

TATA KELOLA DUNIA MAYA DAN ANCAMAN KEDAULATAN NASIONAL

Cyber Governance and Threat of National Sovereignty

Indra Cahyadi

Universitas Trunojoyo Madura
Alamat e-mail: indra.cahyadi@trunojoyo.ac.id

Naskah Diterima: 1 Agustus 2016
Naskah Direvisi: 11 Oktober 2016
Naskah Disetujui: 4 November 2016

Abstract

The significant growth of internet technology has the potential to promote economic growth. On the other hand, it also causes increasing threats to state's sovereignty in cyber world. Sovereignty in cyberworld, or cyber sovereignty, has become an important topic of both national and international security, especially after Edward Snowden's disclosure of the secret surveillance programs of the government of the United States of America. This article aims to understand the current international disputes over governance in cyberworld and to identify challenges and threats in cyber sovereignty. This article discusses the cyber sovereignty issues including; concept of sovereignty in cyberworld, challenges in process of building cyberspace governance based on sovereign equality, as well as Indonesia's strategy in exercising cyber sovereignty. It finds that China and USA have applied cyber sovereignty principles to guide the governance of global cyberspace, and Indonesia must follow and act in integrative manner to efficiently protect and safeguard its cyber sovereignty.

Keywords: cyber security, national sovereignty, national security, governance.

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, terutama setelah Edward Snowden mengungkapkan program pengawasan rahasia milik pemerintah Amerika Serikat. Artikel ini bertujuan untuk memahami perdebatan internasional mengenai tata kelola dunia maya dan mengidentifikasi tantangan dalam penegakan kedaulatan di dunia maya. Untuk itu, artikel ini membahas isu-isu terkait kedaulatan di dunia maya termasuk; konsep kedaulatan di dunia maya, tantangan dalam pembentukan tata pemerintahan dunia maya yang berdasarkan kesetaraan kedaulatan, serta strategi yang sudah dilakukan Indonesia dalam menegakan kedaulatan di dunia maya. Artikel ini berkesimpulan bahwa China dan Amerika Serikat telah menerapkan prinsip-prinsip kedaulatan untuk memandu tata pemerintahan dunia maya global, dan oleh karena itu Indonesia harus segera menyusul dan bertindak secara terintegrasi agar dapat melindungi dan menjaga kedaulatannya di dunia maya secara efisien.

Kata kunci: keamanan cyber, kedaulatan nasional, keamanan nasional, tata kelola pemerintahan.

I. Pendahuluan

A. Latar Belakang

Sejak tahun 2010, berbagai isu-isu terkait dengan internet dan dunia maya mengemuka dalam agenda keamanan nasional, dan secara

bertahap terangkat menjadi salah satu isu penting dalam hubungan internasional. Pada tahun 2010, situs resmi WikiLeaks membocorkan kabel rahasia dan dokumen penting milik Departemen Pertahanan dan Departemen Luar

Negeri Amerika Serikat.¹ Perusahaan raksasa Google menantang yurisdiksi China atas kebijakan sensor di internet.² Pada tahun 2011, sebuah gerakan yang diberi istilah “Arab Spring” merombak struktur geopolitik tradisional di Timur Tengah,³ dan pada tahun yang sama, Amerika Serikat memperkenalkan “*Cyberspace International Strategy*” yang mempertegas maksud pemerintah Amerika Serikat untuk membangun tatanan hegemonik di dunia maya. Pada tahun 2012-2013, serangkaian berita tentang serangan espionase internet oleh China diterjemahkan sebagai ancaman baru terhadap keamanan nasional AS.⁴ Pada tahun 2013, dunia dihebohkan oleh tindakan mantan kontraktor *Central Intelligence Agency* bernama Edward Snowden membocorkan rahasia tentang *Privacy in Mobile Information and Communication Systems* (PRISM) sebagai program intelijen Amerika Serikat yang dikembangkan untuk mendapatkan dan mengetahui segala bentuk data pengguna yang dimiliki perusahaan-perusahaan besar dunia.⁵

Pada tahun 2014, Kementerian Perdagangan Amerika Serikat mengumumkan niatnya untuk mengelola fungsi *root server* dan alamat domain internet. Sebuah organisasi bernama *Internet Corporation for Assigned Names and Numbers* (ICANN) dibentuk untuk di atas fungsi *Internet Assigned Numbers Authority* (IANA) yang sejak 1998 mengelola nama domain internet. ICANN berada di bawah koordinasi

National Telecommunications and Information Administration (NTIA), sebuah lembaga di bawah Kementerian Perdagangan Amerika Serikat. Pada bulan Agustus 2015, pemerintah Amerika Serikat mengumumkan perpanjangan kontrak dengan ICANN selama 1 tahun. Hal ini memunculkan kekhawatiran publik terhadap kemampuan dan kewenangan pemerintah Amerika Serikat untuk mendapatkan semua informasi yang berlalu-lalang di dunia maya.

B. Permasalahan

Tantangan sosial politik yang ditimbulkan perkembangan teknologi jejaring komputer dan keamanan dunia maya merupakan permasalahan penting sejak awal abad ke-21. Perkembangan teknologi menjadi tantangan baru bagi strategi pertahanan dan keamanan yang harus dihadapi oleh seluruh negara di dunia, baik di tingkat pemerintahan, entitas bisnis maupun masyarakat sipil. Pelanggaran keamanan di dunia maya yang telah disorot di atas menyadarkan para pembuat kebijakan dan masyarakat bahwa penegakan kedaulatan di dunia maya adalah hal yang semakin serius dan memiliki implikasi pada politik, ekonomi dan sosial suatu negara. Oleh karena itu, berbagai negara telah memulai melakukan tata kelola dunia maya yang melibatkan pemangku kepentingan baik dari pejabat pemerintahan maupun pihak swasta.

Namun, munculnya modus-modus baru dalam pelanggaran keamanan dunia maya dan sulitnya mempersatukan pandangan pemerintahan berbagai negara dan pelaku bisnis terkait tata kelola dunia maya, menimbulkan berbagai tekanan dalam permasalahan kedaulatan suatu negara di dunia maya. Artikel ini akan mengidentifikasi dan menganalisa permasalahan pelanggaran keamanan dunia maya suatu negara, pengaruh dari perubahan-perubahan kebijakan di dunia maya terhadap keamanan nasional suatu negara, serta upaya pemerintah Indonesia dalam pertahanan keamanan dan penegakan kedaulatan dunia maya, melalui pendekatan hubungan internasional.

¹ G. Kessler, *Wikileaks's unveiling of secret State Department cables exposes US diplomacy*, *The Washington Post*, <http://www.washingtonpost.com/wp-dyn/content/article/2010/11/28/AR2010112802395.html> diakses 7 Juli 2016.

² D. Gross, *Google quits censoring search in China*, <http://www.cnn.com/2010/TECH/03/22/google.china/>, diakses 7 Juli 2016.

³ F. Ajami, “The Arab spring at one”, *Foreign Affairs*, Vol. 91, No. 2, 2012, h. 56–65.

⁴ B. Krekel, P. Adams, dan G. Bakos, “Occupying the information high ground: Chinese capabilities for computer network operations and cyber espionage”, *International Journal of Computer Research*, Vol. 21, No. 4, 2014, h. 333.

⁵ 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 7 Juli 2016.

C. Tujuan Penulisan

Untuk menjawab permasalahan di atas, artikel ini mengeksplorasi struktur pemerintahan tata kelola dunia maya dan meninjau prinsip-prinsip yang dapat menjadi acuan dalam tata kelola dunia maya. Artikel ini menggunakan studi literatur untuk membandingkan dan menganalisa perbedaan prinsip kedaulatan yang diterapkan di berbagai negara untuk mengelola dunia maya. Tujuan dari artikel ini adalah untuk mengemukakan bahwa peningkatan kolaborasi dan kerja sama antar negara sangat dibutuhkan dalam penerapan prinsip-prinsip kedaulatan dan pemerintahan di dunia maya.

D. Landasan Teori

Terbentuknya dunia maya dimulai karena penggunaan internet yang semakin bertambah di berbagai belahan dunia. Menurut data *International Telecommunication Union* (ITU), jumlah pengguna internet mencakup sekitar 30-40% dari populasi dunia.⁶ Internet dan dunia maya merupakan pisau bermata dua bagi pemerintahan negara-negara di dunia. Di satu sisi, dunia maya telah memiliki karakteristik suatu pemerintahan yang mengelola berbagai sarana dan menyediakan kondisi yang nyaman bagi warganya. Sementara di sisi lain, terbentuknya dunia maya juga memunculkan tantangan baru dalam penentuan batas yurisdiksi suatu negara. Oleh karena itu, pertanyaan tentang bagaimana memahami peran, fungsi, dan karakteristik serta bagaimana membangun kedaulatan di dunia maya, menjadi topik yang sering diperdebatkan.⁷

Para peneliti telah menunjukkan, dunia maya sejatinya adalah ruang logis yang sulit dikendalikan atau dikelola secara tepat, dunia maya tidak akan terbentuk tanpa adanya dukungan dari dunia fisik. Salah satu kesulitan dalam pembentukan tata pemerintahan

dunia maya adalah bagaimana memunculkan keberadaan otoritas dan administrasi di dunia maya. Keberadaan otoritas dan administrasi ini harus diterima dan disetujui oleh sebanyak mungkin pihak-pihak yang terlibat di dunia maya. Keberadaan otoritas dan administrasi ini bisa berbentuk sebuah sistem penyediaan, atau bahkan sistem pengawasan kehadiran. Tantangan yang muncul adalah bagaimana persepsi tentang otoritas dan administrasi dunia maya ini dapat mewakili berbagai kepentingan, dimana penerapannya dilaksanakan oleh para pihak-pihak terkait berdasarkan kerangka kerja yang obyektif dan pengawasan yang subjektif.⁸

Apakah kedaulatan dapat beradaptasi dengan tantangan pengelolaan dunia maya adalah salah satu pertanyaan kunci dalam pembahasan isu tentang dunia maya. Hal tersebut juga menjadi salah satu masalah yang paling sulit dalam menangani konflik di dunia maya.⁹ Tantangan utama dalam penegakan kedaulatan pada isu-isu pemerintahan, termasuk keamanan dunia maya, adalah meningkatnya peran pihak-pihak di luar pemerintahan yang menyulitkan penerapan hukum internasional secara tradisional karena belum jelasnya aturan kedaulatan di dunia maya.¹⁰ Meski demikian, penegakan kedaulatan tetap harus dilakukan secara tegas untuk menangani isu-isu keamanan dunia maya, seiring dengan semakin meningkatnya serangan-serangan yang muncul di dunia maya.¹¹

Pada Juni 2015, dalam rangka pengembangan perspektif keamanan internasional di bidang informasi dan telekomunikasi, *UN Group of Governmental Experts* (UNGGE) menyerahkan

⁶ B. Sanou, *ICT Facts and Figures*, <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>, diakses 7 Juli 2016.

⁷ K. D. Barcomb, R. Krill, R. Mills dan M. Saville, *Establishing cyberspace sovereignty*, Prosiding *7th International Conference on Information Warfare and Security*, Academic Conferences Limited, 2012.

⁸ P. A. Lyons, *Cyberspace and the law: your rights and duties in the on-line world*, Information Processing and Management, ed. E. A. Cavazos, G. Morin, Vol. 31, No. 6, 1996, h. 910.

⁹ C. Czosseck, dan K. Geers, *Borders in cyberspace: can sovereignty adapt to the challenges of cyber security?*, *The Virtual Battlefield: Perspectives on Cyber Warfare*, Vol.3, 2009, h. 88.

¹⁰ S. D. Krasner, "Abiding sovereignty", *International Political Science Review*, Vol. 22, No. 3, 2001, h. 229-251.

¹¹ H. Stephen, "Revisiting the Estonian cyber attacks: digital threats and multinational responses", *Journal of Strategic Security*, Vol. 4, No. 2, 2011, h. 4.

laporan konsensus kepada Majelis Umum Perserikatan Bangsa-Bangsa (PBB). Dalam laporan tersebut dinyatakan pentingnya penerapan 'Piagam PBB' dan prinsip kedaulatan, sebagai dasar untuk memperkuat peningkatan keamanan di bidang teknologi informasi dan telekomunikasi.¹² Laporan ini juga menyatakan bahwa untuk mengetahui penggunaan prinsip kedaulatan dalam pemerintahan dunia maya secara akurat, perlu dilakukan studi lanjut guna memahami karakteristik dasar dunia maya yang dapat mempengaruhi mekanisme penerapan prinsip-prinsip kedaulatan dalam peningkatan keamanan di dunia maya.

Meskipun sering menjadi topik perdebatan di kalangan akademisi, konsep kedaulatan terbukti dapat beradaptasi secara mudah dari waktu ke waktu. Konsep tentang kedaulatan telah mengalami berbagai era -dekolonisasi, globalisasi, bahkan digital dan internet-, namun masih tetap dapat bertahan. Bahasan berikut menguraikan tentang kedaulatan sebagai landasan hukum internasional, konsep kedaulatan dunia maya dan pentingnya kerjasama internasional dalam menjaga kedaulatan di dunia maya.

1. Kedaulatan sebagai Landasan Hukum Internasional

Dalam pengertian yang paling umum, kedaulatan berarti hak dan kewajiban internasional suatu negara yang diakui oleh hukum internasional secara menyeluruh.¹³ Landasan hukum paling mendasar dan tepat dari pengertian ini tercantum pada Piagam PBB Pasal 2 ayat 1, yang menetapkan prinsip kesetaraan kedaulatan negara,¹⁴ dan sekaligus menjamin kesetaraan hukum negara¹⁵ Salah satu

prinsip dalam konsep kedaulatan adalah prinsip kedaulatan teritorial, yang mendefinisikan kedaulatan dengan mengacu pada wilayah fisik suatu negara. Terdapat semacam konsensus mengenai sejauh mana suatu negara dapat menjalankan otoritas secara penuh dan eksklusif atas wilayah teritorialnya. Secara praktis, beberapa peneliti Eropa dan Amerika membuat ringkasan sistematis dan meninjau penerapan prinsip-prinsip penting dalam hukum internasional tradisional untuk mewakili prinsip kedaulatan di dunia maya. Konsep yang diutarakan adalah bahwa prinsip kedaulatan berlaku untuk ruang maya, dimana dinyatakan negara dalam wilayah kedaulatannya dapat menerapkan pengendalian dan pengawasan pada infrastruktur dan kegiatan yang berkaitan dengan informasi. Berdasarkan kasus putusan hukum internasional tentang Pulau Palmas (Miangas) tahun 1928, kedaulatan negara merupakan urusan internal suatu negara yang bebas dari campur tangan dari negara lain.¹⁶ Mahkamah Internasional bahkan menyatakan bahwa pengakuan kedaulatan teritorial di antara negara-negara merdeka merupakan fondasi penting dari hubungan internasional. Dengan demikian, pembahasan tentang kedaulatan selalu didasarkan pada gagasan teritorial, dan seberapa jauh jangkauan kedaulatan suatu negara yang diputuskan oleh batas-batas geografis, bahkan hingga ke wilayah perairan dan ruang udara di atas wilayah negara tersebut.¹⁷ Oleh karena itu, aspek wilayah teritorial tidak hanya merupakan aspek penting dari kedaulatan, tetapi juga menentukan kapasitas kedaulatan negara. Kapasitas kedaulatan mengacu bagaimana suatu negara dapat menetapkan hukum yang berlaku di wilayah teritorialnya, tanpa tergantung pada pihak lain yang mungkin memiliki kewenangan lebih tinggi.¹⁸

¹² Majelis Umum PBB, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174, diakses 8 Juli 2016.

¹³ J. Crawford, *Chance, Order, Change: The Course of International Law*, The Hague: Hague Academy of International Law, 2014, h. 88.

¹⁴ Piagam PBB, Pasal 2 ayat 1.

¹⁵ K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*. Tallinn: NATO CCD COE Publications, 2013, h. 156.

¹⁶ A. G. Hamid, "Maritime Terrorism, the Straits of Malacca, and the Issue of State Responsibility", *Journal of International and Company Law*, Vol. 15, 2006, h. 155.

¹⁷ R. Buchan, "Cyber attacks: unlawful uses of force or prohibited interventions?", *Journal of Conflict and Security Law*, Vol. 17, No. 2, 2012, h. 212-227.

¹⁸ M. Koskenniemi, *From apology to utopia: the structure of international legal argument*, Cambridge University Press, 2006, h. 87.

Dalam hubungan internasional, suatu negara yang berdaulat tidak akan tunduk pada kehendak negara lain. Hal tersebut sesuai dengan prinsip negara merdeka yang memiliki posisi hukum yang sama dengan negara lain.¹⁹ Oleh karena itu, penandatanganan perjanjian antar negara bukan berarti bahwa kedaulatan suatu negara telah dilanggar. Justru, suatu negara dapat dikatakan telah memiliki ciri sebagai negara berdaulat yang diakui oleh negara lain bila negara tersebut mampu melakukan perjanjian dengan negara-negara lain di dunia.²⁰ Selain hak untuk menentukan nasibnya sendiri, negara yang berdaulat memiliki kewajiban untuk mengakui kedaulatan negara lain, kewajiban untuk tidak mencampuri urusan negara lain dan kewajiban untuk mengendalikan tindakan-tindakan yang terjadi dalam perbatasan geografis negara lain.²¹

2. Konsep Tradisional Kedaulatan dan Perkembangan Dunia Maya

Kedaulatan dianggap sebagai landasan hukum dan politik internasional. Namun, arti dari kedaulatan kembali diperdebatkan dalam konteks dunia maya.²² Para peneliti telah memperkirakan bahwa suatu teknologi baru nantinya akan merombak konsep lama tentang kedaulatan serta mengubah strategi politik suatu negara.²³ Dalam konteks dunia maya, tampaknya kedaulatan telah berubah menjadi suatu formalitas tanpa arti yang dapat dengan mudah dilanggar tanpa adanya konsekuensi. Dampak teknologi informasi pada bentuk kedaulatan telah diramalkan sejak tahun 1990an.²⁴ Banyak peneliti mengatakan bahwa era teknologi informasi akan mengarah pada runtuhnya batas-batas negara dan

akan menggerus kekuasaan dan kedaulatan negara.²⁵ Perkembangan internet yang demikian pesat telah menyadarkan banyak orang akan keberadaan dunia maya yang tidak mengenal batas-batas negara, karena dunia maya merupakan kontruk yang secara inheren dibangun melintasi perbatasan berbagai negara. Jejaring infrastruktur teknologi informasi, mulai dari kabel bawah laut, satelit, jaringan telekomunikasi, server komputer lain-lain, terhubung dari berbagai lokasi di seluruh dunia. Akibatnya, pembahasan tentang lalu lintas data yang mengalir melalui jaringan tersebut menjadi tantangan bagi konsep kedaulatan yang berdasarkan pada wilayah teritorial suatu negara.²⁶

Beberapa peneliti berpendapat bahwa definisi kedaulatan yang didasarkan pada wilayah teritorial kurang relevan lagi untuk digunakan dalam pembahasan tentang operasional dan pengelolaan dunia maya. Namun demikian, banyak peneliti lain yang berbeda pendapat. Menurut mereka, pada dasarnya kedaulatan di dunia maya, *cyber sovereignty*, adalah merupakan perpanjangan dari kedaulatan teritorial.²⁷

3. Kedaulatan di Dunia Maya

Semakin meluasnya penggunaan Internet telah mendorong munculnya kebijakan untuk melakukan pengendalian terhadap infrastruktur dan penggunaannya, dan pengendalian terhadap data dan informasi yang mengalir di dunia maya.²⁸ Dalam hal ini berbagai negara telah menegaskan kedaulatannya dan berusaha mengatur perilaku warganya di dunia maya.

Dengan mempertimbangkan arsitektur sistem operasi dan infrastruktur dunia maya, suatu negara sebenarnya secara *de facto*

¹⁹ *Ibid*, h. 237.

²⁰ B. Simma (ed.), *The Charter of the United Nations: a commentary*, Vol. 2, Oxford: Oxford University Press, 2002, h.136.

²¹ E. T. Jensen, "Cyber Sovereignty: The Way Ahead", *Texas International Law Journal*, vol. 50, 2015, h. 282.

²² *Ibid*

²³ W. B. Wriston, "Technology and Sovereignty", *Foreign Affairs*, Vol. 67, 1988, h.73.

²⁴ H. H. Perritt Jr., "Cyberspace and State Sovereignty", *Journal of International Legal Studies*, Vol. 3, 1997, h. 157.

²⁵ C. Kavanagh, "Cybersecurity, Sovereignty, and U.S. Foreign Policy", *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy*, Vol. 37, 2015, h. 100–101.

²⁶ A. A. Ross, *A Textbook of International Law*, London: Longmans, Green & Co, 1967, h. 34.

²⁷ Gary D. Brown, "The Wrong Questions about Cyberspace", *Military Law Review*, Vol. 217, No. 214, 2013, h. 225–226.

²⁸ K. Sarikakis, *Mapping the ideologies of Internet policy, Ideologies of the Internet*, Cresskill: Hampton Press, 2006, h. 163–178.

menjalankan kewenangannya atas infrastruktur dunia maya yang secara fisik terletak di wilayah kedaulatannya dan segala kegiatan terkait arus informasi yang berasal dari wilayah tersebut. Pelaksanaan kewenangan suatu negara atas infrastruktur dunia maya dapat diterapkan karena suatu negara memiliki batas kedaulatan yang jelas atas wilayahnya, baik itu darat, laut maupun ruang udara.²⁹

Adapun, pelaksanaan kewenangan yang terkait dengan pengendalian informasi dan aliran data sulit diwujudkan karena sifatnya yang *intangible* alias tidak berwujud.³⁰ Walaupun demikian, suatu negara dapat mulai melaksanakan tindakan pengendalian atas aliran data dan informasi yang beredar di dunia maya pada titik-titik pengiriman penerimaan atau ketika informasi tersebut melintasi sarana infrastruktur yang berada dalam wilayah teritorialnya.³¹ Pada kenyataannya, tindakan ini seringkali berujung pada pemblokiran atau penutupan akses ke situs-situs internet tertentu, yang dapat menurunkan produktifitas dan efisiensi para pengguna internet yang membutuhkan situs-situs tersebut.³²

Dengan demikian, meski suatu negara tidak dapat sepenuhnya mengklaim kedaulatannya di dunia maya, negara tersebut masih dapat melaksanakan kedaulatannya atas dunia maya, selama komponen infrastruktur dunia maya tersebut secara fisik terletak di wilayah darat, perairan laut, kepulauan, atau ruang udara mereka. Pemerintah Amerika Serikat, misalnya, secara terus-menerus menegaskan wewenangnya untuk mencegah serangan dunia maya dari dalam maupun luar negeri, dengan cara mengendalikan dan melindungi

infrastruktur teknologi informasi yang berada di wilayah teritorial mereka. Karena serangan melalui dunia maya memiliki dampak nyata bagi warga negara atau lembaga, negara tersebut perlu untuk menerapkan kewenangan yurisdiksinya atas infrastruktur dunia maya yang terletak di wilayahnya dan atas kegiatan dunia maya yang dilakukan melalui infrastruktur tersebut. Kedaulatan terkait dengan dunia maya sejauh ini lebih mengacu kepada kedaulatan atas infrastruktur informasi dalam wilayah darat, wilayah udara, dan wilayah laut perairan (termasuk dasar laut dan tanah di bawahnya) suatu negara. Konsekuensi langsung dari pernyataan ini adalah bahwa infrastruktur informasi, terlepas dari siapapun pemilik atau penggunaannya, berada di bawah kedaulatan yurisdiksi hukum dan administratif suatu negara, yang dilindungi oleh hukum di negara tersebut.

Implikasi dari penerapan prinsip kedaulatan teritorial dalam konteks dunia maya adalah munculnya kewajiban suatu negara untuk melindungi kedaulatan dan keutuhan negara lain di dunia maya. Kedaulatan teritorial tidak hanya berarti pengakuan hak untuk mengatur wilayah tertentu, tetapi mencakup juga kewajiban untuk menghormati integritas wilayah negara lain, dengan cara menghindari konflik mengenai wilayah teritorial dan tidak mencampuri urusan dalam negeri. Dalam konteks dunia maya, hal ini berarti suatu negara berhak untuk bebas dari campur tangan negara lain, tapi di sisi lain, harus mencegah segala bentuk pelanggaran atas integritas wilayah negara lain yang berasal dari wilayahnya.

4. Manfaat Penegakan Kedaulatan Dunia Maya

Kedaulatan teritorial di dunia maya memungkinkan suatu negara untuk mendapatkan dua manfaat. Manfaat pertama adalah manfaat kesejahteraan, dimana suatu negara dapat mengejar pembangunan ekonomi, sosial dan budaya dan bersaing secara sehat untuk meraih keuntungan tanpa paksaan dari negara lain. Kesetaraan kedaulatan menawarkan kebebasan bagi setiap negara

²⁹ J. E. Kastenber, "Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law", *Air Force Law Review*, Vol. 64, 2009, h. 64.

³⁰ M. N. Schmitt, *Tallinn manual on the international law applicable to cyber warfare*, Cambridge University Press, 2013, h. 14.

³¹ S. Kanuck, "Sovereign Discourse on Cyber Conflict Under International Law", *Texas Law Review*, Vol. 88, No. 7, 2010, h. 1273-1575.

³² N. Tsagourias, *The Legal Status of Cyberspace*, Chapters, 2015, h. 19.

untuk melakukan apa saja, termasuk untuk mengembangkan kemampuan pengelolaan dunia maya demi kepentingan negara mereka.³³

Manfaat kedua adalah terkait dengan keamanan nasional. Penegakan kedaulatan di dunia maya akan mendorong suatu negara untuk mengembangkan kemampuan strategis dalam kegiatan defensif dan ofensif mereka. Di samping itu, penegakan kedaulatan di dunia maya menciptakan pembatas yang melindungi suatu negara dari tindakan pelanggaran hukum oleh negara lain dan menjadi dasar penyelesaian sengketa apabila batas-batas tersebut dilanggar.³⁴

5. Kerja Sama Internasional dan Kedaulatan Di Dunia Maya

Sebagaimana disebutkan di atas, karakteristik dari dunia maya yang berkembang demikian pesat memberikan tantangan berat bagi upaya penegakan kedaulatan suatu negara. Pada dasarnya dunia maya adalah hubungan jaringan komputer yang secara fisik terletak di berbagai negara dengan yurisdiksi hukum yang berbeda-beda, sehingga tidak ada satu negara pun yang bisa sepenuhnya mengatur atau mengendalikannya. Oleh karena itu, berbagai negara berusaha menjalin kerja sama internasional, baik bilateral maupun multilateral, sebagai upaya untuk mengelola dan mengkoordinasi upaya penegakan kedaulatan di dunia maya.

Tanpa adanya kerja sama internasional, upaya penegakan kedaulatan di dunia maya akan sulit dilakukan. Hal ini disebabkan oleh beberapa hal. Pertama, klaim tentang adanya pelanggaran kedaulatan suatu negara membutuhkan dukungan dari negara-negara lain yang mengakui kedaulatan negara tersebut.³⁵ Kedua, substansi hukum tentang upaya penegakan kedaulatan harus disepakati oleh semua negara yang terlibat.³⁶ Terakhir,

prosedur dan tindakan terhadap pelanggaran kedaulatan harus disetujui sebagai bentuk kerja sama dalam upaya mempertahankan diri dari serangan negara lain.³⁷ Hal ini menjadi sangat relevan apabila dihubungkan dengan upaya peretasan atau pengrusakan fasilitas jejaring komputer di suatu negara. Penyelidikan tentang tindakan pelanggaran kedaulatan tersebut tentunya akan melibatkan berbagai yurisdiksi yang membutuhkan adanya pembagian informasi antar negara-negara dan pengungkapan bukti pelanggaran yang mungkin tersimpan dan berasal dari yurisdiksi yang berbeda.³⁸

Kerja sama internasional di tingkat bilateral dan multilateral dalam tata kelola dunia maya telah dimulai sejak dua dekade silam. Pada awalnya, bentuk kerja sama ini masih terbatas dalam bentuk berbagai *best practice* antar satu negara dengan negara lain. Mengingat perkembangan teknologi internet yang makin pesat dan munculnya berbagai bentuk pelanggaran kedaulatan dunia maya yang semakin rumit dari tahun ke tahun, pemahaman umum tentang kerangka hukum keamanan dan tata kelola dunia maya menjadi semakin penting. Organisasi internasional seperti PBB dan *Organization of Economic Co-operation and Development* (OECD) mulai membahas berbagai kerja sama internasional dan menggagas resolusi mengenai keamanan dan tata kelola dunia maya. Keamanan dan tata kelola dunia maya bahkan telah menjadi salah satu agenda utama dalam sidang Majelis Umum PBB di beberapa tahun terakhir.

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.

³³ M. D. Caverty & Mauer V., *Power and security in the information age: Investigating the role of the state in cyberspace*, Routledge, 2016.

³⁴ *Ibid.*

³⁵ S. K. Gourley, *Cyber Sovereignty, Conflict and Cooperation in Cyberspace: The Challenge to National Security*, 2013, h.277.

³⁶ P. Cornish, D. Livingstone, D. Clemente, dan C. Yorke, *On Cyber Warfare*, Chatham House, 2010.

³⁷ *Ibid.*

³⁸ Y. Radziwill, *Cyber-Attacks and the Exploitable Imperfections of International Law*, Brill, 2015, h.101-108.

Oleh karena itu, Amerika Serikat akan melakukan segala upaya untuk mencegah perusakan infrastruktur jejaring dan pencurian informasi atau data rahasia dengan beralih 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 pengawasan jejaring internet, melalui kegiatan intelijen 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, mengungkap kerja sama 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.³⁹ 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.⁴⁰

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.⁴¹ 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.⁴²

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 2016.⁴³ Proses pengalihan atas pengelolaan *file root* dan server akan dilakukan oleh NTIA dan perusahaan

³⁹ G. Greenwald dan E. MacAskill, *loc. cit.*

⁴⁰ M. Hayden, *Ex-NSA chief: safeguards exist to protect Americans' privacy*, <http://edition.cnn.com/2013/08/01/opinion/hayden-nsa-surveillance/>, diakses 19 Juli 2016.

⁴¹ L. Schmidt, *Perspective on 2015 DoD Cyber Strategy*, Santa Monica CA: RAND Corporation, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA621794>, diakses 19 Juli 2016.

⁴² D. Sanger, 2015, *US decides to retaliate against China's hacking*, <http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html>, diakses 19 Juli 2016.

⁴³ 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_proposal-relatedtoiana_functionsstefinal.pdf, diakses 19 Juli 2016.

swasta, VeriSign, secara independen. Namun, dokumen pelaksanaan proses tersebut juga mengungkapkan bahwa terdapat masa percobaan untuk jangka waktu 3 bulan dalam proses pengalihan tersebut. Apabila dalam masa percobaan 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 menghalangi upaya penerapan sistem, kebijakan atau strategi negara lain berdasarkan prinsip kedaulatan. 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 Xi Jinping untuk menghadapi 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.⁴⁴ 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 melalui 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 salah satu tugas dalam upaya menjaga keamanan nasional.⁴⁵

Untuk menjelaskan pengertian tentang kedaulatan dan bagaimana upaya untuk menegakkan kedaulatan China di dunia maya dari Beijing, pemerintah China menjabarkan kedaulatan dunia maya dalam beberapa komponen kunci agar definisinya bisa dipahami. Bagian pertama kedaulatan maya mengacu pada 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.⁴⁶

Alasan utama mengapa pemerintah China merasa perlu untuk mempertahankan kedaulatannya di dunia maya adalah ketika pada tahun 2009 pemerintah Amerika Serikat mulai menggunakan internet sebagai sarana diplomasi dan pertukaran informasi untuk mendorong perubahan rezim secara damai di seluruh dunia.⁴⁷ Pemerintah China menganggap bahwa strategi ofensif yang diterapkan oleh Amerika Serikat akan digunakan untuk mengendalikan atau mengubah sistem dan jejaring informasi global demi kepentingan Amerika Serikat. Bahkan Amerika Serikat dikhawatirkan dapat membuat atau mengendalikan eskalasi konflik di suatu negara.⁴⁸ Oleh karena itu, pemerintah

⁴⁴ S. Yi, "Transform and construction: the design of national cybersecurity strategy and the capacity build in a post-Snowden age", *China Information Security*, Vol. 5, 2014, h. 41-43.

⁴⁵ D. M. Lampton, "Xi Jinping and the National Security Commission: policy coordination and political power", *Journal of Contemporary China*, Vol. 24, No. 95, 2015, h. 759-777.

⁴⁶ *Ibid*

⁴⁷ L. Jason, *Facebook, Twitter and Youtube are tools for diplomacy*, http://www.huffingtonpost.com/jason-liebman/perspective-on-digital-di_b_416876.html, diakses 20 Juli 2016.

⁴⁸ 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 20 Juli 2016.

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 menghalang-halangi negara-negara lain yang hendak melindungi kepentingan nasional mereka di dunia maya. Kekhawatiran atas penyalahgunaan model *multistakeholder* semakin bertambah dengan dirilisnya 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.⁴⁹

Sejak 2013, pemerintah China semakin giat mengupayakan perlindungan kedaulatan dunia maya sebagai prioritas utama dalam strategi keamanan nasional. Tantangan yang dihadapi saat ini adalah pengembangan teknologi canggih dan penyusunan definisi kedaulatan China 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 payung hukum dalam upaya

penegakan kedaulatan di dunia maya. 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 Transaksi 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 mendukung 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 bertanggung 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 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-undang No. 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

⁴⁹ C. de Bossey, Report of the Working Group on Internet Governance, <http://www.wgig.org/docs/WIGREPORT.pdf>, diakses 20 Juli 2016.

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 11/2008 dan PP 82/2012 telah meletakkan 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).⁵⁰ Secara umum, kedua Direktorat tersebut bertanggung jawab dalam merumuskan

⁵⁰ Direktorat Jenderal Sumber Daya, Pos dan Informatika Kemekominfo, Tugas dan fungsi, <http://kominfo.go.id/index.php/node/711/Tugas+dan+Fungsi>, diakses 21 Juli 2016.

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.⁵¹ 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)*.⁵² 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 Centre (id-SIRTI/CC)* yang berada di bawah pengawasan Direktorat Jenderal Penyelenggaraan Pos dan Informatika.⁵³

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.⁵⁴ Selain dari sektor pemerintah,

⁵¹ Direktorat keamanan informasi Kemenkominfo, <http://aptika.kominfo.go.id/index.php/profile/direktoratkeamanan-informasi>, diakses 21 Juli 2016.

⁵² GovCSIRT, Profil, <http://govcsirt.kominfo.go.id/tentangidgovcert/profil>, diakses 21 Juli 2016.

⁵³ ID SIRTII, struktur organisasi, <http://www.idsirtii.or.id/halaman/tentang/struktur-organisasi.html>, diakses 21 Juli 2016.

⁵⁴ Lembaga Sandi Negara, Tugas dan Fungsi, www.lemsaneg.go.id/index.php/profil/tugas-dan-fungsi/, diakses 21 Juli 2016.

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.⁵⁵

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 masyarakat 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.

⁵⁵ ID CERT, Profil, <http://www.cert.or.id/tentang-kami/id/> diakses 21 Juli 2016.

B. Inisiatif Kerja Sama Pengaturan Tata Kelola Dunia Maya Global

Pada tahun 2005, laporan dari satuan kerja tata kelola internet yang disponsori oleh PBB, menunjukkan bahwa pengelolaan sistem, file dan alokasi domain internet, sebenarnya berada di bawah kendali Pemerintah Amerika Serikat secara sepihak. Sejak itu, reformasi pemerintahan dunia maya berdasarkan prinsip-prinsip kesetaraan kedaulatan terus digulirkan untuk mengubah model tata kelola fasilitas-fasilitas utama dunia maya yang diwakili oleh pengelolaan file, sistem dan domain secara bersama dan lebih transparan.

Namun, reformasi yang disebutkan di atas belum menunjukkan hasil yang berarti. Hingga akhirnya, setelah keberadaan Program PRISM dibocorkan oleh Edward Snowden pada Maret 2014, pemerintah Amerika Serikat yang terdesak oleh tekanan internasional menyatakan bahwa kewenangan peraturan dan pengelolaan di IANA dan ICANN akan dialihkan ke sektor swasta yang diselenggarakan sebagai lembaga *multi-stakeholder*.

Agar perkembangan dari pengalihan wewenang dari pemerintahan ke pihak swasta tersebut lebih mudah dipahami, maka latar belakang dari pembentukan lembaga *multi-stakeholder* perlu dijelaskan terlebih dahulu. Pada era 1980-an, internet merupakan zona peraturan bebas yang tidak mengenal istilah tata kelola.⁵⁶ Saat itu teknologi internet dianggap sebagai kegiatan distribusi data melewati jaringan komputer yang menembus batas negara. Kondisi ini memicu dibentuknya *Internet Engineering Task Force* (IETF) sebagai inisiatif untuk mengembangkan standar internet dan mempelajari masalah-masalah teknik Internet melalui proses konsensus yang melibatkan berbagai individu dan lembaga non-pemerintah.

Di era 1990-an, mulai terdapat komersialisasi internet dan terjadi perebutan

⁵⁶ D. Drissel, "Contesting Internet governance: global dissent and disparities in the management of cyberspace resources", *The Internet Society II: Advances in Education, Commerce & Governance Transactions on Information and Communication Technologies*, Vol. 36, WIT Press, 2006.

alamat domain internet. Untuk memecahkan permasalahan tersebut, Pemerintah Amerika Serikat sebuah lembaga *hybrid multi-stakeholder* yakni ICANN, yang meliputi perusahaan, lembaga swadaya masyarakat (LSM) dan pejabat pemerintahan yang bertanggung jawab atas pengelolaan dan pengawasan infrastruktur internet yaitu, *Internet Protocol* (IP), nama domain, dan *root server*. Pemerintah Amerika Serikat berdalih bahwa ICANN tidak mengatur seluruh Internet dan tidak memiliki otoritas atas *cyber security*, kebijakan konten, perlindungan hak cipta, perlindungan privasi, pemeliharaan keanekaragaman budaya, atau menjembatani *digital divide*.⁵⁷ Namun, pada kenyataannya ICANN masih berada pada wilayah administrasi dan yurisdiksi Amerika Serikat. Oleh karena itu, berdasarkan kepada penafsiran atas kesetaraan kedaulatan di dunia maya, berbagai pihak telah berupaya untuk melakukan reformasi atas model pengelolaan dan pengendalian yang dilakukan Amerika Serikat tersebut.

Salah satu upaya yang menonjol adalah sebuah proposal yang disebut *NETMundial Initiatives* yang diusulkan oleh Brazil dan negara-negara lain yang tergabung pada konferensi NETMundial di Sao Paulo, pada April 2014. Ada tiga hal utama yang diusulkan pada proposal ini. Pertama, kerangka pengambilan keputusan dan peran Komite Penasihat Pemerintahan di ICANN harus ditingkatkan. Usul kedua bertujuan untuk memisahkan kebijakan ICANN terhadap pemerintahan dunia maya dari pengelolaan dan pengaturan nama *file root server*. Sedangkan usul terakhir bertujuan untuk melepaskan keterlibatan ICANN dalam pengelolaan server yang berada pada wilayah yurisdiksi Amerika Serikat, dan selanjutnya ICANN hanya perlu mengelola tiga server utama yang merupakan kerja sama antara ICANN dan sebuah perusahaan swasta, Verisign. Proposal ini sesungguhnya telah mencerminkan preferensi Brazil dan negara-negara lain untuk melepaskan diri dari ketergantungan terhadap

Amerika Serikat. Mereka berharap bahwa ICANN dapat melakukan pengawasan secara independen terhadap sejumlah *root server* dan negara-negara maju dapat mendisiplinkan dirinya sendiri dalam menjalankan tata kelola pemerintahan dunia maya.

Berbeda dengan *NETMundial Initiatives*, pada konferensi ICANN yang diadakan di Busan pada tahun 2014, India menawarkan proposal yang jauh lebih agresif. Pada proposal tersebut India mengusulkan bahwa tata kelola dunia maya seharusnya berada di bawah pengawasan ITU. Pada konferensi ITU di tahun yang sama, India juga mengusulkan agar ICANN mengalihkan seluruh teknologi dan wewenangnya ke ITU. Selain itu, India juga menyarankan agar struktur dunia maya dirombak ulang dengan mengacu pada tata kelola dan mekanisme sambungan langsung komunikasi internasional. Dengan cara ini, tiap negara memiliki semacam kode sambung yang harus diberikan apabila pihak dari negara lain hendak berhubungan atau membutuhkan akses atas data antar negara melalui Internet. Akibatnya, setiap negara dapat menjaga data-data penting di bawah yurisdiksinya sendiri. Pada konferensi ITU di Berlin, India kembali mengajukan proposalnya dan berpendapat bahwa ITU seharusnya berperan penting dalam manajemen internet dan tata kelola dunia maya.

C. 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,

⁵⁷ J. Kurbalija, *An Introduction to Internet Governance*, 4Th Edition, DiploFoundation, 2010.

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-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 negara-negara 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,⁵⁸ 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%.⁵⁹ 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.⁶⁰

⁵⁸ B. Sanou, *loc. cit*

⁵⁹ Internet World Stats, *Internet Users in the 20 Top Countries*, <http://www.internetworldstats.com/top20.htm>, diakses 9 Oktober 2016.

⁶⁰ International Telecommunication Union, *ITU Facts and Figures 2016*, <http://www.itu.int/en/media-centre/pages/2016-PR30.aspx>, diakses 9 Oktober 2016.

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 optik 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.

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.⁶¹ Pengelolaan infrastruktur dan sistem distribusi data seperti di atas sering digunakan sebagai contoh untuk membuktikan keberadaan dan hegemoni negara maju di dunia maya.⁶²

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.

⁶¹ SSAC, ICANN, *Overview and history of the IANA functions*. SAC067. <https://www.icann.org/en/system/files/files/sac-067-en.pdf>, diakses 28 Juli 2016.

⁶² 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, h.183.

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 aplikasi-aplikasi 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,⁶³ dan dengan demikian dapat mengurangi sikap saling tidak percaya yang ada saat ini. Penyusunan peraturan tersebut, bagaimanapun, membutuhkan modal kepercayaan di 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.

⁶³ S. D. Krasner, *loc. cit*

Pertama, para pemangku kepentingan belum dapat mengelola penggunaan sumber daya bersama secara kolektif,⁶⁴ untuk mengurangi upaya eksploitasi dan pemungutan dana oleh pihak-pihak tertentu yang telah menggunakan sumber daya itu terlebih dulu.⁶⁵ 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.⁶⁶

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.⁶⁷ Akibatnya, harapan untuk melakukan kerja sama keamanan bergantung pada keseimbangan antara jumlah senjata dan kemampuan pertahanan masing-masing negara.⁶⁸ 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.⁶⁹ Dalam bidang kejahatan komputer, sulit untuk menentukan apakah kode pemrograman yang dibuat hendak digunakan untuk tujuan pertahanan atau untuk menyusup dan/atau menyerang jejaring komputer 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 pemantauan dan pengumpulan data intelijen di dunia maya.⁷⁰ 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.⁷¹ 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

⁶⁴ E. Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge: Cambridge University Press, 1990, h. 108.

⁶⁵ M. Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups*, Cambridge: Harvard University Press, 1965, h. 76.

⁶⁶ 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.

⁶⁷ C. L. Glaser, *The Security Dilemma Revisited*, *World Politics*, Vol. 50, No. 1, 1997, h. 171–201.

⁶⁸ R. Jervis, "Cooperation Under the Security Dilemma", *World Politics*, Vol. 30, No. 2, 1978, h. 167–214.

⁶⁹ 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 19 Juli 2016.

⁷⁰ J. A. Lewis dan G. Neuneck, *The Cyber Index: International Security Trends and Realities*, Geneva: United Nations Institute for Disarmament Research (UNIDIR), 2013.

⁷¹ G. Smith, "Security Chief's Cyberwar Testimony Seen As Veiled Threat To Enemies", *The Huffington Post*, http://www.huffingtonpost.com/2013/03/14/security-chief-cyberwar_n_2875516.html, diakses 19 Juli 2016.

menolak sama sekali proposal India tersebut 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 initiative* 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.

D. Kerja Sama Internasional dalam Tata Kelola Dunia Maya

Masih adanya ketidaksepakatan di antara masyarakat internasional tentang konsepsi tata kelola dunia maya menunjukkan bahwa perdebatan mengenai hal ini akan terus berlangsung. Dengan mempertimbangkan berbagai perspektif dan preferensi masing-masing negara, sebuah kerangka normatif yang mengatur perilaku penggunaan fasilitas dunia maya sehingga dapat meningkatkan transparansi dan mempermudah terjalannya kerja sama antar negara, merupakan pendekatan yang paling mungkin dilakukan untuk menjaga stabilitas dunia internasional di dunia maya.

Oleh karena itu, dialog antara pemerintah negara-negara perlu terus dilakukan agar pemahaman dan peraturan pengelolaan dunia maya yang seragam segera dapat diwujudkan. Sejak dua dekade silam, masyarakat internasional sebenarnya telah mulai mendefinisikan parameter dan preferensi hukum yang dapat memberikan kesempatan pada setiap negara untuk menunjukkan batas kedaulatan mereka di dunia maya.⁷²

⁷² K. W. Abbott dan D. Snidal, "Hard and Soft Law in International Governance", *International Organization*, Vol. 54, No. 3, 2000, h. 421-456.

Pada tahun 2013, Majelis Umum PBB merekomendasikan kerja sama dalam pengelolaan dunia maya, antara lain melalui pertukaran informasi tentang strategi nasional, pembentukan organisasi yang menangani insiden keamanan informasi (CSIRT), pembagian pengalaman insiden keamanan dunia maya, dan mekanisme kerja sama antar penegak hukum.⁷³ Langkah-langkah ini merupakan langkah nyata yang dapat dilakukan masing-masing negara untuk membiasakan diri dengan ranah dunia maya, dengan tujuan untuk membangun kepercayaan yang pada akhirnya mencapai konsensus tentang perilaku yang dapat diterima di dunia maya.

Sebagai contoh, *Organization for Security and Cooperation in Europe* (OSCE) merilis sebuah dokumen kerja sama dalam penanggulangan risiko konflik antar negara yang disebabkan oleh penyalahgunaan teknologi informasi dan komunikasi. Dokumen ini menetapkan bahwa negara-negara yang berpartisipasi dalam organisasi tersebut secara sukarela memberikan masukan, memfasilitasi kerja sama antara badan-badan nasional yang kompeten untuk saling bertukar informasi, mengadakan konsultasi, berbagi *best practice*, dan memfasilitasi kerja sama bilateral dalam menyelesaikan permasalahan keamanan dunia maya yang melibatkan beberapa negara anggota.⁷⁴

Dengan demikian, walaupun jaringan komunikasi global sebagian besar dikelola oleh perusahaan-perusahaan swasta, pendekatan multilateralisme telah dianggap sebagai pendekatan yang lebih tepat dalam tata kelola dunia maya.⁷⁵ Tentunya kebijakan pemerintah di tingkat multilateral perlu diselaraskan dengan

⁷³ Majelis Umum PBB, *loc. cit.*

⁷⁴ Organization for Security and Cooperation in Europe (OSCE), Decision No. 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict stemming from the use of information and communication technologies, <http://www.osce.org/pc/109168?download=true>, diakses 30 Agus-tus 2016.

⁷⁵ A. Segal, *Cyberspace Governance: The Next Step*, Council on Foreign Relations, <http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397>, diakses 30 Agustus 2016.

kegiatan operator dan pemangku kepentingan lainnya, seperti perusahaan-perusahaan swasta yang mengandalkan infrastruktur dunia maya sebagai upaya dari pemerintah untuk membangun transparansi dan mendapatkan kepercayaan dari para pelaku bisnis.⁷⁶

Konferensi di mengenai pengelolaan dunia maya, *Convention on Cyberspace*, yang diadakan di London, Budapest, Seoul, dan terakhir di Den Haag pada bulan April 2015, mewakili semangat multilateral dalam pengelolaan dunia maya. Dalam konferensi ini dibahas kerangka pembangunan dan sinergi antara berbagai kerangka kerja politik dan strategis sebagai upaya untuk menjalin hubungan internasional pengelolaan dunia maya yang lebih dapat diprediksi dan stabil. Pada akhirnya, tujuan dari kerja sama internasional dalam tata kelola dunia maya adalah untuk membangun pengarusutamaan perspektif dunia maya dalam penegakan kedaulatan suatu negara. Pengarusutamaan tersebut berfokus pada kesadaran akan permasalahan keamanan dunia maya dan langkah-langkah pencegahan pelanggaran yang dilaksanakan seluruh lapisan baik pemerintahan, perusahaan atau kelompok masyarakat sipil.⁷⁷

III. Kesimpulan dan Saran

A. Kesimpulan

Beberapa kesimpulan yang dapat diperoleh dari pemaparan di atas adalah sebagai berikut:

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

2. 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 tersebut bertujuan agar seluruh negara mendapatkan manfaat ekonomis dan politis yang seimbang dalam pelaksanaan pengelolaan dunia maya. Inisiatif 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.
3. Walaupun cenderung bersifat reaktif, pemerintah Indonesia telah memiliki berbagai lembaga dan sarana penunjang dalam upaya menegakkan kedaulatan di dunia maya. Selain produk hukum, kegiatan

⁷⁶ B. Baseley-Walker, *Transparency and confidence-building measures in cyberspace: towards norms of behaviour*, Disarmament Forum Confronting Cyberconflict, Geneva: United Nations Institute for Disarmament Research (UNIDIR), 2011, h. 31–40.

⁷⁷ M. Finnemore, "Cultivating International Cyber Norms", *America's Cyber Future Security and Prosperity in the Information Age*, Volume II, 2011, h. 89–101.

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.

B. Saran

Hal-hal yang perlu diperhatikan agar upaya penegakan kedaulatan di dunia maya menjadi lebih baik adalah:

1. Polarisasi struktur kelembagaan tata kelola dunia maya telah menambah dinamika politik dunia. Pemerintah Indonesia perlu memahami dan mengenali sepenuhnya usulan yang dibawa oleh Amerika Serikat maupun China, mengingat kedua negara tersebut merupakan negara adidaya yang memiliki kepentingan besar terhadap Indonesia. Pemerintah Indonesia juga perlu untuk terus melakukan upaya diplomatik dan kerja sama internasional agar upaya penegakan kedaulatan dunia maya tidak menciderai kesepakatan investasi yang telah dibuat dengan negara lain, pihak swasta dan investor asing.
2. Sebagaimana dilakukan oleh pemerintah Amerika Serikat dan China, lembaga pemerintah dan non pemerintah yang memiliki wewenang untuk meningkatkan pertahanan dan keamanan nasional di dunia maya sebaiknya bertugas dalam satu koordinasi yang terintegrasi. Lemsaneg sebagai lembaga pemerintah Indonesia yang memiliki fungsi dan tugas pokok terkait persandian diharapkan dapat menjadi pusat pengembangan dan pengelolaan dunia maya nasional. Lembaga ini harus menjadi lembaga otoritas tunggal dalam keamanan kedaulatan dunia maya di Indonesia. Oleh karena itu, Lemsaneg sangat membutuhkan dukungan lembaga-lembaga lain seperti,

ID-CERT, Gov-CSIRT, id-SIRTI/CC sebagai tulang punggung dalam sistem pertahanan keamanan Indonesia di dunia maya yang komprehensif.

DAFTAR PUSTAKA

Buku

- Barcomb, K. D., Krill, R., Mills R., dan Saville, M., *Establishing cyberspace sovereignty, Prosiding 7th International Conference on Information Warfare and Security*, Academic Conferences Limited, 2012.
- Baseley-Walker, B., *Transparency and confidence-building measures in cyberspace: towards norms of behaviour*, Disarmament Forum Confronting Cyberconflict, Geneva: United Nations Institute for Disarmament Research (UNIDIR), 2011.
- Cavelty, M. D. & Mauer V., *Power and security in the information age: Investigating the role of the state in cyberspace*, Routledge, 2016
- Cornish, P., Livingstone, D., Clemente, D., dan Yorke, C., *On Cyber Warfare*, Chatham House, 2010.
- Crawford, J., *Chance, Order, Change: The Course of International Law*, The Hague: Hague Academy of International Law, 2014.
- Czosseck, C., dan Geers, K., *Borders in cyberspace: can sovereignty adapt to the challenges of cyber security?*, *The Virtual Battlefield: Perspectives on Cyber Warfare*, Vol.3, 2009.
- Drissel, D., *Contesting Internet governance: global dissent and disparities in the management of cyberspace resources*, *The Internet Society II: Advances in Education, Commerce & Governance Transactions on Information and Communication Technologies*, Vol. 36, WIT Press, 2006.

- Gourley, S. K. *Cyber Sovereignty, Conflict and Cooperation in Cyberspace: The Challenge to National Security*, 2013.
- Koskenniemi, M.. *From apology to utopia: the structure of international legal argument*. Cambridge University Press, 2006.
- Kurbalija, J., *An Introduction to Internet Governance*, 4Th Edition, DiploFoundation, 2010.
- Lewis, J. A. dan Neuneck, G., *The Cyber Index: International Security Trends and Realities*, Geneva: United Nations Institute for Disarmament Research (UNIDIR), 2013.
- Lyons, P. A., *Cyberspace and the law: your rights and duties in the on-line world*, Information Processing and Management, ed. Cavazos, E.A., Morin, G., Vol. 31, No. 6, 1995.
- 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: Harvard University Press, 1965.
- Ostrom, E., *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge: Cambridge University Press, 1990.
- Radziwill, Y. *Cyber-Attacks and the Exploitable Imperfections of International Law*, Brill, 2015.
- Ross, A., *A Textbook of International Law*, London: Longmans, Green & Co, 1967.
- Sarikakis, K., *Mapping the ideologies of Internet policy*, *Ideologies of the Internet*, Cresskill, Hampton Press, 2006.
- Schmitt, M.N., *Tallinn manual on the international law applicable to cyber warfare*, Cambridge University Press, 2013.
- Simma, B. (ed.), *The Charter of the United Nations: a commentary*, Vol. 2, Oxford: Oxford University Press, 2002.
- Tsagourias, N., *The Legal Status of Cyberspace*, Chapters, 2015.
- Ziolkowski, K. (ed.). *Peacetime Regime for State Activities in Cyberspace*, Tallinn: NATO CCD COE Publications, 2013.
- Jurnal**
- Abbott, K. W. dan Snidal, D., "Hard and Soft Law in International Governance", *International Organization*, Vol. 54, No. 3, 2000.
- Ajami, F., "The Arab spring at one", *Foreign Affairs*, Vol. 91, No. 2, 2012.
- Bradshaw, S., DeNardis, L., Hampson, F., Jardine, E., dan Raymond, M., "The Emergence of Contention in Global Internet Governance", *Global Commission on Internet Governance Paper Series*, Vol.17, 2015.
- Brown, G. D., "The Wrong Questions about Cyberspace", *Military Law Review*, Vol. 217, No. 214, 2013.
- Buchan, R., "Cyber attacks: unlawful uses of force or prohibited interventions?", *Journal of Conflict and Security Law*, Vol. 17, No. 2, 2012.
- Finnemore, M., "Cultivating International Cyber Norms", *America's Cyber Future Security and Prosperity in the Information Age*, Volume II, 2011.
- Gittlen, S., "Surprise IP address system test creates a stir", *Network World*, Vol. 15, No. 6, 1998.
- Hamid, A. G., "Maritime Terrorism, the Straits of Malacca, and the Issue of State Responsibility", *Journal of International and Company Law*, Vol. 15, 2006.
- Jensen, E.T., "Cyber Sovereignty: The Way Ahead", *Texas Interntaional Law Journal*, Vol. 50, 2015.
- Jervis, R., "Cooperation Under the Security Dilemma", *World Politics*, Vol. 30, No. 2, 1978.

- Kanuck, S., "Sovereign Discourse on Cyber Conflict Under International Law", *Texas Law Review*, Vol. 88, No. 7, 2010.
- Kastenberg, J.E., "Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law", *Air Force Law Review*, Vol. 64, 2009.
- Kavanagh, C., "Cybersecurity, Sovereignty, and U.S. Foreign Policy", *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy*, Vol. 37, 2015.
- Krasner, S. D., "Abiding sovereignty", *International Political Science Review*, Vol. 22, No. 3, 2001.
- Krekel, B., Adams, P., dan Bakos, G., "Occupying the information high ground: Chinese capabilities for computer network operations and cyber espionage", *International Journal of Computer Research*, Vol. 21, No. 4, 2014.
- Lampton, D. M., "Xi Jinping and the National Security Commission: policy coordination and political power", *Journal of Contemporary China*, Vol. 24, No. 95, 2015.
- Mueller, M., Schmidt, A. and Kuerbis, B., "Internet Security and Networked Governance in International Relations", *International Studies Review*, Vol. 15, No. 1, 2013.
- Glaser, C. L., "The Security Dilemma Revisited", *World Politics*, Vol. 50, No. 1, 1997.
- Perritt Jr. H.H., "Cyberspace and State Sovereignty", *Journal of International Legal Studies*, Vol. 3, 1997.
- 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.
- Stephen, H., "Revisiting the Estonian cyber attacks: digital threats and multinational responses", *Journal of Strategic Security*, Vol. 4, No. 2, 2011.
- Wriston, W.B., "Technology and Sovereignty", *Foreign Affairs*, Vol. 67, 1988.
- Yi, S., "Transform and construction: the design of national cybersecurity strategy and the capacity build in a post-Snowden age", *China Information Security*, Vol. 5, 2014.

Makalah

- Heintschel von Heinegg, W., *Legal Implications of Territorial Sovereignty*, Prosiding 4th International Conference on Cyber Conflict (CYCON 2012), 2012.

Portal

- Cave, D., *It's time for ICANN to go*, http://www.salon.com/2002/07/02/gilmore_2/, diakses 28 Juli 2016.
- Chandrasekaran, R., *Internet reconfiguration concerns federal officials*, The Washington Post, <https://www.washingtonpost.com/archive/business/1998/01/31/internet-reconfiguration-concerns-federal-officials/c98b71a0-8e4a-4aab-96f6-1868c81fe60c/>, diakses 28 Juli 2016.
- De Bossey, C., *Report of the Working Group on Internet Governance*, <http://www.wgig.org/docs/WGIGREPORT.pdf>, diakses 20 Juli 2016.
- 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 7 Juli 2016.
- GovCISRT, Profil, <http://govcsirt.kominfo.go.id/tentangidgovcert/profil>, diakses 21 Juli 2016.
- Gross, D., *Google quits censoring search in China*, <http://www.cnn.com/2010/TECH/03/22/google.china/>, diakses 7 Juli 2016.
- Hayden, M., *Ex-NSA chief: safeguards exist to protect Americans' privacy*, <http://edition.cnn.com/2013/08/01/opinion/hayden-nsa-surveillance/>, diakses 19 Juli 2016.

- ICANN, *Overview and history of the IANA functions*. SAC067. <https://www.icann.org/en/system/files/files/sac-067-en.pdf>, diakses 28 Juli 2016.
- Id CERT, Profil, <http://www.cert.or.id/tentang-kami/id/>, diakses 21 Juli 2016.
- Id SIRTII, Struktur organisasi, <http://www.idsirtii.or.id/halaman/tentang/struktur-organisasi.html>, diakses 21 Juli 2016.
- Internet World Stats, Internet Users in the 20 Top Countries, <http://www.internetworldstats.com/top20.htm>, diakses 9 Oktober 2016.
- International Telecommunication Union, ITU Facts and Figures 2016, <http://www.itu.int/en/mediacentre/pages/2016-PR30.aspx>, diakses 9 Oktober 2016.
- Jason, L., *Facebook, Twitter and Youtube are tools for diplomacy*, http://www.huffingtonpost.com/jason-liebman/perspective-on-digital-di_b_416876.html, diakses 20 Juli 2016.
- Kemenkominfo, Direktorat Jenderal Sumber Daya, Pos dan Informatika Kemekominfo, Tugas dan fungsi, <http://kominform.go.id/index.php/node/711/Tugas+dan+Fungsi> diakses 21 Juli 2016.
- Kemenkominfo, Direktorat keamanan informasi Kemenkominfo, <http://aptika.kominform.go.id/index.php/profile/direktoratkeamanan-informasi>, diakses 21 Juli 2016.
- Kessler, G., *Wikileaks's unveiling of secret State Department cables exposes US diplomacy*, The Washington Post, <http://www.washingtonpost.com/wp-dyn/content/article/2010/11/28/AR2010112802395.html>, diakses 7 Juli 2016.
- Kruger, L.G., Internet Governance and the Domain Name System: issues for congress. Library of Congress: Congressional Research Service, <http://www.davidellis.ca/wp-content/uploads/2012/05/kruger-internet-governance-2016.pdf>, diakses 28 Juli 2016.
- Lembaga Sandi Negara, Tugas dan Fungsi, <http://www.lemnane.go.id/index.php/profil/tugas-dan-fungsi/>, diakses 21 Juli 2016.
- 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 20 Juli 2016.
- Majelis Umum PBB, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174, diakses 8 Juli 2016.
- 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_proposal_relatedtoiana_functionsstefinal.pdf, diakses 19 Juli 2016.
- NTIA, Department of Commerce, *NTIA announces intent to transition key internet domain name functions*, <https://www.ntia.doc.gov/press-release/2014/ntia-announcesintent-transition-key-internet-domain-name-functions>, diakses 21 Juli 2016.
- Organization for Security and Cooperation in Europe (OSCE), *Decision No. 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict stemming from the use of information and communication technologies*, <http://www.osce.org/pc/109168?download=true>, diakses 30 Agustus 2016.
- Philip S.C., *ICANN@ 15: Born in the USA— But Will It Stay?* http://www.circleid.com/pdf/ICANN_at_15_Born_in_the_USA_But_will_it_Stay.pdf, diakses 28 Juli 2016.

- Pirker, B., *Territorial sovereignty and integrity: peacetime regime for state activities in cyberspace*, <http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf>, diakses 28 Juli 2016.
- Rekha, J., *A Model for Internet Governance and Implications for India*, Indian Institute of Management Ahmedabad, Research and Publication Department, <http://icmrindia.vikalpa.com/assets/snippets/workingpaperpdf/8992574912015-03-23.pdf>, diakses 28 Juli 2016.
- Sanger, D., 2015, *US decides to retaliate against China's hacking*, <http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html>, diakses 19 Juli 2016.
- Sanou, B., *ICT Facts and Figures*, <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>, diakses 7 Juli 2016.
- Schmidt, L., *Perspective on 2015 DoD Cyber Strategy*, RAND Corporation, Santa Monica CA, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA621794>, diakses 19 Juli 2016).
- Segal, A., *Cyberspace Governance: The Next Step*, Council on Foreign Relations, <http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397>, diakses 30 Agustus 2016.
- Smith, G., *Security Chief's Cyberwar Testimony Seen As Veiled Threat To Enemies*, The Huffington Post, http://www.huffingtonpost.com/2013/03/14/security-chief-cyberwar_n_2875516.html, diakses 19 Juli 2016.
- 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 19 Juli 2016.