



**PERAN
INTERNATIONAL TELLECOMMUNICATION UNION
DALAM MENGATASI CYBER CRIME DI INDONESIA
TAHUN 2011 - 2013**

Ahmad Daniel Kusumah Anshary

Program Studi 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

International Telecommunication Union (ITU) is an organization founded in 1865 with the goal of developing the technology and Informatics. Indonesia is one country that has an office member of ITU since 1984 as a coordination center in the Southeast Asia region working together to develop and secure ICT in the countries of Southeast Asia. This research seeks to analyze the role of ITU in combatting cyber crime rate in Indonesia in 2011 - 2013, at which time the level of criminal activity in Indonesia cyber crime has increased. By using the method descriptive study, researchers found that the ITU has been instrumental in making every effort to develop and secure ICT in Indonesia, but there are factors that make cyber crime in Indonesia has increased in 2011 - 2013. However after further testing through a variety of data and a pooled analysis, the researchers concluded that there are barriers that keep cyber crime in Indonesia increased despite the ITU has been instrumental in Indonesia.

Keywords: role, ITU, intergovernmental organizations, international organizations, cyber crime

1. Pendahuluan

Telah 150 tahun lamanya *International Tellecommunication Union* (ITU) menjadi yang pertama dan menjadi organisasi internasional tertua yang berfokus pada pengembangan teknologi informatika dan telekomunikasi dunia. Berawal dari 17 Mei 1865, ITU pertama kali didirikan di Paris oleh 20 negara yang pada saat itu sedang melakukan konvensi dan berusaha menemukan cara untuk mengatasi hambatan dan membuat layanan telekomunikasi yang lebih efisien. Negara-negara tersebut berkumpul membuat kerangka kerja untuk membakukan peralatan telegrafi, mengatur petunjuk pengoperasian yang sesuai, dan menentukan tarif serta aturan internasional umum (www.itu.int, 2015).

Selama masa yang panjang itu, ITU yang sekarang bekerja dalam naungan Perserikatan Bangsa-bangsa (PBB) telah melalui berbagai jenis pengembangan dalam melakukan regulasi, mengikuti perkembangan zaman dari telegram dan telepon kabel, hingga penggunaan satelit yang pertama kali diluncurkan oleh Uni Soviet pada 4 Oktober 1947, *Sputnik1* sebagai media komunikasi maupun penggunaannya sebagai penghubung antar wilayah fana yang lebih dikenal dengan sebutan internet. Dengan berbagai tantangan

baru inilah, ITU membentuk wilayah-wilayah dengan pusat kantor yang berbeda, untuk mengatasi luasnya jangkauan regulasi telekomunikasi negara-negara di dunia (www.itu.int, 2015). Pembentukan bagian ini terbagi menjadi enam wilayah utama, antara lain Afrika, Amerika, negara-negara Arab, Asia Pasifik, Eropa, dan wilayah bekas Uni Soviet.

Peran ITU dalam membangun kenyamanan dan keamanan negara saat menggunakan alat telekomunikasi kembali diperjelas pada perkumpulan negara anggota di WSIS (*World Summit of the Information Society*) tahun 2013 yang didasari dari *Plenipotentiary Conference* tahun 2006. Perkumpulan ini menjelaskan bahwa ITU memiliki peran penting sebagai fasilitator guna membangun aksi C5, yaitu: *Cybersecurity, Collaborative, Corporation, Child*, dan *Cyberthreat* (www.itu.int, 2015).

Bila dibandingkan dengan kantor ITU regional lain, kantor ITU di Asia Pasifik yang berpusat di Bangkok menjadi salah satu cabang yang memiliki negara anggota paling banyak, sehingga ITU juga membuka kantor cabang di Indonesia sebagai pusat negara di wilayah Asia Tenggara. Secara global, Asia memang merupakan wilayah terluas dengan pengguna internet yang mencapai 45,7% pada tahun 2014 dari seluruh populasi masyarakat dunia (www.internetworldstats.com)

Dalam penelitian ini, peneliti memilih untuk menggambarkan secara tepat bagaimana peran ITU sebagai organisasi internasional yang berada di bawah PBB dalam mengatasi *cyber crime* di Indonesia. Indonesia merupakan salah satu negara di wilayah Asia Pasifik dengan tingkat pengguna internet paling rawan menjadi korban *cyber crime*, penelitian ini dapat menjadi model upaya yang harus dipahami oleh tiap-tiap negara dalam mengembangkan teknologi informasi dan telekomunikasi (www.internetworldstats.com, 2015).

Mempertimbangkan dari permasalahan di atas peneliti kemudian memberi hipotesa bahwa ITU berperan dalam melakukan berbagai upaya untuk mengembangkan dan mengamankan ICT di Indonesia, namun terdapat faktor yang membuat *cyber crime* di Indonesia mengalami peningkatan pada tahun 2011 - 2013. Perbedaan kredibilitas kekuatan yang dimiliki setiap negara anggota dalam organisasi menimbulkan keinginan kuat bagi negara-negara berkembang untuk mendapatkan keuntungan lebih dari negara lain di dalam organisasi walaupun terkadang dengan mengabaikan kepentingan dan tujuan organisasi yang sebenarnya dibuat untuk kepentingan bersama. Perbedaan kredibilitas ini juga memunculkan hegemoni di dalam organisasi yang sesungguhnya dapat menjadi dasar bagi keuntungan yang didapat, sehingga keaktifan negara anggota dalam memanfaatkan organisasi internasional demi kepentingan nasionalnya sangat mempengaruhi keuntungan yang didapatnya dalam permainan yang disebut *zero sum gain*.

Untuk membuktikan hipotesis tersebut, peneliti menggunakan tipe penelitian deskriptif dengan teknik pengumpulan data dalam penelitian menggunakan metode studi kepustakaan, wawancara dan studi lapangan. Penelitian ini tidak hanya memanfaatkan data-data dalam perpustakaan yang berbentuk sekunder seperti buku, koran, jurnal, dokumentasi dan website terkait, namun juga melakukan analisa langsung ke lapangan, yakni kantor area ITU yang berada di Jakarta serta melakukan wawancara dengan kepala ITU regional Asia Tenggara dan kepala bagian kejahatan ekonomi khusus bidang *cyber crime* INTERPOL Polri.

2. Pembahasan

Perkembangan Teknologi Informatika dan Pengaruhnya Terhadap Keamanan Nasional

Peran teknologi memiliki kaitan yang erat dengan perkembangan manusia menuju era informatika. Berbagai revolusi telah terjadi dan mempengaruhi hampir segala aspek kehidupan manusia, baik secara industri, sistem politik, ekonomi, budaya dan bahkan informatika. Segala kemudahan dalam berkomunikasi, kecepatan dan ketepatan dalam

menerima atau menyebarkan berbagai berita dan pesan dapat didapatkan pada saat ini, perubahan yang demikian diyakini oleh Fakhmi Tamzil seorang dosen fakultas ilmu komputer universitas esa unggul Jakarta dalam tulisannya yang berjudul “Peran Teknologi Informasi Dalam Dunia Komunikasi” sebagai revolusi teknologi komunikasi atau revolusi informasi.

Internet termasuk salah satu teknologi baru yang sangat berharga bagi sejarah perkembangan teknologi informatika, internet telah membuktikan keberhasilannya dalam menciptakan ruang digital yang dapat terhubung secara instan melalui media komunikasi seperti komputer, laptop dan handphone. Ruang digital inilah yang kemudian dinamakan ruang siber (*cyberspace*), seperti pernyataan yang menyatakan bahwa *cyberspace* merupakan realitas yang tidak terbantahkan sebagai bentuk kompleksitas dunia informasi dan komunikasi, *cyberspace* telah menjadi ruang tersendiri yang dapat menjadi tempat berkompetisi secara politik maupun non-fisik, sebagai berikut:

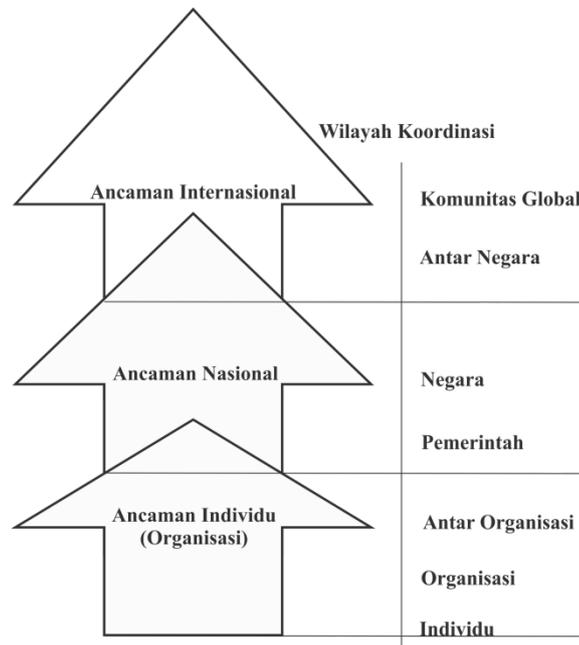
“cyberspace is an unavoidable reality that wraps our planet in a complex information and communication skin...cyberspace has become a battleground, a ground zero, for geopolitical contest and armed struggle” (Deibert, 2013: 11)

Istilah *cyberspace* kemudian didefinisikan oleh Caveltry dalam jurnal yang berjudul *Contemporary Security Studies* sebagai sebuah arena di mana semua jaringan komunikasi, data, sumber, dan pengguna informasi melebur dalam sebuah dimensi elektronik yang berinteraksi dengan kecepatan sangat tinggi, beragam, dan dapat menampung volume sangat besar (Cavelty, 2013).

Dalam perkembangannya, *cyberspace* tidak hanya menjadi sarana dalam melakukan komunikasi atau tempat berinteraksi, namun juga telah menjadi arena memperebutkan kekuasaan di dalamnya, yakni kekuasaan di dalam *cyberspace* tersebut. Proses perebutan kekuasaan ini menimbulkan banyak ancaman bagi penggunanya yang meliputi seluruh masyarakat dunia yang kemudian menjadi perhatian khusus bagi negara-negara. Ancaman siber (*cyberthreat*) dikategorikan menjadi tiga bagian; ancaman kepada individu dan organisasi, ancaman kepada organisasi pemerintahan negara, dan ancaman global (Nugroho, 2014: 73).

Ancaman yang dapat ditimbulkan oleh *cyber crime* kepada organisasi pemerintahan dan institusi negara dapat mengancam pelayanan publik, ekonomi, sosial, politik, budaya, pertahanan, hukum dan bahkan keselamatan masyarakatnya. Dengan bentuk *cyberthreat* yang sistematis tersebut, tercipta pola pengamanan ideal yang saling berpengaruh terhadap keamanan satu sama lain antara individu, organisasi, negara dan kemanan global, yang digambarkan sebagai berikut:

Grafik 1
Wilayah Koordinasi bagi *Cyberthreat*



Sumber: diolah dari Nugroho, 2014: 73.

Grafik 1 memperlihatkan wilayah koordinasi secara terstruktur dimana ancaman bagi individu dan organisasi dapat diselesaikan melalui individu, organisasi dan kerjasama antar organisasi yang membangun keamanan mereka. Ancaman nasional dapat mempengaruhi ancaman individu dan organisasi, ancaman ini hanya dapat diselesaikan jika negara dan pemerintah membentuk keamanan nasional yang memadai. Ancaman internasional menempati tingkat teratas yang dapat mempengaruhi keamanan negara, individu, dan organisasi di bawahnya, ancaman ini hanya dapat terselesaikan jika kerjasama antar negara dan komunitas global dapat membangun keamanan global.

Peran “ITU” dalam Membangun Kenyamanan dan Keamanan Telekomunikasi Informatika di Indonesia

Berbagai langkah dilakukan ITU dalam usahanya untuk mengatasi keamanan ICT di Indonesia, antara lain advokasi kepada pemerintah dan pihak-pihak terkait di tingkat nasional terkait kebijakan, peraturan dan perbaikan hukum untuk memperkuat rencana aksi nasional untuk mengatasi *cyber crime*; pengaturan kapasitas anggota dan kelompok strategis terkait *cyber crime* melalui dukungan teknis dan pelatihan; pengumpulan data tentang situasi *cyber crime* di dunia melalui serangkaian survey, jajak pendapat dan penelitian; dan penyebarluasan informasi terkait keamanan *cyber* melalui sosialisasi, seminar, diskusi dan konferensi (www.itu.int, 2015).

Sebagai organisasi internasional yang bergerak di bidang telekomunikasi, ITU berusaha meningkatkan kemampuan Indonesia dan negara berkembang lainnya dalam mengembangkan *wireless broadband*, ITU pada tahun 2011 bekerja sama dengan pemerintah Korea demi mengimplementasikan program yang disebut “*Master Plan for Wireless Broadband in the Asia Pacific Region*”. Program ini berlangsung sepanjang tahun 2011 dan berhasil diimplementasikan pada tahun 2012, menghasilkan peningkatan kapasitas *broadband* di wilayah Indonesia dan Asia Pasifik dan pengembangan sumber

daya yang dilatih untuk mengembangkan program ini. Peningkatan teknologi di Indonesia kemudian diikuti dengan pelatihan intensif yang dilakukan ITU pada tanggal 16-18 September 2012 dengan negara-negara Asia Pasifik mengadakan pelatihan dalam menghadapi *cyber crime* di Jakarta (www.itu.int, 2015).

Dalam upaya untuk meningkatkan pengetahuan negara Indonesia dalam menangani *cyber crime*, ITU bekerja sama dengan IMPACT dan INTERPOL (*International Criminal Police Organization*) dalam mengadakan workshop di Malaysia pada 19-21 Februari 2014 dengan fokus utama negara-negara di Asia Tenggara termasuk Indonesia. Workshop ini diadakan dalam rangka bekerja bersama untuk mengatasi permasalahan investigasi internet tingkat tinggi dan teknik dalam merespon *cyber crime*, bersamaan dengan memperkuat hubungan kerja sama antara penegak hukum dengan komunitas CERT (*Computer Emergency Response Team*) di negara Asia Tenggara (www.itu.int, 2015).

INTERPOL merupakan suatu organisasi yang terbentuk untuk mengkoordinasikan kerja sama antar kepolisian di seluruh dunia (www.interpol.int, 2015). Terbentuknya INTERPOL tidak terlepas dari adanya persamaan kepentingan negara-negara di dunia dalam memberantas kejahatan internasional dan transnasional yang secara resmi berdiri tahun 1923 berdasarkan kongres polisi reserse internasional di Monaco tahun 1914, salah satu alasan utama diperlukan adanya kerja sama ini juga dikarenakan perkembangan teknologi yang mengakibatkan dampak signifikan dalam kehidupan internasional berupa meningkatnya kejahatan internasional dan transnasional yang memberikan kesulitan bagi penegak hukum yang bersifat yuridis maupun prosedur sehingga kehadiran INTERPOL menjadi penting dalam mengatasi *cyber crime* karena aparat hukum suatu negara dalam menegakkan hukum dibatasi oleh suatu wilayah berdaulat dengan yurisdiksi hukum yang dimilikinya, sementara di sisi lain para pelaku kejahatan dapat melakukan kejahatan lintas-batas negara tanpa adanya yurisdiksi hukum yang jelas (Divhubinter, 2012).

Berfokus pada kebijakan dan regulasi nasional, pada 16-17 Desember 2014 ITU bersama ASEAN mengadakan forum menangani Sosial Media di Jakarta yang menghadirkan Menteri Komunikasi dan Informatika, Komisi Multimedia dan Komunikasi Malaysia. Pertemuan ini bertujuan untuk berbagi kebijakan, penerapan, isu dan tantangan yang akan dihadapi oleh negara-negara ASEAN dalam sosial media; pertukaran pandangan mengenai regulasi ICT dalam menghadapi ancaman sosial media; meneliti kemungkinan yang akan terjadi dalam menerapkan kebijakan mengenai sosial media di ASEAN (www.itu.int, 2015).

Refleksi Peran “ITU di Tengah Peningkatan Cyber Crime di Indonesia

Berdasarkan pada pembagian tugas yang berada dalam ITU, *area office* ITU di Asia Pasifik berpusat pada proyek dan perencanaan regional untuk pengembangan wilayah-wilayah yang telah diprioritaskan. Hal tersebut meliputi peran ITU dalam mengatasi kebutuhan negara-negara berkembang dan pulau-pulau kecil dalam mendapatkan infrastruktur ICT agar setara dengan negara maju; mendampingi negara-negara anggota dalam segala upaya yang berhubungan dengan jaringan telekomunikasi; memberikan fasilitas guna kelancaran negara-negara anggota yang berada dalam masa transisi dari analog ke model digital serta memaksimalkannya; memfasilitasi pengembangan infrastruktur *broadband* yang berada di wilayah akses perkotaan maupun pedesaan; dan memberikan kerangka kerja dalam rangka penguatan regulasi nasional (www.itu.int, 2016).

Clive Archer dalam sebuah bukunya yang berjudul *International Organizations* mengutarakan peran sebuah organisasi internasional bagi negara terbagi menjadi tiga aspek, antara lain instrumen, arena, dan aktor (Archer, 1983:136 – 137). Organisasi internasional seperti IGO (*intergovernmental organization*) memiliki sesuatu yang dapat mempengaruhi kebijakan nasional suatu negara, dalam beberapa hal kebijakan pemerintah

masing-masing negara didasari oleh keputusan dan diplomasi dari sejumlah negara-negara yang berbeda melalui wadah konferensi yang diadakan dalam organisasi internasional. Ketika sebuah organisasi antar pemerintahan atau IGO telah menyepakati suatu keputusan dan mengaturnya, secara tidak langsung telah menyiratkan kepada seluruh negara-negara anggota untuk memiliki tujuan dan keinginan yang sama akan hal tersebut. Dilihat dari dinamika yang terjadi dalam pengambilan kebijakan nasional ini, maka organisasi internasional menjadi sangatlah penting sebagai acuan dasar pemerintah nasional dalam membuat sebuah keputusan berdasarkan koordinasi multinasional yang secara berkelanjutan terjadi di lingkungan IGO (Myrdal, 1955: 4-5).

Upaya pertama yang dilakukan ITU untuk dapat membantu dalam mengembangkan dan mengamankan ICT di Indonesia adalah dengan melalui sebuah instrumen atau perantara yang dapat menjembatani ITU sebagai organisasi internasional dengan Indonesia sebagai sebuah negara berdaulat. Organisasi internasional tidak mungkin dapat melakukan sebuah pergerakan tanpa melalui sebuah instrumen. Sebagai tempat berkoordinasi dan berdiskusi, ITU bekerjasama melalui sebuah lembaga pemerintahan yang berfokus atau ditugaskan pada sektor telekomunikasi dan informatika. Di Indonesia lembaga yang sesuai dengan bidang tersebut dan berhubungan secara langsung dengan Pemerintah Indonesia adalah Kemkominfo (Kementerian Komunikasi dan Informatika). Sebagai kementerian yang bergerak dalam sektor komunikasi dan informatika, Kemkominfo aktif dalam mengeluarkan produk hukum terutama pada periode 2011 – 2013 yang didapati sebagai tahun dengan tingkat kejahatan *cyber crime* tertinggi di Indonesia.

Upaya yang selanjutnya dilakukan ITU setelah berkoordinasi dengan Kemkominfo sebagai instrumen adalah menyediakan sebuah arena atau wadah untuk melakukan kegiatan yang mendukung perkembangan dan pengamanan ICT di Indonesia. Setelah Indonesia menandatangani dan meratifikasi perjanjian penggabungan ITU sebagai organisasi internasional yang berada di bawah naungan PBB, pada tahun 1984 ITU membentuk kantor cabang di Indonesia dengan status sebagai kantor area cabang dari ITU di Thailand yang berfokus pada penanganan perkembangan dan pengamanan ICT di wilayah Asia Tenggara. Langkah ini merupakan salah satu bagian yang memperlihatkan peran ITU di suatu wilayah melalui bentuk fisik kantor areanya di wilayah Asia Tenggara. Melalui berbagai kegiatan seperti seminar, pelatihan dan forum yang telah dibahas di bab II penelitian ini, ITU mulai melakukan beberapa langkah taktis dalam mengembangkan dan mengamankan ICT dengan Pemerintah Indonesia. Hal ini dapat dilihat pada akhir tahun 2014 Pemerintah Indonesia bersama dengan negara-negara anggota ASEAN dan ITU mengadakan sebuah forum pembahasan menangani penanganan sosial media yang diselenggarakan di Jakarta.

Upaya terakhir, adalah dengan memberikan kontribusi secara analisa dan penelitian yang kemudian dilaporkan mengenai kebutuhan negara Indonesia dalam proses pengembangan dan pengamanan di sektor Teknologi dan Informatika sebagai bentuk upaya ITU untuk berperan sebagai organisasi internasional yang memiliki fokus di sektor tersebut, laporan diawali dengan penjabaran kualitas dari sarana dan infrastruktur Indonesia dalam sektor *cybersecurity* untuk kemudian dijadikan dasar pemikiran bagi Pemerintah dalam mengambil langkah pengembangan selanjutnya.

Guna mengukur hal tersebut di atas, ITU menjabarkan ke dalam lima bagian penting pendukung *cybersecurity* di tingkat nasional, antara lain regulasi nasional, langkah operasional, struktur pendukung, *capacity building*, dan kerja sama (ITU, 2014: 1-3). Dalam hal regulasi nasional, Indonesia memiliki dasar Undang-Undang No. 11 Tahun 2008 mengenai Alat Transaksi dan Informatika sebagai dasar aturan mengenai *cyber crime*, Peraturan Pemerintah No. 80 Tahun 2012 mengenai Implementasi Sistem Transaksi Elektronik, dan sistem pengaturan keamanan informasi pada tahun 2013.

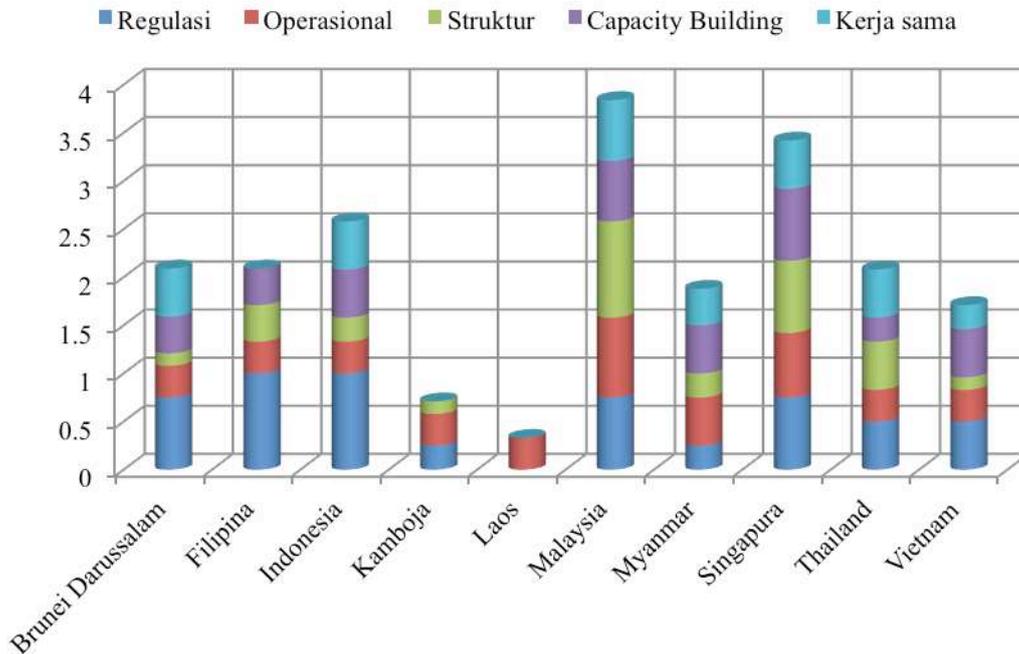
Sementara itu, dalam hal langkah operasional, ITU melihat potensi Indonesia memiliki tim khusus dalam CIRT (*Computer Incident Response Team*) yang bertugas untuk menyelidiki dan menyelesaikan insiden keamanan komputer nasional (www.ucsd.edu, 2016). Pertama, Gov-CSIRT (*Government Computer Security Incident Response Team*), yang berfungsi sebagai pusat pengawasan dan penanganan insiden keamanan informasi milik instansi atau lembaga pemerintah Indonesia (www.govscirt.kominfo.go.id, 2016). Kedua, ID-SIRTII (*Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center*) yang didirikan sebagai langkah pemerintah dalam meningkatkan pertumbuhan internet di Indonesia melalui upaya kampanye kesadaran terhadap pengamanan dan sistem informasi, mengawasi potensi insiden keamanan, mendukung penegakan hukum, serta menyediakan dukungan secara teknis (www.idsirtii.or.id, 2016). Selain itu, Indonesia juga memiliki Akademi CERT (*Computer Emergency Response Team*) sebagai organisasi yang bekerja sama dengan universitas di Indonesia yang berfokus pada pengembangan keamanan teknologi informatika di Indonesia yang kegiatannya meliputi penelitian dan pelatihan (www.acad-csirt.or.id, 2016). Terakhir, adalah ID-CERT (*Indonesia Computer Emergency Response Team*), sebagai tim koordinasi teknis Indonesia terkait insiden internet di seluruh dunia

Sedangkan untuk struktur pendukung, Indonesia dapat dinilai belum memiliki strategi domestik khusus menangani *cybersecurity*, yang kemudian mempengaruhi sektor *capacity building* seperti pengembangan standarisasi IT, pengembangan sumber tenaga ahli dan tenaga profesional di Indonesia.

Sektor terakhir yang dinilai oleh ITU dalam mendukung *cybersecurity* di Indonesia adalah sektor kerja sama. Indonesia memiliki kerja sama dengan NISC (*National Information Security Council*) Jepang guna memfasilitasi aset keamanan *cyber* (www.nisc.go.jp, 2016), dan juga menjadi negara anggota dalam kerja sama ITU – IMPACT menangani *cybersecurity*.

Semua hasil analisa ini menempatkan Indonesia di posisi ke-3 di antara negara-negara ASEAN berdasarkan pada hasil survei GCI (*Global Cybersecurity Index*) Score. Penilaian dilihat dari aset per sektor tiap-tiap negara yang dinilai berdasarkan 0 untuk yang tidak ada dan 1 untuk yang dinilai paling maksimal memanfaatkan sektor tersebut. Adapun grafik GCI Score negara-negara di Asia Tenggara adalah sebagai berikut:

Grafik 2
GCI Score Negara Asia Tenggara

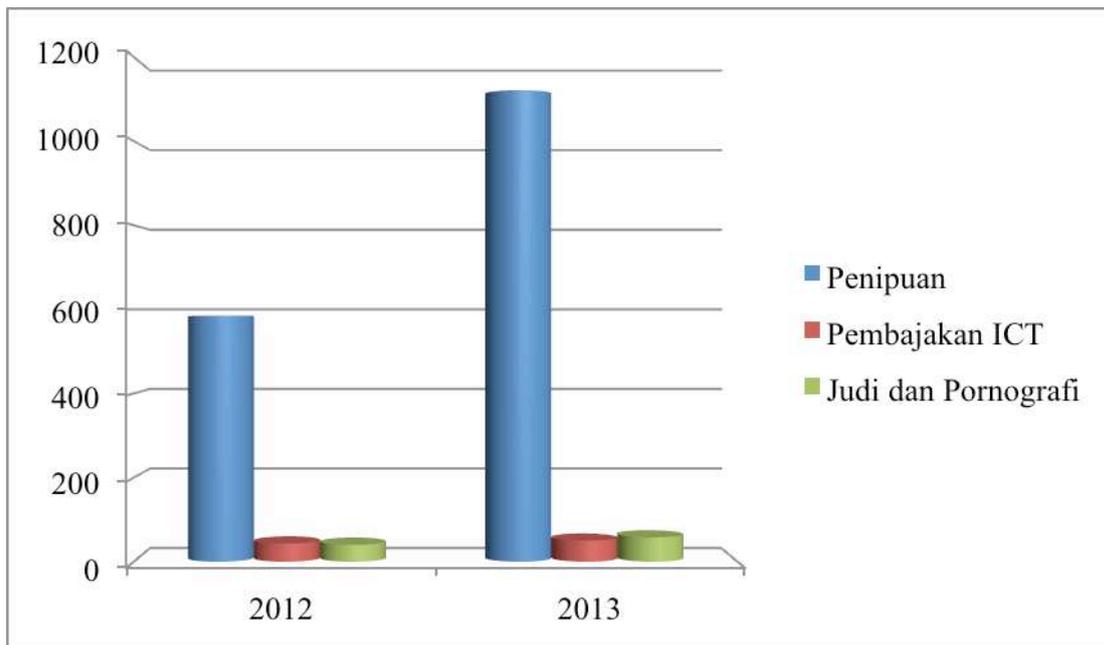


Kerja sama	0.5	0	0.5	0	0	0.63	0.38	0.5	0.5	0.25
Capacity Building	0.38	0.38	0.5	0	0	0.63	0.5	0.75	0.5	0.5
Struktur	0.13	0.38	0.25	0.13	0	1	0.25	0.75	0.5	0.13
Operasional	0.33	0.33	0.33	0.33	0.33	0.83	0.5	0.67	0.33	0.33
Regulasi	0.75	1	1	0.25	0	0.75	0.25	0.75	0.5	0.5

Sumber: diolah dari itu.int, 2015.

Berdasarkan beberapa data dan analisa di atas mengenai langkah yang dilakukan ITU di Indonesia, dapat dikatakan bahwa ITU telah berperan dengan menjalankan upayanya mengatasi perkembangan maupun peningkatan *cyber crime* di wilayah Indonesia. Tetapi, mengacu pada data yang dilaporkan oleh BARESKRIM (Badan Reserse Kriminal) Polisi Republik Indonesia divisi pidana ekonomi khusus bidang *cyber crime* pada tahun 2012 – 2013, aktivitas kejahatan tersebut belum mengalami penurunan, seperti yang dapat dilihat pada tabel berikut:

Grafik 3
Jumlah *Cyber Crime* di Indonesia Tahun 2012 -2013



Sumber: diolah dari data Badan Reserse Kriminal dirpidexsus *cyber crime* Polri mengenai jumlah kejahatan dunia maya di Indonesia tahun 2012 – 2013.

Berdasarkan dari tabel di atas, jumlah *cyber crime* di Indonesia pada tahun 2012 – 2013 belum mengalami penurunan. Sebaliknya, jumlah aktivitas kejahatan dunia maya mengalami peningkatan yang besar dibandingkan tahun sebelumnya. Meskipun ITU telah berperan dengan melakukan berbagai upaya dalam mengembangkan dan mengamankan ICT di Indonesia melalui langkah-langkah yang telah dijelaskan di atas, namun pada kenyataannya terdapat faktor lain yang dapat memberikan pengaruh dan menjadi hambatan bagi peran ITU dalam mengatasi *cyber crime* di Indonesia.

Hambatan ITU dalam Mengembangkan ICT dan Mengatasi Cyber Crime di Indonesia

Direktur *South East Asia and the Pacific Multidisciplinary Advisory Team*, W. R. Bohning dalam sebuah artikelnya mengenai “*The Role and Functions of International Organizations in the Field of Migrant Workers*” mengatakan bahwa peran dari organisasi internasional dapat dilihat berdasarkan kepentingan dari negara-negara anggota. Negara bekerjasama dan masuk dalam organisasi internasional untuk mencapai tujuan yang tidak dapat dicapai oleh negara tersebut, begitu juga jika negara tidak menginginkan adanya intervensi dari luar maka organisasi internasional tersebut tidak akan memiliki izin untuk melakukan sesuatu dalam negaranya. Pendapat tersebut didukung oleh pernyataan Dag Hammarskjold mengenai organisasi internasional adalah bentuk negosiasi multilateral baru yang digunakan sebagai alat untuk berpolitik, instrumen pemerintah nasional, dan menjadi sebuah teknik baru dalam berdiplomasi (Cordier & Foote, 1972: 661).

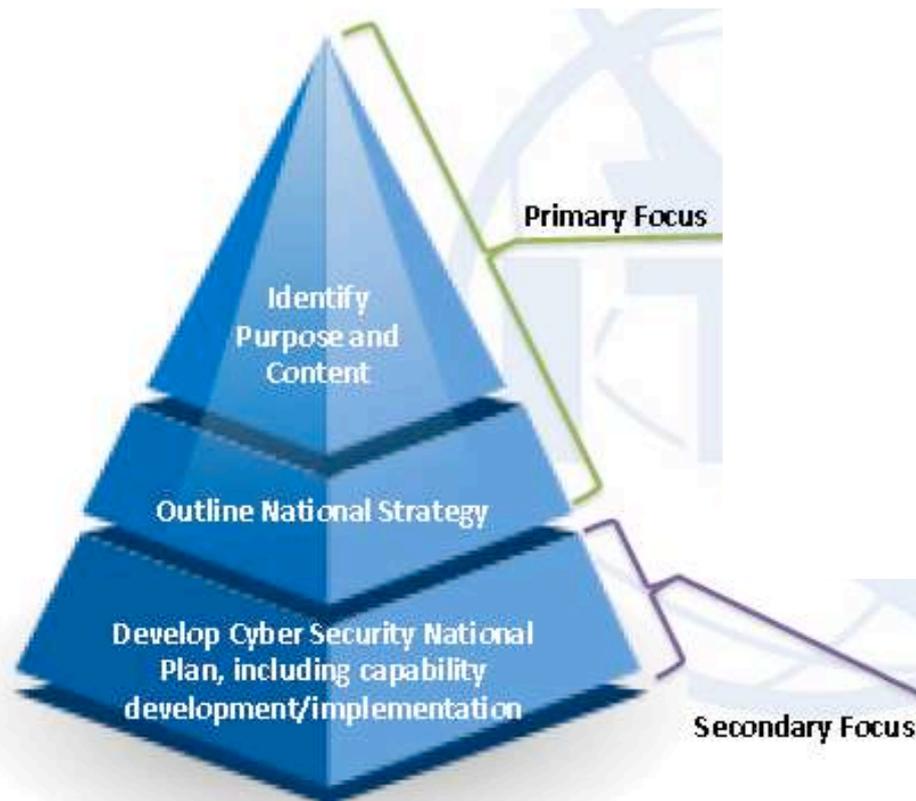
Pernyataan di atas mencoba untuk memperlihatkan bahwasanya organisasi internasional seperti ITU hanya dianggap sebagai sebuah alat politik yang digunakan oleh negara-negara dalam beradu diplomasi guna memasukan kepentingannya sebagai kepentingan bersama. Kepentingan negara-negara menciptakan suatu rangkaian tindakan, dan keberhasilan negara diukur dari bagaimana negara dapat memelihara dan memperkuat negaranya dengan memanfaatkan organisasi internasional sebagai alat (Waltz, 1979: 117). Sebuah alat hanya dapat bergerak jika terdapat subyek lain yang menggerakkannya, begitu

juga dengan ITU yang tidak dapat melakukan apapun tanpa adanya kekuatan absolut yang mendukungnya yaitu negara.

Dalam melakukan perannya di Indonesia, ITU membutuhkan kesediaan dari Pemerintah nasional untuk menjalankan dan bersama-sama mencapai tujuan. Pada tahun periode 2010 – 2014, Kemkominfo Republik Indonesia memiliki program prioritas yang dirasa sangat diperlukan oleh masyarakat Indonesia dalam sektor telekomunikasi saat itu, yaitu: program pengelolaan sumber daya dan perangkat pos dan informatika; program penyelenggaraan pos dan informatika; program pengembangan aplikasi informatika; program pengembangan informasi dan komunikasi publik; dan program penelitian dan pengembangan sumber daya manusia kominfo (Menkominfo, 2010: 29 – 33).

Pemilihan program prioritas ini juga menentukan hubungan antara Indonesia dengan ITU, dimana Indonesia pada periode tersebut memprioritaskan pengembangan ICT di bidang sumber daya, perangkat pos dan informatika, dan komunikasi publik. Sedangkan ITU lebih berfokus pada pengelolaan risiko keamanan informasi dan kerangka kerja keamanan informasi. ITU telah merencanakan kerangka kerja terkait keamanan informasi yang bisa diterapkan dalam keamanan nasional. Adapun rancangannya disebut dengan *NCS (National Cybersecurity Strategy) Toolkit*, yang secara sederhana dapat dilihat pada gambar di bawah ini:

Gambar 1
Proses NCS Toolkit



Sumber: www.itu.int, 2015.

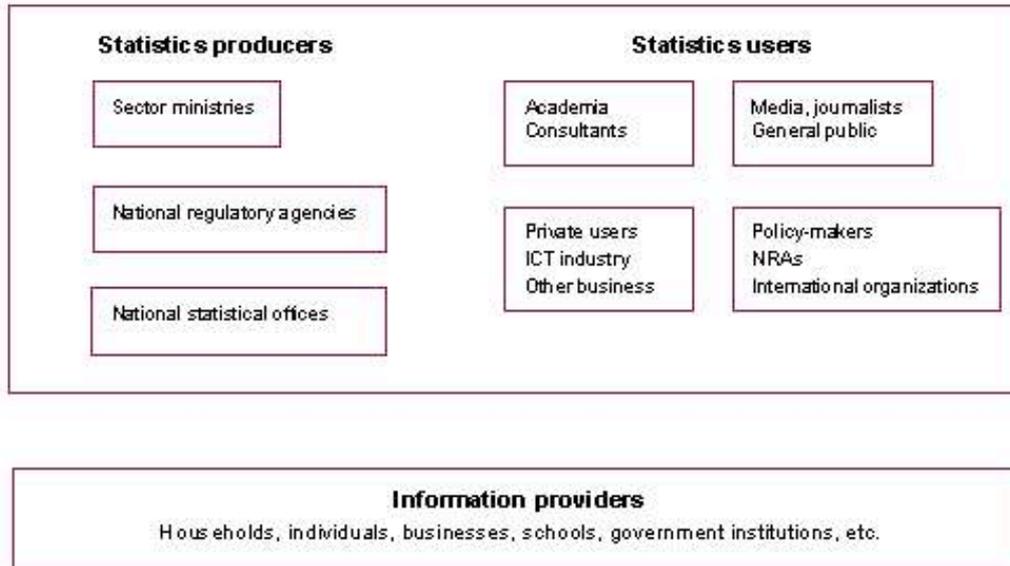
Fokus utama dalam *NCS Toolkit* adalah mengembangkan kebijakan nasional, dengan sarana mengevaluasi status negara saat ini serta mengidentifikasi area yang diharuskan melakukan perbaikan berdasarkan identifikasi tujuan dan isi dari strategi keamanan nasional, pemetaan daerah strategis kemanan nasional, proses manajemen siklus hidup untuk menerapkan pelaksanaan strategi, menetapkan proses terstruktur dalam

mengembangkan strategi dan menambah sumber daya untuk mendukung pengembangan strategi keamanan. Hal yang menjadi rancangan di atas merupakan kegiatan dan rencana yang hanya bisa terealisasi jika dilaksanakan oleh pemerintah nasional sebagai dasar acuan dalam melakukan kebijakan domestik. Keterbatasan ITU sebagai organisasi internasional dalam melakukan upaya pengembangan *cybersecurity* di wilayah kedaulatan Indonesia menjadi sebuah hambatan bagi kegiatan yang telah dirancang dalam sebuah konferensi.

Di sisi lain, intitusional anarki menjadikan kehadiran sebuah organisasi internasional dalam wilayah kedaulatan Indonesia sebagai sebuah ancaman bagi pemerintah, ketika negara yang tidak memiliki otoritas tertinggi dalam tatanan internasional didorong untuk aktif dalam kegiatan organisasi internasional yang secara praktis tidak memiliki kepentingan dan semangat yang sama untuk membangun negara tersebut (Baylis 2005: 304).

Organisasi internasional seperti ITU tidak bisa melepas karakteristik utamanya yang didirikan sebagai perwakilan dari aspirasi kolektif pemerintah negara-negara di dunia, dan disanalah letak keterbatasan kekuatannya. ITU dapat memberikan masukan, mempengaruhi kebijakan domestik dan merespon kegiatan nasional secara langsung, namun hal itu hanya terjadi disaat ITU mendapat persetujuan dari negara (Myrdal 1955: 23). ITU juga tidak dapat dilepas dari kepentingan kolektif untuk membangun dunia yang lebih baik, tujuan ini semua dipengaruhi oleh *stakeholder*, pemberi investasi, dan hasil dari konferensi. Dalam konteks domestik, terdapat tiga bagian *stakeholders* yang terlibat dalam sistem statistik ICT, yaitu:

Tabel 1
Pembagian *Stakeholders* dalam *ICT Statistics System*



Sumber: ITU, 2014, *Manual for Measuring ICT Access and Use by Households and Individuals*, Geneva, Switzerland, hal 16.

Jika melihat tabel di atas, tiga bagian dari *stakeholders* dibagi menjadi: Pemberi Data/Produsen Data yang didalamnya termasuk NSO (*national stastical offices*), kementerian nasional di sektor telekomunikasi dan sumber lain yang berasal dari perusahaan swasta, universitas, dan pusat penelitian lainnya; pengguna data yang termasuk pembuat kebijakan dari kementerian nasional sektor telekomunikasi, media, akademisi, industri ICT, perusahaan swasta, organisasi internasional, dan individu; yang terakhir

adalah responden/penyedia data yang terdiri dari individu, institusi pemerintahan, akademi, dan lain-lain (ITU, 2014: 16).

Secara umum, negara masih melihat organisasi internasional sebagai pola baru pembagian kekuasaan dalam sistem internasional dan regional (Hobson, 2000: 38). Sehingga, kehadiran ITU di wilayah ASEAN secara umum, dan di Indonesia secara khusus, seperti memberikan sebagian wilayah yurisdiksi kepada negara lain secara tidak langsung. Baylis dalam bukunya *The Globalization of World Politics: An Introduction to International Relations* mengingatkan pada sistem internasional yang anarki membuat negara-negara untuk memilih bekerjasama sebagai opsi terbaik dalam menjamin keamanan dan kepentingan nasionalnya (Baylis, 2005: 305), begitu pula dengan Indonesia yang memilih untuk bekerjasama dengan ITU.

3. Kesimpulan

Peran ITU dapat dilihat dari bagaimana mereka bekerjasama dengan Pemerintah Indonesia, melalui Kemkominfo, sebagai jembatan dalam berkoordinasi untuk mengembangkan dan mengamankan ICT (*Information Communication Technologies*) di Indonesia. ITU juga melakukan langkah-langkah operasional, seperti membuka cabang di wilayah Jakarta, mengadakan forum diskusi, pelatihan, dan konferensi untuk mengumpulkan informasi dan berbagi pengalaman dengan negara-negara lain guna meningkatkan kualitas sumber daya manusia dan pengetahuan Pemerintah Indonesia mengenai perkembangan ICT di dunia. Lebih lanjut, ITU secara rutin melakukan survei dan penelitian terkait proses pengembangan dan mengevaluasi kekurangan Pemerintah Indonesia dalam setiap proses yang dilakukan oleh Pemerintah di sektor Teknologi dan Informatika.

Upaya yang dilakukan ITU pada kenyataannya belum memberikan dampak positif bagi keamanan ICT di Indonesia, setelah melihat peningkatan yang terjadi pada aktivitas kejahatan dunia maya tahun 2011 – 2013. Peneliti melihat adanya faktor yang menjadi sebuah hambatan. Pertama, Pemerintah Indonesia tidak dapat mengambil kebijakan dalam negerinya sesuai dengan apa yang telah dianalisa dan dievaluasi oleh ITU. Hal ini dikarenakan Pemerintah tidak sepenuhnya dapat bergantung dan menjadikan ITU sebagai bahan acuan dasar tunggal dalam mengambil sebuah kebijakan, mengingat ITU adalah organisasi internasional yang membawa kepentingan banyak negara. Kedua, Pemerintah Indonesia sebagai kedaulatan tertinggi tidak memiliki prioritas pada bidang keamanan pada tahun 2011 – 2013. Hal ini menyebabkan segala upaya dan kegiatan yang dilakukan ITU tidak selalu dapat diaplikasikan dan Pemerintah berfokus pada pengelolaan sumber daya, penyelenggaraan, penelitian dan pengembangan.

Daftar Pustaka

Buku

- Archer, Clive., 1983. *International Organizations*. London: George Allen and Unwin.
- Baylis, J; Smith, S., 2005. *The Globalization of World Politics: An Introduction to International relations*. Oxford University Press. Second ed.
- Deibert, Ronald J., 2013, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*, Toronto:McClelland & Stewart/Random House.
- Hobson, John M., 2000. *The State and International Relations*. Cambridge University Press.
- ITU, 2014. *Manual for Measuring ICT Access and Use by Households and Individuals*, Geneva, Switzerland, hal 16.

Nugroho, Dr. Riant., 2014, “*National Security Policy Sebuah Pengantar*”, Cetakan 1, Yogyakarta: Pustaka Pelajar. Hal: 73.

Waltz, Kenneth N., 1979. *Theory of International Politics*. Michigan: Addison Wesley Pub Company.

Jurnal

Cavelty, Myriam Dunn, 2013, “Cyber Security”, *Contemporary Security Studies*, Edisi ke-3, Oxford:Oxford University Press.

Cordier, A.W. & Foote, W., 1972. “Public Papers of the Secretaries-General of the United Nations”, Vol. 2, *Dag Hammarskjold 1953–1956*, London and New York: Columbia University Press.

ITU., 1965, "International Telegraph Conference in Paris, 1865: Signature of the Convention by Twenty Sovereign States Opens Era of International Co-operation." *Telecommunication Journal*, 32(5). Hal: 180-184.

Myrdal, G., 1955. ‘Realities and Illusions in Regard to Intergovernmental Organisations’, *Hobhouse Memorial Lecture 1955*, London: Oxford University Press, 3–28.

Website

Gov-CSIRT, 2012. *Government Computer Security Incident Response Team: Tentang Kami* . [Online]. govcsirt.kominfo.go.id [Diakses 27 Februari 2016].

Id-SIRTII/CC, 2013. *Id-SIRTII/CC: Tentang Id-SIRTII/CC*. [Online]. www.idsirtii.or.id [Diakses 27 Februari 2016].

IMPACT, 2011. *IMPACT Alliance*. [Online] Available at: www.itu.int [Diakses 25 Maret 2015].

Internet World Stats, 2014. *Internet World Stats: Internet User in The World*. [Online] Available at: www.internetworldstats.com [Diakses 18 Maret 2015].

ITU, 2015. *International Telecommunication Union: Discover ITU's History*. [Online] Available at: itu.int/go [Diakses 18 Maret 2015].

ITU, 2015. *International Telecommunication Union: Regional Presence*. [Online] Available at: www.itu.int [Diakses 18 Maret 2015].

ITU, 2015. *International Telecommunication Union: Partnership*. [Online] Available at: www.itu.int/en/ITU [Diakses 25 Maret 2015].

ITU, 2015. *International Telecommunication Union: Cyberthreat Insight*. [Online] Available at: www.itu.int [Diakses 25 Maret 2015].

ITU, 2015. *International Telecommunication Union: Abuse Watch Alerting & Reporting Engine*. [Online] Available at: www.itu.int [Diakses 25 Maret 2015].

ITU, 2015. *International Telecommunication Union: Honeypot Research Network*. [Online] www.itu.int [Diakses 25 Maret 2015].

ITU, 2015. *International Telecommunication Union: Telephone and Telephone Conferences*. [Online]. http://www.itu.int/ [Diakses 25 Maret 2015]

KOMINFO, 2013. *Kementerian Komunikasi dan Informatika Republik Indonesia: Indeks Keamanan Informasi*. [Online]. kominfo.go.id/ [Diakses 27 Februari 2016].

NISC, 2015. *National center of Incident readiness and Strategy for Cybersecurity: Contents*. [Online]. http://www.nisc.go.jp/eng/ [Diakses 27 Februari 2016].