KERJASAMA INDONESIA DENGAN AUSTRALIA DALAM KEAMANAN SIBER

Oleh: Afifah
Pembimbing: Dr. Yessi Olivia, S.IP., M.IntRel
Jurusan Hubungan Internasional
Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Riau
Kampus Bina Widya, Jl. H. R. Soebrantas Km 12,5 Simp. Baru, Pekanbaru 28293
Telp/Fax. 0761-63277

ABSTRAK

Keamanan siber merupakan salah satu upaya melindungi dan menjaga keamanan nasional dari ancaman yang dapat merusak dikarenakan adanya perkembangan globalisasi yang ditandai dengan kemajuan teknologi dan konektivitas digital antar negara sehingga memiliki resiko terhadap penyebaran kejahatan siber lintas negara.

Penelitian ini menggunakan metode kualitatif deskriptif dengan teknik pengumpulan data yang dilakukan melalui analisis dokumen berdasarkan sumber yang diperoleh dari dokumen resmi pemerintah, berita, dan artikel jurnal yang berkaitan dengan kerja sama keamanan siber. Penelitian ini menggunakan teori diplomasi siber untuk menjelaskan upaya kerja sama bagi keamanan siber pada kedua negara.

Hasil penelitian menunjukkan bahwa Indonesia dan Australia melakukan kerja sama sebagai upaya meningkatkan kepentingan nasional dari masing-masing negara berupa peningkatan keamanan Indonesia dan Australia serta kawasan Indo-Pasifik, dan juga sebagai upaya dalam mempererat hubungan antar kedua negara.
Kata Kunci: Kerja Sama Bilateral, Keamanan Siber, Indonesia, Australia, Kejahatan Siber

ABSTRACT

Cybersecurity is one of the efforts to protect and maintain national security from treats that can damage due to the development of globalization which is marked by technological advances and digital connectivity between countries so that it has a risk of spreading cybercrime across countries.

The research uses descriptive qualitative methods with data collection techniques carried out through document analysis based on sources obtained from official government documents, news, and journal articles related to cybersecurity cooperation. This research uses cyber diplomacy theory to explain cooperation efforts for cybersecurity in both countries.

The results showed that Indonesia and Australia cooperated as an effort to improve the national interests of each country in the form of increasing the security of Indonesia and Australia and the Indo-Pacific region, and also as an effort to strengthen relations between the two countries.
Keywords: *Bilateral Cooperation, Cyber Security, Indonesia, Australia, Cyber Crime*

PENDAHULUAN

Kejahatan siber menjadi aktivitas kejahatan pada era ini yang terjadi karena adanya dampak negatif dari perkembangan teknologi yang dapat dilakukan oleh individu maupun kelompok terorganisir yang dapat merugikan targetnya dengan menyebarkan perangkat lunak berbahaya *(malware)* yang bersifat ilegal. Kejahatan ini menggunakan komputer dan jaringan komputer sebagai unsur utamanya dalam mempermudah terjadinya kejahatan yang dilakukan dalam aktivitas kejahatan transnasional.[1]

Kejahatan siber berbeda dari kejahatan tradisional karena memanfaatkan infrastruktur digital yang berbasis pada kemajuan teknologi informasi dan komunikasi, tanpa identitas *(anonymous)*, tanpa kekerasan *(non-violence)*, bersifat transnasional, dan menimbulkan kerugian yang lebih buruk dari kejahatan lain baik secara material maupun non-material berupa waktu, uang, dan informasi dan data yang bersifat rahasia.

Indonesia merupakan salah satu negara dengan tingkat kejahatan siber tertinggi karena berada pada peringkat ke-8 serangan berbasis web *(Web Based Attack)* serta termasuk dalam peringkat 10 besar negara dengan jumlah insiden tertinggi di wilayah Asia Pasifik, hal tersebut dikarenakan jumlah penduduk Indonesia yang terus bertambah dengan pengguna internet yang cukup banyak mengakibatkan Indonesia menjadi rentan terhadap ancaman kejahatan siber terutama penipuan yang dilakukan secara online.[2]

Sama halnya dengan Indonesia, tingkat kejahatan siber di Australia juga cukup tinggi. Berdasarkan data dari ACSC, sekitar 50% responden dalam survei menyatakan pernah mengalami insiden kejahatan siber minimal satu kali pada tahun 2015 dengan berbagai macam jenis kasus kejahatan siber, diantaranya *malware*, virus, email berbahaya *(malicious email)*, pencurian informasi, akses tidak sah *(unauthorised access)*, RATs, dan DDOS.[3]

Salah satu kasus kejahatan siber yang dialami secara global yaitu serangan *Ransomware WannaCry* yang terjadi pada bulan Mei 2017. Serangan ini menginfeksi lebih dari 200.000 komputer di lebih dari 150 negara yang terdampak secara global dimana Indonesia dan Australia menjadi salah satu negara yang terinfeksi *cyber attack Ransomware WannaCry*.

Di Indonesia *cyber attack Ransomware WannaCry* menginfeksi komputer dengan mengenkripsi dan memblokir akses terhadap data serta informasi pasien di Rumah Sakit Dharmais di Jakarta pada 13 Mei 2017.[4] Di Australia, serangan ini menyerang pelaku usaha kecil pada tahun 2017[5] serta menyerang

[1] Hadion Wijoyo et al., "Cyber Crime," in *Encyclopedia of Cyber Warfare* (PT Mafy Media Literasi Indonesia, 2024), 1–3.

[2] Bambang Supriyadi, "Persepsi Bersama Indonesia-Australia Hibah Dana Dan Peralatan Investigasi Cyber Crime Australia Kepada Indonesia," *Journal of International Relations* 3, no. 1 (2017): 144–145.

[3] Ibid., 144.

[4] "Kasus Ransomware Di Indonesia: Ancaman, Contoh Kasus, Dan Cara Melindungi Bisnis Anda," *Rizki Tujuhbelas Kelola*, last modified 2024, https://r17.co.id/insight/article/kasus-ransomware-di-indonesia-ancaman-contoh-kasus-dan-cara-melindungi-bisnis-anda.

[5] Dominic Powell, "'WannaCry' Ransomware Hits 12 Australian Small Businesses: Four Ways To Protect Your

komputer yang mengendalikan kamera pengawas kecepatan dan lampu lalu lintas di negara bagian Victoria yang digunakan untuk mendenda para pengendara.[6]

Situasi ini memerlukan upaya kerja sama dari berbagai negara untuk menjaga keamanan pada ruang siber. Tanpa adanya kerja sama dari berbagai negara maka keamanan pada ruang siber tidak dapat terbentuk mengingat kejahatan siber bersifat lintas batas. Karena itu gabungan dari kekuatan internasional diperlukan untuk menciptakan ruang siber yang aman dan stabil.

KERANGKA TEORI

Teori: Diplomasi Siber

Penelitian ini menggunakan teori Diplomasi Siber yang menekankan pentingnya melakukan diplomasi dan bekerja sama dalam bidang siber. Menurut Danca, diplomasi siber merupakan serangkaian tindakan dan sikap para aktor internasional yang melibatkan beberapa hal penting termasuk menjaga komunikasi dengan negara lain, bekerjasama dalam forum internasional untuk mencari solusi, dan mengatasi kesalahpahaman, membangun budaya global yang peduli terhadap keamanan dunia maya, serta memperkuat kepercayaan antar negara. Selain itu, kerja sama ini juga bertujuan untuk mendorong transparansi dalam komunikasi, memahami potensi dan keunggulan dunia maya, fokus pada kerentanan internal dibandingkan eksternal, dan perlu menyadari akan resiko, ancaman, dan kerentanan siber.[7]

Tingkat Analisa: Negara

Penelitian ini menggunakan tingkat analisis negara *(nation-state)* yang memandang negara sebagai aktor utama dalam hubungan internasional karena negara memiliki otoritas penuh untuk menetapkan kebijakan dan bertindak berdasarkan kepentingan nasional, termasuk menjaga kedaulatan, keamanan, serta stabilitas pada keamanan siber. Pendekatan ini memungkinkan penelusuran terhadap bentuk kerja sama bilateral antara Indonesia dan Australia dalam penguatan keamanan siber.

Fokus utama terletak pada kerja sama untuk penguatan keamanan pada bidang siber yang dilakukan antara Indonesia dan Australia, dimana pada tahun 2013 Indonesia pernah mengalami penyadapan pada masa pemerintahan mantan Presiden Susilo Bambang Yudhoyono yang dilakukan oleh Australia. Tindakan yang dilakukan memperlihatkan upaya pemulihan hubungan yang sempat renggang antar kedua negara serta untuk kepentingan negara dan kawasan Indo-Pasifik.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif. Pendekatan ini bertujuan untuk menjelaskan dan memahami suatu fenomena berdasarkan data

Systems," *SmartCompany*, last modified 2017, https://www.smartcompany.com.au/technology/wannacry-ransomware-hits-12-australian-small-businesses-four-ways-to-protect-your-systems/.

[6] Tom Brant, "WannaCry Ransomware Hits Honda Plant, Traffic Cams," *PC Magazine,* last modified 2017, https://www.pcmag.com/news/wannacry-ransomware-hits-honda-plant-traffic-cams.

[7] Dana DANCĂ, "Cyber Diplomacy-A New Component of Foreign Policy," *Journal of Law and Administrative Sciences* 3, no. 3 (2015): 93, https://heinonline.org/HOL/License.

yang telah dikumpulkan melalui narasi dan analisis kontekstual. Fokus diarahkan pada upaya kerja sama yang dilakukan oleh Indonesia dan Australia dalam keamanan siber, sehingga interpretasi data bersifat mendalam dan berfokus pada makna strategis yang berkaitan dengan kerja sama.

Teknik pengumpulan data dilakukan melalui analisis dokumen, yaitu mengevaluasi dokumen maupun sumber yang berkaitan dengan kerja sama pada bidang siber secara mendalam berupa artikel jurnal, laporan, kebijakan pemerintah, buku, berita, maupun dokumen lainnya yang relevan. Pendekatan ini memberikan landasan yang komprehensif untuk menjelaskan bentuk dari kerja sama yang dilakukan oleh Indonesia dan Australia dalam bidang siber berdasarkan informasi yang telah tersedia secara sah dan terverifikasi. Data yang diperoleh dianalisis secara sistematis untuk membangun pemahaman terhadap kerja sama yang dilakukan oleh Indonesia dan Australia pada keamanan bidang siber secara bilateral serta kawasan.

HASIL DAN PEMBAHASAN

Kondisi Kejahatan Siber di Indonesia

Pada tahun 2002, Indonesia berada pada urutan kedua sebagai negara dengan tingkat kejahatan siber tertinggi di dunia setelah Ukraina dengan jenis kejahatan *carding* berdasarkan *data clear commerce*.[8] Pada tahun 2013, Indonesia menjadi salah satu negara korban serangan kejahatan siber global sebesar 38% dan melampaui Tiongkok sebagai negara sumber nomor satu dengan serangan siber terbesar di dunia yang memperlihatkan keseriusan pada permasalahan keamanan di bidang siber Indonesia.[9]

Berdasarkan analisis data pada sistem *monitoring* lalu lintas siber yang dilakukan oleh ID-SIRTII, website utama milik pemerintah Indonesia mulai dari tahun 1998 hingga 2008 telah menjadi sasaran utama dari serangan siber sebanyak 2.138 serangan.[10]

Pada tahun 2015, terdapat serangan kejahatan siber yang menyerang Indonesia sebesar 28.430.843 kasus dan pada tahun 2016 meningkat menjadi 135.672.984 kasus. Dari total keseluruhan kasus, sebanyak 47% berasal dari serangan *malware*, sebanyak 44% berasal dari penipuan, dan sisanya berasal dari bentuk ancaman kejahatan siber lain seperti perusakan situs web, aktivitas manipulasi data, dan kebocoran data.[11]

Pada tahun 2016, pengguna internet Indonesia meningkat sebesar 44,6 juta dengan total sebesar 132,7

[8] Hamsu Abdul Gani and Andika Wahyudi Gani, "Penyelesaian Kasus Kejahatan Internet (Cybercrime) Dalam Perspektif UU ITE No . 11 TAHUN 2008 Dan UU No . 19 Tahun 2016," *Prosiding Seminar Nasional LP2M UNM - 2019*, no. 11 (2019): 122.

[9] Thomas Paterson, "Indonesian Cyberspace Expansion: A Double-Edged Sword," *Journal of Cyber Policy* 4, no. 2 (2019): 219, https://doi.org/10.1080/23738871.2019.1627476.

[10] Afifah Fidina Rosy, "Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional Di Bidang Keamanan Siber," *Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan* 1, no. 2 (2020): 126.

[11] Maulia Jayantina Islami, "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index," *Masyarakat Telematika Dan Informasi* 8, no. 2 (2017): 139.

juta pengguna internet dari tahun 2014 yang hanya berjumlah sebesar 88,1 juta pengguna internet. Dalam kurun waktu 2 tahun (2014-2016) terjadi peningkatan yang begitu besar, maka jumlah ini akan terus bertambah seiring dengan perkembangan teknologi.[12] Pada tahun yang sama kasus ujaran kebencian menjadi kasus terbanyak di Indonesia dan terus mengalami peningkatan hingga tahun 2017 menjadi 3.325 kasus ujaran kebencian.[13]

Tingkat keamanan siber Indonesia masih rentan terhadap serangan kejahatan siber dikarenakan fasilitas yang masih minim, kurangnya tenaga ahli, dan juga kurangnya edukasi terhadap masyarakat Indonesia mengenai keamanan ruang digital yang mengakibatkan sejumlah besar komputer di Indonesia mudah diretas. Hal tersebut dibuktikan dengan data ITU pada tahun 2017 Indonesia menempati urutan ke-70 dalam GCI yang memperlihatkan bahwa tingkat keamanan yang dimiliki Indonesia masih rendah dalam menghadapi ancaman siber.[14]

Kondisi Kejahatan Siber di Australia

Masyarakat Australia mengalami kerugian finansial yang diakibatkan kejahatan siber yang secara keseluruhan kurang dari 1.000 dolar pada tahun 2009. Pada tahun tersebut kerugian finansial yang dialami tersebut mayoritas berasal penipuan *online*, tetapi beberapa diantaranya mencapai hingga lebih dari 50.000 dolar.[15]

Salah satu perusahaan siber terkemuka yaitu *Symantec* memperkirakan pada tahun 2013 Australia menanggung biaya aktivitas kejahatan siber sebesar US$1 Miliar atau 0,1 % dari PDB. *Symantec* juga memperkirakan terdapat 60% orang dewasa Australia menjadi korban kejahatan siber dengan biaya rata-rata per korban sekitar US$187 pada tingkat mikro (individu).[16]

Dalam segi infrastruktur, penting bagi Australia untuk mempertimbangkan kerentanan terhadap ancaman siber. Dalam survei global yang dilakukan dengan melibatkan 600 eksekutif pada bidang TIK dari berbagai perusahaan yang mengelola infrastruktur penting, terdapat 54% yang menyatakan bahwa mereka pernah mengalami serangan siber berskala besar sistem sektor infrastruktur mereka.[17]

Pada akhir bulan Desember tahun 2014 terdapat sebanyak lebih dari 12,6 juta pengguna internet *(broadband mobile)* dan sebanyak 21 juta pengguna layanan seluler dengan koneksi internet di Australia. Pada tahun yang sama CERT Australia merespon sekitar 11.073 insiden keamanan siber yang mempengaruhi bidang bisnis di Australia, 153

[12] Ahmad Saroji, Triana Harmini, and Muhammad Taqiyuddin, "Sejarah Evolusi Generasi Internet," *Jurnal Lani:Kajian Ilmu Sejarah & Budaya* 2, no. 2 (2021): 74.

[13] Ervina Chintia et al., "Kasus Kejahatan Siber Yang Paling Banyak Terjadi Di Indonesia Dan Penanganannya," *Journal of Information Engineering and Educational Technology* 2, no. 2 (2018): 66.

[14] ITU, *Global Cybersecurity Index (GCI) 2017*, 2017, 55, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[15] Bambang Supriyadi, "Persepsi Bersama Indonesia-Australia Hibah Dana Dan Peralatan Investigasi Cyber Crime Australia Kepada Indonesia," 144.

[16] Chris Brookes, *Cyber Security: Time For an Integrated Whole-of-Nation Approach in Australia*, *Indo-Pacific Strategic Papers*, 2015, 3.

[17] Ibid., 4.

diantaranya melibatkan kepentingan nasional, infrastruktur penting, dan pemerintah.[18]

Pada tahun 2014 jenis kejahatan siber yang menargetkan Australia yaitu serangan *malware* beberapa diantaranya yaitu Intrusi Siber, *Spear Phishing*, RAT, dan *Watering-Hole Techniques* mengakibatkan CERT Australia menangani lebih dari 8.100 insiden terkait malware ini. AISI melaporkan lebih dari 15.000 serangan *malware* setiap hari antara 17 Oktober 2014 hingga 14 Januari 2015 ke ISP Australia untuk ditindaklanjuti, 3 diantaranya yang sering kali terdeteksi yaitu *Zeus*, *ZeroAccess*, dan *Conficker*.[19]

Antara 01 Januari 2015 hingga 30 Juni 2016, ASD menanggapi sekitar 1.095 insiden siber pada sistem pemerintah yang diserang menggunakan ransomware dianggap cukup serius dan memerlukan tanggapan operasional.[20] Kemudian antara Juli 2015 hingga Juni 2016, CERT Australia menanggapi sekitar 14.804 insiden keamanan siber yang mempengaruhi sektor bisnis Australia, 418 diantaranya melibatkan sistem kepentingan nasional dan infrastruktur penting yang diakibatkan oleh tingginya aktivitas DDoS serta *email-phishing*.[21]

Aturan dan Badan Penegakan Hukum Mengenai Kejahatan Siber di Indonesia dan Australia

Keamanan siber berperan dalam struktur keamanan yang dilakukan untuk mengurangi hambatan dan melindungi hal yang bersifat rahasia. Ketiadaan dasar hukum yang kuat dalam siber dan kurangnya tenaga profesional membuat penguatan keamanan siber menjadi tantangan terbesar saat ini. Oleh karena itu, untuk mengantisipasi hal tersebut setiap orang perlu pemahaman mengenai teknologi agar melindungi data pribadi agar dapat terhindar dari kejahatan siber.

Bagi pemerintah, penting untuk mempersiapkan tenaga profesional yang dibutuhkan dalam meningkatkan keamanan siber, terus memperbarui sistem keamanan dan meningkatkan kesadaran masyarakat akan pentingnya berhati-hati dalam menggunakan internet terhadap resiko dari kejahatan siber, serta upaya untuk meningkatkan keamanan siber.

Di Indonesia, terdapat lembaga yang dibentuk secara khusus untuk menangani berbagai macam ancaman pada ruang digital yaitu BSSN. Terdapat aturan mengenai tindak pidana siber dibahas secara khusus yang terdapat dalam Undang Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik (ITE) yang telah diamandemen menjadi UU 19/2016. Dalam bab VII dalam UU ITE membahas mengenai perbuatan yang dilarang yang terdapat dari Pasal 27 hingga Pasal 35, serta terdapat ketentuan pidana yang dimuat dalam bab XI yang terdapat dari Pasal 45 hingga Pasal 51.[22]

[18] ACSC, *ACSC Australian Cyber Security Centre 2015 Threat Report, Australian Cyber Security Center*, 2015, 5–7.
[19] Ibid., 11–14.
[20] ACSC, *ACSC Australian Cyber Security Centre 2016 Threat Report, Australian Cyber Security Centre*, 2016, 10.
[21] Ibid., 14–15.
[22] *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi*

Australia memiliki aturan yang berlaku di negaranya untuk menangani kejahatan siber. Pada tingkat federal, *Criminal Code Act 1995* dan *Telecommunications (Interception and Access) Act 1979* mencakup kejahatan yang mengarah pada komputer, teknologi, infrastruktur, dan sistem telekomunikasi. Cakupan kejahatan tersebut seperti akses tidak sah (ilegal) dan DDoS. Pemerintah Australia mengamati bahwa perlunya pembaharuan hukum lebih lanjut untuk perkembangan teknologi yang semakin pesat dan kemudian menghadirkan *Cybercrime Act 2001*.[23]

Negara bagian juga memiliki aturan yang berlaku di wilayahnya masing masing, aturan tersebut telah disesuaikan agar selaras dengan *Criminal Code Act 1995*. Beberapa diantaranya seperti negara bagian New South Wales yang memiliki *Crimes Act 2001* (NSW) terkait dengan tindak pidana teknologi dan komunikasi serta negara di negara bagian Victoria yang memiliki *Crimes Act 1958* (Vic) terkait dengan kejahatan digital.[24]

Di Australia, tanggung jawab keamanan siber secara operasional didominasi oleh ASD yang merupakan departemen pertahanan sebagai otoritas utama dan ACSC yang bertanggung jawab dalam menangani insiden keamanan siber, intelijen, dan analisis ancaman yang bertanggung jawab dalam aspek operasional dan teknis secara nasional di Australia.[25]

Kejahatan siber yang Dilakukan oleh Indonesia dan Australia Satu Sama Lain

Pada tahun 2013, terungkap adanya kasus penyadapan yang dilakukan oleh Australia terhadap Indonesia yang diketahui melalui data yang dibocorkan oleh Edward Snowden yang berisi daftar dari negara negara yang menjadi target penyadapan beserta pelaku penyadapan yaitu badan intelijen Amerika Serikat dan Australia. Jauh sebelum itu, ternyata Australia telah menyadap Indonesia yaitu sejak pertengahan tahun 1950.[26]

Kasus tersebut membuat Indonesia merespon dengan meminta penjelasan resmi dari Pemerintah Australia, kemudian Perdana Menteri Tony Abbott menanggapi dengan menyatakan bahwa Australia tidak perlu mengeluarkan pernyataan maaf atas tindakan tersebut karena Indonesia diduga menyadap anggota Parlemen Australia pada dekade 1990-an.

Tanggapan tersebut membuat Indonesia mengungkapkan protes dengan cara menghentikan sementara seluruh kerja sama, mengutus Duta Besar Indonesia untuk Australia agar pulang serta meminta keterangan

Dan Transaksi Elektronik, 2008, 14–17, https://peraturan.bpk.go.id/Home/Details/37589/uu-no-11-tahun-2008.

[23] Nelson Chan, Simon Coronel, and Yik Chiat Ong, "The Threat of The Cybercrime Act 2001 To Australian IT Professionals" (2003): 25–33..

[24] Niloufer Selvadurai, "The Relevance of Technology Neutrality to the Design of Laws to Criminalise Cyberbullying," *International Journal of Law and Public Administration* 1, no. 2 (2018): 14–22.

[25] Leuprecht Christian and Stephanie MacLellan, *Governing Cyber Security in Canada, Australia and the United States*, *Center for International Governance Innovation*, 2018, 14.

[26] Ahmad Mafud Shaffan, "Respons Indonesia Terhadap Kasus Penyadapan Australia," *Journal of International Relations* 4, no. 2 (2018): 285–294.

resmi dari Duta Besar Australia untuk Indonesia.[27]

Kasus penyadapan tersebut juga memicu tanggapan para kelompok peretas Indonesia (AnonIndo). Dua pekan setelahnya terdapat laporan bahwa lebih dari 170 situs Australia telah diretas termasuk AFP dan RBA serta sebagian besar mengarah pada bisnis kecil karena mayoritas serangan diarahkan pada situs web yang berakhiran dengan alamat "au.' Berbentuk serangan *deface* dan DDoS.

Para peretas Australia (AnonAU) tidak terima hal tersebut karena sebelumnya mereka telah melakukan percakapan dimana sesuai dengan pertanyaan AnonIndo, AnonAU menyarankan AnonIndo mengarahkan serangan pada badan intelijen Australia yaitu ASIO dan tidak mengarahkan serangan pada website ".au" secara random karena akan berdampak pada warga sipil. AnonAU kemudian memberikan serangan balasan atas perlakuan AnonIndo tersebut dengan menyerang berbagai lembaga milik negara yaitu Kementerian Pendidikan, Garuda Indonesia, dan Bandara Solo yang dikelola oleh Angkasa Pura.[28]

Selain penyadapan juga terdapat kasus *carding* yang dilakukan oleh Indonesia. Berdasarkan riset yang dilakukan oleh *Clearcommerce* bahwa 20% total dari transaksi kartu kredit secara *online* dari Indonesia merupakan *cyber fraud* dengan menyurvei pada 1.137 pedagang, 6 juta transaksi, dan 40 ribu. Serta dari data Polri menyatakan bahwa rata-rata dari 200 kasus kejahatan siber yang ditangani telah didominasi oleh kejahatan *card fraud* dengan korban luar negeri seperti Australia, Amerika Serikat, dan Kanada.[29]

Berbagai ancaman kejahatan yang dihadapi Indonesia dan Australia merupakan permasalahan global yang saling terhubung terutama kasus penyadapan yang dimana hal tersebut melanggar kedaulatan negara Indonesia. Tetapi untuk menjaga keamanan negara serta kawasan diperlukan kerja sama. Adanya kesamaan kedua negara dalam menghadapi permasalahan dan serta pemikiran terhadap kejahatan transnasional menjadi titik balik terciptanya kepentingan bersama antar kedua negara dimana kedua negara sempat mengalami kerenggangan dalam hubungan bilateral.

Kerja Sama antara Indonesia dan Australia dalam Siber

Cyber Policy Dialogue merupakan upaya tidak langsung dalam mengembalikan krisis kepercayaan Indonesia terhadap Australia karena merupakan bagian dari strategi diplomatik jangka panjang melalui pendekatan kerja sama teknis dalam keamanan bidang siber. Kerja sama ini menegaskan komitmen terhadap keterbukaan, kebebasan, dan keamanan pada dunia digital serta memperkuat kerja sama dalam perlindungan dunia digital

[27] Ibid.

[28] David Yacobus, "Konflik Hacker Sebagai Non-State Actor Dalam Ketegangan Hubungan Indonesia - Australia Pada Tahun 2013," *Jurnal Prodi Peperangan Asimetris* 3, no. 2 (2017): 17–23.

[29] Herman et al., "Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia," *Halu Oleo Legal Research* 5, no. 2 (2023): 636..

untuk mempromosikan internet yang aman dan terbuka.

Dialog ini dilakukan sebanyak tiga kali dan pertama kali dilaksanakan pada hari Kamis, 4 Mei 2017 di Canberra, Australia. Pertemuan ini dipimpin oleh Dr. Tobias Feakin selaku Duta Besar Australia dalam bidang siber dan dari Indonesia yaitu Duta Besar Desra Percaya selaku Direktur Jenderal Urusan Asia Pasifik dan Afrika, Kementerian Luar Negeri juga dihadiri oleh perwakilan dari kedua negara. Pertemuan ini membahas mengenai berbagai isu siber sebagai permulaan termasuk pandangan dari masing masing negara terhadap internet, dunia maya, dan bertukar pendapat mengenai ancaman siber, kebijakan dan strategi, serta perkembangan secara regional dan internasional.[30]

Dialog kedua diselenggarakan di Jakarta, Indonesia pada hari Juma, 03 Agustus 2018. Pertemuan ini dipimpin oleh Dr. Tobias Feakin selaku Duta Besar Australia dalam bidang siber dan dari Indonesia yaitu Duta Besar Desra Percaya selaku Direktur Jenderal Urusan Asia Pasifik dan Afrika, Kementerian Luar Negeri juga dihadiri oleh perwakilan dari kedua negara.

Pertemuan ini membahas mengenai laporan PBB tahun 2013 dan 2015 dari UNGGE tentang perilaku suatu negara dalam dunia maya yang tetap perlu mengikuti hukum. Dalam laporan UNGGE tahun 2015, aturan aturan tersebut bersifat sukarela dan tidak mengikat tetapi kedua negara sepakat bahwa aturan internasional yang berlaku di dunia nyata juga berlaku di dunia digital dan kedua negara juga sepakat untuk bertindak sesuai dengan aturan tersebut. Kedua negara juga menyadari pentingnya bekerja sama secara regional untuk mengurangi resiko dari kejahatan dunia maya.[31]

Dialog ketiga diselenggarakan secara virtual pada hari Rabu, 02 September 2020. Delegasi Australia dipimpin oleh Duta Besar Bidang Siber dan Teknologi Kritis, Dr. Tobias Feakin dan dari Indonesia yaitu Letnan Jenderal (Purn.) Hinsa Siburian selaku Kepala Badan Siber dan Sandi Negara juga dihadiri oleh perwakilan dari kedua negara.

Pertemuan ini membahas mengenai komitmen dalam mempererat kerja sama dan menekan pentingnya lembaga penegak hukum dari kedua negara dalam menangani kejahatan siber seta menegaskan kembali komitmen kedua negara dalam kerja sama regional untuk membangun kepercayaan dan peningkatan kapasitas. Selain itu, kedua negara juga meninjau Nota Kesepahaman (MoU) Indonesia-Australia mengenai kerja sama siber pada tahun 2018, manfaat yang didapatkan dari berbagi informasi dan praktik, serta mengembangkan keterampilan dalam *Boot Camp*. Kedua negara sepakat untuk terus bekerja sama dan memperpanjang MoU selama dua tahun kedepan serta

[30] Australian Government Department of Foreign Affairs and Trade, *Australia-Indonesia Cyber Policy Dialogue Joint Statement*, 2018.

[31] Australian Government Department of Foreign Affairs and Trade, "Second Australia-Indonesia Cyber Policy Dialogue Joint Statement," *2018*, last modified 2018, https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/second-australia-indonesia-cyber-policy-dialogue.

kerja sama secara regional untuk memperkuat keamanan siber.[32]

Pembentukan MoU dibentuk secara resmi setelah Indonesia dan Australia menyepakati perjanjian secara menyeluruh dalam bidang keamanan siber yang ditandatangani pada 31 Agustus 2018 di Istana Kepresidenan Bogor, Indonesia oleh Dr. Djoko Setiadi selaku Kepala Badan Siber dan Sandi Negara Republik Indonesia dan Dr. Tobias Feakin selaku Duta Besar dalam Urusan Siber pada Departemen Luar Negeri dan Perdagangan Pemerintahan Australia. Kesepakatan ini dibentuk akibat meningkatnya ancaman kejahatan siber serta kerentanan yang dapat berdampak pada ketentraman dan keamanan nasional.

Terdapat empat bidang utama dalam cakupan MoU kerja sama yaitu pertukaran informasi dan praktik terbaik, pengembangan kapasitas dan penguatan koneksi, ekonomi digital, dan pelatihan terhadap kejahatan dunia maya. *Focal point* dari Indonesia yaitu BSSN dan dari Australia yaitu DFAT. MoU bersifat tidak mengikat dan dapat diperpanjang setiap saat sesuai kesepakatan kedua perwakilan.

MoU menghasilkan berbagai program nyata yang memperkuat kapasitas kedua negara dalam menghadapi ancaman siber berupa penyelenggaraan dialog kebijakan siber secara rutin, program pelatihan, lokakarya, serta webinar untuk meningkatkan sumber daya manusia pada bidang siber yang diawasi oleh lembaga perwakilan bidang siber dari masing masing negara.[33]

Peningkatan Kerja Sama melalui Lembaga BSSN dan DFAT yang mewakili lembaga dari masing masing negara. DFAT menjadi perwakilan Australia yang bertanggung jawab terkait hubungan diplomatik antar negara pada berbagai bidang resmi, salah satunya bidang siber dan bertindak sebagai penghubung resmi dikarenakan tantangan pada dunia global berpotensi mempengaruhi keamanan nasional.

Cyber Boot Camp merupakan kegiatan yang memberikan pembelajaran serta pelatihan bagi partisipan untuk menumbuhkan kesadaran serta pengetahuan peserta kamp terhadap seberapa siap teknologinya, ancaman siber, pengambilan keputusan yang tepat, serta cara kerja dunia maya. Kegiatan ini dilakukan selama dua minggu di Australia karena program ini merupakan pelatihan mendalam yang mengajarkan tentang keamanan siber, teknologi terbaru, pengambilan keputusan yang tepat terhadap ancaman yang dihadapi, dan peretasan jaringan komputer yang aman.

Program ini dibentuk oleh DFAT pada 2016 untuk meningkatkan keamanan siber dibawah kerja sama siber antara Australia dan berbagai mitra Indo-Pasifik, juga menjadi salah satu bentuk kerja sama Indonesia dan Australia yang telah dilakukan secara rutin sejak tahun 2018 dan berpotensi memberikan dampak positif dalam menanggulangi ancaman kejahatan

[32] Australian Government Department of Foreign Affairs and Trade, "Third Australia-Indonesia Cyber Policy Dialogue Joint Statement," *2020,* last modified 2020, https://www.dfat.gov.au/news/news/third-australia-indonesia-cyber-policy-dialogue.

[33] DFAT, "MoU Between Indonesia & Australia on Cyber Cooperation," 2018.

siber melalui penguatan sumber daya manusia di Indonesia.[34]

Australian Strategic Policy Institute* (ASPI) *Cyber Workshop bertujuan untuk mengadakan lokakarya mengenai perilaku negara yang bertanggung jawab di dunia maya bagi berbagai negara yang menjadi mitra dari keamanan siber Australia. Materi yang disampaikan berhubungan dengan dunia siber dan keamanan siber. Kemudian terdapat manajemen resiko, yang membedakan ancaman menjadi dua yaitu ancaman yang disengaja serta ancaman yang tidak disengaja. Juga terdapat strategi dan pengendalian resiko, keamanan siber dan keamanan *software*, serta struktur.

Kegiatan ini dilaksanakan di Jakarta, pada tanggal 01 November 2018. Kerja sama yang dilakukan antara BSSN dan ASPI bertujuan untuk meningkatkan analisis mengenai ancaman pada dunia maya, berpartisipasi dalam membahas kebijakan mengenai jaringan, dan bekerja sama dengan berbagai lembaga pemerintah. Melalui program ini Indonesia berpotensi merumuskan kebijakan dan strategi keamanan yang lebih kuat serta menyeluruh dan memungkinkan identifikasi, evaluasi, serta mitigasi resiko dunia maya.[35]

Cyber Security Webinar dilaksanakan sebagai bentuk kerja sama dengan mengundang para pakar dalam bidang keamanan siber dari berbagai pihak, baik dari pemerintah hingga sektor swasta yang berasal dari Australia. Kegiatan ini dilaksanakan sejak tahun 2020 hingga 2021. Topik yang diangkat dalam webinar ini berawal dari kesepakatan yang didapatkan oleh Indonesia dan Australia.

Dalam webinar *Capacity Building and Strength Connection* membahas topik mengenai pengelolaan teknologi. Topik ini hadir sebagai bentuk respon terhadap perkembangan teknologi terbaru seperti internet 5G yang merupakan teknologi super cepat, *Internet of Things* (IoT) yang merupakan teknologi yang menghubungkan berbagai perangkat ke internet, dan kecerdasan buatan (AI). Selain itu juga membahas tentang kebijakan terkait keamanan yang dimiliki oleh Indonesia dan Australia.

Webinar tersebut juga mengangkat isu aspek teknis, ilmu komputer, dan keamanan jaringan. Webinar tersebut juga menekankan konsep *deep cyber security* yang merupakan pendekatan menyeluruh terhadap perlindungan data, jaringan, dan infrastruktur digital yang mencakup perangkat lunak yang kuat, prinsip manajemen resiko yang baik, kesadaran pengguna akan pentingnya keamanan, dan kerjasama lintas sektor.[36]

Cyber Business Connection*: *Austrade* dan *Austcyber dilakukan dalam bentuk pengembangan keamanan siber dalam bidang ekonomi digital. Perusahaan keamanan siber Australia melakukan kunjungan yang dilakukan oleh *Austrade* ke Jakarta yang dilakukan pada 08 Januari 2019 oleh para perwakilan *Austrade* dan *Austcyber* untuk bertemu dengan pejabat dan

[34] Muhammad Rafi Shiddique and Mansur Juned, "Human Capital Development for Cybersecurity: Examining BSSN's Contributions in the Indonesia-Australia Cyber Policy Dialogue (2018-2020)," *Journal of Social and Political Sciences* 6, no. 4 (2023): 218–219.
[35] Ibid., 220.
[36] Ibid., 221.

pebisnis di Indonesia. Selain rancangan dalam pengembangan sektor ekonomi digital seperti memperkenalkan penggunaan sertifikat digital dalam ekspor impor pada kegiatan *cyber business connection* in, Australia juga menganggap bahwa Indonesia memiliki potensi dalam perekonomian digital dan mengharapkan agar para pelaku ekonomi digital di Indonesia dapat mengembangkan bisnisnya serta melindungi konsumennya.[37]

Seiring perkembangan waktu, terbentuk **MoU pada sektor ekonomi digital** terkait penguatan ketahanan dan keamanan siber dalam upaya pengembangan sumber daya manusia yang ditandatangani oleh Infinite Learning (Nongsa Digital Park), PT. Innoveight Technofarm Indonesia (Innov8), *Royal Melbourne Institute of Technology* (RMIT), dan Kementerian Koordinator Bidang Perekonomian RI melalui Deputi Bidang Koordinasi Kerja Sama Ekonomi dan Investasi pada hari Rabu tanggal 12 Februari 2025 di Kantor Kementerian Koordinasi Bidang Perekonomian.

Penandatanganan tersebut sekaligus membentuk *Indonesian Centre of Excellence for Cybersecurity* (ICEC) yang merupakan hasil kolaborasi keseluruhan dengan tujuan menjadi pusat unggulan dalam mengatasi kekurangan SDM yang kompeten melalui penyediaan pendidikan dan pelatihan serta perkembangan penelitian.

Kesepakatan ini bertujuan untuk melatih tenaga kerja di Indonesia terkait keamanan dan ketahanan siber untuk meningkatkan daya saing di sektor ekonomi digital. Selain itu, kerja sama ini juga merupakan bentuk kolaborasi jangka panjang antara Indonesia dan Australia dalam pendidikan dan keterampilan.[38]

Pengaruh Kerja Sama Terhadap Kedua Negara

Pengaruh dari kerja sama bilateral dalam keamanan siber yang dapat dirasakan Indonesia yaitu terjadinya peningkatan GCI milik Indonesia. Pada tahun 2017, Indonesia menempati peringkat 70 yang termasuk pada tahap memiliki inisiatif dan sedang mengembangkan berbagai program keamanan siber tetapi belum memiliki komitmen tinggi terhadap keamanan siber (*maturing stage)*. Kemudian pada tahun 2018, Indonesia mengalami peningkatan si peringkat 41 dengan berada pada *leading stage* yang

[37] Dhiyanka Magrisa, "Kerja Sama Badan Siber Dan Sandi Negara (BSSN) Dengan Department of Foreign Affairs and Trade (DFAT) Australia Dalam Pengembangan Cyber Security," *Jom Fisip* 7, no. 11 (2020): 7, http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI.

[38] Kementerian Koordinator Bidang Perekonomian Republik Indonesia, "Perkuat Sektor Keamanan Siber, Indonesia Dan Australia Jalin Kerja Sama Pengembangan SDM," *Kementerian Koordinator Bidang Perekonomian Republik Indonesia*, last modified 2025, accessed June 4, 2025, https://www.ekon.go.id/publikasi/detail/6186/perkuat-sektor-keamanan-siber-indonesia-dan-australia-jalin-kerja-sama-pengembangan-sdm.

berarti telah memiliki komitmen tinggi terhadap keamanan siber.[39]

Pada tahun 2020, Indonesia kembali mengalami peningkatan menjadi peringkat 24 pada tingkat global, pada tingkat kawasan Asia Pasifik peringkat Indonesia meningkat menjadi peringkat 6. Hingga pada tahun 2024 ITU tidak lagi menggunakan peringkat dalam menentukan urutan GCI, melainkan telah mengelompokkannya menjadi 5 *tier* dan menilai berdasarkan skor yang dimiliki suatu negara. Pada tahun yang sama Indonesia masuk dalam *Tier 1* bersama dengan Australia, dimana pada profil negara Indonesia memiliki 20 poin pada setiap pilarnya yang berarti memenuhi standar tinggi secara keseluruhan pilar GCI.[40] Kemudian adanya bantuan berupa hibah dana serta peralatan investasi kejahatan siber, pelatihan melalui berbagai program terhadap peningkatan SDM.

Dari sisi Australia, kerja sama ini dapat meningkatkan kerja sama dalam bidang siber, ekonomi digital, dan meningkatkan keamanan negara, serta kawasan. Bagi kedua negara, kerja sama ini merupakan salah satu upaya mempererat hubungan bilateral antar kedua negara.

KESIMPULAN

Kerja sama antara Indonesia dan Australia merupakan upaya bilateral untuk meningkatkan dan menjaga ruang keamanan siber dari perkembangan ancaman kejahatan siber yang bersifat transnasional sekaligus menjadi upaya membangun kembali krisis kepercayaan yang sempat terjadi antara Indonesia dan Australia pada tahun 2013 dikarenakan penyadapan yang dilakukan oleh Australia.

Indonesia yang merupakan salah satu negara dengan jumlah penduduk terbesar di dunia dan diperkirakan akan terus mengalami pertumbuhan populasi termasuk dengan peningkatan jumlah pengguna internet. Sementara itu, Australia yang merupakan negara maju dengan tingkat kecanggihan teknologi yang tinggi dan masyarakatnya yang umumnya telah melek terhadap teknologi digital. Tetapi keseluruhan hal dari dua negara tersebut justru menjadi celah bagi potensi ancaman kejahatan siber yang semakin kompleks dan terus berkembang.

Persamaan persepsi yang dimiliki oleh kedua negara dalam menanggapi kejahatan siber menjadi titik balik dari terbentuknya kerja sama dalam bidang keamanan siber yang dimulai pada tahun 2017 berbentuk dialog melalui *Cyber Policy Dialogue* yang diadakan sebanyak 3 kali hingga tahun 2020. Kemudian terbentuknya MoU yang dibentuk pada pertemuan kedua pada *Cyber Policy Dialogue* dan ditandatangani pada 31 Agustus 2018 dan memperpanjangnya kembali hingga 2 tahun mendatang. Adanya kerja sama melalui lembaga bidang siber dari masing masing negara yaitu BSSN dan DFAT sebagai penyelenggara, perwakilan, partisipan, hingga pengawas dari hasil kerja sama berupa pelatihan, lokakarya, hingga webinar pada bidang siber hingga ekonomi digital.

Upaya peningkatan keamanan pada bidang siber tidak hanya

[39] ITU, *Global Cybersecurity Index (GCI) 2018*, 2019.
[40] ITU, *Global Cybersecurity Index 2024 5th Edition*, 2024, https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf.

berfokus pada keamanan negara secara bilateral saja, tetapi juga secara regional pada kawasa Indo-Pasifik, maka penting untuk melakukan kerja sama dalam upaya untuk menguatkan, meningkatkan, serta menjaga keamanan pada bidang siber negara serta kawasan.

DAFTAR PUSTAKA

ACSC. *ACSC Australian Cyber Security Centre 2015 Threat Report*. *Australian Cyber Security Center*, 2015.

———. *ACSC Australian Cyber Security Centre 2016 Threat Report*. *Australian Cyber Security Centre*, 2016.

Australian Government Department of Foreign Affairs and Trade. *Australia-Indonesia Cyber Policy Dialogue Joint Statement*, 2018.

———. "Second Australia-Indonesia Cyber Policy Dialogue Joint Statement." *2018*. Last modified 2018. https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/second-australia-indonesia-cyber-policy-dialogue.

———. "Third Australia-Indonesia Cyber Policy Dialogue Joint Statement." *2020*. Last modified 2020. https://www.dfat.gov.au/news/news/third-australia-indonesia-cyber-policy-dialogue.

Bambang Supriyadi. "Persepsi Bersama Indonesia-Australia Hibah Dana Dan Peralatan Investigasi Cyber Crime Australia Kepada Indonesia." *Journal of International Relations* 3, no. 1 (2017): 140–149.

Brant, Tom. "WannaCry Ransomware Hits Honda Plant, Traffic Cams." *PC Magazine*. Last modified 2017. https://www.pcmag.com/news/wannacry-ransomware-hits-honda-plant-traffic-cams.

Brookes, Chris. *Cyber Security: Time For an Integrated Whole-of-Nation Approach in Australia*. *Indo-Pacific Strategic Papers*, 2015.

Chan, Nelson, Simon Coronel, and Yik Chiat Ong. "The Threat of The Cybercrime Act 2001 To Australian IT Professionals" (2003): 25–33. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.4.3391&rep=rep1&type=pdf.

Chintia, Ervina, Rofiqoh Nadiah, Humayyun Nabila Ramadhani, Zulfikar Fahmi Haedar, Adam Febriansyah, and Nur Aini Rakhmawani. "Kasus Kejahatan Siber Yang Paling Banyak Terjadi Di Indonesia Dan Penanganannya." *Journal of Information Engineering and Educational Technology* 2, no. 2 (2018): 65–69.

Christian, Leuprecht, and Stephanie MacLellan. *Governing Cyber Security in Canada, Australia and the United States*. *Center for International Governance Innovation*, 2018.

DANCĂ, Dana. "Cyber Diplomacy-A New Component of Foreign Policy." *Journal of Law and Administrative Sciences* 3, no. 3 (2015): 91–97.

DFAT. "MoU Between Indonesia & Australia on Cyber Cooperation," 2018.

Gani, Hamsu Abdul, and Andika Wahyudi Gani. "Penyelesaian Kasus Kejahatan Internet (

Cybercrime) Dalam Perspektif UU ITE No . 11 TAHUN 2008 Dan UU No . 19 Tahun 2016." *Prosiding Seminar Nasional LP2M UNM - 2019*, no. 11 (2019): 121–129.

Herman, Oheo Kaimuddin Haris, Sabrina Hidayat, Zahrowati, and Riski Dwitasari. "Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia." *Halu Oleo Legal Research* 5, no. 2 (2023): 633–646.

Islami, Maulia Jayantina. "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index." *Masyarakat Telematika Dan Informasi* 8, no. 2 (2017): 137–144.

ITU. *Global Cybersecurity Index (GCI) 2017*, 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

———. *Global Cybersecurity Index (GCI) 2018*, 2019.

———. *Global Cybersecurity Index 2024 5th Edition*, 2024.

Kementerian Koordinator Bidang Perekonomian Republik Indonesia. "Perkuat Sektor Keamanan Siber, Indonesia Dan Australia Jalin Kerja Sama Pengembangan SDM." *Kementerian Koordinator Bidang Perekonomian Republik Indonesia*. Last modified 2025. Accessed June 4, 2025. https://www.ekon.go.id/publikasi/detail/6186/perkuat-sektor-keamanan-siber-indonesia-dan-australia-jalin-kerja-sama-pengembangan-sdm.

Magrisa, Dhiyanka. "Kerja Sama Badan Siber Dan Sandi Negara (BSSN) Dengan Department of Foreign Affairs and Trade (DFAT) Australia Dalam Pengembangan Cyber Security." *Jom Fisip* 7, no. 11 (2020): 1–11.

Paterson, Thomas. "Indonesian Cyberspace Expansion: A Double-Edged Sword." *Journal of Cyber Policy* 4, no. 2 (2019): 216–234. https://doi.org/10.1080/23738871.2019.1627476.

Powell, Dominic. "'WannaCry' Ransomware Hits 12 Australian Small Businesses: Four Ways To Protect Your Systems." *SmartCompany*. Last modified 2017. https://www.smartcompany.com.au/technology/wannacry-ransomware-hits-12-australian-small-businesses-four-ways-to-protect-your-systems/.

Rosy, Afifah Fidina. "Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional Di Bidang Keamanan Siber." *Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan* 1, no. 2 (2020): 118–129.

Saroji, Ahmad, Triana Harmini, and Muhammad Taqiyuddin. "Sejarah Evolusi Generasi Internet." *Jurnal Lani:Kajian Ilmu Sejarah & Budaya* 2, no. 2 (2021): 65–75.

Selvadurai, Niloufer. "The Relevance of Technology Neutrality to the Design of Laws to Criminalise Cyberbullying." *International Journal of Law and Public Administration* 1, no. 2 (2018): 14–22.

Shaffan, Ahmad Mafud. "Respons Indonesia Terhadap Kasus Penyadapan Australia." *Journal of International Relations* 4, no.

2 (2018): 285–294.
Shiddique, Muhammad Rafi, and Mansur Juned. “Human Capital Development for Cybersecurity: Examining BSSN’s Contributions in the Indonesia-Australia Cyber Policy Dialogue (2018-2020).” *Journal of Social and Political Sciences* 6, no. 4 (2023).
Wijoyo, Hadion, Beno Jange, Agung Putra Andira, Roni Chandra, and Fery Wongso. “Cyber Crime.” In *Encyclopedia of Cyber Warfare*, 1–90. PT Mafy Media Literasi Indonesia, 2024.
Yacobus, David. “Konflik Hacker Sebagai Non-State Actor Dalam Ketegangan Hubungan Indonesia - Australia Pada Tahun 2013.” *Jurnal Prodi Peperangan Asimetris* 3, no. 2 (2017): 17–23.
“Kasus Ransomware Di Indonesia: Ancaman, Contoh Kasus, Dan Cara Melindungi Bisnis Anda.” *Rizki Tujuhbelas Kelola*. Last modified 2024. https://r17.co.id/insight/article/kasus-ransomware-di-indonesia-ancaman-contoh-kasus-dan-cara-melindungi-bisnis-anda.
Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 2008.