GLOBAL INSIGHTS 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.v2i2.3234
Vol. 02 No. 02 Tahun 2025

Article Informations
Corresponding Email:
annisanaliyah@gmail.com

Received: 04/02/2025; *Accepted*: 19/02/2025; *Published*: 30/06/2025

KERJASAMA INDONESIA DAN AUSTRALIA DALAM MEMPERKUAT *CYBER SECURITY* INDONESIA TAHUN 2018-2020

Annisa Nur Aliyah[1)] Yusep Ginanjar[2)] Jusmalia Oktaviani[3)]

[1,2,3)]Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Jenderal Achmad Yani

Abstrak

Maraknya ancaman yang dihasilkan dari ruang siber semakin berkembang dan kompleks, ini terbukti oleh fakta bahwa penyalahgunaan ini dilakukan bukan hanya oleh negara saja tetapi juga oleh individu atau organisasi non-negara seperti aktivis dan teroris. Dengan penempatan siber nasional yang terbuka, Indonesia harus mengembangkan strategi yang efektif dan memiliki daya perlindungan tinggi dalam keamanan siber salah satunya kerjasama dengan Australia. Metode penelitian yang digunakan yakni metode kualitatif, dengan berfokus pada kerjasama antara Indonesia dan Australia. Penelitian ini menyoroti urgensi dan implementasi dari kerjasama ini serta dampak dan tantangan yang muncul dalam meperkuat infrastruktur keamanan siber di Indonesia. Penelitian ini menjelaskan pentingnya kerjasama internasional dalam mengatasi tantangan keamanan siber yang semakin meningkat dan kompleks. Kerjasama antara Indonesia dan Australia dianggap sebagai langkah strategis dalam memperkuat keamanan siber di Indonesia dan implementasi kerjasama kedua negara tersebut menghasilkan dampak positif serta memberikan kontribusi yang signifikan dalam memperkuat keamanan siber di Indonesia melalui peningkatan kapasitas dan kerjasama.

Kata Kunci : Indonesia, Australia, Siber, Kerjasama

Abstract

The rise of threats resulting from cyberspace is increasingly growing and complex, this is evidenced by the fact that this abuse is carried out not only by the state alone but also by individuals or non-state organizations such as

activists and terrorists. With an open national cyber deployment, Indonesia must develop an effective strategy and have high protection in cybersecurity, one of which is cooperation with Australia. The research method used is a qualitative method, focusing on cooperation between Indonesia and Australia. This research highlights the urgency and implementation of this collaboration as well as the impacts and challenges that arise in strengthening the cybersecurity infrastructure in Indonesia. This research explains the importance of international cooperation in overcoming increasing and complex cybersecurity challenges. The cooperation between Indonesia and Australia is considered a strategic step in strengthening cybersecurity in Indonesia and the implementation of the cooperation between the two countries has produced a positive impact and made a significant contribution in strengthening cybersecurity in Indonesia through capacity building and cooperation.

Keywords : Indonesia, Australia, Cyber, Cooperation

PENDAHULUAN

Perkembangan Globalisasi serta pertumbuhan digital saat ini berkembang dengan sangat pesat, yangmana pesatnya perkembangan teknologi informasi dan komunikasi, segala jenis informasi dan data, baik lokal maupun internasional, kini mudah dijangkau. Pertukaran informasi dan data yang luas ini kemudian membuat komunikasi antar negara menjadi lebih mudah. Indonesia menjadi salah satu negara yang hingga saat ini berupaya meningkatkan aspek teknologinya di era globalisasi ini. Hal tersebut dikarenakan Pada tahun 2018, Indonesia menempati nomor 6 di seluruh dunia dalam hal penggunaan internet, Indonesia selalu mengalami pertumbuhan angka yang cukup masif dari tahun-tahun sebelumnya. Adanya kenaikan jumlah penggunaan internet di Indonesia pada lima tahun terakhir yakni salah satunya diakibatkan oleh mulai maraknya penggunaan handphone atau telepon selular (Badan Pusat Statistik, 2018).

Tingginya angka kenaikan jumlah penggunaan internet di Indonesia dari tahun 2013 hingga tahun 2018, menandai bahwa Indonesia adalah negara besar dari aspek sumber daya dan populasinya, tetapi tingginya angka penggunaan internet juga menjadi hal yang perlu diwaspadai, dimana adanya nilai trend positif dari penggunaan akses internet diikuti juga oleh beberapa kejahatan-kejahatan yang dapat mengancam setiap individu penggunanya, bahkan dapat juga mengancam sebuah negara. Hal-hal seperti pembajakan, penipuan, pemalsuan, bahkan pelecehan dapat mengancam dan memimpa setiap individu pengguna jaringan internet. Kemudian ada pula kejahatan-kejahatan yang dapat mengancam cyber security di Indonesia, yakni: Malware, Emotet, DoS (*Denial of Service*), MITM (*Man in the Middle*), Phising, Injeksi SQL (*Structured Query Language*), dan juga Serangan kata sandi. Serangan siber ini tentu saja akan menimbulkan kerugian salah satunya adalah *financial* serta kebocoran data. Dimana menurut laporan Pusat Operasi Keamanan Siber Nasional (IDSN) tahun 2018, terdapat lebih dari 205 juta serangan siber yang terjadi di Indonesia. Serangan tersebut meliputi pencurian data, peretasan website, penyebaran malware, dan aktivitas ilegal

lainnya. Dengan meningkatnya aktivitas ekonomi digital dan e-government di Indonesia, kebutuhan akan keamanan siber semakin mendesak (Arianti V, 2019).

Indonesia juga kerap kali menjadi sasaran spionase asing atau yang berada diluar negara yang salah satu bentuknya adalah perang siber atau *cyber warfare.* Strategi dan teknik perang siber ini menjadi sangat canggih dan kompleks karena kemajuan teknologi yang tumbuh dengan sangat pesat. Dikarenakan semakin hari ancaman siber semakin meningkat, kemampuan intelijen siber Indonesia sangatlah penting untuk ditingkatkan. Berdasarkan GCI (*Global Cybersecurity Index*) pada tahun 2017, Indonesia menempati negara dengan nilai keamanan siber yang rendah. Peringkat yang ditempati oleh Indonesia tidak berbeda jauh dengan apa yang ditempati oleh negara-negara dikawasan Afrika dan Amerika Selatan yang mana memiliki nilai paling lemah terhadap serangan siber. Dari 195 negara di dunia, Indonesia menduduki peringkat 70 dengan nilai 0,424. Bahkan dengan nilai *index* tersebut, Indonesia berada sangat jauh dibawah negara-negara tetangganya seperti Singapura yang menempati peringkat pertama dan disusul oleh Malaysia yang berada di peringkat ketiga dalam hal *cybersecurity index* tahun 2017. Badan Reserse Kriminal atau Bareskrim juga melaporkan bahwa terjadinya peningkatan laporan kejahatan siber yang semakin marak dari tahun ke tahun, yang mana telah terdapat sekitar 25.759 pengaduan masyarakat dengan total kerugian yang hampir mencapai 5,05 triliun rupiah (BSSN, 2018).

Akibatnya pemerintah Indonesia telah melakukan berbagai upaya, antara lain membentuk Badan Siber dan Sandi Negara (BSSN), menerbitkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta menjalin kerjasama dengan negara-negara mitra seperti Australia. Keamanan siber di Indonesia mempunyai gambaran yang dianggap rentan dari segala ancaman siber termasuk *ransomware* yang mana dari ancaman tersebut Indonesia diperkirakan mengalami kerugian yang cukup besar. Banyaknya serangan siber yang masuk ke Indonesia berasal dari beberapa negara seperti Rusia, China dan juga Amerika Serikat. Dan serangan sibernya pun menargetkan berbagai sektor dan lembaga seperti sektor pemerintahan, sektor perbankan dan keuangan, *e-commerce*, telekomunikasi, kesehatan, serta infrastruktur kritis, maupun individu dan organisasi non pemerintahan. Menurut Frost dan Sullivan, Indonesia berpotensi memiliki kerugian ekonomi mencapai 34,2 miliar dollar AS yang disebabkan oleh serangan siber.

Kurangnya kesadaran dari masyarakat Indonesia tentang keamanan siber dinilai masih terlalu rendah yang membuat pengguna internet rentan terhadap penipuan online, pencurian data, serta serangan yang lainnya. Kemudian belum memadainya infrastruktur serta fasilitas keamanan digital Indonesia, Dan juga regulasi keamanan siber di Indonesia pada tahun 2018 yang mana rancangan UU perlindungan data pribadi serta keamanan siber masih pada tahap pengembangan serta belum disahkan. Terjadinya peningkatan serangan siber di Indonesia setiap tahunnya serta maraknya

ancaman *cyberspace* juga membuktikan bahwasanya penyalahgunaan ini dilakukan bukan hanya oleh negara saja tetapi juga oleh individu atau organisasi non-negara seperti aktivis dan teroris Oleh sebab itu Indonesia mencoba berupaya mengatasi permasalahan tersebut salah satunya adalah dengan melakukan kerjasama dengan Australia

Kerjasama ini berlandaskan pada kepentingan bersama untuk memperkuat persahabatan kedua negara yang didasari prinsip persamaan dan resiprositas. Kemudian yang mana Australia mempunyai peringkat keamanan siber ke 11 dari seluruh negara didunia dan peringkat ke 3 dari seluruh negara kawasan Asia-Pasifik pada tahun 2018. Hubungan Kerjasama antara Indonesia dan Australia dalam bidang cyber security telah terjalin sejak lama. Kedua negara telah menandatangani beberapa perjanjian kerjasama, seperti Persetujuan *Cyber Engagement* (*Cyber Engagement Agreement*) yang menjadi landasan awal bagi kerjasama keamanan siber pada tahun 2017 dan *Memorandum of Understanding* (MoU) di Bidang *Cyber Security* pada tahun 2018. Ruang lingkup kerjasama ini mencakup beberapa area kerjasama utama, antara lain: pertukaran informasi dan intelijen terkait ancaman siber, peningkatan kapasitas sumber daya manusia melalui pelatihan dan program pengembangan, kolaborasi dalam penanganan insiden siber, penelitian dan pengembangan teknologi keamanan siber, serta kerjasama regulasi dan standardisasi di bidang *cyber security.* Kerjasama antara kedua negara ini juga melibatkan lembaga-lembaga dari kedua negara diantaranya melibatkan Lembaga dari Indonesia yakni: Badan Sandi dan Siber Negara (BSSN), Kementerian Komunikasi dan Informatika, dan instansi pemerintah terkait, kemudian dari Australia yakni: Pusat siber nasional Australia (*Australian Cyber Security Centre*), Departemen dalam negeri, dan instansi lain yang terkait. Meskipun sebelum disepakatinya kerjasama tersebut hubungan kedua negara sempat bersitegang akibat adanya dugaan *spionase* yang dilakukan Australia kepada Indonesia Tahun 2013.

Terjalinnya kembali kerjasama antara kedua negara tersebut, diharapkan dapat mendapat capaian serta manfaat bagi kedua negara dalam meningkatkan dan memperbaiki keamanan siber, Namun masih terdapat beberapa tantangan dan hambatan dalam pelaksanaan kerjasama antara kedua negara ini, salah satunya adalah terkait perbedaan teknologi yang mengakibatkan kesenjangan ini dapat menyulitkan transfer pengetahuan dan teknologi secara efektif dari Australia ke Indonesia. Dan hal ini pun dapat berpotensi menghambat kelancaran pertukaran informasi yang krusial dalam kerjasama. Oleh karena itu, penelitian ini akan mengkaji hubungan kerjasama Indonesia dan Australia dalam memperkuat *cyber security* Indonesia.

PEMBAHASAN

Gambaran Umum Hubungan Bilateral Indonesia dan Australia

Hubungan kerjasama antara Indonesia dan Australia bisa tergolong memiliki hubungan yang cukup unik. Hubungan dari kedua negara kerap kali dapat

digambarkan sebagai *rollercoaster*, hal ini yakni dapat naik secara perlahan namun dapat turun dengan sangat tajam. Gambaran tersebut menjadi sejarah hubungan antara kedua negara yang disatu sisi sangat menjanjikan berbagai peluang kerjasama namun disisi yang lainnya terkadang penuh dengan berbagai tantangan. Kondisi tersebut diakibatkan oleh berbagai perbedaan kebudayaan, kemajuan, dan orientasi politik di antara kedua negara dan bangsa yang menyebabkan perbedaan prioritas kepentingan. Tidak diragukan lagi, perbedaan-perbedaan inilah yang menyebabkan banyak masalah yang selalu mengganggu dan mewarnai hubungan bilateral kedua negara.

Dalam dinamika hubungan bilateral Indonesia dan Australia dibidang siber, terdapat berbagai upaya yang dilakukan oleh kedua negara. Mulai dari pelatihan personel kepolisian nasional Indonesia dan Australia hingga hibah dana dan peralatan investigasi kejahatan siber dari Australia kepada Indonesia untuk membangun CCIC atau *Cyber Crime Investigation Centre* dan CCISO atau *Cyber Crime Investigation Satellite Office*. CCIC dan CCISO ini merupakan kantor investigasi kejahatan siber yang berada di markas besar Polri serta berada di beberapa Polda lain di Indonesia. Pembangunan CCIC dan CCISO ini sebagian besar disebabkan oleh hibah yang diberikan oleh Australia melalui Australian Federal Police atau AFP, yang memberikan sejumlah dana dan peralatan komputer senilai 20 juta dollar Australia. AFP dan Polri telah melakukan berbagai upaya untuk memastikan bahwa CCIC dan CCISO tetap beroperasi sejak didirikan Salah satu contohnya adalah perbaikan dan pemeliharaan peralatan, serta pelatihan kembali staf kepolisian Indonesia oleh AFP. Pembangunan CCIC dan CCISO ini juga menggelontorkan dana anggaran yang cukup besar, bahkan hingga puluhan juta dollar (Bambang S, 2017).

Dalam hal keamanan siber Indonesia sendiri memiliki satu lebaga yaitu BSSN. Badan Siber dan Sandi Negara atau BSSN merupakan suatu organisasi atau lembaga utama di Indonesia untuk intelijen sinyal, intelijen siber, intelijen ancaman siber, pertahanan siber, dan keamanan siber. BSSN merupakan lembaga pemerintahan yang bertugas dan berada dibawah serta bertanggung jawab kepada presiden, yang mana kegiatan organisasi dan tata kerja BSSN diatur dalam peraturan BSSN No.6 Tahun 2021 tentang organisasi dan tata kerja. Selain itu BSSN juga dalam melaksanakan tugasnya memiliki 8 fungsi, yaitu perumusan dan penetapan kebijakan teknis di bidang keamanan siber dan sandi, pelaksanaan kebijakan teknis di bidang keamanan siber dan sandi, penyusunan norma, standar, prosedur, dan kriteria di bidang persandian, pelaksanaan bimbingan teknis dan supervisi di bidang persandian, koordinasi pelaksanaan tugas, pembinaan, dan dukungan administrasi kepada seluruh unsur organisasi di lingkungan BSSN, pengelolaan barang milik negara yang menjadi tanggung jawab BSSN, pelaksanaan dukungan yang bersifat substantif kepada seluruh unsur organisasi di lingkungan BSSN, dan pengawasan atas pelaksanaan tugas di lingkungan BSSN.

Sedangkan Australia memiliki suatu lembaga yang dikenal dengan DFAT atau *The Department of Foreign Affairs and Trade* merupakan departemen milik Australia yang kegiatannya mempromosikan dan melindungi kepentingan internasional Australia untuk mendukung keamanan dan kemakmuran Australia. Departemen ini bekerja dengan mitra internasional dan negara lain untuk mengatasi tantangan global, meningkatkan peluang perdagangan dan investasi, melindungi aturan internasional, menjaga wilayah kami tetap stabil, dan membantu warga Australia di luar negeri. DFAT memiliki nilai dalam menetapkan cara untuk mencapai tujuannya yang didasari oleh tindakan dan perilaku departemen. Hal tersebutlah yang menciptakan rasa identitas bersama dalam DFAT dan mendefinisikan bagaimana mereka bekerja dan berinteraksi satu sama lain, baik dengan mitra atau klien, dan komunitas yang lebih luas. Hal itu penting untuk kinerja dan reputasi departemen untuk mencapai visi positif sebagai organisasi. Tujuan DFAT adalah membuat nilai-nilai itu tersebar ke seluruh departemen yang mana nilai-nilai inti DFAT tetap konstan dan budaya didalamnya terus berkembang. Keberhasilan organisasi yang berkelanjutan ditentukan oleh sejauh mana organisasi memperkuat dan menjalankan nilai-nilai tersebut, serta kualitas dan efektivitas sistem dan proses yang dilakukan. Nilai-nilai DFAT ini adalah komitmen dari departemen kepada pemerintah Australia, komunitas dan mitra, serta anggota organisasi global, Yang mana nilai-nilai ini menunjukan ambisi departemen sebagai lembaga berwawasan kedepan yang dapat dibanggakan.

Dinamika Perkembangan Keamanan Siber di Indonesia

Keamanan siber merupakan isu yang relatif cukup baru, isu ini muncul pada pertengahan abad ke-20. Keamanan siber atau *cyber security* merupakan beberapa teknologi, proses, serta praktik yang dimaksudkan untuk melindungi perangkat, jaringan, program dan data dari berbagai macam serangan seperti pencurian, modifikasi, peretasan, kerusakan, dan akses yang ilegal. Pengertian lain dari keamanan siber yakni suatu teknik yang berguna melindungi sistem, perangkat, jaringan, serta data yang tersimpan dalam suatu atau lebih perangkat dari serangan siber dengan menggunakan alat seperti *firewall* dan perangkat antivirus untuk melindungi perangkat dari peretasan dan malware, serta mempertahankan diri dari berbagai serangan siber seperti phising dan DdoS. Menurut Tim Stevens didalam bukunya menjelaskan arti dari keamanan siber dalam perspektif politik, ia menjelaskan bahwa keamanan siber merupakan tanggapan dari ancaman serta resiko modern yang dirasakan oleh infrastuktur teknologi informasi secara global yang dikenal sebagai internet. Kemudian UNODC menjelaskan ancaman kejahatan siber sebagai *cyber-dependent offences* atau penggunaan teknologi informasi dan komunikasi untuk melakukan kejahatan dan serangan. Menurut laporan *Data Breach Investigations Report* 2020 yang dilansir oleh Verizon, sekitar 55% hingga 60% serangan siber berasal dari organisasi kriminal, 10% berasal dari negara atau negara affiliasi, 10% berasal dari admin sistem, 10% besaral dari *end user*, dan 10% berasal dari yang lainnya (Verizone.com, 2020).

- Sejarah Dan Perkembangan Keamanan Siber Indonesia

Awal mula perkembangan siber di Indonesia tidak lepas dari peristiwa pada masa awal kemerdekaan Indonesia pada 4 April 1946. Hal itu bewaral dari menteri pertahanan saat itu yakni Amir Sjarifuddin yang memerintahkan dr. Roebiono Kertopati, seorang dokter di kementerian pertahanan bagian intelijen untuk membentuk suatu badan pemberitaan rahasia atau dinas code yang menjadi cikal bakal terbentuknya lembaga sandi negara atau BSSN. Mulanya penggunaan internet di Indonesia hanya digunakan oleh lembaga pendidikan atau penelitian yang memerlukan akses informasi ke luar negeri melalui jaringan akses internet global. Kemudian selang beberapa tahun mulai banyak perusahaan yang menawarkan jasa layanan internet. Kemudian masuk diawal abad ke-20 yang mana pertumbuhan internet diiringi oleh munculnya teknologi baru serta keadaan sosial masyarakat Indonesia. Namun hal ini juga terdapat sisi negatif, mulai munculnya informasi-informasi palsu, munculnya konten seksual dan pornografi, hingga ketergantungan terhadap internet. Semakin berkembangnya teknologi dan munculnya dinamika yang ada di Indonesia dalam masalah siber ini memberikan masalah serta tantangan tersendiri yang harus dihadapi. Munculnya serangan-serangan siber seperti malware, phising, DDoS, hingga masalah spionase dari negara luar harus diiringi juga oleh kemajuan teknologi serta pengembangan sumber daya yang dimiliki. Strategi keamanan nasional, koordinasi multi pihak, sistem peringatan dini, dan rencana pemulihan, dan kerjasama antar negara harus dapat dilakukan oleh Indonesia guna menjaga keamanan serta kedaulatan negara baik di dunia siber ataupun tidak.

- Infrastruktur Keamanan Siber Indonesia

Dalam konteks pertahanan negara, keamanan siber saat ini belum ditangani secara sektoral, tidak terkoordinasi dengan baik, dan tidak terintegrasi secara menyeluruh. . Kementerian Pertahanan membentuk tim operasi keamanan siber yang bertujuan untuk memerangi dan menanggulangi kejahatan siber dan menjaga kedaulatan negara didunia siber. Melalui taktik pencegahan, penuntutan, dan pemulihan pertahanan siber, Indonesia harus dapat memperkuat *soft power* dan *smart power* dalam sektor bidang pertahanan untuk mengantisipasi terjadinya perang siber. Kemudian Kementerian Komunikasi dan Informatika yang merupakan lembaga pemerintahan tertinggi di sektor informatika, telekomunikasi, dan digital, mempunyai lima tujuan keamanan siber. Paradigma strategi "*Ends-Ways-Means*", yang menekankan tujuan, prioritas, dan tindakan terukur, adalah cara mereka melakukan hal ini. Kelima kebijakan tersebut terdiri dari, pengembangan kapasitas, Menetapkan kebijakan dan kerangka hukum, struktur pengorganisasian, tindakan teknis dan operasional, dan kerjasama internasional. Dalam rangka menjaga kepentingan nasional, Pemerintah harus memahami, menyelidiki, menilai, memprediksi, dan merencanakan insiden-insiden yang mungkin akan timbul di dunia maya dan menimbulkan ancaman terhadap pertahanan negara. Ancaman tidak lagi berbentuk

tradisional. Sebaliknya, mereka kini harus menjadi virtual dan asimetris berkat teknologi.

- Kebijakan Keamanan Siber Indonesia

Karena keterbelakangan teknologi yang terus berlanjut, implementasi kebijakan keamanan siber di Indonesia menjadi diragukan. Sebagai negara berkembang, Indonesia sedikit tertinggal dalam hal kemajuan teknologi informasi dan komunikasi. Pemerintah Indonesia telah membuat beberapa kebijakan serta regulasi terkait keamanan siber yang diatur oleh undang-undang, seperti UU No.11 Tahun 2008 tentang informasi dan transaksi elektronik (ITE). Kemudian muncul UU No. 19 Tahun 2016 tentang Perubahan UU ITE, yang mana sebelumnya UU ITE tahun 2008 menimbulkan pro kontra serta terdapat beberapa pasal karet didalam isinya. Isi dari UU tentang perubahan ITE tahun 2016 secara garis besar dapat meberikan perlindungan hukum bagi masyarakat dan agar masyarakat semakin cerdas dalam menggunakan internet dan dapat menjaga etika ketika berkomunikasi dan menyebarkan informasi, serta dapat menghindari kegiatan di dunia maya yang berunsur SARA, pornografi, dan radikalisme. Indonesia juga membentuk suatu lembaga yang bernama Badan Siber dan Sandi Negara atau BSSN pada tahun 2017, Tujuan lembaga ini guna mewujudkan rangka keamanan, perlindungan, serta kedaulatan siber nasional dan menumbuhkan perekonomian nasional. Sementara itu, Indonesia memiliki dua organisasi komunitas yang didedikasikan untuk keamanan siber. *Indonesia Communication Emergency Response Team* (ID-CERT) serta *Indonesia Academic Computer Security Incident Response Team* (ID-ACAD-CSIRT).

- Tantangan Keamanan Siber Indonesia

Tantangan terbesar keamanan siber salah satunya yakni meningkatnya angka dan kompleksitas lanskap yang diakibatkan oleh serangan siber. Kemudian dampak yang dihasilkan dari serangan siber, serta target penyerangan yang sangat bervariasi di ruang siber. Kemudian tantangan yang dihadapi oleh keamanan siber nasional yaitu karena kurangnya pengetahuan otoritas negara mengenai isu keamanan siber, tidak ada sistem yang aman di Indonesia, terdapat server internasional dari beberapa layanan internet, belum ada perundang-undangan yang membahas secara khusus penanganan dan pengaturan serangan siber, permasalahan administrasi lembaga keamanan siber, berulangnya insiden kejahatan siber, kurangnya pengetahuan mengenai risiko global serangan siber yang berpotensi melumpuhkan infrastruktur, serta kurangnya industri yang mengembangkan dan memproduksi perangkat keras terkait IT untuk memperkuat pertahanan kita di dunia siber.

Potensi Penguatan Keamanan Siber Di Indonesia Melalui Kerjasama Antara Indonesia Dan Australia

1. Urgensi Kerjasama Keamanan Siber Antara Indonesia Dan Australia

Kerjasama antara Indonesia dan Australia dalam bidang keamanan siber memiliki urgensi yang besar dan penting, termasuk dalam konteks peningkatan ancaman keamanan siber pada era digital sekarang ini. Acuan penting dalam konteks keamanan siber yakni GCI atau *Global Cybersecurity Index* yang merupakan sebuah referensi terpercaya untuk mengukur suatu komitmen negara-negara di dunia terhadap keamanan siber ditingkat global. *Global Cybersecurity Index* ini menggambarkan 82 pertanyaan yang berkaitan dengan komitmen keamanan siber dari setiap negara anggota dan untuk kerjasama multi pemangku kepentingan internasional dalam keamanan siber yang bertujuan untuk membangun sinergi antara inisiatif saat ini dan masa depan. Indonesia dan Australia sama-sama memiliki kepentingan bersama dan berkeinginan untuk mendorong penggunaan ruang siber yang terbuka, bebas, aman, dan damai, guna mendorong pertumbuhan ekonomi, melindungi keamanan nasional, dan mendorong stabilitas internasional.

Lalu pada periode 2018-2020, Indonesia sendiri menghadapi tantangan besar dalam keamanan siber, termasuk meningkatnya *ransomware, phising*, serta ancaman terhadap infrastruktur kritis. Situasi ini diperburuk oleh keterbatasan kapasitas teknis, sumber daya manusia, serta kerangka regulasi yang belum memadai yang dialami oleh Indonesia. Berdasarkan *Global Cybersecurity Index* yang diterbitkan oleh UN ITU, skor Indonesia pada tahun 2018 berada di angka 0,776, yang menempatkannya di peringkat 41 secara global. Hal ini menunjukkan bahwa Indonesia masih memiliki banyak ruang untuk memperbaiki kebijakan, kemampuan, dan kesadaran terkait keamanan siber. Indonesia memilih Australia sebagai mitra utama dalam memperkuat *cybersecurity* karena Australia memiliki infrastruktur keamanan siber yang lebih matang, pengalaman dalam menangani ancaman siber, serta keahlian teknis yang tinggi. Australia juga memiliki kebijakan dan regulasi keamanan siber yang kuat, termasuk peran aktif dalam forum internasional dan kerjasama di bidang siber, serta keunggulan Australia dibandingkan negara lain terletak pada pengalamannya dalam mengelola ancaman siber lintas negara, serta keunggulan teknologi dan riset di sektor keamanan siber yang dapat memberikan dukungan langsung bagi Indonesia dalam membangun kapasitas dan infrastruktur keamanannya.

Selanjutnya Kerja sama dengan Australia didorong oleh kebutuhan Indonesia untuk meningkatkan kesadaran, kapasitas teknis, dan kesiapan dalam keamanan siber. Sebagai perbandingan, Australia memiliki skor GCI yang jauh lebih tinggi, yaitu 0,890 pada tahun 2018, dengan peringkat 10 secara global, mencerminkan tingkat kesiapan dan kemampuan keamanan siber yang jauh lebih maju. Dengan pengalaman dan teknologi yang jauh lebih baik, Australia menjadi mitra strategis bagi Indonesia dalam transfer pengetahuan, pelatihan, dan pengembangan infrastruktur siber. Berdasarkan hasil dari persetujuan MoU pada tahun 2018 tersebut juga terdapat urgensi kerjasama antara Indonesia dan Australia mencakup dari dua pilar yaitu *capacity building* dan *cooperation*. *capacity building*, berfokus pada pengembangan kapasitas dan penguatan koneksi untuk meningkatkan keamanan siber dan meningkatkan kemampuan investigasi kejahatan dunia maya, sementara dalam evaluasi *cooperation*, berfokus pada kemitraan

antara berbagai pemangku kepentingan dalam bidang tersebut seperti melakukan pertukaran informasi dan berkoordinasi untuk merespon insiden siber. Urgensi kerjasama antara kedua negara tersebut yakni Indonesia dan Australia dibidang keamanan siber juga menjadi sangat penting karena ancaman siber yang semakin kompleks dan menyeluruh, yang dapat merusak ekonomi dan stabilitas nasional.

Urgensi kerjasama *capacity building* atau peningkatan kapasitas merupakan intrinsik dari tiga pilar pertama yakni hukum, teknis dan organisasi. Keamanan siber paling sering ditangani dari perspektif teknologi meskipun ada banyak implikasi sosial-ekonomi dan politik. Peningkatan kapasitas manusia dan kelembagaan sangat penting untuk meningkatkan kesadaran, pengetahuan, dan pengetahuan lintas sektor, untuk solusi sistematis dan tepat, dan untuk mempromosikan pengembangan profesional yang berkualitas. Peningkatan kapasitas dievaluasi berdasarkan jumlah penelitian dan pengembangan, program pendidikan dan pelatihan, serta profesional bersertifikat dan lembaga sektor publik. Peningkatan kapasitas juga termasuk kampanye kesadaran publik, kerangka kerja untuk sertifikasi dan akreditasi profesional keamanan siber, kursus pelatihan profesional dalam keamanan siber, program pendidikan atau kurikulum akademik, dan lain-lain. Pengembangan kapasitas keamanan siber inilah yang menjadi suatu urgensi yang tidak dapat diabaikan oleh Indonesia. Sebagai sebuah negara berkembang yang mempunyai tingkat konektivitas yang semakin meningkat serta populasi yang besar, dan Australia sebagai sebuah negara yang maju dengan peran yang kuat dalam bidang teknologi dan pengembangan inovasi, membuat kerjasama antara kedua negara tersebut menjadi sangat penting untuk memperkuat keamanan siber Indonesia, mengingat peran teknologi informasi yang memiliki peran semakin vital dalam perekonomian dan kehidupan sehari-hari. Tujuan utama dari program pengembangan kapasitas dalam kerjasama keamanan siber antara Indonesia dan Australia adalah untuk meningkatkan kemampuan sumber daya manusia dan institusi yang ada di Indonesia dalam menangani masalah ancaman siber, memperkuat kebijakan dan regulasi keamanan siber, serta membangun infrastruktur yang lebih aman dan tangguh. Program yang dilaksanakan ini bertujuan untuk memperkuat kapasitas teknis, pengetahuan, dan keterampilan praktis para pejabat pemerintah, para profesional keamanan siber, dan sektor swasta dalam menghadapi tantangan siber yang semakin kompleks. Didalam pelaksanaan pengembangan kapasitasnya pada tahun 2018, Indonesia dan Australia melaksanakan berbagai kegiatan-kegiatan seperti *workshop* ASPI dan Indonesia-Australia *digital forum*, kemudian diikuti dengan peluncuran Australia-Indonesia *digital network*. Selain itu terdapat juga berbagai pelatihan dan kunjungan, seperti *Cyber Boot Camp* dan pertemuan dengan ACSC, yang mana untuk memperkuat kapasitas Indonesia. Pada 2019, kerja sama berlanjut dengan seminar, workshop internasional, dan partisipasi BSSN dalam ACSC's ASEAN Capture the Flag serta kegiatan lainnya untuk meningkatkan pemahaman dan keterampilan siber. Pada 2020, Indonesia dan Australia memperkuat kerjasama melalui *Cyber Policy Dialogue*, pelatihan *International Cyber Law*, dan sesi berbagi untuk penyusunan Sistem Keamanan Siber Nasional atau SKSN, serta *Cybersecurity Training for*

MSME. Semua kegiatan ini tidak hanya memperkuat kapasitas dan ketahanan siber di kawasan Indo-Pasifik, tetapi juga membantu mengatasi perbedaan tingkat kematangan keamanan siber antara kedua negara dengan berbagi keahlian, teknologi, dan pengalaman.

Urgensi kerjasama atau *cooperation* merupakan proses memerangi kejahatan dunia maya yang merupakan masalah global dan tidak terbatas pada batasan negara atau perbedaan sektoral. Dengan demikian, penanggulangan kejahatan dunia maya memerlukan pendekatan multi-pihak kepentingan dengan masukan dari semua sektor dan disiplin ilmu termasuk perjanjian bilateral dan multilateral, partisipasi forum/asosiasi internasional, kemitraan publik-swasta, kemitraan antar Lembaga, praktik terbaik, dan lain-lain. Kerjasama yang lebih besar dapat memungkinkan pengembangan kemampuan keamanan siber yang jauh lebih kuat, membantu mencegah ancaman *online* atau daring yang berulang dan terus menerus serta memungkinkan dilakukannya penyelidikan, penangkapan, dan penuntutan para pelaku atau agen kejahatan yang lebih baik. Dari kerjasama bilateral antara Indonesia dan Australia ini terdapat ruang lingkup kerjasama dalam hal berbagi informasi dan praktik terbaik, peningkatan kapasitas dan penguatan koneksi, ekonomi digital dan kejahatan siber serta dialog kebijakan siber sangat penting untuk menunjukkan komitmen berkelanjutan kedua belah pihak Kemudian adapun area kejahatan siber terkait lembaga penegak hukum Indonesia dan Australia dalam memerangi tantangan kejahatan siber. Kemudian dalam hal ini, Australia berkontribusi dalam kerjasama keamanan siber dengan Indonesia melalui pelatihan teknis, pengembangan kapasitas, dan berbagi teknologi. Melalui ACSC, Australia menyediakan beberapa pelatihan seperti *Cyber Boot Camp* dan mendukung pengembangan kebijakan, termasuk Strategi Keamanan Siber Nasional atau SKSN.

2. Implementasi Kerjasama Indonesia Dan Australia

Implementasi kerjasama antara Indonesia dan Australia didalam kerjasamanya merupakan hasil dari analisis urgensi dan juga perwujudan dari dasar nilai kerjasama baik Indonesia maupun Australia. Implementasi ini adalah wujud dari kolaborasi yang erat antara dua negara yang memiliki pemahaman yang sama akan pentingnya keamanan siber sebagai aset strategis. Kerjasama ini juga merupakan cerminan dari nilai-nilai dasar persahabatan dan kerjasama yang telah lama terjalin antara Indonesia dan Australia. Dengan memanfaatkan keahlian dan sumber daya masing-masing, kedua negara tersebut membangun kerangka kerja yang kokoh untuk menyatukan upaya dalam menghadapi tantangan *cyber* yang semakin beragam. Dari perspektif liberalisme interdependensi dalam hubungan internasional, implementasi ini didasari dari adanya kepentingan dari kedua negara yang membutuhkan satu sama lainnya. Kerjasama ini tidak hanya didorong oleh kepentingan keamanan nasional masing-masing negara, tetapi juga oleh nilai-nilai universal tentang pentingnya menjaga stabilitas global dan keamanan bersama serta adanya kebutuhan dalam menumbuhkan kegiatan ekonomi. Dalam kerangka liberalisme, kerjasama antara Indonesia

dan Australia juga menggambarkan komitmen kedua negara dalam mempromosikan ruang siber yang terbuka dan keamanan siber sebagai bagian integral dari agenda global untuk mencapai perdamaian dan keamanan yang berkelanjutan.

Keterlibatan keduanya dalam membangun dan memperkuat keamanan siber Indonesia menunjukkan bahwa tantangan keamanan siber tidak dapat diselesaikan secara unilateral, tetapi memerlukan kerjasama antar negara. Dengan mengakui saling ketergantungan dalam menghadapi ancaman siber, Indonesia dan Australia memperkuat jaringan kerjasama internasional yang dapat membantu mengatasi tantangan bersama dalam domain keamanan siber. Selain itu, implementasi kerja sama ini juga mencerminkan komitmen kedua negara untuk membangun kemitraan yang saling menguntungkan dan berkelanjutan. Dengan saling memanfaatkan keahlian dan sumber daya yang dimiliki, baik Indonesia maupun Australia dapat mencapai hasil yang lebih optimal dalam upaya bersama mereka untuk meningkatkan ketahanan siber.

Dalam pengimplementasian kerjasama antara Indonesia dan Australia di bidang keamanan siber ini terdapat serangkaian langkah atau kegiatan yang konkret dalam mengkoordinasikan serta melaksanakan kerjasama ini. Pada tahun 2018, Indonesia dan Australia melakukan serangkaian kegiatan kerjasama dalam bidang keamanan siber. Dari implementasi kerjasama MoU *on Cyber Cooperation* antara Indonesia dengan Australia dengan ruang lingkup yang meliputi *sharing of information and best practice, capacity building and strengthening the connection, digital economy, cybercrime* dan *cyber dialogue*, kepala BSSN yakni Hinsa Siburian menanggapi bahwa Indonesia berterima kasih dan sangat mengapresiasi karena MoU tersebut telah memberi banyak manfaat bagi peningkatan kapasitas siber Indonesia melalui beberapa kegiatan sesuai dengan *work plan* MoU seperti *cyber bootcamp, workshop, cyber business connection, best practice sharing, fellowship program* dan sebagainya. Tobias Freakin sebagai duta besar urusan siber pemerintahan Australia juga menyampaikan kegembiraan atas terlaksana dan keberhasilan dari kegiatan dari implementasi MoU tersebut serta dia berharap Australia dapat memberikan program "*cyber security long term award,*"

KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa Kerjasama antara Indonesia dan Australia dalam bidang keamanan siber memiliki urgensi yang besar dan penting. Yang mana terdapat acuan penting dalam konteks keamanan siber yakni GCI atau *Global Cybersecurity Index* yang merupakan sebuah referensi terpercaya untuk mengukur suatu komitmen negara-negara di dunia terhadap keamanan siber ditingkat global. Indonesia dan Australia sama-sama memiliki kepentingan bersama dan berkeinginan untuk mendorong penggunaan ruang siber yang terbuka, bebas, aman, dan damai, guna mendorong pertumbuhan ekonomi, melindungi keamanan nasional, dan mendorong stabilitas internasional, serta kedua negara tersebut memiliki komitmen tinggi dalam kelima pilar indeks. Indonesia memilih Australia

sebagai mitra utama dalam memperkuat *cybersecurity* karena Australia memiliki infrastruktur keamanan siber yang lebih matang, pengalaman dalam menangani ancaman siber, serta keahlian teknis yang tinggi. Australia juga memiliki kebijakan dan regulasi keamanan siber yang kuat, termasuk peran aktif dalam forum internasional dan kerjasama di bidang siber, serta keunggulan Australia dibandingkan negara lain terletak pada pengalamannya dalam mengelola ancaman siber lintas negara, serta keunggulan teknologi dan riset di sektor keamanan siber yang dapat memberikan dukungan langsung bagi Indonesia dalam membangun kapasitas dan infrastruktur keamanannya.

Implementasi kerjasama antara Indonesia dan Australia di bidang keamanan siber ini terdapat serangkaian langkah atau kegiatan yang konkret dalam mengkoordinasikan serta melaksanakan kerjasama ini. Didalam pengimplementasiannya, kerjasama keamanan siber antara Indonesia dan Australia dilaksanakan melalui mekanisme-mekanisme yang melibatkan koordinasi secara langsung antara instansi terkait, seperti BSSN di Indonesia dan ACSC di Australia, dengan dukungan tim teknis dari kedua negara. Dalam hal ini juga memiliki ruang lingkup kerjasama dalam hal berbagi informasi dan praktik terbaik, peningkatan kapasitas dan penguatan koneksi, ekonomi digital dan kejahatan siber serta dialog kebijakan siber yang sangat penting untuk menunjukkan komitmen berkelanjutan dari kedua belah pihak. Yang mana jika dilihat dari indikator keberhasilan serta dampak positif yang dihasilkan dari kerjasama ini, kerjasama ini diharapkan dapat terus berlanjut kedepannya, sehingga dapat menciptakan ekosistem siber yang aman dan kondusif bagi pertumbuhan berbagai sektor di kawasan, terutama yang terkait dengan infrastruktur informasi kritis nasional dan ekonomi digital.

DAFTAR PUSTAKA

Ariyanti, V. dan Fathi, R.”Tantangan Keamanan Siber di Indonesia pada Tahun 2018,” *Jurnal Keamanan Siber Nasional*. Vol.5 No.2 (2019)

Asani.”Apa itu Cyber Crime-Pengertian,Pelaku, dan Alasan Terjadi.” Asani.co.id (2023) internet. 5 November 2024, https://asani.co.id/blog/cyber-crime/#Siapakah_Pelaku_Cyber_Crime

Badan Pusat Statistik, *Statistik Telekomunikasi Indonesia.* Jakarta: Badan Pusat Statistik, 2018.

Badan Siber dan Sandi Negara, *Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019*. Jakarta: Badan Siber dan Sandi Negara, 2018.

Bambang Supriyadi.”Persepsi Bersama Indonesia-Australia dalam Hibah Dana dan Peralatan Investigasi Cyber Crime dari Australia Kepada Indonesia,” *Journal of International Relations* Vol.3 No.1 (2017)

BSSN.”Bahas Tindak Lanjut Kerja Sama Keamanan Siber, Kepala BSSN Gelar Diskusi dengan Dubes Urusan Siber Australia.” bssn.go.id (2020) internet. 18 Desember 2024, https://www.bssn.go.id/bahas-tindak-lanjut-kerja-sama-keamanan-siber-kepala-bssn-gelar-diskusi-dengan-dubes-urusan-siber-australia/

BSSN.”Mengenali serangan siber global dan nasional melalui laporan tahunan honeynet project BSSN-IHP tahun 2018.” Bssn.go.id (2019) internet. 11 Juni 2024, https://www.bssn.go.id/mengenali-serangan-siber-global-dan-nasional-melalui-laporan-tahunan-honeynet-project-bssn-ihp-tahun-2018/

BSSN.”Press Release Indonesia dan Australia Sepakat Jalin Kerjasama di Bidang Siber.” bssn.go.id (2018) internet. 10 Juni 2024, https://www.bssn.go.id/press-release-indonesia-dan-australia-sepakat-jalin-kerjasama-di-bidang-siber/

BSSN.”Tentang BSSN.” Bssn.go.id (2021) internet. 18 Desember 2024, https://www.bssn.go.id/tentang-bssn/

DFAT.”About us.” Dfat.gov.au (2024) internet. 18 Desember 2024, https://www.dfat.gov.au/about-us

Dfat.gov.au.” Agreement Between the Republic of Indonesia and Australia on the Framework for Security Cooperation.” Dfat.gov.au (2015) internet. 1 Oktober 2024, https://www.dfat.gov.au/geo/indonesia/agreement-between-the-republic-of-indonesia-and-australia-on-the-framework-for-security-cooperation#:~:text=The%20Agreement%20Between%20the%20Republic%20of%20Indonesia%20and%20Australia%20on

Elva Azzahra Puji Lestari.”Complex Interdependence Between Indonesia-Australia Through Cybersecurity Cooperation Post-Indonesia-Australia Cyberwar in 2013,” *Jurnal Hubungan Internasional*. Vol.9 No.2 (2020)

Handrini Ardiyanti. "Cyber-Security dan Tantangan Pengembangannya di Indonesia," *Jurnal Politica*. Vol.5 No.1 (2014)

Ramadhani, Nibras. Hikam, Muhammad. dan Munabari, Fahlesa.”The Joint Efforts of Indonesian and Australian Governments in Countering Terrorism: Intelligence Cooperation,” *Deviance Jurnal Kriminologi*. Vol.5 No.1 (2021)

Ratna Christianingrum dan Ade Nurul Aida, *Tantangan Penguatan Keamanan Siber Dalam Menjaga Stabilitas Keamanan Nasional*. Jakarta: Pusat Kajian Anggaran Badan Keahlian DPR RI, 2021

Verizon.”*Data Breach Investigations Report 2020*.” Verizon.com (2020) internet. 5 November 2024, https://www.verizon.com/business/en-

gb/resources/reports/2020-data-breach-investigations-report.pdf?msockid=3aa4f47c28b06b1c0a0de08429746a44