CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA

Handrini Ardiyanti*

Abstract

Indonesia is reportedly facing a serious cyber-security threat due to the fact that the level of cyber crime in the country has reached critical condition. Unlike in coping with other crimes, to counter cyber-security, a comprehensive solutions should be found out. This paper discusses the ways of how cyber-security in the country has been handling, how its prospect, and new challenges coming from its development today.

Keywords: cyber, cyber crime, cyber-security, defense, Indonesia

Abstrak

Indonesia saat ini tengah dalam keadaan mendesak *cyber-security* atau keamanan dunia maya karena melihat kenyataan bahwa tingkat kejahatan di dunia maya atau *cyber crime* di Indonesia sudah mencapai tahap memprihatinkan. Namun berbeda dengan penanganan kejahatan lainnya, *cyber-security* membutuhkan pemikiran yang komprehensif untuk menanganinya. Karena itu tulisan ini membahas tentang bagaimana kebijakan *cyber-security* yang telah dijalankan di Indonesia selama ini dan bagaimana prospek dan tantangan bagi pengembangan kebijakan *cyber-security* di Indonesia.

Kati Kunci: kejahatan *cyber*, keamanan *cyber*, *cyber-security*, pertahanan, Indonesia

I. PENDAHULUAN

Saat ini dunia tengah berada dalam era informasi yang merupakan tahapan lanjutan dari era prasejarah, era agraris, dan era industri. Pada era informasi, keberadaan suatu informasi mempunyai arti dan peranan yang sangat penting bagi semua aspek kehidupan, serta merupakan salah satu kebutuhan hidup bagi semua orang baik individual maupun organisasi, sehingga dapat dikatakan bahwa dalam masyarakat informasi, informasi telah berfungsi sebagaimana layaknya aliran darah sumber kehidupan bagi tubuh manusia.[1]

Salah satu temuan yang memberikan pengaruh paling besar dalam masyarakat informasi adalah ditemukannya internet. Hadirnya internet sebagai bentuk teknologi baru menyebabkan manusia tidak mampu terlepas dari arus komunikasi dan informasi. Internet telah menyebabkan terjadinya satu lompatan besar dalam kehidupan. Sama halnya dengan teknologi lainnya, internet tidak bebas nilai. Teknologi akan menjadi efektif jika kita memberi perhatian pada kegunaan dari teknologi yang disesuaikan dengan nilai-nilai sosial maupun pribadi serta adanya peraturan pemerintah yang melindungi masyarakat dari dampak negatif yang ditimbulkannya.

Terkait dengan internet terdapat sejumlah konsep yang berhubungan yaitu telematika, multimedia dan *cyber space*. Istilah telematika dikenal sebagai *the new hybrid of technology* yang muncul karena perkembangan teknologi digital yang membuat perkembangan teknologi telekomunikasi dan informatika semakin terpadu atau yang biasa disebut dengan konvergensi. Konvergensi antara teknologi telekomunikasi, media dan informatika tersebut akhirnya mendorong penyelenggaraan sistem elektronik berbasis teknologi digital yang kemudian di kenal dengan istilah *the net*. Konvergensi itu sendiri adalah merupakan gejala yang mengemuka dalam industri jasa Teknologi Informasi Komunikasi (TIK) yang muncul sejalan dengan pesatnya kemajuan teknologi elektronika pada akhir abad 20. Dampak konvergensi secara sosial telah

* Penulis adalah Peneliti Muda Bidang Komunikasi pada Pusat Pengkajian, Pengolahan Data dan Informasi Sekretariat Jenderal DPR RI. Alamat *e-mail*: handrini@gmail.com dan handrini.ardiyanti@dpr.go.id

1 Anne W. Brascomb (ed), Toward A Law of Global Communication Network, New York: Lognman, 1986, hal.1

dirasakan masyarakat baik itu positif maupun negatif.[2] Salah satu dampak negatif yang muncul dalam *cyber-space* adalah terjadinya *cyber crime*. Maraknya *cyber crime* memerlukan perhatian dan keseriusan dalam mengembangkan *cyber-security* bagi sebuah negara termasuk Indonesia.

Perkembangan selanjutnya para praktisi menyebut media dalam telematika tersebut dengan istilah multimedia. Sementara seiring dengan pemakaian jaringan sistem komputer yang mengunakan infrastruktur sistem telekomunikasi maka masyarakat penggunanya kemudian seolah-olah mendapati dunia baru yang dinamakan *cyber space*.[3] Awalan *cyber*, adalah awalan yang dipakai untuk hampir segala sesuatu yang melibatkan komunikasi lewat komputer. *Cyber space* adalah tempat maya dimana komunikasi terjadi. Istilah *cyber-space* diperkenalkan oleh novelis sains-fiksi William Gibson dalam bukunya Neuromancer. Pada saat itu, tahun 1984 dia melihat ada semacam integrasi antar komputer dengan manusia.[4] Berdasarkan data Kementerian Komunikasi dan Informatika (Kemkominfo) pengguna internet di Indonesia hingga saat ini telah mencapai 82 juta orang. Dengan capaian tersebut, Indonesia berada pada peringkat ke-8 di dunia.[5]

Berdasarkan berbagai kejadian pada beberapa tahun ke belakang, Indonesia merupakan negara yang lemah *cyber-security*nya. Hal ini dapat diketahui dari maraknya berbagai kejadian, salah satunya adalah peretasan terhadap data kartu debit nasabah sebuah bank karena *hacker* berusaha menyusup ke sistem pengamanan kartu nasabah bank yang terjadi pertengahan Mei 2014 menjadikan catatan betapa buruknya *cyber-security* di Indonesia.

Satu fakta yang mengejutkan datang dari perusahaan *monitoring internet* Akamai yang mengungkap bahwa kejahatan internet di Indonesia meningkat dua kali lipat. Angka ini menempatkan Indonesia di posisi pertama negara berpotensi menjadi target *hacker*, menggantikan Tiongkok. Dari 175 negara yang diinvestigasi, Indonesia berkonstribusi sebanyak 38 persen dari total sasaran trafik *hacking* di internet. Angka ini meningkat seiring dengan meningkatnya kecepatan internet di Indonesia. Menurut David Belson dari Akamai *Research*, kecepatan internet tidak memiliki hubungan dengan potensi besar kejahatan internet yang mengancam Indonesia. Aksi *hacking* lebih dikarenakan lemahnya sistem keamanan internet dan komputer di Indonesia.[6]

Kerugian yang disebabkan karena tindak kejahatan dengan memanfaatkan maupun di dunia *cyber* di Indonesia menurut data CIA telah mencapai 1,20 % dari tingkat kerugian akibat *cyber crime* yang terjadi di dunia sebagaimana terlihat dalam tabel berikut ini:

Tabel Perkiraan Kerugian Akibat *Cyber crime* di dunia dan Indonesia

	Global	Indonesia
GDP:*	USD 71,620 bn	USD 895 bn
Percent of global GDP*:		1,20 %
Cost of:**		
Genuine cyber crime:	USD 3,457 m	USD 43 m
Transitional Cyber crime:	USD 46,600 m	USD 582 m
Cyber criminal infrastructure:	USD 24,840 m	USD 310 m
Traditional crimes becoming cyber	USD 150,200 m	USD 2,748 m

Sumber: Meeting the cyber-security challenge in Indonesia An analysis of threats and responses A report from DAKA advisory, hal 21[7]

[2] Pusat Teknologi Informasi dan Komunikasi Badan Pengkajian dan Penerapan Teknologi (BPPT), Kajian Konvergensi Teknologi Informasi dan Komunikasi, Jakarta: Pusat Teknologi Informasi dan Komunikasi BPPT, 2007, hal.3

[3] M. Arsyad Sanusi, Hukum Teknologi dan Informasi, Bandung: Tim Kemas Buku, 2005, hal.92-93.

[4] John Vivian, Teori Komunikasi Massa, Jakarta: Kencana, 2008, hal. 264.

[5] Kemkominfo: Pengguna Internet di Indonesia Capai 82 Juta, http://kominfo.go.id/index.php/content/detail/3980/Kemkominfo%3A+Pengguna+Internet+di+Indonesia+Capai+82+Juta/0/berita_satker#.U9G4o5R_tfs, diakses Jumat 24 Juli 2014 pukul 09.00 WIB.

[6] Ketika Hacker Lebih Menakutkan Ketimbang Teroris, Tidak hanya berbahaya bagi keamanan negara, tapi juga ekonomi dunia, *http://m.news.viva.co.id/news/read/507480-ketika-hacker-lebih-menakutkan-ketimbang-teroris,* diakses Kamis, 17 Juli 2014 pukul 11.55 WIB.

[7] *Meeting the cyber security challenge in Indonesia An analysis of threats and responses A report from DAKA advisory* http://dakaadvisory.com/wp-content/uploads/DAKA-Indonesia-cyber-security-2013-web-version.pdf diakses 22 Juli 2014 2014 pukul 13.30 WIB.

Dari tabel perkiraan kerugiaan akibat *cyber crime* yang memperbandingkan antara perkiraan kerugiaan akibat *cyber crime* di Indonesia USD 895 billion yang artinya mencapai 1,20% dari total keseluruhan perkiraan kerugian akibat *cyber crime* secara global mencapai USD 71,620 billion.

Dalam tataran kebijakan, penanganan *cyber crime* berbeda dengan penanganan kejahatan lainnya. Pemerintah umumnya dapat dengan mudah mengendalikan dan menerapkan hukum di dalam wilayah kedaulatan negaranya. Namun tidak demikian terhadap aktifitas-aktifitas *on-line* yang letak atau lokasinya secara fisik dapat berubah sewaktu-waktu, bahkan hanya dapat dibayangkan.[8]

Permasalahannya kemudian, ketika menentukan pilihan hukum dan yuridiksi telah mengakibatkan berbagai pemikiran tentang bagaimana mendekati permasalahan tersebut. Salah satu pemikiran yang timbul adalah menempatkan internet sebagai ruang internasional keempat sama seperti halnya antartika, luar angkasa dan samudera.[9]

II. PERUMUSAN MASALAH

Indonesia sebenarnya saat ini tengah dalam keadaan mendesak *cyber-security* atau keamanan dunia maya karena melihat kenyataan bahwa tingkat kejahatan di dunia maya atau *cyber crime* di Indonesia sudah mencapai tahap memprihatinkan. Namun berbeda dengan penangganan kejahatan lainnya, *cyber-security* membutuhkan pemikiran yang komprehensif untuk menangganinya. Berdasarkan hal tersebut maka permasalahan yang akan dibahas dalam tulisan ini adalah bagaimana kebijakan *cyber-security* yang telah dijalankan di Indonesia selama ini? Bagaimana prospek dan tantangan bagi pengembangan kebijakan *cyber-security* di Indonesia?

III. TUJUAN

Tulisan ini bertujuan:

1. Memperoleh gambaran tentang kebijakan *cyber-security* di Indonesia saat ini.
2. Memetakan prospek pengembangan *cyber-security* di Indonesia dan tantangannya.

IV. KERANGKA PEMIKIRAN

A. Manajemen Teknologi Informasi

Ada 4 (empat) pondasi utama yang mendukung perkembangan teknologi informasi yaitu: perkembangan perangkat lunak (*software)* seperti sistem dan aplikasi dan perkembangan alat keras (*hardware)* perkembangan sarana dan prasarana teknologi informasi, manajemen isi (*content management*), *telecommunication and networking*, perkembangan internet serta perdagangan *online* atau melalui internet.[10]

Sementara untuk pengorganisasian terkait dengan pengunaan sistem teknologi informasi setidaknya ada empat hal utama yang harus diperhatikan yaitu: pertama, sistem informasi (*information systems*) dan kedua, kompetisi organisasi (*organizational competition*); ketiga, *information systems* (sistem informasi) dan *organizational decision making* (sistem informasi dan pengambilan keputusan dalam organisasi); keempat, pengorganisasian penggunaan sistem informasi (*organizational use of information systems*).

Pada dasarnya sistem informasi itu terintegrasi, teknologi informasi dibangun berbasis sistem yang dirancang untuk dapat mendukung kerja, manajemen dan pengambilan keputusan dalam organisasi. Teknologi Informasi Komunikasi (TIK) adalah salah satu komponen paling penting dalam pengembangan sistem informasi.[11]

Pengelolaan sumber daya sistem informasi adalah permasalahan selanjutnya terkait dengan tantangan pengembangan TIK. Ada empat kunci utama yang harus diperhatikan agar pengelolaan sumber daya sistem informasi berhasil yaitu: pertama, bahwa pengelolaan sumber daya sistem informasi haruslah ditempatkan sebagai proses manajemen bisnis. Kedua, Pembangunan sistem

---

8 Elizabeth Longworth, *The Possibilities for legal framework for cyberspace- Including New Zealand Perspective,* Theresa Fuentes et.al (editor), The International Dimesions of Cyberspace Law: Law of Cyberspace Series, Vol.1, Aldershot: Ashgate Publishing Limited, 2000, hal,14.

9 D. Menthe, *Jurudiction in Cyberspace: A Theory of International Space,* Michigan Telecommunications and Technology Law Review, 23 April 1998, hal. 59.

10 Ronald Thompson & William Cats Barril, *Information Technology and Management,* New York: Mc Graw Hill, 2003, hal.29.

11 *Ibid*, hal. 200-203.

informasi. Ketiga, sumber daya *external* sistem informasi. Keempat, manajemen sumber daya informasi.[12]

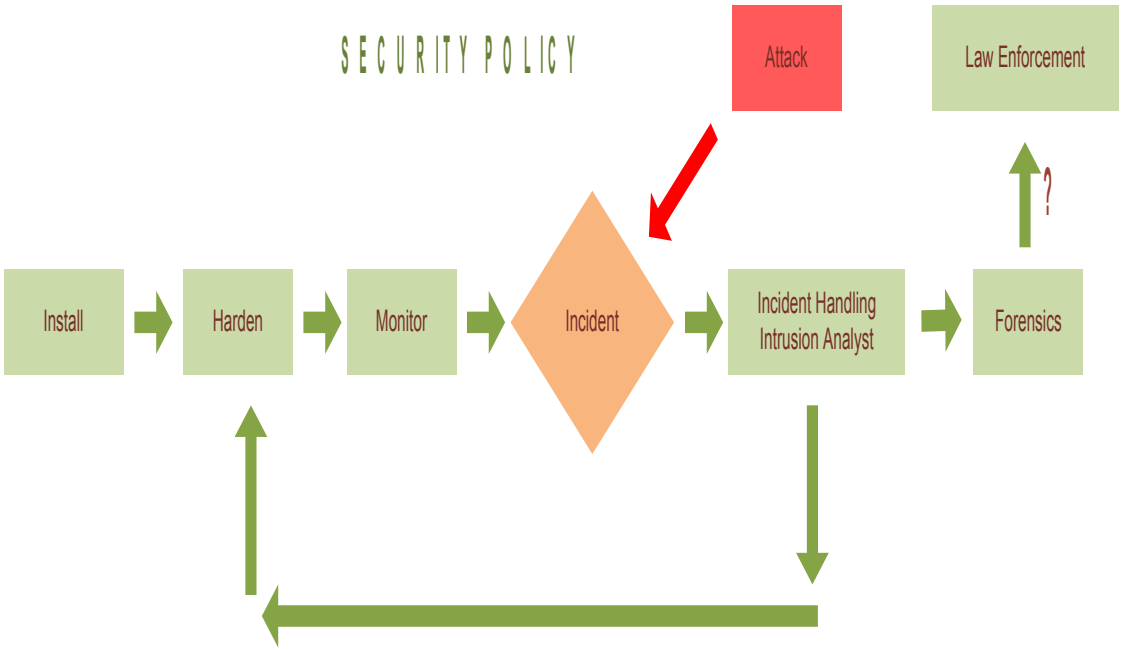
B. *Cyber-security* dan Pertahanan Negara

Cyber-security adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna. Organisasi dan aset pengguna dalam *cyber-security* termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya.

Cyber-security merupakan upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan *cyber*. Tujuan keamanan umum terdiri dari: ketersediaan; Integritas termasuk didalamnya keaslian dan kemungkinan upaya mengurangi terjadinya penolakan serta terakhir kerahasiaan.

Global cyber-security dibangun di atas lima bidang kerja: *Global cyber-security* dibangun di atas lima bidang kerja: Kepastian Hukum (undang-undang *cyber crime*); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *capacity building* dan pendidikan Pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*) (undang-undang *cyber crime*); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *capacity building* dan pendidikan Pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*).[13]

Bagan Ruang Lingkup Kebijakan *Cyber Security*



sumber: *Technology Perscpetive: National Cyber-Security, Universitas Pertahanan Indonesia*

[12] *Ibid*, hal. 339.

[13] Edmon Makarim, *Indonesian Legal Framework for Cybersecurity http://www.nisc.go.jp/security-site/campaign/ajsympo/pdf/lecture2.pdf* diakses Kamis, 17 April 2014 pukul 15. 40 wib.

Dari gambar tersebut dapat diketahui bahwa ruang lingkup *cyber-security* dimulai dari install, harden atau keamanan terkait dengan perangkat keras yang digunakan dalam mengoperasikan internet, monitor, yang menyebabkan terjadinya insiden atau kejadian dan insiden itu dapat pula berasal dari serangan atau *cyber attact* yang membutuhkan penangganan terhadap insiden tersebut dengan melakukan uji forensik sebagai pembuktian dalam penegakan hukum terhadap terjadinya *cyber crime*.

Cyber-security lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Mekanisme ini harus bisa melindungi informasi baik dari *physical attack* maupun *cyber attack*. *Cyber-security* merupakan upaya untuk melindungi informasi dari adanya *cyber attack*, adapun elemen pokok *cyber-security* adalah:

1. Dokumen *security policy* merupakan dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi.
2. *Information infrastructure* merupakan media yang berperan dalam kelangsungan operasi informasi meliputi *hardware* dan *software*. Contohnya adalah *router*, *switch*, *server*, sistem operasi, *database*, dan *website*.
3. *Perimeter Defense* merupakan media yang berperan sebagai komponen pertahanan pada infrastruktur informasi misalnya IDS, IPS, dan *firewall*.
4. *Network Monitoring System* merupakan media yang berperan untuk memonitor kelayakan, utilisasi, dan *performance* infrastruktur informasi.
5. *System Information and Event Management* merupakan media yang berperan dalam memonitor berbagai kejadian di jaringan termasuk kejadian terkait pada insiden keamanan.
6. *Network Security Assessment* merupakan elemen *cyber-security* yang berperan sebagai mekanisme kontrol dan memberikan *measurement level* keamanan informasi.
7. *Human resource* dan *security awareness* berkaitan dengan sumber daya manusia dan *awareness*-nya pada keamanan informasi.

Selain *cyber-security* kelangsungan operasi informasi juga bergantung pada *physical security* yang tentunya berkaitan dengan semua elemen fisikal misalnya bangunan *data center*, *disaster recovery system*, dan media transmisi.[14]

IV. PEMBAHASAN

IV.A. Kebijakan *cyber-security* di Indonesia Saat Ini

IV.A.1. Kepastian Hukum

Kebijakan *cyber-security* secara khusus di Indonesia telah diinisiasi sejak tahun 2007 dengan dikeluarkannya Peraturan Menteri Komunikasi dan Informatika No.26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet yang kemudian direvisi dengan Peraturan Menteri Komunikasi dan Informatika No.16/PER/M.KOMINFO/10/2010 yang kemudian diperbaharui lagi dengan Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMINFO/12/2010. Salah satu yang diatur dalam peraturan tersebut adalah pembentukan ID-SIRTII, yang merupakan kepanjangan dari *Indonesia Security Incident Response Team on Internet Infrastructure* adalah Tim yang ditugaskan Menteri Komunikasi dan Informatika (Kominfo) untuk membantu pengawasan keamanan jaringan telekomunikasi berbasis protokol internet.

Tugas dan fungsi dari ID-SIRTII diantaranya melakukan pemantauan, pendeteksian dini, peringatan dini terhadap ancaman dan gangguan pada jaringan, berkoordinasi dengan pihak-pihak terkiat di dalam maupun luar negeri di dalam menjalankan tugas pengamanan jaringan telekomunikasi berbasis protokol internet, mengoperasikan, memelihara dan mengembangkan sistem *database* sistem ID-SIRTII, menyusun katalog-katalog dan silabus

[14] Indonesian Defense University, *Technology Perscpetive: National Cyber Security*, http://binkorpspelaut.tnial.mil.id/index.php?option=com_docman&task=doc_download&gid=6&Itemid=22. diakses Kamis, 17 April 2014 pukul 15. 40 wib.

yang berkaitan dengan proses pengamanan pemanfaatan jaringan, memberikan layanan informasi atas ancaman dan gangguan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet, menjadi *contact point* dengan lembaga terkait tentang keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet serta menyusun program kerja dalam rangka melaksanakn pekerjaan yang berkaitan dengan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet.[15]

Menurut Hasyim Gautama, kerangka hukum *cyber-security* di Indonesia saat ini dibangun diantaranya berdasarkan atas dasar UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012 serta surat edaran menteri dan peraturan menteri.

Terkait dengan upaya menjamin kepastian hukum dalam pengembangan *cyber-security* telah dilakukan antara lain dengan melaksanakan serangkaian program yang sudah mulai berjalan diantaranya: menginisiasi peraturan perundang-undangan yang terkait dengan *cyber-security* seperti UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012, menyusun kerangka nasional *cyber-security.*

Namun demikian, legalitas penanganan kejahatan di dunia *cyber* masih lemah karena meski telah ada peraturan perundang-undangan yang melarang bentuk penyerangan atau perusakan sistem elektronik dalam UU Informasi dan Transaksi Elektronik No.11 Tahun 2008 namun belum terdapat peraturan perundang-undangan yang mengatur secara khusus *cyber crime* dan penanganan *cyber crime* padahal dilain sisi bentuk kejahatan dunia *cyber* semakin meningkat dan pola kejadiannya sangat cepat sehingga sulit untuk ditangani oleh aparat penegak hukum.

IV.A.2. Teknis Dan Tindakan Prosedural

Secara nasional, menurut Hasyim Gautama terdapat sejumlah permasalah terkait dengan pembangunan *cyber-security* yang tangguh di antaranya:

1. Lemahnya pemahaman penyelenggara negara atan *security* terkait dengan dunia *cyber* yang memerlukan pembatasan pengunaan layanan yang servernya berada di luar negeri dan diperlukan adanya pengunaan *secured system*.
2. Legalitas penanganan penyerangan di dunia *cyber.*
3. Pola kejadian c*yber crime* sangat cepat sehingga sulit ditangani.
4. Tata kelola kelembagaan *cyber-security* nasional.
5. Rendahnya *awareness* atau kesadaran akan adanya ancaman *cyber attack* internasional yang dapat melumpuhkan infrastruktur vital suatu negara.
6. Masih lemahnya industri kita dalam memproduksi dan mengembangkan perangkat keras atau *hardware* terkait dengan teknologi informasi yang merupakan celah yang dapat memperkuat maupun memperlemah pertahanan dalam dunia *cyber.*[16]

Penangganan kejahatan *cyber* yang masih parsial dan tersebar serta tidak adanya koordinasi yang baku dalam penanganan masalah *cyber-security.* Rendahnya *awarenees* atau kesadaran akan adanya ancaman *cyber attack* yang berdampak melumpuhkan infrastruktur vital contohnya adalah sistem radar penerbangan di bandara internasional Soekarno Hatta yang beberapa kali mengalami gangguan. Tidak menutup kemungkinan *cyber attack* menyerang infrastruktur vital negara seperti itu.

Terkait dengan kebijakan *cyber-security* di Indonesia perlu diatur sebuah kebijakan yang mengatur tentang berbagai elemen yang terkait dengan *cyber-security* dalam berbagai

[15] Pasal 9 Peraturan Menteri Komunikasi dan Informatika No. 29/PER/M.KOMINFO/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

[16] Hasyim Gautama, *Ibid.*

kebijakan yang mengatur tentang sistem teknologi informasi komunikasi yang digunakan yang meliputi pengaturan perlu adanya dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait dengan keamanan informasi, standar infrastruktur yang wajib dipenuhi yang sesuai dengan standar internasional dalam menghadapi *cyber war* termasuk didalamnya adanya *perimeter defense* yang memadai, adanya *network monitoring system, system information and event management* yang berfungsi memonitor berbagai kejadian di jaringan terkait dengan insiden keamanan, *network security assement* yang berperan sebagai *control* dan *measurement* keamanan.

IV.A.3. Struktur Organisasi

Permasalahan lainnya adalah penanganan *cyber-security* dalam kerangka pertahanan negara hingga saat ini masih bersifat sektoral dan belum terkoodinasi serta belum terpadu. Sebagai contoh seperti dijelaskan Eris Herryanto bahwa selama ini konsep *cyber defence* yang dilaksanakan Kemhan dan TNI masih bersifat sektoral, belum menyeluruh sebagai satu kesatuan.[17]

Guna mengatasi *cyber crime*, kebijakan yang telah dilaksanakan kementerian pertahanan keamanan adalah dengan membentuk Tim Kerja Pusat Operasi Dunia Maya (*Cyber Defence Operation Centre*) yang bertujuan menjaga keamanan dan perlindungan internal (Kemhan) maupun keamanan dan perlindungan eksternal (nasional) dalam dunia *cyber*. *Cyber Defence Operation Centre* dalam tataran kebijakan *cyber-security* nasional pembentukannya ditujukan untuk membangun sistem pertahanan semesta yang melibatkan seluruh warga negara, wilayah dan sumber daya nasional lainnya untuk menegakkan kedaulatan negara, keutuhan wilayah dan keselamatan segenap bangsa dari ancaman *cyber.*[18]

Guna menyikapi *cyber crime* yang sudah mencapai tahap memprihatinkan tersebut maka salah satu alternatif kebijakannya adalah dengan menempatkan *cyber-security* dalam kontek pertahanan. Berbagai kebijakan yang telah dilakukan terkait dengan *cyber-security* dalam konteks pertahanan di tingkat nacional antara lain, pada tahun 2010, Kementerian Pertahanan (Kemhan) memulai program penanggulangan terhadap *cyber attack* dengan membentuk Tim Kerja Pusat Operasi Dunia Maya (*Cyber Defence Operation Centre*) yang telah menyusun rencana pembentukan Tim Penanganan Insiden Keamanan Informasi.

IV.A.4. *Capacity Building*

Program pelatihan dan peningkatan keahlian *cyber-security* dilakukan dalam koordinasi Tim Kerja Pusat Operasi Dunia Maya (*Cyber Defence Operation Centre*). Selain itu diperlukan pembinaan SDM tentang arti pentingnya *cyber-security* guna meningkatkan pemahaman langkah-langkah preventif dalam menangkal segala tindak *cyber crime*.

Guna pengembangan kapasitas SDM dalam penangganan *cyber-security*, dalam tubuh TNI telah melakukan kerjasama dengan *stakeholder* yang memiliki kemampuan di bidang Informasi Teknologi diantaranya seperti kerjasama yang dilakukan oleh TNI AD dengan Institut Teknologi Del (*IT Del*), Sumatera Utara. Kerjasama ini direncanakan berlangsung selama tiga tahun, dari tahun 2014 sampai 2017 dalam tiga program. Ketiga program itu antara lain: penyiapan model perang *cyber*, seminar *military cyber intelligence and cyber operation*, serta *cyber camp* atau pekan *cyber.*[19]

IV.A.5. Kerjasama Internasional

Langkah lainnya yang dilakukan adalah dengan melakukan kerjasama internasional dengan organisasi regional maupun internasional dalam rangka penanggulangan *cyber crime*. Kerjasama dalam rangka penanggulangan *cyber crime* yang telah dilakukan Indonesia di antaranya dengan menjadi anggota *ASEAN*

[17] Penjelasan Sekretaris Jenderal Kementerian Pertahanan Marsdya TNI Eris Herryanto pada seminar nasional keamanan Infrastuktur Internet yang diselenggarakan *Indonesia Security Incident Response Team on Internet Infrastruktur (ID-SIRTI)* di Universitas Pertahanan di tahun 2011.

[18] Kemhan dan TNI Membangun Pertahanan Cyber, http://dmc.kemhan.go.id/post-kemhan-dan-tni-membangun-kekuatan-pertahanan-cyber.html, diakses Jumat, 18 Juli 2014 pukul 14.15.

[19] TNI Gandeng IT Del Antisipasi Penjahat di Dunia Internet, http://www.jpnn.com/read/2014/05/13/234115/TNI-Gandeng-IT-Del-Antisipasi-Penjahat-di-Dunia-Internet- diakses Selasa, 22 Juli 2014 pukul 14.30 WIB.

Network Security Action Council, menjadi anggota *International Telecommunication Union* (ITU), menjadi steering committee Asia Pacific Computer Emergency Response *Team* (APCERT), anggota dari *Forum of Incident Response and Security* (FIRST), melakukan kerja sama bilateral di bidang *cyber-security* dengan Jepang, Inggris serta beberapa negara lainnya.

Terkait dengan kerjasama internasional dalam bidang *cyber-security*, Indonesia juga ikut berperan aktif dalam program *Global Cyber security Agenda* (GSA) yang diluncurkan pada *World Telecommunication and Information Society Day* 2007 yang merupakan program kerjasama internasional yang bertujuan untuk menciptakan strategi dan solusi untuk meningkatkan kepercayaan dan keamanan di tengah masyarakat informasi.[20]

IV.B. Prospek dan Tantangan Pengembangan Kebijakan *Cyber security* Di Indonesia

IV.B.1. Kepastian Hukum

Terkait dengan kepastian hukum. pembangunan *cyber-security* adalah tersedianya dokumen *security policy* merupakan dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi.

Pengembangan dan penguatan kebijakan *cyber-security* di Indonesia hendaknya menyatu dengan strategi nasional dalam membangun ekosistem *cyber-security* nasional yang telah disusun pemerintah. Strategi nasional dalam membangun ekosistem *cyber-security* nasional yang telah disusun pemerintah tersebut meliputi upaya hukum, upaya teknis yang melingkupi standar dan operasional, penataan organisasi dan kelembagaan penangganan *cyber-security* dalam lingkup kepentingan nasional, *capacity building* atau peningkatan kapasitas Sumber Daya Manusia (SDM) di bidang *cyber-security* dan meningkatkan kerjasama internasional.

IV.B.2. Teknis dan Tindakan Prosedural

Adapun elemen pokok *cyber-security* yang harus terpenuhi dalam tersedianya *information infrastructure* merupakan media yang berperan dalam kelangsungan operasi informasi meliputi *hardware* dan *software*. Contohnya adalah *router*, *switch*, *server*, sistem operasi, *database*, dan *website*; tersedianya *perimeter defense* merupakan media yang berperan sebagai komponen pertahanan pada infrastruktur informasi misalnya IDS, IPS, dan *firewall;* adanya *network monitoring system* merupakan media yang berperan untuk memonitor kelayakan, utilisasi, dan *performance* infrastruktur informasi; terbangunnya *system information and event management* merupakan media yang berperan dalam memonitor berbagai kejadian di jaringan termasuk kejadian terkait pada insiden keamanan; terbentuknya *network security assessment* merupakan elemen *cyber-security* yang berperan sebagai mekanisme kontrol dan memberikan *measurement level* keamanan informasi.

Terkait dengan pengembangan kebijakan *cyber security* secara teknis, hal lain yang perlu dipikirkan menurut Kuntjara Pinardi dan Taufik Arief hal pertama yang patut diperhatikan adalah diperlukannya satelit khusus dalam rangka pertahanan dan keamanan dalam menyikapi secara serius *cyber crime*. Dimilikinya satelit khusus dalam rangka pertahanan dan keamanan mutlak diperlukan karena telah dimilikinya sejumlah *provider* telekomunikasi oleh pemilik modal asing. Sebagaimana diketahui, kebijakan *cyber-security* berkaitan erat dengan pembangunan dan penyelenggaraan telekomunikasi, khususnya di sektor pertahanan, dalam keadaan penyelenggaraan telekomunikasi Dephankam dan/atau TNI belum atau tidak mampu mendukung kegiatan penyelenggaraan telekomunikasi pertahanan keamanan negara, Dephankam dan/atau ABRI dapat menggunakan dan memanfaatkan telekomunikasi yang disediakan oleh badan penyelenggara atau badan lain atau telekomunikasi untuk keperluan khusus, saat ini satelit yang digunakan Kemhan/TNI saat

[20] Menteri Kominfo Pada "*High Level Segment ITU Council* 2008" Yang Membahas *Cyber security*, http://www.postel.go.id/info_view_c_26_p_814.htm diakses Jumat, 24 Juli 2014 pukul 13.30 WIB.

ini untuk komunikasi *video conference* Kemhan/TNI menyewa kapasitas *bandwidth* satelit Potensi Nasional (Binpotnas) dan fungsi lainnya.

Gambar Penggunaan Satelit Pertahanan di Masa Damai

Sumber: Taufik Arief, *Satelit Pertahanan*[21]

c-band milik PT Indosat, untuk komunikasi data Kemhan/TNI, VPN IP menyewa dari PT. Telkom dan untuk komunikasi *voice* Kemhan/TNI, PTSN dan VPN IP menyewa dari PT Telkom.

Dari gambar dapat diketahui bahwa satelit khusus sangat diperlukan oleh sektor pertahanan baik pada saat melancarkan operasi di masa damai mulai dari pengawalan Presiden/Wakil Presiden, membantu pengawalan tamu-tamu negara, mencegah terjadinya konflik akibat isu separatisme, pengamanan perbatasan dan berbagai fungsi lainnya seperti mengatasi aksi terorisme, pengamanan perbatasan sebab di daerah perbatasan sangat rawan tindak pidana penyelundupan narkoba dan senjata api, pengamanan pelayanan penerbangan dan tranportasi massal lainnya, pencegahan tindak separatisme, membantu upaya pertolongan dan pencarian berbagai musibah dalam satu rangkaian *search and rescue* (SAR), Pembinaan

Hal lain yang membuat pentingya segera dimilikinya satelit khusus pertananan menurut Taufik Arief adalah, satelit telah digunakan sejak Uni Soviet meluncurkan "*Sputnik*" pada tahun 1957. Dewasa ini militer di dunia (termasuk TNI) telah menggunakan satelit guna mendukung operasionalnya. Digunakan baik dalam masa damai (OMSP) dan masa perang (OMP). Sementara TNI membutuhkan satelit komunikasi bergerak yang bersifat *closed group*. (Surat Panglima TNI Nomor: B/2446/VI/2013 tanggal 14 Juni 2013).

Berbagai kejadian yang terkait dengan terjadinya *cyber crime* diantaranya perentasan situs Kepolisian RI, situs TNI AD termasuk diantaranya situs www.pusdikkav.mil.id yang merupakan situs Pusat Pendidikan Kavaleri TNI AD. Tercatat *hacker* Malaysia pernah menyambangi situs TNI AD. Begitu membuka situs TNI yang diretas, maka yang ada adalah tulisan *'This Website Has Been Hacked By* m33h00n.' Ketika diamati lebih seksama, pada bagian atas *website*, peretas meninggalkan jejak berupa *'Greetings From Malaysia! By* m33h00n

[21] Taufik Arief, *Satelit Pertahanan* pada Focus Group Discussion dalam rangka penyusunan proposal penelitian "Pembangunan TIK dalam kerangka Keamanan Nasional" Jumat, 7 Maret 2014.

& m0rn!ngw00d!'. Demikian pula dengan situs www.pusdikkav.mil.id yang merupakan situs Pusat Pendidikan Kavaleri TNI AD disatroni peretas pada Rabu, 15 Oktober 2013. Bila membuka website tersebut, maka yang akan tampil adalah latar hijau dan tulisan warna hijau berbunyi '*Secret* 404 *Was HERE*.' Hacker tersebut juga meninggalkan jejak nama yaitu 404 *Cyber Attack*.[22] Berbagai kasus *cyber crime* tersebut menunjukkan kenyataan bahwa di bidang *cyber* dalam kerangka pertahanan, Indonesia masih sangat jauh tertinggal.

Kondisi ini disebabkan karena keseriusan dalam menyikapi *cyber-security* membutuhkan insentif yang sangat besar, sebab bukan hanya karena ruang lingkup penanganan *cyber-security* yang kompleks namun juga penanganan *cyber-security* yang serius membutuhkan pembangunan infrastruktur penunjang yang membutuhkan pembiayaan yang tidak sedikit serta memerlukan sumber daya manusia yang seimbang dengan kompleksitas infrastruktur pendukung yang akan dibangun.

Langkah berikutnya dalam *cyber-security* secara teknis adalah penyempurnaan terhadap perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan totalitas informasi yang dikirimkan dan/atau disimpan dalam dunia *cyber*.

IV.B.3. Struktur Organisasi

Tantangan lainnya ke depan dalam pengembangan kebijakan *cyber-security* adalah sifat dari ancaman *cyber* yang multidimensional membuat penanganannya tidak hanya menjadi tanggungjawab dari TNI dan/atau Polri. Kemhan maupun Kemenkominfo. Menurut Sjafrie Sjamsoeddin, ancaman *cyber* termasuk dalam ancaman asimetris yang penanganannya membutuhkan pendekatan komprehensif. Karena sifatnya multidimensional, membuat *cyber-security* tidak dan bukan merupakan urusan satu kementerian saja, tetapi juga urusan berbagai kementerian lainnya. Karena itu diperlukan kebijakan *cyber-security* atau *cyber defence* yang dalam implementasinya membutuhkan badan koordinasi.[23]

Pengaturan dan penataan kelembagan *cyber-security* nasional yang kuat merupakan salah satu prasyarat terwujudnya *cyber-security* yang handal. Karenanya pembentukan pengaturan dan penataan kelembagaan yang menanggani *cyber-security* secara nasional tersebut harus terintegrasi sebagaimana dijelaskan dalam bagan berikut:

Dari bagan pengorganisasian dan kelembagaan penangganan *cyber-security* secara nasional tersebut dapat diketahui bahwa penangganan *cyber-security* harus terintegrasi secara kuat dan melibatkan berbagai lembaga terkait yaitu intelejen, penegak hukum, pertahanan dan keamanan baik itu Kementerian Pertahanan maupun TNI serta pemerintah sebagai regulator yang dalam hal ini diwakili oleh Kominfo dan ISSIRTI serta Lembaga Sandi Negara.

Terkait dengan pengorganisasian penangganan *cyber-security*. salah satu strategi menarik yang patut dicermati dalam menghadapi *cyber war* diantaranya upaya serius pemerintah Amerika Serikat dalam mengembangkan *The National Cyber Security Division (NCSD)* atau satu divisi khusus yang bertugas menanggani keamanan *cyber* secara nasional yang didukung oleh sektor swasta dan masyarakat yang memiliki tugas untuk membangun dan memelihara nasional yang efektif sistem keamanan *cyber* atau dunia maya, membuat dan menerapkan program manajemen resiko untuk dunia *cyber* guna melindungi infrastruktur telekomunikasi dan cyber dari situasi kritis yang dikenal dengan *the National Cyber space Response System*. Pembentukan Komando khusus satuan *cyber* oleh Departemen Pertahanan yang dipimpin oleh Jenderal Keith Alexander pada tahun 2009 merupakan langkah strategis yang perlu segera diimplementasikan dalam upaya menyikapi lebih serius dalam kerangka pertahanan dan menjaga kedaulatan di bidang *cyber*.

[22] Situs TNI Kembali Disatroni, http://www.merdeka.com/teknologi/situs-tni-kembali-disatroni-hacker.html diakses Selasa, 22 Juli 2014 pukul 14.20 WIB.

[23] Penjelasan Wakil Menteri Pertahanan Sjafrie Sjamsoeddin pada seminar nasional keamanan Infrastuktur Internet yang diselenggarakan Indonesia Security Incident Response Team on Internet Infrastruktur (ID-SIRTI) di Universitas Pertahanan di tahun 2011.

Bagan Organisasi dan Kelembagaan *Cyber security* Nasional

Sumber: Penerapan *Cyber security*, Hasyim Gautama[24]

Keseriusan dari militer Amerika menunjukkan bahwa *cyber* dalam kerangka pertahanan, dipandang tidak hanya sebagai jaringan melainkan telah diposisikan sebagai medan peperangan yang harus dimenangkan. Pandangan tersebut menjadikan militer Amerika secara serius meningkatkan sistem pertahanan negaranya di bidang *cyber* dengan dikomandoi militer, sipil dan *stakeholder* yang memiliki kemampuan di bidang informasi teknologi sebagai *supporting system* untuk membangun strategi dan taktik sistem pertahanan yang senantiasa diperbaharui sesuai dengan perkembangan pesat di *cyber* dan memperluas batas-batas strategi pertahanan yang ada. Perjuangan untuk mendominasi dunia *cyber* dalam pandangan *US Army Cyber Command* merupakan bagian yang tidak terpisahkan dari peperangan *cyber* atau *cyber war* itu sendiri baik saat ini maupun di kemudian hari.

Berbagai ancaman di dunia *cyber* atau *cyber threats* menuntut pendekatan baru untuk mengelola informasi, mengamankan informasi dan tantangan serta kondisi itulah yang mendorong dari pembentukan *US Army Cyber Command*. *Cyber space* atau dunia *cyber* itu sendiri ditempatkan Amerika setara dengan domain matra lainnya yaitu darat, laut, udara dan antariksa. Karenanya *US Army Cyber Command* bertugas merencanakan, mengkoordinasikan, mengintegrasikan, mensinkronisasikan, dan melakukan kegiatan untuk: mengarahkan operasi dan pertahanan ditentukan Departemen Pertahanan dan jaringan informasi; mempersiapkan diri untuk, dan ketika diarahkan, melakukan spektrum penuh operasi militer dunia maya untuk memungkinkan tindakan di semua domain, memastikan keamanan Amerika di dunia *cyber* dan menangkal berbagai ancaman yang ada di dunia *cyber*.[25]

Dengan adanya komando khusus satuan *cyber* pengelolaan terhadap manajemen risiko dunia maya melalui upaya seperti peningkatan pelatihan, informasi tentang keamanan dan kerahasiaan serta pembangunan jaringan yang aman dan tangguh hingga membentuk industri pertahanan *cyber* yang tangguh antara lain dengan membuat program-program pertahanan dan perlindungan *cyber* yang dapat digunakan untuk melindungi berbagai sistem

[24] Hasyim Gautama, *Ibid.*

[25] *US Army Cyber Command*, http://www.arcyber.army.mil/org-arcyber.html diakses Selasa, 22 Juli 2014 pukul 15.00 WIB.

pelayanan publik dan pemerintahan serta militer dari serangan di dunia maya tidak hanya berupa Tim Kerja Pusat Operasi Dunia Maya (*Cyber Defence Operation Centre*) sebagaimana dibentuk oleh Kemenhan.

Pengorganisasian terkait dengan *cyber security* tersebut hendaknya selaras dengan pengorganisasian pengunaan sistem teknologi informasi dengan memperhatikan empat hal utama yaitu: pertama, sistem informasi (*information systems*) dan kedua, kompetisi organisasi (*organizational competition*); ketiga, *information systems* (sistem informasi) dan *organizational decision making* (sistem informasi dan pengambilan keputusan dalam organisasi); keempat, pengorganisasian penggunaan sistem informasi (*organizational use of information systems*).

Pengembangan *cyber security* itu terintegrasi, teknologi informasi dibangun berbasis sistem yang dirancang untuk dapat mendukung kerja, manajemen dimana *cyber-security* tersebut dibangun. Selain itu Kedua, pembangunan sistem informasi. Ketiga, sumber daya eksternal sistem informasi. Keempat, manajemen sumber daya informasi.

Berbagai konsep dan langkah terkait dengan penyempurnaan pengorganisasian dan penangganan kelembagaan yang menangani *cyber-security* tersebut dilakukan dalam rangka untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna baik itu di tingkat kelembagaan maupun nasional terhadap risiko keamanan yang relevan dalam lingkungan *cyber*.

IV.B.4. *Capacity Building*

Penguasaan tehnologi masih terkendala merupakan permasalahan utama dalam pengembangan kebijakan *cyber-security*. Karenanya pengembangan kapasitas SDM merupakan salah satu hal yang harus diperhatikan selain

Karenanya, pengembangan strategi nasional dalam membangun *cyber-security* di Indonesia ke depan dilakukan dengan memenuhi empat pondasi yang mendukung perkembangan teknologi pengembangan perangkat lunak (*software)* seperti sistem dan aplikasi dan perkembangan alat keras (*hardware)* perkembangan sarana dan prasarana teknologi informasi, manajemen isi (*content management*), *telecommunication and networking*, perkembangan internet serta perdagangan *online* atau melalui internet.

Mengingat pesatnya perkembangan teknologi maka pengelolaan sumber daya *cyber security* haruslah ditempatkan sebagai proses manajemen bisnis. Hal ini diperlukan karena penangganan *cyber-security* bukanlah sesuatu yang murah dan mengalami perkembangan yang sangat pesat. Pengembangan kapasitas infrastruktur dengan ditempatkan sebagai proses manajemen bisnis maka potensi kerugian atau biaya yang harus dikeluarkan karena perkembangan teknologi dapat dikurangi.

Demikian pula dengan pengembangan kapasitas SDM yang bergerak di bidang *cyber-security*. Dengan dikelolanya SDM *cyber-security* dengan manajemen bisnis maka diharapkan akan mampu mempercepat terpenuhinya kebutuhan SDM yang menguasai bidang *cyber-security*.

IV.B.5. Kerjasama Internasional

Yang menjadi permasalahan adalah hingga saat ini belum ada kesepakatan internasional yang mengikat terkait dengan *cyber-security* sehingga diperlukan inisiatif Indonesia sebagai satu negara untuk mengupayakan tercapainya kesepakatan bersama yang mengikat terkait pengamanan dunia *cyber* secara internasional. Namun demikian, mengingat belum adanya kesepakatan secara internasional terkait dengan *cyber-security* maka penguatan pengamanan *cyber-security* nasional mutlak diperlukan.

Kerjasama internasional lainnya terkait dengan pengembangan *cyber-security* adalah dalam rangka meningkatkan kapasitas kemampuan *cyber security* baik itu untuk infrastruktur, sarana prasarana maupun dalam pengembangan kemampuan SDM dalam bidang *cyber-security* baik bilateral antar dua negara maupun regional ataupun internasional.

Peningkatan kerja sama teknologi informasi dan *cyber-security* selain itu juga diharapkan mampu membuka peluang bagi pengembangan industri media baru terkait dengan IT di

Indonesia sebagai salah satu bagian dari pengembangan industri strategis.

Terkait dengan pengembangan kerjasama internasional dalam rangka pengembangan *cyber-security* Indonesia perlu meningkatkan peran aktif mendorong berbagai kesepakatan bersama yang sepakati bersama dalam ITU yang merupakan organisasi terdepan dalam menciptakan *cyber space* yang aman bagi negara, pemerintah, masyarakat maupun dunia usaha. Selain itu Indonesia juga dapat mengembangkan kerjasama dengan negara-negara anggota ITU lainnya yang memiliki kemampuan IT lebih baik dari Indonesia untuk memberikan asistensi dalam upaya peningkatan sumber daya manusia, memberikan perlindungan kepada penguna dari kemungkinan terjadinya *cyber crime* dan meningkatkan kebermanfaatan internet untuk masyarakat informasi. Di samping itu juga Indonesia perlu terus meningkatkan peran aktifnya dalam program *Global Cyber security Agenda* (GSA).

V. KESIMPULAN DAN REKOMENDASI

Indonesia saat ini tengah dalam keadaan mendesak *cyber-security* atau keamanan dunia maya karena melihat kenyataan bahwa tingkat kejahatan di dunia maya atau *cyber crime* di Indonesia sudah mencapai tahap memprihatinkan. Salah satu fakta yang menunjukkan *cyber crime* di Indonesia sudah mengkhawatirkan adalah data CIA yang menyebutkan kerugian yang disebabkan karena tindak kejahatan dengan memanfaatkan maupun di dunia *cyber* di Indonesia telah mencapai 1,20% dari tingkat kerugian akibat *cyber crime* yang terjadi di dunia.

Dalam tataran kebijakan, penangganan *cyber crime* berbeda dengan penangganan kejahatan lainnya. Namun berbeda dengan penangganan kejahatan lainnya, *cyber-security* membutuhkan pemikiran yang komprehensif untuk menangganinya. Karena itu tulisan ini membahas dua hal yaitu: pertama, bagaimana kebijakan *cyber-security* yang telah dijalankan di Indonesia selama ini. Kedua, bagaimana prospek dan tantangan bagi pengembangan kebijakan *cyber-security* di Indonesia.

Kebijakan *cyber-security* yang telah dijalankan di Indonesia telah diinisiasi sejak tahun 2007 dengan dibentuknya *Indonesia Security Incident Response Team on Internet Infrastructure* adalah Tim yang ditugaskan Menteri Komunikasi dan Informatika (Kominfo) untuk membantu pengawasan keamanan jaringan telekomunikasi berbasis protokol internet. Tugas dan fungsi dari ID-SIRTII di antaranya melakukan pemantauan, pendeteksian dini, peringatan dini terhadap ancaman dan gangguan pada jaringan, berkoordinasi dengan pihak-pihak terkiat di dalam maupun luar negeri didalam menjalankan tugas pengamanan jaringan telekomunikasi berbasis protokol internet, mengoperasikan, memelihara dan mengembangkan sistem database sistem ID-SIRTII, menyusun katalog-katalog dan silabus yang berkaitan dengan proses pengamanan pemanfaatan jaringan, memberikan layanan informasi atas ancaman dan gangguan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet, menjadi *contact point* dengan lembaga terkait tentang keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet serta menyusun program kerja dalam rangka melaksanakan pekerjaan yang berkaitan dengan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet.

Kerangka hukum *cyber-security* di Indonesia saat ini dibangun diantaranya berdasarkan atas dasar UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012 serta surat edaran menteri dan peraturan menteri. Secara nasional, terdapat sejumlah permasalah terkait dengan pembangunan *cyber-security* yang tangguh di antaranya lemahnya pemahaman penyelenggara negara atan *security* terkait dengan dunia *cyber* yang memerlukan pembatasan pengunaan layanan yang *server*nya berada di luar negeri dan diperlukan adanya pengunaan *secured system*; belum adanya legalitas yang memadai terhadap penanganan penyerangan di dunia

cyber; tata kelola kelembagaan *cyber-security* secara nasional yang masih parsial dan tersebar serta tidak adanya koordinasi yang baku dalam penanganan masalah *cyber-security;* masih lemahnya industri kita dalam memproduksi dan mengembangkan perangkat keras atau *hardware* terkait dengan teknologi informasi.

Pengaturan dan penataan kelembagan *cyber-security* nasional yang kuat merupakan salah satu prasyarat terwujudnya *cyber-security* yang handal. penangganan *cyber-security* harus terintegrasi secara kuat dan melibatkan berbagai lembaga terkait yaitu intelejen, penegak hukum, pertahanan dan keamanan baik itu kementerian pertahanan maupun TNI serta pemerintah sebagai regulator yang dalam hal ini diwakili oleh Kominfo dan ISSIRTI serta Lembaga Sandi Negara.

Guna menyikapi *cyber crime* yang sudah mencapai tahap memprihatinkan tersebut maka salah satu alternatif kebijakannya adalah dengan menempatkan *cyber-security* dalam kontek pertahanan. penanganan *cyber-security* yang serius membutuhkan pembangunan infrastruktur penunjang diantaranya diperlukannya satelit khusus untuk pertahanan termasuk didalamnya kerja penangganan *cyber-security* karena telah dimilikinya sejumlah *provider* telekomunikasi oleh pemilik modal asing.

Tantangan lainnya ke depan dalam pengembangan kebijakan *cyber-security* adalah sifat dari ancaman *cyber* yang multidimensional membuat penangganannya tidak hanya menjadi tanggungjawab dari TNI dan/atau Polri. Kemhan maupun Kemenkominfo. Salah satu strategi menarik yang patut dicermati dalam menghadapi *cyber war* di antaranya upaya serius pemerintah Amerika Serikat dalam mengembangkan *The National Cyber Security Division (NCSD)* atau satu divisi khusus yang bertugas menanggani keamanan *cyber* secara nasional yang didukung oleh sektor swasta dan masyarakat yang memiliki tugas untuk membangun dan memelihara nasional yang efektif sistem keamanan *cyber* atau dunia maya, membuat dan menerapkan program manajemen risiko untuk dunia *cyber* guna melindungi infrastruktur telekomunikasi dan *cyber* dari situasi kritis yang dikenal dengan *the National Cyber space Response System*.

Terkait dengan pengembangan strategi nasional dalam membangun *cyber-security* di Indonesia ke depan dilakukan dengan memenuhi empat pondasi yang mendukung perkembangan teknologi informasi termasuk didalamnya pengembangan *cyber-security* yaitu: perkembangan perangkat lunak (*software)* seperti sistem dan aplikasi dan perkembangan alat keras (*hardware)* perkembangan sarana dan prasarana teknologi informasi, manajemen isi (*content management*), *telecommunication and networking*, perkembangan internet serta perdagangan *online* atau melalui internet.

Selain memenuhi keempat pondasi utama pengembangan *cyber-security* langkah lainnya yang mutlak dilakukan adalah pengorganisasian terkait dengan pengunaan sistem teknologi informasi dengan memperhatikan empat hal utama yaitu: pertama, sistem informasi (*information systems*) dan kedua, kompetisi organisasi (*organizational competition*); ketiga, *information systems* (sistem informasi) dan *organizational decision making* (sistem informasi dan pengambilan keputusan dalam organisasi); keempat, pengorganisasian penggunaan sistem informasi (*organizational use of information systems*).

Secara singkat, *cyber-security* ke depan hendaknya dibangun atas lima bidang dasar yaitu adanya kepastian hukum (undang-undang *cyber crime*); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *capacity building* & pendidikan pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*).

DAFTAR PUSTAKA

Buku

Anne W. Brascomb (ed), Toward A Law of Global Communication Network, New York: Lognman, 1986.

Elizabeth Longworth, *The Possibilities for legal framework for cyber space- Including New Zealand Perspective,* Theresa Fuentes et.al (editor), The International Dimesions of Cyberspace Law: Law of Cyberspace Series, Vol.1, Aldershot: Ashgate Publishing Limited, 2000.

John Vivian, Teori Komunikasi Massa, Jakarta: Kencana, 2008

M. Arsyad Sanusi, Hukum Teknologi dan Informasi, Bandung: Tim Kemas Buku, 2005

Pusat Teknologi Informasi dan Komunikasi Badan Pengkajian dan Penerapan Teknologi (BPPT), Kajian Konvergensi Teknologi Informasi dan Komunikasi, Jakarta: Pusat Teknologi Informasi dan Komunikasi BPPT, 2007

Ronald Thompson & William Cats Barril, *Information Technology and Management,* New York: Mc Graw Hill, 2003.

Jurnal

Nathalie Chaplan, *Cyber War: the Challenge to National Security,* Global Security Studies, Winter 2013, Volume 4, Issue 1, University of North Carolina Wilmington

Peraturan Perundang-Undangan

Peraturan Nomor 24 Tahun 2008 Tentang Penyelenggaraan Sistem Komunikasi Dan Elektronika Pertahanan Negara.

Peraturan Kepala Divisi Teknologi Informasi Kepolisian Negara Republik Indonesia No.1 Tahun 2011 tentang Hubungan Tata Cara Kerja Di Lingkungan Divisi Teknologi Informasi Kepolisian Negara Republik Indonesia.

Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMINFO/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi dan Informatika No.26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet

Majalah

D. Menthe, *Jurudiction in Cyber space: A Theory of International Space,* Michigan Telecommunications and Technology Law Review, 23 April 1998.

Internet

David S Alberts, *Informastion Age Anthology: The Information Age Military* http://www.dodccrp.org/files/Alberts_Anthology_III.pdf diakses Rabu, 16 April 2014 pukul 13.00 WIB.

Edmon Makarim, *Indonesian Legal Framework for Cyber security http://www.nisc.go.jp/securitysite/campaign/ajsympo/pdf/lecture2.pdf* diakses Kamis, 17 April 2014 pukul 15. 40 wib.

Dirjen Pothan: Ancaman Nonmiliter Lebih Banyak, http://www.kemhan.go.id/kemhan/?pg=73&id=928 diakses Rabu, 16 April 2014 pukul 13.00 WIB.

Indonesian Defense University, *Technology Perscpetive: National Cyber Security*, http://binkorpspelaut.tnial.mil.id/index.php?option=com_docman&task=doc_download&gid=6&Itemid=22. diakses Kamis, 17 April 2014 pukul 15. 40 wib.

Iran Luncurkan Sistem Komunikasi Pertahanan Udara Canggih, *http://www.islamtimes.org/vdcjaoe8auqehxz.bnfu.html* diakses Kamis, 17 April 2014 pukul 12.40 wib.

Kathleen Rustici, *Indonesia's Cyber security: An Opportunity for Deeper Cooperation,* http://csis.org/publication/indonesias-cyber security-opportunity-deeper-cooperation diakses Kamis, 17 April 2014 pukul 16.25 wib.

Kemhan dan TNI Membangun Pertahanan *Cyber*, http://dmc.kemhan.go.id/post-kemhan-dan-tni-membangun-kekuatan-pertahanan-cyber.html, diakses Jumat, 18 Juli 2014 pukul 14.15

Ketika Hacker Lebih Menakutkan Ketimbang Teroris, Tidak hanya berbahaya bagi keamanan negara, tapi juga ekonomi dunia, *http://m.news.viva.co.id/news/read/507480-ketika-hacker-lebih-menakutkan-ketimbang-teroris,* diakses Kamis, 17 Juli 2014 pukul 11.55 WIB.

Meeting the cyber security challenge in Indonesia An analysis of threats and responses A report from DAKA advisory http://dakaadvisory.com/wp-content/uploads/DAKA-Indonesia-cyber-security-2013-web-version.pdf diakses 22 Juli 2014 2014 pukul 13.30 WIB.

Menteri Kominfo Pada "*High Level Segment ITU Council* 2008" Yang Membahas *Cyber security*, http://www.postel.go.id/info_view_c_26_p_814.htm diakses Jumat, 24 Juli 2014 pukul 13.30 WIB.

Penerapan *Cyber security*, Hasyim Gautama, http://kemhubri.dephub.go.id/pusdatin/files/materi/Penerapan_Cybersecurity.pdf, diakses Jumat, 18 Juli 2014 pukul 14.15

Kemkominfo: Pengguna Internet di Indonesia Capai 82 Juta, http://kominfo.go.id/index.php/content/detail/3980/Kemkominfo%3A+Pengguna+Internet+di+Indonesia+Capai+82+Juta/0/berita_satker#.U9G4o5R_tfs diakses Jumat 24 Juli 2014 pukul 09.00 WIB.

Struktur TNI, http://www.tni.mil.id/pages-13-mabes-tni.html diakses Sabtu 5 Juli 2014, pukul 14.30 wib.

Situs TNI Kembali Disatroni, http://www.merdeka.com/teknologi/situs-tni-kembali-disatroni-hacker.html diakses Selasa, 22 Juli 2014 pukul 14.20 WIB

TNI AD Berdayakan Kopassus Menjadi Hacker, http://www.republika.co.id/berita/nasional/umum/14/05/16/n5noce-tni-ad-berdayakan-kopassus-jadi-hacker, diakses Sabtu 5 Juli 2014, pukul 14.00 wib.

TNI Gandeng IT Del Antisipasi Penjahat di Dunia Internet, http://www.jpnn.com/read/2014/05/13/234115/TNI-Gandeng-IT-Del-Antisipasi-Penjahat-di-Dunia-Internet- diakses Selasa, 22 Juli 2014 pukul 14.30 WIB.

US Army Cyber Command, http://www.arcyber.army.mil/org-arcyber.html diakses Selasa, 22 Juli 2014 pukul 15.00 WIB.

Bahan lain yang tidak dipublikasikan

Taufik Arief, *Satelit Pertahanan* pada Focus Group Discussion dalam rangka penyusunan proposal penelitian "Pembangunan TIK dalam kerangka Keamanan Nasional" Jumat, 7 Maret 2014

Taufik Arief, *Intelligent Integrated Information System Dan Intelligent Surveillance System Dlm Sistem Pertahanan Negara,* disampaikan pada Focus Group Discussion dalam rangka penyusunan proposal penelitian "Pembangunan TIK dalam kerangka Keamanan Nasional" Jumat, 7 Maret 2014.

Penjelasan Sekretaris Jenderal Kementerian Pertahanan Marsdya TNI Eris Herryanto pada seminar nasional keamanan Infrastuktur Internet yang diselenggarakan *Indonesia Security Incident Response Team on Internet Infrastruktur (ID-SIRTI*) di Universitas Pertahanan di tahun 2011.

Penjelasan Wakil Menteri Pertahanan Sjafrie Sjamsoeddin pada seminar nasional keamanan Infrastuktur Internet yang diselenggarakan Indonesia Security Incident Response Team on Internet Infrastruktur (ID-SIRTI) di Universitas Pertahanan di tahun Pertahanan di tahun 2011.