GLOBAL INSIGHT JOURNAL
Jurnal Mahasiswa Program Studi
Ilmu Hubungan Internasional - FISIP - UNJANI
https:/ejournal.fisip.unjani.ac.id/index.php/GIJ
DOI : https://doi.org/10.36859/gij.v1i1.2528
Vol. 01 No. 01 Tahun 2024

Article Informations
Received: 03/08/2024; *Accepted*: 23/10/2024; *Published*: 23/10/2024
Corresponding Email:
astidwi2107@gmail.com

KERJA SAMA INDONESIA - INGGRIS DALAM MENGATASI KEJAHATAN SIBER TAHUN 2018 – 2022

Asti Dwi Ashartati[1)], Yusep Ginanjar[2)], Renaldo Benarrivo[3)].
[1,2,3,)] Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Jenderal Achmad Yani

Abstrak

Perkembangan teknologi yang sangat maju mampu memberikan banyak kemudahan namaun, dengan kemajuan perkembangan tersebut tidak hanya memberikan dampak posisitif saja namun juga mampu memberikan dampak negatif. Indonesia dan Inggris merupakan negara kedua negara yang tidak dapat terhindar dari ancaman dan serangan siber. Sehingga kedua negara perlu memperkuat ketahanan dan keamanan siber. Penelitian ini menggunakan teori neorealisme, kepentingan nasional, internasional,kerjasama pertahanan,keamanan siber. Tujuan penelitian untuk menganalisa mengenai hubungan timbal balik yang didapatkan oleh Inggris atas kerja sama dengan Indonesia dalam memperkuat keamanan siber. Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian kualitatif deskriptif. Hasil dari implementasi dari kerjasama Indonesia - Inggris telah menunjukkan bahwa Indonesia berhasil meningkatkan keamanan sibernya, yang tercermin dalam peningkatan peringkat Indonesia menjadi negara ke-24 dengan keamanan siber terbaik di dunia menurut penilaian Global Cyber-security Index (GCI).
Kata kunci: Kerjasama Siber,Indonesia,Inggris,kepentingan nasional

Abstract

The development of very advanced technology is able to provide many conveniences, however, with the progress of this development not only provides positive impacts but also can provide negative impacts. Indonesia and England are two countries that cannot avoid cyber threats and attacks.

So both countries need to strengthen cyber resilience and security. This study uses the theory of neorealism, national interests, international cooperation, defense cooperation, cyber security.The purpose of the study is to analyze the reciprocal relationship obtained by England from cooperation with Indonesia in strengthening cyber security. The research method used in this study is a descriptive qualitative research method.The results of the implementation of the Indonesia-England cooperation have shown that Indonesia has succeeded in improving its cyber security, which is reflected in the increase in Indonesia's ranking to the 24th country with the best cyber security in the world according to the Global Cyber-security Index assessment.
Keyword: Cyber Cooperation, Indonesia, UK, national interest

1. PENDAHULUAN

Kejahatan dunia maya memiliki implikasi yang signifikan terhadap hubungan internasional, karena kejahatan ini melampaui batas-batas negara dan dapat merenggangkan hubungan diplomatik. Kejahatan terorganisir transnasional di dunia maya dapat merusak perdamaian, kebebasan, dan demokrasi global, serta menjadi ancaman bagi keamanan dan kemakmuran negara. Dampak konflik siber, operasi siber, dan kejahatan siber terhadap interaksi internasional kini dianggap sebagai bagian dari hubungan internasional yang normal. Diplomasi siber memainkan peran penting dalam menjaga kepentingan nasional dan mempromosikan hubungan damai dalam menghadapi ancaman siber. Contoh-contoh kejahatan siber, seperti peretasan dan pelanggaran data, telah menyebabkan hubungan yang tegang antar negara, menyoroti efek luas dari insiden siber terhadap hubungan internasional.

Oleh karena itu, menangani kejahatan siber dalam konteks hubungan internasional membutuhkan kerja sama yang efektif dan upaya diplomatik untuk mengurangi pengaruhnya yang mengganggu. Kejahatan siber merupakan kejahatan yang menggunakan teknologi informasi dan komunikasi untuk melakukan tindak

pidana. Kejahatan siber memiliki dampak yang luas, baik bagi individu, organisasi, maupun negara. Dampak kejahatan siber dapat berupa kerugian finansial, pelanggaran privasi, hingga ancaman terhadap keamanan nasional. Indonesia dan Inggris merupakan dua negara yang memiliki hubungan bilateral yang kuat di berbagai bidang termasuk politik, ekonomi, dan pertahanan.

Dalam bidang keamanan siber, kedua negara telah menjalin kerja sama sejak tahun 2018. Sejarah kerja sama siber Indonesia- Inggris dimulai pada tahun 2018 ketika kedua negara menandatangani Nota Kesepahaman Kerja Sama Keamanan Siber.[1] Sejak saat itu, kedua negara telah bekerja sama untuk meningkatkan kerja sama keamanan siber, bertukar pandangan dan praktik terbaik terkait strategi nasional dalam keamanan siber dan ekonomi digital, serta berkolaborasi untuk meningkatkan keamanan infrastruktur nasional yang penting.[2]

Pada tahun 2021, Menteri Luar Negeri Inggris Liz Truss bertemu dengan pejabat Indonesia untuk membahas hubungan keamanan siber dan ekonomi yang lebih erat, dan kedua negara menyepakati peta jalan untuk kerja sama yang lebih erat, yang mencakup fokus pada keamanan siber, standar teknologi 5G dan 6G, kecerdasan buatan, dan kuantum.[3] Inggris dan Indonesia juga menjajaki kemungkinan untuk memperbarui Nota Kesepahaman Kerja Sama Keamanan Siber. Inggris dengan bangga mendukung

---

[1] "UK-Indonesia Partnership Roadmap 2022 to 2024." GOV.UK, www.gov.uk/government/publications/uk- indonesia-partnership-roadmap-2022-to-2024/uk-indonesia-partnership-roadmap-2022-to-2024. Accesed 2 Feb 2024

[2] Post, The Jakarta. "UK Must Build New Long-Term Partnerships with Countries That Will Shape the Future." The Jakarta Post, Owen Jenkins, 17 Dec. 2022, www.thejakartapost.com/opinion/2022/12/17/uk-must-build- new-long-term-partnerships-with-countries-that-will-shape-the-future.html. Accessed 2 Feb 2024.

[3] NDEPENDENT. "Indonesia, UK Discuss Future Technology and Cybersecurity." The Independent, 11 Nov.
2021, www.independent.co.uk/news/liz-truss-indonesia-jakarta-european-union-southeast-asia-b1955720.html.
Accessed 2 Feb 2024.

program-program Indonesia untuk mendorong industri digital yang inklusif, keamanan siber, dan pengembangan kapasitas.[4] Kemitraan Inggris-Indonesia didasarkan pada saling menguntungkan dan keyakinan bersama dalam perdagangan bebas dan kedaulatan wilayah.

Kerja sama Indonesia dan Inggris dalam mengatasi kejahatan siber penting untuk dilakukan untuk melindungi kepentingan nasional kedua negara. Kejahatan siber merupakan ancaman yang semakin serius bagi kedua negara. Kerjasama kedua negara ini meliputi salah satu contohnya yaitu *Cyber Dialogue* dimana, Inggris dan Indonesia mengadakan Dialog Dunia Maya untuk membahas isu-isu keamanan siber, bertukar pandangan dan praktik terbaik, serta mencari peluang untuk berkolaborasi.

Kerjasama kedua negara ini juga memberikan manfaat seperti Inggris dan Indonesia dapat berbagi pengetahuan dan keahlian dalam keamanan siber, ekonomi digital, dan kontra terorisme untuk meningkatkan kemampuan mereka dalam memerangi kejahatan siber,[5] lalu Inggris dan Indonesia dapat berkolaborasi untuk meningkatkan keamanan infrastruktur nasional yang penting, termasuk melalui hubungan yang lebih kuat yang membentuk teknologi digital yang akan menentukan masa depan dunia online,[6] disamping itu Inggris dan Indonesia dapat bekerja sama untuk memperkuat kerja sama internasional di bidang keamanan siber, yang dapat membantu meningkatkan arsitektur keamanan siber.[7] Inggris

[4] CBE, Natalie Black. "Natalie Black CBE on LinkedIn: Building Future UK-Indonesia Digital Trade."
Www.linkedin.com, 18 Aug. 2022, www.linkedin.com/posts/natalie-black-cbe_building-future-uk-indonesia-
digital-trade-activity-6965952046168494080-JaMR. Accessed 2 February 2024.
[5] UK GOVERNMENT. "Foreign Secretary Visits Indonesia to Build Partnership for the Future." GOV.UK, 11
Nov. 2021, www.gov.uk/government/news/foreign-secretary-visits-indonesia-to-build-partnership-for-the-
[6] Ibid.
[7] Terry, Michael. OPPORTUNITIES to ENHANCE INDONESIAN CYBER SECURITY through THEATER

dan Indonesia juga dapat bekerja sama untuk memperkuat kerja sama politik, keamanan, dan pertahanan mereka, yang dapat membantu melindungi rakyat mereka dari ancaman yang inovatif dan berfokus pada masa depan.[8] Dengan bekerja sama, harapannya Inggris dan Indonesia dapat memanfaatkan kekuatan dan keahlian mereka untuk mengatasi kejahatan siber dan tantangan bersama lainnya, yang pada akhirnya meningkatkan postur keamanan siber serta melindungi masyarakat dan kepentingan mereka.

2. PEMBAHASAN

Pertahanan negara menurut Undang-Undang Nomor 3 Tahun 2002 Tentang Pertahanan Negara adalah segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara.[9]

Adanya kepentingan pertahanan negara didasarkan atas perkembangan lingkungan strategis yang mendorong kompleksitas ancaman terhadap pertahanan dan kedaulatan negara, sehingga negara merumuskan strategi pertahanan sebagai upaya dalam melindungi keselamatan negaran dari ancaman, dimana upaya dalam mewujudkan pertahanan negara erat kaitannya dengan sumber daya strategis pertahanan yang terdiri atas anggaran pertahanan infrastruktur militer, postur pertahanan, industri pertahanan, serta kemampuan logistik pertahanan. Nuechterlein menyebutkan bahwa kepentingan pertahanan dan keamanan adalah suatu kepentingan negara dalam memberikan perlindungan pada masyarakat dari ancaman yang berasal dari luar (eksternal)

SECURITY COOPERATION. 26 Oct. 2018, https://apps.dtic.mil/sti/pdfs/AD1077881.pdf. Accessed 2
February 2023.

[8] Ibid.

[9] Undang-Undang Republik Indonesia Nomor 3 Tahun 2002 Tentang Pertahanan Negara

maupun dari dalam (internal).[10]

Maka dari itu, berdasarkan uraian data-data yang diperoleh, peneliti menarik dua kepentingan pertahanan dan keamanan Inggris dalam isi Kerjasama MoU di bidang siber bersama Indonesia, diantaranya manajemen insiden dan pengembangan kapasitas.

2.1 MANAJEMEN INSIDEN

Manajemen insiden merupakan salah satu poin utama yang tercantum dalam MoU kerjasama Indonesia-Inggris dalam bidang keamanan siber. Selain itu, manajemen insiden merupakan strategi penting yang dilakukan kedua negara untuk menanggulangi ancaman siber dan menjadi salah satu faktor pendorong peningkatan keamanan siber di dalam negeri. Strategi ini melibatkan berbagai langkah konkret yang bertujuan untuk memastikan respons cepat dan efektif terhadap insiden siber.

Salah satu langkah dalam strategi manajemen insiden adalah optimalisasi keamanan siber melalui evaluasi upaya manajemen insiden siber yang pernah dilakukan. Evaluasi ini melibatkan peninjauan terhadap insiden-insiden siber sebelumnya, mengidentifikasi kelemahan dan kekuatan dari respons yang telah diberikan, serta membuat perbaikan yang diperlukan untuk meningkatkan kesiapan di masa depan. Melalui proses ini, Indonesia dapat belajar dari pengalaman sebelumnya dan mengimplementasikan langkah-langkah yang lebih baik dalam menanggulangi ancaman siber.

Selain itu, optimalisasi keamanan siber juga dilakukan melalui pertukaran informasi dan rekomendasi dari negara atau tenaga ahli yang memiliki pengetahuan dan kapabilitas dalam bidang siber. Pertukaran ini mencakup berbagi praktik terbaik, teknologi, dan metodologi terbaru yang dapat membantu dalam mengidentifikasi, mencegah, dan merespons insiden siber. Dengan

[10] Donald E. Nuechterlein, "National Interest and Foreign Policy: A Conceptual Framework for Analysis and Decision-Making". British Journal of International Studies. Vol. 2. No. 3, Oktober

memanfaatkan pengetahuan dan pengalaman dari ahli-ahli internasional, Indonesia dapat memperkuat sistem keamanannya dan meningkatkan efektivitas manajemen insiden.

Kerjasama ini juga mencakup pelatihan dan pengembangan kapasitas untuk personel keamanan siber di Indonesia. Pelatihan ini tidak hanya meningkatkan keterampilan teknis tetapi juga mempersiapkan personel untuk menghadapi berbagai jenis ancaman siber. Dengan adanya pelatihan berkelanjutan, Indonesia dapat memastikan bahwa tenaga kerja di bidang keamanan siber selalu siap dan mampu merespons insiden dengan cepat dan efisien.

Implementasi dari strategi manajemen insiden yang tercantum dalam MoU kerjasama Indonesia-Inggris ini diharapkan dapat memberikan kontribusi yang signifikan dalam meningkatkan keamanan siber di Indonesia. Dengan adanya kolaborasi erat antara kedua negara, Indonesia dapat terus meningkatkan kapabilitasnya dalam menanggulangi ancaman siber, melindungi infrastruktur kritis, dan memastikan keamanan data di dunia digital yang semakin kompleks. Hal ini juga menunjukkan komitmen Indonesia dan Inggris dalam membangun lingkungan siber yang lebih aman dan stabil, yang pada akhirnya akan mendukung pertumbuhan ekonomi dan kesejahteraan sosial kedua negara.

Gambar 4.1

Global Overview Report.[11]

[11] Data Reportal,"Global Overview Report" https://datareportal.com/reports/digital-2021-global-overview-report

Sumber; Data Reportal,"Global Overview Report"

Manajemen insiden tentunya sangat diperlukan negara khususnya hal tersebut didasar kan atas besarnya ancaman siber terhadap negara yang berbanding lurus dengan penggunaan siber yang semakin meningkat di setiap tahunnya. Berdasarkan riset Data Reportal, jumlah pengguna internet global mencapai 4,66 miliar atau 66,6% populasi global. Secara tahun ke tahun, tecatat peningkatan pengguna sejumlah 4,20% dibandingkan periode tahun sebelumnya Peningkatan signifikansi platform- platform digital juga memunculkan risiko serangan siber, Riset WEF Global Risks Report menunjukkan bahwa dalam 5 tahun terakhir, risiko keamanan siber (baik secara intensitas dampak maupun kemungkinan terjadi) relatif lebih tinggi dibandingkan bencana lain.

Di Inggris, upaya untuk mewujudkan keamanan siber di dalam negeri dilakukan dengan mengadopsi strategi yang komprehensif. Salah satu pendekatan utama yang diterapkan adalah peningkatan kapabilitas dalam bidang keamanan siber melalui manajemen insiden. Manajemen insiden ini merupakan bagian integral dari strategi keamanan siber nasional yang disusun untuk periode 2016-2021 dan telah secara resmi dilegalkan oleh pemerintah

Inggris.[12] Melalui strategi ini, Inggris berkomitmen untuk mengidentifikasi, merespons, dan memitigasi ancaman siber secara efektif guna melindungi infrastruktur kritis dan data sensitif dari berbagai ancaman digital. Implementasi dari manajemen insiden keamanan siber yang dilakukan oleh negara Inggris, diantaranya;[13]

1. Bekerjasama dengan antar instansi dalam negara, khususnya instansi yang paling dikaitkan dalam manajemen insiden dan mewujudkan keamanan siber dalam negaranya adalah CSC, Kementerian Dalam Negeri, Kepolisian, Otoritas Pencegahan Penipuan Nasional, Badan Investasi dan Perdagangan Inggris, Departemen Bisnis, Inovasi dan Keahlian, Badan Strategi Teknologi, Sekretariat Kabinet, Agen Keamanan dan Intelijen, Kementerian Pertahanan, Departemen Kebudayan,Media dan Olahraga, dan Kantor Persemakmuran dan Luar Negeri. Dimana tiap-tiap instansi ini, saling berhubungan dalam menanggulangi serangan dan ancaman siber melalui terbukanya jalur komunikasi dan informasi yang baik.
2. Selain bekerja sama dengan beberapa instansi dalam negara, upaya yang dilakukan negara Inggris dalam bidang manajemen insiden, seringkali negara melakukan evaluasi terhadap serangan, yang diantaranya dilakukan dengan cara klasifikasi dari jenis serangan dan ancaman, aktor yang melakukan serangan, serta klasifikasi mendalam mengenai tujuan dari seranganya.
3. Upaya penanggulangan serangan siber dalam negara, dilakukan secara cepat dan tanggap melalui pemanfatan media dan alat deteksi yang tinggi, serta dilakukan oleh tenaga terlatih yang Memahami dengan baik amalan siber dalam negara dan cara menanggulangi ancamannya. Hal tersebut tentunya sebagai langkah optimalisasi negara dalam

[12] HM Government "National Cyber Security Strategy 2016-2021" (UK : Gov.UK,2016)
[13] Rachma Fitriati,"Membangun Model Kebijakan Nasional Keamanan Siber dalam Sistem Pertahanan Negara"
Juni 2018, Jakarta : Universitas Pertahanan Indonesia, hlm 13-14

menjaga dan melindungi kualitas dan keamanan sehingga di dalam negaranya. Dari pelaksanaan yang telah dilakukan oleh negara Inggris tersebut melalui adanya kerjasama indonesia- inggris dalam bidang keamanan siber negara Indonesia kemudian melakukan langkah-langkah yang sama seperti halnya upaya pencegahan Serangan yang dilakukan oleh para pelaku kejahatan siber melalui adanya kerjasama antara instansi pemerintah khususnya Kementerian Pertahanan Republik Indonesia, Kementerian Luar Negeri Republik Indonesia badan saya badan Sandi Negara Badan Intelijen Negara kominfo serta bekerja sama dengan akademisi baik tingkat universitas negeri maupun swasta yang mempelajari secara khusus mengenai IT.

Penerapan Program Computer Security Incident Response Team (CSIRT) Oleh BSSN. Implementasi dari kerjasama Indonesia – Inggris dalam bidang keamanan siber tahun 2018-2022 adalah dimana pemerintah melakukan peningkatan keamanan siber di dalam negaranya, salah satunya yaitu dengan memaksimalisasi peran BSSN melalui program computer Security Incident Response Team (CRIST). CRIST sendiri merupakan sekelompok anggota organisaasi atau suatu tim yang terdiri dari orang – orang yang bertanggung jawab untuk menangani respon terhadap suatu insiden biasanya merupakan gabungan dari anggota staf yang mempunyai kemmapuan dalam bidang IT atau memahami mengenai keamanan siber.[14]

Pada perkembangannya pada tahun 2018, negara Indonesia masih belum menerapkan program CSIRT dalam negaranya. Hal tersebut dikarenakan oleh bberapa factor yang mempengaruhi salah satunya adalah masih barunya Lembaga BSSN yang dimana pada sturukturnya belum terbentuk. Sedangkan di negara Inggris, pemerintah Ingris telah membentuk CSIRT sebagai salah satu

[14] UK Government "Build A cyber security insiden response team (CSIRT) https://www.ncsc.gov.uk/collection/incident-management/creating-incident-response-team

bentuk maksimalisasi peran pemrintah dalam melindungi dan menciptakan keamanan siber.

Pembentukan dan upaya mengelola titik kontak mengenai manajemen insisden nasional dan mengidentifikasi mekanisme komunikasi yang dilakukan negara , merupan bentuk kerjasama dari Mou nota kepahaman kerjasama antara Indonesia – Inggris dalam bidang kemanan siber. Dalam hal ini, langkah yang dilakukan negara untuk mewujudkan jeamanan siber dalam negaranya, anatra laindibuktikannya dengan adanya terhubungnya antar instansi untuk menanggulangi anacaman yang dapat mengggangu keamanan siber, dengan dibentuknya program-program baru diharpakan mampu terwujudkan komunkasi yang bauk dalam menjaga keamanan siber yang sringkali menggangu dan mengancam setiap instansi di dalam negara. Program yang diimplimentasikan secara langsung sebagai wujud dari kerjasama bidang keamanan siber Indonesia- Inggris , lebih spesifiknya adalah sebagai berikut :

2.1.1 Mengkoordinasikan Dalam Menghadapi Insiden Keamanan Siber Kedua Negara

Salah satu wujud implementası dari kerjasama Indonesia-Inggris dalam bidang keamanan siber (manajemen insiden) tahun 2018-2022 adalah upaya yang dilakukan kedua negara melalun penyebaran informasidan komunikasi dengan cara mengkonsultasikan dan mengkoordinasikan secara langsung dalam menghadapi insiden keamanan siber kedua negara. Seperti yang telah dijelaskan pada BAB II dan BAB III mengenai dinamika keamanan siber kedua negara, dapat dilihat bahwa negara Indonesia dan Inggris memiliki ancaman yang sama, dimana ancaman ini terbentuk atas adanya serangan yang dilakukan oleh aktor individu, kelompok atau bahkan negara, terutama serangan saber yang paling mengancam yang dilakukan oleh aktor negara adalah seperti yang dilakukan negara Rusia, dimana kejahatan siber yang dilakukan negara Rusia tersebut seringkali melakukan

aksi-aksi spionase dan penyadapan informasi penting milik negara baik negara Indonesia maupun Inggris.

Tentunya dalam hal ini upaya yang dilakukan pemerintah untuk menekan dan mengantisipasi serangan siber terhadap negara, dapat diwujudkan melalui adanya pertukaran informasi dengan mengkonsultasikan dan mengkoordinasikan dalam menghadaps insiden keamanan saber kodua negara. Hal tersebut tentunya diharapkan dapat mewujudkan kedaulatan dan stabilitas dalam negara. Tentunya dalam hal ini, negara Indonesia mendapatkan keuntungan lebih, dimana keuntungan ini terletak pada :

1. Informasi yang diberikan negara Inggris, dapat mendorong keamanan siber di dalam negara Indonesia.
2. Banyaknya langkah-langkah strategis yang didapatkan Indonesia, khususnya dalam menanggulangi masalah yang mengancam keamanan siber negara.
3. Selain mewujudkan keamanan siber di dalam negara, tetapi juga mendorong kemajuan pada sistem perbankan, pertahanan siber negara yang aman,serta terwujudnya ejonomi digital negara.

2.2 PENGEMBANGAN KAPASITAS

Salah satu bentuk strategi dan fokus pelaksanaan kegiatan kerjasama yang dilakukan oleh pemerintah Indonesia-Inggris dalam bidang keamanan siber adalah mengenai pengembangan kapasitas Dimana hal ini sesuai dengan teori neorealis mengenai hubungan kerjasama intemasional yang terbentuk antara negara satu dengan negara lain didasarkan atas adanya anarki pada sistem interasional yang akhirya mendorong kerjasama tersebut untuk dilakukan, Selain itu, meninjau pada korelasi yang lebih signifikan mengenai pengembangan kapasitas negara, hal ini merupakan perwujudan lain dari adanya relative gain. Dimana dalam hal ini, negara Indonesia mendapatkan keuntun gan ebih dari adanya kerjasama siber dengan negara Inggris. Terstrukturnya dengan baik khususnya dalam proteksi dan wuijud keamanan

siber yang ditunjukan dari besarnya potensi dan kapabilitas sumber daya manusia dan teknologi di dalam negara, hal tersebut tentunya membuktikan bahwa negara Inggris memiliki kemampuan yang sangat baik dalam menjaga keamanan siber dalam negaranya.

Sementara itu, negara Indonesia pada aspek pertahanan siber di dalam negaranya, baik dalam persiapannya, sumber daya manusianya dan teknologinya masih jauh dari negara-negara lain khususnya jika dibandingkan dengan negara-negara yang ada di Asia Tenggara itu sendiri. Sehingga dalam hal ini upaya yang dilakukan dalam meningkatkan kapasitas keamanan siber dalam negara, negara Indonesia menekankan pada hasil implementasi kerjasama Indonesia-Inggris dalam bidang keamanan siber. Wujud nyata dari implementasi kerjasama Indonesia - Inggris dalam bidang siber tahun 2018-2022 diantaranya:

2.2.1 Pratical Exchange Dalam Antisipasi dan Keamanan Siber

Dalam mewujudkan keamanan siber di dalam negara, upaya yang dilakukan negara melalui kerjasama bidang keamanan siber yaitu melalui practical exchange. Dalam kerjasama keamanan siber Indonesia membawa kepentingan nasionalnya dengan cara mengembangkan program pelatihan untuk pengembangan kapasitas keamanan siber nya melalui pertukaran informasi dan tenaga terlatih dalam bidang siber. Hal tersebut berdasarkan masih kurangnya SDM Indonesia mengenai pentingnya keamanan siber, sehingga diperlukan pembinaan yang dilakukan melalui langkah-langkah yang dilakukan, guna mencegah tindak kejahatan siber dalam negara. Program pelatihan yang dilakukan diantaranya dapat dilakukan melalui koordinasi Tim Kerja Pusat Operasi Dunia Maya (Cyber Defence OperationCentre).[15]

Selain itu, wujud nyata dari implementasi kerjasama Indonesia-Inggris dalam bidang siber khususnya dalam bidang

[15] Handini Ardiyanti,"Cyber-Security Dan Tantangan Pengembangannya Di Indonesia", Politica Vol. 5 No. 1

practical exchange dalam antisipasi dan keamanan siber yaitu dengan ditandai adanya pembentukan CSIRT yang telah dijelaskan sebelumnya pada sub-bab manajemen insiden. Dimana pembentukan CSIRT yang dilakukan oleh instansi pemerintahan di setiap wilayah Indonesia ini, dibantu langsung oleh NCSC dengan melakukan pengembangan terhadap SDM di Indonesia yang juga menjadi salah satu prioritas BSSN. Hal tersebut dikarenakan pengembangan teknologi yang semakin meningkat sehingga diperlukan suatu perluasan terhadap SDM untuk dapat memahami perkembangan teknologi tersebut.[16]

Bekerjasama untuk Menfasilitasi Hubungan Kerja Antar Institusi Indonesia dan Inggris Dalam Bidang Keamanan Siber.

Dalam mewujudkan keamanan dan pertahanan siber negara, atau langkah atau upaya selanjutnya yang dilakukan oleh negara Indonesia-Inggris adalah dengan cara bekerjasama untuk memfasilitasi hubungan kerja antar institusi Indonesia dan Inggris dalam bidang keamanan siber. Hal ini tentunya dilakukan sebagai optimalisasi dalam mewujudkan keamanan siber kedua negara, yang khususnya dalam penelitian ini adalah mewujudkan keamanan siber negara Indonesin Wujud atau implementasi dari kerjasama Indonesia-Inggris tahun 2018-2021 ini adalah dengan cara bekerjasama secara langsung anatara BSSN dan NCSC.

Dalam kerjasama Indonesia-Inggris bidang keamanan siber ini, lembaga yang menjadi ujung tombak dari pelaksanan dan implementasi kerjasama siber tersebut adalah Badan Sandi dan Siber Negara (BSSN) dan The National Cyber Security Center NCSC), yang dimana dalam pelaksanaannya terbagi atas dua program, yaitu program teknis (Program Pengembangan iber dan Sandi Negara) dan program generik (Program Dukungan Manajemen dan pelaksanaan Tugas Teknis BSSN Lainnya), upaya yang dilakukan oleh kedua instansi tersebut adalah diantaranya

[16] Rizky Pratama, "Kerjasama Indonesia-Inggris Dalam Mengatasi Kejahatan Siber Di Indonesia Tahun 2018-2020." Fisip Universitas Mulawarman. Vol, 8 No.4 (2021).hlm 652

dengan dilakukannya :

1. Penguatan Kebijakan dan Hukum

NCSC Inggris memberikan dukungan yang signifikan dalam memperkuat kerangka hukum dan kebijakan BSSN. Kerjasama ini dimulai dengan diskusi strategi yang mendalam, bertujuan untuk melakukan analisis bersama mengenai kebutuhan regulasi yang diperlukan.

- Analisis Kebutuhan Regulasi : NCSC membantu BSSN dalam mengidentifikasi celah hukum yang perlu diisi untuk menunjang kewenangan BSSN. Diskusi ini mencakup pembahasan mengenai perlindungan infrastruktur kritis, respons terhadap insiden siber, dan regulasi terkait pengelolaan data pribadi serta keamanan informasi.
- Penyusunan Regulasi yang Efektif: Hasil dari analisis ini kemudian diimplementasikan dalam bentuk penyusunan regulasi baru atau revisi regulasi yang ada, untuk memastikan bahwa BSSN memiliki landasan hukum yang kuat dalam menjalankan tugasnya. Dukungan NCSC mencakup penyediaan contoh regulasi dari Inggris yang dapat diadaptasi sesuai dengan konteks Indonesia.
- Tindak Lanjut Hasil Analisis : Setelah analisis dan penyusunan regulasi, NCSC juga membantu BSSN dalam proses implementasi dan penegakan regulasi tersebut. Langkah-langkah ini memastikan bahwa kebijakan yang telah disusun dapat diterapkan secara efektif di lapangan.

2. Pengembangan Roadmap dan Pedoman Keamanan Siber

Sebagai bagian dari upaya mendukung pelaksanaan tugas BSSN, NCSC bekerja sama dalam penyusunan roadmap dan pedoman atau standar yang komprehensif.

- Diskusi dan Identifikasi Masalah : Diskusi awal yang dilakukan pada konferensi Cyber Security tahun 2019 di Jakarta Convention Center (JCC) menjadi fondasi untuk memahami kondisi keamanan siber di Indonesia. Dari diskusi

ini, isu-isu utama dan prioritas strategis diidentifikasi.

- Penyusunan Roadmap : Berdasarkan diskusi tersebut, NCSC membantu BSSN dalam merancang roadmap yang memberikan arahan strategis untuk jangka panjang. Roadmap ini mencakup langkah-langkah prioritas dalam penguatan infrastruktur, regulasi, dan respon terhadap ancaman siber.
- Pedoman atau Standar : Bersamaan dengan roadmap, NCSC juga mendukung penyusunan pedoman atau standar operasional yang berfungsi sebagai referensi bagi seluruh unit kerja di BSSN dalam menjalankan tugas mereka. Pedoman ini dirancang agar sesuai dengan standar internasional, namun disesuaikan dengan konteks lokal Indonesia.

3. Pengembangan Sarana, Prasarana, dan Teknologi

Dalam menghadapi ancaman siber yang terus berkembang, penguatan sarana, prasarana, dan teknologi menjadi sangat penting. NCSC memberikan dukungan strategis dalam hal ini melalui perencanaan pengadaan dan pengembangan teknologi.

- Strategi Pengadaan Teknologi : Bersama BSSN, NCSC merancang strategi pengadaan yang fokus pada pemeliharaan dan pengembangan teknologi yang esensial untuk keamanan siber dan sandi nasional. Strategi ini mencakup pengadaan perangkat lunak dan perangkat keras yang mutakhir serta peningkatan infrastruktur pendukung.
- Transfer of Technology (ToT): Salah satu komponen penting dari kerjasama ini adalah perencanaan untuk transfer teknologi (ToT), yang bertujuan untuk memastikan bahwa Indonesia memiliki akses ke teknologi terkini dan kemampuan untuk mengoperasikan serta memelihara sistem keamanan yang canggih. ToT ini dirancang untuk memperkuat sistem pertahanan siber di Indonesia, dengan fokus pada teknologi enkripsi, deteksi ancaman, dan respon insiden.

4. Pengembangan Sumber Daya Manusia (SDM)

Keberhasilan strategi keamanan siber tidak hanya bergantung pada teknologi, tetapi juga pada kualitas SDM yang kompeten. Oleh karena itu, pengembangan SDM menjadi salah satu fokus utama dalam kerjasama antara BSSN dan NCSC.

- Program Pendidikan dan Pelatihan: NCSC mendukung BSSN dalam menyusun program pendidikan dan pelatihan yang bertujuan untuk meningkatkan kompetensi SDM di bidang keamanan siber. Program ini mencakup pelatihan teknis, manajerial, serta pemahaman mengenai kebijakan dan regulasi keamanan siber.
- Pelatihan oleh Yayasan Infra Digital : Sebagai bagian dari inisiatif ini, pada tahun 2020, pemerintah Inggris melalui Yayasan Infra Digital memberikan pelatihan kepada SDM terkait di Indonesia. Pelatihan ini difokuskan pada penguatan keterampilan teknis dan strategi, dengan tujuan untuk meningkatkan kemampuan deteksi, mitigasi, dan manajemen insiden siber.

Kolaborasi antara BSSN dan NCSC Inggris menunjukkan komitmen kedua negara dalam memperkuat keamanan siber melalui pendekatan yang menyeluruh dan terkoordinasi. Mulai dari penguatan regulasi, pengembangan roadmap strategis, pengadaan teknologi canggih, hingga pengembangan SDM, semua upaya ini dirancang untuk memastikan bahwa Indonesia siap menghadapi tantangan keamanan siber di masa depan. Dukungan dari NCSC Inggris memainkan peran kunci dalam memastikan bahwa BSSN memiliki landasan yang kuat, baik dalam hal kebijakan, infrastruktur, maupun SDM, untuk menjaga keamanan digital nasional.

2.3 Kepentingan Ekonomi

Kepentingan ekonomi merupakan komponen penting dalam teori kepentingan nasional yang dikemukakan oleh Donald E. Nuechterlein. Dalam konteks kerja sama siber antara Indonesia dan Inggris, aspek ini menjadi sangat relevan mengingat peran krusial ekonomi digital di kedua negara. Kolaborasi ini tidak hanya

bertujuan untuk memperkuat pertahanan siber, tetapi juga berfungsi sebagai langkah strategis untuk melindungi ekonomi digital dari berbagai ancaman yang dapat berdampak signifikan. Dengan meningkatnya ketergantungan pada teknologi informasi dan komunikasi (TIK), keamanan siber menjadi prioritas utama dalam menjaga stabilitas dan kelangsungan kegiatan ekonomi.

Melalui penguatan keamanan siber, kerja sama antara Indonesia dan Inggris secara langsung berkontribusi pada upaya mitigasi risiko yang dapat merugikan sektor ekonomi. Ancaman seperti pencurian data, serangan *ransomware*, dan sabotase terhadap infrastruktur keuangan merupakan ancaman yang nyata dan terus berkembang di era digital saat ini. Menurut laporan oleh Symantec, serangan ransomware global meningkat sebesar 36% pada tahun 2021, menunjukkan betapa seriusnya ancaman ini terhadap ekonomi global . Dengan adanya kerja sama ini, Indonesia dan Inggris dapat berbagi pengetahuan dan teknologi untuk memperkuat pertahanan mereka terhadap ancaman ini, sehingga meminimalkan dampak ekonomi yang dapat ditimbulkan oleh serangan siber.

Selain itu, kemitraan ini juga membuka peluang investasi dan transfer teknologi yang dapat mendorong pertumbuhan ekonomi di sektor TIK. Indonesia, sebagai salah satu pasar digital terbesar di Asia Tenggara, memiliki potensi besar untuk menarik investasi di bidang teknologi. Dengan dukungan teknologi dan keahlian dari Inggris, Indonesia dapat memperkuat ekosistem digitalnya, meningkatkan kapasitas lokal dalam pengembangan teknologi siber, dan mendorong inovasi. Ini tidak hanya akan meningkatkan daya saing Indonesia di kancah global, tetapi juga menciptakan lapangan kerja baru dan memperkuat perekonomian nasional. Menurut McKinsey, potensi ekonomi digital Indonesia bisa mencapai USD 150 miliar pada tahun 2025, menunjukkan betapa pentingnya keamanan siber dalam mewujudkan potensi ini.

Dengan demikian, kerjasama siber antara Indonesia dan

Inggris tidak hanya melindungi infrastruktur ekonomi yang ada, tetapi juga memajukan perkembangan ekonomi digital melalui investasi, transfer teknologi, dan peningkatan kapasitas lokal. Ini sejalan dengan kepentingan ekonomi nasional yang ditekankan oleh Nuechterlein, di mana kebijakan luar negeri dan kerja sama internasional harus mendukung pertumbuhan ekonomi yang berkelanjutan dan menguntungkan bagi negara.

3. KESIMPULAN

Serta adanya pengembangan kapasitas yang diantaranya ditandai dengan adanya *praktikal exchange* dalam antisipasi dan keamanan siber, kerjasama ini juga memfasilitasi hubungan antara institusi Indonesia dan Inggris dalam bidang keamanan siber. *Praktikal exchange* ini melibatkan

berbagai pelatihan dan pertukaran keahlian antara ahli keamanan siber dari kedua negara, yang membantu meningkatkan kemampuan teknis dan operasional dalam menghadapi ancaman siber. Hasil dari implementasi ini telah menunjukkan bahwa Indonesia berhasil meningkatkan keamanan sibernya, yang tercermin dalam peningkatan peringkat Indonesia menjadi negara ke-24 dengan keamanan siber terbaik di dunia menurut penilaian Global Cyber-security Index (GCI). Peningkatan ini tidak hanya mencerminkan keberhasilan kebijakan dan kerjasama yang dilakukan tetapi juga menegaskan posisi Indonesia sebagai salah satu negara yang serius dalam mengembangkan keamanan siber di tingkat global.

REFERENSI

A.A, Perwita. & Y.M, Yani. 2005. Pengantar Ilmu Hubungan Internasional.
Bandung: PT.Remaja Rosdakarya.

Donald E. Nuechterlein "*National Interests and Foreign Policy: A Conceptual Framework for Analysis and Decision-Making." British Journal of International Studies, vol. 2, no. 03.*

K.J Holsti, *International Politics A Framework for Analysis, Terjemahan Wawan Juanda (Bandung, 1992) hlm 650.*

Moleong, Lexy. (2010). *Metodologi Penelitian Kualitatif*. Bandung: PT Remaja Rosdakarya.

Roxana Radu, "*Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace," in Cyberspace and International Relations: Theory, Prospects and Challenges, vol. 9783642374814, 2014*

Sugiyono. (2012). *Metode Penelitian Bisnis*. Bandung : Alfabeta.

Thalhah Al Hamid dan budurAnufia, "Instrumen Pengumpulan Data", resume, Sekolah Tinggi Agama Islam Negeri (STAIN), 2019, 4

Artikel Jurnal

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

Handini Ardiyanti,"*Cyber-Security Dan Tantangan Pengembangannya Di Indonesia", Politica Vol. 5 No. 1*

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

Magrisa, D. (2020). Kerja Sama Badan Siber dan Sandi Negara (BSSN) Indonesia dengan Departement Of Foreign Affairs And Trade (DFAT) Australia Dalam Pengembangan Cyber Security. *JOM FISIP*, *7*(2), 1–11.

Rachma Fitriati,"Membangun Model Kebijakan Nasional Keamanan Siber dalam Sistem Pertahanan Negara" Juni 2018, Jakarta : Universitas Pertahanan Indonesia, hlm 13-14

Suryanti, B. T. (2021, February 22). Pendekatan Neorealis terhadap Studi Keamanan Nasional. Jurnal Diplomasi Pertahanan. https://doi.org/10.33172/jdp.v7i1.674.

Terry. (2018, October). *Opportunities To Enhance Indonesian Cyber Security Through Theater Security Cooperation. Faculty of the United States Naval War College Newport. Retrieved January 21, 2024, from https://apps.dtic.mil/sti/pdfs/AD1077881.pdf.*

Weu, M. R. (2020). Kerjasama Pemerintah Indonesia dan Pemerintah Kerajaan Inggris Dalam Bidang Keamanan Siber. *Global Political Studies Journal*, *4*(2), 154–169. https://doi.org/10.34010/gpsjournal.v4i2.5879.

Internet

Badan Siber dan Sandi Negara (BSSN), " BSSN Tandatangani Nota Kesepahaman Kerjasama di Bidang Keamanan Siber Dengan Pemerintah Inggris Raya", (14 Agustus 2018)

https://www.bssn.go.id/bssn-tandatangani-nota-kesepahaman- kerjasama-di-bidang-keamanan-siber-dengan-pemerintah-inggris- raya/

Bapenda Jabar, "Jenis Cybercrime Berdasarkan Motif dan Aktivitasnya", Bapenda Jabar (10 November 2017) https://bapenda.jabarprov.go.id/2017/11/10/jenis-cybercrime- berdasarkan-motif-dan-aktivitasnya/

Cbe, N. B. (2022, August 18). *Building Future UK-Indonesia Digital Trade. https://www.linkedin.com/pulse/building-future-uk-indonesia-digital- trade-natalie-black-cbe/*

CNN Indonesia, "225 juta serangan siber masuk indonesia sepanjang 2018", CNN Online(7Februari2019) https://www.cnnindonesia.com/teknologi/20190207210646185 36734 7/225-juta-serangan-siber-masuk-indonesia-sepanjang-2018

Foreign, C. D. O. (2021, November 11). *Foreign Secretary visits Indonesia to build partnership for the future. GOV.UK. https://www.gov.uk/government/news/foreign-secretary-visits- indonesia-to-build-partnership-for-the-future*

Indonesia, *UK discuss future technology and cybersecurity. (2021, November 11). The Independent. https://www.independent.co.uk/news/liz-truss- indonesia-jakarta-european-union-southeast-asia-b1955720.html*

Jenkins. (2022, December 17). *UK must build new long-term partnerships with countries that will shape the future. The Jakarta Post. Retrieved January 21, 2024, from https://www.thejakartapost.com/opinion/2022/12/17/uk-must-build- new-long-term-partnerships-with-countries-that-will-shape-the- future.html*

UK-Indonesia Partnership Roadmap 2022 to 2024. (2022, April 19). *GOV.UK. https://www.gov.uk/government/publications/uk-indonesia- partnership-roadmap-2022-to-2024/uk-indonesia-partnership-roadmap- 2022-to-2024*

UK Government "*Build A cyber security insiden response team (CSIRT) https://www.ncsc.gov.uk/collection/incident-management/creating- incident-response-team*

Yuswardi A. Suud "Ini Dia Negara dengan Keamanan Siber Terbaik Dunia" yber threat.id, 12 Maret 2020, https:/cyberthreat.id/read/5743/Ini- Dia-Negara-dengan-Keamanan-Siber-Terbaik-Dunia

Riva Dessthania Suastha, "Di Tengah Ancaman Rusia, Inggris Bentuk Pusat KeamananSiber"CNNIndonesia https://www.cnnindonesia.com/internasional/20 1702140947511341 93361/di-tengah-ancaman-rusia-inggris-bentuk-pusat-keamanan- siber