Journal of International Relations, Volume 3, Nomor 1, Tahun 2017, hal. 140-149
Online di http://ejournal-s1.undip.ac.id/index.php/jihi

Persepsi Bersama Indonesia-Australia dalam Hibah Dana dan Peralatan Investigasi *Cyber Crime* dari Australia Kepada Indonesia

Bambang Supriyadi
Departemen Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Diponegoro
Jalan Prof. H. Soedarto, SH, Tembalang, Semarang, Kotak Pos 1269
Website: http://www.fisip.undip.ac.id Email: fisip@undip.ac.id

ABSTRACT

The history of the relations between Indonesia and Australia highlighted by several events that create relations of two countries became heaving and worries some people in Australia who considers Indonesia as one of the threats to the security of Australia. But these two things does not impede Indonesia and Australia to conduct a number of cooperation and other collective efforts to overcome the various threats to the security of both countries, one of which is the threat of cyber crime. This research aimed to analyze factors that affect policies taken by Australia in providing financing and equipment of cyber crime investigation to Indonesia. This research uses the concept of collective identity from the constructivist theory that driven by perceptions of a threat in explaining the behavior of a state. The results of this research indicate that the perception of the two countries in view of the threat of cyber crime made the two countries have a collective identity as the two countries that tried to combat cyber crime.

Keywords: *cyber crime, cooperation, funds and equipment assistance, common perception, collective identity, Australian Government*

Pendahuluan

Kehidupan manusia pada abad ke-21 telah mengalami perkembangan di berbagai bidang, salah satunya adalah bidang teknologi dan informasi. Salah satu perkembangan dalam bidang teknologi tersebut adalah munculnya sistem jaringan komunikasi global bernama *international networking* (internet). Menurut International Telecomunication Union, sejak tahun 2000 sampai 2011 jumlah pengguna internet di seluruh dunia terus meningkat setiap tahunnya. Pengguna internet diperkirakan mencapai 580 juta orang pada pertengahan 2002, hampir 10 persen dari populasi manusia pada tahun tersebut (Khadam, 2012: 64). Bahkan pada tahun 2011, setidaknya sekitar 2,3 miliar orang memiliki akses ke jaringan internet (Malby dkk., 2013: 1).

Sejak kemunculannya, internet telah mempengaruhi berbagai aspek kehidupan manusia dan telah membawa dampak negatif dan positif. Salah satu dampak negatif tersebut antara lain adalah kemunculan *cyber crime*. *Cyber crime*, disebut juga *computer crime*, menggunakan kecanggihan perangkat komputer dan internet yang dapat terhubung ke berbagai penjuru dunia untuk melakukan tindakan kejahatan. Tidak ada definisi pasti yang digunakan untuk mendefiniskan *cyber crime*. Namun, United Nation Office on Drugs and Crime (UNODC) menjelaskan bahwa *cyber crime* sebagai kegiatan yang berkaitan dengan komputer untuk mencapai kepentingan pribadi atau keuntungan finansial atau tindakan merusak, termasuk bentuk-bentuk kejahatan yang berhubungan dengan identitas,

dan tindakan yang berhubungan dengan konten komputer (www.unodc.com, 2016). Dalam situs resmi International Police (Interpol), penegak hukum secara umum membedakan dua tipe kejahatan yang berhubungan dengan internet yakni *advanced cyber crime* dan *cyber-enabled crime* (www.interpol.int, 2016). *Advanced cyber crime* adalah serangan yang sifatnya menggunakan peralatan mutakhir terhadap perangkat keras komputer dan perangkat lunak. *Cyber-enabled crime adalah* kejahatan tradisional yang mulai memanfaatkan dunia maya seperti kejahatan terhadap anak, kejahatan finansial, dan bahkan terorisme.

Dalam beberapa tahun terakhir, *cyber crime* telah berkembang menjadi salah satu ancaman utama dari kesejahteraan masyarakat di seluruh dunia (Droogan & Ziemke-Dickens, 2010: 162-166). Bentuk kejahatan ini sulit untuk diatasi karena sifat dari *cyber crime* itu sendiri *anonymous* (tanpa nama) serta tidak mengenal batas virtual. Sifat dari *cyber crime* yang dilakukan di dunia maya membuat akibat yang timbul dari kejahatan ini dapat meluas bahkan melewati batas-batas wilayah. Banyak pihak telah menyadari bahaya yang ditimbulkan *cyber crime*, tidak terkecuali negara-negara di seluruh dunia. Dalam Konferensi Anggota PBB tentang Kejahatan Transnasional Terorganisir tahun 2010 mengidentifikasi *cyber crime* sebagai salah satu dari lima *New Emerging Crimes*. Hal ini membuktikan bahwa *cyber crime* telah menjadi permasalahan yang mendapat perhatian dari dunia.

Dalam upaya untuk mengatasi ancaman *cyber crime*, negara-negara mulai tergerak untuk membahas dan melakukan berbagai tindakan kolektif seperti membahas kerangka hukum nasional atau pun lintas nasional dan melakukan kerja sama dengan negara lain, salah satunya adalah Australia dan Indonesia. Dalam kerja sama ini, berbagai upaya dilakukan oleh kedua negara mulai dari pelatihan kedua personel kepolisian nasional masing-masing hingga hibah dana dan peralatan investigasi *cyber crime* dari Australia kepada Indonesia dalam pembangunan Cyber Crime Investigation Centre (CCIC) dan Cyber Crime Investigation Satellite Office (CCISO). CCIC dan CCISO merupakan kantor investigasi *cyber crime* yang terletak di Markas Besar Polri dan beberapa Polda lain di Indonesia. Pembangunan CCIC dan CCISO ini sebagian besar merupakan hasil hibah dari pihak Australia melalui Australian Federal Police *(*AFP) yang memberikan sejumlah dana dan peralatan komputer yang totalnya mencapai 20 juta dolar Australia (Sondakh, 2015: 188).

Dalam periode sejak dibangunnya CCIC dan CCISO, berbagai upaya AFP dan Polri telah lakukan untuk mempertahankan kelanjutan CCIC dan CCISO, salah satunya adalah pembaruan dan pemeliharaan peralatan hingga pelatihan kembali staf kepolisian Indonesia oleh AFP. Berbagai upaya tersebut didanai oleh bantuan pembangunan resmi Australia (Connery, Sambhi, McKenzie, 2014: 5-6). Anggaran yang dibutuhkan untuk pembangunan CCIC ini pun tidak sedikit, bahkan mencapai puluhan juta dolar.

Ada beberapa hal yang menarik untuk dicermati dari kerja sama dan bantuan Australia kepada Indonesia dalam upaya mengatasi *cyber crime* di Indonesia. *Pertama*, kerja sama dan bantuan tersebut lebih banyak menguntungkan Indonesia. *Kedua*, semua program dari kerja sama tersebut ditujukan untuk mengatasi permasalahan *cyber crime* yang ada di Indonesia. Padahal Australia sendiri mengalami permasalahan *cyber crime* yang lebih parah di negaranya. Droogan dan Ziemke-Dickens dalam *The Council for Asian Transnational Threat Research* (2010: 162-166) menyebutkan bahwa salah satu ancaman besar yang dihadapi Australia dewasa ini adalah *cyber crime*.

Jika melihat pada sejarah hubungan kedua negara, maka perilaku Australia dalam membantu Indonesia untuk penanganan *cyber crime* di Indonesia menjadi suatu hal yang menarik. Sepanjang sejarah, Indonesia dan Australia beberapa kali bersitegang dan terlibat perselisihan akibat perbedaan paham, kecurigaan satu sama lain, dan persepsi ancaman

antar kedua negara. Tindakan Indonesia dalam merebut Irian Barat, konfrontasi dengan Malaysia, dan integrasi Timor Timur menjadi bagian Indonesia membuat beberapa kalangan di Australia memandang Indonesia sebagai negara yang ekspansionis dan agresif (www.aph.gov.au, 1995). Indonesia juga dianggap sebagai negara "dari dan melalui mana serangan terhadap Australia bisa dilakukan" (Sinaga, 2014: 22)

Pembahasan

Sejarah dan Dinamika Hubungan Indonesia-Australia

Sepanjang sejarah, hubungan Indonesia dan Australia sering mengalami pasang surut. Hal ini disebabkan oleh berbagai hal di antaranya perbedaan dalam hal budaya dan politik dan peristiwa-peristiwa yang melibatkan kedua negara seperti konflik Timor Timur, hingga kasus eksekusi warga negara Australia yang terlibat kasus narkoba di Indonesia. Prof. Richard Tanter (2013: 3-15) dalam tulisannya tentang *Shared Problems, Shared Interests: Reframing Australia-Indonesia Security Relations,* menyebutkan bahwa ada empat hal yang berperan dalam hubungan Indonesia dan Australia. *Pertama,* adanya kesenjangan yang membingungkan di berbagai aspek seperti ukuran populasi dan kekuatan militer kedua negara. Kedua hal tersebut menjadi faktor yang menentukan dalam hubungan internasional (www.jpri.org, 2000). Namun di sisi lain, Australia memiliki daya tawar yang lebih tinggi dalam politik internasional.

Kedua, perbedaan dalam hal persepsi ancaman yang dapat muncul dari negara lain. Saat Indonesia menganggap Amerika dalam memanipulasi media internasional dan Lembaga Swadaya Masyarakat mampu menjadi ancaman bagi Indonesia, beberapa kalangan di Australia menganggap Indonesia memiliki potensi ancaman bagi keamanan Australia.

Ketiga, hubungan antara pemerintah kedua negara yang dominan namun lemah dalam hubungan bisnis dan tidak adanya pertukaran masyarakat antar kedua negara yang seimbang. *Keempat,* dominannya hubungan di sektor antar pemimpin negara. Dengan tidak diimbangi dengan penguatan hubungan di sektor lain, maka hubungan Indonesia dan Australia rentan mengalami pasang surut. Sistem politik kedua negara yang memiliki pembatasan pada masa jabatan pemimpin negara memungkinkan perubahan hubungan ketika terjadi pergantian pemimpin.

Sejarah hubungan yang pasang surut di antaranya keduanya dimulai setelah Indonesia meraih kemerdekaannya. Di awal masa pemerintahan Presiden Soekarno, hubungan yang cukup baik akhirnya memburuk disebabkan kedekatan Soekarno dengan blok komunis. Hal ini ditambah lagi dengan perbedaan pandangan dalam melihat status Irian Barat. Kemudian di awal masa pemerintahan Soeharto, hubungan keduanya kembali membaik. Bahkan Australia dan Indonesia sempat menyepakati *Agreement on Maintaining Security*. Namun peristiwa terbunuhnya lima wartawan Australia tahun 1979 dan ditambah dengan masalah Papua Barat di mana Australia mengkritik Pemerintah Indonesia yang dianggap melakukan pelanggaran HAM yang cukup banyak di sana (Firth, 2011: 198).

Sejak era reformasi hingga era pemerintahan Presiden Joko Widodo pun, hubungan Indonesia dan Australia masih terus mengalami pasang surut. Yang terakhir adalah ketika kasus penyadapan terhadap beberapa pejabat penting di Indonesia oleh pihak intelijen Australia tahun 2009 dan kasus pemberian *Temporary Protection Visa* oleh Departemen Imigrasi dan Masalah-Masalah Penduduk Asli Australia (DMIIA) kepada 42 dari 43 WNI asal Papua (Indah, 2009: 10).

Selama abad ke 21, hubungan kedua negara bisa dikatakan cukup dekat di berbagai bidang seperti keamanan, politik, budaya, perdagangan, pendidikan, dan lain-lain. Walaupun masih diwarnai beberapa insiden, namun sejak isu terorisme mencuat di dalam ranah politik internasional dan kasus Bom Bali I dan II di awal abad ke 21 menjadikan

hubungan kedua negara dapat dikatakan menjadi lebih dekat. Bahkan bisa dikatakan efek dari eksekusi terpidana '*Bali Nine'* terhadap hubungan kedua negara, terlepas dari penarikan Duta Besar Australia untuk Indonesia, tidak terlalu berarti dan dapat dilupakan (Harvey, 2016).

Kerja Sama Penanganan Cyber Crime Dalam Dinamika Kerangka Kerja Lombok Treaty

Pada tahun 2010, Indonesia dan Australia melalui Polri dan Australian Federal Police memulai rencana pengembangan pembangunan kantor investigasi *cyber crime* di Mabes Polri dan di beberapa Polda lainnya. Pembangunan CCIC dan CCISO dimulai sejak tahun 2010 dan diresmikan pada tahun 2011 oleh Kapolri saat itu, Jenderal Timur Pradopo, dan *Commissioner* AFP, Tony Negus. Menurut Ipda Geo Fernanda, salah satu staf CCIC, biaya pembangunan dan peralatan CCIC dan CCISO mayoritas diberikan oleh Australia dalam bentuk hibah. Kerja sama tersebut juga menandai kelanjutan kerangka kerja sama bilateral di bidang keamanan yang dilakukan kedua negara dalam *Lombok Treaty*.

Sebelum *Lombok Treaty*, Indonesia dan Australia tercatat telah melakukan kerja sama keamanan bilateral pada tahun 1995 yang disebut AMS. Walaupun dibatalkan empat tahun kemudian, kerja sama ini menjadi landasan kerja sama kedua negara. Pembuatan perjanjian ini memiliki tujuan agar Indonesia dan Australia saling mendukung dalam menciptakan keamanan kedua negara dan regional (DuPont, 1996: 49-52). Perjanjian ini kemudian juga menjadi salah satu landasan kerja sama keamanan kedua negara.

Setelah AMS, kerja sama keamanan Indonesia dan Australia berlanjut dengan adanya *Joint Investigation Team* untuk menanggapi berbagai aktivitas terorisme. Pada tahun 2006, disepakati *Agreement between the Government of the Republic Indonesia and the Government of Australia on Framework for Security Cooperation* yang dilakukan di Canbera dan secara resmi ditandatangani pada 13 November 2006 di Lombok. Alex Downer, mantan Perdana Menteri Australia, menjelaskan bahwa kesepakatan ini menyediakan kerangka yang kuat untuk mendorong dialog intensif, pertukaran dan implementasi kegiatan kerja sama (Taylor, 2008: 109). Selain menyerukan konsultasi reguler pada masalah pertahanan dan keamanan, perjanjian ini juga mengkhususkan kerja sama di beberapa area tertentu yang meliputi (1) kerja sama pertahanan, (2) kerja sama penegakan hukum, (3) kerja sama *counter-terrorism*, (4) kerja sama intelijen, (5) keamanan maritim, (6) keselamatan dan keamanan penerbangan, (7) proliferasi senjata pemusnah massal, (8) kerja sama dalam tanggap darurat (9) kerja sama di organisasi internasional yang terkait dengan masalah-masalah keamanan dan (10) kerja sama antar masyarakat (*people to people cooperation*) (www. treaty.kemlu.go.id, 2006).

Makna disepakatinya *Lombok Treaty* secara simbolik adalah adanya hubungan erat antara Indonesia dan Australia dalam menghadapi masalah keamanan. Menteri Pertahanan Australai, Stephen Smith, dalam kunjungannya ke Indonesia pada tahun 2012 mengatakan bahwa *Lombok Treaty* menciptakan kerangka kerja modern untuk Australia dan Indonesia dalam bidang-bidang di atas. Perjanjian ini juga memperjelas bahwa kedua negara menghargai dan mendukung kedaulatan, integritas teritorial, kesatuan nasional dan kemandirian politik satu sama lain. pentingnya hubungan strategis dan keamanan antara Indonesia dan Australia ditunjukkan oleh Lombok Treaty.

Kerja sama kedua negara dalam penanganan *cyber crime* merupakan kelanjutan dari kerja sama yang dilakukan sejak penandatanganan *Lombok Treaty*. Dalam situs resmi Kedutaan Australia untuk Indonesia, Michael Keenan, mantan Menteri Kehakiman Australia, mengatakan bahwa kerja sama ini merupakan kelanjutan dari upaya-upaya yang sedang dilakukan kedua negara dalam melawan perkembangan kejahatan transnasional antara AFP dan Polri (www.indonesia.embassy.gov.au, 2016). Kedua negara memang berkomitmen untuk memperluas kerja sama dalam bidang kejahatan transnasional

terorganisir dan ancaman non tradisional yang mulai berkembang. Sebagai salah satu ancaman non tradisional yang muncul akibat perkembangan di bidang teknologi informasi, maka kedua negara sepakat untuk mulai memberikan perhatian dalam bidang *cyber crime*.

Cyber Crime sebagai Permasalahan Indonesia-Australia

Pasca Perang Dingin, kejahatan transnasional menjadi salah satu ancaman utama terhadap keamanan nasional sebuah negara. Hal ini dibuktikan dengan diadakannya United Nations Convention against Transnational Organized Crime (UNCTOC) pada akhir 2003 (www.unodc.org, 2016). Salah satu bentuk kejahatan transnasional yang dianggap menjadi tantangan utama saat ini adalah *cyber crime*. Hal ini tidak lepas dari perkembangan internet yang telah merambah negara-negara di dunia, tak terkecuali Indonesia dan Australia.

Ada beberapa jenis kegiatan yang dapat digolongkan sebagai *cyber crime*, namun setidaknya ada delapan aktivitas yang digolongkan ke dalam *cyber crime* dan menjadi perhatian khusus dan oleh Pemerintah Australia. Beberapa bentuk aktivitas yang tergolong *cyber crime* di Australia adalah serangan terhadap sistem komputer, *cyber-bullying*, konten yang bersifat ofensif dan ilegal, konten yang mengandung material pelecehan seksual anak secara *online*, pencurian identitas, masalah perdagangan *online* (biasanya berupa penipuan dalam hal perdagangan), email *spam* dan *phishing*, dan penipuan *online* (www.acorn.gov.au, 2016). Walaupun pemerintah dan masyarakat telah menyadari potensi ancaman *cyber crime*, namun ketergantungan terhadap teknologi membuat kerugian yang ditimbulkan diperkirakan akan terus meningkat.

Banyaknya serangan *cyber crime* di Australia akhirnya menyebabkan kerugian finansial yang cukup banyak. Seperti yang dijelaskan pada diagram di atas, pada tahun 2009 kerugian yang diakibatkan oleh kejahatan yang berhubungan dengan komputer mencapai jutaan dolar. Kerugian finansial yang dialami masyarakat Australia pada tahun 2009 mayoritas kurang dari 1000 dolar. Meskipun pada tahun 2009 tercatat bahwa mayoritas kerugian finansial yang diakibatkan penipuan *online* tidak lebih dari 1.000 dolar, namun beberapa di antaranya ada yang mencapai lebih dari 50.000 dolar (AIC, 2010). Data tersebut menunjukkan Australia mengalami kerugian finansial yang cukup banyak dari tindak *cyber crime.*

Berdasarkan data dari Australian Cyber Security Centre (ACSC), sebuah lembaga bentukan pemerintah untuk pengawasan *cyber security,* tingkat *cyber crime* yang terjadi di Australia memang cukup tinggi. Pada tahun 2015 terdapat setengah dari responden pernah mengalami insiden *cyber crime* setidaknya satu kali. Bentuk-bentuk *cyber crime* yang dialami responden tersebut bermacam-macam, di antaranya *malware*, *malicious email*, virus, *unauthorised acces*, pencurian informasi, *remote access trojans* (RATs), dan DDOS (ACSC, 2015: 16). Lebih lanjut, Australia Crime Commission memberikan beberapa contoh kejahatan tradisional mulai bertransformasi menjadi *cyber crime*, seperti pencucian uang melalui sistem pembayaran *online* seperti PayPal, kejahatan seks anak melalui situs pornografi anak, pencurian melalui kejahatan identitas seperti mencuri rincian rekening bank *online* atau rincian dari situs-situs lain, pengintaian, pelecehan dan intimidasi melalui pesan *online*, dan kerusakan berbahaya melalui serangan DDoS dan virus.

Seperti halnya Australia, Indonesia juga menghadapi ancaman dari tindak *cyber crime*. Dengan jumlah pengguna internet yang cukup banyak banyak (88 juta orang pada tahun 2014, sekitar 34,9 persen dari total jumlah penduduk) tentunya membuat Indonesia menjadi salah satu negara yang rentan menghadapi ancaman *cyber crime* (APJII, 2014: 20). Lebih jauh lagi, Internet World Stats pada tahun 2016 mencatat bahwa Indonesia masuk dalam 8 besar negara dengan jumlah pengguna internet terbanyak. Di kawasan Asia Pasifik sendiri, Indonesia berada dalam sepuluh besar dengan jumlah kasus *cyber crime*

terbanyak dan masuk 10 besar negara dengan jumlah aktivitas kegiatan jahat (*malicious*) serta berada di peringkat 8 *Web-Based Attack* (www.tekno.kompas.com, 2010). Menurut laporan Badan Reserse Kriminal (Bareskrim) Mabes Polri, jumlah kasus *cyber crime* yang dilaporkan ke kepolisian cenderung meningkat setiap tahunnya. Pada tahun 2012, tercatat 781 laporan kasus *cyber crime* dengan tingkat laporan yang berhasil diselesaikan adalah 86 kasus. Setahun berselang, jumlah laporan kasus *cyber crime* yang masuk ke kepolisian mencapai 1.347 kasus, jauh meningkat dibanding tahun sebelumnya. Namun tingkat kasus *cyber crime* yang dapat diselesaikan pun meningkat menjadi 115 kasus. Sepanjang 2014, terdapat 1324 laporan yang masuk dengan penyelesaian kasus mencapai 307. Dari berbagai kasus yang dilaporkan, kasus *cyber crime* yang ada di Indonesia didominasi oleh penipuan via komunikasi *online* dengan jumlah kasus yang dilaporkan mencapai 427 kasus.

Dari serangkaian kasus *cyber crime* yang melanda Indonesia dan Australia, ada kesamaan pola yang dimiliki kedua negara. Sektor bisnis atau *e-commerce* dan situs resmi pemerintah kedua negara menjadi salah satu target utama dari serangan *cyber*. Disebutkan situs Kementrian Dalam Negeri Republik Indonesia bahwa pada 2015 terjadi peningkatan jumlah serangan *cyber* sampai empat kali lipat dibandingkan tahun 2014 dan sebanyak 54,5 persen kasus serangan dunia maya yang melanda Indonesia menyerang sektor bisnis *e-commerce*. Dalam artikel *Cyber Security: A Major Issue for Australian Business* (2016: 3-4) yang dikeluarkan oleh Hogan Lovells, salah satu lembaga hukum bagi sektor bisnis di Australia, disebutkan bahwa *cyber security* menjadi masalah utama bagi sektor bisnis di Australia dengan perkiraan kerugian mencapai 4,9 milyar dolar setiap tahunnya. Hal ini membuktikan bahwa *cyber crime* telah menjadi tantangan yang dihadapi oleh sektor bisnis di Indonesia dan Australia.

Bank Pusat di Indonesia dan Australia juga sama-sama pernah menjadi target serangan pelaku *cyber crime*. Tercatat, pada 22 Juni 2016 diberitakan bahwa Bank Pusat *(Central Bank)*, Bank Indonesia, mendeteksi 273 virus dan 67.000 surel sampah terhadap *server* dan surel dari situs Bank Indonesia (www.zdnet.com, 2016). Serangan terhadap Bank Indonesia tersebut terjadi di bulan yang sama di mana sekelompok peretas berjanji untuk menjadikan Sistem Perbankan di seluruh dunia sebagai target mereka. Sebelumnya Bank Pusat Australia, The Reserve Bank of Australia (RBA), disebutkan juga telah menjadi target dari serangan kelompok peretas. China disebut-sebut sebagai pihak yang disalahkan atas terjadinya serangan kelompok peretas yang menjadikan informasi ekonomi dan bisnis sebagai target mereka (www.bbc.com, 2013).

Komitmen Bersama Indonesia dan Australia dalam Memerangi Cyber Crime dan Kejahatan Transnasional Lainnya

Dengan semakin meluasnya penggunaan internet di segala aspek kehidupan, Indonesia dan Australia juga menghadapi ancaman *cyber crime* yang sama dengan negara lainnya. Kesamaan permasalahan berupa *cyber crime* yang dihadapi kedua negara membuat Indonesia dan Australia memiliki pandangan yang sama terhadap *cyber crime* sebagai kejahatan transnasional yang menjadi ancaman bagi keamanan nasional. Kesamaan persepsi ini kemudian membuat kedua negara memiliki identitas kolektif sebagai dua negara yang menderita akibat *cyber crime* dan menjadi negara yang memerangi *cyber crime*. Identitas yang didorong oleh pemahaman bersama tersebut mendorong Australia dan Indonesia terlibat dalam upaya bersama untuk mengatasi *cyber crime* demi terciptanya *cyber security* di kedua negara. Hal ini menjadi jawaban untuk memahami perilaku kedua negara dalam persoalan keamanan. Walaupun dengan latar belakang hubungan kedua negara yang sering dilanda krisis dan pasang surut, namun pendekatan baru untuk memahami kerja sama keamanan yang dilakukan kedua negara dapat didasarkan pada kemungkinan terciptanya kepentingan bersama untuk menghadapi

masalah global yang dihadapi masyarakat kedua negara (Richard Tanter, 2012: 1). Hal ini dibuktikan dalam *Memorandum of Understanding* (MoU) antara pemerintah kedua negara dalam memerangi kejahatan transnasional dan mengembangkan kerja sama kepolisian pada tahun 2010. Dalam Latar belakang MoU tersebut disebutkan bahwa kedua negara telah menyadari meningkatnya ancaman kejahatan transnasional yang semakin kompleks. Ancaman kejahatan transnasional yang semakin kompleks tersebut membutuhkan kerja sama internasional untuk mengatasi ancaman tersebut. Kedua negara kemudian secara bersama memutuskan untuk melanjutkan dan meningkatkan kerja sama yang telah ada sebelumnya. Dalam MoU tersebut, tercantum bahwa *cyber crime* menjadi salah satu dari beberapa masalah utama yang menjadi fokus kerja sama kedua negara.

Salah satu bentuk nyata dari upaya bersama antara kedua negara dalam rangka mengatasi masalah *cyber crime* adalah hibah dana dan peralatan investigasi *cyber crime* yang diberikan oleh Pemerintah Australia kepada kepolisian Indonesia untuk mengatasi permasalahan *cyber crime* di Indonesia. Bantuan dana dan peralatan investigasi tersebut kini menghasilkan sebuah kantor pusat investigasi *cyber crime* di Mabes Polri yakni Cyber Crime Investigation Centre (CCIC) dan Cyber Crime Investigation Satellite Office (CCISO) di beberapa Polda lainnya di Indonesia. Hibah dana dan peralatan investigasi dalam pembangunan CCIC dan CCISO di Indonesia tersebut kembali menguatkan bahwa Indonesia dan Australia memiliki pandangan yang sama terkait permasalahan *cyber crime*. Bantuan yang diberikan Australia tersebut menunjukkan bahwa kedua negara memandang *cyber crime* sebagai kejahatan transnasional yang perlu diatasi bersama.

Keinginan Australia untuk membangun hubungan baik dan kerja sama dalam bidang keamanan dan pertahanan dengan Indonesia disebutkan oleh John Howard (www.dfat.gov.au, 2005). Mantan Perdana Menteri Australia tersebut dalam situs Departemen Luar Negeri dan Perdagangan menekankan keinginan Australia untuk terus meningkatkan kerja sama dalam menangani bentuk-bentuk lain dari kejahatan transnasional dan ancaman keamanan nontradisional. Indonesia dan Australia akan bekerja bersama untuk meningkatkan kapasitas mereka dalam menghadapi permasalahan tersebut dan komitmen bersama untuk terus membangun hubungan pertahanan kedua negara.

Dalam kunjungan bilateral resmi pertamanya pada 2 November 2010, Mantan Perdana Menteri Australia ke-27, Julia Gillard, menggaris bawahi kedekatan dan pentingnya hubungan kedua negara sebagai tetangga dan mitra strategis (www.dfat.gov.au, 2010). Julia Gillard mengatakan bahwa Indonesia adalah 'teman dekat' dan rekan dalam memajukan kesejahteraan, perdamaian dan keamanan di kawasan. Dalam kunjungannya tersebut, Julia Gillard juga menekankan bahwa Indonesia dan Australia berbagi kepentingan dalam menghadapi tantangan keamanan dan pertahanan dan keduanya akan melanjutkan kerja sama yang erat dalam menghadapi ancaman ini demi kepentingan kedua negara.

Upaya yang Dilakukan Australia dan Indonesia dalam Mengatasi Cyber Crime

Permasalahan *cyber crime* yang dihadapi oleh Australia membuat melakukan sejumlah upaya dan kebijakan untuk mengatasi masalah tersebut. Berdasarkan *National Plan to Combat Cybercrime* (2013: 8) yang dikeluarkan oleh Attorney-General of Australia, salah satu dari lima prioritas Pemerintah Australia dalam upaya memerangi permasalahan *cyber crime* adalah dengan meningkatkan keterlibatan internasional dan berkontribusi dalam upaya global untuk mengatasi *cyber crime*. Kontribusi yang dilakukan oleh Australia ini adalah dengan mempromosikan kerangka hukum internasional serta membantu negara-negara lain untuk menghadapi *cyber crime*. Salah satu negara yang telah dibantu oleh Australia dalam upaya menangani permasalahan *cyber crime* adalah Indonesia.

Pada tahun 2011, AFP dan Polri secara bersama-sama meresmikan Cyber Crime Investigation Centre (CCIC). CCIC ini sendiri berada dalam area Markas Besar Kepolisian Republik Indonesia di Jakarta Utara. Pembangunan CCIC yang merupakan bantuan dari pemerintah Australia pada awalnya bertujuan untuk membangun dan meningkatkan kemampuan *cyber forensic* Polri (Connery, Sambhi, & McKenzie, 2014: 9-10). Beberapa bulan setelah itu, kantor investigasi *cyber crime* lainnya dibangun di empat kota besar lainnya, tepatnya berada di area Polda kota tersebut. Kantor investigasi *cyber crime* yang dibangun di empat Polda lainnya itu dinamakan Cyber Crime Investigation Satellite Office (CCISO).

Khusus dalam pembangunan CCIC dan CCISO, Australia telah memberikan bantuan senilai puluhan juta dolar. Secara total, Pemerintah Australia telah memberikan bantuan dana dan hibah peralatan investigasi mencapai 20 juta dolar Australia untuk pembangunan kantor investigasi *cyber crime* di Mabes Polri dan beberapa Polda di Indonesia (Sondakh, 2015: 188). Bantuan yang diberikan oleh Australia ini tidak semuanya berbentuk dana, namun termasuk di dalamnya peralatan investigasi berupa komputer yang tergolong canggih untuk melakukan investigasi terkait tindak *cyber crime* dan mengumpulkan bukti-bukti yang ada.

Kontribusi Australia dalam penanganan *cyber crime* di Indonesia tidak hanya sebatas pada hibah dana dan peralatan investigasi tersebut. Setelah pembangunan CCIC dan CCISO selesai, Australia masih terus berkontribusi dalam bentuk pengawasan dan pemeliharaan peralatan komputer di CCIC dan CCISO. Mayoritas bantuan ini didanai melalui bantuan pembangunan resmi Australia guna mempertahankan usaha operasi kedua negara melawan kejahatan transnasional (Connery, dkk, 2014: 5-9). Australia berharap bahwa dengan meningkatnya jumlah analis dunia maya yang terampil di Indonesia akan berdampak baik bagi Australia sendiri

Pemberian hibah dana dan peralatan pembangunan CCIC dan CCISO dari Australia tersebut merupakan bagian dari empat hal yang dilakukan kedua negara dalam upaya mengatasi *cyber crime* di Indonesia. *Pertama*, kegiatan kooperatif kedua negara di bidang *cyber forensics*. *Kedua*, hibah peralatan investigasi *cyber crime* di Mabes Polri dan beberapa Polda di Indonesia. *Ketiga*, pelatihan personel Polri oleh personel AFP berupa tugas belajar, pelatihan, dan konferensi dalam menanggulangi tindak kejahatan, termasuk *cyber crime*. *Keempat*, pengumpulan dan pertukaran informasi intelijen tentang berbagai isu keamanan (Sondakh, 2015: 187-189).

Kesimpulan

Sejak tahun 2010, Australia telah memberikan hibah dana dan peralatan investigasi *cyber crime* dalam rangka pembangunan CCIC dan CCISO serta beberapa pelatihan lain kepada Indonesia. Pembangunan kedua kantor investigasi *cyber crime* tersebut selesai pada tahun 2011, dengan CCIC terletak di Mabes Polri dan CCISO pada beberapa Polda di Indonesia. Dalam pembangunan kantor investigasi *cyber crime* tersebut, Australia telah mengucurkan dana hingga puluhan juta dolar yang berasal dari dana pembangunan resmi Pemerintah Australia.

Walaupun memiliki sejarah hubungan yang pasang surut, namun hal tersebut tidak menghalangi kerja sama dan berbagai tindakan kolektif yang dilakukan Australia, karena adanya kesamaan persepsi tentang *cyber crime* di antara kedua negara. Adanya kesamaan persepsi tersebut membuat kedua negara memiliki identitas kolektif, yakni sebagai negara yang sama-sama memiliki permasalahan *cyber crime*. Permasalahan yang sama tersebut menjadikan kedua negara rekan dalam mengatasi kejahatan dunia maya dan memicu berbagai tindakan kolektif.

Referensi

Droogan, J., & Zeimke-Dickens, C. (Penyunt.). (2010). Asian Transnational Security Challenges: Emerging Trends, Regional Visions. *The Council for Asian Transnational Threat Research*.

Firth, S. (2011). *Australia in International Politics : An Introduction to Australia's Foreign Policy.* New South Wales: Allen & Unwin.

Malby, S., Mace, R., dkk. (2013). *Comprehensive Study on Cyber Crime.* Vienna: UNODC.

Richard Tanter. (2012). *Shared Problems, Shared Interests: Reframing Australia-Indonesia Security Relations, in Knowing Indonesia : Intersections of Self, Discipline and Nation.* Dalam J. Purdey (Edt) Victoria: Australia Monash University Publishing.

Taylor, B. (Penyunt.). (2008). *Australia as an Asia-Pacific Regional Power: Friendships in Flux?*. Canberra: Routledge.

Indah, R. S. (2009). *Pencarian Suaka Politik Oleh 43 Warga Papua Ke Australia Ditinjau Dari Konvensi Hukum Jenewa 1951 Tentang Status Pengungsi.* Pekanbaru: Univesitas Islam Riau.

Sinaga, C. M. (2014). *Dinamika Hubungan Australia-Indonesia Dalam Bidang Politik.* Makasar: Universitas Hasanuddin.

Connery, D., Sambhi, N., & McKenzie, M. (2014). *A return on investment The future of police cooperation between Australia and Indonesia.* Australian Strategic Policy Institute.

DuPont, Alan. (1996). The Australia-Indonesia Security Agreement. *The Australian Quarterly,* Vol. 68 No. 2, 49-62.

Khadam, N. (2012). Insight to Cybercrime. *Hanyang Law Review,* Vol. 29, No.1, 55-57.

Sondakh, A. R. (2015). Kerjasama Polri dan AFP Dalam Menaggulangi Cyber Crime di Indonesia Tahun 20010-2012. *eJournal Ilmu Hubungan Internasional*.

Asosiasi Penyelenggara Jasa Internet Indonesia (2015). *Profil Pengguna Internet Indonesia 2014*. Diakses pada tanggal 12 Agustus 2016 dari Asosiasi Penyelenggara Jasa Internet Indonesia: https://apjii.or.id/downfile/file/PROFILPENGGUNAINTERNETINDONESIA2014.pdf

Australian Embassy for Indonesia. (2010). *Indonesia-Australia Joint Statement*. Diakses pada 15 Oktober 2015 dari Australian Embassy for Indonesia: http://indonesia.embassy.gov.au/jakt/JS2010.html

Australian Institute of Criminology (2010). *Australian crime: Facts & figures.* Diakses pada tanggal 2 Oktober 2016 dari Australian Institute of Criminology: http://www.aic.gov.au/media_library/publications/facts/2010/facts_and_figures_2010.pdf

BBC. (2016). Australia's Central Bank Targeted by Hackers. Diakses pada tanggal 30 Desember 2016 dari BBC: http://www.bbc.com/news/business-21738540

Department of Foreign Affairs and Trade. (2005). *Joint Declaration on Comprehensive Partnership Between Australia and the Republic of Indonesia*. Diakses pada tanggal 4 Oktober 2016 dari Department of Foreign Affairs and Trade: http://dfat.gov.au/geo/indonesia/Pages/joint-declaration-on-comprehensive-partnership-between-australia-and-the-republic-of-indonesia.aspx

Detikcom. (2016). *Asah Kemampuan Cybercrime, Polri Gandeng FBI*. Diakses pada tanggal 16 September 2016 dari Detikcom: http://inet.detik.com/read/2007/06/11/134803/792165/399/asah-kemampuan-cybercrime-polri-gandeng-fbi

Harvey, J. (2016). *Indonesia-Australia Relations: A Year After the Executions*. Diakses pada tanggal 10 Oktober 2016 dari The Diplomat : http://thediplomat.com/2016/05/indonesia-australia-relations-a-year-after-the-executions/

Interpol. (2010). *1st Interpol Information Security Conference*. Diakses pada tanggal 16 September 2016 dari Interpol: http://www.interpol.int/content/download/4815/41832/version/1/file/SGinformationSecurityConf20100915.pdf

Kementrian Luar Negeri. (2006). *Naskah Lombok Treaty*. Diakses pada tanggal 12 Desember 2016 dari Kementrian Luar Negeri: http://treaty.kemlu.go.id/uploads-pub/5554_AUS-2014-0212.pdf

Kompas. (2012). *Indonesia Masuk 10 Besar Penyumbang "Cyber Crime" Terbanyak*. Diakses pada tanggal 14 September 2016 dari Kompas: http://tekno.kompas.com/read/2012/05/16/09403718/Indonesia.Masuk.10.Besar.Penyumbang.Cyber.Crime.Terbanyak

Nancy Viviani. (2000). *Australia-Indonesia Relations After the East Timor Upheaval*. *JPRI Working Paper No. 64*. Diakses pada tanggal 15 September 2016 dari : http://www.jpri.org/publications/workingpapers/wp64.html

United Nations Office On Drugs and Crime. (2016). *Emerging Crimes*. Diakses pada tanggal 15 September 2016 dari United Nations Office On Drugs and Crime: https://www.unodc.org/unodc/organized-crime/emerging-crimes.html

ZDNET. (2016). Hackers hit central banks in Indonesia and South Korea. Diakses pada tanggal 30 Desember 2016 dari ZDNET: http://www.zdnet.com/article/hackers-hit-central-banks-in-indonesia-and-south-k