Diplomacy

M.Hafeez Andhri Abdillah Lubis¹, Helga Yohana Simatupang²

^{a,b}Program Studi Hubungan Internasional UPU, Jl. K.L. Yos Sudarso KM 6.5 Tj. Mulia, Medan, 20241, Indonesia
eezh150@gmail.com¹, helgayohana@potensi-utama.ac.id²

ABSTRAK

Karena jumlah pengguna Internet terbesarnya, Indonesia menghadapi banyak masalah keamanan siber. Untuk mengatasi masalah ini, pemerintah telah melakukan berbagai upaya, baik di dalam maupun di luar negeri. Indonesia membentuk Badan Siber dan Sandi Negara (BSSN) sebagai organisasi nasional untuk operasi dalam negeri. Indonesia bekerja sama dengan negara-negara yang mampu menjaga keamanan siber, termasuk Inggris, untuk meningkatkan keamanan siber nasional. Kedua negara menghadapi tantangan dalam menerapkan kolaborasi ini di bidang keamanan siber, tetapi keduanya optimis bahwa kerja sama ini akan menguntungkan masyarakat dan memperkuat hubungan mereka. Penelitian ini bertujuan untuk menganalisis bagaimana proses, faktor-faktor yang melatarbelakangi, serta kendala yang dihadapi dari kerjasama Indonesia dan Inggris di bidang keamanan siber. Metode yang dipakai yakni kualitatif deskriptif dengan konsep kerjasama bilateral, kepentingan nasional, dan interdependensi. Hasil penelitian ini menunjukkan bahwa kerja sama di bidang keamanan siber antara Indonesia dan Inggris menunjukkan peningkatan strategi keamanan siber dan pemberantasan kejahatan siber di Indonesia. Dapat disimpulkan bahwa prinsip implementasi keamanan siber yang lemah, sumber daya manusia yang masih lemah, dan kurangnya kesadaran tentang cybersecurity adalah penyebab kejahatan siber yang terjadi di Indonesia.

Kata Kunci : Kerjasama Keamanan Siber, Kejahatan Siber, Kepentingan Nasional, Indonesia, Inggris

ABSTRACT

Due to its largest number of Internet users, Indonesia faces many cybersecurity issues. To address these issues, the government has made various efforts, both at home and abroad. Indonesia established the National Cyber and Crypto Agency (BSSN) as a national organization for domestic operations. Indonesia collaborates with capable cybersecurity countries, including the UK, to improve national cybersecurity. Both countries face challenges in implementing this collaboration in the field of cybersecurity, but both are optimistic that this cooperation will benefit society and strengthen their relationship. This research aims to analyze the process, factors behind, and obstacles faced by Indonesia and the UK's cooperation in the field of cybersecurity. The method used is descriptive qualitative with the concepts of bilateral cooperation, national interest, and interdependence. The results of this study show that cooperation in the field of cybersecurity between Indonesia and the UK shows an increase in cybersecurity strategies and the eradication of cybercrime in Indonesia. It can be concluded that weak cybersecurity implementation principles, weak human resources, and lack of awareness about cybersecurity are the causes of cybercrime that occurs in Indonesia.

Keywords : Cyber Security Cooperation, Cyber Crime, National Interest, Indonesia, United Kingdom

Info Artikel :

Disubmit: 10 Januari 2024

Direview: 05 Februari 2024

Diterima : 08 April 2024

Copyright © 2022 - Journal UPU. All rights reserved.

1. PENDAHULUAN

Kepentingan keamanan dan keselamatan nasional sangat penting bagi setiap negara. Karena itu, masalah ini menjadi dasar kebijakan politik negara terhadap negara lain. Fokus sektor keamanan saat ini adalah menjaga kepentingan negara dan keselamatan warga negara. Oleh karena itu, konsep keamanan dianggap sebagai satu kesatuan yang terdiri dari pertahanan negara (national defence),

keamanan dalam negeri (internal security), keamanan publik (public security), dan keamanan manusia (human security) (Fakhrul dkk., 2022). Berbagai teknologi informasi digital semakin diminati oleh masyarakat di seluruh dunia. Teknologi ini berkaitan dengan penggunaan ruang maya. Secara umum, cyberspace, atau internet, telah menjadi bagian dari kehidupan sehari-hari. Namun, hal ini tidak hanya membawa keuntungan bagi pengguna, tetapi juga mengancam keamanan dan hak asasi mereka (Simatupang & Ridwan, 2022). Pengembangan keamanan siber nasional merupakan salah satu isu krusial dalam era digital saat ini. Dalam konteks global, negara-negara di seluruh dunia memiliki perhatian yang semakin meningkat terhadap ancaman dan tantangan keamanan siber.

Tidak terkecuali Indonesia dan Inggris sebagai dua negara yang memiliki perkembangan teknologi informasi yang pesat. Oleh karena itu, pengembangan keamanan siber nasional melalui Cyber Diplomacy menjadi sangat penting dalam upaya melindungi kepentingan nasional dan menjaga stabilitas dunia maya. Sebelum membahas tentang pengembangan keamanan siber nasional melalui Cyber Diplomacy, penting bagi kita untuk memahami arti dari keamanan siber nasional itu sendiri. Keamanan siber nasional dapat didefinisikan sebagai upaya perlindungan terhadap serangan dan ancaman yang dilakukan melalui jaringan komputer dan sistem informasi yang dimiliki oleh suatu negara. Serangan-serangan ini dapat dilakukan oleh individu, kelompok, maupun negara lain yang bertujuan merusak, menghancurkan, atau mencuri informasi yang sangat penting dari suatu negara (Dewan Teknologi Informasi dan Komunikasi Nasional, 2018).

Perkembangan teknologi komunikasi dan informasi yang pesat telah mendorong negara-negara di seluruh dunia untuk meningkatkan perhatian terhadap keamanan siber nasional. Hal ini dikarenakan serangan dan ancaman di dunia maya dapat memiliki dampak yang merusak dan signifikan terhadap kepentingan nasional. Pengembangan keamanan siber nasional sangat penting karena melindungi infrastruktur kritis, seperti jaringan listrik, transportasi, telekomunikasi, dan sistem perbankan. Jika ada kerentanan maupun celah keamanan dalam infrastruktur ini, maka negara dapat mengalami gangguan yang serius dan tak terduga. Cyber Diplomacy, atau diplomasi siber, adalah pendekatan internasional dalam mempromosikan kerjasama dan negosiasi antara negara-negara dalam mengatasi masalah keamanan siber (Attatfa dkk., 2020). Peran Cyber Diplomacy sangat penting dalam pengembangan keamanan siber nasional, khususnya dalam hubungan antara Indonesia dan Inggris.

Negara-negara ini bisa saling berbagi informasi dan pengalaman, bekerjasama dalam melacak dan menangani serangan siber, serta mengembangkan Kerjasama dalam melawan kejahatan siber lintas batas. Indonesia dan Inggris memiliki hubungan yang erat dalam bidang keamanan siber nasional. Terhitung, Kerjasama ini sudah terjalin sejak 2018 ditandai dengan penandatanganan *Memorable of Understanding (MoU)* dan terus terjalin hingga saat ini. Kedua negara ini memiliki kepentingan yang sama dalam melindungi infrastruktur kritis dan data sensitif dari serangan siber. Melalui kerjasama bilateral dan multilateral, Indonesia dan Inggris bisa saling mendukung dalam upaya melawan ancaman keamanan siber melalui pertukaran pengetahuan dan pengalaman antar kedua negara (BSSN, 2023). Pertumbuhan teknologi serta data yang pesat di masa ini membawa akibat yang besar dalam dunia hubungan internasional, saat ini bukan hanya negara-negara maju namun negara berkembang juga turut meningkatkan teknologi serta data mereka. Bersamaan dengan kemajuan yang sangat pesat, negara-negara berlomba-lomba meningkatkan teknologi mereka supaya bisa bertahan dalam masa globalisasi saat ini (Ghernaouti-Hélie, 2009). Kemajuan teknologi saat ini menuntut peningkatan fitur komputer yang didukung oleh pertumbuhan jaringan internet yang pesat. Akibatnya, pertumbuhan komputer dan jaringan internet ini menyebabkan efek negatif dari penyalahgunaan internet yang terus meningkat dan rumit, yang dapat menghancurkan infrastruktur penting suatu negara yang terhubung ke internet. Orang-orang di seluruh dunia sangat khawatir tentang peningkatan ancaman cyber crime saat ini. Ini disebabkan oleh fakta bahwa pihak-pihak tertentu terus melakukan cybercrime dengan mudah.

Serbuan siber (cyber- attack) adalah salah satu bentuk dari cyber crime yang dapat dilakukan secara menyerbu, baik secara individu ataupun digunakan untuk menyerbu suatu kelompok maupun organisasi dari negara lain. Kemajuan teknologi komputer serta kemajuan internet di masa ini berbuntut menimbulkan terus terjadinya peningkatan permasalahan yang ditimbulkan oleh peretas komputer (computer hackers). Aktivitas para peretas komputer ini dapat dilakukan dalam tujuan positif ataupun negatif. Dalam tujuan positif, para peretas komputer umumnya merambah sesuatu sistem dengan menggunakan kekurangan ataupun celah yang terdapat pada sesuatu sistem tersebut lalu memperbaikinya (Sterling, 2010).

Untuk meningkatkan pertumbuhan ekonomi dan keamanan nasional, pemerintah harus meningkatkan keamanan dunia siber nasional. Salah satu negara dengan jumlah pengguna internet tertinggi adalah Indonesia. Saat ini, Indonesia sudah menjadi salah satu negara yang paling rentan terhadap serbuan siber karena populasi pengguna internetnya yang besar. Laman pemerintah tercatat diserbu hampir 3000 kali setiap hari. E-commerce, saham, perbankan, dan masalah jasa keuangan biasanya terkena serangan siber. Selain itu, serangan siber biasanya menyerang database online pemerintah yang berisi informasi nasional penting seperti data penduduk, keuangan, dan sumber energi alam.

Serangan cyber telah menyebabkan banyak masalah, seperti kasus WannaCry, yang merupakan salah satu contoh kasus serbuan cyber terbesar yang pernah terjadi di dunia. Ransomware ini mengunci sistem komputer di lebih dari 150 negara, termasuk Indonesia. WannaCry lebih “sakti” daripada ransomware pendahulunya karena menggunakan alat senjata cyber dari National Security Agency (NSA), yang dicuri oleh hacker dan dibocorkan di internet. Ini menunjukkan alasan WannaCry dapat menyebar dengan cepat. Program berbahaya ini dapat menginfeksi ribuan sistem komputer di puluhan negara dalam waktu singkat. Serangannya tidak pandang bulu, mulai dari Industri otomotif, telekomunikasi, perbankan, dan rumah sakit semuanya menjadi korban dan harus membayar tebusan. Bahkan tidak hanya negara Indonesia saja yang terkena serangan Cyber tersebut namun Negara Inggris juga ikut terkena serangan virus ini.

Karena ransomware mengunci dan "menyandera" data pasien di komputer rumah sakit, jaringan National Health Service (NHS) di Inggris menjadi tertekan. Inggris Raya National Cyber Security Center (NCSC) melakukan upaya untuk memulihkan sistem komputer NHS. Pelayanan medis untuk pasien menjadi tertunda sementara itu. Beberapa prosedur pembedahan dibatalkan, dan ambulans harus dialihkan ke rumah sakit lain yang tidak terpengaruh. Inggris menyatakan bahwa setidaknya 45 organisasi kesehatan terpengaruh. Bukan dicuri, tetapi ransomware mengunci dan meminta tebusan untuk data rekam jejak medis penderita (Pettit, 2017).

Konsep-konsep Kerjasama bilateral, kepentingan nasional, dan interdependensi memainkan peran penting dalam pengembangan keamanan siber nasional melalui Cyber Diplomacy antara Indonesia Inggris. Melalui Kerjasama bilateral, kedua negara dapat mengembangkan strategi Bersama, memperkuat kapasitas teknologi, serta melakukan pelatihan dan Pendidikan guna meningkatkan kemampuan dalam menghadapi serangan siber (Anindita, 2020). Kerjasama ini juga melibatkan penciptaan kerangka hukum dan kebijakan yang memfasilitasi Tindakan Bersama dalam menghadapi masalah keamanan siber. Indonesia dan Inggris memiliki kepentingan nasional yang sama dalam melindungi infrastruktur kritis, menjaga privasi dan integritas data, serta melindungi kepentingan ekonomi dan politik dalam lingkup nasional. Kerjasama bilateral dalam pengembangan keamanan siber nasional melalui Cyber Diplomacy menjamin bahwa kepentingan nasional kedua negara akan terpenuhi. Melalui interdependensi, kedua negara dapat berbagi informasi tentang ancaman yang ada, bekerja sama dalam perencanaan dan pelaksanaan tindakan preventif, serta menyusun mekanisme tanggap darurat yang efektif jika terjadi serangan atau insiden keamanan siber.

Dalam konteks kerjasama Indonesia-Inggris dalam pengembangan keamanan siber nasional melalui Cyber Diplomacy, terdapat beberapa rumusan masalah yang dapat dianalisis sebagai dasar

penelitian kali ini , yakni: Bagaimana kerjasama bilateral antara Indonesia dan Inggris dalam pengembangan keamanan siber nasional melalui Cyber Diplomacy terwujud? Apa saja kepentingan nasional yang mendorong Indonesia dan Inggris untuk bekerjasama dalam mengembangkan keamanan siber nasional? Apa saja hambatan dan tantangan yang dihadapi dalam implementasi Kerjasama Indonesia-Inggris dalam pengembangan keamanan siber nasional melalui Cyber Diplomacy?

2. TINJAUAN PUSTAKA

Dalam era digital yang semakin maju, keamanan siber nasional menjadi semakin penting bagi setiap negara. Indonesia dan Inggris tidak terkecuali dalam menghadapi ancaman dan tantangan keamanan siber. Dalam upaya melindungi kepentingan nasional dan menjaga stabilitas dunia maya, kerjasama bilateral antara kedua negara menjadi krusial. Konsep-konsep kerjasama bilateral, kepentingan nasional, dan interdependensi memainkan peran penting dalam pengembangan keamanan siber nasional melalui cyber diplomacy antara Indonesia dan Inggris.

A. Kerjasama Bilateral

Kerjasama bilateral adalah bentuk kerja sama antara dua negara dalam berbagai bidang, termasuk keamanan siber nasional (Rana, 2018). Dalam kerjasama ini, Indonesia dan Inggris dapat saling berbagi informasi, pengalaman, dan sumber daya untuk melawan ancaman keamanan siber. Melalui kerjasama bilateral, kedua negara dapat mengembangkan strategi bersama, memperkuat kapasitas teknologi, serta melakukan pelatihan dan pendidikan guna meningkatkan kemampuan dalam menghadapi serangan siber. Kerjasama ini juga melibatkan penciptaan kerangka hukum dan kebijakan yang memfasilitasi tindakan bersama dalam menangani masalah keamanan siber.

B. Kepentingan Nasional

Kepentingan nasional merupakan faktor yang mendorong negara untuk melakukan langkah-langkah dalam mengatasi ancaman (Navari, 2016) keamanan siber. Indonesia dan Inggris memiliki kepentingan nasional yang sama dalam melindungi infrastruktur kritis, menjaga privasi dan integritas data, serta melindungi kepentingan ekonomi dan politik dalam lingkup nasional. Kerjasama bilateral dalam pengembangan keamanan siber nasional melalui cyber diplomacy menjamin bahwa kepentingan nasional kedua negara akan terpenuhi. Negara-negara ini akan bekerja sama untuk mencegah serangan dan ancaman keamanan siber yang dapat merusak kepentingan nasional mereka.

C. Interdependensi

Interdependensi mengacu pada ketergantungan antara negara-negara (Owen dan Joseph Nye., 2011) dalam hal keamanan siber. Dalam dunia maya yang saling terhubung, serangan dan ancaman keamanan siber yang terjadi di satu negara dapat berdampak pada negara lainnya. Oleh karena itu, kerjasama bilateral antara Indonesia dan Inggris dalam pengembangan keamanan siber nasional melalui cyber diplomacy menjadi penting. Melalui interdependensi, kedua negara dapat berbagi informasi tentang ancaman yang ada, bekerja sama dalam perencanaan dan pelaksanaan tindakan preventif, serta menyusun mekanisme tanggap darurat yang efektif jika terjadi serangan atau insiden keamanan siber.

3. METODE

Metode penelitian kualitatif digunakan dalam penelitian ini. Penelitian ini menjelaskan dan menganalisis data yang diperoleh dari penelitian tentang kerja sama Indonesia-Inggris dalam menanggulangi kejahatan siber di Indonesia dari tahun 2018 hingga sekarang. Penelitian juga menyajikan hasilnya ke dalam jurnal. Data yang dikumpulkan dalam penelitian ini dikumpulkan

melalui studi pustaka dan penelusuran data online. Informasi sekunder adalah jenis informasi yang digunakan dalam penelitian. Informasi ini berasal dari sumber seperti buku, jurnal ilmiah, dokumen, akses internet, dan postingan di media internet. Untuk mengolah data, peneliti menggunakan metode deskriptif dari penjumlahan atau analisis data dari penelitian sebelumnya. Pustaka mengacu pada berita swasta, praktik keamanan siber yang tersedia online, dan berbagai tindakan yang dilakukan di institusi publik dan swasta, serta organisasi internasional.

4. HASIL DAN PEMBAHASAN

Indonesia dan pemerintah Inggris telah bekerja sama dalam bidang keamanan siber. Pada bulan Agustus 2018, pemerintah Inggris memulai kerja sama langsung dengan Badan Sandi dan Siber Negara Indonesia dalam bidang keamanan siber. Untuk mencapai kesepakatan dan meningkatkan kerja sama dalam bidang keamanan siber, Pemerintah Republik Indonesia dan Pemerintah Inggris menandatangani Nota Kesepahaman pada 14 Agustus 2018. Badan Sandi dan Siber Negara mewakili Republik Indonesia, dan Wakil Perdana Menteri Inggris mewakili Inggris. Bergantung pada jumlah porsi dan konteks pembahasan yang diperlukan untuk ulasan dalam cyber diskusi forum, lembaga pemerintahan lain juga dapat mengikuti kerja sama ini. Dalam kasus ini, topik utama untuk ulasan adalah Pengembangan Kapasitas. Kedutaan Besar Inggris menerapkan pengembangan kapasitas. Karena telah ada MOU dengan Badan Sandi dan Siber Negara, penerapan Kenaikan Kapasitas dimulai pada tahun 2019 dengan dua program ulasan, Cyber Law dan Cyber Security Awareness.

Pada ulasan undang-undang siber, kedua peserta berbicara tentang United Nations Group of Governmental Experts (UN GGE). Indonesia dan Inggris ditunjuk sebagai anggota Kelompok Ahli Pemerintahan PBB, yang didirikan oleh PBB untuk meningkatkan dan mendorong sikap dalam negeri untuk bertanggung jawab di dunia siber dalam rangka melindungi keamanan internasional. Pembicaraan tentang United Nations Group of Governmental Experts (UN GGE) berfokus pada peningkatan kapasitas suatu negara, standar yang ditetapkan tentang bagaimana suatu negara bersikap dalam dunia siber, dan peningkatan kepercayaan negara-negara dalam melakukan kerja sama keamanan siber, baik bilateral maupun multilateral (Nadhifah, 2020). Sebagai tambahan pada diskusi terpaut yang diadakan oleh United Nations Group of Governmental Experts (UN GGE), Tallinn Manual 2.0 juga dibahas. Manual ini berfokus pada pengkajian siber yang dilakukan oleh negara dan mengkaji kerangka hukum internasional yang dapat diterapkan dalam operasi serbuan siber.

Pemerintah Inggris sedang berusaha untuk menggambarkan Manual Tallinn 2.0, yang merupakan pedoman komprehensif untuk pengendalian pengolahan siber (Schmitt, 2017). Pedoman ini akan mengulas upaya kerja sama siber yang dilakukan oleh Inggris dan Indonesia. Namun, pemerintah Indonesia belum mempertimbangkan Manual Tallinn 2.0 saat membuat kebijakan keamanan siber. Karena Indonesia tidak terlibat dalam perumusan, tidak jelas apakah kepentingan Indonesia tercakup atau tidak. Akibatnya, Tallinn Manual 2.0 masih menjadi penyelidikan untuk Indonesia untuk mengetahui apakah itu dapat berfungsi sebagai jembatan untuk memenuhi kebutuhan Indonesia, terutama dalam hal keamanan siber. Cyber Security Awareness akan dibahas dalam ulasan berikutnya.

Dalam ulasan ini, penjelasan tentang keamanan siber seperti kabar hoax, pengamanan data individu dan masalah pribadi diperluas. Selain itu, ulasan ini juga mencakup pengetahuan tentang keamanan siber, yaitu teknik untuk menganalisis dan menginvestigasi malware, menguasai strategi, dan strategi untuk menciptakan kendala, kerentanan, dan perawatan insiden, yang dapat dianggap sebagai langkah awal yang harus dilakukan jika serbuan siber menyerang pemerintah dan lembaga pemerintah.

Diskusi kerjasama ini menegaskan komitmen kedua negara untuk terus meningkatkan kerjasama dalam bidang keamanan siber antara Indonesia dan Inggris serta memahami masalah siber. Selain itu, kedua negara juga berbicara tentang meningkatnya angka serbuan siber dan efeknya. Kedua negara setuju bahwa kerja sama seluruh pihak akan sangat penting dalam memerangi kejahatan siber. Delegasi Inggris mengucapkan terima kasih kepada Indonesia pada akhir diskusi karena telah mengadakan penyelenggaraan cyber diskusi forum (KEMHAN, 2018).

Keterlibatan ini masih dalam bentuk ulasan dan belum dilaksanakan dalam bentuk pelatihan bersama. Namun, melalui kerja sama ini, pihak-pihak yang terlibat dapat saling berbagi data untuk membantu dan meningkatkan penjelasan organisasi dan lembaga tentang keamanan siber saat mengelola informasi, sistem, dan peninggalan tercantum sumber daya manusia.

Sumber energi yang mendukung dan memadai memungkinkan identifikasi, pemahaman, dan penyebaran perlindungan dan pertahanan, serta menjawab dan memastikan perilaku dalam mengambil tindakan pada saat terjalin serbuan siber, serta membantu pemulihan serbuan siber untuk meminimalkan dampak yang disebabkan oleh serbuan siber.

A. Kepentingan Indonesia

Pemerintah Indonesia menyadari bahwa ancaman dunia siber merupakan tantangan yang akan berdampak pada ekonomi dan keamanan nasional dan berpotensi mengancam kedaulatan negara karena aktor tindak kejahatan siber akan terus berusaha untuk mengancam, menyelidiki, dan menyerang wilayah pemerintahan, swasta, dan bisnis. Jadi, diperlukan peningkatan sumber energi manusia dan kemampuan untuk meningkatkan keamanan siber. Namun, untuk memerangi kejahatan siber yang berskala internasional, perlu ada kerja sama internasional. Ini karena kejahatan siber tidak hanya terjadi di dalam negeri tetapi juga di luar negeri.

Oleh karena itu, Indonesia membutuhkan peningkatan efisiensi dan optimalisasi strategi keamanan siber nasionalnya. Namun, ada beberapa wilayah yang belum dapat dioptimalkan dengan baik dalam strategi keamanan siber nasional tersebut. Ini termasuk zona pemerintah, yang mencakup departemen negeri dan lembaga pemerintah, zona usaha dan bisnis, yang mencakup perbankan dan e-commerce, zona akademisi, yang mencakup praktisi dan akademisi semacam Hacker (Ayu, 2023). Sudah jelas bahwa Indonesia memiliki banyak kepentingan dalam keamanan siber yang dapat dipenuhi saat bekerja sama dengan Inggris. Berikut adalah beberapa kepentingan Indonesia dalam melakukan kerja sama siber dengan Inggris:

1) Memperkuat Kerjasama Keamanan Siber di Sektor Pemerintah

Pemerintah Indonesia berpikir bahwa kerja sama ini akan memungkinkan mereka untuk belajar dari Pemerintah Inggris, khususnya dari Headquarters for Communications (GCHQ) pemerintah Inggris, tentang cara mengelola keamanan siber di zona pemerintahan. GCHQ juga akan berupaya untuk mengidentifikasi ancaman siber dan akan memainkan peran penting dalam bekerja sama dengan pemerintah untuk melindungi Inggris dari ancaman siber tersebut. Dalam kerjasama ini, Computer Security Incident Response Team (CSIRT) Sektor Pemerintah (Gov-CSIRT Indonesia) akan bekerja sama dengan CSIRT Organisasi di Lembaga Pusat (baik Departemen maupun Lembaga Non Departemen), Provinsi dan Kabupaten/Kota tingkat wilayah untuk mengatur keamanan siber di wilayah pemerintahan Indonesia (BSSN, 2021). Diharapkan setiap zona pemerintahan dapat bekerja sama dengan baik dalam mengendalikan dan mengelola keamanan siber, terutama dengan Badan Siber dan Sandi Negara Indonesia sebagai kontak utama yang dapat bekerja sama dengan lembaga pemerintahan yang lain untuk menghasilkan keadaan keamanan siber yang baik untuk melindungi keamanan siber Indonesia.

2) Memperoleh Pembelajaran Melalui Akademisi

Inggris akan memberikan kesempatan dan peluang kepada Indonesia untuk menerapkan keamanan siber di Indonesia mereka juga memiliki kualifikasi pembelajaran yang baik (Kementerian Kesehatan Republik Indonesia, 2021). Di Indonesia, ada beberapa pusat penelitian yang berfokus pada keamanan siber, tetapi belum secara menyeluruh dan efektif, terutama di bidang akademik untuk jenjang universitas. Pemerintah Indonesia sudah menambahkan mata pelajaran komputer ilmu, rekayasa komputer, sistem data, teknologi data, dan pengembangan Internet ke dalam kurikulum sekolah mereka. Dengan bekerja sama dengan Inggris, Indonesia dapat belajar bagaimana meningkatkan dan mengoptimalkan keahlian akademisi dalam bidang keamanan siber. Ini akan memungkinkan mereka untuk bekerja sama dengan pemerintah, industri, dan kelompok komunitas masyarakat dalam menerapkan strategi, terutama untuk memberi tahu orang awam tentang uraian dan pengetahuan, serta membagikan langkah-langkah keamanan siber yang dapat dicoba secara berkesinambungan.

Oleh karena itu, kerjasama ini dapat memberikan data dan pengetahuan yang lebih rinci kepada pemerintah Indonesia, terutama pemerintah dan Badan Siber dan Sandi Negara, yang akan membuat dan mengawasi strategi keamanan siber nasional Indonesia. Namun, untuk mendukung penguatan di bidang ini, tentu saja hal ini membutuhkan dukungan dan pendekatan dari seluruh pemangku kepentingan.

3) Meningkatkan Keamanan Siber Infrastruktur Penting

Sangat penting untuk memanfaatkan teknologi data dan komunikasi dan sangat penting pula untuk memanfaatkan Infrastruktur Penting Nasional. Infrastruktur Penting adalah jaringan, sistem, atau peninggalan yang sangat penting, dan kegagalan mereka dapat mempengaruhi kestabilan ekonomi negara, keamanan, dan keselamatan masyarakat. Area keuangan dan perbankan, transportasi, tenaga, pertahanan, intelijen dan keamanan, telekomunikasi, kesehatan, pemerintahan elektronik, dan sektor lain adalah bagian penting dari infrastruktur nasional Indonesia. Infrastruktur penting nasional yang terhubung ke internet atau terhubung ke cyberspace akan mengalami konsekuensi yang berbahaya jika tidak dilindungi dengan baik (Soewardi, 2013). Dengan bekerja sama, Indonesia dapat belajar dari Inggris tentang memberikan perlindungan dan menjaga infrastruktur nasional penting Inggris. Her Majesty's Government (HMG) menangani keamanan infrastruktur nasional kritis Inggris. HMG mengembangkan kebijakan untuk segala bidang pemerintahan dan infrastruktur nasional yang diperlukan, serta melalui proses pengecekan keamanan nasional. Selain itu, HMG bekerja sama dengan Perlindungan Infrastruktur Nasional Inggris untuk menghasilkan kontrol keamanan terhadap infrastruktur kritis nasional Inggris.

B. Kepentingan Inggris

Inggris secara langsung memulai kerjasama dalam bidang keamanan siber, yang merupakan salah satu tujuan dari National Strategy 2016–2021. Salah satu tujuan dari strategi ini adalah untuk menjadi negara yang aman di dunia maya untuk melakukan bisnis. Sangat penting bagi pemerintahan Inggris untuk berkolaborasi secara internasional, karena kemakmuran ekonomi dan kesejahteraan sosial mereka bergantung pada keterbukaan dan keamanan jaringan. Ini dapat dicapai melalui kerjasama bilateral dan multilateral, serta dengan mendukung organisasi internasional untuk memastikan keamanan siber dan keamanan dunia maya. Pemerintah Inggris menyadari bahwa sejumlah besar serbuan siber yang melanda Inggris tidak hanya terjadi di dalam negeri tetapi juga di luar negeri. Oleh karena itu, untuk melindungi kepentingan nasional Inggris baik di dalam negeri maupun di luar negeri, pemerintah Inggris harus memastikan pelaksanaan hukum internasional di internet dan pelaksanaan hak asasi manusia di internet (Usman, 2021).

Inggris berkolaborasi secara internasional untuk mendapatkan berbagai sumber data terpaut ancaman serta aplikasi penyerangan yang terus tumbuh saat ini dan di masa mendatang, serta untuk memenuhi tujuan melindungi keamanan dunia siber yang leluasa, terbuka, damai, dan nyaman, serta untuk mendesak perkembangan ekonomi serta menunjang keamanan nasional Inggris. Selain itu, Inggris berkolaborasi secara internasional untuk melaksanakan latihan dan meningkatkan keamanan siber. Dalam hal ini, Inggris akan terus bekerja sama secara internasional untuk memastikan bahwa keamanan dan kemakmuran Inggris akan dijamin oleh aturan internasional. Untuk mencapai tujuan tersebut, Inggris memulai kerjasama internasional secara bilateral dengan Indonesia. Hal ini disebabkan oleh kapasitas keamanan siber yang terbatas di Indonesia dan jumlah serbuan siber yang tinggi. Inggris mendukung kerja sama dengan Indonesia dengan memberikan dorongan pendanaan dan teknologi untuk pembangunan kapasitas. Namun, Indonesia tidak secara langsung menerima dorongan ini karena diperlukan ulasan dan persetujuan lebih lanjut. Selain itu, kerjasama siber dengan Indonesia akan memberi Inggris kesempatan untuk melihat peluang di dunia siber Indonesia.

Tujuannya adalah untuk mendorong perekonomian pasar digital dan sekaligus meningkatkan posisi bisnis Inggris di pasar global. Pemerintah Inggris melihat kemungkinan dan kemampuan Indonesia yang dapat membantu Inggris, terutama bagi industri Inggris yang bergerak di bidang penyedia layanan keamanan siber dan teknologi data dan komunikasi. Namun, selain itu, Inggris sangat tertarik untuk mengumpulkan data penting, yang berkontribusi pada kelangsungan negaranya. Kepentingan lain Inggris dalam melindungi keamanan negaranya di luar wilayah Inggris termasuk mengumpulkan dan memberikan data yang diperlukan untuk pemerintah Inggris mengenai kemajuan suatu negeri yang diuji oleh intelijen Inggris. Data-data ini berkaitan dengan kebijakan dan pengambilan keputusan, ekonomi, dan peta kekuatan di bidang politik, ekonomi, dan militer. Sehingga pemerintah Inggris dapat dengan mudah menetapkan arah kebijakan luar negara, organisasi intelijen Inggris yang berada di luar daerah kedaulatan nasional Inggris akan bertanggung jawab secara langsung kepada Departemen Luar Negara Inggris, seperti Secret Intelligence Service (SIS-MI 6), dan Government Communications Headquarters (GCHQ) (Mata-mata News, 2016).

Selain itu, intelijen Inggris akan terus memperketat keamanan dan rahasia informasi. Ini berarti bahwa intelijen negara lain tidak akan dapat meretas sistem data informasi, apalagi komunikasi elektronik yang diupayakan oleh pemerintah Inggris. Semua data yang dikumpulkan berasal dari persebaran anggota intelijen Inggris, yang kemudian dilaporkan atau diproses melalui pengawasan dari seluruh sistem teknologi data dan komunikasi elektronik, seperti internet. Jadi, jelas bahwa Inggris menawarkan kerjasama keamanan siber dengan Indonesia untuk mengurangi tindak kejahatan siber dan memastikan bahwa informasi yang dimiliki Indonesia aman dan rahasia. Pemerintah Inggris akan sangat terbantu dengan data ini untuk mengetahui kekuatan keamanan siber Indonesia, mengidentifikasi penyerangan dan ancaman keamanan nasional Inggris, dan mengambil tindakan pencegahan dan penangkalan jika terjadi penyerangan. Selain itu, pemerintah Inggris berusaha mendapatkan data secara langsung untuk digunakan dalam perundingan diplomasi.

Strategi Keamanan Siber Nasional Pemerintah Inggris bertujuan untuk melindungi dan mempromosikan Inggris di dunia digital, dengan menyatakan bahwa pemerintah akan bekerja sama dengan industri dan akademisi untuk membuat Inggris lebih tahan terhadap serangan dunia siber. Akibatnya, pemerintah Inggris terus meningkatkan pemahaman dan keterampilan keamanan siber di sektor pendidikan. Tujuan dari inisiatif ini adalah untuk meningkatkan kualitas dan kuantitas penelitian keamanan siber dan pelatihan pascasarjana. Ini juga akan membantu para akademisi melakukan proses identifikasi penelitian tentang keamanan siber dan memberikan pelatihan terbaik untuk program pascasarjana pemerintah Inggris yang berkaitan dengan dunia siber. Dengan memaksimalkan kemampuan akademisi, khususnya dalam bidang keamanan siber, pemerintah Inggris akan dapat mencapai visi dan tujuan bersama di antara komunitas riset keamanan siber di dalam dan di luar kampus.

Ini juga akan membantu masyarakat negara bagian Inggris dalam memperoleh pemahaman yang lebih baik tentang cara melindungi diri sendiri di internet, dan membantu industri dan pemerintah dalam menerapkan pengembangan terbatas. Di Inggris Raya, ada 19 perguruan tinggi yang sangat baik dan berkualifikasi di bidang keamanan siber. Ke-19 perguruan tinggi ini memiliki jurusan terpaut siber dan keamanan siber, yang diakui oleh Pusat Keunggulan Akademik dalam Studi Keamanan Siber (DIT UK, 2020). Tidak perlu diragukan lagi bahwa Pusat Keunggulan Akademik bertanggung jawab atas studi keamanan siber. Ini diakui secara resmi oleh Dewan Riset Teknik dan Fisika atau Engineering and Physical Sciences Research Council (EPSRC) dan Dewan Komunikasi Pemerintah atau Government Communications Headquarters (GCHQ) untuk memimpin dan mempertimbangkan rencana untuk mengakui peran pusat keunggulan akademik Inggris dalam riset keamanan siber.

C. Hambatan Dalam Proses Kerjasama

Bidang keamanan siber Indonesia dan Inggris menghadapi kendala selama proses kerjasama, sehingga tidak banyak konvensi kerjasama yang dicoba diterapkan. Terdapat beberapa kendala yang mungkin menghambat pelaksanaan kerjasama Cyber Diplomacy antara Indonesia dan Inggris. Berikut adalah beberapa contoh kendala yang dapat terjadi: Perbedaan Kebijakan dan Pendekatan: Indonesia dan Inggris mungkin memiliki kebijakan dan pendekatan yang berbeda terkait keamanan siber nasional. Perbedaan ini dapat menghambat pemahaman dan koordinasi antara kedua negara dalam mengimplementasikan kerjasama yang efektif. Perbedaan Infrastruktur dan Kapasitas: Indonesia dan Inggris mungkin memiliki tingkat perkembangan infrastruktur keamanan siber yang berbeda. Perbedaan ini bisa menyebabkan kesenjangan dalam kapasitas dan kemampuan untuk melakukan kegiatan kerjasama yang sebanding.

Masalah Hukum dan Regulasi: Perbedaan dalam sistem hukum dan regulasi masing-masing negara dapat menjadi kendala dalam pelaksanaan kerjasama cyber diplomacy. Keberadaan perbedaan ini bisa menghambat harmonisasi kebijakan, perlindungan data, dan implementasi aturan cyber security yang seragam antara Indonesia dan Inggris. Keterbatasan Sumber Daya dan Anggaran: Pada beberapa kasus, keterbatasan sumber daya dan anggaran dapat mempengaruhi tingkat komitmen dan dedikasi kedua negara terhadap kerjasama. Jika salah satu negara memiliki keterbatasan dalam hal sumber daya atau anggaran, hal ini bisa menghambat pelaksanaan kerjasama secara optimal. Kesenjangan Teknologi dan Keahlian: Perbedaan dalam tingkat perkembangan teknologi dan keahlian dalam bidang keamanan siber juga dapat menjadi hambatan. Jika terdapat kesenjangan ini, maka koordinasi dan implementasi kerjasama secara efektif dapat terhambat.

Masalah Keamanan dan Kerahasiaan: Dalam kerjasama cyber diplomacy, kerahasiaan dan keamanan informasi sangat penting. Tetapi, risiko potensial terkait dengan serangan siber atau pelanggaran keamanan dapat menjadi kendala dalam berbagi informasi dan kolaborasi secara terbuka. Aspek Politik dan Diplomatik: Adanya dinamika politik dan kepentingan nasional yang beragam antara Indonesia dan Inggris bisa menjadi kendala. Faktor politik dan diplomatik ini dapat mempengaruhi kebijakan, prioritas, dan kemauan politik untuk menjalankan kerjasama cyber diplomacy dengan maksimal. Penting untuk diingat bahwa kendala-kendala ini bersifat umum dan dapat berbeda dalam setiap konteks kerjasama antara Indonesia dan Inggris dalam pengembangan keamanan siber nasional melalui cyber diplomacy. Dalam mengatasi kendala-kendala ini, komunikasi yang efektif, negosiasi yang baik, dan kesepakatan yang solid menjadi penting untuk memastikan pelaksanaan kerjasama yang sukses.

5. KESIMPULAN

Karena posisi strategis Indonesia terhadap negara-negara kuat di bidang siber, diperlukan kelembagaan siber yang menangani aspek keamanan siber dan diplomasi siber. Oleh karena itu, Indonesia harus membentuk Badan Siber dan Sandi Negara (BSSN), yang merupakan pengembangan dari Lembaga Sandi Negara. BSSN bertanggung jawab atas koordinasi dan kerja sama antara institusi dan pemangku kepentingan di bidang siber. Sebagai salah satu lembaga yang bertanggung jawab untuk melaksanakan diplomasi siber di Indonesia, BSSN telah menjalin kerjasama secara bilateral dengan Inggris dalam hal ini. Strategi Keamanan Siber Indonesia berfokus pada beberapa bidang, seperti ketahanan siber, keamanan layanan publik, penguatan hukum siber, budaya keamanan siber, dan keamanan siber pada ekonomi digital, sebagai tujuan strategis. Strategi keamanan informasi Indonesia yang diantisipasi dalam berbagai forum keamanan dunia maya internasional akan berfungsi sebagai satu-satunya landasan penting untuk penerimaan dunia global terhadap Indonesia. Strategi Keamanan Siber Indonesia merupakan landasan upaya pemerintah Indonesia untuk memajukan keamanan nasional. Kesimpulan dari rumusan masalah adalah bahwa kerjasama bilateral antara Indonesia dan Inggris dalam pengembangan keamanan nasional melalui cyber diplomacy membutuhkan upaya yang signifikan untuk terwujud. Terdapat berbagai kepentingan nasional yang mendorong kedua negara untuk bekerjasama dalam mengembangkan keamanan siber nasional.

Beberapa kepentingan nasional yang mendorong Indonesia dan Inggris untuk bekerjasama dalam pengembangan keamanan siber nasional antara lain: Perlindungan Data dan Infrastruktur Kritis: Keamanan siber menjadi prioritas nasional bagi kedua negara untuk melindungi data dan infrastruktur kritis dari serangan siber yang merusak. Peningkatan Kemampuan Teknologi dan Penanganan Serangan Siber: Melalui kerjasama, kedua negara dapat saling berbagi pengetahuan, teknologi, dan taktik dalam menangani serangan siber. Menghadapi Ancaman Bersama: Ancaman siber tidak mengenal batas negara, oleh karena itu, kerjasama antara Indonesia dan Inggris sangat penting untuk menghadapi ancaman siber yang bersifat transnasional. Peningkatan Kerja Sama Ekonomi: Keamanan siber yang kuat dapat mendorong pertumbuhan ekonomi dan investasi dari kedua negara dengan menciptakan lingkungan berbisnis yang aman dan terpercaya.

Namun, dalam implementasi kerjasama Indonesia dan Inggris dalam pengembangan keamanan siber nasional melalui cyber diplomacy, terdapat beberapa hambatan dan tantangan yang harus dihadapi, antara lain: Perbedaan Kebijakan dan Pendekatan: Perbedaan dalam kebijakan dan pendekatan keamanan siber nasional dapat menghambat pemahaman dan koordinasi antara kedua negara. Perbedaan Infrastruktur dan Kapasitas: Keterbatasan dalam infrastruktur dan kapasitas keamanan siber dapat menjadi kendala dalam implementasi kerjasama yang sebanding. Masalah Hukum dan Regulasi: Perbedaan dalam sistem hukum dan regulasi dapat menghambat harmonisasi kebijakan dan implementasi aturan keamanan siber yang seragam. Keterbatasan Sumber Daya dan Anggaran: Keterbatasan sumber daya dan anggaran dapat mempengaruhi tingkat komitmen dan dedikasi kedua negara terhadap Kerjasama.

Kesenjangan Teknologi dan Keahlian: Perbedaan dalam tingkat perkembangan teknologi dan keahlian dapat menghambat koordinasi dan implementasi kerjasama yang efektif. Masalah Keamanan dan Kerahasiaan: Risiko terkait dengan serangan siber atau pelanggaran keamanan dapat menyulitkan pertukaran informasi dan kolaborasi secara terbuka. Aspek Politik dan Diplomati: Dinamika politik dan kepentingan nasional yang beragam dapat mempengaruhi kebijakan, prioritas, dan kemauan politik untuk menjalankan kerjasama dengan maksimal. Dalam mengatasi kendala-kendala ini, penting untuk menjaga komunikasi yang efektif, negosiasi yang baik, dan mencapai kesepakatan yang solid antara Indonesia dan Inggris. Bertukar pengetahuan, berbagi sumber daya, dan meningkatkan kerja sama akan membantu mewujudkan tujuan bersama dalam pengembangan keamanan siber nasional melalui cyber diplomacy.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah banyak memberikan masukan dan saran dalam penyelesaian penelitian ini.

REFERENSI

- [1] Anindita, H. (2020). *Hubungan Bilateral : Pengertian, Tujuan dan Manfaatnya*. Jojonomic.
<https://www.jojonomic.com/blog/hubungan-bilateral/>
- [2] Attatfa, A., Renaud, K., & de Paoli, S. (2020). Cyber diplomacy: A systematic literature review. *Procedia Computer Science*, 176, 60–69. <https://doi.org/10.1016/j.procs.2020.08.007>
- [3] Ayu, M. G. (2023). *Tingkatkan Keamanan Siber di Indonesia, Pemerintah Perlu Lakukan Kerja Sama dengan Developer Lokal*. Cloud Computing Indonesia..
- [4] BSSN. (2021). *Perkuat Keamanan dan Ketahanan Siber Nasional, BSSN Selenggarakan Sosialisasi dan Simulasi Penilaian Tingkat Kematangan Keamanan Siber Berbasis Cyber Security Framework untuk Sektor Pemerintah* www. Badan Siber Dan Sandi Negara.
- [5] BSSN. (2023). *RI-Inggris Sepakat Lanjutkan Kerja Sama Keamanan Siber* www. BSSN.Go.Id.
<https://www.bssn.go.id/ri-inggris-sepakat-lanjutkan-kerja-sama-keamanan-siber/>
- [6] Dewan Teknologi Informasi dan Komunikasi Nasional. (2018). Pengembangan keamanan siber nasional. *Policy Paper*, 1–30.
- [7] DIT Uk. (2020). *Cyber security inggris*. Great.Gov.Uk.
<https://www.events.great.gov.uk/website/4308/bah/home/>
- [8] Fakhrol Muhammad, Abdul Rivai Kardi Ras, K. K. (2022). KEAMANAN NASIONAL SEBAGAI SEBUAH KONSEP SISTEM PERTAHANAN DAN KEAMANAN BAGI INDONESIA. *Jurnal Ilmiah Indonesia*, 7(8.5.2017).
- [9] Ghernaouti-Hélie. (2009). Cybersecurity Guide for Developing Countries. *Development*, 178.
<https://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf>
- [10] Kementerian Kesehatan Republik Indonesia. (2021). *Kemenkes Ri -Kedutaan Inggris Gelar Workshop Pengembangan Keamanan Siber dan Perlindungan Data Pribadi Pada Layanan Telemedicine Di Indonesia*. <https://www.kemkes.go.id/article/print/21011900002/kemenkes-ri--kedutaan-inggris-gelar-workshop-pengembangan-keamanan-siber-dan-perlindungan-data-priba.html>
- [11] KEMHAN. (2018). Badan Instalasi Strategis Pertahanan. In *Kementerian Pertahanan Republik Indonesia*. [cybersecurityindo.com. https://www.kemhan.go.id/bainstrahan/2016/08/01/hadirnya-badan-intel-kemhan-jadi-benteng-ancaman-nonmiliter.html](https://www.kemhan.go.id/bainstrahan/2016/08/01/hadirnya-badan-intel-kemhan-jadi-benteng-ancaman-nonmiliter.html)
- [12] Mata-mata News. (2016). Mengenal Lebih Dekat Badan Intelijen Asing. In *Badan Intelijen Negara*.

<http://www.bin.go.id/internasional/detil/103/5/13/06/2012/mengenal-lebih-dekat-badan-intelijen-asing>

- [13] Nadhifah, H. N. (2020). *Diplomasi Siber Indonesia dalam United Nations Group of Governmental Experts on Development in the Field of Information and Telecommunication in the Context of International Security 2012-2019*. i–140. <https://repository.uinjkt.ac.id/dspace/handle/123456789/59997>
- [14] Navari, C. (2016). Hans Morgenthau and the National Interest. In *Carnegie Council for Ethics in International Affairs*. <https://doi.org/10.1016/B978-0-323-46294-5.00028-5>
- [15] Pettit, H. (2017). Ransomware and the WannaCry virus that crippled the NHS | Daily Mail Online. In *Daily Mail*. <http://www.dailymail.co.uk/sciencetech/article-4500614/All-need-know-ransomware-WannaCry-virus.html>
- [16] Rana, K. S. (2018). Bilateral Diplomacy. *The Encyclopedia of Diplomacy, March 2018*, 1–11. <https://doi.org/10.1002/9781118885154.dipl0023>
- [17] Robert Owen Keohane and Joseph S. Nye. (2011). " *Power and Interdependence*." *Fourth Edition* (pp. 5–6). Longman Classic in Political Science.
- [18] Simatupang, H. Y., & Ridwan, R. (2022). Penyuluhan Dampak Cyber-crime Terhadap Keamanan Nasional Di Kalangan Pelajar MAS YASPI Labuhan Deli Medan. *Publidimas*, 2(1). <https://e-journal.potensi-utama.ac.id/ojs/index.php/PUBLIDIMAS/article/view/1633>
- [19] Soewardi, B. A. (2013). Perlunya pembangunan sistem pertahanan siber (Cyber defense) yang tangguh bagi Indonesia. *Potensi Pertahanan*, 31–35.
- [20] Usman, B. F. (2021). Faktor-Faktor Yang Melatar Belakangi Kerjasama Indonesia Dengan Inggris Dibidang Keamanan Siber Tahun 2018. *Moestopo Journal of International Relations*, 1(2), 107–114. <https://journal.moestopo.ac.id/index.php/mjir/article/view/1484>