Dharmasisya

Volume 1 *NOMOR 2 JUNI 2021* Article 29

July 2021

PERAN NEGARA D ALAM MENJAGA KEDAULATAN PADA RUANG MAYA (CYBERSPACE) SEBAGAI UPAYA PERLINDUNGAN TERHADAP MASYARAKAT

Nurharis Wijaya
nurharislaw@gmail.com

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-1060
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

PERAN NEGARA D ALAM MENJAGA KEDAULATAN PADA RUANG MAYA (*CYBERSPACE*) SEBAGAI UPAYA PERLINDUNGAN TERHADAP MASYARAKAT

Nurharis Wijaya
Fakultas Hukum Universitas Indonesia
Korespodensi: nurharislaw@gmail.com

Abstrak

Perkembangan teknologi internet memiliki potensi untuk mendorong pertumbuhan ekonomi suatu negara. Di sisi lain, teknologi internet juga turut meningkatkan jumlah dan bentuk ancaman terhadap kedaulatan suatu negara di dunia maya. Kedaulatan di dunia maya menjadi topik penting dalam pembahasan keamanan nasional maupun internasional. Dalam konteks Definisi ruang tidaklah lagi relevan jika dipandang hanya terbatas kepada Wilayah Darat, Laut, dan Udara. Perkembangan Zaman kian membuai Negara dengan kemanjaan akan kemudahan dalam mengakses Teknologi Informasi, yang tentunya tanpa berhasil mengambil peran bahwa Ruang-Maya juga merupakan sebagai wilayah yurisdiksi mutlak sebagai bagian kedaulatan daripada suatu Negara, sehingga abstain nya Negara dalam memaknai Ruang-Maya perlu dikaji ulang oleh negara, bukan hanya sebatas regulasi bagi pengguna ruang maya, akan tetapi Ruang-maya (Cyberspace) merupakan suatu wilayah yang harus dikelola dan dimanfaatkan sendiri secara mandiri oleh Negara serta dituangkan kembali (amandemen) UUD 1945.
Kata kunci: keamanan *cyber*, kedaulatan Negara, keamanan nasional, tata kelola pemerintahan, perlindungan terhadap masyarakat.

Abstract

Development of Internet technology has the potential to boost economic growth of a country. On the other hand, Internet technology also increases the amount and form of threat to the sovereignty of a state in the virtual world. Sovereignty in cyberspace become an important topic in the discussion of national and international security. In the context of the definition of space was no longer relevant in the light confined to the Regional Land, Sea, and Air. Developments Period increasingly cradles State with indulgence will ease in accessing information technology, which is certainly without successfully taking on the role that space-Maya also as jurisdictions absolute as part of sovereignty rather than a State, so that abstentions his State of understanding of space-Maya should be reexamined by countries, not merely the regulation of virtual space, but the space-virtual (Cyberspace) is an area that must be managed and utilized its own independently by the state and poured back (amendment) 1945.
Keyword: cyber security, national sovereignty, national security, governance, protection of the public.

I. PENDAHULUAN

Negara sebagai organisasi yang berdaulat tergambar dalam konstitusinya, secara substansial kekuasaan yang diberikan kepada negara dalam realitas hubungan sosial masyarakat dipegang oleh penguasa yang mendapat legitimasi untuk mewujudkan cita-cita dan tujuan negara tersebut. Kekuasaan itu tidaklah mudah terwujud dalam dinamika kehidupan, dalam konteks ini peran negara dalam berbagai pengaruh, seperti ideologi global telah mengalami kelemahan.

Perkembangan peranan negara dari mulai teori klasik sampai kontemporer ditandai dengan dinamika yang selalu merupakan persoalan kompleks. Pada awal abad ke 21 pembicaraan soal peranan negara masih mengenai tujuan dan kegiatan negara yang bertumpu pada keleluasaan intervensi dalam hubungan negara dengan individu, kepentingan dan kelas sosial yang terorganisasi.

Realitas perbedaan kekuatan negara pada era globalisasi telah membuat negara yang "kecil atau lemah" makin sulit menghindari kondisi saling ketergantungan yang cenderung merugikan negara lemah/kecil. Ketergantungan itu meliputi komponen, seperti : tingkat dan kualitas perdagangan, kepentingan geografis dan geostrategis, tingkat perkembangan budaya dan teknologi, perbedaan ekonomi dan derajat ekslusivitas sistem ekonomi negara dan

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-970
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

konstelasi politik kekuatan negara-negara besar (Stojanovic).[1]

Dalam nomenklatur hukum internasional, kedaulatan negara menjadi diktum primer yang demikian penting. Tiap-tiap negara di dunia diakui eksistensinya berkat kedaulatan yang dimiliki oleh negara-negara tersebut. Jika dikatakan bahwa suatu negara berdaulat, maka yang dimaksud adalah bahwa negara itu mempunyai suatu kekuasaan tertinggi terhadap wilayah tertentu sebangun dengan kewenangan negara untuk menerapkan hukum di wilayah tertentu yang dikuasainya, yang disebut sebagai yurisdiksi.

Sejak kelahiran negara modern (*modern state*) pada abad ke enambelas dan ke-tujuh belas di Eropa, kedaulatan negara terus-menerus diperteguh Perjanjian Westphalia pada 1648 menandai otonomi negara-negara atas "negara induk" Imperium Romawi. Saat itulah negara-negara modern berdaulat mulai terbentuk. Puncak dari narasi historis kedaulatan negara tersebut adalah pada penyelenggaraan konferensi Internasional Ketujuh Negara-negara Amerika di Montevideo, Uruguay.

Dalam konferensi internasional yang digelar pada 26 Desember 1933 itu, negara-negara peserta merumuskan dokumen hukum yang masyhur sebagai Konvensi Montevideo (*convention on Rights and Duties of States,* 1933). Konvensi tersebut mengatur sejumlah unsur yang mesti dimiliki oleh negara berdaulat, yakni (1) rakyat yang tetap, (2) wilayah yang terbatas, (3) pemerintah, dan (4) kemampuan untuk menjalin hubungan dengan negara-negara lain.

Wilayah atau ruang yang berbatas adalah unsur penting yang mesti dimiliki oleh suatu negara. Tanpa mempunyai wilayah tertentu, sebuah negara hanya nonsens belaka. Sebab, terhadap dan melalui wilayahlah negara menegakkan kekuasaan tertingginya; menjalankan yurisdiksi dan menerapkan hukum nasionalnya. Wilayah selama ini dipahami dalam tiga dimensi, yaitu wilayah daratan, lautan, dan ruang udara. Dengan demikian, dapat juga dikatakan bahwa kedaulatan negara dibatasi oleh tiga dimensi tersebut.

Perkembangan sains dan teknologi telah menyebabkan pelbagai perubahan di bidang politik, ekonomi, sosial, dan budaya. Salah satu perkembangan sains dan teknologi yang tengah melaju dengan sangat pesat adalah perkembangan di bidang teknologi informasi. Itu, antara lain, ditandai dengan kelahiran internet, secara keilmuan disebut ruang-maya (*cyberspace*). Dimensi kedaulatan negara pun meluas: tidak lagi terdiri dari wilayah daratan, lautan, dan ruang-udara, melainkan juga Ruang-maya. Ruang-maya tercitra dari internet telah menciptakan suatu rezim hukum baru yang dikenal dengan hukum internet (*the law of the internet*), hukum ruang-maya (*cyberspace*), atau hukum telematika.[2]

II. PEMBAHASAN

A. Praktek Penegakan *Cyber Sovereignty* strategi Pemerintah Amerika Serikat tentang Kedaulatan Dunia Maya

Pemerintah Amerika Serikat memandang bahwa dunia maya sebagai wahana dimana setiap individu memiliki perlindungan privasi, hak asasi manusia, dan kebebasan berekspresi. Oleh karena itu Amerika Serikat akan melakukan segala upaya untuk mencegah perusakan infrastruktur jejaring dan pencurian informasi atau data rahasia dengan berdalih pada kewajiban untuk melindungi hak-hak warga negaranya. Untuk mencapai hal tersebut, pemerintah Amerika Serikat merasa perlu untuk memperluas pengaruhnya di dunia maya.

Meluasnya pengaruh Amerika Serikat di dunia maya terjadi sejak tahun 2013, dimana praktiknya dapat digambarkan dalam beberapa hal. Pertama, adanya pembelaan atas tindakan

[1] Peranan Negara Dalam UUD 1945, https://www.esaunggul.ac.id/peranan-negara-dalam-undang-undang-dasar-1945/, diakses pada tanggal 14 November 2019.

[2] AP Edi Atmaja, "*Kedaulatan Negara Di Ruang Maya: Kritik UU ITE Dalam Pemikiran Satjipto Rahardjo*", Jurnal Opinio Juris. Vol. 16. Ed. Mei-September 2014, hlm. 48-50.

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-1060
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

pengawasan jejaring melalui kegiatan intelijen PRISM berdasarkan pada kebutuhan akan penegakan kedaulatan dan keamanan nasional. Pengungkapan keberadaan PRISM, dengan berdasarkan pada kebutuhan akan penegakan kedaulatan dan keamanan nasional. Pengungkapan keberadaan PRISM berasal dari informasi yang diberikan oleh mantan karyawan *Central Intelligence Agency* (CIA) bernama Edward Snowden kepada media Eropa dan Amerika. Sebuah artikel yang diterbitkan oleh harian *The Washington Post* pada tanggal 6 juni 2013, mengungkapkan kerjasama intelijen pemerintah Amerika Serikat dan Inggris untuk mendapatkan data pengguna dari perusahaan-perusahaan internet di Amerika Serikat. Artikel tersebut menyebutkan bahwa Badan Amerika Serikat, *National Security Agency* (NSA) menggunakan dan mengumpulkan sinyal-sinyal intelijen dari perusahaan-perusahaan tersebut melalui program yang disebut PRISM. Karena peran penting PRISM dalam memberikan data bagi kegiatan intelijen Amerika Serikat, PRISM disebut-sebut sebagai sumber intelijen yang paling penting bagi NSA.[3] Setelah kegiatan PRISM terungkap, mantan Direktur NSA Michael Hayden berkilah bahwa pengumpulan data yang didapat dari pemantauan dalam dunia maya perlu dilakukan sebagai upaya intelijen demi mempertahankan keamanan nasional.[4]

Kedua, pemerintah Amerika Serikat melakukan berbagai operasi di dunia maya untuk memastikan keamanan nasional secara maksimal, termasuk di antaranya menerapkan upaya pencegahan sebagai bagian dari strategi pertahanan nasional. Pemerintah Amerika Serikat berlindung di balik hak untuk mempertahankan diri sebagai alasan untuk melakukan berbagai operasi di dunia maya secara bebas. Hal ini menyiratkan bahwa pemerintah Amerika Serikat memiliki hak untuk menyerang suatu sumber ancaman apabila keamanan Amerika Serikat dianggap berada di bawah ancaman. Pada April 2015, Departemen Pertahanan Amerika Serikat menyetujui konsep Strategi Pertahanan Dunia Maya yang secara eksplisit memiliki wewenang untuk memblokir atau mengendalikan semua jenis konflik melalui jejaring internet.[5] Dalam hal menggunakan hak untuk membela diri, pemerintah Amerika Serikat berpendapat bahwa fasilitas jejaring yang ada di negara lain dapat menjadi target yang sah. Sebuah kasus yang terjadi pada juli 2015 menunjukkan bagaimana pemerintah Amerika Serikat secara terbuka mengakui serangan terhadap jejaring komputer yang berada di China sebagai tindakan balasan atas peretasan data 20 juta karyawan pemerintah Amerika Serikat.[6]

Ketiga, adanya niat pemerintah Amerika Serikat untuk mempertahankan kendali atas proses pengalihan wewenang ICANN. Pada tanggal 17 Agustus 2015, direktur lembaga telekomunikasi dan informasi dari Departemen Perdagangan Amerika Serikat (NTIA) mengumumkan rencana untuk memperpanjang kontrak dengan ICANN hingga 2016.[7] Proses pengalihan atas pengelolaan *file root* dan server akan dilakukan oleh NTIA dan perusahaan

---

[3] Greenwald dan MacAskill, *NSA Prism program taps in to user data of Apple, Google and Others*, http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf, diakses 1 Februari 2020.

[4] M. Hayden, *Ex-NSA chief: safeguards exist to protect Americans' privacy*, http://edition.cnn.com/2013/08/01/opinion/hayden-nsa-surveillance/, diakses 2 Februari 2020.

[5] L. Schmidt, *Perspective on 2015 DoD Cyber Strategy*, SantaMonica CA: RAND Corporation, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA621794, diakses 2 Februari 2020.

[6] D. Sanger, 2015, *US decides to retaliate against China'shacking,* http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html, diakses 2 Februari 2020.

[7] NTIA, Department of Commerce, *Verisign/ICANN proposal in response to NTIA request root zone administrator proposal related to the IANA Functions Stewardship Transition*, https://www.ntia.doc.gov/files/ntia/publications/root_zone_administrator_proposalrelat dtoiana_functionsstefinal.pdf, diakses 2 Februari 2020.

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-970
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

swasta, VeriSign, secara independen. Namun, dokumen pelaksanaan proses tersebut juga mengungkapkan bahwa terdapat masa percobaan untuk jangka waktu 3 bulan dalam proses pengalihan tersebut, NTIA menemukan adanya data hasil pengalihan yang mencurigakan, proses pengalihan akan diulang dan dimulai dari awal.

Dengan sikap yang ditunjukkan oleh pemerintah Amerika Serikat di atas, dapat dilihat bahwa, diakui atau tidak, mereka berusaha mengahalangi upaya penerapan sistem, kebijakan atau strategi negara lain berdasarkan prinsip kedaulatan. Sebaliknya, pemerintah. Sebaliknya, pemerintah Amerika Serikat justru bermaksud memperluas lingkup kedaulatannya di dunia maya.

1. Strategi Pemerintah China tentang Kedaulatan Dunia Maya

Sejak 2013, keamanan dunia maya telah menjadi salah satu isu yang paling penting dari agenda strategi keamanan nasional china, terutama setelah berdirinya satuan tugas di bidang keamanan internet dan telekomunikasi yang dipimpin langsung oleh Presiden Xin Jinping untuk meghadapi tantangan dan ancaman yang meningkat di dunia maya. Pemerintah China menetapkan tujuan yang signifikan di dunia maya yaitu hendak membangun China menjadi kekuatan baru di dunia maya.[8] Strategi utama yang digunakan adalah untuk memastikan bahwa China berkembang dari pemasok teknologi dan kemudian menjadi kekuatan besar di dunia maya. Hal ini berarti China tidak hanya memiliki kemampuan untuk bertahan dari kemungkinan ancaman melaui dunia maya, tetapi juga mampu mempengaruhi penyusunan aturan-aturan dalam pengelolaan dunia maya. Penegakan kedaulatan dunia maya menempati posisi sentral dari strategi keamanan dunia maya pemerintah China. Bahkan dalam Undang-undang Keamanan Nasional China disebutkan bahwa perlindungan kedaulatan di dunia maya adalah saah satu tugas dalam upaya menjaga keamanan nasional.[9]

Untuk menjelaskan pengertian tentang kedaulatan dan bagaimana upaya untuk menegakkan kedaulatan China di dunia maya dari Beijing, pemerintah China menjabatkan kedaulatan dunia maya dalam beberapa komponen kunci agar definisinya bisa dipahami. Bagian pertama kedaulatan Negara untuk mengelola arus informasi di dalam wilayah itu. Kedua, adalah bahwa setiap Negara memiliki wewenang untuk membuat kebijakan mengenai dunia maya secara independen. Ketiga adalah bahwa setiap Negara harus memiliki kedudukan dan hak yang sama untuk berpartisipasi dalam proses pengambilan keputusan mengenai aturan, norma, atau kode etik yang mengatur dunia maya. Terakhir, pengakuan atas kedaulatan harus menjadi satu prinsip panduan yang paling penting untuk menangani isu-isu internasional yang terkait dengan dunia maya.[10]

Alasan utama mengapa pemerintah China merasa perlu untu mempertahankan kedaulatannya di dunia maya adalah ketika pada tahun 2009 pemerintah Amerika Serikat mulai meggunakan internet sebagai sarana diplomasi dan pertukaran informasi untuk mendorong perubahan rezim secara damai di seluruh dunia. Pemerintah China menganggap bahwa strategi ofensif yang diterapkan Amerika Serikat akan digunakan untuk mengendalikan atau mengubah sistem dan jejaring informasi global demi kepentingan Amerika Serikat, bahkan Amerika Srikat

[8] S. Yi, "Transform and construction: the design of national cyber security strategy and the capacity build in a post-Snowden age", *China Information Security*, Vol. 5, 2014, hlm. 41–43.

[9] D. M. Lampton, "Xi Jinping and the National Security
Commission: policy coordination and political power",
Journal of Contemporary China, Vol. 24, No. 95, 2015, hlm.759-777.

[10] *Ibid*

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-1060
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

dikhawatirkan dapat membuat atau mengendalikan eskalasi konflik di suatu Negara.[11] Oleh karena itu pemerintah China semakin menaruh perhatian khusus pada upaya penegakan kedaulatan dan hukum di dunia maya untuk memastikan keamanan nasional di masa depan. Pemerintah China menggunakan pola pikir yang berbeda dengan Amerika Serikat untuk menyusun norma atau kode etik baru dalam pemerintahan dunia maya. Hal ini tercermin dari sikap China yang lebih memilih model pengelolaan *multilateral* daripada *multi-stakeholder*. Dengan model *multilateral,*peraturan dan pengelolaan infrastruktur kunci, yaitu DNS dan sistem *file root,* yang menjalankan operasi dunia maya seharusnya dibahas oleh di tingkat petinggi pemerintahan antar Negara saja. Pemerintah China berpendapat bahwa model *multi-stakeholder* akan digunakan oleh Amerika Serikat, yang telah memiliki keunggulan di bidang teknologi informasi, untuk memperluas pengaruhnya di dunia maya, dan menjadikannya dasar untuk mengahalang-halangi Negara-negara lain yang hendak melindungi kepentingan nasional mereka di dunia maya. Kekhawatiran atas penyalahgunaan model *multi-stakeholder* semakin bertambah dengan dilirisnya laporan dari *Working Group on Internet Governance* (WGIG) pada tahun 2005, yang menegaskan bahwa administrasi dan pengelolaan zona *file root* dari DNS dikendalikan oleh pemerintah Amerika Serikat secara sepihak.[12]

Sejak 2013, pemerinttah China semakin giat mengupayakan perlindungan kedaulatan dunia maya sebagai prioritas utama dalam strategi keamanan nasional. Tantangan yang dihadapi saat ini adalah pengembangan teknologi canggih secara tepat, sehingga China dapat menjadi lebih aktif dan partisipatif dalam proses penciptaan kode etik pengelolaan dunia maya.

2. Strategi Pemerintah Indonesia tentang Kedaulatan Dunia Maya

Pemerintah Indonesia telah memiliki beberapa pedoman yang dapat menjadi panduan dan paying hukum dalam upaya penegakan kedaulatan di dunia maya, Undang-undang No. 19 Tahun 2016 tentang perubahan atas Undang-undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah No. 82 Tahun 2012 (PP 82/2012) tentang Penyelenggaraan Sistem dan Elektronik merupakan dasar pengelolaan pertahanan dan keamanan nasional di dunia maya. Dengan kedua peraturan tersebut, penyelenggaraan sistem elektronik di Indonesia termasuk jejaring telekomunikasi dan internet wajib menndukung pembangunan pertahanan dan nasional secara semesta dan berkesinambungan.

Secara spesifik, pasal 15 UU ITE mengatur bahwa Penyelenggara Sistem Elektronik harus menyelenggarakan sistem elektroniknya secara aman, andal, dan bertanggung-jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. Hal ini berarti bahwa seluruh penyelenggara sistem elektronik, terlepas apakah sistem itu digunakan untuk kepentingan pemerintahan, komersial, atau pribadi harus memastikan pengoperasian sistem berjalan secara andal, aman dan bertanggung jawab. Selanjutnya, PP 82/2012 memberikan pedoman bagaimana Penyelenggara Sistem Elektronik menyelenggarakan sistemnya secara andal, aman, dan beratanggung jawab sebagaimana diamanatkan oleh UU ITE. Kemudian PP 82/2012 mengatur bahwa Penyelenggara Sistem Elektronik harus menjamin standar yang tinggi terhadap lima komponen, yaitu: Perangkat keras Perangkat lunak, Tenaga ahli, Tata kelola dan Pengamanan.

Dengan adanya pedoman tersebut, diharapkan Sistem Elektronik yang ada di

[11] K. Lieberthal dan W. Jisi, "Addressing U.S.-China Strategic Distrust", *John L. Thornton China Center Monograph Series*,Number 4, http://yahuwshua.org/en/Resource-584/0330_china_lieberthal.pdf, diakses 3 Februari 2020.

[12] C. de Bossey, Report of the Working Group on Internet Governance,http://www.wgig.org/docs/WGIGREPORT.pdf, diakses 3 Februari 2020.

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-970
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

Indonesia dapat menjadi satu kesatuan sistem yang kokoh, andal dan aman secara semesta atau secara nasional. Hal ini selaras dengan prinsip pertahanan nasional yaitu bahwa pertahanan dilakukan secara semesta. Menurut Pasal 1 butir 1 Undang-undangNo. 3 Tahun 2002 (UU Pertahanan Negara) pertahanan negara adalah segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara. Pasal 1 butir 2 UU Pertahanan Negara menyebutkan bahwa, sistem pertahanan Negara Indonesia bersifat sistem pertahanan semesta, yaitu melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainnya, serta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut untuk menegakkan kedaulatan negara, keutuhan wilayah, dan keselamatan segenap bangsa dari segala ancaman. Pengelolaan Sistem Elektronik yang diselenggarakan di Indonesia juga diharapkan dapat menjadi upaya pertahanan negara sebagai usaha membangun dan membina kemampuan, daya tangkal negara dan bangsa, serta menanggulangi setiap ancaman, sebagaimana tercantum pada Pasal 6 UU Pertahanan Negara tersebut.

Meskipun UU No. 19 Tahun 2016 tentang perubahan atas UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah No. 82 Tahun 2012 (PP 82/2012) tentang Penyelenggaraan Sistem dan Elektronik merupakan dasar pengelolaan pertahanan dan keamanan nasional di dunia maya, telah meletakan dasar pengaturan untuk membangun sistem Keamanan dan Pertahanan dunia maya yang bersifat semesta, diperlukan kontrol, koordinasi, dan pengawasan secara strategis dan efektif. Dalam hal ini, Kementerian Komunikasi dan Informatika (Kemenkominfo) sangat berperan dalam membangun dan mengembangkan keamanan dan pertahanan dunia maya secara menyeluruh.

Kemenkominfo bertanggung jawab untuk membantu Presiden Republik Indonesia melaksanakan segala hal yang berkaitan dengan teknologi telekomunikasi dan informasi. Kemenkominfo juga bertanggung jawab dalam penatakelolaan *e-Government*, *e-Business*, dan keamanan informasi, peningkatan teknologi dan infrastruktur aplikasi informatika serta pemberdayaan informatika (di bawah pengawasan Direktorat Jenderal Aplikasi Informatika), dan penentuan kebijakan dan standardisasi teknis perangkat pos dan informatika (di bawah pengawasan Direktorat Jenderal Sumber Daya, Pos dan Informatika).[13] Secara umum, kedua Direktorat tersebut bertanggung jawab dalam merumuskan dan melaksanakan kebijakan, serta memberikan bimbingan teknis yang terkait dengan bidang mereka. Dalam Direktorat Jenderal Aplikasi Informatika, bagian yang khusus bertanggung jawab terhadap perumusan kebijakan tentang perlindungan dan keamanan data-data privasi adalah Direktorat Keamanan Informasi. Mereka bertanggung jawab di bidang tata kelola, teknologi dan infrastruktur, monitoring dan evaluasi, penanganan insiden, penyidikan dan penindakan, dan budaya keamanan informasi, sertifikasi kelaikan untuk Penyelenggara Sistem Elektronik.[14] Kemenkominfo juga bertanggung jawab untuk melakukan pemantauan dan penanganan insiden keamanan informasi di instansi-instansi Pemerintah melalui sebuah tim yang bernama *Government Computer Security Incident Response Team* (Gov-CSIRT).[15] Sedangkan, upaya pengamanan dan penanganan insiden keamanan jejaring komunikasi berbasis internet bagi pengguna umum menjadi tugas dari *Indonesia Security Incident Response Team on Infrastruktur Internet/Coordination*

[13] Direktorat Jenderal Sumber Daya, Pos dan Informatika Kemekominfo, Tugas dan fungsi, http://kominfo.go.id/index.php/node/711/Tugas+dan+Fungsi, diakses 3 Feburari 2020.

[14] Direktorat keamanan informasi Kemenkominfo, http://aptika.kominfo.go.id/index.php/profile/direktoratkeamana-informasi, diakses 3 Februari 2020.

[15] GovCISRT, Profil, http://govcsirt.kominfo.go.id/tentangidgovcert/profil, diakses 3 Februari 2020.

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-1060
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

Centre (id- SIRTI/CC) yang berada di bawah pengawasan Direktorat Jenderal Penyelenggaran Pos dan Informatika.[16] Pemerintah Indonesia juga memiliki lembaga pemerintah nonkementerian yang bergerak di bidang pengamanan informasi rahasia negara, bernama Lembaga Sandi Negara (Lemsaneg).

Dalam penanganan kejahatan di dunia maya, lembaga ini dibantu oleh Kemkominfo serta berkoordinasi dengan instansi pemerintah lainnya seperti Kepolisian Negara Republik Indonesia, Tentara Nasional Indonesia, Kementerian Luar Negeri, Kementerian Dalam Negeri, dan Kementerian Pertahanan.[17] Selain dari sektor pemerintah, para pemerhati masalah keamanan informasi di Indonesia membentuk suatu komunitas yang dinamai *Indonesian Computer Emergency Response Team* (ID-CERT) sebagai pusat koordinasi keamanan informasi berbasis komunitas masyarakat yang independen untuk membantu menangani insiden yang melibatkan pihak Indonesia dan luar negeri.[18]

Paparan diatas menunjukkan bahwa meskipun upaya penegakan kedaulatan telah dilakukan dan didelegasikan pada badan-badan keamanan informasi yang terkait, beberapa badan tampaknya memiliki tugas-tugas yang serupa namun bertanggung jawab kepada atasan yang berbeda. Fakta bahwa setiap tim tidak bertanggung jawab langsung kepada satu otoritas dapat menyebabkan terjadinya tumpang tindih kewenangan antara mereka. Disamping itu, landasan hukum tentang keamanan dan pertahanan informasi yang ada di Indonesia saat ini cenderung bersifat reaktif. Akibatnya, ancaman yang muncul dari perkembangan modus-modus baru dari kejahatan informasi atau pelanggaran kedaulatan dunia maya sulit untuk dicegah.

Penegakan kedaulatan dunia maya di Indonesia kini diuji dengan hadirnya berbagai aplikasi bisnis berbasis konten, *over-the-top content* (OTT), yang makin marak digunakan oleh masyakat Indonesia. Layanan OTT, seperti WhatsApp, YouTube, Facebook, dan Twitter, tersebut dapat beroperasi dan mendapatkan keuntungan finansial di Indonesia tanpa perlu membuat badan hukum yang tunduk pada perundang-undangan yang berlaku di Indonesia. Ditambah lagi, keberadaan server dan pengelolaan aplikasi, yang berada di luar Indonesia, menjadi ancaman bagi perlindungan pelayanan dan jaminan keamanan data konsumen Indonesia. Upaya untuk menegakkan kedaulatan Indonesia di dunia maya tentu perlu dilakukan dengan cara mendukung terbentuknya aturan dan tatanan kedaulatan dunia maya yang lebih pasti.

B. Faktor Penghambat Pembentukan Tata Kelola Dunia Maya Global

1. Aspek Teknis

Sejak tahun 1990-an, perkembangan teknologi informasi, internet dan dunia maya telah melaju dengan pesat. Hal tersebut semakin memunculkan ketimpangan sumber daya dan kemampuan dalam pengembangan teknologi. Kesenjangan teknologi, inovasi, penelitian dan pengembangan ilmu pengetahuan, menyebabkan negara maju dan berkembang memiliki perbedaan dalam kemampuan adopsi teknologi dunia maya. Akibatnya, Negara-negara berkembang sering terpinggirkan di dunia maya, dimana partisipasi pemerintah, masyarakat sipil, dan industri Internet dari negara-negara berkembang seringkali kurang terwakili dalam pembahasan pengelolaan dunia maya. Marjinalisasi tersebut sangat mengkhawatirkan karena dapat memperlemah status negara-negara berkembang di dunia nyata. Sebaliknya, negara-

[16] ID SIRTII, struktur organisasi, http://www.idsirtii.or.id/halaman/tentang/strukturorgansasi.html., diakses 3 Februari 2020.

[17] Lembaga Sandi Negara, Tugas dan Fungsi, http://www.lemsaneg.go.id/index.php/profil/tugas-dan-fungsi/, diakses 3 Februari 2020.

[18] ID CERT, Profil, http://www.cert.or.id/tentang-kami/id/, diakses 3 Februari 2020.

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-970
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

negara maju, terutama mereka yang memiliki kemampuan lebih dalam industri dan teknologi, menjadi pelaku utama dan makin berkuasa di dunia maya. Hambatan pembentukan tata kelola dunia maya karena adanya ketimpangan antara kemampuan adopsi teknologi di antara negaranegara tersebut, tercermin pada aspek teknis berikut ini.

Aspek pertama adalah distribusi pengguna internet dilihat dari sisi geografis. Meskipun jumlah total kelompok pengguna internet di seluruh dunia meningkat, proporsi relatif dari kelompok pengguna dan klasifikasi kelompok pengguna internet berbeda-beda secara signifikan di masing-masing negara. Secara keseluruhan, proses ekspansi pemakaian internet memang bergerak dari negara maju ke negara berkembang.

Menurut statistik dari berbagai lembaga penelitian, termasuk ITU,[19] jumlah total pengguna internet di seluruh dunia mencapai lebih dari 2,5 miliar, yang berarti hampir 40% dari populasi global. Sejak tahun 2006, jumlah pengguna Internet dari negara-negara berkembang makin bertambah, dimana penetrasi internet di negara-negara berkembang tersebut mencapai kurang lebih dari 40%.[20] Namun demikian, hal ini tidak berarti bahwa penetrasi internet di Negara-negara berkembang telah berjalan lancar.

Statistik menunjukkan bahwa dibandingkan dengan Amerika dan Eropa, di mana penetrasi internet telah mencapai 80%, 85% populasi dunia yang belum terkoneksi dengan internet berasal dari negara-negara berkembang.[21]

Kedua, adanya kesenjangan fasilitas yang berhubungan dengan transmisi dan distribusi data digital di antara negara-negara maju dan berkembang. Sebagai contoh, sistem kabel bawah laut adalah infrastruktur utama yang mendukung pengembangan jejaring dunia maya. Penanaman kabel bawah laut yang melintasi samudra, *Transatlantic Telecommunications Cable* (TAT-8), telah melayani kebutuhan komersial sejak bulan Desember 1988.

Hingga tahun 2008, berbagai perusahaan dari Amerika dan Eropa memonopoli pasar kabel serat optic global. Amerika dan Eropa menjadi titik sentral atau titik penghubung utama untuk semua kabel bawah laut yang dibangun. Meskipun sejak 2008, beberapa perusahaan telah mengalihkan fokus investasi ke wilayah dengan infrastruktur terbatas, seperti benua Afrika, monopoli perusahaan Amerika dan Eropa di bidang kabel telekomunikasi bawah laut belum berubah.

Statistik menunjukkan bahwa dalam 5 tahun, antara tahun 2008 dan 2012, sistem kabel bawah laut baru senilai $10 Milyar telah dibangun dan siap melayani kebutuhan dunia, dengan $ 2 Milyar atau 53.000 km per tahun, dan 70% dari sistem dikembangkan di wilayah Sub-Sahara Afrika. Selanjutnya data dari proyek tersebut menunjukkan bahwa proporsi investasi dari operator dan konsorsium berukuran besar asal Amerika dan Eropa mencapai 80% dari seluruh investasi. Sebaliknya, investasi swasta dari organisasi non-telekomunikasi menyumbang 14%, sedangkan proporsi investasi dari pemerintah dan bank-bank pembangunan hanya sebesar 5%.

Hal ini semakin menunjukkan dominasi Amerika dan Eropa. Ditambah lagi, perusahaan transnasional dari negara-negara maju memiliki keuntungan besar di bidang komputer. Statistik menunjukkan bahwa lima perusahaan dari Amerika Serikat dan Jepang, termasuk HP, IBM, Dell, Oracle dan Fuji, menduduki 84,7% dari pangsa pasar pada tahun 2012, yang mencerminkan keunggulan besar mereka di pasar teknologi informasi.

---

[19] B Sanou, *ICT Facts and Figures*, https://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFactsFigures2015.pdf , diakses 4 Februari.

[20] Internet World Stats, *Internet Users in the 20 Top Countries*, http://www.internetworldstats.com/top20.htm, diakses 3 Februari 2020.

[21] International Telecommunication Union, *ITU Facts and Figures 2016*, http://www.itu.int/en/mediacentre/pages/2016-PR30.aspx, diakses 3 Februari 2020.

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-1060
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

Ketiga, keunggulan negara-negara maju juga tercermin dalam mekanisme distribusi dan manajemen fasilitas fisik dari infrastruktur utama yang menjalankan berbagai sistem operasi dunia maya. Sebagai contoh. Sistem resolusi penentuan nama *domain* atau situs terdiri dari 13 tingkat server yang mana melibatkan 3 perusahaan, 3 organisasi yang berhubungan dengan pemerintah, 3 universitas dan 1 lembaga swasta nirlaba di Amerika Serikat, 1 perusahaan dan 1 lembaga swasta dari Eropa, dan 1 organisasi Jepang masing-masing. Selanjutnya, distribusi file di antara ke-13 server tersebut dilakukan oleh sebuah *mainframe* server yang dimiliki dan dikelola oleh VeriSign Inc. sebuah perusahaan raksasa dari Amerika Serikat.[22] Pengelolaan infrastruktur dan sistem distribusi data seperti di atas sering digunakan sebagai contoh untuk membuktikan keberadaan dan hegemoni negara maju di dunia maya.[23]

Keempat, teknologi yang dimiliki Amerika Serikat dalam pengelolaan dunia maya. ICANN secara prosedural bertanggung jawab dalam persetujuan dan perjanjian tertulis tentang sebuah program, dimana tanggung jawab dalam konfigurasi dan modifikasi *root server* utama dilakukan oleh sebuah badan khusus lain di bawah koordinasi lembaga telekomunikasi dan informasi, NTIA, milik Kementerian Perdagangan Amerika Serikat. Sejak tahun 1998, para ilmuwan Amerika Serikat diketahui telah menerapkan sebuah metode untuk mengalihkan file-file yang ada pada suatu *root server* ke *server* lain untuk dijalankan secara paralel atau bersamaan. Walaupun kemudian metode tersebut hanya diakui sebagai upaya percobaan laboratorium oleh Pemerintah Amerika Serikat, hal ini memicu munculnya kekhawatiran akan tindakan pengawasan dan spionase di dunia maya yang dilakukan oleh pemerintah Amerika Serikat melalui kedua lembaga, ICANN dan NTIA tersebut.

Di dunia maya saat ini, negara-negara berkembang lebih banyak berperan sebagai pengguna sementara negara-negara maju menjadi pemain utama dan pemasok infrastruktur, sistem operasi dan aplikasiaplikasi intinya. Struktur dunia maya yang timpang seperti ini semakin memperburuk kesenjangan kemampuan yang ada di antara negara maju dan berkembang. Oleh karena itu, seluruh negara di dunia, baik negara maju atau negara berkembang, perlu menyadari pentingnya upaya yang sistematis untuk menerapkan prinsip-prinsip kedaulatan di dunia maya.

Melalui teknologi, metode dan penerapan strategi keamanan dunia maya, Amerika Serikat telah menunjukkan bagaimana suatu hegemoni dapat memperluas kedaulatan satu negara dan memperlemah atau bahkan mengabaikan kedaulatan negara lain di dunia maya. Melihat hal itu, negara-negara yang tidak diuntungkan oleh keadaan tersebut mencoba untuk menerapkan prinsip kesetaraan kedaulatan guna mengurangi dampak hegemoni dan ekspansi negara-negara maju di dunia maya.

2. Aspek Politik

Pengelolaan keamanan dunia maya sangat membutuhkan peraturan internasional untuk menyusun beberapa "aturan main" yang mendasar untuk mengatur penggunaan dan pencegahan spionase dan konflik dunia maya antar negara. Pemerintahan dan lembaga internasional seharusnya bekerja sama dalam menyusun aturan, norma, prinsip dan prosedur,[24] dan dengan demikian dapat mengurangi sikap saling tidak percaya yang ada saat ini.

Penyusunan peraturan tersebut, bagaimanapun, membutuhkan modal kepercayaan di

[22] SSAC, ICANN, *Overview and history of the IANA functions. SAC067*. https://www.icann.org/en/system/files/files/sac-067-en.pdf , diakses 3 Februari 2020.

[23] S. P. Sonbuchner, "Master of your domain: should the US Government Maintain Control over the Internet's Root", *Minnesota Journal of International Law*, Vol. 17, 2008, hlm.183.

[24] S. D. Krasner, "Abiding sovereignty", *International Political Science Review*, Vol. 22, No. 3, 2001, hlm. 229–251.

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-970
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

antara pemerintah dan masing-masing instansi yang terlibat. Selain itu, setiap pengaturan dan tata kelola keamanan dunia maya harus bergerak dan beradaptasi dengan cepat untuk mengimbangi teknologi dan dinamika keamanan dunia maya itu sendiri. Hambatan pembentukan tata kelola dunia maya, tercermin pada hal-hal politis sebagai berikut.

Pertama, para pemangku kepentingan belum dapat mengelola penggunaan sumber daya bersama secara kolektif,[25] untuk mengurangi upaya eksploitasi dan pemungutan dana oleh pihak-pihak tertentu yang telah menggunakan sumber daya itu terlebih dulu.[26] Begitu juga dengan apa yang terjadi di dunia maya, dimana seperangkat norma dan prosedur yang demikian longgar telanjur terbentuk dan dimanfaatkan oleh negara-negara maju sebagai akibat dari kompleksitas jejaring dunia maya.[27]

Kedua, norma, aturan dan institusi dalam bentuk formal telah diterapkan di bidang-bidang yang berkaitan dengan standar kebijakan internasional dan teknis pengelolaan internet. Akan tetapi, penyusunan peraturan dan pengelolaan di bidang-bidang keamanan dunia maya, khususnya berkaitan dengan perang, konflik, sabotase dan spionase antar negara, belum menunjukkan kemajuan yang berarti. Dinamika dilema keamanan disinyalir menjadi alasan mengapa permasalahan tersebut terjadi.

Ketiga, dilema keamanan yang menyebabkan setiap negara saling berlomba-lomba berinvestasi untuk meningkatkan kemampuan militer mereka sendiri.[28] Akibatnya, harapan untuk melakukan kerja sama keamanan bergantung pada keseimbangan antara jumlah senjata dan kemampuan pertahanan masing-masing negara.[29] Di dunia maya, menyerang pihak lain merupakan hal yang lebih baik daripada bertahan. Penyerangan terhadap jejaring dan infrastruktur pihak lawan jauh lebih mudah daripada menahan serangan. Penyerang hanya perlu menemukan satu cara untuk membobol sistem komputer, sedangkan pihak yang memilih bertahan harus memperbaiki dan menambal semua lubang keamanan yang rawan serangan.[30] Dalam bidang kejahatan komputer, sulit untuk menentukan apakah kode pemrograman yang dibuat hendak digunakan untuk tujuan pertahanan atau untuk menyusup dan/atau menyerang jejaring computer lainnya. Hal yang sama juga berlaku dalam penyusunan strategi keamanan dunia maya.

Keempat, kebijakan strategi keamanan dunia maya yang telah diambil masing-masing negara. Beberapa strategi keamanan dunia maya dapat bersifat defensif, seperti yang ada di Denmark, dan dapat juga bersifat ofensif, seperti di Inggris dan Amerika Serikat. Strategi Inggris, misalnya, bertumpu pada upaya untuk mengurangi risiko serangan melalui

---

[25] E. Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge: Cambridge University Press, 1990, hlm. 108.

[26] M. Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups*, Cambridge: Harvard University Press, 1965, hlm. 76.

[27] J. S. Nye Jr., "The Regime Complex for Managing Global Cyber Activities", *Global Commission on Internet Governance Paper Series No. 1*, London: Global Commission on Internet Governance, 2014.

[28] C. L. Glaser, *The Security Dilemma Revisited*, World Politics, Vol. 50, No. 1, 1997, hlm. 171–201.

[29] R. Jervis, "Cooperation Under the Security Dilemma", *World Politics*, Vol. 30, No. 2, 1978, hlm. 167–214.

[30] World Economic Forum, The Reshaping of the World: Consequences for Society, Politics and Business. Annual Meeting,http://www3.weforum.org/docs/AM14/WEF_AM14_Public_Report.pdf, diakses 3 Februari 2020.

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-1060
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

pemantauan dan pengumpulan data intelijen di dunia maya.[31] Angkatan Bersenjata Amerika Serikat telah menciptakan sebuah tim prajurit dunia maya yang siap membalas setiap serangan dunia maya yang terjadi. Tim ini dibentuk sebagai sebuah tim ofensif yang dapat segera digunakan untuk membela kepentingan Amerika Serikat apabila diserang di dunia maya.[32] Perkembangan tersebut tidak hanya kontraproduktif tetapi juga berbahaya karena dapat memperluas lingkup konflik antar negara.

Kelima, tanpa persetujuan dan reformasi sistemik secara menyeluruh, upaya untuk merubah praktek kekuasaan yang dilakukan oleh negara-negara maju yang telanjur mendominasi pengelolaan dunia maya akan menemui banyak hambatan. Isi usulan India yang membutuhkan perubahan radikal pada infrastruktur dunia maya, terkesan melangkahi banyak wewenang. Oleh karena itu rencana India ini mendapat perlawanan yang kuat dari pemerintah Amerika Serikat. Bahkan, pemerintah Amerika Serikat menolak sama sekali proposal India terebut tanpa kompromi, dengan dalih kebijakan dan peraturan tentang keamanan negara. Perwakilan pemerintah Amerika Serikat berpendapat bahwa mereka tidak akan mengalihkan wewenang yang dimiliki lembaga bentukan mereka kepada lembaga yang dioperasikan oleh negara lain.

Terlepas dari *NETmundial initiaitive* yang diusulkan oleh Brasil maupun usulan dari pemerintah India, upaya untuk menegakkan kedaulatan pemerintahan di dunia maya masih sulit dicapai dalam waktu dekat. Sehingga, apa yang dapat dilakukan saat ini adalah menunggu terjadinya keseimbangan kekuasaan dan mempersiapkan munculnya lembaga baru yang mampu mengimbangi dominasi lembaga buatan negara-negara maju tersebut dan bersedia mengikuti prinsip kesetaraan kedaulatan serta disiplin dalam melakukan pengelolaan dunia maya.

III. KESIMPULAN

Globalisasi kontemporer yang timbul berkat perkembangan teknologi informasi semenjak penemuan internet telah bermetamorfosis menjadi suatu rezim hukum baru dengan elemen yang berbeda dari rezim hukum konvensional. Semenjak rezim hukum baru seperti ruang-maya (Cyberspace) tercipta dengn bergandengan tangan bersama globalisasi kontemporer, Negara pun merasa perlu untuk hadir dalam rangka menegakkan hukummnya. Gagasan kedaulatan Negara yang secara tradisional hanya terbatas pada aspek teritorialitas (darat, laut, dan ruang-udara) kini berkembang menjadi ekstrateritorialitas (ruang-maya) dengan jangkauan hukum yang tidak terbatas. Kedaulatan Negara di ruang-maya, dengan demikian, adalah sebentuk hasrat negar untuk memperluas wilaya dan menegakkan hukumnya serta dikelola dan dimanfaatkan oleh Negara. Seiring dengan perkembangan teknologi informasi, penegakan kedaulatan, yang terkait dengan aliran data, keamanan dan operasi informatika, sebagai upaya pertahanan dan keamanan nasional di dunia maya perlu diwujudkan.

Meskipun definisi tentang kedaulatan dunia maya sendiri belum ditetapkan secara pasti, pengelolaan dunia maya dapat didekati dengan konsep kedaulatan yang berdasarkan wilayah teritorial dan kewajiban suatu negara dalam tatanan hubungan internasional. Hal ini berarti bahwa setiap negara memiliki hak untuk mengatur semua infrastruktur dan arsitektur sistem dunia maya yang berada di wilayah teritorialnya, dan memiliki kewajiban untuk

[31] J. A. Lewis dan G. Neuneck, *The Cyber Index: International Security Trends and Realities*, Geneva: United Nations Institute for Disarmament Research (UNIDIR), 2013.

[32] G. Smith, "Security Chief's Cyberwar Testimony Seen AsVeiled Threat To Enemies", *The Huffington Post*, http://www.huffingtonpost.com/2013/03/14/securitychiefcyberwar_n_2875516.html, diakses 4 Februari 2020.

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-970
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

menghormati sistem keamanan dunia maya milik negara lain dengan cara mencegah segala bentuk pelanggaran atas integritas dunia maya negara lain yang berasal dari wilayahnya.

Inisiatif pengelolaan dunia maya yang dominan saat ini dilakukan oleh ICANN, sebuah lembaga *multistakeholder* bentukan pemerintah Amerika Serikat dimana pemerintah negara-negara lain tidak memiliki peran yang setara. Inisiatif Amerika Serikat ini dikritik karena seringkali kebijakan yang diambil dalam ICANN lebih menguntungkan bagi negara-negara yang terlebih dulu memiliki dan menguasai teknologi internet. Hal tersebut mendorong usulan berupa inisiatif *NetMundial* yang diusulkan Brazil, dan inisiatif berbasis ITU yang diusulkan India, yang menginginkan agar tata kelola Internet dirancang dengan melibatkan negara-negara berkembang dan menghargai hak kedaulatan negara lain sesuai yurisdiksi masing-masing negara dan hukum internasional. Pada akhirnya, usulan terebut bertujuan agar seluruh Negara mendapatkan manfaat ekonomis dan politis yang seimbang dalam pelaksanaan pengelolaan dunia maya. Inisitatif kelembagaan yang bersifat *multilateral* ini mendapat dukungan kuat dari China yang menginginkan agar arus informasi di dunia maya tetap dapat dikendalikan oleh pemerintahan suatu negara demi tujuan keamanan nasional.

Walaupun cenderung bersifat reaktif, pemerintah Indonesia telah memiliki berbagai lembaga dan sarana penunjang dalam upaya menegakkan kedaulatan di dunia maya. Selain produk hukum, kegiatan pertahanan dan keamanan nasional di dunia maya juga telah dilaksanakan oleh berbagai instansi seperti Kemenkominfo yang berkoordinasi dengan instansi pemerintah lainnya seperti Kepolisian Negara Republik Indonesia, Tentara Nasional Indonesia, Kementerian Luar Negeri, Kementerian Dalam Negeri, dan Kementerian Pertahanan, disamping lembaga lain seperti ID-CERT, Gov-CSIRT, id-SIRTI/CC dan Lemsaneg.

Daftar Pustaka

Artikel

Glaser, C. L., "*The Security Dilemma Revisited*", World Politics, Vol. 50, No. 1, 1997.

Jervis, R., "Cooperation Under the Security Dilemma", *World Politics*, Vol. 30, No. 2, 1978.

Krasner, S. D., "*Abiding sovereignty*", *International Political Science Review*, Vol. 22, No. 3, 2001.

Lampton, D. M., "Xi Jinping and the National Security Commission: policy coordination and political power",*Journal of Contemporary China*, Vol. 24, No. 95, 2015.

Sonbuchner, S. P., "Master of your domain: should the US Government Maintain Control over the Internet's Root", *Minnesota Journal of International Law*, Vol. 17, 2008.

Yi, S. "*Transform and construction: the design of nationalcybersecurity strategy and the capacity build in a post-Snowden age"*, *China Information Security*, Vol. 5, 2014.

Buku

Edi Atmaja, AP. "*Kedaulatan Negara Di Ruang Maya: Kritik UU ITE Dalam Pemikiran Satjipto Rahardjo*", Jurnal Opinio Juris. Vol. 16. Ed. Mei-September 2014, hlm. 48-50.

Lewis, J. A. dan Neuneck, G., *The Cyber Index: International Security Trends and Realities,* Geneva: United Nations Institute for Disarmament Research (UNIDIR), 2013.

Nye Jr., J. S., *The Regime Complex for Managing Global Cyber Activities*, Global Commission on Internet Governance Paper Series No. 1, London: Global Commission on Internet Governance, 2014.

Olson, M., *The Logic of Collective Action: Public Goods and the Theory of Groups*, Cambridge:

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-1060
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

Harvard University Press, 1965, hlm. 76.

Ostrom, E., *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge: Cambridge University Press, 1990.

Internet

De Bossey, C., *Report of the Working Group on Internet Governance*, http://www.wgig.org/docs/WGIGREPORT.pdf, diakses 3 Februari 2020.

GovCISRT, Profil, http://govcsirt.kominfo.go.id/tentangidgovcert/profil, diakses 3 Februari 2020.

Greenwald dan MacAskill, *NSA Prism program taps into user data of Apple, Google and Others*, http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf, diakses 1 Februari 2020.

Hayden, M., *Ex-NSA chief: safeguards exist to protect Americans' privacy*, http://edition.cnn.com/2013/08/01/opinion/hayden-nsa-surveillance/, diakses 2 Februari 2020.

ICANN, *Overview and history of the IANA functions. SAC067*. https://www.icann.org/en/system/files/files/sac-067-en.pdf , diakses 3 Februari 2020.

Id CERT, Profil, http://www.cert.or.id/tentang-kami/id/, diakses 3 Februari 2020.

Id SIRTII, struktur organisasi, http://www.idsirtii.or.id/halaman/tentang/strukturorganisasi.html., diakses 3 Februari 2020.

International Telecommunication Union, *ITU Facts and Figures 2016*, http://www.itu.int/en/mediacentre/pages/2016-PR30.aspx, diakses 3 Februari 2020.

Internet World Stats, *Internet Users in the 20 Top Countries*, http://www.internetworldstats.com/top20.htm, diakses 3 Februari 2020.

Kemenkominfo, Direktorat Jenderal Sumber Daya, Pos dan Informatika Kemekominfo, Tugas dan fungsi, http://kominfo.go.id/index.php/node/711/Tugas+dan+Fungsi, diakses 3 Feburari 2020.

Lembaga Sandi Negara, Tugas dan Fungsi,http://www.lemsaneg.go.id/index.php/profil/tugas-dan-fungsi/, diakses 3 Februari 2020.

Lieberthal, K, dan Jisi, W., "Addressing U.S.-China Strategic Distrust", *John L. Thornton China Center Monograph Series*, Number 4, http://yahuwshua.org/en/Resource-584/0330_china_lieberthal.pdf, diakses 3 Februari 2020.

NTIA, Department of Commerce, *Verisign/ICANN proposal in response to NTIA request root zone administrator proposal related to the IANA Functions Stewardship Transition*, https://www.ntia.doc.gov/files / ntia /publications/root_zone_administrator_proposalrelat dtoiana_functionsstefinal.pdf, diakses 2 Februari 2020.

Peranan Negara Dalam UUD 1945,https://www.esaunggul.ac.id/peranan-negara-dalam-undang-undang-dasar-1945/, diakses pada tanggal 14 November 2019.

Sanger, D., 2015, *US decides to retaliate against China'shacking,* http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html, diakses 2 Februari 2020.

DHARMASISYA
Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia
Volume 1 Nomor 2 (Juni 2021) 957-970
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx

Sanou, B., *ICT Facts and Figures*, https://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFactsFigures2015.pdf, diakses 4 Februari 2020.

Schmidt, L., *Perspective on 2015 DoD Cyber Strategy*, SantaMonica CA: RAND Corporation, http://www.dtic.mil/cgibin/GetTRDoc?AD=ADA621794, diakses 2 Februari 2020.

Smith, G., "*Security Chief's Cyberwar Testimony Seen AsVeiled Threat To Enemies*", *The Huffington Post*, http://www.huffingtonpost.com/2013/03/14/securitychiefcyberwar_n_2875516.html, diakses 4 Februari 2020.

World Economic Forum, *The Reshaping of the World: Consequences for Society, Politics and Business. Annual Meeting*,http://www3.weforum.org/docs/AM14/WEF_AM14_Public_Report.pdf, diakses 3 Februari 2020.