DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 1, No. 1 Tahun 2024 Hal. 339-349
e-ISSN: _____ DOI: 10.36859/dgsj.v1i1.2889

Article History:
Submitted: Sept 10, 2024
Accepted:Oct 24, 2024
Published:Oct 27, 2024

KERJASAMA KEAMANAN SIBER INDONESIA-INGGRIS PADA PERIODE 2018-2028

Ridwan Adi Nurdiyanto[1], Agus Subagyo[2], Suwarti Sari[3]

1. Program Studi Magister Hubungan Internasional Universitas Jenderal Achmad Yani, Cimahi, Indonesia

2. Program Studi Magister Hubungan Internasional Universitas Jenderal Achmad Yani, Cimahi, Indonesia

2. Program Studi Magister Hubungan Internasional Universitas Jenderal Achmad Yani, Cimahi, Indonesia

ABSTRACT

Cybercrime is not only a technical issue but also impacts ideological, political, economic, social, cultural, and national security aspects. Therefore, cybersecurity is essential to protect telematics systems from threats in cyberspace. This study aims to analyze and examine in detail the national interests sought by Indonesia and the strategies employed in its cyber cooperation with the United Kingdom. The research employs a descriptive qualitative method, with data collection techniques including literature studies and interviews. The results show that the cooperation between Indonesia and the United Kingdom in the field of cybersecurity aims to strengthen the cyber resilience of both countries through a Memorandum of Understanding signed on August 14, 2018. The main focus of this cooperation is capacity building, particularly in Cyber Law and Cybersecurity Awareness, involving initiatives such as training seminars, increasing internet access, and establishing the Computer Security Incident Response Team (CSIRT). Despite facing challenges such as differences in policies, regulations, and resource limitations, this cooperation remains crucial for addressing transnational cyber threats and protecting critical data and infrastructure. Future prospects include enhancing information sharing to tackle cyber-attacks more effectively.

Keywords: Cybersecurity, defense cooperation, national interest

ABSTRAK

Kejahatan siber tidak hanya menjadi masalah teknis tetapi juga berdampak pada aspek ideologi, politik, ekonomi, sosial, budaya, dan keamanan nasional. Oleh karena itu, keamanan siber menjadi penting untuk melindungi sistem telematika dari ancaman di dunia maya. Penelitian ini dilaksanakan dengan maksud guna menganalisa dan mengetahui secara detail dan mendalam mengenai kepentingan nasional yang berusaha diperoleh oleh Indonesia dan strategi apa yang berusaha dilakukan oleh Indonesia dalam melakukan Kerjasama siber dengan Inggris. Metode yang digunakan pada penelitian ini adalah metode kualitatif deskriptif. Teknik pengumpulan data yang digunakan berupa studi Pustaka dan wawancara. Hasil penelitian menunjukan Kerjasama antara Indonesia dan Inggris dalam bidang keamanan siber bertujuan memperkuat ketahanan siber kedua negara melalui nota kesepahaman yang ditandatangani pada 14 Agustus 2018. Fokus utama kerjasama ini adalah peningkatan kapasitas, terutama dalam hal Cyber Law dan Cybersecurity Awareness, yang melibatkan inisiatif seperti seminar pelatihan, peningkatan akses internet, dan pembentukan Computer Security Incident Response Team (CSIRT). Meski menghadapi kendala seperti perbedaan kebijakan, regulasi, dan keterbatasan sumber daya, kerjasama ini tetap penting untuk menghadapi ancaman siber transnasional serta melindungi data dan infrastruktur kritis. Prospek kedepannya mencakup peningkatan information sharing untuk menghadapi serangan siber secara lebih efektif.

Kata kunci : Keamanan siber, Kerjasama pertahanan, kepentingan nasional

PENDAHULUAN

Globalisasi dan kemajuan teknologi telah mengubah ancaman pertahanan dan keamanan, dari yang konvensional menjadi non-konvensional seperti terorisme, perubahan

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 1, No. 1 Tahun 2024 Hal. 339-349
e-ISSN: _____ DOI: 10.36859/dgsj.v1i1.2889

Article History:
Submitted: Sept 10, 2024
Accepted:Oct 24, 2024
Published:Oct 27, 2024

iklim, pandemi, dan serangan siber. Internet, meskipun memudahkan akses informasi dan hubungan antarnegara, juga menimbulkan tantangan keamanan seperti kejahatan siber, yang mencakup pencurian informasi, penyebaran ide destruktif, dan penyerangan terhadap infrastruktur kritis.

Kejahatan siber tidak hanya menjadi masalah teknis tetapi juga berdampak pada aspek ideologi, politik, ekonomi, sosial, budaya, dan keamanan nasional. Oleh karena itu, keamanan siber menjadi penting untuk melindungi sistem telematika dari ancaman di dunia maya. Indonesia mengalami peningkatan kejahatan siber seiring pertumbuhan pengguna internet, yang menandakan perlunya penguatan keamanan siber.

Untuk mengatasi hal ini, Indonesia membentuk Badan Siber dan Sandi Negara (BSSN) serta menerapkan UU ITE. Selain itu, Indonesia bekerja sama dengan negara lain, termasuk Inggris, dalam memperkuat keamanan siber. Pada 2018, Indonesia dan Inggris menandatangani MoU tentang keamanan siber, yang mencakup pengembangan strategi, penanganan kejahatan siber, serta pelatihan di bidang keamanan siber. Inggris dipilih karena reputasinya yang kuat, termasuk dalam penanganan serangan ransomware WannaCry pada 2017. Kerja sama ini diperpanjang hingga 2027 untuk menghadapi tantangan siber di masa depan.

Kolaborasi ini menunjukkan komitmen kedua negara dalam memperkuat kapasitas keamanan siber dan pentingnya kerjasama internasional dalam mengatasi ancaman kejahatan siber yang semakin kompleks.

KERANGKA ANALITIK

Kerangka pemikiran dalam penelitian ini mulai berkembang dengan mempertimbangkan berbagai jenis kerjasama bilateral antar negara di dunia, dan pada akhirnya penelitian ini terfokus pada Indonesia sebagai objek penelitian utama dan berbagai negara mitra lainnya mencoba menerapkan Kerjasama (James E. Dougherty dan Robert L, 1986). Dalam konteks ini, peneliti fokus pada topik dan permasalahan di bidang pertahanan dan keamanan, suatu bidang yang sangat penting bagi semua negara di dunia untuk menjaga dan terus meningkatkan kemampuan pertahanannya. Pada akhirnya, peneliti mengambil pilihan pada Kerjasama pertahanan dan keamanan pada bidang siber yang dilakukan oleh Indonesia dan Inggris dalam rentan waktu sejak tahun 2018 hingga 2022,

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 1, No. 1 Tahun 2024 Hal. 339-349
e-ISSN: _____ DOI: 10.36859/dgsj.v1i1.2889

Article History:
Submitted: Sept 10, 2024
Accepted:Oct 24, 2024
Published:Oct 27, 2024

penelitian ini pada akhirnya melihat berbagai macam metode atau bentuk Kerjasama dalam aspek pertahanan siber.

Peneliti menggunakan berbagai teori dan konsep dalam memahami permasalahan mengenai Analisa Kerjasama keamanan siber yang dilakukan oleh Indonesia dan Inggris, pada akhirnya peneliti mencoba untuk memahami melalui pendekatan liberalism sebagai dasar dalam memandang permasalahan yang sedang terjadi melalui sisi teoritis. Setelah itu, peneliti mendalami kembali melalui konsep yang berkaitan dengan permasalahan tersebut seperti konsep Kerjasama internasional, konsep keamanan siber, hingga kepentingan nasional. Dalam penelitian ini, penulis membahas bagaimana bentuk dan implementasi dari Kerjasama bilateral ini yang dilaksanakan oleh Indonesia dan Inggris dalam keamanan siber, dalam hal ini apakah kerja sama tersebut dapat memberikan dampak yang positif kepada kedua negara dalam keamanan sibernya (Handrini Ardiyanti, 2014).

Pada akhirnya, dengan adanya pemahaman yang mendalam mengenai bentuk dan implementasi kerja yang dilakukan oleh Indonesia dan Inggris, peneliti akan menganalisis secara mendalam mengenai aspek kepentingan nasional yang melatarbelakangi adanya Kerjasama ini. Pada keadaan ini peneliti akan membahas mengenai kemungkinana adanya relevansi pada kepentingan nasional Indonesia dengan Kerjasama yang dilakukan bersama dengan Inggris, yakni terdapat keadaan yang lebih membaik dari keamanan siber yang ada di Indonesia dengan adanya kekuatan baru dalam menjaga keamanan dan kedaulatannya di dunia siber

METODE PENELITIAN

Untuk melakukan penelitian, peneliti menggunakan metode penelitian kualitatif sebagai alat bantunya. Penelitian ini disusun berdasarkan data deskriptif yang menggambarkan kerjasama keamanan siber indonesia-inggris pada periode 2018-2028. Penelitian kualitatif merupakan metode penelitian yang cocok untuk menjawab pertanyaan penelitian yang memerlukan penyelidikan variabel dan mempelajari fenomena secara lebih mendalam untuk memahami pertanyaan penelitian. Dalam hal ini penelitian yang menggunakan metode kualitatif memusatkan perhatian pada fenomena atau proses permasalahan yang diteliti, dan hasilnya memuat makna-makna yang muncul dari eksplorasi peneliti dalam proses tersebut (Creswell, 2011).

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 1, No. 1 Tahun 2024 Hal. 339-349
e-ISSN: _____ DOI: 10.36859/dgsj.v1i1.2889

Article History:
Submitted: Sept 10, 2024
Accepted:Oct 24, 2024
Published:Oct 27, 2024

Teknik pengumpulan data yang digunakan penulis dalam makalah ini adalah studi pustaka. Dengan menggunakan teknik pengumpulan data tertentu, penulis bermaksud memberikan penjelasan tentang Kerjasama keamanan siber Indonesia-inggris.. Metode analisis data yang digunakan dalam penelitian ini adalah analisis kualitatif yang digunakan secara interaktif dalam proses reduksi data, penyajian, dan penarikan kesimpulan

PEMBAHASAN

Pemerintah Indonesia dan Inggris memulai kerja sama dalam keamanan siber dengan menandatangani Nota Kesepahaman (MoU) pada 14 Agustus 2018, yang berlangsung selama lima tahun. Pada 2023, kerja sama ini diperpanjang hingga 2028. MoU ini diwakili oleh Badan Siber dan Sandi Negara dari Indonesia dan Wakil Perdana Menteri Inggris. Fokus utama dari kerja sama ini adalah pengembangan kapasitas dalam bidang keamanan siber, yang dimulai pada 2019 dengan dua program utama: Cyber Law dan Cyber Security Awareness.

Dalam program ini, diskusi mengenai United Nations Group of Governmental Experts (UN GGE) menekankan pada peningkatan kapasitas negara dalam keamanan siber serta membangun kepercayaan untuk kerja sama siber baik secara bilateral maupun multilateral. Selain itu, Tallinn Manual 2.0 juga dibahas sebagai pedoman terkait hukum internasional dalam operasi siber. Dalam ulasan keamanan siber, topik yang dibahas meliputi penanganan hoaks, pengamanan data pribadi, serta teknik analisis malware, strategi mitigasi, dan langkah-langkah yang harus diambil jika terjadi serangan siber. Diskusi ini bertujuan memperkuat kesiapan Indonesia dan Inggris dalam menghadapi ancaman siber di masa depan.

Kepentingan Nasional Indonesia

Pemerintah Indonesia menyadari bahwa ancaman siber merupakan tantangan serius yang dapat memengaruhi ekonomi, keamanan nasional, dan kedaulatan negara. Kejahatan siber yang berskala internasional mengharuskan adanya kerja sama global untuk memerangi ancaman ini. Dalam konteks ini, Indonesia bekerja sama dengan Inggris untuk meningkatkan efisiensi dan optimalisasi strategi keamanan sibernya, khususnya dalam tiga area utama:

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 1, No. 1 Tahun 2024 Hal. 339-349
e-ISSN: _____ DOI: 10.36859/dgsj.v1i1.2889

Article History:
Submitted: Sept 10, 2024
Accepted:Oct 24, 2024
Published:Oct 27, 2024

1. Memperkuat Keamanan Siber di Sektor Pemerintah

Kerja sama dengan Inggris memungkinkan Indonesia belajar dari Government Communications Headquarters (GCHQ) tentang manajemen keamanan siber di sektor pemerintahan. Melalui kerja sama ini, Gov-CSIRT Indonesia akan bekerja sama dengan lembaga-lembaga pemerintah di berbagai tingkat untuk memperkuat keamanan siber nasional. Tujuannya adalah agar seluruh zona pemerintahan dapat mengelola dan melindungi keamanan siber dengan lebih efektif, dengan Badan Siber dan Sandi Negara (BSSN) sebagai penghubung utama.

2. Pembelajaran melalui Akademisi

Kerja sama ini memberi Indonesia kesempatan untuk memperkuat pembelajaran akademik terkait keamanan siber. Meskipun Indonesia telah memasukkan mata pelajaran teknologi komputer ke dalam kurikulum sekolah, pusat penelitian keamanan siber di tingkat universitas masih kurang optimal. Inggris akan memberikan panduan untuk meningkatkan kapasitas akademik dalam bidang ini, yang diharapkan dapat membantu memperkuat kolaborasi antara pemerintah, industri, dan masyarakat dalam menerapkan strategi keamanan siber dan meningkatkan kesadaran publik.

3. Meningkatkan Keamanan Infrastruktur Penting Nasional

Kerjasama dengan Inggris juga akan membantu Indonesia melindungi infrastruktur penting yang terhubung ke dunia siber, seperti sektor keuangan, transportasi, energi, pertahanan, dan kesehatan. Her Majesty's Government (HMG) di Inggris menangani keamanan infrastruktur kritis dan bekerja sama dengan Perlindungan Infrastruktur Nasional Inggris untuk memastikan kontrol keamanan terhadap infrastruktur vital. Indonesia berharap dapat menerapkan pendekatan serupa untuk melindungi infrastrukturnya dari ancaman siber yang berbahaya (Soewardi, 2013).

Secara keseluruhan, kerja sama Indonesia-Inggris diharapkan dapat meningkatkan kapasitas keamanan siber Indonesia dengan melibatkan berbagai pemangku kepentingan dan memperkuat perlindungan terhadap ancaman siber yang terus berkembang.

Kepentingan Nasional Inggris

Pemerintah Inggris menganggap keamanan siber sebagai salah satu prioritas utama dalam Strategi Nasional Inggris 2016-2021. Tujuan utamanya adalah menjadikan Inggris negara yang aman untuk berbisnis di dunia maya, dengan mendorong kolaborasi

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 1, No. 1 Tahun 2024 Hal. 339-349
e-ISSN: _____ DOI: 10.36859/dgsj.v1i1.2889

Article History:
Submitted: Sept 10, 2024
Accepted:Oct 24, 2024
Published:Oct 27, 2024

internasional melalui kerjasama bilateral dan multilateral. Hal ini penting karena serangan siber tidak hanya terjadi di dalam negeri tetapi juga di luar negeri, sehingga Inggris memerlukan pendekatan global untuk melindungi keamanan dan kepentingan nasionalnya (Usman, 2021).

Kerjasama siber dengan Indonesia menjadi salah satu bagian penting dari strategi ini. Inggris melihat potensi besar dalam bekerja sama dengan Indonesia, terutama karena keamanan siber di Indonesia masih terbatas dan jumlah serangan siber cukup tinggi. Inggris mendukung pengembangan kapasitas keamanan siber Indonesia dengan menyediakan pendanaan dan teknologi, meski hal ini masih memerlukan ulasan lebih lanjut dari pihak Indonesia.Kerjasama tersebut tidak hanya menguntungkan Indonesia dalam memperkuat keamanan sibernya, tetapi juga memberi Inggris akses ke data penting terkait keamanan, ekonomi, dan politik yang membantu Inggris dalam pengambilan kebijakan luar negerinya. Secret Intelligence Service (MI6) dan Government Communications Headquarters (GCHQ) memainkan peran penting dalam mengawasi keamanan siber, mengumpulkan informasi intelijen, serta melindungi infrastruktur data dari ancaman eksternal.

Selain itu, strategi Inggris juga mencakup penguatan di bidang pendidikan dengan meningkatkan penelitian dan pelatihan terkait keamanan siber. Inggris memiliki 19 universitas terkemuka yang diakui sebagai Pusat Keunggulan Akademik dalam Studi Keamanan Siber, di mana akademisi dan profesional dilatih untuk meningkatkan keterampilan mereka di dunia siber. Ini bertujuan untuk memperkuat kemampuan penelitian, meningkatkan kualitas sumber daya manusia, serta mendukung pemerintah dan industri dalam menerapkan kebijakan keamanan siber.

Kerjasama siber Inggris-Indonesia berperan penting dalam meningkatkan keamanan kedua negara. Di satu sisi, Indonesia dapat memperkuat perlindungan terhadap infrastruktur penting dan mengurangi tindak kejahatan siber, sementara di sisi lain, Inggris mendapatkan akses ke peluang bisnis di sektor keamanan siber dan data yang membantu memperkuat posisinya di kancah global.

Implementasi Kerjasama Keamanan Siber Indonesia dan Inggris

Kerjasama Indonesia dan Inggris dalam bidang keamanan siber telah berjalan selama lima tahun sejak ditandatangani pada tahun 2018. Nota kesepahaman ini dilanjutkan untuk lima tahun berikutnya, dengan fokus pada peningkatan kapasitas keamanan siber melalui

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 1, No. 1 Tahun 2024 Hal. 339-349
e-ISSN: _____ DOI: 10.36859/dgsj.v1i1.2889

Article History:
Submitted: Sept 10, 2024
Accepted:Oct 24, 2024
Published:Oct 27, 2024

pertukaran pengetahuan. Kedua negara, melalui Badan Siber dan Sandi Negara (BSSN) dari Indonesia dan National Cyber Security Centre (NCSC) dari Inggris, berkomitmen untuk menciptakan ruang siber yang terbuka, aman, dan bertanggung jawab. Kerjasama ini mencakup berbagai inisiatif penting, di antaranya:

1. Seminar Pelatihan dan Keamanan Siber: Sejak 2019, BSSN dan NCSC Inggris mengadakan pelatihan teknis keamanan siber yang bertujuan meningkatkan kapasitas SDM di bidang keamanan jaringan dan pengelolaan ancaman siber.
2. Cyber Practitioners Course: Webinar dan sertifikasi keamanan siber untuk meningkatkan kompetensi SDM Indonesia, khususnya pada sektor Infrastruktur Informasi Kritikal Nasional (IIKN), di mana peserta dari kementerian dan institusi non-kementerian mendapatkan pelatihan kebijakan keamanan siber internasional.
3. Kolaborasi Peningkatan Akses Internet melalui Digital Access Programme: Program ini bertujuan untuk memberikan akses kesehatan melalui teknologi komunikasi, terutama selama pandemi Covid-19, dengan menggunakan bahasa lokal untuk memastikan informasi dapat diterima dengan baik oleh masyarakat.
4. Sharing Experience dalam Budaya Keamanan Siber: Berbagi pengalaman dan pengetahuan dari Inggris dalam mengembangkan budaya keamanan siber di Indonesia, termasuk di sektor layanan telemedis yang terus berkembang.
5. Peningkatan Kapasitas melalui Digital Health Programme: Kerjasama ini melibatkan sektor kesehatan, dengan tujuan membentuk Computer Emergency Response Team (CERT) untuk menangani insiden keamanan siber dan melindungi data kesehatan.
6. Pembentukan dan Pengembangan CSIRT (Computer Security Incident Response Team)**: Sejak 2019, Indonesia membentuk Gov-CSIRT untuk sektor pemerintah, dengan dukungan dari Inggris. Pada 2023 dan 2024, BSSN meluncurkan 17 dan 19 tim CSIRT baru di berbagai kementerian, lembaga, dan pemerintah daerah.

Kerjasama siber antara Indonesia dan Inggris ini bertujuan untuk memperkuat perlindungan terhadap infrastruktur kritikal dan mendukung pengembangan kapasitas siber nasional melalui berbagai program dan pelatihan, serta berbagi pengalaman dari Inggris yang memiliki sistem pertahanan siber yang kuat.

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 1, No. 1 Tahun 2024 Hal. 339-349
e-ISSN: _____ DOI: 10.36859/dgsj.v1i1.2889

Article History:
Submitted: Sept 10, 2024
Accepted:Oct 24, 2024
Published:Oct 27, 2024

Kendala dan Prospek Kerjasama Indonesia-Inggris

Kerjasama Internasional dapat dilakukan secara bilateral maupun multilateral, yang berarti kerjasama ini pasti dilakukan dengan 2 atau lebih negara sebagai pihak. Oleh karena itu, didalam pelaksanaan kerjasama ini pasti terdapat adanya kendala dan hambatan yang dirasakan dan dihadapi. Hal tersebut adalah hal yang pasti terjadi dan harus diatasi. Dikarenakan terdapat kepentingan-kepentingan tersendiri yang diinginkan oleh para pihak negara dalam perjanjian tersebut.

Selain terdapat kendala, dalam sebuah perjanjian kerjasama internasional pasti juga terdapat prospek yang diharapkan dari adanya perjanjian kerjasama tersebut. Prospek itu harus dilihat dari bagaimana keadaan di masa yang akan datang dan harus disesuaikan dengan nota kesepahaman yang ditandatangani. Peneliti dalam penelitian ini juga meneliti tentang bagaimana kendala serta prospek dalam Perjanjian Kerjasama Keamanan Siber antara Pemerintah Indonesia dan Pemerintah Inggris.

Kendala Pelaksanaan Kerjasama Keamanan Siber

Dalam pelaksanaan kerjasama keamanan siber antara Indonesia dan Inggris, terdapat berbagai kendala yang menyebabkan lambatnya implementasi beberapa kesepakatan. Beberapa faktor yang mempengaruhi hal ini antara lain:

1. Pergantian Kepemimpinan: Pada 24 Mei 2019, terjadi pergantian pimpinan di Badan Siber dan Sandi Negara (BSSN) dari Mayjen TNI (Purn.) Djoko Setiadi kepada Letjen TNI (Purn.) Hinsa Siburian. Hal ini menyebabkan perlu adanya penyesuaian ulang jadwal pelaksanaan kerjasama yang sebelumnya sudah ditetapkan. Proses penyesuaian ini memakan waktu karena koordinasi antara BSSN dan pemerintah Inggris harus direncanakan kembali.
2. Pandemi Covid-19: Pandemi menjadi hambatan besar dalam interaksi fisik antara kedua negara, terutama ketika dialog yang melibatkan topik-topik sensitif dalam keamanan siber dianggap lebih efektif dibahas secara langsung. Pertemuan yang seharusnya terjadi secara tatap muka tidak dapat dilaksanakan, dan forum online dinilai kurang memadai untuk membahas isu yang memerlukan kerahasiaan tingkat tinggi.
3. Perbedaan Kebijakan dan Pendekatan: Kebijakan nasional terkait keamanan siber di Indonesia dan Inggris mungkin berbeda, yang memengaruhi pemahaman dan koordinasi kedua negara. Inggris memiliki sistem keamanan siber yang lebih mapan dan maju,

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 1, No. 1 Tahun 2024 Hal. 339-349
e-ISSN: _____ DOI: 10.36859/dgsj.v1i1.2889

Article History:
Submitted: Sept 10, 2024
Accepted:Oct 24, 2024
Published:Oct 27, 2024

sementara Indonesia masih dalam tahap pengembangan, sehingga perbedaan infrastruktur dan kapasitas ini menjadi tantangan.

4. Masalah Hukum dan Regulasi: Perbedaan dalam regulasi dan sistem hukum antara Indonesia dan Inggris juga mempersulit harmonisasi dalam kebijakan keamanan siber. Perlindungan data pribadi dan regulasi terkait penanganan ancaman siber di kedua negara memiliki standar yang berbeda, sehingga menghambat implementasi kesepakatan secara seragam.
5. Keterbatasan Sumber Daya dan Anggaran. Beberapa kendala juga terkait dengan keterbatasan sumber daya dan anggaran, terutama dari pihak Indonesia. Keterbatasan ini dapat mempengaruhi komitmen dan pelaksanaan kerjasama, terutama dalam proyek-proyek yang membutuhkan teknologi canggih dan sumber daya manusia yang terlatih.
6. Kesenjangan Teknologi dan Keahlian: Adanya perbedaan dalam tingkat kemajuan teknologi dan keahlian di bidang keamanan siber di antara kedua negara juga menghambat efektivitas kerjasama. Inggris memiliki infrastruktur siber yang lebih berkembang, sementara Indonesia masih membangun sistemnya, sehingga koordinasi dan pelaksanaan program sering kali terhambat oleh kesenjangan ini.
7. Masalah Keamanan dan Kerahasiaan: Keamanan informasi dan kerahasiaan menjadi faktor penting dalam kerjasama ini. Kedua negara perlu berhati-hati dalam berbagi informasi sensitif yang terkait dengan pertahanan siber. Kekhawatiran terhadap potensi kebocoran data atau serangan siber yang dapat mengekspos informasi rahasia menjadi kendala dalam berbagi informasi secara terbuka.
8. Dinamika Politik dan Diplomatik: Aspek politik dan kepentingan nasional yang berbeda antara Indonesia dan Inggris juga dapat memengaruhi kerjasama ini. Isu- isu politik tertentu mungkin mengubah prioritas atau mempengaruhi komitmen kedua negara terhadap pelaksanaan program kerjasama keamanan siber.

Untuk mengatasi kendala-kendala tersebut, dibutuhkan komunikasi yang efektif, koordinasi yang baik, serta negosiasi yang terencana antara kedua belah pihak. Hal ini penting untuk menciptakan kesepakatan yang solid dan memastikan bahwa kerjasama dapat berjalan dengan lancar dan menghasilkan manfaat yang maksimal bagi keamanan siber kedua negara.

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 1, No. 1 Tahun 2024 Hal. 339-349
e-ISSN: _____ DOI: 10.36859/dgsj.v1i1.2889

Article History:
Submitted: Sept 10, 2024
Accepted:Oct 24, 2024
Published:Oct 27, 2024

Prospek Kerjasama Indonesia-Inggris

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 Indonesia 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.

KESIMPULAN

Kerjasama antara Indonesia dan Inggris dalam bidang keamanan siber bertujuan memperkuat ketahanan siber kedua negara melalui nota kesepahaman yang ditandatangani pada 14 Agustus 2018. Fokus utama kerjasama ini adalah peningkatan kapasitas, terutama dalam hal Cyber Law dan Cybersecurity Awareness, yang melibatkan inisiatif seperti seminar pelatihan, peningkatan akses internet, dan pembentukan Computer Security Incident Response Team (CSIRT). Meski menghadapi kendala seperti perbedaan kebijakan, regulasi, dan keterbatasan sumber daya, kerjasama ini tetap penting untuk menghadapi ancaman siber transnasional serta melindungi data dan infrastruktur kritis. Prospek kedepannya mencakup peningkatan information sharing untuk menghadapi serangan siber secara lebih efektif.

DAFTAR PUSTAKA

Jurnal

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 1, No. 1 Tahun 2024 Hal. 339-349
e-ISSN: _____ DOI: 10.36859/dgsj.v1i1.2889

Article History:
Submitted: Sept 10, 2024
Accepted:Oct 24, 2024
Published:Oct 27, 2024

James E. Dougherty dan Robert L, Contending Theories of International Relations: A Comprehensive Survey (New York : Longman, 1986) 419.

Buku/Disertasi

Handrini Ardiyanti, Cyber Secutity dan Tantangan Pengembangan di Indonesia, Badan Riset Inovasi Nasional Vol.3 No.1, Agustus (2014), pp.98-99

Usman, B. F. (2021). Faktor-Faktor Yang Melatar Belakangi Kerjasama Indonesia Dengan Inggris Dibidang Keamanan Siber Tahun 2018. (Jakarta:Moestopo Journal of International Relations, 1(2), 107–114.)

Holsti, K. J. (1998) Politik Internasional, Kerangka Untuk Analisis Jilid II,)Jakarta : Errlangga)

Creswell, John. Research Design . 4th. (SAGE,2018)

Artikel

BSSN. (2018). BSSN Tandatangani Nota Kesepahaman Kerjasama di Bidang Keamanan Siber Dengan Pemerintah Inggris Raya. Tersedia dalam https://www.bssn.go.id/bssn-tandatangani-nota-kesepahaman-kerjasama-di-bidang-keamanan-siber-dengan-pemerintah-inggris-raya/ diakses pada 20 Agustus 2024

BSSN. (2024). Launching CSIRT Bersama Sektor Pemerintahan dan Pembangunan Manusia. Tersedia dalam https://www.bssn.go.id/launching-csirt-bersama-sektor-pemerintahan-dan-pembangunan-manusia/ diakses pada 24 Agustus 2024

BSSN (2019). BSSN Luncurkan Government – Computer Security Incident Response Team (Gov-CSIRT) Indonesia. Tersedia dalam https://www.bssn.go.id/bssn-luncurkan-government-computer-security-incident-response-team-gov-csirt-indonesia/ diakses pada 24 Agustus 2024