# KERJA SAMA BADAN SIBER DAN SANDI NEGARA (BSSN) INDONESIA DENGAN *DEPARTMENT OF FOREIGN AFFAIRS AND TRADE* (DFAT) AUSTRALIA DALAM PENGEMBANGAN *CYBER SECURITY*

**Oleh: Dhiyanka Magrisa**
(dmagrisya11@gmail.com)
**Dosen Pembimbing: Ahmad Fuadi, S.IP, M.Si**
**Bibliografi: 14 Jurnal, 20 Buku, 2 Laporan Resmi, dan 67 Website**
Jurusan Hubungan Internasional
Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Riau
Kampus Bina Widya Jl. HR. Soebrantas Km. 12,5 Simp. Baru Pekanbaru 28294
Telp/Fax. 0761-63277

***Abstract***

*The development of technology has gradually permeated all aspects of modern human life. One of them is the ease of getting information and communication. Unlimited internet access creates new threats, namely cyber threats. Various countries are trying to improve their cybersecurity, including Indonesia by working with Australia. In its implementation, this cooperation is represented by the National Cyber and Crypto Agency (BSSN) from Indonesia and the Department of Foreign Affairs and Trade (DFAT) from Australia. This research describes the forms of cooperation between the National Cyber and Crypto Agency (BSSN) with the Department of Foreign Affairs and Trade (DFAT) in the development of cyber security.*

*This research uses descriptive qualitative research methods. The perspective used in this research is neorealism, and uses the theory of international cooperation with the form of bilateral cooperation. Bilateral cooperation is a situation that illustrates the mutual and influencing relationship between the two countries and arises as a result of the commitment between the two countries.*

*The results of this research describe the forms of cooperation that exist between the National Cyber and Crypto Agency (BSSN) and the Department of Foreign Affairs and Trade (DFAT) which is based on the MoU between the two countries in the cybersecurity sector in 2018. There are several forms, namely; Cyber Boot Camp, ASPI (Australian Strategic Policy Institute) Cyber Policy Workshop, Cyber Business Connection: Austrade and AustCyber in the digital economy, and Cyber Policy Dialogue.*

***Keywords****: National Cyber and Crypto Agency (BSSN), Department of Foreign Affairs and Trade (DFAT), International Cooperation, Cybersecurity.*

## PENDAHULUAN

Teknologi informasi telah memberikan kontribusi yang besar terhadap keberlangsungan hidup masyarakat sosial dalam suatu negara. Teknologi informasi mempermudah negara dan individu dalam menyampaikan dan menyebarluaskan informasi melalui media komunikasi digital.

Akses internet yang tak terbatas memungkinkan individu menyalahgunakan perkembangan ini. Dampak negatif yang ditimbulkan akibat perkembangan teknologi tidak sedikit. Pornografi, penipuan, perjudian, pencurian data, dan *hacking* yang masuk ke dalam kategori kejahatan *cyber (cyber threat)* menjadi suatu ancaman yang serius. *Cyber threat* adalah tindak kejahatan melalui jaringan internet yang memanfaatkan perkembangan teknologi yang dimana pelaku mencari keuntungan pribadi atau kelompoknya.

Internet sebagai media komunikasi global telah berkembang menjadi sebuah kebutuhan bagi kehidupan manusia saat ini. Menurut ITU (*International Telecommunication Union*) pada akhir 2019 53,6 persen dari populasi global atau 4,1 miliar orang menggunakan internet.[1]

Internet sebagai media komunikasi global telah berkembang menjadi sebuah kebutuhan bagi kehidupan manusia saat ini. Menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), penetrasi pengguna internet di Indonesia mengalami peningkatan setiap tahunnya. Pada tahun 2017 pengguna internet di Indonesia mencapai 143,26 juta jiwa dimana angka ini merupakan 54,68 persen dari total penduduk di Indonesia. Sedangkan pada tahun 2018 pengguna internet di Indonesia mencapai 171,17 juta jiwa yang merupakan 64,8 persen dari total penduduk di Indonesia.[2]

Tidak jauh berbeda dengan Australia, negara ini mengalami peningkatan pengguna internet sebesar 3,6% dari Juni 2018 hingga Desember 2017. Tercatat ada sekitar 14,7 juta jiwa pengguna internet di Australia dari 24,99 juta jiwa populasinya.[3] Dengan memiliki pengguna internet aktif yang banyak dan terus berkembang, menjadikan Indonesia dan Australia sebagai negara potensial yang terkena serangan di dunia *cyber*.

*Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII) yang berada di bawah naungan Badan Siber dan Sandi Negara (BSSN) mendeteksi pada 10 bulan pertama di tahun 2018 terdeteksi lebih dari 207,9 juta serangan siber ke Indonesia. Hal ini disampaikan oleh Kepala Badan Siber dan Sandi Negara (BSSN) Djoko Setiadi pada Seminar Diseminasi Deteksi Ancaman Siber Tahun 2018.[4]

[1] ITU, "Statistics" International Telecommunication Union (diakses dari *https://www.itu.int/en/ITUD/Statistics/Pages/stat/default.aspx* pada 18 Januari 2020).

[2] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). *"Laporan Survei Penetrasi & Profil Perilaku Pengguna Internet Indonesia"* (diakses dari *https://apjii.or.id/survei* pada 29 Januari 2020).

[3] Internet Activity Australia, (diakses dari *https://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/* pada 09 Juli 2020).

[4] Agus Tri Haryanto "Indonesia Dibombardir 207 Juta Serangan Siber dalam 10 Bulan", (diakses dari *https://inet.detik.com /security/d4340493* pada 25 Juli 2020).

Pada malam acara *Stay Smart Online Week* 2018 Alastair MacGibbon, kepala *Australian Cyber Security Centre* (ACSC) mengatakan satu dari empat warga Australia terkena ancaman *cyber* pada tahun lalu yang mana ini berjumlah lebih dari 6 juta warga Australia. Selain itu, menurut *website cyber* yang dimiliki Australia tercatat 43% dari serangan cyber yang terjadi di Australia ditujukan untuk bisnis kecil dengan pendapatan rata-rata $ 10.000, 59% orang menggunakan kata sandi yang sama di semua perangkat dan akun mereka, 80% pengguna Android dan 23% pengguna iOS belum menginstal pembaruan perangkat lunak terbaru pada perangkat mereka, membuat mereka terpapar pada ancaman *cyber*, dan 87% orang rentan akan risiko dalam menggunakan Wi-Fi publik.[5]

Kerja sama di bidang *cyber security* adalah salah satu kegiatan yang dapat meningkatkan keamanan siber suatu negara untuk mencegah dan menanggulangi kejahatan siber. Kerja sama Badan Siber dan Sandi negara (BSSN) mewakili Indonesia, dengan *Department Of Foreign Affairs And Trade* (DFAT) mewakili Australia dalam pengembangan *cyber security* merupakan sebuah strategi Indonesia di tingkat internasional dalam mencegah kejahatan siber.

Kemajuan teknologi dan informasi kini telah mengubah peradaban dunia dan menyebabkan ancaman terhadap sebuah negara menjadi semakin kompleks. Salah satunya ditandai dengan adanya ancaman *cyber*. Untuk mencegah dan menanggulangi ancaman ini, maka suatu negara memiliki urgensi untuk mengembangkan aspek keamanan nasionalnya menjadi lebih luas, dalam hal ini yakni: keamanan siber atau *cyber security*. Salah satu strategi sebuah negara dalam mengembangkan *cyber security* adalah dengan menjalin kerja sama dengan negara lain. Indonesia dan Australia merupakan negara yang *concern* dalam bidang *cyber security*, untuk itu kedua negara ini bekerja sama dalam pengembangan *cyber security*. Berdasarkan penjelasan diatas, maka dapat dirumuskan suatu masalah yaitu: **"Apa bentuk kerja sama Badan Siber dan Sandi Negara (BSSN) Indonesia dengan *Department Of Foreign Affairs And Trade* (DFAT) Australia dalam pengembangan *cyber security di Indonesia*?"**

## KERANGKA TEORI

Perspektif yang digunakan dalam penelitian ini adalah neorealisme. Neorealisme berasumsi bahwa negara adalah aktor yang rasional maka selalu mengejar strategi yang meminimalkan kerugian dan memaksimalkan keuntungan. Neorealis memaparkan bahwa negara dituntut untuk meningkatkan kapabilitas negaranya untuk bertahan dalam kondisi yang anarki. Hal tersebut didasari oleh situasi dunia yang anarki dan mengharuskan suatu negara dapat bersaing dalam menjaga eksistensi kapabilitas negaranya.

Neorealisme beranggapan bahwa kerja sama internasional dinilai masih tetap dapat dilakukan dengan cara terbuka, dimana negara harus mencapai keuntungan masing-masing dalam melakukan kerja sama. Konsep

[5] One in four Australians hit by cybercrime - reversing the threat, (diakses dari *https://www.cyber.gov.au/acsc/view-all-content/media-releases/one-four-australians-hit-cybercrime-reversing-threat* pada 09 Juli 2020).

kerja sama yang diterapkan oleh kaum neorealis adalah konsep *absolute gains*. Dimana salah satu pihak yang terlibat dalam suatu kerja sama akan mendapatkan keuntungan lebih dari pihak lainnya.[6]

Teori yang digunakan pada penelitian ini adalah Teori Kerja Sama Internasional. Setiap negara membutuhkan kerja sama dengan negara lainnya karena adanya kondisi saling ketergantungan sesuai dengan kepentingan masing-masing pihak. Kerja sama internasional merupakan suatu bentuk hubungan yang dilakukan oleh aktor internasional dengan aktor lainnya yang bertujuan untuk meraih keuntungan dan kepentingan nasional.

Dalam penelitian ini teori kerja sama internasional yang digunakan adalah kerja sama bilateral. Kerja sama bilateral merupakan keadaan yang menggambarkan adanya hubungan timbal balik dan saling mempengaruhi antara dua negara. Kerja sama bilateral tidak terlepas dari kepentingan nasional masing-masing negara dan tidak tergantung pada letak geografis dan memiliki tujuan untuk mewujudkan kepentingan nasional negara tersebut.[7]

Konsep yang digunakan dalam penelitian ini adalah *cyber security*. *Cyber security* yang lemah dapat menciptakan ketegangan di antara negara-negara dan mengganggu stabilitas keamanan, menciptakan dampak sosial, ekonomi, dan lingkungan, serta mengganggu hubungan antar negara. *Cyber security* memiliki dua kata kunci: *cyber* dan *security*. Berbicara tentang *cyber* berarti berbicara tentang informasi, koneksi (telekomunikasi, jaringan), *gateway* (komputer, perangkat, pengguna) dan ini tentang melibatkan, menggunakan, atau berkaitan dengan komputer, jaringan, dan internet. Sementara itu, *security* biasanya terkait dengan aset dan perlindungan aset. *Security* melindungi aset, melindungi komputer, jaringan, program, dan data dari akses, perubahan, atau perusakan yang tidak disengaja atau tidak sah, melindungi informasi dan sistem dari *cyber attack*.[8]

## HASIL DAN PEMBAHASAN

Penelitian ini berfokus pada kerja sama bilateral di bidang keamanan siber antara Indonesia dan Australia yang diwakili oleh Badan Siber dan Sandi Negara (BSSN) dan *Department of Foreign Affairs and Trade* (DFAT). Peneliti memaparkan apa saja bentuk-bentuk kerja sama bilateral antara BSSN dan DFAT dalam pengembangan keamanan siber atau *cyber security* di Indonesia.

### Bentuk Kerja Sama Bilateral BSSN dan DFAT dalam Pengembangan Cyber Security di Indonesia

Indonesia dan Australia sepakat untuk menjalin kerja sama di bidang *cyber security* yang dilandasi dengan MoU antara kedua negara pada tanggal 31 Agustus 2018. Di dalam MoU telah disepakati bahwa untuk implementasi

[6] David A. Baldwin, *Neorealism and Neoliberalism: The Contemporary Debate*, (Columbia University Press, 1993). Hal 4-5.

[7] Dwi Wahyu Handayani, Agus Hadiawan, Aman Toto Dwijono, Dinamika Kerjasama Indonesia Dan Malaysia Tentang Penempatan Dan Perlindungan Tenaga Kerja, *Jurnal Sosiologi*, Vol. 17, No. 1: 31-41.

[8] S. Ghernaouti-Hélie, *Cybersecurity Guide for Developing Countries*, (Geneva: International Telecommunication Union, 2009) Hal. 18.

kerja sama ini diserahkan kepada dua pihak yaitu; untuk Republik Indonesia adalah Badan Sandi dan Siber Negara (BSSN), untuk Australia adalah *Department of Foreign* and *Affairs* (DFAT). Selama perjanjian ini berlangsung, telah terlaksana beberapa kegiatan sesuai dengan MoU diantaranya *cyber boot camp, ASPI (Australian Strategic Policy Institute) cyber policy workshop, cyber business connection*, dan *cyber policy dialogue.*

## A. *Cyber Boot Camp*

*Cyber Boot Camp* merupakan sebuah *project* dari *Cyber Cooperation Program* yang dimiliki oleh DFAT. Program ini merupakan bentuk kerja sama Australia dengan negara mitra nya di seluruh Indo-Pasifik untuk meningkatkan *cyber security*. 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.

**Gambar 1. *Cyber Boot Camp* BSSN dan DFAT**

Sumber: *Australian National University; National Security College*

BSSN sebagai salah satu mitra kerja sama DFAT di bidang *cyber security* juga melaksanakan kegiatan *Cyber Boot Camp* ini. *Cyber Boot Camp* merupakan kegiatan yang memberikan pelatihan serta pembelajaran kepada utusan dari BSSN. Kegiatan ini bertujuan untuk membangun pengetahuan dan kesadaran peserta di mulai dari kesiapan teknologi, ancaman *cyber*, hingga pengambilan keputusan dan sifat *cyberspace*.

*Cyber Boot Camp* merupakan program intensif selama dua minggu di Australia. Dalam kegiatan ini para peserta megikuti *workshop*, latihan, kunjungan lokasi industri, dan dialog dengan lembaga pemerintah Australia. Dengan kegiatan ini, Australia berharap peserta akan mengimplementasikan pelatihan dan pembelajaran dalam menanggapi ancaman *cyber* yang relevan di Indonesia dan akan berkontribusi untuk *cyber security* yang kuat di Indo-Pasifik.

Melalui kegiatan *cyber boot camp* ini, CEO ANU *Cyber Institute* Dr. Lesley Seebeck mengatakan kegiatan ini berfokus pada pengembangan keterampilan bagi para delegasi untuk dapat lebih memahami, membangun, dan merawat sistem *cyber security* dalam mencegah *cyber attack*. Australia juga merancang kegiatan ini untuk menyatukan keterampildan dan keahlian dari para delegasi yang akan memperluas keahliannya kepada sektor pemerintah, akademisi, maupun swasta.[9] Seperti yang dilansir oleh KOMINFO, Indonesia kekurangan sumber daya manusia dalam aspek *cyber security* dan setidaknya

[9] ANU, "New bootcamp to help build cyber resilience in the region" (diakses dari *https://crawford.anu.edu.au/news-events/news/15523/new-bootcamp-help-build-cyber-resilience-region* pada 30 September 2020).

membutuhkan 1000 tenaga ahli dalam bidang ini.[10] Maka dengan adanya *cyber boot camp* ini diharapkan akan dapat menutup kekurangan sumber daya manusia Indonesia di dalam bidang *cyber security*.

## B. *ASPI (Australian 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.[11]

Kegiatan ini dilaksanakan pada 01 November 2018 di Jakarta. Materi yang dipaparkan mengenai *Cyberspace and Cybersecurity, Risk Management, Strategy and Risk Controls, Network Security,* dan *Software Security, Security Architecture*. Dalam *cyber risk management*, ancaman dapat dibagi menjadi dua yaitu secara sengaja dan tidak sengaja, misal ancaman secara sengaja adalah tindakan kriminal dan teroris sehingga akan berdampak pada sosial, ekonomi, politik, pemerintahan.

**Gambar 2. *ASPI (Australian Strategic Policy Institute) Cyber Policy Workshop***

Sumber: *Twitter Tobias Feakin*

Dengan adanya kegiatan *ASPI Cyber Policy Workshop*, Indonesia yang masih memerlukan tindakan yang akurat dalam *risk management* di bidang *cyber security* diharapkan lebih dapat memperkuat analisis ancaman cyber yang masih sering terjadi di Indonesia. *Risk management* merupakan elemen fundamental dari sebuah strategi. Dari *risk management* dapat diperhitungan sebuah anggaran biaya yang diperlukan.

Dalam penanggulangan *cyber attack*, tidak sedikit biaya yang dikeluarkan dalam pengamanan kerahasian informasi dan data sebuah negara. Oleh karena itu, *risk management* yang strategis menjadikan langkah dalam menanggulangi *cyber attack* lebih terjangkau.[12] Selain itu, melalui kegiatan *ASPI Cyber Policy Workshop* ini diharapkan para

[10] KOMINFO, "Indonesia kekurangan Bakat Cyber Security" (diakses dari *https://kominfo.go.id/content/detail/8574/indonesia-kekurangan-bakat-cyber-security/0/sorotan_media* pada 30 September 2020).

[11] DFAT, "Cyber Cooperation Program: Partner" (diakses dari *https://www.dfat.gov.au/international-relations/themes/cyber-affairs/cyber-cooperation-program/Pages/meet-our-partners* pada 19 September 2019).

[12] Ineu Rahmawati, Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense, *Jurnal Pertahanan & Bela Negara* Volume 7 Nomor 2 (Agustus 2017) Hal. 60

pemangku kepentingan yang berada di bidang *cyber security* di Indonesia dapat saling koordinasi dan berkolaborasi untuk mengatasi ancaman *cyber* dan memperkuat *cyber security* dengan memanfaatkan langkah yang strategis.

### C. *Cyber Business Connection*: *Austrade* dan *AustCyber* dalam Pengembambang *Cyber Security* di Bidang Ekonomi Digital

Kunjungan perusahaan *cyber security* Australia yang diselenggarakan oleh *Austrade* ke Jakarta memperlihatkan beberapa solusi agar bisnis di era ekonomi digital dapat bekerja. Delegasi tersebut terdiri dari perusahaan yang memiliki sistem untuk perlindungan data, enkripsi, dan pengujian. Diselenggarakan bersama oleh organisasi perwakilan industri *AustCyber* dan *Austrade*, kunjungan pada 08 Janurari 2019 tersebut mempertemukan perusahaan Australia dengan pejabat dan bisnis Indonesia.

**Gambar 3. *AustCyber dalam rangka cyber security di bidang ekonomi digital***

Sumber: *Australia-Indonesia Centre*

Direktur Pengkajian Identifikasi dan Kerentanan BSSN yaitu Nur Achmadi telah bekerja sama dengan delegasi Australia sebagai bentuk kerja sama bilateral antara Indonesia dengan Australia di bidang *cyber security*. Dalam sektor ekonomi digital Indonesia sedang menguji sistem pemerintah, termasuk yang di daerah. Hal ini dilakukan untuk keamanan dan perlindungan data tingkat tinggi yang sesuai dengan standar ISO 27000 dalam aktivitas menggunakan *e-commerce*.

Melalui kegiatan *cyber business connection* ini, selain rancangan dalam pengembangan sektor ekonomi digital seperti mengembangkan penggunaan sertifikat digital dalam perdagangan impor dan ekspor, Indonesia yang dianggap oleh Australia sebagai negara potensial dengan perekonomian digital terbesar diharuskan siap dalam era digital beserta ancamannya. Munculnya berbagai *e-commerce* berarti menimbulkan ancaman baru seperti data 13 juta akun Bukalapak yang bocor dan diperjualbelikan di dalam forum *hacker*.[13] Dengan adanya kegiatan ini, diharapkan akan memberi pemahaman bagi para pelaku ekonomi digital di Indonesia untuk dapat mengembangkan bisnisnya dan melindungi pelanggannya.

### D. *Third Cyber Policy Dialogue*

*Cyber Policy Dialogue* yang ketiga diselenggarakan secara virtual pada tanggal 2 September 2020. Kegiatan ini dipimpin oleh Kepala BSSN Hinsa Hasibuan, delegasi Australia dipimpin oleh Duta Besar untuk *cyber affairs*, Dr. Tobias Feakin. *Cyber Policy Dialogue* merupakan kegiatan rutin tahunan tindak lanjut

[13] CNN "13 Juta Data Bocor Bukalapak Dijual di Forum Hacker" (diakses dari *https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker* pada 30 September 2020).

kesepakatan bilateral antara Presiden Republik Indonesia dan Perdana Menteri Australia pada tahun 2017.[14]

*Cyber Policy Dialogue* tersebut bertujuan mempererat kerja sama di bidang *cyber security* 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 *cyberspace*, termasuk tantangan utama dan pendekatan praktik terbaik untuk mengelola ancaman strategis, strategi keamanan siber nasional, dan legislasi yang relevan.

**Gambar 4. *Third Indonesia-Australia Cyber Policy Dialogue***

Sumber: *DFAT*

*Cyber Policy Dialogue* ini menunjukkan komitmen berkelanjutan lembaga penegak hukum Indonesia dan Australia untuk menangani *cyber threat*. Para peserta menggaris bawahi pentingnya lembaga penegak hukum nasional yang mampu dan kuat, serta kemitraan internasional yang melibatkan pemerintah, organisasi internasional, dan sektor industri digital.

Dengan adanya dialog ini, memberikan kesempatan untuk meninjau MoU Indonesia Australia tentang kerja sama di bidang *cyber security* 2018, termasuk hasil positif yang diperoleh dari berbagi informasi dan praktik terbaik, serta mendukung pengembangan keterampilan, termasuk melalui *Cyber Boot Camp*. Para peserta sepakat untuk terus berkolaborasi dalam inisiatif bersama untuk memperkuat ketahanan siber secara nasional dan di kawasan serta setuju untuk memperpanjang MoU selama dua tahun ke depan.[15]

## Analisis Kerja Sama BSSN dan DFAT dalam Pengembangan *Cyber Security*

Sebagaimana yang tercantum dalam MoU Indonesia dan Australia tentang kerja sama di bidang *cyber security*, kerja sama ini terbentuk karena kedua negara saling mengakui adanya peningkatan interkonektivitas serta sistem informasi dan jejaring yang berdampak kepada peningkatan ancaman dan kerawanan yang dapat mengancam kesejahteraan dan keamanan nasional. Maka dari itu, kedua negara berkeinginan untuk mempromosikan penggunaan internet di *cyberspace* yang terbuka, bebas, dan aman yang diharapkan akan mendorong pertumbuhan ekonomi,

[14] DFAT, "Third Australia-Indonesia Cyber Policy Dialogue" (diakses dari *https://www.dfat.gov.au/news/news/third-australia-indonesia-cyber-policy-dialogue* pada 19 September 2020).

[15] BSSN, "BSSN Inisiasi Lanjutan Kerja Sama Keamanan Siber Indonesia-Australia dalam 3rd Indonesia-Australia Cyber Policy Dialogue" (diakses dari *https://bssn.go.id/bssn-inisiasi-lanjutan-kerjasama-keamanan-siber-indonesia-australia-dalam-3rd-indonesia-australia-cyber-policy-dialogue/* pada 19 September 2020).

perlindungan keamanan nasional, dan stabilitas internasional.

Upaya kedua negara diwujudkan dengan adanya kerja sama di bidang *cyber security* ini. Dalam kurun waktu 2 tahun, kerja sama telah terjalin dengan beberapa bentuk seperti *Cyber Boot Camp, ASPI (Australian Strategic Policy Institute) Cyber Policy Workshop, Cyber Business Connection*: *Austrade* dan *AustCyber*, dan *Cyber Policy Dialogue*.

Bagi Indonesia, kerja sama ini selain untuk meningkatkan kapabilitas *cyber security*, juga untuk meningkatkan peringkat Indonesia di *Global Cybersecurity Index* yang dimiliki oleh ITU (*International Telecommunication Union*). Survey yang dilakukan ITU untuk mengukur komitmen negara-negara anggota terhadap *cyber security*. Tujuan GCI adalah untuk membantu negara-negara mengidentifikasi area yang harus diperbaiki dalam dunia *cyber security*, sehingga membantu meningkatkan tingkat komitmen keseluruhan terhadap *cyber security* di seluruh dunia.[16]

**Tabel 1.** ***Indonesia-Australia Global Cybersecurity Index (GCI) 2017-2018***

| 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 |

Sumber: *ITU Global Cybersecurity Index* Tahun 2017 dan 2018

Menurut tabel diatas yang berdasarkan survey oleh ITU terhadap komitmen negara-negara di dunia terhadap cyber security, pada tahun 2017 Indonesia termasuk pada *maturing stage* yeng 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*. Menurut BSSN, hal ini merupaka pencapaian atas keberhasilan kinerja seluruh pemangku kepentingan *cyber security* yang dikonsolidasikan oleh BSSN dalam membangun dan mengembangkan ekosistem *cyber security*[17]

Kerja sama bilateral yang dijalin antara Indonesia dan Australia di bidang cyber security meningkatkan nilai komitmen Indonesia terhadap cyber security sesuai dengan point ke-lima dari ITU yaitu *cooperation*. Melalui berbagai bentuk kerja sama yang telah dilaksanakan antara kedua negara juga meningkatkan kapabilitas Indonesia di bidang *cyber security*. Dengan peningkatan Indonesia di GCI 2018 membuktikan bahwa kerja sama antara Indonesia dan Australia memberi keuntungan kepada Indonesia.

[16] Maulia Jayantina Islami, "Tantangan Dalam Implementasi Strategi Keamanan Sibernasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index" *Jurnal Masyarakat Telematika dan Informasi* Volume: 8 No. 2 (Oktober - Desember 2017) Hal. 139

[17] Christoforus Ristianto, "BSSN Raih Peringkat ke-41 dalam Global Cyber Security Index" (diakses dari *https://nasional.kompas.com/read/2019/05/24/16374011/bssn-raih-peringkat-ke-41-dalam-global-cyber-security-index* pada 20 September 2020).

## PENUTUP

Indonesia dan Australia sepakat untuk menjalin kerja sama di bidang *cyber security* yang dilandasi dengan MoU antara kedua negara pada tanggal 31 Agustus 2018. Di dalam MoU telah disepakati bahwa untuk implementasi kerja sama ini diserahkan kepada dua pihak yaitu; untuk Republik Indonesia adalah Badan Sandi dan Siber Negara (BSSN), untuk Australia adalah *Department of Foreign* and *Affairs* (DFAT). Merujuk pada MoU, BSSN dan DFAT akan melakukan kerja sama di bidang; Berbagi Informasi dan *Best Practice*, Peningkatan Kapasitas dan Penguatan Koneksi, Ekonomi Digital, dan Kejahatan *Cyber*. Selain itu terdapat juga *Cyber Policy Dialogue* yang tetap diteruskan pelaksanaannya sebagai salah satu bentuk kerja sama BSSN dan DFAT di bidang *cyber security*. Bentuk kerja sama antara BSSN dan DFAT yaitu berupa; *Cyber Boot Camp*, ASPI (*Australian Strategic Policy Institute*) *Cyber Policy Workshop*, *Cyber Business Connection* (*Austrade* dan AustCyber), dan *Cyber Policy Dialogue*.

## DAFTAR PUSTAKA


ANU, "New bootcamp to help build cyber resilience in the region" (diakses dari *https://crawford.anu.edu.au/news-events/news/15523/new-bootcamp-help-build-cyber-resilience-region* pada 30 September 2020).

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). Laporan Survei Penetrasi & Profil Perilaku Pengguna Internet Indonesia (diakses dari *https://apjii.or.id/survei* pada 29 Januari 2020).

Baldwin, David A., Neorealism and Neoliberalism: The Contemporary Debate. Columbia University Press. 1993.

BSSN, "BSSN Inisiasi Lanjutan Kerja Sama Keamanan Siber Indonesia-Australia dalam 3rd Indonesia-Australia Cyber Policy Dialogue" (diakses dari *https://bssn.go.id/bssn-inisiasi-lanjutan-kerjasama-keamanan-siber-indonesia-australia-dalam-3rd-indonesia-australia-cyber-policy-dialogue/* pada 19 September 2020).

CNN, "*13 Juta Data Bocor Bukalapak Dijual di Forum Hacker*" (diakses dari *https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker* pada 30 September 2020).

DFAT, "Cyber Cooperation Program" (diakses dari *https://www.dfat.gov.au/international-relations/themes/cyber-affairs/cyber-cooperation-program/Pages/cyber-cooperation-program* pada 18 September 2020).

_____, "Third Australia-Indonesia Cyber Policy Dialogue" (diakses dari *https://www.dfat.gov.au/news/news/third-australia-indonesia-cyber-policy-dialogue* pada 19 September 2020).

Ghernaouti-Hélie, S. Cybersecurity

Guide for Developing Countries, Geneva: International Telecommunication Union. 2009.

Handayani, Dwi Wahyu, Agus Hadiawan, Aman Toto Dwijono. "Dinamika Kerjasama Indonesia Dan Malaysia Tentang Penempatan dan Perlindungan Tenaga Kerja". *Jurnal Sosiologi*, Vol. 17, No. 1

Haryanto, Agus Tri. "Indonesia Dibombardir 207 Juta Serangan Siber dalam 10 Bulan", (diakses dari *https://inet.detik.com/security/d-4340493/indonesia-dibombardir-207-juta-serangan-siber-dalam-10-bulan* pada 25 Juli 2020).

Internet Activity Australia, (diakses dari *https://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/* pada 09 Juli 2020).

Islami, Maulia Jayantina. "Tantangan Dalam Implementasi Strategi Keamanan Sibernasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index" *Jurnal Masyarakat Telematika dan Informasi* Volume: 8 No. 2 (Oktober - Desember 2017).

ITU, "Statistics" International Telecommunication Union (diakses dari *https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx* pada 18 Januari 2020).

KOMINFO, "Indonesia kekurangan Bakat Cyber Security" (diakses dari *https://kominfo.go.id/content/detail/8574/indonesia-kekurangan-bakat-cyber-security/0/sorotan_media* pada 30 September 2020).

One in four Australians hit by cybercrime - reversing the threat, (diakses dari *https://www.cyber.gov.au/acsc/view-all-content/media-releases/one-four-australians-hit-cybercrime-reversing-threat* pada 09 Juli 2020).

Rahmawati, Ineu. "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense". *Jurnal Pertahanan & Bela Negara* Volume 7 Nomor 2 (Agustus 2017).

Ristianto, Christoforus ."BSSN Raih Peringkat ke-41 dalam Global Cyber Security Index" (diakses dari *https://nasional.kompas.com/read/2019/05/24/16374011/bssn-raih-peringkat-ke-41-dalam-global-cyber-security-index* pada 20 September 2020).