KEAMANAN SIBER DAN PEMBANGUNAN DEMOKRASI DI INDONESIA

Editor:
Suwandi Sumartias

Judul:
Keamanan Siber dan Pembangunan Demokrasi di Indonesia

Perpustakaan Nasional:
Katalog Dalam Terbitan (KDT)
x+156 hlm.; 16 x 24 cm

ISBN: 978-602-60367-2-8
Cetakan Pertama, 2018

Penulis:
Prayudi
Ahmad Budiman
Aryojati Ardipandanto
Aulia Fitri

Editor:
Suwandi Sumartias

Desain Sampul:
Fajar Wahyudi

Tata Letak:
Tim Kreatif Lingkar Muda Mandiri

Diterbitkan oleh:
Pusat Penelitian Badan Keahlian DPR RI
Gedung Nusantara I Lt. 2
Jl. Jenderal Gatot Subroto Jakarta Pusat 10270
Telp. (021) 5715409 Fax. (021) 5715245

Bekerjasama dengan:
Inteligensia Intrans Publishing, Anggota IKAPI
Jl. Joyosuko Metro 42 Malang, Jatim
Telp. 0341- 573650 Fax. 0341-588010
redaksi.intrans@gmail.com
www.intranspublishing.com

Pengantar Editor

Sejak reformasi, bangsa Indonesia teramat sibuk dengan urusan politik praktis dengan segala persoalan dan tantangannya. Kini di era industri 4.0 yang didukung teknologi komunikasi dan informasi yang sangat cepat, telah merubah tatanan sosial dan bisnis serta perilaku masyarakat, terutama masyarakat kota menengah ke atas. Era disrupsi komunikasi dan informasi bukan hanya menjadi tantangan, juga peluang yang membutuhkan jawaban dari semua elemen kebangsaan. Dalam dimensi politik dan atau demokratisasi, sedang terjadi gejala komunikasi yang luar biasa di dunia maya (media sosial). Salah satu efek negatif dari kebebasan ekspresi warga, kini disalurkan melalui media sosial dengan segala kontennya yang sangat mengancam keutuhan relasi kebangsaan. Media sosial (*twitter*, *instagram*, *youtube*, dlsb) seakan terbelah menjadi komunitas *lovers* dan *haters* yang berlebihan dan atau kebablasan. Kondisi ini menjadi "bom waktu" dalam membangun SDM yang berkualitas dan berkarakter di seluruh wilayah NKRI.

Salah satu artikel dari Crispin Thurlow, dkk. (2004) yang berjudul *Unwanted Cammmunication; Aggression and Abuse; Sexual Harassment; Ethical and Unethical Communication*"). Dia mengatakan bahwa media sosial *online* (media virtual) memiliki peran amat penting dan telah menjadi media alternatif bagi masyarakat, khususnya dalam berdemokrasi. Apresiasi tinggi masyarakat dalam penggunaan sistem jejaring sosial (*social-networking systems*) untuk berkomunikasi dan sekaligus menyalurkan, mengartikulasikan kepentingan secara *online* untuk hal yang bermanfaat ataupun merugikan. Dampak yang merugikan, para peneliti menemukan sejumlah pers populer telah mengingatkan kita tentang bahaya potensial yang tersembunyi dari *online* dan CMC (*Computer Mediated Communication*) yang tak

beretika. "*Online potential dangers lurking online and unethical CMC); Online harassment; hate speech online dan online ethics*.

Indonesia pengguna media sosial sungguh luar biasa. Menurut lembaga riset pasar *e-Marketer*, populasi netter tanah air mencapai 83,7 juta orang pada 2014. Angka yang berlaku untuk setiap orang yang mengakses internet setidaknya satu kali setiap bulan itu mendudukkan Indonesia di peringkat ke-6 terbesar di dunia dalam hal jumlah pengguna internet. Pada 2017, *e-Marketer* memperkirakan netter Indonesia bakal mencapai 112 juta orang, mengalahkan Jepang di peringkat ke-5 yang pertumbuhan jumlah pengguna internetnya lebih lamban. Secara keseluruhan, jumlah pengguna internet di seluruh dunia diproyeksikan bakal mencapai 3 miliar orang pada 2015. Tiga tahun setelahnya, pada 2018, diperkirakan sebanyak 3,6 miliar manusia di bumi bakal mengakses internet setidaknya sekali tiap satu bulan. (*Kompas.com*)

Dengan dinamika yang sangat cepat di atas, tentunya antisipasi lembaga negara terkait sangat diperlukan tidak hanya pendekatan dan penegakkan formalitas yuridis melalui UU ITE, khususnya yang berkaitan dengan ujaran kebencian dan atau negatif di media sosial, juga terhadap dinamika gerakan *netizen* dan atau komunitas yang seringkali melakukan perlawanan sosial terhadap penyimpangan dari praksis demokrasi yang ditampilkan para elit politik. Aksi ini juga merupakan jalan terbaik untuk memperingatkan bahwa legitimasi dan optimalisasi fungsi demokrasi melalui lembaga-lembaga formal (eksekutif, legislatif, yudikatif) bentukan pemilu akan menjadi lembaga yang tak lagi memiliki legitimasi rakyat dan kehilangan makna dan kepercayaan di mata rakyatnya.

Untuk menjawab berbagai fenomena di atas, melalui buku Keamanan Siber yang ditulis para pakar di bidang media sosial sebagai hasil riset, tentunya menjadi menarik untuk disimak dan dikaji lebih dalam.

Bagian I, karya tulis Prayudi tentang Politik Siber dan Kedaulatan Negara yang menguraikan sub tema tentang: Politik Siber; Sentralisasi dan Desentralisasi Pemerintahan; Memudarnya Batas-Batas Teritorial Kedaulatan Negara; Masih Politik Partisan Jangka Pendek; dan Penyesuaian Kondisi Lapangan.

Bagian II, Ahmad Budiman menyajikan Tata Kelola *Cyber Security* Pemerintah Daerah dalam Upaya Meningkatkan Pelayanan Publik, dengan membahas sub tema: Pelayanan Publik Berbasis IT; ***Cyber Security* untuk Pelayanan Publik;** Tata Kelola *Cyber Security* di Pemerintah Daerah: Pelaksanaan di Sulawesi Tenggara, Pelaksanaan di Kalimantan Barat dan Pemutakhiran Tata Kelola *Cyber Security.*

Bagian III, Aryojati Ardipandanto menyajikan bahasan tentang Peran *Cyber Security* dalam Mencegah Konflik Politik Masyarakat di Daerah, dengan sub bahasan: Perkembangan Media Sosial dalam Demokrasi di Indonesia; Kasus HOAX; Sikap Pemerintah terhadap Dinamika Media Sosial; UU ITE, Apakah sudah Efektif?; *Cyber Security* di Indonesia; Daerah-daerah Rawan Konflik Akibat Lemahnya *Cyber Security* dan contoh kasus di Provinsi Sulawesi Tenggara dan Kalimantan Barat; Bagaimana Mengembangkan *Cyber Security* Sulawesi Tenggara dan Kalimantan Barat? Apa yang Perlu Diperbaiki?

Bagian IV, Aulia Fitri menyajikan pembahasan tentang Kebijakan Siber Nasional di Era Globalisasi Informasi, dengan sub tema tentang: Globalisasi Informasi; Kebijakan Siber di Berbagai Negara (Amerika Serikat; Australia; India; Singapura); Kebijakan Keamanan Siber di Indonesia; Problematika Kebijakan Siber di Indonesia dan Rekomendasi Implementasi Kebijakan Siber Nasional di Indonesia

Dengan uraian yang ada dalam buku ini, pentingnya *Cyber Security* dalam menata dan mengelola arus komunikasi dan informasi yang berkembang di masyarakat tentunya menjadi teramat penting

dan utama. Keberadaan lembaga formal yang serius, profesional dan berkelanjutan dalam bidang ini tentu menjadi tuntutan yang segera. Alih-alih kehadiran UU ITE No. 11 tahun 2008 masih belum dipahami dengan baik dan benar oleh para *netizen* atau warga masyarakat di seluruh pelosok negeri. Keadaan ini tentunya tidak bisa dibiarkan, karena pada gilirannya menjadi kontra produktif dalam mengawal dan mewujudkan karakter bangsa dan nasionalisme. Selamat menyimak.

Editor,

Suwandi Sumartias
Dosen Komunikasi Politik Fikom Unpad

Daftar Isi

BAGIAN 3
PERAN *CYBER SECURITY* DALAM MENCEGAH KONFLIK POLITIK MASYARAKAT DI DAERAH

Aryojati Ardipandanto

BAGIAN 4
KEBIJAKAN SIBER NASIONAL DI ERA GLOBALISASI INFORMASI

Aulia Fitri

Prolog
"Keamanan Siber dalam Pembangunan Demokrasi di Indonesia"

A. Perkembangan Teknologi Informasi

Pada era teknologi informasi modern dikenal internet dan komputer yang mampu mentransmisikan secara elektronis (komunikasi elektronis) segala bentuk data informasi secara cepat, tepat, efektif efisien serta *convenient* (nyaman, gampang). Bahkan para industri teknologi informasi mengklaim dapat pula menjamin kerahasiaan berita/ informasinya dalam sistem komunikasi yang umum dan terbuka itu. Perlu diamati lebih dalam dan tajam apakah "umum dan terbuka" itu benar-benar mampu melindungi kerahasiaan pada umumnya.[1]

Perkembangan teknologi informasi komunikasi (TIK) semakin pesat yang berimbas juga pada aktivitas pemerintahan daerah dan interaksi komunikasi di masyarakat. Komunikasi melalui saluran media maya (*cyber*), sesuai dengan perkembangan teknologi yang menyertainya juga harus berhadapan dengan potensi ancaman keamanan dalam pengelolaan (termasuk penyimpanan), serta penggunaannya. Pada sisi yang lain, kita tidak bisa memungkiri kemajuan TIK khususnya melalui saluran komunikasi maya (*cyber*) telah banyak digunakan dalam aktivitas pemerintahan atau interaksi di dalam masyarakat. Keamanan saluran media maya (*cyber security*) harus berhadapan dengan berbagai tantangan, baik yang bersifat umum maupun yang bersifat khusus di satu daerah.

---

[1] "*Persandian Indonesia*", http://www.lemsaneg.go.id/index.php/khasanah/persandian-indonesia/, diakses tanggal 12 Februari 2016.

Pilar *cyber security* di pemerintahan terdiri dari kebijakan, pelayanan, proses kerja, teknologi dan masyarakat. Untuk itu pemerintah perlu memperhatikan arsitektur pengelolaan *cyber security* yang meliputi:

a. *Definie and classify your requirements*
b. *Design for management requirements*
c. *Refini for business requirements*
d. *Overlay information architecture and manageability.*[2]

Tingginya penggunaan internet seiring dengan maraknya keterkaitan internet dengan kehidupan sehari-hari, mengakibatkan frekuensi serangan dan kejahatan *cyber space* semakin meningkat. Kejahatan-kejahatan *cyber space* atau yang dikenal dengan istilah *cybercrime* tersebut meliputi pencurian identitas dan data (sumber daya informasi), pembajakan *account* (*email, IM, social network*), penyebaran *malware* dan *malicious code*, *fraud, spionase industry*, penyanderaan sumber daya informasi kritis serta *cyber warfare* atau perang di dalam dunia maya.[3]

Keamanan saluran media maya (*cyber security*) juga diperlukan dalam rangka mengantisipasi terjadinya ancaman yang terkait dengan keamanan data dan informasi. *Cyber security* adalah aktivitas untuk melakukan pengamanan terhadap sumber daya telematika demi mencegah terjadinya tindakan *cyber crime.*[4]

Ancaman terhadap data dan informasi dapat dibagi menjadi 2 macam, yaitu ancaman aktif dan ancaman pasif. Adapun ancaman aktif

---

[2] Dani Firmansyah, "*Cybersecurity for governance",* disampaikan pada FGD Proposal Penelitian Tata Kelola *Cyber Security* pada Pemerintahan Daerah, di Puslit BKD, 17 Maret 2017.

[3] Kementerian Komunikasi Informatika RI, *Buku Putih 2011 Komunikasi dan Informatika Indonesia*, 2011, hal. 22.

[4] Mochamad James Falahuddin, Sekilas Tentang *Cyber Crime*, *Cyber Security* dan *Cyber War*, https://inet.detik.com/security/d-3005339/sekilas-tentang-cyber-crime-cyber-security-dan-cyber-war, diakses tanggal 26 Januari 2017.

antara lain, *pertama*, pencurian data, *kedua,* penggunaan sistem secara ilegal, *ketiga,* penghancuran data secara ilegal, *keempat*, modifikasi secara ilegal. Sedangkan ancaman pasif antara lain berupa, *pertama,* kegagalan sistem atau kegagalan *software* dan *hardware* yang dapat menyebabkan data menjadi tidak konsisten, transaksi tidak berjalan dengan lancar sehingga data menjadi tidak lengkap atau bahkan data menjadi rusak. *Kedua*, kesalahan manusia, yakni kesalahan dalam pengoperasian sistem yang dilakukan oleh manusia yang dapat mengancam integritas sistem dan data. *Ketiga,* bencana alam sumber daya pendukung sistem informasi menjadi luluh-lantak dalam waktu yang singkat.[5]

Namun dengan bertambahnya jumlah laporan insiden keamanan siber yang terus meningkat, ancaman siber tidak hanya membahayakan infrastruktur informasi penting yang ada, namun juga bisa mengancam kerahasiaan, keutuhan, dan ketersediaan informasi yang sensitif yang umumnya kita proses, kirim dan simpan secara *online*. Oleh karena itu, untuk memitigasi ancaman siber, pemerintah Indonesia berencana untuk lebih memperkuat dan memperluas kapasitas keamanan siber dalam hal struktur kelembagaan dan koordinasi terkait pengembangan keamanan siber nasional.[6]

B. Fenomena Siber

Fenomena ruang siber menggambarkan sebuah realitas bahwa aktifitas kegiatan masyarakat modern saat ini sudah saling terkoneksi melalui ruang siber dan internet. Dari perspektif keamanan siber, pemanfaatan internet juga dimungkinkan untuk tujuan negatif atau destruktif oleh

---

[5] Paryati, *Keamanan Sistem Informasi,* http://repository.upnyk.ac.id/143/1/47_Keamanan_Sistem_Informasi.pdf, laman diakses pada Hari Selasa, 9 Agustus 2016, pukul 16.10 WIB.

[6] Peta Masa Depan Keamanan Siber Indonesia, http://aptika.kominfo.go.id/index.php/artikel/138-peta-masa-depan-keamanan-siber-indonesia, diakses tanggal 5-3-2017

pihak-pihak yang punya kemampuan baik dilakukan secara perorangan, kelompok hingga oleh negara.[7]

Penataan keamanan siber menjadi lebih relevan, terutama bila dikaitkan dengan kebijakan pemerintah dalam mengembangkan *e-government* terutama di pemerintah daerah (Pemda). Tata kelola keamanan siber ini sangat diperlukan untuk tetap menjaga kepercayaan masyarakat dalam mendapatkan layanan publik dan layanan perijinan berbasis *online*. Pengembangan sistem *e-Government* tidak terlepas dari pengamanan siber, karena pengembangan *e-Government* dapat dimulai dengan pembangunan situs yang menyediakan peluang interaksi pelayanan publik dan penyimpanan data dan informasi.

Keamanan siber tidak hanya terkait dengan persoalan tata kelola keamanan siber utama yang terjadi di Pemda, namun juga terkait dengan permasalahan konten yang disebarluaskan melalui media *online* ini, seperti pada penerapan kehidupan demokrasi melalui kegiatan pemilihan umum utamanya yang terjadi di daerah. Dalam konteks tata kelola informasi dan kemanan informasi di era globalisasi informasi terutama pada era demokrasi pilkada, maka sistem persandian (*kriptografi*) sejatinya juga merupakan bagian integral yang tidak dapat dipisahkan. Tata kelola informasi dan keamanan informasinya bahkan menjadi lebih relevan jika dikaitkan dengan kebijakan pemerintah mengembangkan *e-gov* di lingkungan Pemda, termasuk aparatur sipil negara (ASN)-nya, karena dalam filosofis keamanan informasi diyakini bahwa *human factor is the weakest link*. Di lingkungan Pemda, tata kelola informasi dan keamanan informasi diperlukan untuk tetap menjaga kepercayaan masyarakat dalam mendapatkan layanan publik dan layanan perijinan yang prima.[8]

---

[7] Rudy Agus Gemilang Gultom, Membangun Tata Kelola Informasi dan Keamanan Informasi Pemerintahan Daerah di Era Globalisasi Informasi dalam Rangka Menjaga Keutuhan dan kedaulatan NKRI", disampaikan pada FGD Penelitian Tata Kelola *Cyber security* pada Pemerintahan Daerah, Puslit BKD, Jakarta, 17 Maret 2017.

[8] *Ibid.*

Keberadaan *cyber security* dalam konteks kehidupan demokrasi, tidak terlepas dari dinamika pemilu yang diselenggarakan. Ini biasanya dikaitkan dengan tahapan kampanyenya. Kampanye pemilu dan keberadaan media sangat kuat ditekankan dalam draft RUU Penyelenggara Pemilu 2016, tidak saja terkait proses penetapan hasil pemilu, tetapi juga di tahapan proses awal rekrutmen dan pengumuman kandidat penyelenggaranya, baik KPU maupun Bawaslu di tingkat nasional dan daerah. Pada rentang tahapan demikian, pemilu dan kampanye sangat kuat dipengaruhi oleh media dengan segala dinamika politik konten berita yang disebarkannya. Apalagi terdapat fenomena iklan politik yang mendorong budaya populer dalam politik, seperti logika seolah-olah bagi siapa saja anggota masyarakat yang berminat terjun ke dalam kompetisi politik tidak absah jika belum melakukan publikasi iklan politik. Ini berlaku nyaris jamak bagi setiap anggota masyarakat, apakah itu semula berprofesi kiai, santri, guru, artis, pengusaha, petani, dan lain sebagainya.[9]

Media yang penting bagi politisi dan partai tidak lagi sekedar pada konteks promosi melalui iklan diri secara terbuka, tetapi juga dapat dimanipulasi bagi sarana mendiskreditkan lawan atau saingan politik yang dilakukan secara tertutup. Sebaran manipulasi iklan politik semacam ini sangat terbuka peluang penggunaannya melalui media sosial yang nihil filter kebenaran atau akurasi konten pemberitaannya.

Peraturan KPU No. 12 Tahun 2016 tentang Kampanye Pilkada yang menjabarkan UU Nomor 10 Tahun 2016 tentang Pemilihan Gubernur, Bupati/Walikota hanya mengatur soal kewajiban pasangan calon (paslon) mendaftarkan akun resmi di media sosial kepada KPU setempat. Akun itu juga harus ditutup maksimal sehari setelah masa kampanye berakhir. Penggunaan media sosial saat pilkada serentak 101 daerah di tahun 2017, tidak hanya terjadi pada kasus di Jakarta. Tetapi penggunaannya juga marak berkembang di pilkada di daerah-daerah

[9] Sufyanto, *Selebrisasi Politik: Kajian Dramaturgi, Habitus dan Tindakan Komunikatif Aktor Pemilu*, Penerbit Nusa Media, Bandung, 2015, h. 17.

lainnya. Tanggung jawab dianggap menjadi penting dalam perkembangan pesat media sosial dalam pemilu dan pilkada, tidak sekedar pada konteks kendali atau pengawasan terhadap penggunaannya. Kalau terlampau prioritas pada aspek pengawasan penggunaan media sosial dalam momentum pilkada atau pemilu, maka dapat mengarah pada kekhawatiran adanya belenggu tertentu bagi kebebasan berekspresi dan memperoleh akses informasi publik.[10]

Kampanye pemilu yang mensyaratkan *fairness* sebagai fondasi bagi persaingan yang setara tidak akan terwujud maksimal, atau dapat diganggu oleh media sosial yang sifatnya sebaran beritanya dilakukan melalui genggaman individual. Bahkan, infiltrasi gangguan tidak saja di tingkat *fairness* kampanye, tetapi juga dapat menekan stabilitas politik dan jadi godaan bagi rezim penguasa melakukan tindakan represif. Tindakan represif diambil dengan alasan untuk menjaga kepentingan yang lebih besar dan stabilitas politik menjadi muatan kepentingan dimaksud. Kebijakan rezim Jokowi-Jusuf Kalla dalam mengendalikan media komunikasi masyarakat, terutama pada konteks media sosial, tampaknya tidak terlepas dari kontroversi media sosial dalam kampanye pemilu.

Media sosial sebagai sarana komunikasi menghadapi tantangan agar partisipasi publik dalam pemerintahan dapat berjalan dan menghasilkan substansi yang konstruktif. Ini menjadi tantangan, mengingat sumber dan topik berita bohong (*hoax*) yang paling sering diterima masyarakat adalah berita seputar isu politik. Produksi konten-konten negatif dari sektor ini sangat banyak karena melibatkan tim, mulai dari produser, penyokong, hingga pengikut. Gambaran betapa isu politik menjadi bahan perbincangan paling ramai di media sosial dapat terpantau dari hasil analisis perangkat *Social Topic Analysis*. Hanya dalam beberapa jam, khususnya di saat Pilkada DKI Jakarta hari pemungutan suara 15 Februari 2017, total *mentions* terhadap setiap paslon yang bersaing mencapai ratusan ribu. Pengamat sosial, Ismail Fahmi, berharap agar

[10] "Pengaturan Lebih Rinci Dibutuhkan", *Kompas*, 20 Februari 2017.

selain terhadap *facebook* yang menyaring konten-konten negatif dan meningkatkan literasi penggunanya, pemerintah, melalui Dewan Pers dan Kementerian Informasi dan Komunikasi, juga harus ikut andil dan tegas dalam membuat edukasi dan kriteria bagi situs-situs media yang sehat *vis a vis* yang tidak sehat.[11]

Ada 4 (empat) tulisan dalam buku yang sedang kita baca saat ini. Tulisan pertama berjudul "Politik Siber dan Kedaulatan Negara," ditulis oleh Prayudi. Konteks politik siber biasanya menyangkut persaingan kekuasaan dalam pemilu dan kesetiaan warga bangsa terhadap kepentingan nasional. Hal ini menyebabkan bahwa politik siber terkoneksi kuat dengan masalah kedaulatan negara. Kontestasi antar-peserta pemilu, pihak penyelenggara, dan masyarakat, dalam konteks politik siber juga tidak lepas dari pengaruh dunia internasional. Birokrasi negara seolah tertinggal langkahnya oleh kecepatan gerak politik siber dengan segala dimensi luas yang dimiliki oleh siber itu sendiri. Momentum politik tertentu memiliki konsekuensi bagi ikatan kebangsaan dalam konteks memudarnya kedaulatan negara. Masalahnya adalah, bagaimana regulasi siber di tengah semakin memudarnya batas-batas antar-kedaulatan wilayah negara saat ini? Bagaimana alternatif solusi yang dapat dilakukan dalam mengatasi dampak negatif dari fenomena siber di tengah semakin kaburnya batas teritorial antar negara?

Penulis kedua yaitu Ahmad Budiman yang membahas masalah "Tata Kelola *Cyber Security* Pemerintah Daerah dalam Upaya Meningkatkan Pelayanan Publik." Pada hakekatnya, keberhasilan pelayanan publik yang dilakukan oleh penyelenggara pelayanan publik kepada masyarakat sangat ditentukan oleh seberapa besar kemanfaatan pelayanan publik yang dapat dirasakan masyarakat. Semakin cepat masyarakat memperoleh pelayanan publik sesuai dengan kebutuhan yang dimilikinya, akan menjadi salah satu indikator dari telah dilaksanakannya pelayanan publik dengan baik. Untuk itu perlu dibangun sebuah sistem informasi yang dapat membantu meningkatkan pelayanan publik penyelenggara

[11] "Hoaks Politik Dominan", *Kompas*, 16 Februari 2017.

kepada masyarakat. Upaya untuk memberikan pelayanan publik berbasis internet, sesungguhnya sejalan dengan program pemerintah dalam mengembangkan *e-government* di semua kelembagaan baik di tingkat pusat hingga ke tingkat daerah. Untuk itu tata kelola keamanan siber sangat diperlukan untuk tetap menjaga kepercayaan masyarakat dalam mendapatkan layanan publik dan layanan perijinan berbasis *online*. Hal inilah yang mendasari pertanyaan dalam tulisan ini, yaitu, bagaimana tata kelola keamanan siber dalam meningkatkan pelayanan publik kepada masyarakat?

Tulisan ketiga mengangkat judul "Peran *Cyber Security* dalam Mencegah Konflik Politik Masyarakat di Daerah" yang ditulis oleh Aryojati Ardipandanto. Media sosial seperti *Facebook, Twitter, Instagram,* dan lain-lain memang dapat membuat masyarakat semakin "melek" politik dan selalu dapat mengikuti perkembangan politik yang ada. Tetapi di sisi lain, kekuatan media sosial dapat dimanfaatkan untuk hal-hal berbahaya oleh pihak-pihak yang tidak bertanggung-jawab, terutama dalam momen menjelang Pemilu atau Pilkada. Hal yang berbahaya tersebut antara lain adalah bahwa media sosial dapat digunakan untuk menyebarkan *hoax* dalam perang kampanye di dunia maya. Bila masyarakat Indonesia tidak dibekali dengan kesadaran tentang pentingnya menggunakan media sosial dengan bijak dan hati-hati, tentunya ini akan sangat membahayakan kestabilan kehidupan bermasyarakat, berbangsa, dan bernegara. Hal ini dikarenakan *hoax* yang disebarkan di media sosial berdampak luas dan menimbulkan potensi konflik yang akibatnya bisa sangat menakutkan. Dalam memandang kondisi tersebut, tentunya logika kita akan mengarah pada pentingnya suatu sistem pengamanan arus informasi di media sosial. *Cyber security* yang dilaksanakan dengan profesional setidaknya akan menangkal dampak negatif dari penggunaan media sosial yang diarahkan pada timbulnya konflik oleh pihak-pihak tertentu yang memang ingin mengacaukan stabilitas politik negara.

Tulisan keempat ditulis oleh Aulia Fitri dengan judul tulisan "Kebijakan Siber Nasional di Era Globalisasi Informasi." Fenomena globalisasi informasi yang ditandai dengan pesatnya kemajuan teknologi, informasi, komunikasi dan interaksi lintas batas membawa dampak tersendiri terhadap keamanan suatu negara, khususnya di ruang siber. Perubahan ini juga mengakibatkan terjadinya pergeseran ancaman yang dihadapi oleh suatu negara, dari ancaman yang bersifat tradisional menjadi ancaman asimetris. Beberapa kasus mengenai serangan siber yang terjadi di beberapa negara termasuk Indonesia menandakan ketergantungan negara terhadap teknologi informasi membawa tantangan dan ancaman tersendiri. Besarnya potensi ancaman di ruang siber baik secara langsung maupun tidak langsung telah mendorong berbagai negara untuk melakukan penataan kebijakan di bidang siber. Indonesia belum memiliki kebijakan di bidang siber yang bersifat integratif, dengan kata lain kebijakan yang dijalankan masih bersifat sektoral. Oleh karena itu tulisan ini akan memetakan permasalahan kebijakan siber nasional di Indonesia dan merekomendasikan penerapan kebijakan siber yang terintegratif berdasarkan komparasi atas penerapan kebijakan siber dari berbagai negara di dunia.

Keempat tulisan dalam buku ini menjadi menarik untuk kita baca dan pahami isinya dengan cermat. Hal menarik dalam tulisan di buku ini yaitu adanya kesamaan pandangan dari semua penulis, bahwa siber dalam penerapannya di berbagai aspek akan dapat mempengaruhi pembangunan demokrasi di tanah air. Tentunya pembangunan demokrasi dimaksud adalah pembangunan demokrasi menuju pada arah yang lebih positif. Seberapa besar tujuan dari tulisan buku ini akan dapat tercapai, mari kita baca semua tulisan ini dengan seksama.

Editor

Epilog

Tantangan politik siber yang erat bagi penguatan integrasi bangsa harus dijawab dengan komitmen melahirkan regulasi siber di tingkat peraturan perundang-undangan yang sejalan dengan iklim globalisasi. Pada titik inilah, ketentuan yang tertuang dalam regulasi siber diharapkan benar-benar dapat diandalkan dalam rangka menjaga kedaulatan negara dan sekaligus menjaga hak privasi individu sebagai bagian dari demokrasi.

Pemerintah di tengah membanjirnya informasi, termasuk informasi sampah atau muatan terorisme atau sekedar radikalisme, jangan sampai berfikir untuk menutup siber. Langkah yang tepat adalah dilakukan pengaturan secara tegas dalam pengelolaan siber agar media digital digunakan sebagai bentuk kemajuan bangsa dalam pengelolaan kedaulatan negara secara kondusif melalui kehadiran pemerintahan yang baik (*good governance*).

Pada hakikatnya tata kelola keamanan siber ditujukan untuk membangun keamanan sistem informasi baik di tingkat daerah, maupun saat berintegrasi dengan sistem di tingkat nasinal. Keamanan Sistem Informasi Internal bertujuan untuk menjaga, *pertama* Kerahasiaan. Untuk melindungi data dan informasi dari penggunaan yang tidak semestinya oleh orang-orang yang tidak memiliki otoritas. Sistem informasi eksekutif, sumber daya manusia, dan sistem pengolahan transaksi, adalah sistem-sistem yang terutama harus mendapat perhatian dalam keamanan informasi. *Kedua,* Ketersediaan. Supaya data dan informasi perusahaan tersedia bagi pihak-pihak yang memiliki otoritas untuk menggunakannya. *Ketiga* Integritas. Seluruh sistem informasi harus memberikan atau menyediakan gambaran yang akurat mengenai sistem fisik yang mereka wakili.

Kunci untuk mengembangkan *cyber security* oleh Pemda adalah 'menuntaskan infrastruktur *online* dan mempersiapkan SDM nya', setelah itu dituntaskan, barulah Pemda akan mampu menata diri bagi pengembangan *cyber security.* Pemda harus memacu diri untuk menerapankan sistem pemerintahan berbasis *online.* Hanya dengan kemajuan dalam dunia maya lah maka perang *cyber* dapat ditangani oleh Pemda. Serangan-serangan dari pihak-pihak yang tidak bertanggung jawab dalam dunia *cyber* yang mengedepankan sistem memecah-belah persatuan dan kesatuan masyarakat, harus diimbangi dengan kemampuan Pemda dalam menguasai teknologi *online,* terutama *cyber security.* Tanpa itu, tentu Pemda akan menjadi "bulan-bulanan" dari para kriminal *cyber* yang demi kepentingan pribadi atau golongannya semata, bisa menghancurkan kerukunan antar-warga.

Semakin pesatnya perkembangan teknologi informasi berdampak pada resiko ancaman di ruang siber yang mendorong negara untuk menata ulang kebijakan keamanan dalam merespon ancaman siber yang semakin nyata. Pencapaian kekuatan siber bergantung pada strategi dan kebijakan suatu negara dalam mengembangkan keamanan siber. Indonesia belum memiliki kebijakan khusus untuk mengelola dan menangani keamanan siber secara terintegrasi.

Terdapat empat permasalahan utama dalam implementasi kebijakan keamanan siber di Indonesia. Pertama, pemahaman mengenai keamanan siber yang belum terintegrasi. Kedua, kurangnya regulasi keamanan siber. Ketiga, lemahnya koordinasi dan kerjasama antar-lembaga. Keempat, perlunya peningkatan kapabilitas sumber daya manusia. Penetapan regulasi yang tepat dan kerjasama dengan semua pihak baik pemerintah, sektor swasta dan masyarakat sipil, dapat menjadi kunci dalam menghadapi tantangan dunia siber yang semakin kompleks.

Indeks

Profil Penulis

Ahmad Budiman, Lahir di Jakarta, 22 April 1969. Memperoleh gelar sarjana bidang komunikasi dari Institut Ilmu Sosial Ilmu Politik (IISIP) Jakarta tahun 1993 dan Magister Penelitian dan Evaluasi Pendidikan dari Universitas Muhammadiyah Prof. DR. HAMKA (2004). Jabatan saat ini adalah Peneliti Madya IV/b untuk bidang kepakaran komunikasi politik. Menjadi tim asistensi untuk pembahasan RUU tentang Keterbukaan Informasi Publik, RUU Rahasia Negara, RUU Intelijen Negara, RUU Penyiaran, RUU Hukum Disiplin Militer dan RUU Radio Televisi Republik Indonesia. Tulisan yang telah dibukukan di antaranya berjudul: "Bunga Rampai Keterbukaan Informasi Publik", dan "Aspirasi Masyarakat dan Respons DPR RI". Tulisan dalam bagian dari buku di antaranya "Peningkatan Citra Bangsa melalui Kemandirian Industri Pertahanan", "Optimalisasi Pengelolaan Keterbukaan Informasi Publik di DPR RI", "Kesiapan Lembaga Penyiaran Melaksanakan Digitalisasi Penyiaran", "Tata Kelola Keterbukaan Informasi di Era Pemerintahan Elektronik", dan "Urgensi Sistem Keamanan Telekomunikasi Bagi Peningkatan Kualitas Komunikasi Organisasi Pemerintah Daerah". Juga tulisan dalam jurnal ilmiah di ataranya berjudul "Pola Komunikasi Pembangunan Pada Daerah Pemekaran" dan "Mekanisme Pengaduan Masyarakat ke DPR RI".
Email: a.budiman69@gmail.com

Aryojati Ardipandanto, menyelesaikan pendidikan sarjana Ilmu Pemerintahan dari Universitas Langlangbuana (Yayasan Bhrata Bhakti Polri) Bandung pada tahun 2003. Penelitian-penelitan yang dilakukannya terkait dengan masalah-masalah pemerintahan, politik, dan industri pertahanan. Ia pernah menjadi Tim Asistensi Penyusunan Rancangan Undang-Undang tentang Industri Pertahanan, yang sudah

disahkan menjadi UU No. 16 Tahun 2012 tentang Industri Pertahanan. Selain itu, penulis adalah anggota tim Pidato Sekretariat Jenderal DPR RI sejak tahun 2011 hingga sekarang. Ia terlibat pula sebagai anggota Tim Buku Kinerja Tahunan DPR RI.

Email: aryojati.ardipandanto@gmail.com

Prayudi, bekerja di Sekretariat Jenderal DPR RI sejak tahun 1990. Peneliti Bidang Politik Pemerintahan Indonesia di Pusat Pengkajian, Pengolahan Data dan Informasi Sekretariat Jenderal (P3DI Setjen DPR RI). Aktif melakukan beberapa penelitian lapangan dan riset kepustakaan terkait masalah-masalah sosial politik. Anggota Dewan Redaksi Jurnal *Kajian* P3DI Setjen DPR RI. Beberapa kegiatan lainnya, antara lain pernah ikut sebagai anggota Tim Asistensi pembahasan Rancangan Undang-Undang (RUU) tentang Penyelenggaran Pemilu (2007), RUU tentang Bahan Kimia dan Larangan Penggunaan Bahan Kimia Sebagai Senjata Kimia (2008), RUU tentang Rencana Pembangunan Jangka Panjang Nasional tahun 2005-2025 (2006), RUU tentang MPR, DPR, DPD, DPRD (2008-2009), RUU tentang Intelijen (2011) RUU tentang Desa (2013), dan RUU tentang Pemda (2013-2014).

Email: prayudi_pr@yahoo.com

Aulia Fitri, lahir di Bandung, 19 Mei 1988. Menyelesaikan Pendidikan S1 Hubungan Internasional di Universitas Katolik Parahyangan pada tahun 2010 dan Pendidikan S2 Manajemen Pertahanan di Universitas Pertahanan pada tahun 2015. Saat ini menjabat sebagai Calon Peneliti Bidang Politik Dalam Negeri untuk kepakaran Studi Pertahanan di Pusat Penelitian Badan Keahlian DPR RI. Kajian-kajian yang telah dilakukan penulis adalah mengenai Industri Pertahanan, Reformasi Sektor Keamanan, Terorisme dan Kerjasama Pertahanan.

Email. auliarosadi@gmail.com