# ANALISIS KERJASAMA *CYBER SECURITY* INDONESIA-AUSTRALIA DALAM MENANGANI KEJAHATAN SIBER DI INDONESIA

**[1]Muhamad Rizki Hapizon, [2]Khairur Rizki, [3]Mahmuluddin**

[1]Program Studi Hubungan Internasional, Universitas Mataram, NTB, Indonesia

[2]Program Studi Hubungan Internasional, Universitas Mataram, NTB, Indonesia

[3]Program Studi Hubungan Internasional, Universitas Mataram, NTB, Indonesia

E-mail : rizkihapizon06@gmail.com

***ABSTRACT***

*This paper aims to explore the analysis of cyber security cooperation between Indonesia and Australia in dealing with cyber crime in Indonesia. Cybercrimes that attack various countries around the world pose a serious threat to security. Indonesia in dealing with this problem cooperates with Australia, which basically the relationship between the two countries was not harmonious before. Australia has committed many violations against Indonesia, including cybcrime. By using the concept of national interest and the concept of Cyber Security as an analytical knife, this paper will dissect the reasons why Indonesia cooperates with Australia, how this cooperation occurs, the form of cooperation that is established and what kind of influence the resulting cooperation has for Indonesia in dealing with cybercrime.*

*Keywords: Cybercrime, Cyber Security, Indonesia, Australia, Cooperation, National Security*

**ABSTRAK**

Tulisan ini bertujuan untuk melakukan eskplorasi terkait dengan Analisis Kerjasama kemanan siber yang dilakukan oleh Indonesia dan Australia dalam menangani kejahatan siber di Indonesia. Kejahatan siber yang menyerang berbagai negara diseluruh dunia membawa ancaman yang serius bagi keamanan. Indonesia dalam menghadapi masalah ini menjalin kerjasama dengan Australia yang pada dasarnya hubungan antar kedua negara sebelumnya tidak harmonis. Banyak sekali pelanggaran yang dilakukan oleh Australia terhadap Indonesia termasuk berupa aksi kejahatan siber. Dengan menggunakan konsep kepentingan nasional dan konsep *Cyber Security* sebagai pisau analisis, tulisan ini akan membedah alasan mengapa Indonesia menjalin kerjasama dengan Australia, bagaimana kerjasama ini terjadi, wujud dari kerjasama yang terjalin serta seperti apa pengaruh yang dihasilkan dari terjalinnya kerjasama tersebut bagi Indonesia dalam menangani kejahatan siber.

Kata Kunci : Kejahatan siber, *Cyber security*, Indonesia, Asutralia, Kerjasama, Keamanan Nasional

## Pendahuluan

Perkembangan kondisi dunia internasional yang semakin kompleks diiringi dengan berkembangnya teknologi yang semakin modern akibat dari arus globalisasi yang tidak terbendung membuat setiap negara mulai berlomba-lomba untuk menjadikan negara mereka menjadi negara yang maju dalam berbagai bidang, baik dalam bidang politik, ekonomi, sosial budaya, bahkan dalam bidang pertahanan dan keamanan. Perkembangan teknologi informasi dan komunikasi atau internet telah membawa dampak yang sangat signifikan dalam kehidupan sehari-hari. Perkembangan teknologi yang sangat pesat ini memunculkan beberapa era kemajuan teknologi diantaranya dari era Revolusi Industry ke-1 sampai yang terbaru yaitu Revolusi Industri ke-4.[1] Negara di berbagai belahan dunia telah memasukkan teknologi sebagai unsur yang penting dalam setiap aspek kenegaraan mereka. Peran teknologi yang semakin krusial memaksa setiap negara untuk menggunakan teknologi sebagai syarat agar mereka bisa bertahan dalam dunia internasional.[2]

Peran teknologi yang sudah masuk kedalam semua ranah seperti pendidikan, perbankan, serta pertahanan dan keamanan menjadi bukti bahwa teknologi sudah menguasai setiap aspek kehidupan di dunia. Perkembangan teknologi yang semakin maju walaupun sangat berpengaruh dalam membawa banyak dampak positif, tidak dapat dipungkiri juga diikuti dengan tingkat kejahatan yang semakin modern. Bahkan kejahatan yang biasanya dilakukan dengan interaksi langsung kini sudah bertransformasi menjadi *cybercrime*. Dengan hadirnya masalah ini kemudian menjadi isu penting yang harus dihadapi dalam hubungan internasional, karena jenis kejahatan ini dapat dilakukan oleh siapa saja, baik itu individu, kelompok, *Multinational Corporation* (MNC), maupun sebuah negara sekalipun, *cybercrime* dapat menyerang siapa saja yang bersifat nasional dan transnasional.[3]

---

[1] Meilani Teniwut, Pengertian Revolusi Industri 4.0 ini Persiapan Indonesia, *mediaindonesia.com*, 26 Oktober 2022, https://mediaindonesia.com/

[2] Hendro Setyo Wahyudi, Teknologi dan Kehidupan Masyarakat, *Jurnal Analisa Sosiologi*, vol.3 no.1 April 2014, p.15, https://media.neliti.com/

[3] Supanto, Perkembangan Kejahatan Tekonologi Informasi (Cyber Crime) dan Antisipasinya Dengan Penal Policy, *Yustisia Jurnal Hukum*, Vol.5 No.1, Juli 2018, pp.43-45

Dalam konferensi anggota PBB tentang kejahatan transnasional terorganisir tahun 2010 mengidentifikasi *cybercrime* sebagai salah satu dari lima *New Emerging Crimes* bersama dengan kejahatan lain seperti kejahatan terhadap lingkungan, kejahatan perdagangan organ dan obat-obatan, kejahatan terkait identitas dan perdagangan kekayaan budaya dan pembajakan.[4] Hal ini menjadi bukti bahwa *cybercrime* telah menjadi permasalahan yang mendapat perhatian serius dari dunia. Terdapat begitu banyak jenis dari kejahatan siber (*Cybercrime*) yang tindakan kejahatannya disebut dengan *cyberattacks* (serangan siber). Jenis-jenisnya antara lain seperti tindakan Spionase, *Hacking, Cyber Trafficking, Cyber Terrorism* dan lain-lain.[5] *Cybercrime* yang hadir tidak luput menyerang Indonesia, ID-SIRTII (*Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center)* juga merilis laporan tahunan keamanan siber dalam acara *National Security Days* di Bandung pada November 2014.[6] Menurut laporan tahunan ID-SIRTII, Indonesia mendapat serangan siber lebih dari 42 juta sepanjang 2014 dan berisiko besar terkena dampak keamanan siber yang lemah.[7]

laporan dari CIA *(Central Intellegency Agency)* sendiri, akibat adanya *cybercrime* yang ada di Indonesia, telah membuat Indonesia mengalami kerugian sebesar 1,2 % atau sekitar 454 miliar tahun 2021.[8] Indonesia sebagai salah satu negara dengan kasus kejahatan siber di dunia harus serius meminimalisir tingkat kejahatan siber yang semakin berkembang. Salah satu upaya yang dilakukan Indonesia adalah dengan menjalin kerjasama strategis di bidang siber, dan negara yang memiliki tingkat keamanan siber yang maju yaitu Australia. Australia menjadi *partner* Indonesia dalam menangani kejahatan siber mengingat Australia merupakan negara yang dapat terbilang maju dalam urusan *cyber security*. Upaya kerjasama penanganan *cybercrime* Australia bagi Indonesia diharapkan dapat mengatasi permasalahan keamanan yang serius akibat kemajuan

---

[4] United Nations, Conference of the Parties to the United Nations Convention against Transnational Organized Crime, 2010

[5] Kominfo, Kenali 4 Jenis Kejahatan Siber, *diskominfo kotabogor*, 20 Juni 2019, https://kominfo.kotabogor.go.id/index.php/post/single/740

[6] IDSIRTII, *Laporan analisis Malware*, https://www.idsirtii.or.id/

[7] Ahmad Saudi, Kejahatan Siber Transnasional dan Strategi Pertahanan Siber Indonesia, *Jurnal Demokrasi dan Otonomi Daerah*, Vol. 16 No.3, September 2018, p.165

[8] Dwika Intishar Safara, Globalisasi dan Permasalahan Keamanan Internasional Akibat Cyber Crime di Indonesia, *berau.prokal.co*, 18 Juli 2022, https://berau.prokal.co/read/news/71433-globalisasi-dan-permasalahan-keamanan-internasional-akibatcyber-crimedi indonesia.html

teknologi yaitu *cybercrime*, baik pada saat ini dan yang akan datang. Walaupun demikian Australia merupakan negara yang memili sejarang kurang bagus dengan Indonesia, ini dikarenakan banyak kasus kejahatan yang dilakukan oleh Australia terhadap Indonesia termasuk kejahatan siber, hal ini menimbulkan pertanyaan kepada penulis mengapa Indonesia kembali melakukan kerjasama dengan Australia.

## Kerangka Teori

Untuk menjawab bagaimana mengapa terjadinya kerjasama *cyber security* Indonesia-Australia dalam menanganai kejahatan siber di Indonesia, penulis menggunakan konsep keamanan nasional dan *Cyber Security*.

### 1. Kepentingan Nasional (*National Interest*)

Kepentingan nasional *(national interest)* adalah konsep yang paling populer dalam analisa hubungan internasional, baik untuk mendeskripsikan, menjelaskan, meramalkan, maupun menganjurkan perilaku internasional.[9] Teori ini menjelasakan bahwa untuk kelangsungan hidup suatu negara maka negara harus memenuhi kebutuhan negaranya dengan kata lain yaitu mencapai kepentingan nasionalnya. Dengan tercapainya kepentingan nasional maka negara akan berjalan dengan stabil, baik dari segi politik, ekonomi, sosial, maupun pertahanan keamanan. Artinya, jika kepentingan nasional terpenuhi maka negara akan tetap survive. Kepentingan nasional merupakan tujuan mendasar dan faktor paling menentukan yang memadu para pembuat keputusan dalam merumuskan politik luar negeri.[10] Kepentingan Nasional *(National Interest)* adalah tujuan-tujuan yang ingin dicapai sehubungan dengan kebutuhan bangsa/negara atau sehubungan dengan hal yang dicita-citakan. Dalam hal ini kepentingan nasional yang relatif tetap dan sama diantara semua negara/bangsa adalah keamanan (mencakup kelangsungan hidup rakyatnya dan kebutuhan wilayah) serta kesejahteraan. Kedua hal pokok ini yaitu keamanan (*Security*) dari kesejahteraan (*Prosperity*). Hubungan Indonesia

[9] Gisella Linardy, Kerjasama Bilateral Indonesia-Australia Dalam IA-CEPA, *Jurnal Sentris Diplomasi*, Vol.2 No.1, Oktober 2021, pp.30-31

[10] Astari Marisa, Hubungan Bilateral Indonesia-Australia: Kepentingan Australia Dalam Meratifikasi IA-CEPA tahun 2019, *Jurnal Transborders*, Vol.4 no.1, Desember 2020, pp.29-30

dan Australia terdiri dari persepsi akan saling membutuhkan demi memenuhi kepentingan nasional, hal ini pada akhirnya menyebabkan Indonesia terkesan mengesampingkan fakta bahwa Australia pernah melakukan tindakan kejahatan siber terhadap Indonesia.

**2. Konsep *Cyber Security***

*Cyber-security* nerupakan dimensi keempat dalam konsep keamanan kontemporer selain dari *External security, Internal Security dan Environtmental Security* dalam buku *Cyber Politic in International Relation.*[11]adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna. Organisasi dan aset pengguna dalam *cyber-security* termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya. *Cyber-security* juga merupakan upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan *cyber*.[12]

Upaya peningkatan keamanan siber yang dilakukan oleh negara merupakan salah satu upaya yang berkaitan dengan tujuan menjaga keamanan nasional. Hal tersebut dikarenakan kebijakan dan strategi pertahanan dan keamanan negara bersifat dinamis dan dapat berubah mengikuti perkembangan fenomena dan isu global yang berpotensi menjadi ancaman nasional. Secara spesifik, keamanan siber kini telah mulai menjadi perhatian dan strategi keamanan negara-negara di dunia. Perubahan strategi keamanan negara yang merambah dunia maya disebabkan semakin berkembang dan meluasnya kejahatan siber dengan memanfaatkan perkembangan teknologi informasi dan komunikasi saat ini. Hal ini juga dikarenakan dalam beberapa sektor, negara telah menggunakan jaringan internet sebagai basis dari kontrolnya sehingga akan menjadi kelemahan apabila tidak terdapat kebijakan terkait keamanan siber yang melindungi

---

[11] Nazli Choucri, Cyberpolitics in International Relations, *Cambridge : MIT Press,* (2012): p.43

[12] Handrini Ardiyanti, Cyber Secutity dan Tantangan Pengembangan di Indonesia, *Badan Riset Inovasi Nasional* Vol.3 No.1, Agustus (2014), pp.98-99 https://www.researchgate.net

## Metodologi Penelitian

Penelitian memiliki jenis yang berbeda, dibedakan berdasarkan permasalahan dan tujuan. Penelitian yang bertujuan menjelaskan pengaruh suatu variabel terhadap variabel yang lain disebut penelitian eksplanatif,[13] sedangkan penelitian yang bertujuan mendeskripsikan dan menganalisis fenomena dan karekteristiknya disebut penelitian deskriptif analisis[14] Penelitian deskriptif analisis biasanya dilakukan dengan mendapatkan informasi yang cukup tentang masalah penelitian mengenai apa atau bagaimana tentang suatu fenomena.[15] Terkait dengan penelitian penulis, penelitian ini merupakan penelitian jenis deskriptif analisis, yang bertujuan untuk mendeskripsikan serta menganalisis fenomena dan karakteristik dari fenomena tersebut, tepatnya menjelaskan mengapa dan bagaimana kerjasama *Cyber Security* Indonesia-Australia dalam menangani kejahatan siber di Indonesia.

Teknik pengumpulan data yang digunakan dalam penelitian ini dalam mencari data merupakan teknik studi pustaka yang merupakan teknik pengumpulan data dengan cara sebuah teknik pengumpulan data yang bersumber dari refrensi literatur baik berupa jurnal, buku, artikel, ataupun pendapat peneliti sebelumnya mengenai tema yang diusung. Sedangkan teknik analisis data yang digunakan dalam penelitian ini adalah teknik analisis yang berasal dari Milles dan Huberman, yang mana teknik analisis data ini memiliki 4 tahapan yaitu, pengumpulan data, reduksi data, penyajian data dan kesimpulan. Keempat tahapan tersebut saling terhubung satu sama lain.

## Hasil dan Pembahasan

### 1. Kejahatan Siber di Indonesia dan Latar Belakang Kerjasama Dengan Australia

Indonesia merupakan negara terbesar di kawasan Asia Tenggara yang memiliki potensi ekonomi,keamanan serta politik kawasan regional. Tentu saja masalah kejahatan siber menjadi sebuah masalah serius seiring banyaknya akses dalam bidang ekonomi, politik, pertahanan negara melalui jaringan sistem internet, sehingga hal ini menimbulkan masalah yang serius di terutama dalam keamanan akses data tersebut. Tidak hanya di

---

[13] U. S. Bakry, *Pedoman Penulisan Skripsi Hubungan Internasional*, (Yogyakarta: Deepublish 2016), p. 26.

[14] H. Nassaji, 'Qualitative and Descriptive Research: Data Type Versus Data Analysis,' *Language Teaching Research*, No. 2, Vol. 19, Mei 2015, p. 129.

[15] "*Descriptive Research Designs: Types, Examples & Methods," Formpl*, https://www.formpl.us

negara Indonesia tetapi negara-negara lain juga memiliki masalah yang sama yaitu *cybercrime* ini. Keamanan siber adalah kebutuhan nyata dan mendesak karena pengaruhnya berpotensi merusak atau mengganggu kehidupan, negara, dan bahkan seluruh dunia.[16]

ID-SIRTII merilis laporan tahunan keamanan siber dalam acara National Security Days di Bandung pada November 2014. Menurut laporan tahunan ID-SIRTII (*Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center*) tersebut, Indonesia yang mendapat serangan siber lebih dari 42 juta sepanjang 2014 dan berisiko besar terkena dampak keamanan siber yang lemah.[17]

Kasus serangan siber selanjutnya seperti beberapa tahun yang lalu sejumlah pemberitaan yang menyangkut masalah penyadapan yang dilakukan pihak asing kembali mengemuka, setelah sebelumnya pada akhir bulan Oktober 2013 Indonesia dikejutkan dengan sejumlah pemberitaan tentang tindakan Australia yang terbukti telah melakukan penyadapan terhadap sejumlah pejabat tinggi Pemerintah Indonesia, termasuk penyadapan terhadap Presiden Susilo Bambang Yudhoyono. Nama Indonesia kembali muncul dalam pemberitaan terkait skandal penyadapan oleh Badan Keamanan Nasional Amerika Serikat atau NSA (*No Security Agency*). Isu tersebut dimuat dalam harian The New York Time yang dilansir tanggal 15 Februari 2014, yang dibocorkan oleh mantan kontraktor NSA Edward J Snowden.[18]

Indonesia juga menjadi sasaran penyadapan yang dilakukan oleh Amerika Serikat (AS). Penyadapan terhadap Indonesia dilakukan NSA *(National Security Agency)* Amerika bekerja sama dengan Direktorat Sandi Pertahanan (DSD) Australia. Sebagai contoh, NSA-AS meminta bantuan DSD Australia untuk mematai-matai Indonesia pada waktu Konferensi Perubahan Iklim PBB yang diadakan di Bali, tanggal 3–14 Desember

---

[16] Leo T Panjaitan, Analisis Penanganan *Carding* dan Perlindungan Nasabah Dalam Kaitannya Dengan Undang-Undang Informasi dan Transaksi Elektronik no.11 Tahun 2008, *Jurnal Telekomunikasi dan Komputer*, Vol.3 no.1 Mei 2012, pp.41-42

[17] Putri Azaria Matondang, Kerja sama Internasional Indonesia-Australia: Studi Kasus Kesepakatan Perundingan Indonesia-Australia Comprehensive Economic Partnership Agreement (IA-CEPA) Tahun 2010-2018 (Universitas Islam Indonesia, 2021) p.15-17

[18] Adhi Maulana, 10 Dosa Besar NSA yang Dibocorkan Edward Snowden, *Liputan6*, 5 Maret 2015, https://www.liputan6.com/tekno/read/2185425/10-dosa-besar-nsa-yang-dibocorkan-edward-snowden

2007. Penyadapan kala itu dilakukan Amerika dan Australia untuk memantau struktur jaringan komunikasi keamanan Indonesia. Selain melakukan penyadapan pada waktu Konferensi Perubahan Iklim, DSD Australia juga melakukan penyadapan terhadap komunikasi Presiden Susilo Bambang Yudhoyono (SBY) dan para pemimpin Indonesia lainnya.[19]

Kejahatan dunia maya lainnya yang akhir-akhir ini sering dilakukan adalah *carding*. *Carding* atau yang bisa disebut juga *credit card fraud* (penipuan kartu kredit).[20] . Kasus *carding* di Indonesia bermunculan ketika terjadi *Booming* internet di era tahun 2000-an. Beberapa kota seperti Jakarta, Bandung dan Yogyakarta menjadi pusat-pusat carder dalam melancarkan aksi pencurian data kartu kredit. Aksi-aksi *cybercrime* ini mengakibatkan pada tahun 2004, transaksi online yang berasal dari IP *(Internet Protocol)* Indonesia diblokir oleh dunia internasional.[21] Dari kasus-kasus *cyber-crime* khususnya *carding* tersebut yang benar-benar diproses di pengadilan di Indonesia dapat dihitung dengan jari. Sangat jarang muncul ke media massa para carder dijerat dengan hukum yang setimpal dengan perbuatannya. Serangan siber yang menyerang Indonesia berjenis *ransomware*. *Ransomware* adalah sebuah jenis malicious *software* atau *malware* yang menyerang komputer korban dengan cara mengunci komputer korban atau meng-*encrypt* semua file yang ada sehingga tidak bisa diakses kembali.[22] Situasi keamanan siber yang lemah juga dilihat dalam kurun waktu 2016-2022.[23] Lemahnya *cyber security* Indonesia sendiri dapat terlihat dari banyaknya kejadian kejahatan internet yang terjadi di Indonesia mulai dari permasalahan peretasan data di dunia perbankan seperti peretasan Bank Indonesia tahun 2022, peretasan data rumah sakit Dharmais dan rumah sakit Harapan Kita tahun 2017, peretasan data alumni Universitas Brawijaya tahun 2022 dan kasus-kasus

---

[19] Kominfo, Empat Operator Seluler di Indonesia Disebut Dalam Dokumen Penyadapan, *kominfo.go.id*, 28 Maret 2019, https://www.kominfo.go.id/

[20] Ardela Nabila, Ada *Carding* Ini 8 Modus Kejahatan Kartu Pembayaran yang Perlu Diwaspadai, *Parapuan.co*, 26 Juni 2022, https://www.parapuan.co/

[21] Acer Indonesia, Kebocoran Data (*Data leakage*) kenali Penyebab dan Dampaknya, 14 Juli 2022, https://commercial.acerid.com/

[22] UPT TIK, Mengenal Ransomware dan Pencegahannya, *Upttik.co*, 4 September 2017, https://upttik.undiksha.ac.id/mengenal-ransomware-dan-pencegahannya/

[23] Rezky Yayang, Waspada Kejahatan Siber di Era Serba Daring, *Makarta Bakti Negara*, 5 Maret 2023, https://lan.go.id/?p=13415

lainnya.[24] Bahkan terdapat sekitar 175 negara di mana setelah di investigasi, Indonesia menjadi negara yang berkontribusi terbanyak sebesar 38% total dari sasaran bentuk tindakan hacking yang ada di internet. Adapun menurut laporan dari CIA (*Central Intellegency Agency*) sendiri, akibat adanya *cybercrime* yang ada di Indonesia, telah membuat Indonesia mengalami kerugian sebesar 1,2 % atau sekitar 454 miliar tahun 2021.[25]

Latar belakang Indonesia menjalin kerjasama kemanan siber dengan Australia terdiri dari 5 alasan antara lain:

Pertama, pemerintahan Indonesia melalui BSSN memiliki tujuan untuk memenuhi salah satu pilar dalam GCI, yaitu kemitraan nasional dan internasional serta untuk mempromosikan kemitraan dan menyediakan kerangka kerjasama dalam bidang siber. Baik Indonesia dan Australia terlibat dalam kerjasama yang saling menguntungkan dengan poin-poin sebagai berikut: a) Berbagi informasi dan best practice; b) Peningkatan kapasitas dan penguatan koneksi; c) Kerjasama dalam bidang ekonomi digital; dan d) Penanganan kejahatan siber (Biro Hukum dan Hubungan Masyarakat, 2018).[26] Kerjasama ini berlanjut hingga pertemuan ke-3 Dialog Kebijakan Siber Indonesia-Australia pada tanggal 2 September 2020. Dialog dihadiri oleh beberapa petinggi negara dari kedua belah pihak dengan tujuan untuk membicarakan kerjasama siber dan kemitraan kedua negara dalam bidang keamanan siber. Dialog antar kedua negara ini terjadi akibat semakin meningkatnya serangan siber di seluruh dunia yang terjadi pada masa pandemi Covid-19.[27]

Kedua, kerjasama siber antar kedua negara yang tetap berlanjut juga dipengaruhi oleh kedekatan wilayah serta ancaman yang sama yang dihadapi oleh keduanya berupa kejahatan siber yang merugikan pertahanan dan ekonomi kedua negara sehingga menutut

---

[24] Polri, Kejahatan Siber di Indonesia Naik Berkali-kali Lipat, *pusiknas.polri.id*, 10 Agustus 2022, https://pusiknas.polri.go.id/

[25] Data Indonesia, Kerugian Kejahatan Siber Diproyeksi 844 Triliun Tahun 2022, *dataindonesia.id*, 5 Desember 2022, https://dataindonesia.id/

[26] Muhammad Prakoso Aji, Sistem Keamanan Siber dan Kedaulatan Data di Indonesia Dalam Perspektif Ekonomi Politik (Studi Kasus perlindungan Data Pribadi), *Jurnal Politica*, Vol.13 No.2, Mei 2022, pp.220-221

[27] BSSN, BSSN Inisiasi Lanutan Kerjasama Keamanan Siber Indonesia-Australia Dalam 3rd Indonesia-Australia Cyber Policy Dialogue, *bssn.go.id*, 2 September 2020, https://bssn.go.id/

mereka untuk tetap saling menjaga hubungan baik.[28] Australia dalam hal ini membutuhkan Indonesia sebagai "negara penyangga" dari kemungkinan munculnya gangguan keamanan dari utara. Misalnya, membendung aliran kejahatan transnasional seperti penyelundupan narkotika, perdagangan manusia, imigran ilegal, dan lain sebagainya. Dengan demikian, dari pandangan geopolitik Australia, Indonesia merupakan mitra utara untuk menangkal segala ancaman kawasan. Jaringan terorisme, pembajakkan, penyelundupan hingga kejahatan siber harus melalui jalur utara yang mana Indonesia adalah tameng terakhir terpenting bagi Australia untuk menyaring segala bentuk ancaman keamanan.[29] Sebaliknya, Indonesia memerlukan Australia untuk bantuan teknis dan keuangan dalam operasi-operasi menjaga keamanan dan stabilitas kawasan dari tindak kejahatan transnasional. Salah satu bukti dari tingginya kebutuhan Indonesia akan peralatan keamanan Siber sebagai bentuk kejahatan transnasional ini bisa dilihat pada dana hibah pemerintah Australia terhadap keamanan siber kepolisian Indonesia.[30]

Adanya kedekatan geografis ini juga menyebabkan Australia memiliki Kerjasama strategis lainnya dengan negara-negara ASEAN. Australia sudah dikenal baik sebagai mitra kerjasama potensial di kawasan ASEAN. Australia merupakan negara yang mengembangkan keamanan siber-nya secara serius dan Australia juga merupakan negara tetangga terdekat ASEAN yang memprioritaskan berbagai kerjasamanya dengan ASEAN.[31] Baik negara anggota ASEAN dan Australia juga mengadakan kerjasama siber sehingga kerjasama siber ASEAN-Australia dirasa merupakan rekomendasi yang baik bagi Indonesia untuk mengadakan kontak kerjasama keamanan bilateral, khususnya dibidang siber dengan Australia. Adanya kerjasama dengan Australia diharapkan ASEAN mendapatkan keuntungan berupa peningkatan *cyber security* di kawasan. Artinya, Australia adalah negara terdekat yang paling berpotensi dalam menjalin kerjasama

[28] Siti Mutiah, Security Complex Indonesia-Australia dan Pengaruhnya Terhadap Dinamika Hubungan Kedua Negara, *Jurnal Ilmu social dan Ilmu Politik*, Vol.19 no.2 Juli 2020, pp. 1415-1416

[29] Siti Muti'ah Setyawati, p.1418

[30] Bambang Supriyadi, Bambang Supriyadi, Persepsi Bersama Indonesia-Australia Dalam Hibah Dana dan Peralatan Investigasi *Cyber* Crime Dari Australia Kepada Indonesia, *Journal of International Relation* 3 No.1 (2017) pp.146-147

[31] Ministry of Foreign affairs Kingdom of Thailand, ASEAN-Australia Cyber Security Workshop: Strengthening Legal Implementation in Tackling Cyber Security Challenges in the Region, *mfa.go.th*, 29 November 2022, https://www.mfa.go.th/

keamanan siber dengan Indonesia sebagai negara anggota ASEAN mengingat Australia juga menjalin kerjasama siber dengan ASEAN.

Ketiga, Australia juga dikenal sebagai negara yang memiliki beberapa ahli di bidang keamanan siber dan memiliki kualifikasi yang bagus dibidang teknologi, tentu akan memberikan peluang dan kesempatan bagi Indonesia untuk menerapkan hal tersebut di dalam negeri.[32] Beberapa ahli dari Australia di bidang siber seperti Mike Sentonas yang merupakan spesialisasi keamanan siber terkemuka Crowdstrike, Sanjay Jha yang merupakan kepala ilmuwan institute keamanan siber universitas South Wales di mana keduanya aktif dan ikut serta dalam memberikan masukan keamanan bahkan arah kerjasama keamanan siber Australia dengan Indonesia dan negara lainnya.[33] kemudian ada Trace Mackey merupakan *Director Cyber Security Strategy and Governance Department of Home Affairs, Australian Government* yang beberapa tahun 2021 lalu melakukan diskusi dengan pihak BSSN terkait dengan kondisi *cyber security* . Yang ke empat ada nama Rachael Falk yang merupakan salah satu pakar keamanan dunia maya terkemuka di Australia dan juga merupakan anggota dewan ASPI (*Australian Strategic Policy Institue)* yang dimana Aspi merupakan badan yang dimiliki oleh Australia yang bekerjasama dengan Indonesia untuk melakukan pelatihan dalam bidang *cyber security.* Dengan adanya peran dari para pakar kemanan siber Australia dapat membantu Indonesia dalam menangani kejahatan siber baik dalam melakukan pelatihan maupun pembentukan dan pengembangan pusat penelitian terkait *cyber security*. Di Indonesia, sudah ada pusat penelitian terkait keamanan siber, namun belum ditingkat secara intensif dan efektif terkhususnya pada bidang akademik untuk jenjang universitas.[34]

Persepsi akan saling membutuhkan demi memenuhi kepentingan nasional ini pada akhirnya menyebabkan Indonesia terkesan mengesampingkan fakta bahwa Australia pernah melakukan tindakan kejahatan siber berupa penyadapan terhadap para petinggi Indonesia. Kedua negara berusaha menyelesaikan masalah tersebut dengan tetap

[32] Feline Cloramidine, p.65

[33] Dhiyanka Magrisa, Kerjasama BSSN dengan Departement of Foregign Affairs and Trade (DFAT) Australia Dalam Pengembangan Cyber Security, JOM Fisip Vol.7 No.2 Desember 2020, pp.5-6

[34] Hery Purwata, Tingkat Keamanan Siber Indonesia Masih Lemah, *jogpaper.net*, 16 Juni 2021, https://www.jogpaper.net/

mengadakan kerjasama siber.[35] Hal ini mengindikasikan bahwa penyadapan tampaknya telah bergeser makna menjadi tidak lagi sebagai kejahatan, melainkan lebih merupakan pelanggaran kode etik diplomatik karena tidak ada lagi unsur pelanggaran territorial di mana penyadap harus menerobos masuk ke wilayah negara lain secara ilegal untuk memasang perangkat spionase. Negara yang terlibat dalam kasus penyadapan lintas negara saat ini juga tidak ada satu pun yang membawa persoalan penyadapan tersebut ke Pengadilan Internasional. Hal ini karena faktor *globalization is used as a wave of information technology*, yang berakibat batas kedaulatan negara-negara menjadi *borderless*.[36]

Yang keempat, untuk menciptakan stabilitas keamanan di kawasan Indo-Pasifik dan mendukung tercapainya keamanan nasional Indonesia. Hadirnya dua kubu kekuatan yang menghimpit Indonesia membuat keamanan nasional Indonesia dan kawasan menjadi terancam. Indonesia yang merupakan negara non blok yang berada dikawasan Indo-Pasifik dapat dikatakan cukup dekat dengan dua kekuatan adidaya yaitu Tiongkok dan Amerika Serikat termasuk seketunya salah satunya adalah Australia. Dengan hadirnya dinamika hubungan Indonesia dengan dua kubu kekuatan yang seimbang secara tidak lansung menimbulkan tantangan bagi Indonesia dikarenakan Indonesia menjadi titik lokasi konflik. Indonesia dituntut untuk bisa menjadi episentrum atau penengah yang netral untuk meredakan ketegangan antar dua kubu kekuatan.

Rizal Sukma, seorang analis dari *Centre for Strategic and International Studies (CSIS)*, mengatakan bahwa Indonesia perlu dan harus siap dalam menghadapi yang namanya "real politik". Dengan politik luar negeri bebas aktif Indonesia yang digunakan sebagai pedoman dalam mengambil kebijakan harus terguncang dengan kemunculan beberapa kekuatan aliansi seperti *Five Eyes* dan AUKUS. Ditambah dengan kekuatan Tiongkok yang semakin neresahkan dikawasan laut cina selatan. Melihat permasalahan ini Indonesia dituntut untuk bisa menjaga keamanan kawasan. Dengan besarnya kekuatan Tiongkok dan Aukus mengharuskan Indonesia mencari jalan yang paling aman yaitu

[35] Quranul Syafira, Kerjasama Indonesia dan Australia Dalam Penanganan Kasus Penipuan Online Melalui Program Cyber Policy Dialogue Tahun 2018-2020, *Jurnal Unas*, Vol.3 No.1, Agustus 2021, pp.83-84

[36] Jahawir Thontowi, p.195

dengan menjalin kerjasama dengan dengan kedua negara sehingga Indonesia dapat terhindar dari pusaran konflik. Indonesia memperkuat kerjasama ekonomi dengan Tiongkok sedangkan dengan Australia Indonesia menjalin kerjasama keamanan yaitu *Cyber Security*. Indonesia harus berhenti bersikap netral tanpa menentukan posisi; sebaliknya, Indonesia harus mulai berhati-hati dan menyesuaikan orientasi kebijakannya untuk kepentingan nasional. Dalam memenuhi kepentingan nasional, Indonesia akan condong dan sangat rasional menjalin kerjasama keamanan siber dengan Autralia, ini untuk mengimbangi peran dan dapat merangkul dua kekuatan di kawasan Indo-Pasifik. dalam sistem internasional yang anarki, Indonesia dapat menekankan sifat asertif bahwasanya tidak ada kawan maupun lawan yang abadi. Kedekatan Indonesia dengan Australia dalam *cyber security* bukan berarti menyingkirkan Tiongkok dan sepenuhnya berkiblat kearah Australia, karena sikap Indonesia ini sesuai dengan kepentingan nasional di bidang pertahananan dan keamanan. Di satu sisi, Indonesia juga tetap dekat dengan Tiongkok dalam bidang ekonomi dan hal ini bisa ditegaskan bahwasanya sektor kepentingan yang berbeda seharusnya tidak pernah menghalangi hubungan baik antar negara.[37] Seperti halnya mendayung diantara dua karang, Indonesia mampu merangkul serta mendapat keuntungan dari masing masing pihak yang berseteru dari dua bidang sekaligus yaitu pertahanan dan keamanan dan juga ekonomi.

Kelima, Untuk meredakan ketegangan dengan Australia dan harmonisasi hubungan (*Confidence Building Measure*). merupakan salah satu strategi dalam diplomasi yang bertujuan untuk mencegah atau mengurangi risiko konflik dengan mengurangi atau menghilangkan atau menghilangkan penyebab ketidakpercayaan (m*istrust*), kesalahpahaman (*misunderstanding*) dan salah perhitungan (*miscalculation*) diantara negara yang terlibat konflik.[38] Kerjasama dengan Australia ini dibentuk untuk

[37] Putro, Yehuda Bimo Yudanto Purwantoro. "Menyikapi Potensi Eskalasi Konflik Di Kawasan Indo-Pasifik Sebagai Dampak Dari Kesepakatan Aukus." Sekretariat Kabinet Republik Indonesia, November 17, 2021. https://setkab.go.id/menyikapi-potensi-eskalasi-konflik-di-kawasan-indo-pasifik-sebagai-dampak-dari-kesepakatan-aukus/

[38] Patryk Pawlak, Confidence-Building Measures in Cyberspace: Current Debates and Trends. Dalam Anna-Maria Osula and Henry Rõigas(Eds). International Cyber Norms:Legal, Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn. (2016).

menghilangkan atau mengurangi adanya kesalahpahaman yang sebelumnya pernah terjadi terkait isu penyadapan yang dilakukan oleh Australia kasus kejahatan lainnya.

## 2. Wujud Kerjasama Indonesia-Australia Dalam Menangani kejahatan siber Di Indonesia

Melihat potensi yang dimiliki Australia dalam menanggulangi kejahatan siber, Indonesia kemudian menggandeng negara tersebut untuk membantu penanggulangan kejahatan siber melalui kerjasama strategis dalam bidang siber. Adapun kerjasama strategis tersebut seperti:

### A. Kerjasama Kepolisian Republik Indonesia dan Kepolisian Federal Australia (AFP) Dalam Menanggulangi Kejahatan Siber di Indonesia

Polri dan AFP memasukkan unsur-unsur pencegahan, daya tangkap dan penelusuran atas kejahatan lintas negara, direalisasikan melalui pendirian JCLEC *(Jakarta Centre Law Enforcement Cooperation)* yang dimaksudkan untuk melatih para penegak hukum yang ingin meningkatkan keahlian operasionalnya dalam menangani kejahatan lintas negara yang awalnya berfokus pada tindak kejahatan terorisme yang kemudian meluas dengan mencakup tindak kejahatan siber *(cybercrime)*. Tujuan dari pusat kerjasama ini adalah untuk membantu Polri dan badan penegak hukum lainnya dalam mengembangkan kemampuan penyidikan baik dalam penyidikan *cybercrime* maupun kejahatan lainnya, melalui pendidikan dan pelatihan di JCLEC tersebut.[39] Hal ini juga sesuai dengan konsep *cyber security* yang terdiri dalam beberapa aspek, seperti perlindungan keamanan, pedoman pelaksanaan, pendekatan manajemen resiko, tindakan, serta pelatihan yang kemudian digunakan untuk melindungi ruang siber yang pada dasarnya dibangun atas kepastian hukum, tindakan prosedural, struktur organisasi, *capacity building*, dan kerjasama internasional.

Wujud Kerjasama siber keduanya juga bisa dilihat dari pembangunan gedung TNCC *(Transnational Crime Coordination Centre)* dan pembangunan laboraturium *Cybercrime Investigations Sattelite* (CCIS). TNCC ini berfungsi sebagai pusat pengumpulan analisis dan sharing informasi antara Polri dan AFP.

[39] Yayasan JCLEC, Tentang JCLEC, 20 Maret 2020, https://jclec.org/

TNCC ini juga merupakan jaringan informasi antara Polri dan AFP untuk memberantas kejahatan transnasional termasuk di dalamnya *cybercrime*.[40]

Program *capacity building* yang diberikan AFP terhadap Polri memberikan hasil yang relatif cukup baik dimana semenjak program *capacity building* dicanangkan, kinerja Polri dalam penanganan *cyber crime* kian meningkat. Beberapa contoh kasus penanganan syber crime yang berhasil diselesaikan oleh kepolisian Indonesia seperti penangkapan bos *cyber crime* asal Tiongkok beserta 27 warga negara asing lainnya asal Taiwan dan Tiongkok serta 3 orang warga negara Indonesia dalam kasus penipuan online pada tahun 2015. Kemudian pada tahun 2018, Polri juga berhasil melacak dan mengantongi identitas penyebar isu *rush money* yang meresahkan masyarakat Indonesia.[41] Namun, penanganan kasus tersebut masih jauh dari yang diharapkan di mana hal tersebut dapat dilihat melalui data dari *Cyber Crime Investigation Centre* Bareskrim Mabes Polri pada tahun 2019 kasus terselesaikan sebanyak 86 kasus, 2020 sebanyak 115 kasus dan Januari-Juni 2022 sebanyak 94 kasus.[42]

**B. Kerjasma BSSN dengan *Departemen Of Foreign Affairs dan Trade* (DFAT)**

Bentuk kerjasama antar keduanya bisa dilihat dari keberadaan *Cyber Boot Camp* yang merupakan sebuah project dari *Cyber Cooperation Program* yang dimiliki oleh DFAT. Program ini merupakan bentuk kerjasama Australia dengan negara mitra nya di seluruh Indo-Pasifik untuk meningkatkan keamanan siber. Didirikan pada tahun 2016, *Cyber Cooperation Program* ini memainkan peran penting dalam mendukung keterlibatan Australia di dalam *cyberspace* yang mengutamakan internet yang terbuka, bebas, dan aman dan dapat melindungi keamanan nasional serta mendorong stabilitas internasional, sekaligus mendorong pertumbuhan ekonomi global dan pembangunan berkelanjutan.[43] *Cyber Boot*

---

[40] Dian Ekawati Ismail, Cybercrime di Indonesia, *Jurnal Inovasi*, Vol.6 no.3, 20 Agustus 2019, pp. 127-129, https://e-journal.ung.ac.id

[41] Alif Ramadan, Tim Cyber Polri Berhasil Lacak Penyebar Isu Rush Money, *jurnalsecurity.com*, 22 November 2018, https://jurnalsecurity.com/tim-cyber-polri-berhasil-lacak-penyebar-isu-rush-money/

[42] Katya Loviana, Cyber Security and Cyber Resilience in Indonesia: Challenges and Oportunity, *cfds.fisipol.ugm.ac.id*, 10 Mei 2022, https://cfds.fisipol.ugm.ac.id/

[43] Damar Apri Sudarmadi, Stretagi BSSN Dalam Menghadapi Ancaman Siber di Indonesia, *Jurnal Kajian Strategik Ketahanan Nasiona*l2 no.2 (2019), pp.18-20

*Camp* bertujuan untuk membangun pengetahuan dan kesadaran peserta di mulai dari kesiapan teknologi, ancaman siber, hingga pengambilan keputusan dan sifat *cyberspace*. kegiatan ini berfokus pada pengembangan keterampilan bagi para delegasi untuk dapat lebih memahami, membangun, dan merawat sistem keamanan siber dalam mencegah serangan siber. Australia juga merancang kegiatan ini untuk menyatukan keterampilan dan keahlian dari para delegasi yang akan memperluas keahliannya kepada sektor pemerintah, akademisi, maupun swasta.[44]

Dalam meningkatkan *Cyber security* Indonesia, BSSN juga mengikuti ASPI *(Australia Strategic Policy Institute) Cyber Policy Workshop*. ASPI bertujuan untuk menyelenggarakan serangkaian *workshop* bagi negara-negara mitra kerja sama di bidang *cyber security* dengan Australia tentang perilaku negara yang bertanggung jawab di *cyber* space. ASPI juga bekerja sama dengan BSSN untuk memperkuat analisis ancaman *cyber*, keterlibatan dalam masalah kebijakan *cyber*, dan koordinasi antar lembaga pemerintahan. Dengan adanya kegiatan ASPI *Cyber Policy Workshop*, Indonesia yang masih memerlukan tindakan yang akurat dalam risk management di bidang keamanan siber diharapkan lebih dapat memperkuat analisis ancaman siber yang masih sering terjadi di Indonesia. *Risk management* merupakan elemen fundamental dari sebuah strategi. Melalui kegiatan ASPI *Cyber Policy Workshop* ini diharapkan para pemangku kepentingan yang berada di bidang *cyber security* di Indonesia dapat saling koordinasi dan berkolaborasi untuk mengatasi ancaman siber.[45]

Indonesia dan Australia juga mengadakan *3rd Indonesia-Australia Cyber Policy Dialogue* yang merupakan kegiatan rutin tahunan tindak lanjut kesepakatan bilateral antara Presiden Republik Indonesia dan Perdana Menteri Australia pada tahun 2017. Pertemuan pertama dilaksanakan pada 4 Mei 2017 di Australia, pertemuan kedua dilaksanakan pada 3 Agustus 2018 di Jakarta sedangkan

[44] Dhiyanka Magrisa, p.5

[45] Ineu Rahmawati, Analisis Manajemen Resiko Ancaman Kejahatan Siber Dalam Peningkatan Cyber Defense, *Jurnal Pertahanan dan Bela Negara*7 no.2 (2017), pp.91-93

pertemuan ketiga tersebut digelar dalam jaringan pada 2 September 2020 dari kantor masing-masing perwakilan. Pertemuan ketiga ini bertujuan mempererat kerja sama siber dan kemitraan antara kedua negara dalam hal berbagi informasi, praktik terbaik keamanan siber, pengembangan kapasitas dan peningkatan ekonomi digital serta penanganan kejahatan siber. Para peserta membahas situasi yang berkembang di ruang siber, termasuk tantangan utama dan pendekatan praktik terbaik untuk mengelola ancaman strategis, strategi keamanan siber nasional, dan legislasi yang relevan.[46]

### 3. Pengaruh Kerjasama Cyber Security Indonesia dan Australia Dalam Menangani Kejahatan Siber di Indonesia

Terjalinnya kerjasama keamanan siber dengan Australia membawa beberapa pengaruh bagi Indonesia, adapun diantara pengaruh tersebut naiknya posisi Indonesia dalam ITU.

| Tahun | Indonesia | | Australia | |
|---|---|---|---|---|
| | Peringkat | Skor | Peringkat | Skor |
| 2017 | 70/164 | 0,424 | 7/164 | 0,820 |
| 2018 | 41/175 | 0,776 | 11/177 | 0,890 |

Tabel 4.1 GCI 2017-2018 (ITU Global *Cyber security* Index)

Indonesia pada tahun 2017 termasuk pada *maturing stage* yang berarti telah mempunyai inisiatif dan sedang mengembangkan program-program *cyber security* namun belum berkomitmen tinggi. Sedangkan Australia berada di *leading stage* yang mempunyai komitmen sangat tinggi terhadap *cyber security*. Pada tahun 2018, Indonesia meningkat dari *maturing stage* ke *leading stage*. Hal ini merupakan pencapaian atas keberhasilan kinerja seluruh pemangku kepentingan *cyber security* yang dikonsolidasikan oleh BSSN dalam membangun dan mengembangkan ekosistem *cyber security* nasional.

[46] Komunikasi Publik BSSN, BSSN Inisiasi Lanjutan Kerjasama Keamanan Siber Indonesia-Australia Dalam 3rd Indonesia-Australia Cyber Policy Dialogue, *bssn.go.id*, 2 September 2020, https://bssn.go.id

| No | Sasaran Strategis | Indikator | Capaian 2018 (target) | Capaian 2018 (realisasi) | Capaian 2019 (target) | Capaian 2019 (realisasi) |
|---|---|---|---|---|---|---|
| 1 | Terselenggaranya keamanan siber secara andal, profesional, terpercaya | Peringkat Indonesia pada publikasi ITU | 64 | 41 | 64 | 41 |
| 2 | Terselenggaranya pendayagunaan kapabilitas identifikasi dan deteksi yang andal | Tingkat cakupan potensi ancaman siber yang berhasil dideteksi | 25% | 37,18% | 30% | 44,77% |
| 3 | Terselenggaranya pengembangan kapabilitas proteksi yang optimal | Tingkat penerapan proteksi keamanan siber | 0.600 | 0.571 | 0.615 | 0.657 |

Tabel 1. Capaian Kinerja BSSN (Peraturan BSSN Nomor 5 Tahun 2020)

Walaupun dengan adanya capaian yang berhasil diraih oleh Indonesia dalam menangani kejahata siber di Indonesia , itu semua masih belum cukup dikarenakan masih banyak kasus serangan siber yang menyerang Indonesia. Berdasarkan data yang dimiliki BSSN, sejak Januari hingga Juni pada 2020, ada kenaikan serangan sebanyak 54%, yang artinya terjadi anomali (serangan siber) sebanyak 149 juta dengan serangan paling banyak berupa *malware*. Serangan siber dengan menggunakan *malware* tersebut memanfaatkan isu covid 19 untuk menjebak para korbannya, melalui email phising, sms phising, web phising dan lainnya. Tahun 2022 indeks keamanan siber Indonesia berada pada peringkat ke-3 terendah diantara negara G20. Laporan NCSI mencatat, skor indeks keamanan siber Indonesia sebesar 38,96 poin dari 100 pada 2022. Angka ini menempatkan Indonesia berada di peringkat ke 3 terendah diantara negara-negara G20. Oleh NCSI, Indonesia berada di peringkat ke-6 di Asia Tenggara, tentu saja ini masih menjadi masalah besar yang harus segera mungkin diatasi.

Riset terkait buruknya keamanan siber Indonesia juga dikeluarkan oleh Reboot Digital PR Service. Lembaga riset yang berbasis di Inggris ini melakukan sebuah riset dan menemukan bahwa Indonesia menjadi negara dengan indeks keamanan siber terburuk di Asia dan dunia.[47] Terjadinya peningkatan serangan siber juga disebabkan karena Indonesia kekurangan bakat *cyber security* dan itu menimbulkan masalah yang sangat nyata dalam industri strategis, pertahanan, kesatuan bangsa dan bisnis. Hal ini disebabkan karena kekuatan SDM (sumber daya manusia) sama pentingnya dengan kekuatan teknologi itu sendiri. Dalam dunia industri, baik perbankan, telko dan instansi pemerintahan, hampir seluruh negara didunia, telah memakai teknologi sebagai basis aktifitas kinerja kerjanya. Teknologi akan terus berkembang pesat tiap tahun kedepan tanpa batas. Menurut Eva Noor, CEO PT Xynexis International mengatakan bahwa dunia butuh 15 juta tenaga expertis untuk *cyber security*. Indonesia kini butuh 10000 tenaga ahli (expert) *cyber security* diluar officer untuk berbagai kebutuhan instansi pemerintah, dunia industri, perbankan, telko dan lain sebagainya.[48] Dari berbagai penjelasan tersebut, dapat diketahui bahwa peningkatan jumlah serangan siber tidak sebanding dengan banyaknya jumlah tenaga ahli *cyber security*, meskipun dalam hal ini Indonesia sudah melakukan kerjasama dengan Australia dalam menjaga keamanan siber, kenyataannya serangan siber yang terjadi justru semakin meningkat, terutama ketika memasuki tahun 2020.[49]

Dengan demikian, meskipun Indonesia sudah menjalin Kerjasama keamanan Siber dengan Australia, berbagai kejahatan siber terus terjadi dan semakin sulit untuk dibendung. Seperti diketahui, bahwa masih banyak masyarakat Indonesia yang belum sadar akan pentingnya teknologi atau masih banyak juga distribusi teknologi yang kurang memadai. Oleh karena itu, banyak hal yang belum bisa diselesaikan secara maksimal. Masih banyak masyarakat Indonesia yang memiliki ketertarikan minim terhadap seminar atau campaign bertemakan keamanan siber. Sehingga sulit untuk merealisasikan kesepakatan yang telah dibuat. Selain itu, untuk meningkatkan kualitas SDM di Indonesia perlu adanya sumber daya teknologi dan pendidikan yang memadai. selama Indonesia masih belum bisa menopang sebagian besar keamanan sibernya dengan baik,

---

[47] Karina Shaskara, Indonesia Jadi Negara Dengan Keamanan Siber terburuk di Dunia, *teknologi.id*, 8 Agustus 2022, https://teknologi.id/

[48] Media Indonesia, Xynexis Terus Berinovasi Membangun Keamanan Siber di Indonesia, *Media Indonesia.com*, 22 Desember 2021, https://mediaindonesia.com/

[49] Yunita, Indonesia Kekurangan Bakat Cyber Security, *Kominfo.go.id*, 27 Maret 2022, https://www.kominfo.go.id/content/detail/8574/indonesia-kekurangan-bakat-cyber-security/0/sorotan_media

maka kemungkinan terburuknya ialah ketergantungan. Apalagi negara-negara partner kerjasama Indonesia dikenal sebagai negara yang maju, baik dari segi keamanan siber, politik, ekonomi dan juga militer. Apabila Indonesia tidak dapat menyeimbangi dengan baik maka Indonesia akan ketergantungan dengan kerjasama tersebut sehingga sulit unuk mengembangkan keamanan sibernya sendiri.

**Kesimpulan**

Indonesia sebagai salah satu negara dengan jumlah penduduk terbesar sekaligus negara dengan salah satu pengguna internet terbesar di dunia menghadapi besarnya potensi terjadinya serangan dunia siber oleh pihak yang tidak bertanggung jawab. Indonesia kemuadian menjalin kerjasama dengan Australia untuk menangani masalash tersebut. Alasan Indonesia menjalin kerjasama dengan Australia adalah untuk memenuhi kepentingan nasional untuk dapat meningkatkan kemanan siber khsusunya dalam posisi GCI dan ITU. Yang kedua karena kedekatan geografis, ketiga terdapatnya para ahli yang mempunyai kualifikasi yang bagus dalam bidang siber. Keempat untuk menciptakan keamanan kawasan. Dan yang kelima memperbaiki hubungan dengan Australia.

Bentuk penanganan kejahatan siber di Indonesia melalui kerjasama dengan Australia yakni kerjasama Kepolisian Republik Indonesia dan kepolisian Federal Australia (AFP) dalam menanggulangi kejahatan siber di Indonesia serta Kerjasama keamanan siber BSSN dengan pemerintah Australia. Semua kerjasama tersebut mengarah pada penguatan kapasitas dan kapabilitas keamanan siber di Indonesia, terutama dari segi keamanan nasional. Dalam pelaksanaan kerjasama tersebut, ujung tombak dari keamanan siber Indonesia dipegang oleh BSSN. BSSN sendiri dalam penanganan keamanan siber sudah menetap beberapa indicator diantaranya Peringkat Indonesia pada *Global Cyber security Index* (Publikasi ITU) di mana BSSN berhasil meningkatkan skor dan peringkat Indonesia pada *Global Cyber security Index* (GCI) dengan menempati peringkat ke 41 (empat puluh satu) dari 194 (serratus Sembilan puluh empat) negara anggota The UN International Telecommunication Union (ITU), Tingkat Cakupan Potensi Ancaman Siber yang Berhasil Dideteksi di mana BSSN membentuk pusat *malware* nasional untuk meningkatkan kemampuan mendeteksi kejahatan siber serta Tingkat Penerapan Proteksi Keamanan Siber Nasional. Akan tetapi, Kerjasama antar kedua negara belum maksimal dalam

mencegah berbagai serangan siber karena Indonesia belum memiliki aturan hukum yang memadai soal kejahatan siber, pembangunan kapasitas keamanan siber masih kurang, minimnya SDM ahli siber, masyarakat Indonesia yang pengetahuannya banyak kurang terkait keamanan siber juga mempengaruhi semakin meluasnya kejahatan siber.

## Daftar Pustaka

### Buku


Nazli Choucri, Cyberpolitics in International Relations, *Cambridge : MIT Press,*

U. S. Bakry, *Pedoman Penulisan Skripsi Hubungan Internasional*, (Yogyakarta: Deepublish 2016)


### Jurnal


Ahmad Saudi, Kejahatan Siber Transnasional dan Strategi Pertahanan Siber Indonesia, *Jurnal Demokrasi dan Otonomi Daerah*, Vol. 16 No.3, September (2018).

Astari Marisa, Hubungan Bilateral Indonesia-Australia: Kepentingan Australia Dalam Meratifikasi IA-CEPA tahun 2019, *Jurnal Transborders*, Vol.4 no.1, Desember (2020).

Bambang Supriyadi, Bambang Supriyadi, Persepsi Bersama Indonesia-Australia Dalam Hibah Dana dan Peralatan Investigasi *Cyber* Crime Dari Australia Kepada Indonesia, *Journal of International Relation* 3 No.1 (2017)

Damar Apri Sudarmadi, Stretagi BSSN Dalam Menghadapi Ancaman Siber di Indonesia, *Jurnal Kajian Strategik Ketahanan Nasiona*l2 no.2 (2019), pp.18-20

Dhiyanka Magrisa, Kerjasama BSSN dengan Departement of Foregign Affairs and Trade (DFAT) Australia Dalam Pengembangan Cyber Security, JOM Fisip Vol.7 No.2 Desember (2020).

Dhiyanka Magrisa, Kerjasama BSSN dengan Departement of Foregign Affairs and Trade (DFAT) Australia Dalam Pengembangan Cyber Security, JOM Fisip Vol.7 No.2 Desember (2020)

Dian Ekawati Ismail, Cybercrime di Indonesia, *Jurnal Inovasi*, Vol.6 no.3, 20 Agustus (2019). https://e-journal.ung.ac.id

Dian Ekawati Ismail, Cybercrime di Indonesia, *Jurnal Inovasi*, Vol.6 no.3, 20 Agustus (2019).https://e-journal.ung.ac.id

Gisella Linardy, Kerjasama Bilateral Indonesia-Australia Dalam IA-CEPA, *Jurnal Sentris Diplomasi*, Vol.2 No.1, Oktober (2021).

H. Nassaji, 'Qualitative and Descriptive Research: Data Type Versus Data Analysis,' *Language Teaching Research*, No. 2, Vol. 19, Mei (2015).

Handrini Ardiyanti, Cyber Secutity dan Tantangan Pengembangan di Indonesia, *Badan Riset Inovasi Nasional* Vol.3 No.1, Agustus (2014).https://www.researchgate.net

Hendro Setyo Wahyudi, Teknologi dan Kehidupan Masyarakat, *Jurnal Analisa Sosiologi,* vol.3 no.1 April (2014), , https://media.neliti.com/

Ineu Rahmawati, Analisis Manajemen Resiko Ancaman Kejahatan Siber Dalam Peningkatan Cyber Defense, *Jurnal Pertahanan dan Bela Negara*7 no.2 (2017).

Jahawir Thontowi, Penyadapan dalam Hukum Internasional dan Implikasinya terhadap Hubungan Diplomatik Indonesia dengan Australia, *Jurnal Hukum IUS QUIA IUSTUM* NO. 2 VOL.( 2015).

Leo T Panjaitan, Analisis Penanganan *Carding* dan Perlindungan Nasabah Dalam Kaitannya Dengan Undang-Undang Informasi dan Transaksi Elektronik no.11 Tahun 2008, *Jurnal Telekomunikasi dan Komputer*, Vol.3 no.1 Mei (2012).

Muhammad Prakoso Aji, Sistem Keamanan Siber dan Kedaulatan Data di Indonesia Dalam Perspektif Ekonomi Politik (Studi Kasus perlindungan Data Pribadi), *Jurnal Politica*, Vol.13 No.2, Mei (2022).

Patryk Pawlak, Confidence-Building Measures in Cyberspace: Current Debates and Trends.. International Cyber Norms:Legal, Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn. (2016).

Putri Azaria Matondang, Kerja sama Internasional Indonesia-Australia: Studi Kasus Kesepakatan Perundingan Indonesia-Australia Comprehensive Economic Partnership Agreement (IA-CEPA) Tahun 2010-2018 (Universitas Islam Indonesia, 2021)

Quranul Syafira, Kerjasama Indonesia dan Australia Dalam Penanganan Kasus Penipuan Online Melalui Program Cyber Policy Dialogue Tahun 2018-2020, *Jurnal Unas*, Vol.3 No.1, Agustus( 2021).

Siti Muti'ah Setyawati, Security Complex Indonesia-Australia dan Pengaruhnya Terhadap Dinamika Hubungan Kedua Negara, *Jurnal Ilmu Sosial dan Ilmu Politik*, Vol.19 No.2 November (2015).

Siti Mutiah, Security Complex Indonesia-Australia dan Pengaruhnya Terhadap Dinamika Hubungan Kedua Negara, *Jurnal Ilmu social dan Ilmu Politik*, Vol.19 no.2 Juli (2020)

Supanto, Perkembangan Kejahatan Tekonologi Informasi (Cyber Crime) dan Antisipasinya Dengan Penal Policy, *Yustisia Jurnal Hukum*, Vol.5 No.1, Juli (2018)

**Web**

"*Descriptive Research Designs: Types, Examples & Methods," Formpl*, https://www.formpl.us

Acer Indonesia, Kebocoran Data (*Data leakage*) kenali Penyebab dan Dampaknya, 14 Juli 2022, https://commercial.acerid.com/

Adhi Maulana, 10 Dosa Besar NSA yang Dibocorkan Edward Snowden, *Liputan6*, 5 Maret 2015, https://www.liputan6.com/tekno/read/2185425/10-dosa-besar-nsa-yang-dibocorkan-edward-snowden

Alif Ramadan, Tim Cyber Polri Berhasil Lacak Penyebar Isu Rush Money, *jurnalsecurity.com*, 22 November 2018, https://jurnalsecurity.com/tim-cyber-polri-berhasil-lacak-penyebar-isu-rush-money/

Ardela Nabila, Ada *Carding* Ini 8 Modus Kejahatan Kartu Pembayaran yang Perlu Diwaspadai, *Parapuan.co*, 26 Juni 2022, https://www.parapuan.co/

BSSN, BSSN Inisiasi Lanutan Kerjasama Keamanan Siber Indonesia-Australia Dalam 3rd Indonesia-Australia Cyber Policy Dialogue, *bssn.go.id*, 2 September 2020, https://bssn.go.id/

Data Indonesia, Kerugian Kejahatan Siber Diproyeksi 844 Triliun Tahun 2022, *dataindonesia.id*, 5 Desember 2022, https://dataindonesia.id/

Dwika Intishar Safara, Globalisasi dan Permasalahan Keamanan Internasional Akibat Cyber Crime di Indonesia, *berau.prokal.co*, 18 Juli 2022, https://berau.prokal.co/read/news/71433-globalisasi-dan-permasalahan-keamanan-internasional-akibatcyber-crimedi indonesia.html

Feline Cloramidine, p.65

Hery Purwata, Tingkat Keamanan Siber Indonesia Masih Lemah, *jogpaper.net*, 16 Juni 2021, https://www.jogpaper.net/

IDSIRTII, *Laporan analisis Malware*, https://www.idsirtii.or.id/

Karina Shaskara, Indonesia Jadi Negara Dengan Keamanan Siber terburuk di Dunia, *teknologi.id*, 8 Agustus 2022, https://teknologi.id/

Katya Loviana, Cyber Security and Cyber Resilience in Indonesia: Challenges and Oportunity, *cfds.fisipol.ugm.ac.id*, 10 Mei 2022, https://cfds.fisipol.ugm.ac.id/

Kominfo, Empat Operator Seluler di Indonesia Disebut Dalam Dokumen Penyadapan, *kominfo.go.id*, 28 Maret 2019, https://www.kominfo.go.id/

Kominfo, Kenali 4 Jenis Kejahatan Siber, *diskominfo kotabogor*, 20 Juni 2019, https://kominfo.kotabogor.go.id/index.php/post/single/740

Komunikasi Publik BSSN, BSSN Inisiasi Lanjutan Kerjasama Keamanan Siber Indonesia-Australia Dalam 3rd Indonesia-Australia Cyber Policy Dialogue, *bssn.go.id*, 2 September 2020, https://bssn.go.id

Media Indonesia, Xynexis Terus Berinovasi Membangun Keamanan Siber di Indonesia, *Media Indonesia.com*, 22 Desember 2021, https://mediaindonesia.com/

Meilani Teniwut, Pengertian Revolusi Industri 4.0 ini Persiapan Indonesia, *mediaindonesia.com*, 26 Oktober 2022, https://mediaindonesia.com/

Ministry of Foreign affairs Kingdom of Thailand, ASEAN-Australia Cyber Security Workshop: Strengthening Legal Implementation in Tackling Cyber Security Challenges in the Region, *mfa.go.th*, 29 November 2022, https://www.mfa.go.th/

Polri, Kejahatan Siber di Indonesia Naik Berkali-kali Lipat, *pusiknas.polri.id,* 10 Agustus 2022, https://pusiknas.polri.go.id/

Putri Azaria Matondang, Kerja sama Internasional Indonesia-Australia: Studi Kasus Kesepakatan Perundingan Indonesia-Australia Comprehensive Economic Partnership Agreement (IA-CEPA) Tahun 2010-2018 (Universitas Islam Indonesia, 2021) p.15-17

Putro, Yehuda Bimo Yudanto Purwantoro. "Menyikapi Potensi Eskalasi Konflik Di Kawasan Indo-Pasifik Sebagai Dampak Dari Kesepakatan Aukus." Sekretariat Kabinet Republik Indonesia, November 17, 2021. https://setkab.go.id/menyikapi-potensi-eskalasi-konflik-di-kawasan-indo-pasifik-sebagai-dampak-dari-kesepakatan-aukus/

Rezky Yayang, Waspada Kejahatan Siber di Era Serba Daring, *Makarta Bakti Negara*, 5 Maret 2023, https://lan.go.id/?p=13415

Siti Muti'ah Setyawati, p.1418

United Nations, Conference of the Parties to the United Nations Convention against Transnational Organized Crime, 2010

UPT TIK, Mengenal Ransomware dan Pencegahannya, *Upttik.co*, 4 September 2017, https://upttik.undiksha.ac.id/mengenal-ransomware-dan-pencegahannya/

Yayasan JCLEC, Tentang JCLEC, 20 Maret 2020, https://jclec.org/

Yunita, Indonesia Kekurangan Bakat Cyber Security, *Kominfo.go.id*, 27 Maret 2022, https://www.kominfo.go.id/content/detail/8574/indonesia-kekurangan-bakat-cyber-security/0/sorotan_media