eJournal Ilmu Hubungan Internasional, 2018, 6 (3) 1299-1312
ISSN 2477-2623 (online), ISSN 2477-2615 (print), ejournal.hi.fisip-unmul.ac.id

KEBIJAKAN PEMERINTAH INDONESIA DALAM MENANGANI *HACKER* DI INDONESIATAHUN 2008-2014

Dicky Efraim Simanungkalit[1]
Nim. 1202045051

Abstract

Internet have some positive function, where time and space are not problem to doing communication. But internet have negative side too, where people with capability in technology use it to gain profit for theirself and it can becomes hacker, which is one of cybercrime act.This study aims to explain the policy of Indonesian government to handle hacker case in 2008-2014. The type of research is descriptive, tehnicque of data analyze is qualitative and use secondary data sourcedfrom internet and library research. The problem will be analyzed by cybercrime theory by Serio and Gorkinand policy concept by James P. Lester dan Joseph Stewart Jr. The results indicated that policy of Indonesian Government to solve cybercrime in Indonesia still considered not effective to reduce cybercrime acts that getting more higher. It motivated the government of Indonesia to make the policies which are internal and external policies to face cybercrime acts and those policies has succeed where volume of Indonesia cybercrime acts has decreased and increase theIndonesian cyber police quality.

Keywords: *Indonesian Government Policy, Cybercrime, Indonesian Hacker.*

Pendahuluan

Sejalan dengan perkembangan zaman, kemajuan teknologi juga semakin maju. Teknologi Informasi dan Komunikasi (TIK) berkembang dengan sangat pesat. Perkembangan teknologi informasi itu berpadu dengan media dan komputer, yang kemudian melahirkan piranti baru yang disebut internet.

Internet memiliki beberapa dampak positif, yaitu jarak dan waktu seakan tidak lagi menjadi halangan dalam berkomunikasi. Orang yang berada di pulau yang berbeda bahkan negara yang berbeda kini sudah mampu melakukan komunikasi bahkan mampu ditampilkan secara visual. Setiap orang yang menggunakan teknologi dan terhubung dengan internet dapat dengan mudah mengakses informasi tentang berita yang sedang terjadi di negaranya maupun dari negara lain. Perkembangan internet yang sangat pesat tidak hanya memiliki dampak positif, tapi juga memiliki dampak negatif baik pada penggunanya, maupun bagi orang lain. Penyalahgunaan internet oleh seseorang yang memiliki pengetahuan khusus tentang teknologi komputer dapat menjadi suatu kejahatan dunia maya atau *cybercrime*.

[1]Mahasiswa Program S1 Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Mulawarman Email :dicky_efraim@yahoo.com

Cyber crime dapat mengganggu keamanan internasional, seperti yang dikatakan oleh Richard A. Clarke, seorang jurnalis dan penasehat untuk keamanan *White House* dari tahun 1973 hingga 2003, mengatakan bahwa serangan *cyber* bisa sama berbahaya dengan serangan konvensional. Menurutnya serangan *cyber* bisa memadamkan listrik bagi jutaan orang, yang lebih buruk lagi jika dilakukan terhadap menara *control* pesawat atau fasilitas pembangkit nuklir, serangan *cyber* bisa mengorbankan ribuan nyawa, (Richard A. Clarke, 2010).

Banyaknya kasus *cybercrime* yang terjadi merupakan dampak dari banyaknya para pengguna internet yang semakin mudah untuk mengakses dan mempelajari sebuah informasi dari internet untuk berbuat kejahatan di dunia maya yang berasal dari berbagai sumber.Ketidakmampuan menghadapi era *cyber* dapat menjadi ancaman apabila suatu bangsa dan negara tidak memiliki kapabilitas atau kemampuan untuk memanfaatkan teknologi informasi secara baik, benar dan tepat guna.

Tulisan ini akan menjelaskan bagaimana kebijakan pemerintah Indonesia dalam menangani kasus kejahatan dunia maya tahun 2008-2014.

Kerangka Dasar Teori dan Konsep

Teori Cybercrime

Menurut Serio dan Gorkin, ada beberapa indikator mengapa *cybercrime* terjadi. Pertama, pelajar dari Eropa Timur dan Rusia yang mempunyai kemampuan komputer yang baik, memiliki masalah dalam mencari pekerjaan di negara mereka, karena negara-negara pecahan Uni Soviet tersebut hanya menyediakan sedikit lapangan pekerjaan bagi orang yang memiliki kemampuan komputer.

Kedua, masalah ekonomi, dimana orang yang memiliki kemampuan di bidang komputer tetapi memiliki keterbatasan dana dalam menghidupi dirinya dapat menjadi incaran oleh kelompok kejahatan untuk melakukan kejahatan mereka secara terorganisir dan kelompok tersebut dapat membayar ahli komputer hingga 10 kali lipat dari rata-rata gaji seorang ahli komputer di sebuah perusahaan, yang hanya sekitar 5-7 juta rupiah, apabila aksi kejahatan mereka berhasil dilakukan.

Ketiga, pusat pengaduan kejahatan di Rumania mengatakan bahwa para pelajar yang berbakat dalam ilmu komputer selalu ingin mengeksploitasi sejauh mana mereka mengenal bakat mereka, sehingga mereka menyalurkan bakat mereka menggunakan media *online*, (http://ilmuta.weebly.com/computer-crime/analisis-terjadinya-cybercrime, akses tanggal 7 April 2017).

Sehingga dapat disimpulkan bahwa indikator mengapa *cybercrime* dapat terjadi adalah:

1. Minim lapangan pekerjaan.
2. Kebutuhan ekonomi yang tidak mencukupi.
3. Keinginan untuk mengeksploitasi kemampuan.

Konsep Kebijakan

Menurut James P. Lester dan Joseph Stewart Jr. kebijakan publik memilikibeberapa tahapan proses, (https://www.academia.edu/10176244/proses_perumusan_kebijakan_publik akses tanggal 31 Januari 2017) yakni:

1. Agenda Kebijakan
   Agenda kebijakan merupakan tahap dimana diputuskan masalah yang menjadi perhatian pemerintah untuk dibuat menjadi kebijakan. Pemerintah dihadapkan pada berbagai isu (masalah) yang ada di sekitarnya dan pada saat tertentu isu tersebut menjadi dasar suatu kebijakan publik,(https://www.academia.edu/10176244/proses_perumusan_kebijakan_publik, hal. 10). Agenda setting atau dikenal agenda kebijakan didefinisikan sebagai tuntutan-tuntutan agar para pembuat kebijakan memilih atau merasa terdorong untuk melakukan tindakan tertentu. Tidak semua isu akan masuk ke dalam agenda kebijakan. Isu-isu tersebut harus berkompetisi satu sama lain dan masalah yang dianggap menang akan masuk kedalam agenda kebijakan.

2. Formulasi Kebijakan
   Formulasi merupakan tahap yang terjadi setelah isu diagendakan. Raymond Bauer menyatakan bahwa perumusan kebijakan publik adalah proses transformasi input menjadi output. Proses kebijakan publik bersifat politis karena aktor, kepentingan, dan interaksi antara aktor menjadi fokus utamanya. Hasil yang diharapkan dalam formulasi kebijakan adalah solusi terhadap masalah publik. Formulasi merupakan aktivitas kebijakan yang tidak netral dari politik, sehingga kebijakan yang terbentuk merupakan resultan kompromi politik dari para aktor yang berperan merumuskan kebijakan. Terdapat teori formulasi kebijakan yaitu teori kelembagaan, teori proses, teori kelompok, teori elit, teori rasional, teori inkrementalis, teori permainan, teori pilihan publik, teori sistem, teori demokrasi, (https://www.academia.edu/10176244/proses_perumusan_kebijakan_publik, hal. 18).

3. Implementasi Kebijakan
   Dalam tahap implementasi, isi kebijakan dan akibat-akibatnya mungkin akan mengalami modifikasi dan elaborasi bahkan mungkin akan dinegasikan. Implementasi dapat didefinisikan sebagai proses administrasi dari hukum yang didalamnya tercakup keterlibatan berbagai aktor, organisasi, prosedur, dan teknik yang dilakukan agar kebijakan yang ditetapkan mempunyai akibat, yaitu tercapainya suatu tujuan. Implementasi kebijakan dipahami sebagai suatu proses, output, dan outcome. Implementasi dapat dikonseptualisasikan sebagai proses karena didalamnya terjadi beberapa rangkaian aktivitas yang berkelanjutan, (https://www.academia.edu/10176244/proses_perumusan_kebijakan_publik, hal. 35).

4. Evaluasi Kebijakan
   Sebagian besar ahli kebijakan berpendapat bahwa tahap akhir dari proses kebijakan disebut tahapan evaluasi. Evaluasi digunakan untuk mempelajari tentang hasil yang diperoleh dalam suatu proses untuk dikaitkan dengan pelaksanaannya, mengendalikan tingkah laku dari orang-orang yang

bertanggungjawab terhadap pelaksanaan program, dan mempengaruhi respon dari mereka yang berada diluar lingkungan politik, (https://www.academia.edu/10176244/proses_perumusan_kebijakan_publik, hal. 48).

5. Perubahan Kebijakan
   Setelah evaluasi, tahap berikutnya dalam siklus kebijakan adalah perubahan kebijakan disusul dengan terminasi. Dalam dua tahap ini kebijakan direview dan mungkin akan dihentikan atau mengalami perubahan. Setelah itu siklus kebijakan dimulai dari awal lagi, kebijakan akan direformulasi dan direimplementasi. Konsep perubahan kebijakan menunjuk pada pergantian satu atau lebih kebijakan dengan satu atau lebih kebijakan lain. Perubahan kebijakan dapat terjadi dalam tiga bentuk: perubahan sedikit dari kebijakan yang telah dievaluasi; perubahan statute baru dalam area kebijakan publik tertentu; perubahan drastis dari kebijakan publik sebagai konsekuensi dari munculnya pilihan-pilihan baru, (https://www.academia.edu/10176244/proses_perumusan_kebijakan_publik, hal. 55).

6. Terminasi Kebijakan
   Istilah terminasi kebijakan mengarah pada penghapusan agensi, mengarahkan kembali kebijakan dasar, penghapusan program, penghapusan sebagian (agensi, kebijakan dasar, dan program), dan pengurangan anggaran. Terminasi sebenarnya merupakan fase tersulit dilakukan dalam siklus kebijakan publik, (https://www.academia.edu/10176244/proses_perumusan_kebijakan_publik, hal. 59).

Metodologi Penelitian

Jenis Penelitian yang digunakan adalah penelitian deskriptif. Data yang digunakan menggunakan data sekunder. Metode pengumpulan data yang digunakan secara komprehensif dalam penelitian ini menggunakan *study literature*. Teknik analisa data yang digunakan adalah kualitatif.

Hasil Penelitian

Sebelum tahun 2008, Indonesia masih menggunakan KUHP sebagai hukum positif (hukum yang berlaku) untuk mengadili seseorang yang melakukan tindak kejahatan dunia maya. Dalam penggunaannya, KUHP dirasa belum cukup untuk mengatur sanksi bagi para pelaku tindak kejahatan dunia maya, sehingga dalam upaya menangani kasus-kasus yang terjadi, para penyidik melakukan analogi atau perumpamaan dan persamaaan terhadap pasal-pasal yang ada dalam KUHP. Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu pasal karena melibatkan beberapa perbuatan sekaligus.

Pada tahun 2013, terjadi sebuah kasus kejahatan dunia maya yang melibatkan negara Indonesia dengan Israel. Kasus tersebut dilatarbelakangi oleh rasa solidaritas *hacker* Indonesia kepada negara Palestina yang selalu diinvasi oleh militer Israel, yang membuat hacker Indonesia melakukan peretasan ke situs-situs pemerintahan Israel sebagai bentuk protes atas perlakuan Israel terhadap Palestina. Para *hacker*Indonesia tersebut berharap dengan dilakukannya aksi tersebut Israel mau menghentikan invasi

militernya di negara Palestina, terutama di Jalur Gaza. Tetapi yang terjadi setelahnya merupakan kebalikan dari harapan para *hacker* Indonesia. Para *hacker* Israel justru menyerang balik aksi peretasan yang dilakukan oleh *hacker* Indonesia.

Dalam serangan balasan Israel terhadap Indonesia, selain beberapa situs Indonesia berhasil di *hack*, kerugian lain dari serangan balasan*hacker* Israel menurut Pratama Persadha, ketua CISSReC (*Communication and Information System Security Research Centre*) adalah terjadinya ancaman kedaulatan *cyberspace* Indonesia, dia mengatakan bahwa kedaulatan yang dijaga bukan hanya darat, laut dan udara saja, tetapi saat ini data rahasia, informasi dan komunikasi di negara Indonesia juga harus dijaga agar tidak sampai tersebar ke negara lain. Internet dianggap menjadi wilayah *warfare* (perang) baru antar negara. Isu keamanan data-data Indonesia harus disikapi dengan serius, jangan sampai dengan serangan *cyber*, data strategis negara diambil oleh negara lain, (http://cybermedia.co.id/read/berita/70/badan-cyber-nasional-penjaga-kedaulatan-nkri.html akses tanggal 20 Desember 2016).

Pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika (KOMINFO), menanggapi bahwa aksi apapun yang dilakukan oleh para *hacker* Indonesia terhadap negara lain, termasuk Israel, seperti melakukan peretasan ke situs-situs negara lain, harus segera dihentikan, karena selain akan memperburuk situasi, *hacker* Indonesia juga bisa terjerat Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), (https://kominfo.go.id/content/detail/3500/serang-australia-hacker-indonesia-bisa-dibui/0/sorotan_media akses tanggal 20 September 2017).

Dari pihak pemerintah Israel sendiri mengatakan bahwa meski *Anonymous*dan *hacker* Indonesia mengklaim telah meretas sejumlah situs penting Israel, namun, pemerintah Israel menyatakan belum ada gangguan berarti dan tetap tenang.

Yitzhak Ben Yisrael dari Biro Keamanan Siber Israel mengatakan bahwa sebagian besar peretas gagal melumpuhkan situs penting. Dia mengatakan bahwa, hampir tidak ada kerusakan berarti dan para *hacker* tersebut tidak memiliki kemampuanuntuk merusak infrastruktur vital negara, (http://tekno.kompas.com/read/2013/04/08/15132588/peretas.indonesia.juga.bantu.serang.israel akses tanggal 21 September 2017).

Menurut Annie Machon, mantan agen lembaga keamanan *Military Intelegence*, *Section* 5 (MI5) dari Inggris, serangan yang dilancarkan oleh para *hacker* tersebut bukan berusaha untuk mencuri informasi apa pun. Ia berpendapat, ini hanyalah aksi protes terorganisasi terhadap negara tertentu.

Dalam upaya menghadirkan perangkat hukum yang sesuai untuk menangani kejahatan dunia maya, pemerintah Indonesia mengeluarkan beberapa kebijakan yang dianggap dapat digunakan untuk mengurangi kasus kejahatan dunia maya. Ada kebijakan internal dan juga kebijakan eksternal yang dibuat oleh pemerintah Indonesia.

Kebijakan Internal

Kebijakan internalnya adalah sebagai berikut:

Kebijakan Pemerintah Indonesia Dalam Menangani Kejahatan Dunia Maya

1. Pengesahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Pemerintah Indonesia melalui Kementrian Informasi dan Komunikasi (KOMINFO) mengesahkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) pada tanggal 21 April 2008.

UU ITE sendiri merupakan payung hukum pertama yang khusus mengatur tentang dunia maya (*cyber law*) di Indonesia. Latar belakang adanya UU ITE ini bertujuan untuk menjamin kepastian hukum di bidang informasi dan transaksi elektronik. Jaminan tersebut penting, mengingat perkembangan teknologi informasi telah mengakibatkan perubahan-perubahan di bidang ekonomi dan sosial. Perkembangan teknologi informasi telah memudahkan kita mencari dan mengakses informasi dalam dan melalui sistem komputer serta membantu kita untuk menyebarluaskan atau melakukan pertukaran informasi dengan cepat. Jumlah informasi yang tersedia di internet semakin bertambah dan tidak dipengaruhi oleh perbedaan jarak dan waktu. Perkembangan seperti ini memungkinkan seseorang untuk melakukan kejahatan ataupun kecurangan di dunia maya. Hal ini juga yang mendorong pemerintah untuk membuat hukum di lingkungan *cyber*ini, (Undang-undang tentang infromasi dan transaksi elektronik, 2008).

Komitmen ini juga sebagai suatu bentuk pertanggungjawaban moral pemerintah terhadap masyarakat yang juga perwujudan tugas negara untuk melindungi warga negaranya, sebagaimana tertulis dalam pertimbangan pembentukan UU ITE.

2. Bekerjasama Dengan Lembaga Yang Ada Di Indonesia

Upaya pemerintah Indonesia yang lain dalam menangani kejahatan dunia maya di Indonesia adalah bekerjasama dengan beberapa lembaga di Indonesia yang juga bekerja berlandaskan hukum UU ITE untuk menangani kejahatan dunia maya (*cybercrime*). Beberapa lembaga tersebut ada yang dibentuk oleh pemerintah, namun ada pula yang dibentuk oleh perseorangan atau organisasi.

a. Kementrian Komunikasi dan Informatika Republik Indonesia (KOMINFO)

   Kementerian Komunikasi dan Informatika berperan sebagai regulator, khususnya Direktorat Jenderal Aplikasi Informatika yang memiliki 6 Direktorat, dan juga memiliki Penyidik Pegawai Negeri Sipil untuk menangani kasus-kasus pidana ITE.

   Kementerian Komunikasi dan Informatika mempunyai tugas menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika untuk membantu Presiden dalam menyelenggarakan pemerintahan negara.

Adapun fungsi dari Kementerian Komunikasi dan Informatika, (https://www.kominfo.go.id/tugas-dan-fungsi akses tanggal 20 Juni 2017) yaitu:

1. Perumusan dan penetapan kebijakan di bidang pengelolaan sumber daya dan perangkat pos dan informatika, penyelenggaraan pos dan informatika, penatakelolaan aplikasi informatika, pengelolaan informasi dan komunikasi publik;
2. Pelaksanaan kebijakan di bidang pengelolaan sumber daya dan perangkat pos dan informatika, penyelenggaraan pos dan informatika, penatakelolaan aplikasi informatika, pengelolaan informasi dan komunikasi publik;
3. Pelaksanaan bimbingan teknis dan supervisi atas pelaksanaan pengelolaan sumber daya dan perangkat pos dan informatika, penyelenggaraan pos dan informatika, penatakelolaan aplikasi informatika, pengelolaan informasi dan komunikasi publik;
4. Pelaksanaan penelitian dan pengembangan sumber daya manusia di bidang komunikasi dan informatika;
5. Pelaksanaan dukungan yang bersifat substantif kepada seluruh unsur organisasi di lingkungan Kementerian Komunikasi dan Informatika;
6. Pembinaan dan pemberian dukungan administrasi di lingkungan Kementerian Komunikasi dan Informatika;
7. Pengelolaan barang milik/kekayaan negara yang menjadi tanggung jawab Kementerian Komunikasi dan Informatika;
8. Pengawasan atas pelaksanaan tugas di lingkungan Kementerian Komunikasi dan Informatika

b. Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (Id-SIRTII/CC)

Id-SIRTII/CC sendiri memiliki tugas pokok, yaitu melakukan sosialisasi dengan pihak terkait tentang IT *security* (keamanan sistem informasi), melakukan pemantauan dini, pendeteksian dini, peringatan dini terhadap ancaman jaringan telekomunikasi dari dalam maupun luar negeri khususnya dalam tindakan pengamanan pemanfaatan jaringan, membuat/menjalankan/mengembangkan *database log file* serta statistik keamanan Internet di Indonesia.

Id-SIRTII/CC memberikan bantuan asistensi/pendampingan untuk meningkatkan sistem pengamanan dan keamanan di instansi/lembaga strategis (*critical infrastructure*) di Indonesia dan menjadi sentra koordinasi (*Coordination Center/CC*) tiap inisiatif di dalam dan di luar negeri sekaligus sebagai *single point of contact*. Id-SIRTII/CC juga menyelenggarakan penelitian dan pengembangan di bidang pengamanan teknologi informasi/sistem informasi. Saat ini fasilitas laboratorium yang telah dimiliki antara lain: pusat pelatihan, laboratorium simulasi pengamanan, *digital forensic, malware analysis, data mining* danmenyelenggarakan proyek *content filtering, anti spam*, dll.

Id-SIRTII/CC juga memiliki peran pendukung dalam penegakan hukum khususnya terhadap kejahatan yang memanfaatkan teknologi informasi. Terutama dalam penyajian alat bukti elektronik, Id-SIRTII/CC memiliki fasilitas, keahlian dan prosedur untuk melakukan analisa sehingga dapat menjadikan material alat bukti tersebut bernilai secara hukum. Dalam suatu penyidikan, Id-SIRTII/CC memiliki peran sentral dalam memberikan informasi seputar statistik dan pola serangan (insiden) di dalam lalu lintas internet Indonesia, (http://idsirtii.or.id/halaman/tentang/sejarah-id-sirtii-cc.html akses tanggal 20 Juni 2017).

c. *Indonesia Computer Emergency Response Team* (ID-CERT)
ID-CERT atau *Indonesia Computer Emergency Response Team* adalah tim CERT pertama yang berdiri di Indonesia, pada tahun 1998. ID-CERT merupakan tim koordinasi teknis berbasis komunitas dan untuk komunitas yang bersifat independen.

Pembentukan ID-CERT berdasarkan pertimbangan belum adanya CERT di Indonesia pada saat itu, dan pembentukan ID-CERT juga masih dengan bentuk informal. Setelah Indonesia membentuk ID-CERT, negara-negara di sekitar Indonesia juga mulai mengupayakan pembentukan CERT di negara masing-masing dan hal ini berlanjut ke forum Asia-Pasifik, yang kemudian menjadi cikal-bakal APCERT (*Asia Pacific Computer Emergency Response Team)*.

Peran ID-CERT sebagai fungsi adalahmengkoordinasi teknis terhadap komplain yang diterima dan bersifat reaktif, baik di dalam negeri maupun ke luar negeri.Dengan bentuk yang sekarang, ID-CERT bersikap reaktif (bukan aktif) terhadap kasus yang masuk atau dilaporkan oleh pihak lain. ID-CERT juga tidak memiliki kewenangan untuk menyelidiki kasus secara/hingga tuntas, melainkan hanya menjadi penghubung yang dapat dipercaya, terutama oleh pihak yang melaporkan adanya insiden, (https://www.cert.or.id/tentang-kami/id/ akses tanggal 20 Juni 2017).

d. Unit IV *Cybercrime*, Direktorat Reserse Kriminal Khusus, Badan Reserse Kriminal, Kepolisian Negara Republik Indonesia
Dalam Mabes Polri, penanganan *cybercrime* berada di Direktorat Tindak Pidana Ekonomi Khusus (DIT TIPPID EKSUS) di Subdirektorat IV yang menangani tindak pidana antara lain tindak pidana yang terkait dengan *cybercrime*, tindak pidana informasi dan transaksi elektronik.

Tugas-tugas pokok dari Subdit IV/Bidang *cybercrime*adalah sebagai berikut, (http://www.reskrimsus.metro.polri.go.id/StrukturOrganisasi/StrukturOrganisasi.aspx?Id=6&Menuid=0 akses tanggal 20 Juni 2017):

1. Menyelenggarakan penyelidikan dan penyidikan tindak pidana khusus bidang *cybercrime*yang terjadi di daerah hukum Polda Metro Jaya;
2. Menyelenggarakan pemberkasan dan penyelesaian berkas perkara sesuai dengan ketentuan administrasi penyelidikan dan penyidikan tindak pidana;

3. Menyelenggarakan penerapan manajemen anggaran, serta manajemen penyelidikan dan penyidikan tindak pidana khusus, bidang *cybercrime* yang terjadi di daerah hukum PoldaMetro Jaya;
4. Melaksanakan analisa kasus, isu-isu ekonomi yangmenonjol/meresahkan masyarakat dan tindakan penanganannya, serta pengkajian efektifitas pelaksanaan tugas Subdit *Cybercrime*;
5. Menyelenggarakan pembinaan fungsi dan teknis penyelidikan dan penyidikan tindak pidana *cybercrime*;
6. Melaksanakan tugas-tugas lain yang diperintahkan Dir dan Wadir Reskrimsus Polda Metro Jaya

e. Pengelola Nama Domain Internet Indonesia (PANDI)
PANDI merupakan organisasi nirlaba yang dibentuk pada 29 Desember 2006 oleh Pemerintah Republik Indonesia bersama komunitas internet Indonesia. PANDI dibentuk untuk mengelola nama domain .ID secara profesional, akuntabel, dan transparan sesuai dengan kaidah hukum Republik Indonesia.

PANDI adalah badan hukum berbentuk perkumpulan, beranggotakan individu-individu yang berasal dari *multistakeholder* internet Indonesia. Keanggotaan PANDI mencerminkan keterwakilan dari Pemerintah Republik Indonesia, kalangan akademisi, dan kalangan usaha, (https://pandi.id/profil/tentang-pandi/ akses tanggal 20 Juni 2017).

Adapun tugas dari PANDI, sebagai berikut, (https://pandi.id/profil/tugas-pandi/ akses tanggal 20 Juni 2017):
1. Merumuskan kebijakan di bidang pengelolaan Nama Domain Tingkat Tinggi Indonesia
2. Menyiapkan, mengoperasikan, dan memelihara infrastruktur yang dibutuhkan serta menyediakan sistem elektronik untuk pengelolaan Nama Domain Tingkat Tinggi Indonesia.
3. Menyelenggarakan pendaftaran Nama Domain Tingkat Tinggi Indonesia sesuai dengan ketentuan peraturan perundang-undangan, kepatutan yang berlaku dalam masyarakat, dan prinsip kehati-hatian.

3. Sosialisasi Kepada Masyarakat Tentang Kejahatan Dunia Maya

Selain itu, upaya pemerintah Indonesia lainnya dalam menangani kejahatan dunia maya adalah dengan melakukan sosialisasi kepada masyarakat, agar lebih peduli terhadap kejahatan dunia maya.

Sejak tahun 2008, Kementerian Komunikasi dan Informasi telahmenyelenggarakan sosialisasi berupa seminar dan bimbingan teknis kepada seluruh instansi. Dimana evaluasi ini tidak hanya ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, tetapi sekaligus sebagai perangkat untuk menggambarkan kondisi kesiapan kerangka kerja keamanan informasi pada pimpinan instansi yang dibimbing.

Pendekatan dilakukan melalui sistem manajemen keamanan informasi serta melalui pendekatan teknologi yang cermat dan akurat serta *up to date* agar dapat menutup setiap lubang atau celah bagi penyerangan-penyerangan di dunia maya.Pengamanan Informasi secara teori pada dasarnya ditujukan untuk menjamin integritas informasi, pengamanan kerahasiaan data, ketersediaan informasi, dan pemastian memenuhi peraturan, dan hukum,(https://m.tempo.co/read/news/2013/11/16/072530183/pengguna-teknologi-diajak-peduli-cyber-crime akses tanggal 27 Juli 2017).

Kebijakan Eksternal

Selain kebijakan internal diatas, adapula kebijakan eksternal yang dibuat oleh pemerintah Indonesia untuk menangani kejahatan dunia maya, yaitu:

1. Kerjasama Dengan Australia dan Hongkong

Bentuk usaha lain dari pemerintah Indonesia dalam menangani kejahatan dunia maya adalah melakukan kerjasama dengan menandatangani MoU (*Memorandum of Understanding*) dengan negara lain. Dalam hal ini, dengan negara Australia dan Hongkong.

a. Australia

Perjanjian yang dilakukan dengan negara Australia ini ditandatangani pada tanggal 13 November 2006, yang bertempat di Mataram, Lombok. Ditandatangani oleh Dr. N. Hassan Wirajuda selaku Menteri Luar Negeri Republik Indonesia dan Alexander Downer selaku Menteri Luar Negeri Australia.

Adapun penanganan kasus kejahatan dunia maya tertuang dalam pasal 3 tentang Ruang Lingkup Dan Bentuk Kerjasama, ayat 7 tentang Kerjasama Penegakan Hukum, poin F tentang Kejahatan Dunia Maya, (Perjanjian Antara Republik Indonesia Dan Australia Tentang Kerangka Kerjasama Keamanan, Mataram, Lombok, 2006).

Kegiatan yang dilakukan setelah Mou oleh Indonesia dan Australia adalah didirikannya CCISO (*cyber crime investigations satellite office*) pada tanggal 29 April 2013, yang diresmikan oleh Wakil Kepala Departemen Kepolisian Indonesia, Jenderal Nanan Sukarna (mewakili Kepala Departemen Kepolisian, Jenderal Pol Timur Pradopo) bersama Kepala Kepolisian *Australian Federal Police Commissioner,* Tony Negus. CCISO sendiri telah resmi berdiri di Polda Metro Jaya, Mabes Polri, Polda Medan, Polda Bali dan Polda NTB. Tony Negus juga menjelaskan bahwa Australia akan membantu dalam melengkapi peralatan dan melakukan pelatihan kepada seluruh anggota yang akan bekerja di CCISO Indonesia dan Australia akan menggelontorkan dana sebesar kurang lebih $ 9 juta Australia untuk membantu membangun semuanya, (http://www.plimbi.com/news/84972/indonesia-buka-kantor-cyber-crime-investigations akses tanggal 22 November 2017).

b. Hongkong
Perjanjian berikutnya dengan negara Hongkong, ditandatangani pada tanggal 3 November 2014, yang bertempat di Monako. Ditandatangani oleh Sugeng Priyanto selaku Inspektur Jenderal Polisi Republik Indonesia dan Lo Mung-Hung selaku *Senior Assistant Commissioner Director of Crime and Security Hong Kong Police Force*.

Adapun penanganan kasus kejahatan dunia maya tertuang dalam pasal 2 tentang Tujuan Dan Lingkup Kerjasama, ayat 1 tentang Pencegahan Dan Pemberantasan Kejahatan Internasional, poin D tentang Kejahatan Dunia Maya, (Nota Kesepahaman Antara Kepolisian Negara Republik Indonesia Dan Kepolisian Hong Kong Dalam Pencegahan Dan Penanggulangan Kejahatan Internasional Dan Pengembangan Kapasitas, Monako, 2014).

Pada tahun 2016, Indonesia dan Tiongkok berencana melakukan operasi bersama meliputi simulasi perang *cyber*, respons dan mitigasi perang *cyber*, *monitoring cyber*, manajemen krisis *cyber*, dan perencanaan bagi pemulihan data *center*.

Staf Ahli Desk Ketahanan dan Keamanan Informasi *Cyber* Nasional, Muchlis Ahmady, mengemukakan prinsip kerja sama tersebut bagian dari berbagi pengetahuan karena masalah *cyber* tidak bisa ditangani sendiri-sendiri.

Staf Ahli Desk Ketahanan dan Keamanan Informasi *Cyber* Nasional, Muchlis Ahmady,juga mengatakan pihaknya bersama CAC (*Cyberspace Administration ofChina*) sudah melakukan pertemuan awal pekan ini sebagai pre-MoU (*memorandum of understanding*) terkait dengan pengembangan kapasitas (*capacity building*) bagi SDM *cyberspace*, (https://www.antaranews.com/berita/541577/ri-tiongkok-rintis-kerja-sama-keamanan-cyber akses tanggal 22 November 2017).

2. Melakukan Pelatihan Gabungan Dengan Korea Selatan Untuk Menangani Cybercrime

Upaya penanggulangan dan pencegahaan kejahatan dunia maya telah dimulai dengan dilakukannya pertemuan oleh Badan Pembinaan Hukum Nasional (BPHN) dengan *Korean Institute of Criminology* (*KIC*) dan *United Nation Office on Drugs and Crime* (*UNODC*) yang diadakan pada tanggal 30-31 Oktober 2008 di Seoul, Korea Selatan, (http://www.bphn.go.id/news/2008121213332241/Pencegahan-dan-penanggulangan-kejahatan-Cyber, akses tanggal 7 April 2017).

Dalam pertemuan itu diadakan program pelatihan pencegahan dan penanggulangan kejahatan *cyber* secara *online* yang ditujukan kepada para penegak hukum di Indonesia meliputi jajaran kepolisian, kejaksaan, hakim dan para penyidik tindak pidana di bidang *cyber*.
Cara penanggulangannya dilakukan dengan memperkenalkan sebuah forum Internasional, yaitu *Virtual Forum Against Cybercrime*. Dimana forum tersebut

menyajikan berbagai informasi mengenai *cybercrime*bagi para peneliti dan praktisi hukum dan masyarakat umum serta penyelenggaraan pelatihan *online* bagi penegak hukum untuk menanggulangi dan memberantas kejahatan *cyber*.

Proses pelatihan akan diberikan dengan bentuk silabus dan materi-materi *online* yangdipersiapkan oleh KIC dan UNODC dan akan diterjemahkan kedalam bahasa di negara setempat. Materi *online* meliputi pelatihan tingkat dasar yang terdiri dari 26 pelajaran, menyangkut pengetahuan Teknologi Informasi dan Komunikasi dan regulasi dibidang *cybercrime* dan pelatihan tingkat lanjut yang terdiri dari 119 pelajaran yang menyangkut pengetahuan mengenai *Cybercrime Investigation* (prosedur, teknik dan digital forensik) serta berbagai seminar dengan isu dan topik terkait dengan *cybercrime*.

Kesimpulan

Berdasarkan hasil analisis data yang telah dipaparkan pada bab-bab sebelumnya, dapat disimpulkan bahwa pemerintah Indonesia telah melakukan usaha dan mengeluarkan kebijakan-kebijakan yang dirasa dapat mengurangi dan menangani kasus kejahatan dunia maya dengan membuat beberapa kebijakan, seperti dikeluarkannya kebijakan *cyber law* pertama di Indonesia, dilakukannya kerjasama dengan beberapa lembaga di Indonesia yang bekerja berlandaskan *cyber law*, melakukan pelatihan gabungan dengan negara lain, mensosialisasikan kepada masyarakat agar waspada dan segera melaporkan kepada aparat apabila mengalami atau menyaksikan tindak kejahatan dunia maya dan melakukan MoU dengan negara lain, seperti Australia dan Hongkong.

Namun dengan adanya kebijakan-kebijakan tersebut, kejahatan dunia maya di Indonesia masih belum dapat ditekan, karena beberapa kebijakan masih belum optimal dikarenakan beberapa faktor, diantaranya sosialisasi yang dilakukan oleh pemerintah dan lembaga yang bekerjasama dengan pemerintah tentang kejahatan dunia maya masih kurang giat, sehingga pengetahuan masyarakat tentang bahayanya kejahatan dunia maya atau bahkan menjadi salah satu pelaku dapat dikenai hukuman sesuai dengan undang-undang yang berlaku.

Tidak adanya kebijakan mengenai bagaimana agar para pelaku kejahatan dunia maya tidak harus dipenjarakan, namun dapat dibimbing dan dipekerjakan sebagai salah satu *cyber police* di Indonesia, dibawah pengawasan pemerintah, mengingat SDM Indonesia yang menjadi pasukan *cyber police* sangat sedikit.

Selain itu, ada beberapa hal yang menjadi kendala dalam melakukan penyidikan kasus kejahatan dunia maya, dimana dalam UU ITE yang terdapat pada pasal *43 ayat (5) dan ayat (6), dimana penyidik harus mendapatkan izin dahulu dari Ketua Pengadilan Negeri setempat untuk melakukan penggeledahan atau penangkapan pelaku cybercrime, sedangkan pengadilan negeri hanya buka di hari kerja saja dan berakibat lambatnya penanganan apabila kasus terjadi di akhir pekan dan ditakutkan bukti sempat menghilang.*

Daftar Pustaka

Buku

Richard A. Clarke. 2010. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: HarperCollins Publishers Inc.

Jurnal Online

Indonesia.*Undang-Undang Tentang Informasi dan Transaksi Elektronik*. UU No. 11 Tahun 2008.

Mataram, Lombok. 2006. Perjanjian Antara Republik Indonesia Dan Australia Tentang Kerangka Kerjasama Keamanan.

Monako. 2014. Nota Kesepahaman Antara Kepolisian Negara Republik Indonesia Dan Kepolisian Hong Kong Dalam Pencegahan Dan Penanggulangan Kejahatan Internasional Dan Pengembangan Kapasitas.

Media Online

Analisis Terjadinya Cybercrime dalam situshttp://ilmuta.weebly.com/computer-crime/analisis-terjadinya-cybercrime diakses pada 7 April 2017.

Badan Cyber Nasional, Penjaga Kedaulatan NKRI dalam situshttp://cybermedia.co.id/read/berita/70/badan-cyber-nasional-penjaga-kedaulatan-nkri.htmldiakses pada 20 Desember 2016.

Indonesia Membuka Kantor Cyber Crime Investigations Satellite Office dalam situshttp://www.plimbi.com/news/84972/indonesia-buka-kantor-cyber-crime-investigations diakses pada 22 November 2017.

Pencegahan dan Penanggulangan Kejahatan Cyber dalam situshttp://www.bphn.go.id/news/2008121213332241/Pencegahan-dan-penanggulangan-kejahatan-Cyber diakses pada 7 April 2017.

Pengguna Teknologi Diajak Peduli Cyber Crime dalam situshttps://m.tempo.co/read/news/2013/11/16/072530183/pengguna-teknologi-diajak-peduli-cyber-crime diakses pada 27 Juli 2017.

Peretas Indonesia Juga Bantu Serang Israel dalam situshttp://tekno.kompas.com/read/2013/04/08/15132588/peretas.indonesia.juga.bantu.serang.israeldiakses pada 21 September 2017.

Proses Kebijakan Publik dalam situshttps://www.academia.edu/10176244/proses_perumusan_kebijakan_publikdiakses pada 31 Januari 2017.

RI-Tiongkok Rintis Kerja Sama Keamanan Cyber dalam situs https://www.antaranews.com/berita/541577/ri-tiongkok-rintis-kerja-sama-keamanan-cyber diakses pada 22 November 2017.

Sejarah Id-SIRTII/CC dalam situshttp://idsirtii.or.id/halaman/tentang/sejarah-id-sirtii-cc.html diakses pada 20 Juni 2017.

Serang Australia, Hacker Indonesia Bisa Dibui dalam situshttps://kominfo.go.id/content/detail/3500/serang-australia-hacker-indonesia-bisa-dibui/0/sorotan_mediadiakses pada 20 September 2017.

Tentang Kami dalam situshttps://www.cert.or.id/tentang-kami/id/diakses pada 20 Juni 2017.

Tentang PANDI dalam situshttps://pandi.id/profil/tentang-pandi/ diakses pada 20 Juni 2017.

Tugas & Fungsi Kementerian Komunikasi dan Informatika dalam situshttps://www.kominfo.go.id/tugas-dan-fungsi diakses pada 20 Juni 2017.

Tugas Pokok Subdit IV / Bidang Cyber Crime dalam situshttp://www.reskrimsus.metro.polri.go.id/StrukturOrganisasi/StrukturOrganisasi.aspx?Id=6&Menuid=0 diakses pada 20 Juni 2017.