OPTIMALISASI *CYBER SECURITY* DALAM UPAYA MENINGKATKAN KEAMANAN DATA PENGGUNA DARI *CYBER CRIME*

Adi Ariyanto, 3301421040, PPKN
Fakultas Ilmu Sosial, Universitas Negeri Semarang
E-mail : adiariyanto975@gmail.com

A. PENDAHULUAN

Perkembangan zaman tidak terlepas dari semakin berkembangnya teknologi informasi dan komunikasi yang dapat diakses dengan lebih mudah oleh berbagai kalangan generasi bangsa Indonesia. Perkembangan teknologi informasi dan komunikasi terus berkembang pesat, kini dimungkinkan untuk menggunakan teknologi informasi dan komunikasi melalui perangkat mobile. Kegiatan yang biasanya dilakukan di dunia nyata kini banyak diperdagangkan melalui gadget (seperti perbankan dan pengiriman surat ke dalam kegiatan dunia maya). Perkembangan dari transaksi berpindah dengan menggunakan I-Pad, Smartphone, Handphone, Laptop. Kita tidak lagi mengalami kesulitan untuk mengakses informasi dari seluruh penjuru dunia. Selain banyaknya teknologi informasi dan komunikasi yang telah memberikan dukungan untuk banyak perangkat mobile, juga karena banyak tersedianya hotspot gratis dibanyak tempat. Pesatnya perkembangan teknologi informasi dan komunikasi juga diiringi dengan meluasnya penyalahgunaan teknologi informasi dan komunikasi, sehingga menjadi masalah yang sangat meresahkan yaitu terjadinya kejahatan yang dilakukan di dunia maya atau yang biasa dikenal dengan istilah *"cyber crime".*

Berbagai kejahatan telah terjadi di dunia maya ini, kasus-kasus tersebut tentu saja merugikan dan berdampak negatif, kejahatan dunia maya semacam ini tidak hanya mencakup di Indonesia, tetapi juga mencakup seluruh dunia. Beberapa kejahatan yang terjadi disebabkan oleh maraknya penggunaan data melalui E-mail, E-banking dan E-commerce di Indonesia. Semakin banyaknya kasus *cyber crime* (khususnya di Indonesia) telah menarik perhatian pemerintah untuk segera memberlakukan undang-undang yang dapat digunakan untuk menjebak pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah memasukkan UU *cyber crime* (UU Siber) ke dalam UU ITE Nomor 11 Tahun 2008, dan berharap dengan adanya UU ITE Nomor 11 Tahun 2008 dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya. Berdasarkan kasus dan keadaan *cyber crime* yang berlangsung di Indonesia, bisa terlihat bahwa *cyber crime* melahirkan ancaman serius bagi departemen keamanan non tradisional. Di Indonesia,

kejahatan *cyber crime* merupakan salah satu kejahatan tertinggi di dunia. Situasi ini akan berdampak pada perkembangan problematis masalah politik global, termasuk masalah keamanan. Maka dengan hal tersebut sangat diperlukan adanya optimalisasi *cyber scurity* dalam upaya meningkatkan keamanan data dari *cyber crime.*

B. PEMBAHASAN

Optimalisasi berasal dari kata dasar optimal yang berarti terbaik, tertinggi, paling menguntungkan, (Kamus Besar Bahasa Indonesia, 2011:345). Menjadikan paling baik, menjadikan paling tinggi, pengoptimalan proses, cara, perbuatan mengoptimalkan (menjadikan paling baik, paling tinggi, dan sebagainya), sehingga optimalisasi adalah suatu tindakan, proses, atau metodologi untuk membuat sesuatu (sebagai sebuah desain, system, atau keputusan) menjadi lebih/sepenuhnya sempurna, fungsional, atau lebih efektif. Optimalisasi merupakan upaya seseorang untuk meningkatkan suatu kegiatan atau pekerjaan agar dapat memperkecil kerugian atau memaksimalkan keuntungan agar tercapai tujuan sebaik-baiknya dalam batas-batas tertentu (Andri Rizki Pratama, 2013:6).

Roxana Radu memaparkan bahwa *cyber security* merupakan seperangkat kebijakan, alat, instrumen, manajemen risiko dalam mencegah ancaman yang datang dari dunia maya (Radu dalam Kremer & Muller, 2014). Adapun Madeline Carr menjelaskan dalam jurnalnya yang berjudul *Crossed Wires: International Cooperation on Cyber Security* bahwa keamanan *cyber* merupakan permasalahan *post-state*. Artinya adalah keamanan *cyber* merupakan bentuk ancaman yang tidak bisa ditangani menggunakan paradigma *Westphalia* yaitu mengatasi ancaman melalui instrumen negara seperti militer.

Tipologi ancaman terhadap keamanan *cyber* dapat bermacam-macam. Myriam Dunn Cavelty menjelaskan ancaman tersebut ke dalam tiga tipologi. Contoh tipologi tersebut adalah *cyber crime*, *cyber war* dan *cyber terrorism* (Cavelty dalam Mauer dan Cavelty, 2010). Kejahatan *cyber crime* adalah aktivitas kejahatan yang menggunakan teknologi informasi untuk mencapai kepentingan ekonomi yang dilakukan oleh organisasi kriminal. Sedangkan *cyber war* adalah bentuk perang Von Clausewitz versi digital. Adapun *cyber terrorism* adalah kegiatan peretasan ataupun pelumpuhan sistem informasi negara-bangsa yang dilakukan oleh kelompok terorism (Cavelty dalam Mauer dan Cavelty, 2010).

Optimalisasi cyber security dalam hal ini sangat diperlukan dalam upaya meningkatkan kemanan data pengguna dari pengaruh cyber crime, sebagai upayanya pemerintah telah merancang strategi melalui kebijakan dan peraturan yang ditetapkannya yakni Kebijakan *cyber security* secara khusus di Indonesia yang telah di inisiasi 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.

Mengenai 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 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.

Selanjutnya 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.

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 ke empat 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).*

C. PENUTUP

Optimalisasi *cyber security* merupakan suatu proses kegiatan untuk meningkatkan dan mengoptimalkan suatu pekerjaan dari cyber security menjadi lebih/sepenuhnya sempurna, fumgsional, atau lebih efektif serta mencari solusi terbaik dari beberapa masalah dari *cyber crime* agar tercapai tujuan sebaik-baiknya sesuai dengan tujuannya yakni melakukan upaya perlindungan dari data penggunanya. 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*.

Pengembangan strategi nasional dalam membangun *cyber security* di Indonesia ke depan dapat dilakukan dengan memenuhi empat pondasi yang dapat mendukung perkembangan teknologi informasi termasuk didalamnya pengembangan *cyber security* diantaranya 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.

DAFTAR PUSTAKA

Habibi, Miftakhur Rokhman, and Isnatul Liviani. 2021. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia". *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam* 23 (2):400-426. https://jurnalfsh.uinsby.ac.id/index.php/qanun/article/view/1132.

Ramadhan, I. 2020. Strategi Keamanan Cyber Security Di Kawasan Asia Tenggara: Self-Help Atau Multilateralism?. *Jurnal Asia Pacific Studies*, *3*(2), 181-192. https://doi.org/10.33541/japs.v3i1.1081

Pratama, Andri Rizki. 2013. Optimalisasi Keselamatan Crew Kapal dalam Proses. Kerja Jangkar di AHTS Amber. Semarang: Politeknik Ilmu Pelayaran.

Radu, Roxana. Cyber Security and Cyber Insecurity. Dalam Jan-Frederik Kremer. 2014. Cyberspace and International Relations, New York: Spinge.

Cavelty, M. D. & Mauer V., Power and security in the information age: Investigating the role of the state in cyberspace, Routledge, 2016

Alwi, Hasan. 2011. Kamus Besar Bahasa Indonesia. Jakarta: Gramedia Pustaka Utama.

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.

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.

Link Review Artikel Di Youtube : https://youtu.be/JLM8yJ244DM