COOPERATION BETWEEN INDONESIA AND BRITAIN IN DEALING WITH THE THREAT OF CYBET CRIME IN 2018

Author : Andre Helvani Ginting
Advisor : Dr. Yessi Olivia, S.IP., M.Int.Rel
Bibliographies : 9 Books, 21 Journals, 75 Websites, 1 Thesis

Department of International Relations
Faculty of Socical Science and Political Science Riau University
Bina Widya Campus Jl. H.R. Soebrantas Km. 12,5 Simpang Baru, Pekanbaru 28293 Telp/Fax: 0761-63277

ABSTRACT

The focus of this research is on cybersecurity cooperation between Indonesia and the UK in 2018. Indonesia and the UK, which are geographically quite far apart but both face the threat of borderless cybercrime, decided to cooperate in cybersecurity. The UK, which is one of the top countries in the cybersecurity index, is willing to work with Indonesia to realize its interests in the post-Brexit Asia Pacific region. Indonesia, which is ranked in the middle of the cybersecurity quality index, views this cooperation as a stepping stone that can improve the quality of its cybersecurity. The purpose of this study is to provide an analysis of the implementation of the cooperation agreed by the two countries

The author collects data from various journals, official documents, theses, books and articles on the internet to analyze the implementation of cybersecurity cooperation between Indonesia and the UK. The research technique used is document study. This study uses the level of systems analysis and the theory of Dillemas of Common Aversion proposed by Stein

The realization of the cooperation, although not all have been implemented, has been carried out in accordance with three of the five points of the agreed contents of the MoU, namely the Implementation and Development of the National Cyber Security Strategy, Cyber Security Training and Campaign, and Capacity Building. Two points that have not been implemented are Cyber Crime and Cyber Incident Management. It is hoped that this cooperation can be carried out in accordance with the initial agreement, and it is hoped that this cooperation can be a reflection and the right moment for both countries to achieve their respective national interests.

Keywords : cyber security, cyber crime, cyber attacks

PENDAHULUAN

Penelitian ini akan menganalisis kerja sama antara dua negara dalam menyelesaikan permasalahan yang dihadapi bersama. Studi kasus yang diangkat adalah kerja sama antara Indonesia dengan Inggris dalam bidang keamanan siber yang ditandai dengan penandatanganan Memorandum of Understanding (MoU) pada tahun 2018 di Jakarta.

Kejahatan siber, yaitu segala sesuatu upaya tindakan kriminal di dunia maya. Ancaman dari kejatan siber bersifat nyata, sebagai contoh informasi-informasi rahasia yang dimiliki negara dapat diretas dan digunakan untuk melawan atau merugikan negara. Penipuan – penipuan yang terjadi secara online, sudah banyak terjadi dan memberikan kerugian materil maupun imateril kepada korban, seperti penipuan, phising (upaya memperoleh data pribadi untuk tujuan kejahatan), peretasan data perbankan baik milik bank itu sendiri maupun milik warga secara personal, peretasan data-data pribadi seperti nomor handphone, alamat email beserta kata sandi, lokasi terkini serta transaksi-transaki yang seharusnya menjadi urusan pribadi. dan lainnya yang dapat digunakan sebagai sarana penyalahgunaan.

Masyarakat yang tidak paham mengenai bahaya tercurinya data-data pribadi mereka mungkin tidak sadar akibatnya, padahal kenyataannya data-data yang tercuri tersebut dapat digunakan untuk kepentingan pribadi pelaku yang dapat merugikan korban, sebagai contoh, sudah banyak terjadi kasus penipuan melalui telepon genggam di mana pelaku akan menghubungi calon korban, dan mengaku sebagai kenalan maupun kerabat korban, yang pada akhirnya jika calon korban kurang waspada akan percaya, akhir dari kasus-kasus seperti ini kebanyakan selalu dengan pelaku yang meminta agar ditransfer uang dengan berbagai alasan untuk meyakinkan calon korban.

Bentuk dari penyalahgunaan data pribadi yang muncul belakangan ini adalah penyalahgunaan data pribadi oleh aplikasi kredit melalui Paylater (layanan pinjaman online). Salah satu contoh kasus dialami oleh Ahmad Fauzi Ridwan, juga dikenal sebagai Ridu. “Pengalamannya bermula ketika ia mencoba mengajukan permohonan kartu kredit dari bank pencatat perusahaan. Redu terkejut ketika aplikasinya ditolak karena KOL5 atau kredit macet. Redu mengatakan kepada BBC News Indonesia: “Saya terkejut tenggat waktu belum berlalu. Dia pun memeriksa riwayat kreditnya melalui layanan verifikasi BI yang diubah namanya di Sistem Layanan Informasi Keuangan (SLIK) saat ini dan menemukan bahwa kredit macet yang disebutkan terjadi kepada PT Catturnusa Sejahtera Finance Perusahaan ini merupakan mitra Traveloka Paylater.”[1]

Indonesia dan Inggris adalah negara-negara yang menghadapi kejahatan siber karena jumlah pengguna internet yang tinggi. Berdasarkan data yang dikeluarkan oleh *Statista* melaporkan bahwa penggunaan akses internet di Indonesia per tahun 2018 adalah sebanyak 95.2 juta, mengalami pertumbuhan sebesar 13.3% dari tahun 2017 yang sebanyak 84 juta pengguna. *Statista* memperkirakan pada periode 2018-2023 penggunaan

[1] BBC News Indonesia, “Pinjaman online: 'Bagaimana saya menjadi korban penyalahgunaan data pribadi'” diakses 17 Juni 2021 pukul 15.00 WIB https://www.bbc.com/indonesia/majalah-57046585

internet di Indonesia akan tumbuh sebesar 10,2% yang pada kesimpulannya dikatakan bahwa pada tahun 2023 mendatang penguna internet di Indonesia akan menyentuh angka 150 juta pengguna.[2]

Salah satu kejadian terkait keamanan siber yang terjadi adalah peretesan situs Tiket.com dan Citilink yang dilakukan oleh tiga orang yang berasal dari Tangerang. Akibat perbutan mereka yang masuk secara illegal kedalam sistem aplikasi Tiket.com dan melakukan manipulasi harga tiket yang dijual di aplikasi tersebut, mengakibatkan Tiket.com dan Citilink mengalami total kerugian sebesar enam miliar rupiah.[3]

Begitupula dengan negara Inggris, menurut data yang dirilis oleh Statista pada tahun 2018 pengguna internet di Inggris adalah sebanyak 90.69% dari jumlah warga negaranya.[4]

Alasan mengapa Indonesia – Inggris melakukan kerja sama adalah, dunia internasional bersifat anarki yang artinya tidak ada negara yang lebih tinggi kedudukannya dari negara lain. Kemudian masing-masing negara tentunya menginginkan kedaulatan serta keamanan negaranya agar terpelihara, terjaga serta meningkat. Salah satu cara untuk mencapai hal tersebut adalah dengan melakukan kerja sama yang seimbang dengan negara lain, sebelum kerja sama dengan Inggris ini dilakukan, sebenarnya Indonesia sudah lebih dahulu melakukan kerja sama keamanan siber dengan negara lain seperti Australia. Begitu juga dengan Inggris, mereka juga telah melakukan beberapa kerja sama keamanan siber dengan negara selain Indonesia. Alasan utama Indonesia – Inggris sepakat untuk bekerja sama kali ini adalah karena semakin banyak rekan kerja sama yang dimiliki tentunya berbagai aspek akan semakin meningkat fungsinya akibat dari pertukaran informasi serta teknologi masing-masing negara.

Sebelum kerja sama kemanan siber antara Indonesia – Inggris ini dilakukan, kedua negara juga telah bekerja sama dalam bidang lain, dan juga untuk meningkatkan kualitas hubungan diplomatik kedua negara maka Indonesia – Inggris pun sepakat melakukan kerja sama ini, karena tentunya keuntungan yang diperoleh sudah dipertimbangkan. Dari pihak negara Indonesia sendiri, kualitas Inggris sebagai salah satu negara Eropa bahkan dunia dengan kemampuan tekonologi terdepan tentu akan sangat memberikan keuntungan bagi Indonesia. Begitu juga Inggris pasti akan mendapatkan kegunaan dari kejas sama ini baik dalam segi informasi khusus maupun teknolog maupun penerapan yang dilakukan Indonesia selama ini.

Setelah kerja sama ini dilakukan, bukan berarti kedua negara tidak akan lagi melakukan kerja sama serupa dengan negara lain, karena seperti yang sudah penulis sebutkan tadi, semakin banyak rekan maka akan semakin baik serta banyak keuntungan khusus yang dapat diterima masing-masing

[2]Statista, "Number of internet users in Indonesia from 2015-2025", diakses pada 27 November 2020, https://www.statista.com/statistics/254456/number-of-internet-users-in-indonesia/.

[3] Kompas, Cerita Remaja 19 Tahun Peretas Situs Tiket.com dan Raup Hampir Satu Milliar, diakses 21 Desember 2021 https://nasional.kompas.com/read/2017/04/05/08135311/cerita.remaja.19.tahun.peretas.situs.tiket.com.dan.raup.hampir.rp.1.miliar?page=all

[4] STATISTA, UK internet penetration : percentage of population using the internet in the United Kingdom from 2000-2020, diakses 21 Desember 2021. https://statista.com/statistics/468663/uk-internet-penetration/

negara dari rekan kerja samanya kelak.

Kerja sama ini seperti yang tertulis di dalam MoU adalah melakukan pertukaran informasi – informasi yang berkaitan dengan keamanan siber, dari informasi tersebut nantinya akan diolah dan menjadi pertimbangan serta antisipasi mengenai tindakan yang kelak akan diambil terkait kemanan siber demi meminimalisasi potensi kerugian yang terjadi. Kemudian dariapada itu adanya kerja sama ini juga dapat menjadi pintu masuk bagi kerja sama lainnya antara Indonesia – Inggris kelak, khususnya dalam isu keamanan siber. Di samping itu akan dilakukan pertukaran *point of contact* masing-masing negara sebagai langkah awal perwujudan kerja sama ini

KERANGKA TEORI

Tingkat Analisis

Tingkat analisis beserta level analisa yang akan dipakai dalam penelitian ini adalah sistem internasional (*state-level analysis).* Menurut level analisis ini, interaksi antara satu negara dengan negara lain pada akhirnya akan membentuk suatu sistem internasional. Sistem internasional akan berbicara tentang pengaruh negara adidaya terhadap negara lain. Jadi, tingkat sistem internasional meliputi: bipolar, multipolar, unipolar dan sistem lainnya.[5]

Teori Dilemmas of Common Aversion

Teori yang digunakan penulis adalah buah pemikiran Arthur Stein tentang *dillekilasmas of common interest* dan *dilemmas of common aversion*.

Menurut Stein, yang dimaksud dengan *dilemmas of common interest* adalah, negara-negara melakukan kerja sama karena mereka memiliki kepentingan yang sama yang ingin mereka capai. Negara-negara yang melakukan kerjasama menyadari bahwa suatu tujuan tidak akan dapat mereka capai jika hanya dengan menggunakan kekuatan dan sumber daya sendiri.

Definisi Konsepsional

Pendefinisian konsep digunakan sebagai bantuan untuk memperjelas pemahaman akan pengertian yang akan diteliti

Kerjasama

Kerjasama adalah pengelompokan yang terjadi di antara makhluk makhluk hidup yang kita kenal. Kerja sama atau belajar bersama adalah proses beregu (berkelompok) di mana anggota-anggotanya mendukung dan saling mengandalkan untuk mencapai suatu hasil mufakat kerja sama internasional[6]

Keamanan Siber (cyber security)

Keamanan siber adalah suatu usaha untuk mengontrol serta melindungi sistem informasi dalam hal ini seperti penggunaan internet di komputer, ponsel serta perangkat lainnya yang dapat terhubung ke jaringan internet dari serangan pihak-pihak tak bertanggung jawab yang berniat jahat serta merugikan pengguna jaringan internet[7]

Kejahatan Siber (cyber crime)

Sebagai perbuatan melawan

[5] Mochtar Mas'oed, Ilmu Hubungan Internasional Internasional: Disiplin dan Meodologi, halaman 35-37

[17] Jonathan, "Pengertian Kerjasama : Memahami Arti, Manfaat, dan Bentuk Kerjasama, diakses 19 Maret 2020, https://www.maxmanroe.com/pengertian-kerjasama.html.

[18] "What is Cyber Security? Definition and Best Practices", It Governance, diakses 19 Maret 2020 https://www.itgovernance.co.uk/what-is-cybersecurity.

hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana / alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.[8]

Memorandum of Understanding (MoU)

Adalah sebuah nota yang ditandatangani sebagai awal dan tanda jadi dilakukannya kerja sama antara dua negara atau lebih[9]

Dilemmas of Common Aversion

Sebuah keadaan di mana dua atau lebih negara sama-sama memiliki ketakutan akan suatu hal yang dapat terjadi, yang mana dapat mengganggu keberlangsungan negara mereka, dalam hal ini negara-negara tadi pun memutuskan untuk bekerja sama untuk menghindari terjadinya hal yang ditakutkan tersebut[10].

Internet

Internet adalah sebuah teknologi system jaringan yang menghubungkan satu computer dengan computer lainnya dengan menggunakan standar system global Transmission Control Protocol atau Internet Protocol Suite (TCP/IP) sebagai protocol pertukaran, sehingga orang-orang yang menggunakan system ini dapat saling berkomunikasi, dan saling bertukar informasi walaupun berada dalam jarak yang sangat berjauhan sekalipun[11]

Point of Contact

Point of Contact adalah suatu langkah pertama di dalam kerja sama, di mana pihak-pihak yang bekerja sama akan memberikan orang, titik, lokasi maupun perwakilan yang akan menjadi penghubung kedua negara yang bekerja sama selama proses kerja sama berlangsung[12]

REALISASI KERJASAMA BILATERAL ANTARA INDONESIA DAN INGGRIS DALAM BIDANG KEAMANAN SIBER

Implementasi Kerja Sama

Indonesia dan Inggris bersepakat untuk memperkuat hubungan diplomatik melalui kerjasama keamanan pada bidang siber. Kerjasama bidang ini pada dasarnya merupakan kali pertama terjadi antara kedua negara. Baik Indonesia maupun Inggris, keduanya memiliki kepentingan nasionalnya masing-masing dari menjalin hubungan bilateral ini. Secara umum, mewujudkan keamanan nasional menjadi prioritas utama dari menjalin kerjasama siber dimana Indonesia menilai bahwa melalui kerjasama dengan Inggris, akan membantu mengembangkan sistem pertahanan siber Indoneisa.

---

[19] Dista Amalia Arifah, "Kasus CyberCrime di Indonesia", "Jurnal Bisnis dan Ekonomi (JBE)", vol. 18, no. 2, (2011), hlm.186, https://www.unisbank.ac.id/ojs/index.php/fe3/article/view/2099

[9] BPKP, Penyusunan Memorandum of Understanding (MoU), diakses 21 Desember 2021 http://www.bpkp.go.id/sesma/konten/320/penyusunan-memorandum-of-understanding-mou.bpkp

[10] Arthur Stein, " Coordination and Collaboration : Regimes in Anarchic World", International Organization, vol.36, no.2, International Regimes (Spring, 1982), hlm. 304 & 309. https://www.jstor.org/stable/2706524?seq=1

[21]"Pengertian Dan Perbedaan Dari Internet Dan Intranet," ID Cloud Host, diakses 20 Maret 2020 https://idcloudhost.com/pengertian-dan-perbedaan-dari-internet-dan-intranet/.

[12]" What does Point of Contact means?", "Definitions", diakses 17 Juni 2020 https://www.definitions.net/definition/Point+Of+Contact

Meresmikan kerjasama ini, pemerintah Indonesia yang diwakili oleh institusi Badan Siber dan Sandi Negara (BSSN) dan Inggris yang diwakili oleh Kementerian Luar Negeri menandatangani Nota Kesepahaman (*Memorandum of Understanding*) pada 14 Agustus 2018. Melalui MoU ini, maka kedua negara terikat untuk melaksanakan dialog keamanan siber yang harus dilakukan dalam kurun waktu 5 tahun—selama masa berlaku MoU. Dialog tersebut akan menjadi wadah dialektika atau bertukar pendapat antar institusi siber dan melakukan peninjauan kerjasama siber kedua negara.[13]

Pada pertemuan tersebut, Kepala BSSN dan Menteri Muda untuk Urusan Asia Pasifik menyepakati 5 poin bidang kerjasama siber yang meliputi implementasi dan pengembangan strategi keamanan siber nasional; pengelolaan insiden siber; kejahatan siber; pelatihan dan kampanye kesadaran siber; peningkatan kapasitas siber.[14] Selama berlasungnya kesepakatan yang mengikat kedua negara, terdapat sejumlah kegiatan yang mendukung poin kerjasama dalam MoU antara Indonesia dan Inggris, diantaranya adalah:

Seminar Pelatihan Keamanan Siber

Melalui kerjasama dengan NCSC Inggris, BSSN melakukan pelatihan teknis keamanan siber di Pusdiklat BSSN pada minggu pertama Oktober 2019. Pelatihan ini dipimpin langsung oleh Mayjen Suharyanto selaku Deputi V Bidang Pemantauan dan Pengendalian BSSN. Kegiatan ini dilakukan untuk meningkatkan kapabiltas SDM para peserta mengenai keamanan jaringan, pertahanan dan serangan siber, pengelolaan ancaman, kriptografi, manajemen resiko.[15]

Pada tahun yang sama, Inggris juga hadir membantu Indonesia dalam menyelenggarakan pameran keamanan siber dalam agenda "Cyber Security Indonesia 2019 (CSI)" yang berlangsung di Jakarta Convention Centre. Kegiatan ini menghadirkan sejumlah pejabat luar negeri termasuk duta besar Inggris untuk Indonesia. Pada acara tersebut, pemerintah Indonesia mengundang salah satu industri pertahanan terbesar Inggris sebagai panelis, yakni BAE Systems. Poin yang disampaikan adalah mengenai pengalaman Inggris menghadapi ancaman siber, kunci pokok dari strategi keamanan nasional siber dan implementasinya, serta manajemen resiko siber.[16]

Kolaborasi Peningkatan Akses Internet

Digital Access Programme. yang dikelola oleh Kedutaan Besar Inggris Jakarta bekerjasama dengan

[13] Kementerian Luar Negeri "Memorandum Saling Pengertian", 2018. Diakses 28 September 2021. https://treaty.kemlu.go.id

[14] "BSSN Tandatangani Nota Kesepahaman Kerjasama di Bidang Keamanan Siber dengan Pemeirntah Inggris Raya", Badan Siber dan Sandi Negara, Diakses 30 Agustus 2021. https://bssn.go.id/bssn-tandatangani-nota-kesepahaman-kerjasama-di-bidang-keamanan-siber-dengan-pemerintah-inggris-raya/

[15] (pusdiklat.bssn.go.id, 2019).

[16] BAE Systems, "Cyber Security Indonesia", BAE Systems. Diakses 5 Oktober 2021 https://www.baesystems.com/en/cybersecurity/event/cyber-security-indonesia

Common Room Network Foundation yang memperoleh pendanaan senilai Rp 3,5 miliar dalam jangka waktu dua tahun. Pemerintah Inggris juga mengindikasikan mendukung adanya pemberian literasi digital bagi masyarakat setempat demi pemahaman akan potensi baik buruk dunia siber.[17] Duta Besar Inggris untuk Indonesia juga menyebutkan bahwa program ini dilaksanakan sebagai bentuk upaya dan dukungan pemerintah Inggris dalam membantu masyarakat Indonesia memperoleh kemudahan akses kesehatan melalui teknologi komunikasi.

Program yang dijalankan oleh *Common Room Network Foundation* ini meliputi pembuatan konten-konten mengenai informasi pandemi Covid-19 menggunakan bahasa daerah sehingga dapat dipahami oleh masyarakat setempat. Konten tersebut diprduksi dalam bentuk digital dan konvensional sehingga penyeberan informasi dapat menyesuaikan kapasitas masyarakat tersebut. Melalui kolaobrasi tersebut, *Common Room Network Foundationi* telah menerbitkan *e-book* mengenai informasi pandemi yang dinarasikan ke dalam Bahasa Sunda.[18]

Cyber Practitioners Course

Peningkatan kapasitas SDM melalui webinar juga dilakukan oleh kedua negara dalam kerangka program Webinar dan Sertifikasi Keamanan Siber yang dilaksanakan secara daring pada 9 April 2021. Program ini disusun oleh perwakilan kedua negara, dimana Indonesia diwakili oleh BSSN dan Inggris diwakili oleh KPMG. Kedutaan Besar Inggris, melalui KPMG, menginisasi program tersebut dalam amanat kerjasama peningkatan kompetensi SDM keamanan siber terutama pada sektor IIKN (Infrastruktur Informasi Kritikal Nasional).[19] Sektor IIKN dinilai krusial untuk memperoleh pelatihan ini agar para pembuat kebijakan dapat merumuskan kebijakan keamanan yang efektif dan komprehensif.

Peserta IIKN yang mengikuti kegiatan ini berasal dari masing-masing perwakilan kementerian, kemudian dari BSSN sendiri, serta institusi non-kementerian lain seperti OJK, dan BI. Program tersebut diawali dengan launching kegiatan kursus bagi para peserta dari IIKN, kemudian dilanjutkan dengan kursus yang dilakukan secara daring selama 3 hari. Pelatihan yang diberikan adalah hal-hal seputar kebijakan keamanan siber internasional, webinar ISO series, kemudian program sertifikasi ISO 27001 *Lead Auditor*.[20]

***Sharing Experience* dalam Budaya Keamanan Siber**

Penandatanganan MoU Kerjasama keamanan siber antara Indonesia dan Inggris juga termasuk kolaborasi dengan industri siber yang dibawahi oleh wewenang NCSC. Kepala BSSN juga telah menggarisbawahi bahwa alasan kerjasama siber dengan Inggris didorong oleh faktor kemampuan dan kapasitas sistem pertahanan siber Inggris dalam kancah global.

[17] *ibid*
[18] *Ibid*

[19] BSSN, "BSSN Bekerja Sama dengan UK Embassy Jakarta Meluncurkan Program Webinar dan Sertifikasi Keamanan Siber", Diakses 4 Oktober 2021 https://bssn.go.id/bssn-bekerja-sama-dengan-uk-embassy-jakarta-meluncurkan-program-webinar-dan-sertifikasi-keamanan-siber/
[20] *Ibid*

Sehingga Indonesia membutuhkan kesediaan Inggris untuk berbagi pengalaman dalam mendukung normalisasi budaya keamanan siber terutama pada institusi swasta dan pemerintahan.[21]

Pada Juni 2021 lalu, Kedutaan Besar Inggris berkolaborasi dengan Kementerian Kesehatan melaksanakan *Cyber Security Conference*. Konferensi tersebut bertujuan untuk memberikan pengetahuan mengenai pengaturan kebijakan dalam teknologi pelayanan medis atau kerap disebut telemedis.[22] Platform telemedis yang ada di Indonesia pun semakin meningkat selama berlangsungnya pandemi Covid-19, seperti Alodokter, Halodoc, GrabHealth, KlikDokter dll. Melihat pada dinamika domestik yang terjadi, Kerjasama antara Kemenkes dengan pemerintah Inggris pada sektor telemedis ini sangat krusial bagi kepentingan nasional Indonesia.

Peningkatan Kapasitas melalui *Digital Health Programme*

Inggris dan Indonesia juga telah berkomitmen untuk bekerja sama dalam hal peningkatan kapasitas keamanan siber. Untuk mendukung hal tersebut, Pemerintah Inggris melalui Kedutaan Besar Inggris bekerja sama untuk mempromosikan perkembangan teknologi di Indonesia dengan BSSN untuk melanjutkan program kerjasama kedua negara. Pada Agustus 2021, Pemerintah Inggris mendanai peluang kolaborasi untuk LSM, akademisi, dan organisasi nirlaba Indonesia untuk bergabung dengan Program Kesehatan Digital. Program ini merupakan kerjasama antara BSSN dan Pemerintah Inggris dengan Departemen Kesehatan.[23]

Latar belakang kedua negara menginisasi program ini adalah karena meningkatnya kerentanan sektor kesehatan global yang berpengaruh pada layanan Kesehatan. BSSN bahkan mengungkapkan bahwa hampir 69% kembaga kesehatan memiliki tingkat keamanan siber yang lemah.[24] Oleh karenanya, BSSN dan UK Embassy mendorong peningkatan kapasitas siber bidang kesehatan dengan membentuk Tim *Computer Emergency Response Team* (CERT) dan *multi-agency Health Data Protection and Cyber Security Coordination Group*.

Upaya kerjasama kedua negara pada dasarnya menonjolkan 3 (tiga) poin yang dilampirkan dalam MoU tersebut. Poin-poin tersebut antara lain pengembangan dan implementasi strategi keamanan

[21] Denny Parsaulian, "Inggris-Indonesia Memulai Kerjasama Kemanan Siber", Media Indoneisa, Agustus 2018. Diakses 30 Agustus 2021. https://mediaindonesia.com/internasional/178498/inggris-indonesia-memulai-kerja-sama-keamanan-siber

[22] Jakarta Post, "Rising to the Cybersecurity Challenge in Indonesia's Healthcare System", *The Jakarta Post*, Juni 2021. Diakses 5 Oktober 2021. https://www.thejakartapost.com/adv/2021/06/28/rising-to-the-cybersecurity-challenge-in-indonesias-healthcare-system.html

[23] British Embassy Jakarta, "Indoensia: Call for Proposals to Enhance Cyber Security in Health Sector", UK Government, Agustus 2021. Diakses 4 Oktober 2021. https://www.gov.uk/government/news/indonesia-call-for-proposals-to-enhance-cyber-security-in-the-health-sector

[24] Zoe Deighton Smythe, "British Embassy Jakarta Open Call for Proposals to Enhance Cyber Security Health Sector in Indonesia", SOS, Agustus 2021. Diakses 4 Oktober 2021. https://securityonscreen.com/british-embassy-jakarta-opens-call-for-proposals-to-enhance-cyber-security-health-sector-in-indonesia/

siber nasional, yang dibuktikan dengan pertukaran informasi dalam penyusunan kebijakan keamanan siber bagi staf IIKN. Melalui pelatihan ini, peserta akan mendapatkan pemahaman tentang perkembangan kebijakan dan norma internasional terkait elemen jaringan siber.

Kerja sama antara kedua negara juga menyoroti poin-poin penting untuk mempromosikan kesadaran dan pelatihan keamanan siber serta peningkatan kapasitas. Bentuk kerja sama yang digagas kedua negara juga dilakukan dengan memadukan kondisi nasional setempat dan struktur budaya Indonesia. Oleh karena itu, mengingat tingginya jumlah kasus pandemi di Indonesia, seringkali terjadi kerja sama untuk meningkatkan kapasitas sektor kesehatan, yang juga menjadi efek domino bagi sektor lain, terutama sektor ekonomi. Inggris membantu memperluas akses internet di komunitas terpencil dan memperkuat sistem layanan telemedis untuk meningkatkan akses ke perawatan kesehatan.

Namun, sebelum MoU tersebut disepakati, Indonesia dan Inggris telah pernah melakukan kerjasama dalam bidang kejahatan siber. Kerjasama tersebut dilaksanakan antara Kemenkominfo dengan *UK National Cyber Crime Agency* dengan menghasilkan dokumen rekomendasi peningkatan kapasitas keamanan siber dalam "*The Future of Cyber Security Capacity in Indonesia*". [25] Kerjasama tersebut dilakukan sebelum BSSN terbentuk dan masih berada dibawah pengawasan kemenkominfo.

Analisis Kerjasama Siber Indonesia dengan Inggris terhadap Perkembangan *Cybersecurity* di Indonesia

Implementasi kerjasama keamanan siber Indonesia dengan Inggris secara tidak langsung menunjukkan adanya penekanan pada aspek kapasitas, baik itu kapasitas bagi para pegawai di institusi-institusi pemerintahan maupun peningkatan kapasitas di masyarakat sipil.

Peningkatan kapasitas pada sektor IIKN merupakan langkah taktis yang diambil pemerintah Indoneisa dikarenakan sektor IIKN sebagai instansi-instansi yang berkaitan dengan hajat hidup masyarakat luas dianggap harus memiliki sistem penanggulangan serta pencegahan insiden siber yang mumpuni.

Berkaitan langsung mengenai pengembangan kapasitas sumber daya manusia yang mumpuni, Indonesia dan Inggris juga melakukan pelaksanaan kerjasama dengan peningkatan aksesbilitas teknologi jaringan internet bagi penduduk yang tinggal di pelosok, di mana akses internet masih sulit di dapatkan. Mengingat saat kondisi pandemi belakangan ini, pelayanan kesehatan semakin lama juga memanfaatkan layanan internet dalam memberikan pelayanan dan respon terhadap adanya laporan akan kebutuhan layanan kesehatan karena semakin terintegrasi dengan internet.

MoU yang disepakati antara Indonesia dan Inggris terkait kerja

[25] Cyber Capacity Knowledge Portal, "UK-Indonesian Cyber Crime Knowledge Exchange", Cyber Capacity Knowledge Portal, April 2016. Diakses 8 Oktober 2021. https://cybilportal.org/projects/uk-indonesian-cyber-crime-knowledge-exchange/

sama siber merupakan langkah strategis yang baik untuk meningkatkan kapasitas dan kapabilitas sistem pertahanan dan keamanan siber Indonesia. Mulai dari komponen pengamanan data privasi, pengembangan sumber daya manusia hingga melindungi infrastruktur vital negara. Kerja sama keamanan siber antara Indonesia dan Inggris dianggap sebagai katalisator untuk meningkatkan dan mengembangkan sistem keamanan kedua negara di bidang lain seperti ekonomi dan investasi, terutama yang berkaitan dengan sektor e-commerce atau fintech. Hal ini karena Inggris sendiri merupakan salah satu mitra dagang dan investor terbesar di Indonesia.[26]

Pemerintah Indonesia dan Inggris bahkan telah mengkaji potensi perdagangan kedua negara yang sedang berkembang pesat, yakni sektor *fintech*. Merujuk Komisioner Dagang Inggris, Natalie Black, bidang kerjasama *fintech* ini merupakan sektor yang terus dikaji perkembangannya oleh pemerintahan Inggris.[27] Sehingga, penting bagi pemerintah Indonesia untuk terus mendorong transformasi ekonomi sektor digital yang dapat membuka peluang kerjasama yang lebih masif.

Faktor tersebut mendorong kedua negara untuk mempromosikan penggunaan teknologi dan peningkatan aksesibilitas internet yang aman dan terbuka. Sehingga, hal ini dapat mendukung pertumbuhan ekonomi kedua negara, melindungi keamanan dan stabilitas nasional, serta berkontribusi pada keamanan internasional. Menindaklanjuti MoU kerja sama siber tersebut, kedua negara telah menjalin sejumlah kolaborasi seperti peningkatan akses internet, pelatihan bersertifikasi, *sharing experience*, peningkatan sektor kesehatan digital.

SIMPULAN

Secara keseluruhan, penelitian ini memberikan penjelasan mengenai implementasi dari bentuk-bentuk kesepakatan kerjasama keamanan siber antara Indonesia dan Inggris. Penelitian menggunakan pendekatan teori *common aversion* yang menjelaskan bagaimana negara-negara mau untuk bekerjasama karena memiliki kepentingan yang sama, yakni membentuk keamanan siber nasional dan global. Oleh karenanya, Indonesia dan Inggris berkomitmen untuk menjalin kerjasama bilateral pada sektor keamanan siber.

Pada 14 Agustus 2018 Indonesia dan Inggris menandatangani MoU mengenai keamanan siber yang berlaku selama lima tahun. Faktor yang melatarbelakangi kerjasama adalah konsep dasar bahwa idealnya setiap negara demi mewujudkan kedaulatan nasionalnya maka harus mampu mengimbangi perkembangan zaman serta tekonologi di dalamnya, Indonesia yang secara garis besar masih dapat dikategorikan sebagai negara papan tengah dalam kemajuan dalam proteksi aspek keamanan siber memandang bahwa kerja sama dengan Inggris dapat membantu terwujudnya keinginan Indonesia meningkatkan kualitas keamanan

[26] Kementerian Luar Negeri, "Indonesia-UK Agreed to Strengthen Cooperation in Various Areas in order to Bolster Economic Diplomacy", Kementerian Luar Negeri, Januari 2020. Diakses 7 Oktober 2021. https://kemlu.go.id/portal/en/read/962/berita/indonesia-uk-agreed-to-strengthen-cooperation-in-various-areas-in-order-to-bolster-economic-diplomacy

[27] Rizky Alika, "Jajaki Potensi Perdagangan, Inggris Lirik Sektor Fintech", *Katadata*, Oktober 2019. Diakses 7 Oktober 2021. https://katadata.co.id/ekarina/berita/5e9a4e5f3ba6c/jajaki-potensi-perdagangan-inggris-lirik-sektor-fintech-indonesia

sibernya, Inggris sendiri yang saat ini telah dianggap sebagai salah satu negara dengan sistem keamanan siber terbaik di dunia memandang kerja sama ini dapat sebagai refleksi peningkatan kualitas mereka sendiri, serta menjadi instumen penyaluran kepentingan mereka di wilayah Asia Pasifik.

Berdasarkan pemaparan di bab-bab sebelumnya dapat ditarik kesimpulan bahwasanya tekonologi informasi dan komunikasi itu tidak pernah statis, melainkan terus berkembang semakin pesat seiring berjalannya waktu, maka berbanding lurus dengan itu potensi munculnya modus modus kejahatan siber yang baru juga semakin besar, hal itu mungkin membuat berbagi upaya penanggulangan dan pencegahan insiden siber terlihat tidak dapat memberikan kemanan siber yang hakiki, namun upaya-uapya tersebut tidaklah sia sia.

Meskipun modus serta jenis kejahtan siber terus berkembang, maka negara-negara pun harus semakin memantapkan pondasi serta kualitas keamanan sibernya, baik itu dari inovasi sendiri maupun melalui hasil dari kerja sama internasional. Pola ini lah yang telah menghantarkan umat manusia ke masa saat ini di mana manusia harus terus bergerak maju, tidak peduli bahaya dan ancaman yang ada di depan, karena bersamaan dengan itu maka akan ditemukan juga solusi dari setiap permasalahan, khususnya permasalahan keamanan siber.

Kondisi siber yang berpengaruh secara global, di mana tindak kejahatan siber terus berkembang. Perkembangan ini membawa perubahan besar dan mendasar pada tatanan sosial dan budaya dalam skala global. Bahkan perekonomian dunia saat ini juga bergantung pada aksesibilitas teknologi.

Sebagaimana konsep negara untuk melindungi segenap warga negaranya, pemerintah memiliki tanggungjawab untuk keamanan individu dan melindungi hak warga negara atas terjaminnya keamanan privasi data. Di Indonesia sendiri, permasalahan kebocoran data (*data leak*) kerap terjadi. Pada kasus yang lebih eksistensial, ancaman siber dapat mengganggu keamanan nasional dan menyebabkan kerugian besar. Serangan siber dapat menargetkan infrastruktur vital negara seperti sektor perbankan, kesehatan, departemen pertahanan dan sebagainya. Hal ini juga pernah terjadi di Indonesia dimana virus *malware* atau *ransomware* telah menyulitkan rumah sakit.

Besarnya dampak kejahatan siber ini menjadi ancaman bagi Indonesia yang tengah menghadapi pertumbuhan internet yang masif, mulai dari sektor ekonomi, pertahanan dan keamanan serta pelayanan publik.

Serangan siber ini tidak hanya berasal dari dalam negeri, namun juga bisa datang dari luar negeri. Oleh karenanya ancaman ini bersifat tidak memandang batas negara (*borderless)*. Bagi Indonesia, menggandeng Inggris sebagai mitra kolaborator dalam memperkuat sistem keamanan siber merupakan langkah determinan yang baik. Laporan GCI menunjukkan bahwa Inggris merupakan negara teratas dalam sistem pertahanan dan keamanan siber di dunia.

Inggris sendiri telah maju dari segi perkembangan teknologi dan kesadaran berteknologi. Hal ini tidak lepas dari komitmen pemerintahannya untuk meminimalisir ancaman siber di negaranya, sehingga pemerintah Inggris mengerahkan manajemen siber dalam sinergitas yang komprehen. Secara resmi, komitmen

tersebut diimplementasikan pada tahun 2010 dimana Inggris meluncurkan strategi kebijakan siber dalam *National Security Strategy*. Pemerintah Inggris bahkan mengklasifikasikan kejahatan siber sebagai jenis kejahatan tingkat pertama (*Tier One*) bersama dengan kejahatan terorisme dan bencana alam.

Inggris sendiri telah lebih dahulu mengalami gejala kejahatan dan ancaman siber berupa *cyberwar*. Mulai dari gangguan sistem dan peretasan data hingga pada kasus yang lebih besar yakni perusahaan pertahanan yang mengalami spionase. Pemerintah Inggris mulai menyadari bahwa ancaman siber tidak hanya dilancarkan oleh individu tertentu, namun dapat berafiliasi dengan negara asing atau kelompok teroris yang terorganisir dengan tujuan mengacaukan infrastruktur vital Inggris. Oleh karenanya, pemerintah Inggris menyerukan "*global response"* kepada negara di dunia untuk sama-sama berkomitmen mengatasi persoalan kejahatan siber.

Kerjasama keamanan siber antara Indonesia dan Inggris merupakan bentuk kerjasama keamanan yang baru dan pertama sekali dilakukan oleh kedua negara. Meski demikian, kerjasama keamanan siber ini disebut sebagai pendorong dari kerjasama bilateral yang telah terjadi sebelumnya terutama pada sektor perekonomian dan sektor lainnya. Melalui kerjasama ini, Indonesia berambisi untuk memiliki sistem keamanan siber yang kuat dan mandiri. Inggris sebagai mitra siber Indonesia tidak terlepas dari kemampuan, kapabilitas serta pengalaman yang dimiliki Inggris pada sektor tersebut. Tidak hanya kebijakan yang terintegrasi, Inggris juga telah menggunakan strategi pertahanan siber ofensif yang mampu menyerang balik sumber ancaman.

Sebaliknya, apabila dioptimalisasikan Indonesia dapat memajukan pertumbuhan ekonominya terutama pada sektor digital ekonomi yang kini pertumbuhannya tengah pesat.

Kedua, melindungi kedaulatan dan stabilitas nasional yang berkaitan dengan ruang lingkup sosial budaya dan politik. Dalam hal ini, penelitian menyoroti kasus-kasus disintegrasi yang disebabkan oleh ketidakamanan ruang siber, sebagaimana kasus terorisme siber (*cyber terrorism*). Kelompok yang berafiliasi dengan terorisme kini telah memanfaatkan kemajuan teknologi untuk melakukan perekrutan, *fundraising*, doktrinisasi serta pelatihan perakitan bom. Selain itu, juga terdapat kelompok buzzer yang memecah-belah (*disintegrating*) masyarakat dengan memberikan berita bohong yang kerap disebut sebagai *era post-truth.*

Kedaulatan negara yang menjadi prioritas segenap bangsa Indonesia juga menajdi determinan dalam kerjasama peningkatan keamanan siber ini. Sebagaimana yang telah dialami Indonesia secara empirik ketika dihadapkan pada perang siber

Melalui kerjasama dengan Inggris, Indonesia dapat memanfaatkan kemajuan jasa dan layanan teknologi Inggris melalui pelatihan secara teknis maupun generik. Dalam MoU Kerjasama Keamanan Siber tersebut, kedua negara menyepakati lima poin yang dapat diimplementasikan. Diantaranya adalah implementasi dan pengembangan strategi keamanan siber nasional; pengelolaan insiden siber; kejahatan siber; pelatihan dan kampanye kesadaran siber; peningkatan kapasitas siber.

Selama berlangsungnya periode MoU Kerjasama Keamanan Siber, kedua negara telah melaksanakan sejumlah program atau kegiatan di bidang siber. Secara umum, program tersebut lebih banyak berfokus pada peningkatan kapasitas siber. Meski demikian, bidang kerjasama lainnya juga telah dilakukan yakni pada poin implementasi dan pengembangan strategi keamanan siber nasional serta pelatihan dan kampanye kesadaran siber.

Program dari kerjasama ini dirancang untuk meningkatkan kapabilitas negara dalam mengembangkan manajemen instansi siber termasuk peningkatan kapasitas SDM terutama perumus kebijakan serta memberikan pemahaman terkait pengelolaan data, informasi dan sistem keamanan siber. Melalui program-program tersebut, Indonesia dapat memanfaatkannya untuk mengatur regulasi kebijakan siber yang lebih komprehensif yang juga dapat mendukung pertumbuhan ekonomi nasional.

Pada dasarnya, kerjasama bidang keamanan siber ini sama memberikan landasan kepentingan nasional masing-masing negara. Bagi Indonesia sendiri, pemerintah dapat meningkatkan kemampuan penangkalan serangan siber yang cukup besar di Indonesia, mulai dari isu kebocoran data hingga perlindungan infratruktur vital nasional. Saat ini Indonesia sudah memiliki rancangan UU Perlindungan Data Privasi dan Strategi Nasional Keamanan Siber. Oleh karenanya, pemerintah dapat mempelajari sistematika pengaturan regulasi yang tepat melalui konsolidasi yang sesuai dengan kondisi politik, sosial dan budaya sehingga memperoleh *output* yang berpresisi.

Bagi Inggris, kerjasama keamanan siber ini merupakan bagian dari visi *UK National Security Strategy 2016-2021,* dimana pemerintahan Inggris berkomitmen untuk menjalin kerjasama siber internasional dalam rnagka mendukung kerjasama pada sektor bisnis Inggris yang Sebagian besar telah memanfaatkan kemajuan teknologi. Inggris berambisi untuk menjadi negara yang aman dan terbuka dalam sektor bisnis dan investasi secara digital. Dalam NSS tersebut, Inggris juga meneybutkan akan memberikan investasinya pada bidang siber untuk membantu negara-negara kawasan Indo-Pasifik. Oleh karenanya, dapat disimpulkan bahwa masing-masing negara memiliki tujuan dan kepentingan sama yang pada akhirnya melibatkan adanya hubungan bilateral pada sektor keamanan siber.

Perlu dipahami bahwa pelaksanaan kerjasama keamanan siber ini juga turut memperoleh beberapa kendala yang dihadapi kedua negara sehingga beberapa poin seperti *point of contact* dan penundaan jadwal kegiatan *Cyber Dialogue Forum.* Hal ini karena kedua perwakilan masih menyesuaikan wkatu pelaksanaan kegiatan untuk memaksimalkan diskusi peninjauan MoU. Sehingga dampak dari kerjasama ini belum dapat dilihat secara signifikan dan spesifik. Oleh karenanya, melalui *cyber dialogue forum* mendatang kedua negara diharapkan dapat memaksimalkan kerjasama keamanan siber pada ranah yang lebih praktikal.

DAFTAR PUSTAKA

Buku

Yani, Yanyan Mochamad, dkk, *Pengantar Studi Keamanan*, Malang: Intrans Publishing

(2017)

Jurnal

Arifah, Dista Amalia, "Kasus CyberCrime di Indonesia", "Jurnal Bisnis dan Ekonomi (JBE)", vol. 18, no. 2, (2011)

Stein, Arthur " Coordination and Collaboration : Regimes in Anarchic World", International Organization, vol.36, no.2, International Regimes (Spring, 1982)

Link Internet

Alika, Rizky "Jajaki Potensi Perdagangan, Inggris Lirik Sektor Fintech", Katadata, Oktober 2019. Diakses 7 Oktober 2021. https://katadata.co.id/ekarina/berita/5e9a4e5f3ba6c/jajaki-potensi-perdagangan-inggris-lirik-sektor-fintech-indonesia

BAE Systems, "Cyber Security Indonesia", BAE Systems. Diakses 5 Oktober 2021 https://www.baesystems.com/en/cybersecurity/event/cyber-security-indonesia

BBC News Indonesia, "Pinjaman online: 'Bagaimana saya menjadi korban penyalahgunaan data pribadi'" diakses 17 Juni 2021 pukul 15.00 WIB https://www.bbc.com/indonesia/majalah-57046585

British Embassy Jakarta, "Indoensia: Call for Proposals to Enhance Cyber Security in Health Sector", UK Government, Agustus 2021. Diakses 4 Oktober 2021. https://www.gov.uk/government/news/indonesia-call-for-proposals-to-enhance-cyber-security-in-the-health-sector

BSSN, "BSSN Bekerja Sama dengan UK Embassy Jakarta Meluncurkan Program Webinar dan Sertifikasi Keamanan Siber", Diakses 4 Oktober 2021 https://bssn.go.id/bssn-bekerja-sama-dengan-uk-embassy-jakarta-meluncurkan-program-webinar-dan-sertifikasi-keamanan-siber/

Cyber Capacity Knowledge Portal, "UK-Indonesian Cyber Crime Knowledge Exchange", Cyber Capacity Knowledge Portal, April 2016. Diakses 8 Oktober 2021. https://cybilportal.org/projects/uk-indonesian-cyber-crime-knowledge-exchange

Definition, "What does Point of Contact means?", diakses 17 Juni 2020 https://www.definitions.net/definition/Point+Of+Contact

Frost & Sullivan, "Ancaman Keamanan Siber Menyebabkan Kerugian Ekonomi bagi Organisasi di Indonesia Sebesar US$34.2 Miliar", Microsoft.com, Mei 2018. Diakses 26 September https://news.microsoft.com/id-id/2018/05/24/ancaman-keamanan-siber-menyebabkan-kerugian-ekonomi-bagi-organisasi-di-indonesia-sebesar-us34-2-miliar/

It Governance, "What is Cyber Security? Definition and Best Practices", diakses 19 Maret 2020 https://www.itgovernance.co.uk/what-is-cybersecurity.

Jakarta Post, "Rising to the Cybersecurity Challenge in

Indonesia's Healthcare System", The Jakarta Post, Juni 2021. Diakses 5 Oktober 2021. https://www.thejakartapost.com/adv/2021/06/28/rising-to-the-cybersecurity-challenge-in-indonesias-healthcare-system.html

Jonathan, "Pengertian Kerjasama : Memahami Arti, Manfaat, dan Bentuk Kerjasama, diakses 19 Maret 2020, https://www.maxmanroe.com/pengertian-kerjasama.html.

Kementerian Luar Negeri "Memorandum Saling Pengertian", 2018. Diakses 28 September 2021. https://treaty.kemlu.go.id

Kementerian Luar Negeri, "Indonesia-UK Agreed to Strengthen Cooperation in Various Areas in order to Bolster Economic Diplomacy", Kementerian Luar Negeri, Januari 2020. Diakses 7 Oktober 2021. https://kemlu.go.id/portal/en/read/962/berita/indonesia-uk-agreed-to-strengthen-cooperation-in-various-areas-in-order-to-bolster-economic-diplomacy

Parsaulian, Denny "Inggris-Indonesia Memulai Kerjasama Kemanan Siber", Media Indoneisa, Agustus 2018. Diakses 30 Agustus 2021. https://mediaindonesia.com/internasional/178498/inggris-indonesia-memulai-kerja-sama-keamanan-siber

Pinandita, Apriza "UK, Local NGO Roll Out Digital Public Health Project for W. Java's Remote Communities", Jakarta Post, Mei 2020. Diakses 5 Oktober 2021 https://www.thejakartapost.com/news/2020/05/19/uk-local-ngo-roll-out-digital-public-health-project-for-w-javas-remote-communities.html

Smythe, Zoe Deighton, "British Embassy Jakarta Open Call for Proposals to Enhance Cyber Security Health Sector in Indonesia", SOS, Agustus 2021. Diakses 4 Oktober 2021. https://securityonscreen.com/british-embassy-jakarta-opens-call-for-proposals-to-enhance-cyber-security-health-sector-in-indonesia/

Statista, "Number of internet users in Indonesia from 2015-2025", diakses pada 27 November 2020. https://www.statista.com/statistics/254456/number-of-internet-users-in-indonesia/

Vishnum, "Ancaman Keamanan SIber Menyebabkan Kerugian Ekonomi bagi Oganisasi Besar di Indonesia Sebesar US$43,2 Miliar", Microsoft, Mei 2018. Diakses 30 Agustus 2021. https://news.microsoft.com/id-id/2018/05/24/ancaman-keamanan-siber-menyebabkan-kerugian-ekonomi-bagi-organisasi-di-indonesia-sebesar-us34-2-miliar/