Journal of International Relations, Volume 2, Nomor 1, Tahun 2016, hal. 38-46
Online di http://ejournal-s1.undip.ac.id/index.php/jihi

KERJASAMA KEPOLISIAN NEGARA REPUBLIK INDONESIA (POLRI)-*AUSTRALIAN FEDERAL POLICE* (AFP) SEKTOR *CAPACITY BUILDING* DALAM PENANGGULANGAN TINDAK PIDANA *CYBER CRIME* DI INDONESIA PERIODE 2012-2014

Encik Mochammad Burhansyah A

Program Studi Ilmu 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

In the current era of globalization is growing at a rapid advances in technology. One proof of the technological advances with the internet. But technological advancements, giving a negative effect of the emergence of world crime (cyber crime). In the category of cyber crime, Indonesia is one country under threat of cyber crime in the world. To deal with and overcome this, the Indonesian National Police (INP) formed a partnership with the Australian Federal Police (AFP) in preventing the crime of cyber crime. The cooperation is realized in the form of increased capacity (capacity building) provided by AFP against police personnel through a foundation called the Jakarta Centre for Law Enforcement Cooperation (JCLEC). As a result of cooperation between the Police-AFP gives relatively good results. However, the handling of the case is still far from the expected that in 2012 as many as 86 cases of unresolved cases, as many as 115 cases in 2013 and January-June 2014 as many as 94 cases.

***Keywords*:** *cooperation*, *cyber crime*, *Indonesian National Police, Australian Federal Police, capacity building*

1. Pendahuluan

Pada era globalisasi saat ini, perkembangan teknologi informatika semakin canggih. Hal tersebut dapat dilihat dengan adanya internet (*interconnected network*). Internet merupakan salah satu hasil dari kemajuan teknologi informasi yang diciptakan pada abad ke-20 (Wahid dan Labib, 2005: 31). Saat ini internet digunakan oleh beberapa kalangan masyarakat baik usia muda (remaja), dewasa dan orang tua di berbagai belahan dunia untuk mencari beberapa sumber informasi, mengirim informasi dan melakukan kegiatan

bisnis ataupun *non*-bisnis. Fenomena kegiatan berinternet ini kemudian lebih dikenal dengan sebutan *cyberspace*(Maskun, 2013: 2).

Namun, kemajuan teknologi tidak sepenuhnya memberikan efek positif. Perkembangan teknologi yang pesat juga dapat menimbulkan beberapa efek negatif. Teknologi dapat dikatakan sebagai faktor penyebab timbulnya keinginan seseorang untuk berbuat jahat atau memudahkan terjadinya kejahatan (Wahid dan Labib, 2005: 59). Penyalahgunaan atau dampak negatif dari kemajuan teknologi informasi melalui sistem komputer dan jaringan internet kemudian lebih dikenal dengan istilah "*cyber crime*" (Arief 2003 dalam Wahid dan Labib, 2005: 43). *Cyber crime* merupakan tindak pidana melawan hukum secara sengaja yang dilakukan oleh individu bahkan terkadang dilakukan oleh sekelompok orang dengan memanfaatkan teknologi serta dunia maya sebagai media di dalam melakukan aksi kejahatannya demi memperoleh keuntungan finansial dan cenderung merugikan pihak lain (Suherman 2002 dalam Wahid dan Labib, 2005: 40).

Berdasarkan survei yang dilakukan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia setiap tahun semakin meningkat. pada tahun 2012 jumlah pengguna jasa layanan internet di Indonesia mencapai angka 63 juta orang (tekno.liputan6.com, 12 Desember 2012). Sedangkan pada tahun 2013, jumlah pengguna internet di Indonesia mencapai 71,19 juta. Diperkirakan jumlah pengguna internet di Indonesia pada tahun 2014 mencapai 107 juta dan tahun 2015 diprediksi akan mencapai angka 139 juta pengguna (www.antaranews.com, 15 Januari 2014).

Dalam hal ini, Indonesia termasuk sebagai salah satu negara dengan angka tindak pidana *cyber crime* terbesar di dunia. Pada tahun 2009, Indonesia menduduki peringkat ke Sembilan sebagai negara dengan jumlah tersangka *cyber crime* terbanyak (tekno.kompas.com, 30 April 2010). Kemudian di tahun 2010, peringkat Indonesia turun ke posisi 28 dalam hal kejahatan *cyber*. Sedangkan di tahun 2011 menurut perusahaan keamanan Symantec dalam *Internet Security Threat Report volume* 17, peringkat Indonesia naik ke posisi sepuluh sebagai negara dengan aktivitas kejahatan *cyber* terbanyak (tekno.kompas.com, 16 Mei 2012). Namun di tahun 2013, berdasarkan laporan Akamai yang dirangkum dala laporannya berjudul "*State of The Internet*" Indonesia berada pada urutan pertama mengalahkan posisi Tiongkok sebagai negara dengan kategori jumlah kejahatan *cyber* terbanyak (tekno.kompas.com, 17 Oktober 2013).

Sama halnya dengan jumlah pengguna internet di Indonesia yang semakin meningkat tiap tahunnya, angka tindak pidana *cyber crime* juga selalu mengalami peningkatan tiap tahunnya. Data *Cyber Crime Investigation Centre* Bareskrim Mabes Polri mencatat jika pada tahun 2012 terdapat 845 kasus tindak pidana *cyber crime*, tahun 2013 sebanyak 1.405 kasus dan di Januari-Juni 2014 sebanyak 753 kasus tindak pidana *cyber crime*. Menanggapi hal tersebut, Polri menjalin kerjasama dengan *Australian Federal Police* (AFP) guna meningkatkan kapasitas personil Polri dalam menanggulangi tindak pidana *cyber crime* di Indonesia. Kerjasama antara Polri dengan AFP dalam menanggulangi kejahatan transnasional telahberlangsung sejak tahun 1977 (AFP *Annual Report* 1997-1998 dalam Connery, Sambhi dan McKenzie, 2014: 3).

Salah satu bentuk kerjasama antara Polri dengan AFP yaitu dengan didirikannya Jakarta *Centre for Law Enforcement Cooperation* (JCLEC) untuk penegakan hukum dan pengembangan kapasitas yang didirikan pada tanggal 4 Februari 2004. Di JCLEC, program pengembangan kapasitas bagi para penegak hukum terdiri dari beberapa bidang, diantaranya yaitu bidang forensik, manajemen, intelijen, investigasi serta

konferensi/seminar/lokakarya.Kabareskrim Mabes Polri Komjen Pol. Sutarman berpendapat jika kejahatan *cyber* sudah sangat berbahaya serta mengancam segala aspek kehidupan sehingga dibutuhkan tindakan khusus. Sementara itu, mantan Wakapolri Komjen Nanan Sukarna mengatakan bahwa pihaknya sangat mengapresiasi kerjasama Polri dan AFP dikarenakan kejahatan *cyber* tidak dapat ditangani oleh satu negara saja, namun dibutuhkan koordinasi dengan negara lainnya. Sehingga hal tersebut kemudian menjadi cikal bakalterjalinnya kerjasama bilateral antara Indonesia-Australia melalui institusi keamanannya(metro.sindonews.com, 29 April 2013).

Dikarenakan kemampuan personil Polri masih berada pada tingkat dasar di bidang *cyber crime*, maka diperlukan program berupa pelatihan untuk peningkatan kapasitas personil Polri (inet.detik.com, 11 Juni 2007). Bahkan di dalam Resolusi Kongres PBB VII/1990 tentang *computer related crimes* menghimbau semua negara anggota agar memberikan pelatihan (*training*) bagi para hakim, pejabat serta aparat penegak hukum guna mengintensifkan penanggulangan penyalahgunaan komputer (Arief 2006 dalam Suhariyanto, 2013: 94-95). Sehingga program *capacity building* yang diberikan AFP kepada Polri sangat berguna untuk meningkatkan kemampuan personil Polri. Kerjasama antara Polri-AFP sektor *capacity building* juga bertujuan untuk mengantisipasi terjadinya tindak pidana *cyber crime* yang dapat mengancam stabilitas keamanan kawasan Indonesia, ASEAN dan Australia.

Pada dasarnya, hubungan kerjasama antara Indonesia dengan Australia terkadang berada pada titik tegang dikarenakan beberapa kejadian yang pernah terjadi di antara kedua belah pihak sehingga menyebabkan ketegangan. Salah satu ketegangan tersebut yakni terjadi pada tahun 2013 dimana Australia melakukan aksi penyadapan terhadap mantan presiden Susilo Bambang Yudhoyono. Bahkan akibat kejadian tersebut, hubungan antara Indonesia dengan Australia nyaris tidak dapat diperbaiki (www.bbc.com, 20 November 2013). Dalam program pengembangan kapasitas, *Australian Federal Police* merupakan negara pendonor paling besar bagi kesuksesan peningkatan kapasitas (*capacity building*) di JCLEC. Program pelatihan *cyber crime* di JCLEC telah berlangsung sejak tahun 2008. Namun pada tahun 2008-2010, program donor dalam pelatihan *cyber crime* yang diberikan oleh AFP masih belum begitu banyak, dimana pada waktu itu AFP hanya dua kali menjadi pendonor. Sedangkan program *capacity building* yang telah dilaksanakan tahun 2012-2014 dalam menanggulangi tindak pidana *cyber crime* di Indonesia yang diberikan AFP kepada Polri telah berjalan sebanyak sembilan kali.

2. Pembahasan

Teknologi komputer yang berkembang seiring dengan perkembangan arus globalisasi menciptakan sebuah perangkat yang disebut dengan internet (Wisnubroto 1999 dalam Wahid dan Labib, 2005: 33). Perkembangan internet berawal dari sebuah komputer yang kemudian dirangkai dengan komputer yang lainnya dalam sebuah ruangan yang disebut dengan LAN (*Local Area Network*) (Wahid dan Labib, 2005: 33). Beberapa LAN yang saling berhubung akan membentuk sebuah WAN (*Wide Area Network*). Serangkaian WAN apabila dihubungkan dengan beberapa WAN lainnya akan membentuk sebuah WAN yang memiliki kekuatan besar sehingga dapat terhubung antar-provinsi ataupun antar-negara (Wisnubroto 1999 dalam Wahid dan Labib, 2005: 33).

Pada era globalisasi saat ini, internet telah memberikan kontribusi yang cukup besar bagi semua orang di dunia. Berkat internet, jarak dan waktu menjadi sesuatu hal

yang tidak terbatas. Bahkan dengan adanya internet, setiap orang dapat mengakses suatu informasi ataupun berkomunikasi dengan orang di berbagai belahan dunia lainnya dengan cukup mudah (Wahid dan Labib, 2005: 31). Dengan demikian para pengguna internet (*netizen*) dapat melakukan *cyber space* tanpa terhalang oleh batas teritorial setiap negara (Wahid dan Labib, 2005: 32). Melalui internet, setiap orang dapat melakukan berbagai kegiatan yang jika diasumsikan sama dengan kegiatan di dunia nyata (*real space*) (Wahid dan Labib, 2005: 35).

Seiring dengan perkembangan arus globalisasi, saat ini internet masuk ke dalam kategori internet generasi kedua sehingga lebih memudahkan para penggunanya untuk melakukan komunikasi, transaksi jual beli ataupun mencari informasi. Pada internet generasi kedua, sarana untuk mengaksesnya dapat melalui perangkat apa saja dan cara pengoperasiannya dapat dilakukan dimana saja asalkan terhubung dengan jaringan internet. Jika pada internet generasi pertama sarana dalam mengakses internet hanya melalui komputer (PC) saja dan pengoperasiannya hanya dapat dilakukan di depan meja saja, maka pada internet generasi kedua, sarana untuk mengaksesnya dapat melalui perangkat apa saja dan cara pengoperasiannya dapat dilakukan dimana saja asalkan terhubung dengan jaringan internet(Wahid dan Labib, 2005: 75).Sehingga dengan kemajuan internet pada generasi kedua, lebih memudahkan bagi sebagian orang untuk melakukan tindak pidana *cyber crime*.

Pada umumnya, jenis-jenis tindak pidana *cyber crime* diantaranya (1) *Unauthorized Acces to Computer System and Service*; (2) *Illegal Contents*; (3) *Data Forgery*; (4) *Cyber Espionage*; (5) *Cyber Sabotage and Extortion*; (6) *Offense Against Intellectual Property*; (7) *Infrengments of Privacy*; (8) *Gambling*; (9) *Cyber Porn*/*Cyber Sex*; (10) *Cyber Stalking*; (11) *Hacking*; (12) *Carding*(Wahid dan Labib, 2005: 71-73). Tindak pidana *cyber crime* memiliki beberapa karakteristik yang membedakannya dengan kejahatan konvensional yakni (1) Perbuatan yang dilakukan secara ilegal; (2) Perbuatan tersebut menggunakan perangkat apapun yang terhubung dengan internet; (3) Perbuatan tersebut mengakibatkan kerugian *materill* maupun *immaterial*; (4) Pelakunya merupakan orang yang memiliki kemampuan dalam pengoperasian teknologi dan internet; (5) Perbuatan tersebut sering dilakukan secara transnasional atau melintasi batas wilayah negara (Wahid dan Labib, 2005: 76).Sejarah singkat perkembangan tindak pidana *cyber crime* di dunia yakni pada tahun 1960 dan 1970, kejahatan komputer yang umumnya terjadi yaitu terkait dengan perusakan komputer pada sistem komputer dan perusakan jaringan telepon jarak jauh (Kabay, 2008: 5). Sedangkan di akhir tahun 1990-an dan dekade tahun 2000 seiring dengan kemajuan teknologi, penipuan kartu kredit diidentikan dengan pencurian identitas (Kabay, 2008: 13).

Atas perkembangan tindak pidana *cyber crime* beserta jenis-jenisnya yang semakin beragam, saat ini tindak pidana*cyber crime* merupakan salah satu dari bentuk kejahatan yang mendapatkan perhatian luas dalam dunia internasional (Arief 2001 dalam Suhariyanto, 2013: 92). Hal tersebut dibuktikan oleh beberapa respon global terkait tindak pidana *cyber crime* diantaranya (Broadhurst, 2006: 423-428): (1) G8 *Senior Experts Group on Transnational Organize Crime*, dimana pada tahun 1996, G8 (Kanada, Perancis, Jerman, Itali, Jepang, Inggris, AS dan Rusia) menyusun 40 rekomendasi yang bertujuan untuk meningkatkan efisiensi dalam penindakan terhadap kejahatan terorganisir transnasional melalui dua program yakni kapasitas diperkuat dalam penyidikan dan penuntutan kejahatan teknologi tinggi serta rezim yang lebih efektif untuk kerjasama lintas

batas dalam masalah pidana. (2) ASEAN yang telah melakukan pertemuan empat kali pada *level* menteri dalam hal kejahatan transnasional (Manila tahun 1997, Rangon tahun 1999, Singapura tahun 2001, Bangkok tahun 2003) bertujuan untuk membahas komitmen dalam berkolaborasi antar-negara anggota ASEAN di dalam memerangi segala bentuk kejahatan *cyber*. (3) Uni Eropa dan Europol, mengadopsi posisi umum pada negosiasi yang berkaitan dengan Konvensi*Cyber Crime* dan konvensi Uni Eropa pada bantuan timbal balik dalam masalah pidana dan ekstradisi.Europol juga memiliki fungsi untuk mendukung kegiatan operasional aparat penegak hukum nasional dan baru-baru ini diperluas cakupannya untuk memerangi kejahatan *cyber*.

Respon global berikutnya yakni (4) *The Organization for Economic and Cultural Development* (OECD), aktif di bidang *cyber crime* dan keamanan *online* guna mengevaluasi keseimbangan antara penegakan hukum dan masalah privasi serta sarana negara-negara. Setelah tragedi 11 September 2001, Pemerintah dari negara-negara anggota OECD mengembangkan serangkaian pedoman yang dirancang untuk melawan *cyber* terorisme, virus komputer, *hacking* dan ancaman terkait. (5) Interpol, dimana organisasi Kepolisan Internasional tersebut memiliki dua prioritas utama yang dikategorikan sebagai kejahatan transnasional serius yakni kejahatan keuangan dan teknologi tinggi. Dalam hal ini, Interpol juga telah meningkatkan fokusnya pada kejahatan terkait properti intelektual dikarenakan kelompok kejahatan terorganisir saat ini semakin canggih karena dibiayai untuk melakukan kejahatan pada skala global. (6) Asia Pasific *Economic Council* (APEC), APEC berkomitmen untuk membuat undang-undang keamanan *cyber* yang komprehensif, setara dengan standar internasional yang ada, mengidentifikasi atau membuat unit nasional kejahatan *cyber* dan teknologi tinggi, serta membangun CERT, guna menghadapi ancaman pertukaran dan mengantisipasi kerentanan informasi.

Respon global tersebut juga dapat dilihat melalui beberapa rezim yang dibentuk dunia internasional terkait *cyber crime*. Salah satu rezim tersebut yakni Konvensi Tindak Pidana Telematika Budapest, 23.XI.2001 yang diadakan di Afrika. Dalam konvensi tersebut, terdapat kurang lebih 39 negara yang meratifikasi terdiri dari 35 negara di belahan Eropa, Australia, Republik Dominica, Jepang dan Amerika Serikat (Seger, 2013: 1). Tujuan dari Konvensi Budapest yakni untuk menindaklanjuti dan penilaian terhadap perkembangan *cyber crime* serta memberikan pelatihan guna menanggulangi *cyber crime* kepada negara yang meratifikasi (Seger, 2013: 7). Rezim internasional guna menindaklanjuti terhadap tindak pidana *cyber crime* tidak hanya Konvensi Tindak Pidana Telematika Budapest, namun masih terdapat beberapa rezim internasional lainnya yakni Resolusi Kongres PBB VIII/1990 tentang *computer related crime*, *Draft Convention on Cyber Crime* yang disusun pada bulan November 1996 (Wahid dan Labib, 2005: 155). Selain itu, dalam jaringan Kepolisian Internasional (Interpol) telah mendirikan Interpol *Global Complex for Innovation* (IGCI) di Singapura. IGCI yang dibangun pada 13 April 2015 bertujuan untuk mencegah serangan *cyber crime* internasional serta untuk melatih polisi-polisi dari berbagai negara anggota yang tergabung dalam Interpol (www.dw.com, 13 April 2015).

Melihat respon dunia internasional terhadap *cyber crime*, pada Maret 2008, Indonesia mengesahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang digunakan untuk menindaklanjuti atau mengadili pelaku tindak pidana *cyber crime*. Dalam Undang-Undang ini juga diatur mengenai prosedur dan alat bukti yang mengalami perluasan, yaitu dimasukkannya alat bukti baru yang berkaitan

dengan media elektronik (Suhariyanto, 2013: 6). Pada dasarnya pembentukan UU ITE tahun 2008 dibentuk atas dasar beberapa hal, diantaranya dikarenakan oleh keterdesakan kebutuhan nasional dan keterdesakan kebutuhan internasional. Keterdesakan kebutuhan nasional melingkupi ketidakmampuan sistem hukum nasional dalam menanggulangi *cyber crime* di dalam negeri (Suhariyanto, 2013: 49). Hal tersebut diperkuat dengan kasus *cyber crime* yang pernah terjadi pada tahun 2001 (Suhariyanto, 2013: 57).

Terkait tindak pidana *cyber crime*, Indonesia memiliki organisasi yang menangani segala pengaduan terhadap tindak pidana *cyber crime*, yaitu ID-SIRTII (Indonesia *Security Incident Response Team on Internet Infrastructure*) dan ID-CERT (*Computer Emergency Response Team*). ID-SIRTII dan ID-CERT memiliki tugas dan fungsi yang sama yakni mencatat dan menanggapi segala pengaduan masyarakat terhadap gangguan keamanan dalam berinternet (Setiadi dkk, 2012: 110-111). Sedangkan dalam ruang lingkup Polri guna menanggapi tindak pidana *cyber crime*, Kapolri mengeluarkan Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 1 Tahun 2006 tentang Rencana Kerja Kepolisian Negara Republik Indonesia serta Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 7 Tahun 2009 tentang Sistem Laporan Gangguan Keamanan dan Ketertiban Masyarakat. Dalam membantu kinerja Polri dalam menanggulangi *cyber crime* di Indonesia, Polri melalui bantuan AFP mendirikan *Cyber Crime Investigation Centre* di Bareskrim Mabes Polri serta *Cyber Crime Investigation Satellite Office* (CCISO) di beberapa Polda (tekno.kompas.com, 30 April 2013).Salah satu anggota Pemeriksa Barang Bukti *Digital Cyber Crime Investigation Center* (CCIC) Mabes Polri, Grawas Sugiharto mengatakan bahwa menumpas kejahatan *cyber* di Indonesia tergolong cukup rumit dibandingkan dengan di luar negeri. Hal tersebut dikarenakan penggunaan kartu SIM yang tidak terkendali sehingga penanganannya menjadi terkendala (http://techno.okezone.com, 27 Februari 2013).

Dalam ruang lingkup domestik, upaya yang dilakukan Polri dalam menangani serta menanggulangi terjadinya tindak pidana *cyber crime* di Indonesia yakni (1) Merespon dan menerima setiap pengaduan dari masyarakat atas dugaan terjadinya tindak pidana *cyber crime* serta mendata setiap penanganan kasus terhadap pengaduan serta laporan dari masyarakat tentang terjadinya tindak pidana *cyber crime*; (2) Melakukan penyelidikan secara *online* (penyelidikan melalui internet) terhadap kejahatan-kejahatan yang menggunakan jejaring sosial *facebook*, *email* dan penjualan secara *online*; (3) Melakukan kerjasama dengan Kementrian Komunikasi dan Informatika (Kominfo); (4) Melakukan kerjasama dengan bidang perbankan khususnya Bank Indonesia, untuk menghindari rekening dengan identitas palsu yang nantinya digunakan oleh para pelaku kejahatan Informasi Transaksi Elektronik (ITE); (5) Menghimbau kepada masyarakat agar berinternet yang aman; (6) Meningkatkan pemahaman serta keahlian Polri di bidang *cyber crime*dengan mengirimkan anggotanya untuk mengikuti berbagai macam kursus (pelatihan) di beberapa negara maju.

Sedangkan di Australia, upaya domestic yang dilakukan oleh Pemerintah Australia untuk menanggulangi tindak pidana *cyber crime* yakni melalui beberapa langkah diantaranya (1) Mendidik warga negaranya untuk melindungi dirinya sendiri dengan cara memperketat sistem keamanan internet dan komputerisasinya; (2) Bermitra dengan industri untuk mengatasi masalah *cyber crime*; (3) Membina pendekatan intelijen melalui pertukaran informasi yang lebih baik guna meningkatkan kapasitas dan kapabilitas lembaga-lembaga pemerintahan dalam menanggulangi tindak pidana *cyber crime*; (4)

Memperkuat keterlibatan internasional tentang *cyber crime*; (5) Memastikan kerangka peradilan pidana terus berpacu dengan perubahan teknologi.

Pada tanggal 4 Februari 2004 didirikan Jakarta *Centre for Law Enforcement Cooperation* (JCLEC). JCLEC didirikan guna memberikan pelatihan berupa *capacity building* bagi aparat penegakan hukum. Menurut Brigjen Boy Salamuddin pada tanggal 20 Desember 2010 ketika melakukan kunjungan ke JCLEC Semarang menyatakan bahwa pendirian JCLEC bertujuan untuk meningkatkan kinerja serta kompetensi personil Polri guna menjamin keamanan antar-negara kawasan (news.detik.com, 21 November 2010).Pendirian JCLEC dipelopori oleh Kepala Kepolisian Federal Australia bersama dengan Kepala Kepolisian Negara Republik Indonesia dikarenakan keduanyamendirikan JCLEC akibat aksi terorisme Bom Bali I tahun 2002. Pembentukan JCLEC didasari oleh "*Joint Declaration*" bertujuan untuk meningkatkan kemampuan para personil khususnya Polri agar mampu menangani segala macam kejahatan transnasional dengan baik dan professional (Hasan & Naramurti, 2013: 101). Pendirian JCLEC juga dikarenakan oleh situasi politik di Indonesia yang pada waktu itu rentan terhadap aksi radikalisme serta menindaklanjuti tragedi Bom Bali I yang menewaskan mayoritas warga negara Australia, sehingga kemudian JCLEC dibentuk.

Dalam rangka pencapaian kesejahteraan masyarakat dan keamanan negara, Kepolisian Negara Republik Indonesia bekerjasama dengan *Australian Federal Police* bertujuan untuk memperkuat teknologi di sektor keamanan dan pertahanan guna menghadapi ancaman kejahatan transnasional yang cenderung menggunakan manfaat teknologi. Komitmen kerjasama tersebut dituangkan dalam sebuah program besar dengan didirikannya JCLEC bertujuan untuk memberikan pelatihan berupa pengembangan kapasitas bagi aparat penegak hukum. Program di JCLEC tidak jauh dari isu kejahatan transnasional yang kemudian menjadi suatu alasan dibentuknya Yayasan JCLEC.Program *capacity building* yang diberikan oleh AFP terhadap Polri guna menanggulangi serta mengantisipasi terjadinya tindak pidana *cyber crime* sejak tahun 2012-2014 sebanyak sembilan program. Selain itu dalam program pengembangan kapasitas yang diadakan di JCLEC, salah satu faktor utama yang mendukung kesuksesan berjalannya program yakni berkat bantuan donor dari negara-negara asing serta institusi dalam negeri dimana dalam hal ini Australia merupakan salah satu negara yang memberikan kontribusi donor terbesar bagi kesuksesan program *capacity building* antara Polri dan AFP. Program *capacity building* yang diberikan AFP terhadap Polri memberikan hasil yang relatif cukup baik dimana semenjak program *capacity building* dicanangkan, kinerja Polri dalam penanganan *cyber crime* kian meningkat. Namun, penanganan kasus tersebut masih jauh dari yang diharapkandimana hal tersebut dapat dilihat melalui data dari *Cyber Crime Investigation Centre* Bareskrim Mabes Polri pada tahun 2012 kasus terselesaikan sebanyak 86 kasus, 2013 sebanyak 115 kasus dan Januari-Juni 2014 sebanyak 94 kasus.

3. Kesimpulan

Pada era globalisasi saat ini kejahatan transnasional semakin beragam bentuk dan motifnya. Salah satu dampak negatif dari kemajuan globalisasi yakni munculnya tindak pidana *cyber crime*. *Cyber crime* merupakan tindak pidana melawan hukum secara sengaja yang dilakukan oleh individu atau sekelompok orang dengan memanfaatkan teknologi serta dunia maya di dalam melakukan aksi kejahatannya baik untuk memperoleh keuntungan ataupun tidak dan cenderung merugikan pihak lain. Memandang bahwa *cyber*

crime termasuk tindak pidana yang timbul akibat kemajuan globalisasi, muncul beberapa rezim diantaranya seperti resolusi tentang *computer related crime* pada Kongres PBB VIII/1990, Konvensi Tindak Pidana Telematika Budapest 23.XI.2001 yang diadakan di Afrika, serta beberapa rezim lainnya. Dalam hal ini, Indonesia termasuk dalam kategori salah satu negara dengan jumlah *cyber crime* terbanyak.

Menanggapi respon global tersebut, Indonesia mengambil langkah dengan membentuk Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selain itu Pemerintah Indonesia juga melakukan beberapa tindakan yakni dengan memberikan kesempatan bagi Polri untuk menjalin kerjasama dengan AFP di sektor *capacity building* guna menekan angka *cyber crime* di Indonesia dan untuk meningkatkan kinerja aparat kepolisian. Kerjasama yang dijalin antara Polri-AFP sektor *capacity building* sejak tahun 2012-2014 di bidang *cyber crime* telah berjalan sebanyak sembilan kali. Meskipun sejak tiga tahun terakhir telah dilakukan program *capacity building* antara Polri dan AFP, namun penanganan kasus tindak pidana *cyber crime* di Indonesia masih jauh dari yang diharapkandimana hal tersebut dapat dilihat melalui data dari *Cyber Crime Investigation Centre* Bareskrim Mabes Polri pada tahun 2012 kasus terselesaikan sebanyak 86 kasus, 2013 sebanyak 115 kasus dan Januari-Juni 2014 sebanyak 94 kasus.

Daftar Pustaka

Hasan, SH., M.H., Drs. H. Iskandar, Naramurti, M.M., Drs. Nina. (2013). *Kerjasama Kepolisian dan Penegakan Hukum Internasional*. Jakarta Barat: PT. Firris Bahtera Perkasa.

Maskun, S.H., LLM. (2013). *Kejahatan Siber (Cyber Crime)*. Jakarta: Kencana Pranada Media *Group*.

Suhariyanto, S.H., M.H., Budi. (2013). *Tindak Pidana Teknologi Informasi (Cybercrime)* (2nd ed). Jakarta: PT. Raja Grafindo Persada.

Wahid, SH., MA., Drs. Abdul., & Labib SH., Mohammad. (2005). *Kejahatan Mayantara (Cyber Crime)*. Bandung: PT. Refika Aditama.

Broadhust, Roderic. (2006). *Developments in the Global Law Enforcement of Cyber-Crime*.

Cyber Crime Investigation Centre Bareskrim Mabes Polri (2014). *Rekapitulasi Data Kasus Cyber Crime Polda-Polda Seluruh Indonesia*.

David Connery, Natalie Shambie and Michael McKenzie. (2014). *A Return on Investment the Future of Police Cooperation between Australia and Indonesia*.

Farisya Setiadi, Yudho Giri Sucahyo and Zainal A. Hasibuan. (2012). *An Overview of Development Indonesia National Cyber Security*.

M. E. Kabay, Ph.D, CISSP-ISSMP. (2008). *A Brief History of Computer Crime: An Introduction for Students*.

Seger, Alexander. (2013). *Budapest Convention on Cyber Crime*.

2012, Pengguna Internet Indonesia Capai 63 Juta. (2012). Dalam *http://tekno.liputan6.com/read/467387/2012-pengguna-internet-indonesia-capai-63-juta*. Diunduh pada tanggal17 September 2014 pukul 16:00 WIB.

BIN: Australia Menyadap Indonesia sejak 2007. (2013). Dalam http://www.bbc.com/indonesia/berita_indonesia/2013/11/131120_bin_sadap_australia. Diunduh pada tanggal 24 Februari 2015 pukul 05:00 WIB.

Hein, Matthias von. (2015). Interpol *Fights Cyber Crime in* Singapore. Dalam *http://www.dw.com/en/interpol-fights-cyber-crime-in-singapore/a-18379244*. Diunduh pada tanggal 22 April 2015 pukul 07:16 WIB.

Hidayat, Wicaksono Surya. (2013). Indonesia Bangun Pusat Investigasi Kejahatan "*Cyber*". Dalam *http://tekno.kompas.com/read/2013/04/30/15491539/Indonesia.Bangun.Pusat.Investigasi.Kejahatan.Cyber*. Diunduh pada tanggal 22 April 2015 pukul 10:15 WIB.

JCLEC, Pusat Pelatihan Investigasi Polri Bertaraf Internasional. (2010). Dalam *http://news.detik.com/berita/1498605/jclec-pusat-pelatihan-investigasi-polri-bertaraf-internasional*. Diunduh pada tanggal 24 April 2015 pukul 16:15 WIB.

Kolo, Zenobius Wilfridus. (2013). Dalam http://metro.sindonews.com/read/743087/31/kejahatan-cyber-ancam-keamanan-ekonomi-negara-1367222986. Diunduh pada tanggal 22 Februari 2015 pukul 21:07 WIB.

Panji, Aditya. (2013). Serangan "*Cyber*" Dunia, Terbanyak dari Indonesia. Dalam *http://tekno.kompas.com/read/2013/10/17/0811211/serangan.cyber.dunia.terbanyak.dari.indonesia*. Diunduh pada tanggal 18 September 2014 pukul 04:00 WIB.

Rakhmatulloh. (2013). Mabes Polri Tangkap 25 WNA Pelaku *Cyber Crime*. Dalam *http://nasional.sindonews.com/read/800431/14/mabes-polri-tangkap-25-wna-pelaku-cyber-crime-1383199838*. Diunduh pada tanggal 21 April 2015 pukul 09:45 WIB.

Sinaga, Royke. (2014). APJII: Pengguna Internet di Indonesia terus Meningkat. Dalam *http://www.antaranews.com/berita/414167/apjii-penguna-internet-di-indonesia-terus-meningkat*. Diunduh pada tanggal 17 September 2014 pukul 16:25 WIB.

Suryadhi, Ardhi. (2007). Dalam *http://inet.detik.com/read/2007/06/11/134803/792165/399/asah-kemampuan-cybercrime-polri-gandeng-fbi*. Diunduh pada tanggal 23 Februari 2015 pukul 21:41 WIB.

Wahyudi, Reza. (2012). Indonesia Masuk 10 Besar Penyumbang "*Cyber Crime*" Terbanyak. Diunduh dalam *http://tekno.kompas.com/read/2012/05/16/09403718/indonesia.masuk.10.besar.penyumbang.quotcyber.crimequot.terbanyak*. Diunduh pada tanggal 17 September 2014 pukul 17:35 WIB.

Wiek. (2010). Peringkat Indonesia di *Cyber Crime* Naik. Dalam *http://tekno.kompas.com/read/2010/04/30/10240384/Peringkat.Indonesia.di.CyberCrime.Naik*. Diunduh pada tanggal 17 September 2014 pukul 17:00 WIB.