

Cyberpolitics sebagai Perspektif Baru Memahami Politik di Era Siber

Cyberpolitics as A New Perspective in Understanding Politics in The Cyber Era

Jerry Indrawan*

*Program Studi Ilmu Politik, Universitas Pembangunan Nasional Veteran, Jakarta

email: jerry_indrawan18@yahoo.co.id

Riwayat Artikel

Diterima 7 Maret 2019

Direvisi 2 April 2019

Disetujui 2 Mei 2019

Abstract

Political science studies have developed from conventional perspectives, marked by the use of physical means of campaign, to the era of non-conventional politics, where the use of cyber medium is more prevalent. The use of cyber medium in the study of political science has resulted in many sectors, from democracy, security, defense, social and cultural affairs, education, to political campaigns to conducted through the cyber medium. Cyberpolitics is a new concept that is very interesting to discuss, as interesting as it is to be studied in detail. Cyberpolitics will be the future of political campaign for all political stakeholders, especially those running in political contests. Political activism has already been replaced by a form of virtual communication. Cyberpolitics can in this regard help democracy work as it should. The aim of this research is to understand cyberpolitics more deeply, and that requires an interdisciplinary perspective, not just political science. The significance of this research is to provide a different perspective to the public about the development of political science, which now moves towards the use of cyber technology. This paper will discuss the study of cyberpolitics, which is seen as a new perspective in understanding politics in the cyber era. The author recommends that studies discussing the concept of cyberpolitics be discussed and researched more intensively among political science scholars, so that the combination of political science and information technology in the future can mutually enrich the scientific understanding of both disciplines.

Keywords: Cyberpolitics; Politics in Cyber Era; Cyber Security and Defense.

Abstrak

Kajian ilmu politik sudah berkembang dari yang bersifat konvensional, yaitu menggunakan sarana kampanye yang bersifat fisik, menuju ke era politik non-konvensional, yaitu penggunaan medium siber. Penggunaan medium siber dalam kajian ilmu politik membuat banyak sektor, seperti demokrasi, keamanan, pertahanan, sosial dan budaya, pendidikan, sampai kampanye politik, dilakukan melalui medium siber. Cyberpolitics menjadi sebuah konsep baru yang sangat menarik untuk dibahas, serta diteliti lebih dalam. Cyberpolitics akan menjadi masa depan kampanye politik bagi setiap stakeholder politik, terutama bagi mereka yang akan berkontestasi dalam kompetisi pemilihan politik. Aktivisme politik sudah mulai digantikan oleh bentuk komunikasi secara virtual. Cyberpolitics dengan demikian dapat membantu demokrasi berjalan sebagaimana mestinya. Tujuan penelitian ini adalah untuk memahami cyberpolitics secara lebih dalam, sehingga membutuhkan perspektif inter-disipliner, tidak hanya ilmu politik. Kegunaan penelitian ini adalah untuk memberikan perspektif yang berbeda kepada khalayak umum tentang perkembangan ilmu politik, yang sekarang mengarah ke arah penggunaan teknologi siber. Makalah ini akan membahas kajian cyberpolitics, yang dilihat sebagai sebuah perspektif baru dalam memahami politik di era siber. Penulis merekomendasikan bahwa kajian-kajian yang membahas tentang konsep cyberpolitics mulai lebih banyak dibahas dan diteliti di kalangan akademisi-akademisi ilmu politik, agar perpaduan antara ilmu politik dengan teknologi informasi ke depannya dapat semakin memperkaya khazanah keilmuan masing-masing.

Kata Kunci: Cyberpolitics; Politik di Era Siber; Keamanan dan Pertahanan Siber.

Pendahuluan

Ilmu politik adalah sebuah ilmu yang terus menerus mengalami perubahan karena sifatnya yang dinamis dan menyesuaikan dengan ruang lingkungannya. Begitu pula dengan perkembangan di sektor teknologi informasi (TI) yang terjadi dengan sangat cepat. Politik mau tidak mau harus menyesuaikan dengan perubahan yang cepat tersebut, yang terjadi di dunia TI. Untuk itu, perkembangan kajian ilmu politik di era teknologi informasi seperti sekarang ini membuat penulis merasa tertantang untuk memberikan analisa subjektif terkait hubungan antara keduanya. Pengkajian terhadap hubungan antara ilmu politik dan TI bermuara pada munculnya konsep *cyberpolitics* atau politik siber.

Penulis berpendapat bahwa konsep *cyberpolitics* akan menjadi sarana utama bagi ilmu politik untuk berakselerasi di masa depan karena memiliki ruang lingkup yang sangat luas dan mampu menjangkau banyak *stakeholder*. Untuk itu, mengkaji *cyberpolitics* membutuhkan beragam perspektif dan kajian keilmuan yang berkaitan, seperti teknologi informasi, komunikasi, keamanan, pertahanan, pendidikan, sampai sosial dan budaya. Namun, ke depan kajian ini menawarkan perspektif yang menarik untuk diteliti dan diamati lebih lanjut karena merupakan sebuah kajian yang baru, tapi dapat masuk ke dalam banyak sektor-sektor lainnya.

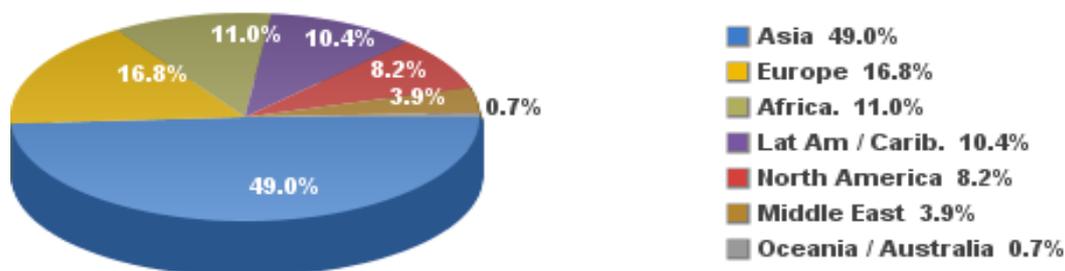
Menilik perkembangan politik (demokrasi) di ranah digital di Indonesia, selama hampir 5 tahun memerintah kita melihat intensitas Presiden Joko Widodo dalam mendorong terwujudnya demokrasi digital di berbagai sektor pemerintahan. Dengan beragam instrumen, seperti *e-government*, misalnya, kualitas pelayanan publik normatif dapat terus ditingkatkan. Berbagai bentuk partisipasi masyarakat juga dapat terus diakomodasi dan difasilitasi melalui beragam media sosial.

Di Indonesia, istilah demokrasi digital memang kerap diidentikkan dengan keriuhan di media massa yang mewarnai beberapa kontestasi politik besar, seperti Pilpres 2014, Pilkada Jakarta 2017, dan tentu saja Pilpres 2019 pada April lalu. Padahal makna demokrasi digital tidak bisa direduksi sebatas pada ramainya keterlibatan masyarakat pada peristiwa tersebut, yang konon telah menimbulkan polarisasi yang cukup tajam di tengah masyarakat hingga kini.

Sebenarnya, dalam beberapa tahun terakhir, ada beberapa praktik positif dari demokrasi digital yang sudah berjalan di Indonesia, misalnya, dalam pelibatan partisipasi publik dalam penggalangan petisi daring, aplikasi tentang pelaporan fasilitas publik atau korupsi yang dilakukan arapat negara, sampai informasi-informasi politik tentang proses kontestasi politik, baik lokal, maupun nasional. Dunia internet menyediakan ruang dan fitur berlimpah untuk dimanfaatkan guna mendorong praktik demokrasi yang lebih mapan. Medium digital bagi kaum milenial menjadi pilihan yang sangat rasional bagi mereka untuk tahu lebih banyak tentang politik. Hal ini bisa diakibatkan karena keterbatasan waktu, maupun juga sikap mental praktis (instan) yang mereka idap seiring perkembangan zaman yang semakin *high-tech*.

Sekalipun istilah "*cyberpolitics*" terkesan baru, namun sesungguhnya menggunakan medium-medium yang kita semua sudah kenal, yaitu ruang siber. Kita akan memulai dengan memberikan fakta bahwa peran siber dalam dunia politik sangatlah besar. Sejalan dengan perkembangan internet yang sangat cepat di tahun 1990-an, istilah ruang siber di dalam politik dunia (*cyberspace in world politics*). Awalnya hanya membahas doktrin-doktrin yang terkait keamanan nasional, namun berkembang menjadi pusat informasi karena membahas arus informasi (*traffic information*)

Internet Users in the World by Regions - June 30, 2018



Source: Internet World Stats - www.internetworldstats.com/stats.htm
 Basis: 4,208,571,287 Internet users in June 30, 2018
 Copyright © 2018. Miniwatts Marketing Group

Gambar 1. Pengguna Internet di Dunia Berdasarkan Wilayah

yang sangat padat di internet. Karena itu, AS, Jepang, dan beberapa negara Eropa Barat sudah mulai melakukan transisi menuju masyarakat informasi. Saat ini, jaringan global internet meliputi 4.2 miliar manusia di bumi (kurang lebih 55.1% populasi dunia). Secara aktif mengembangkan “*internet of things*” (IoT) yang kedepannya akan mengikat tidak hanya manusia, tetapi juga jaringan, perangkat komputer, peralatan sehari-hari, dan barang-barang lainnya. Diramalkan, pada tahun 2020, akan ada 50 miliar perangkat yang memiliki koneksi internet.¹

Melihat pentingnya dan meningkatnya kuantitas dari penggunaan internet di kalangan masyarakat dunia, *cyberpolitics* dapat memainkan peran yang sangat sentral dalam pewujudan praktik-praktik politik di masa depan. Bisa jadi, di masa mendatang internet akan menggantikan televisi sebagai medium utama komunikasi politik. Internet akan menjadi sarana di mana seluruh aktivitas politik berpusat, jika masyarakat dunia lebih menggunakan “*world wide web*” daripada saluran-saluran politik konvensional. Pertemuan-pertemuan politik akan dilakukan secara maya, bukan lagi nyata. Bahkan,

¹ Hans Vestberg, “Ericsson CEO to Shareholders: 50 Billion Connections 2020,” *Ericsson*, 13 April 2010, diakses 7 Februari 2019, <http://www.ericsson.com/thecompany/press/releases/2010/04/1403231>

memilih (*vote*) pun dilakukan secara daring. *Cyberpolitics* menganalisis konten diskusi politik di internet, serta untuk melihat bagaimana internet digunakan secara politis. Internet akan tumbuh terus seiring dengan meningkatnya orang yang menggunakan, sehingga kondisi ini akan mengubah sifat (*nature*) dari ilmu politik yang selama ini dipraktikkan.

Cyberpolitics akan merangsang minat generasi milenial untuk lebih terlibat dalam politik karena medium siber yang digunakannya sangat pas untuk mereka. Di era yang serba cepat dan mudah ini, keterlibatan masyarakat, terutama milenial, di dunia politik sudah seperti layaknya memesan makanan atau taksi *online*. Politik bukan lagi sebuah ilmu kaku yang hanya menasar kalangan berumur, namun bisa menjadi sebuah tren baru. Mengingat politik berurusan dengan banyak aspek dalam kehidupan manusia, sudah sepantasnya generasi milenial memiliki kepedulian terhadapnya. Dengan *cyberpolitics*, upaya untuk “peduli” itu sendiri menjadi semakin dimudahkan karena aksesnya pun mudah.

Tulisan ini akan membahas bagaimana ilmu politik di era milenial ini dijalankan dalam berbagai sektor kehidupan bangsa dan negara, seperti pendidikan, komunikasi,

demokrasi, sistem sosial dan budaya masyarakat, teknologi dan informasi, serta keamanan dan pertahanan, yang akan dibahas secara khusus di bagian subbab terakhir. Praktik-praktik untuk menjalankannya pun sudah tidak lagi konvensional, melainkan melalui medium siber, yang penulis istilahkan sebagai *cyberpolitics*.

Metode Penelitian

Dalam metode penelitian dibahas metode yang merupakan pendekatan praktis dalam setiap penelitian ilmiah. Hal ini dimaksudkan untuk memudahkan bagi setiap peneliti mengetahui suatu peristiwa atau keadaan yang diinginkan. Dalam tulisan ini, penulis melakukan telaah konsep secara kualitatif dengan metode deskriptif. Metode ini biasa digunakan untuk menjelaskan masalah pada penelitian ini karena metode ini adalah sebuah metode penelitian yang membuat gambaran mengenai kejadian untuk menggambarkan secara sistematis, faktual dan akurat mengenai fakta-fakta, sifat-sifat serta hubungan antar fenomena yang diteliti.² Penulis menggunakan metode ini karena tulisan ini hanya menggunakan sumber pustaka tanpa melakukan kajian lapangan langsung. Metode deskriptif berguna untuk menjelaskan secara umum temuan-temuan pustaka yang penulis dapatkan terkait *cyberpolitics*. Desain penelitian yang bersifat deskriptif juga dapat diartikan sebagai prosedur pemecahan masalah yang diselidiki dengan menggambarkan atau melukiskan keadaan subjek atau objek penelitian (individu, komunitas, lembaga masyarakat, dan lain-lain) pada saat sekarang berdasarkan fakta-fakta yang tampak atau sebagaimana adanya.³ Penulis melakukan proses studi pustaka dengan mengunjungi berbagai perpustakaan (*library research*) dan

mengumpulkan data-data primer melalui bahan-bahan tulisan dalam berbagai bentuk, yang diharapkan dapat memudahkan penulis dalam melakukan penelitian ini.

Mengenal *Cyberpolitics*

Sebelum membahas *cyberpolitics*, mari kita pahami dulu apa yang disebut dengan siber. *Cyberspace* (ruang siber) adalah sebuah ruang maya atau ruang elektronik, di mana sebuah masyarakat virtual yang terbentuk melalui komunikasi yang terjalin dalam sebuah jaringan komputer. Dengan kata lain, ruang siber adalah sebuah ruang yang tidak dapat terlihat, di mana terjadi hubungan komunikasi sehingga informasi menjadi tersebar, serta tidak ada jarak fisik dari masing-masing pengguna, dan juga tidak dapat dibatasi oleh kedaulatan suatu negara.⁴

Menurut David Bell yang dikutip dari Rulli Nasrullah, ruang siber adalah sekumpulan data, representasi grafik demi grafik, dan hanya bisa diakses melalui komputer. Istilah ruang siber muncul jauh sebelum teknologi internet berkembang. Kata ini muncul dari permainan video games, di mana pemainnya menyakini bahwa semua bangunan, ruang, interaksi, maupun benda-benda yang ada di permainan tersebut merupakan sebuah kenyataan, meski kenyataan tersebut tidak bisa dijangkau oleh mereka (*some place you can't see, but you know it's there*). Ruang siber lebih dekat dengan penggambaran "*consensual hallucination*" atau "*non-linear reality*", yang kurang lebih berarti realitas semu. Bell dalam Nasrullah, lebih lanjut menggunakan kata ruang siber untuk membawa pikiran menuju tingkat atau level selanjutnya dari kesadaran manusia.⁵

Menurut Stefan Fenz, ruang siber adalah sebuah metafora (kiasan) untuk menjelaskan sebuah wilayah atau medan yang tidak ada

2 Lexy Moelong, *Metode Penelitian Kualitatif* (Bandung: Remaja Rosdakarya, 2001), 3.

3 Hadari Nawawi, *Metode Penelitian Bidang Sosial* (Yogyakarta: Gadjah Mada University Press, 1997), 63.

4 Nudirman Munir, *Pengantar Hukum Siber Indonesia* (Depok: Rajawali Press, 2017), 19.

5 Rulli Nasrullah, *Komunikasi Antarbudaya di Era Budaya Siber* (Jakarta: Kencana, 2014), 20.

secara nyata, yang diciptakan oleh sistem komputer. Ruang ini merepresentasikan dunia nyata melalui objek dan komunikasi virtual yang terjadi diantara penggunaanya. Sistem daring, sebagai contoh, menciptakan sebuah ruang siber di mana setiap orang dapat saling berkomunikasi via email, melakukan penelitian, bahkan untuk sekedar melihat-lihat barang belanjaan.⁶

Istilah ruang siber secara sederhana digunakan untuk merujuk pada sebuah jaringan, yang saat ini dikenal dengan nama internet. Namun, jika kita memahami definisi ruang siber, maka ia didefinisikan melebihi daripada internet karena semua transaksi atau peristiwa yang tidak terjadi di dunia nyata, terjadi di ruang siber.⁷ Internet, atau kita sebut juga *interconnection-networking*, adalah seluruh jaringan komputer yang saling terhubung dengan menggunakan standar sistem global *Transmission Control Protocol/Internet Protocol Suite* (TCP/IP) sebagai protokol pertukaran paket untuk melayani miliaran pengguna di seluruh dunia.⁸

Siber dalam bahasa Inggris (*cyber*) menurut Eneken Tikk-Ringas, adalah kalau tidak kata sifat, atau sebagai *combining form*, yaitu sebuah istilah linguistik yang digunakan untuk menggabungkan satu kata dengan kata lain. Contoh *combining form* adalah *cyberpolitics*, sebuah kajian baru di bidang siber yang ingin penulis kupas di dalam buku ini. Di beberapa negara, ruang siber memiliki definisinya sendiri-sendiri. Internet dianggap sebagai inti dari ruang siber. Kita juga harus memahami bahwa istilah siber digunakan dalam berbagai jenis pengertian yang sangat tergantung pada konteksnya, seperti motivasi pribadi atau motivasi politik misalnya. Kemudian, amati apa sarannya, *server* atau komputer pribadi,

pemerintah atau dunia usaha.⁹

Di Jerman, ruang siber memiliki definisi, sebagai sebuah ruang virtual dari semua sistem *Information Technology* (IT) terhubung pada tingkatan data dalam skala global. Sistem IT dalam ruang virtual yang terisolir bukanlah bagian dari ruang siber. Di Perancis, ruang siber adalah ruang komunikasi yang diciptakan oleh interkoneksi di seluruh dunia dari perangkat otomatis yang memproses data digital. Kemudian, di Inggris, ruang siber adalah domain interaktif terbuat dari jaringan digital yang digunakan untuk menyimpan, memodifikasi, dan mengkomunikasikan informasi. Terakhir, Selandia Baru mendefinisikan ruang siber sebagai jaringan global yang terdiri dari infrastruktur informasi independen, jaringan telekomunikasi, dan sistem pengolahan komputer, di mana komunikasi daring dilakukan.¹⁰

Ruang siber adalah sebuah fakta dalam kehidupan sehari-hari manusia saat ini karena sifatnya yang memiliki cakupan dan skala yang luas, serta praktis saat ini ruang siber dapat ditemukan di mana saja. Ruang siber, termasuk internet dan ratusan juta komputer yang tersambung jaringan internet, lembaga yang memungkinkan hal tersebut terjadi, serta pengalaman yang diberikannya, telah menjadi karakteristik dasar dari dunia di mana kita hidup saat ini. Kondisi ini telah menciptakan sebuah realitas baru kepada hampir semua manusia di dunia, baik belahan dunia maju, maupun dunia negara-negara berkembang. Realitas itulah yang nantinya akan membentuk *cyberpolitics*. Berikut adalah pembahasannya.

Politik siber sangat terkait dengan ruang siber, seperti yang dibahas sebelumnya. Untuk itu, sebelum penulis menjelaskan secara lebih detail tentang *cyberpolitics*, kita

6 Stefan Fenz, *Cyberspace Security: A Definition and A Description of Remaining Problems* (University Vienna and Institute of Government & European Studies, 2005), 2.

7 *Ibid*, 3.

8 Nudirman Munir, *Pengantar Hukum Siber Indonesia*, 17.

9 Eneken Tikk-Ringas, *Cyber Security: Solutions of Tomorrow, Experience of Yesterday*, dalam Bo Huldt, dkk (ed), *The Emerging Global Security Environment* (Vasteras: The Swedish National Defense College, 2013), 151.

10 *Ibid*, 152-153.

pahami dulu hubungan antara ruang siber dengan *cyberpolitics*. Secara umum, ruang siber dikategorikan dalam isu-isu “*low politics*”, sebuah terminologi yang menunjukkan latar belakang proses pengambilan keputusan oleh negara. Kebalikannya, isu-isu “*high politics*” biasanya terkait dengan keamanan nasional, institusi politik, keputusan strategis negara, kepentingan, dan nilai-nilai sebuah negara. Begitu pula nasionalisme, partisipasi politik, kontestasi politik, konflik, kekerasan, dan perang, yang sering juga dianggap sebagai isu-isu *high politics*.

Sekalipun demikian, isu-isu *low politics* tidak selalu berada dibawah permukaan. Apabila dinamika-dinamika, terutama terkait ruang siber dan politik, kerap terjadi, interaksi-interaksi yang biasa terjadi di ranah *high politics*, lama-lama akan tergantikan. Jika ini terjadi, maka isu-isu *low politics* akan menggantikannya. Dengan demikian, ruang siber akan menjadi pusat perhatian politik karena merupakan bagian dari isu-isu *high politics*. Terlebih, dalam beberapa tahun terakhir masalah-masalah yang terkait dengan ruang siber telah bergerak melampaui isu-isu *low politics*. Apa yang mampu dilakukan di ranah siber juga dapat menjadi ancaman bagi keamanan nasional.

Menurut Nazli Choucri, *cyberpolitics* adalah sebuah terminologi yang diciptakan, berkaitan dengan interaksi manusia (politik) yang meliputi kegiatan-kegiatan, seperti siapa mendapat apa, kapan, dan bagaimana, yang dimungkinkan untuk terjadi melalui ranah ruang siber sebagai sebuah arena baru pertarungan dengan pengandai-andaian dan realitanya sendiri. Meskipun ada perbedaan dalam perspektif di seluruh dunia, namun tetap terdapat pemahaman ilmiah umum tentang arti “politik”. Kompleksitas yang muncul terkait awalan “*cyber*” itulah yang membedakan semantik yang baru dibangun ini.¹¹

11 Choucri, Nazli. *Cyberpolitics in International Relations*.

Penulis berpendapat secara umum, bahwa *cyberpolitics* adalah sebuah kegiatan politik yang dilakukan melalui ruang siber. *Cyberpolitics* berkenaan dengan kegiatan-kegiatan politik, seperti pendidikan politik, komunikasi politik, kampanye politik, implementasi demokrasi, keamanan dan pertahanan, negara, serta kegiatan sosial, budaya, dan juga masyarakat. Dahulu, kegiatan-kegiatan seperti ini biasa dilakukan di dunia nyata, serta terkait dengan aktivitas-aktivitas politik. Namun saat ini, kegiatan-kegiatan ini mulai banyak dilakukan juga di ruang siber, karena lebih praktis dan memiliki cakupan dampak yang jauh lebih luas.

Atas dasar itulah, seperti yang dikatakan Choucri, ada semantik baru yang dibangun dalam terminologi politik. Semantik tersebut adalah *cyberpolitics*, di mana kegiatan-kegiatan politik yang memiliki signifikansi besar terhadap jalannya sebuah negara, pemerintahan, termasuk roda kehidupan masyarakat, dilakukan melalui ruang siber. *Cyberpolitics* berkembang menjadi sebuah istilah yang bisa dipakai untuk menjelaskan aktivitas-aktivitas politik modern, yang tidak perlu lagi menggunakan ruang nyata, melainkan cukup ruang siber yang memiliki pengandai-andaian dan realitanya sendiri.

Di bidang pendidikan politik, *cyberpolitics* berperan memberikan pemahaman dan kesadaran (*awareness*) politik kepada masyarakat umum, yang di dunia siber sering diistilahkan sebagai netizen. Netizen dikenal sering bertindak tanpa regulasi yang jelas di dunia siber, apalagi terkait dengan isu-isu politik. Hal ini terjadi karena tidak ada edukasi politik kepada mereka, sehingga mereka tidak paham mana yang boleh dan mana yang tidak. Pendidikan *cyberpolitics* akan menawarkan sebuah konsep yang bernama pendidikan politik siber untuk mencerdaskan netizen tentang konsep-konsep, serta masalah-masalah yang terkait dunia politik.

Cambridge: MIT Press (2012): 3.

Cyberpolitics juga sangat terkait dengan ilmu komunikasi, terutama turunannya, yaitu komunikasi politik. Ruang siber adalah medium komunikasi *netizen*. *Cyberpolitics* adalah medium komunikasi *netizen* untuk berkomunikasi tentang politik. Makanya, *cyberpolitics* akan sangat berkaitan dengan bagaimana kajian politik dimainkan di media-media baru, seperti media daring, media sosial, dll. Komunikasi *cyberpolitics* pun dapat dilakukan untuk pembentukan opini publik dan propaganda melalui media-media baru tadi.

Komunikasi dalam *cyberpolitics* kemudian menjadi bagian dari kampanye *cyberpolitics*. Di saat penggunaan dunia maya dan ruang siber makin luas dan gencar dilakukan masyarakat, kampanye politik akan lebih efektif dilakukan melalui medium tersebut. Melakukan *branding* politik terhadap para calon-calon legislatif, kepala daerah, sampai presiden dan wakil presiden pun dilakukan lewat ranah siber. *Cyberpolitics* akan menjadi masa depan kampanye politik bagi setiap *stakeholder* politik, terutama bagi mereka yang akan berkontestasi dalam kompetisi pemilihan politik.

Demokrasi sebagai sistem politik yang banyak digunakan di dunia adalah katalis yang sempurna bagi *cyberpolitics*. Implementasi *cyberpolitics* akan memiliki efek luas di wilayah-wilayah yang demokratis. *Cyberpolitics* membutuhkan ruang yang bebas berkreasi dan menjamin adanya pengakuan hak dan kebebasan berpendapat (*freedom of speech*). Sebuah konsep yang sangat demokratis. Itulah mengapa demokrasi dan *cyberpolitics* dapat berjalan seiringan, bahkan *cyberpolitics* dapat penulis katakan sebagai pelengkap demokrasi. *Netizen* pun semakin gemar menyuarakan opininya melalui ruang siber terkait masalah-masalah sehari-hari, di mana hal tersebut dikategorikan sebagai sebuah tindakan politik. Aktivisme politik sudah mulai digantikan oleh bentuk komunikasi secara virtual.

Selanjutnya, sistem sosial dan budaya masyarakat dewasa ini, khususnya di kota, sudah mengarah ke arah budaya siber. Sistem budaya lokal saat ini menghadapi derasnya serbuan budaya asing, yang masuk melalui medium ruang siber. Di dalam sistem sosial dan budaya masyarakat saat ini, terjadi akulturasi, asimilasi, globalisasi, dan modernisasi lewat ranah siber. Perpaduan ini melahirkan sebuah generasi baru, yaitu generasi milenial. *Cyberpolitics* adalah alat yang tepat untuk memberikan kesadaran politik dalam bentuk pendidikan politik siber, kepada generasi milenial tersebut. Ke depan, masyarakat harus siap menghadapi budaya siber yang semakin mengglobal, serta menciptakan realitas sendiri kepada setiap individu.

Selanjutnya, *cyberpolitics* dan ruang siber adalah dua hal yang saling berkaitan. *Cyberpolitics* tidak akan bisa berjalan tanpa rel yang bernama ruang siber. Ruang siber akan berjalan hampa tanpa dibumbui oleh konten-konten politik di dalamnya. Ruang siber diciptakan melalui teknologi inovasi, ini adalah tempat yang memungkinkan pengguna untuk terlibat dalam kegiatan yang *borderless* dan *bounderless*. Ruang ini menawarkan peluang baru untuk kompetisi, kontestasi, kekuasaan, pengaruh, persaingan, dan konflik, yang kesemuanya adalah elemen-elemen dasar dari politik itu sendiri.

Internet, yang adalah bagian dari ruang siber itu sendiri, telah menjadi bagian integral dari berkembangnya jaringan infrastruktur komunikasi global. Konten informasi menjadi sangat luas dan berkembang di tingkat yang sangat tinggi. Informasi-informasi baru diciptakan dan disebarluaskan, termasuk mekanisme-mekanisme baru diciptakan untuk memfasilitasi konten-konten yang dibagikan tersebut. Ruang siber yang sempat dianggap sebagai domain netral sebagai hasil inovasi teknologi saja, sekarang didominasi oleh konten-konten politik. Ruang siber menjadi

tempat berkompetisinya kepentingan-kepentingan, sekaligus arena konflik dan persaingan politik, pihak-pihak yang “bermain” di dunia politik, termasuk negara.¹²

Hubungan antara politik dan ruang siber telah memperkuat sejumlah konsep-konsep tentang politik yang dikemukakan David Easton, Harold Laswell, dan lain-lain. Ia telah memperluas manifestasi ilmu politik, meningkatkan potensi untuk berpartisipasi politik secara luas, menciptakan kemungkinan-kemungkinan baru untuk mengekspresikan pandangan-pandangannya, menyuarakan posisi atau sikap politik, termasuk bergabung dalam aktivitas-aktivitas politik. Saat ini, malah sulit untuk mengidentifikasi bidang-bidang politik yang tidak berhubungan dengan siber. Ketika sulit, bahkan tidak mungkin untuk menggambarkan apa saja implikasi dari ruang siber bagi politik secara umum dan perilaku politik secara khusus, beberapa pengamat dan analis secara bertahap berkumpul untuk membahasnya.¹³

Sebagai contoh, politik di ruang siber digambarkan dalam buku Richard N. Rosecrance tahun 1999, berjudul: “*The Rise of the Virtual State*”. Esensi dari negara virtual terletak pada kemampuannya untuk mengumpulkan kekuatannya finansial dan gagasan, kemudian mengubahnya menjadi sumber pengaruh global. Sekalipun terlihat sederhana, namun memiliki implikasi yang luas. Konsep baru ini menantang fundamen dari politik tradisional yang berdasarkan pada kompetisi memperebutkan teritori, perdagangan, kekuatan militer, untuk menggantinya dengan parameter-parameter baru, seperti pendidikan, keahlian, pengetahuan, pengelolaan, serta berbagai bentuk dari kekuatan pikiran (*brain power*). Rosecrance berpendapat bahwa semua negara secara bertahap akan berjalan ke arah negara virtual, bahkan beberapa negara akan dengan cepat melakukannya dan lebih

menyakinkan daripada yang lain. Rosecrance menyarankan investasi pada pengetahuan adalah sumber dasar dari kekuatan nasional dan efektivitas sosial.¹⁴

Contoh lain digambarkan pada artikel yang terbit bulan Juli tahun 2000, berjudul: “*CyberPolitics in International Relations*”. Artikel ini menyoroti domain virtual sebagai bidang penelitian yang penting untuk politik internasional dan hubungan antar-negara. Berjalannya aktivitas politik siber di berbagai isu, sejalan dengan perubahan-perubahan di dalam diskursus dan interaksi politik, telah menimbulkan efek yang mendunia, serta menyebabkan munculnya artikulasi dan agregasi kepentingan-kepentingan baru. *Cyberpolitics* juga mendorong terjadinya perdebatan-perdebatan terkait bagaimana memandang sebuah kebijakan politik. Di sini kita melihat bahwa *cyberpolitics* memiliki peranan untuk mengubah agenda-agenda politik, baik global maupun nasional.¹⁵

Kondisi di atas mengarahkan kita pada kemungkinan terjadinya sinergi antara *cyberpolitics* (arena baru interaksi politik) dan keberlanjutan (teori dan kebijakan). Dibentuk oleh konsep-konsep baru, seperti dematerialisasi, de-sentralisasi, de-nasionalisasi, dan de-teritorialisasi, akan muncul sebuah kondisi di mana ruang siber akan menjadi sarana penyaluran kepuasan dan ketidakpuasan dari masyarakat. Kemungkinan isu-isu politik berkembang di dalam sebuah ranah “politik baru” (*new politics*), sehingga membentuk sebuah sifat dasar yang akhirnya mengubah landasan dari kekuasaan (*power*) dan pengaruh (*influence*) yang selama ini dikenal dalam ilmu politik konvensional, sangatlah besar. Bersamaan dengan munculnya ruang siber, arena baru untuk berpolitik mulai terbentuk. Boleh jadi, ruang politik akan menjadi saksi dari munculnya bentuk baru dari politik, yaitu *cyberpolitics*. Karena itu, ranah siber haruslah

12 *Ibid*, 8.

13 *Ibid*, 10.

14 *Ibid*

15 *Ibid*, 10-11.

dilihat tidak hanya sebagai sarana artikulasi dan agregasi kepentingan politik, tetapi sebagai pengganda yang penting (*important multipliers*).¹⁶

Di negara-negara industri maju dengan sistem politik yang kompetitif, interaksi dan komunikasi di ruang siber telah menjadi hal yang biasa dalam kehidupan politik. Di AS sebagai contoh, penggunaan ruang siber untuk kepentingan politik menunjukkan beberapa pola yang khas. Dalam konteks politik sehari-hari, komunikasi lewat medium siber sudah berjalan optimal dan berkembang pesat. Masyarakat menggunakan email untuk mendiskusikan peristiwa-peristiwa politik, termasuk menyebarkan “link” yang berhubungan. Banyak dari mereka yang mencoba memengaruhi teman mereka untuk bersama-sama terlibat dalam diskusi politik di dalam *blog/blog* di mana penggunaanya dapat membagi pendapat mereka sesuai topik-topik debat yang diadakan.¹⁷

Kelompok-kelompok politik mengumpulkan donasi melalui situs mereka dan pendukungnya dapat mengirimkan sumbangannya melalui kartu kredit secara daring. Kelompok-kelompok politik pun dapat merencanakan pertemuan-pertemuan umum dengan menyebarkan informasi di internet agar semakin banyak orang yang hadir. Dengan menggunakan email dan situs, penyelenggara dapat mengordinasikan usaha mereka ke seluruh pelosok negeri.¹⁸

Pengamat mencatat bahwa partai Demokrat pertama kali menggunakan internet saat mereka sama sekali tidak menguasai Gedung Putih atau pun Kongres, namun medium siber memberikan mereka kesempatan baru untuk mengekspresikan pandangannya. Partai Republik juga menggunakan medium siber karena mereka percaya media massa konvensional (koran dan televisi) lebih bersimpati kepada partai saingannya. Mereka lebih menggunakan ranah siber sebagai cara

untuk menyampaikan opini dan pandangannya, daripada menggunakan *platform* partai yang resmi.¹⁹

Kampanye di era Revolusi Industri 4.0 seperti sekarang ini dilakukan lebih masif melalui internet, sehingga menjadi bagian dari *cyberpolitics*. Sebuah *blog* atau situs, atau bahkan hanya sebuah akun Instagram atau Facebook, dapat dipergunakan untuk merekayasa suatu citra kelompok kepentingan politik tertentu. Hal ini kemudian berkembang dan dipergunakan untuk pengenalan sebuah gagasan atau ide politik tertentu kepada khalayak atau suatu kelompok tertentu yang diharapkan mendapatkan *feedback*, timbal balik, atau tanggapan. Kampanye melalui media daring saat ini merupakan bentuk kampanye yang paling banyak dikerjakan oleh hampir semua kelompok pemangku kepentingan politik. Format pengemasan informasinya pun beragam dan berlapis-lapis, dari penggunaan situs, *blog*, koran, dan majalah daring, serta dilengkapi juga dengan pembuatan akun media sosial. Semua hal ini adalah bagian integral dalam *cyberpolitics*.

Pesan-pesan dari suatu kampanye politik lazimnya memuat gagasan-gagasan yang ditawarkan oleh para kandidat atau partai politik kepada para khalayak calon pemilih. Pesan tersebut lazimnya berisi butir-butir pembicaraan mengenai berbagai persoalan kebijakan. Butir-butir pembicaraan yang memuat gagasan-gagasan utama kampanye tersebut penyampaiannya diulang berkali-kali agar menciptakan kesan akhir mendalam pada calon pemilih. Kebanyakan kampanye politik suka mempertahankan gaya kemasan pesan mencakupan luas agar khalayak calon pemilih paling potensial tertarik. Pesan yang dikemas dengan cakupan terbatas, apalagi sempit, dapat mengurangi minat calon pemilih, dan bahkan memperlambat pengenalan para kandidat.²⁰

16 *Ibid*, 11-12.

17 *Ibid*, 142.

18 *Ibid*, 142-143.

19 *Ibid*, 143.

20 Solatun Dulah Sayuti, *Komunikasi Pemasaran Politik* (Bandung: Remaja Rosdakarya, 2014), 117.

Dalam kampanye politik, peran manajer kampanye (*campaign manager*) dan konsultan politik (*political consultant*) juga diperlukan, terutama jika bisa dilakukan secara siber. Hal ini karena kampanye politik memerlukan sebuah organisasi manajerial yang mampu secara profesional merumuskan, merancang, mengendalikan, serta mengimplementasikan atau mengoperasikan aktivitas kampanye politiknya. Oleh karenanya, seorang manajer kampanye profesional diperlukan untuk memimpin, mengorganisasikan, dan mengordinasikan operasi kampanye politik yang diminta kandidat atau partai politik kepadanya. Para manajer kampanye, beserta timnya, melakukan kampanye yang jauh lebih *feasible* dan lebih mengena dengan situasi calon pemilih audiens kampanye. Seorang manajer kampanye haruslah seorang yang mengerti visi, misi, tujuan, dan sasaran politik yang digagas kandidat atau partai politik yang diusungnya. Secara bersamaan, ia juga harus mampu memimpin manajerial pengelolaan kampanye politik untuk memenangkan kandidat dan partai politik tersebut.²¹

Teknologi komunikasi yang berbasis internet, seperti media sosial, dll, telah memungkinkan komunikasi dalam berbagai bentuknya menjadi jauh lebih cepat dan efisien. Teknologi ini mampu menghubungkan dan melibatkan warga negara dalam jumlah yang massal dan mencapai audiens dalam jumlah besar. Teknologi ini juga dipergunakan untuk penggalangan biaya kampanye, mengumpulkan dan mengorganisasikan relawan kampanye, serta membentuk dan mengaktifkan komunitas yang menjadi pendukung partai politik dan kandidatnya.²²

Konsultan politik tentu sangat penting fungsinya dalam pemasaran dan kampanye politik di negara-negara penganut demokrasi. Posisi dan peranan mereka terlihat dalam

pengembangan dan produksi isi kandungan publikasi politik. Konsultan politik juga mengolah informasi tentang situasi dan kondisi lawan politik, kemudian menggunakannya sebagai bahan rujukan tindakan dan aktivitas kampanye. Para konsultan politik juga tidak jarang bekerja untuk menata bagian organisasi partai politik tertentu, misalnya penataan publikasi, penataan keuangan, sampai penataan pengelolaan kaderisasi dan pendidikan politik. Mereka juga melakukan penelitian ilmiah yang bermanfaat untuk mendukung program pemasaran politik partai dan kandidat mereka.²³

Konsultan politik juga muncul dalam sosoknya sebagai pengelola sistem *polling* dan riset politik. Produknya kemudian menjadi bagian dari strategi kampanye partai politik dalam kontestasi pemilihan umum. Sebagian konsultan politik lainnya menawarkan diri dengan tampilan sebagai pengamat dan analis politik, yang oleh karena beberapa prestasinya di dalam menganalisis suatu rangkaian situasi politik dan ketepatan prediksi mereka. Karena sering tampil di media massa, terutama televisi, para konsultan politik berusaha memanfaatkan medium itu untuk meningkatkan popularitas mereka, untuk kemudian menawarkan jasa mereka kepada partai politik.²⁴

Konsultan politik saat ini juga sudah mulai merambah ranah siber, dengan fokus pada kampanye-kampanye politik di ranah daring saja. mereka menyadari bahwa kampanye politik masa depan adalah sebuah kontestasi maha dahsyat karena menggunakan ruang siber dalam pelaksanaannya. Untuk itu, konsultan politik akan menyarankan pada kandidat yang akan bertarung dalam pilkada, pileg, maupun pilpres, agar memfokuskan kampanyenya di ranah siber. Di sinilah peran konsultan kampanye *cyberpolitics* sangat dibutuhkan. Selain hemat biaya, ruang siber sangat efektif untuk menjangkau khalayak luas.

21 *Ibid*, 118.

22 *Ibid*, 133.

23 *Ibid*, 124.

24 *Ibid*, 126.

Konsultan politik masa depan akan banyak bermain di *cyberpolitics* karena meniru dunia perdagangan (*commerce*), di mana pemasaran dan penjualan sebuah produk sudah menggunakan ruang siber (*e-commerce*). Konsultan politik juga menggunakan konsep yang sama dari pemasaran sebuah produk di dunia dagang, hanya produknya adalah entitas politik yang harus dipasarkan sedemikian rupa kepada khalayak umum. Penggunaan *cyberpolitics* dalam kerja-kerja konsultan politik adalah keharusan karena konsultan politik profesional tidak mungkin lagi menggunakan cara-cara konvensional dalam mem-branding kliennya.

Cyberpolitics dengan demikian menjadi ranah dalam berinteraksi politik di masa depan. Semua *stakeholder* bidang politik akan menggunakan medium siber untuk mengejar kepentingannya masing-masing, baik untuk memilih maupun dipilih. Ruang siber akan menjadi jembatan antara dunia nyata dengan *constructive reality*, di mana politik akan menjadi “pihak” yang mengambil banyak keuntungan darinya. Realita ini membuat cakupan dari ilmu politik menjadi sangat luas, sehingga menawarkan perspektif baru dalam memahaminya.

Keamanan dan Pertahanan Siber

Pada bagian terakhir ini penulis akan membahas tentang *cyberpolitics* dan kaitannya dengan keamanan dan pertahanan negara. Masalah keamanan dan pertahanan negara adalah bagian yang esensial dari *cyberpolitics* karena setiap kebijakan yang dibuat di sektor ini berasal dari pejabat publik, yang notabene adalah orang-orang politik. Untuk itu, politik era siber juga terkait dengan perumusan kebijakan negara di sektor keamanan dan pertahanan negara.

Mari kita bahas keamanan terlebih dahulu. Paradigma keamanan nasional telah bergeser kepada aspek yang lebih luas yaitu termasuk

jaminan keamanan pribadi warga negara. Kewajiban pokok dari suatu negara adalah memberikan keamanan terhadap warganya tersebut termasuk keamanan dari berbagai kejahatan siber. Setiap saat warga negara dapat merasa terancam pada aset yang dimilikinya. Privasi dan berbagai informasi rahasia dapat dengan mudah dihancurkan oleh para pelaku kejahatan siber ini, di mana bila eskalasinya semakin meluas, dapat membuat keresahan yang meluas pada masyarakat. Dalam jangkauan yang lebih luas, keterbatasan penguasaan teknologi negara dan belum adanya regulasi yang lebih tegas mengenai pertahanan siber dapat membahayakan negara secara nyata. Negara lain ataupun kelompok dengan kepentingan tertentu dapat dengan mudah memasuki ranah infrastruktur vital yang dimiliki negara kita.²⁵

Ruang siber merupakan ruang virtual yang terbentuk dari hasil penyatuan antara manusia dan teknologi. Teknologi yang dimaksud ialah teknologi informasi dan komunikasi. Oleh sebab itu, ada banyak terminologi dan interpretasi yang dihubungkan dengan konsep keamanan dan pertahanan siber. Hal ini menyebabkan, konsep keamanan dan pertahanan siber tidak lagi hanya menyentuh wilayah teknologi tapi telah menjadi ancaman terhadap keamanan nasional (sekuritisasi). Sebelumnya, diskusi tentang keamanan nasional sangat jarang dihubungkan dengan teknologi. Namun, seiring dengan meningkatnya ancaman serangan siber domestik dan internasional, terutama pasca peristiwa 9/11, maka muncul kesadaran untuk mempopulerkan bahwa keamanan dunia maya bukanlah sekedar persoalan proteksi *password* yang sederhana.²⁶

25 Bagus Artiadi Soewardi, “Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia”, *Media Informasi Ditjen Potan Kemhan*, (Maret 2013): 32.

26 Dewi Triwahyuni dan Tine Agustin Wulandari, “Strategi Keamanan Cyber Amerika Serikat”, *Jurnal Ilmu Politik dan Komunikasi Universitas Komputer Indonesia*, Vol. 6, No. 1 (Juni 2016): 110.

Keamanan siber lebih jauh membutuhkan serangkaian strategi karena menyangkut kepentingan nasional. Perkembangan teknologi informasi juga telah memberikan perubahan signifikan mengenai konsep keamanan, kini ruang interaksi tidak bisa hanya dibatasi seara fisik, tapi juga meluas ke ruang siber. Konsekuensinya, negara harus beradaptasi dengan perkembangan ini, karena konsep keamanan siber sudah saatnya ditetapkan sebagai salah satu “wilayah” negara yang jaga keamanannya sebagaimana kewajiban negara mengamankan teritorialnya. Apalagi, serangan siber tidak hanya terjadi pada institusi publik saja, namun juga menyerang institusi pemerintah.²⁷

Atas dasar itulah, keamanan siber saat ini dilihat sebagai bagian dari kebijakan yang dibuat oleh sektor keamanan negara, yang tidak lagi menggunakan kekuatan bersenjata (*use of force*), namun cara-cara non-koersif lainnya. Kebijakan keamanan siber digunakan untuk menghadapi risiko ekonomi dan kebebasan sipil, spionase, termasuk serangan militer atau teroris, yang kesemuanya dilakukan melalui medium internet. Menggunakan perspektif mazhab Kopenhagen terkait sekuritisasi, apapun yang membentuk ancaman terhadap sebuah kelompok, entitas yang memiliki nilai-nilai tertentu, cara hidup, atau ideologi, dapat dikategorikan sebagai masalah keamanan.²⁸

Kemudian pertahanan siber. Pertahanan siber sendiri adalah langkah-langkah proaktif untuk mendeteksi atau mendapatkan informasi terkait gangguan siber, serangan siber, atau operasi siber yang akan datang, atau untuk menentukan sumber dari mana operasi tersebut berasal, termasuk meluncurkan serangan terlebih dulu, pencegahan, atau kontra-operasi siber terhadap sumber ancamannya (*A proactive measure for detecting*

or obtaining information as to a cyber intrusion, cyber attack, or impending cyber operation or for determining the origin of an operation that involves launching a preemptive, preventive, or cyber counter-operation against the source).²⁹ Pertahanan siber meliputi tugas-tugas, seperti melindungi, mendeteksi, merespon, dan memulihkan.

Terminologi pertahanan siber merujuk pada semua tindakan untuk mempertahankan ruang siber oleh militer melalui cara-cara yang tepat untuk mendapatkan tujuan strategis. Pertahanan siber adalah sistem yang terintegrasi, terdiri dari implementasi semua tindakan terkait ICT (*Information Communication Technology*), keamanan informasi, CNO (*Computer Network Operations*), termasuk bantuan fisik dari angkatan bersenjata. Karena itulah, pertahanan siber sering digunakan dalam konteks militer, sekalipun dapat pula dikaitkan dengan kriminalitas dan tindakan spionase. NATO (*North Atlantic Treaty Organization*) mendefinisikan pertahanan siber sebagai kemampuan untuk mengamankan pengiriman dan pengelolaan layanan dalam operasional sistem informasi dan komunikasi sebagai respons terhadap potensi aktual kejahatan yang akan segera akan terjadi, yang bersumber di ruang siber.³⁰

Di AS, upaya penanganan masalah keamanan dan pertahanan siber sudah jauh lebih komprehensif dan efektif. Undang-Undang Patriot (*Patriot Act*), setara UU Keamanan Nasional di sana, memungkinkan pemerintah melakukan pengawasan secara maksimal di bidang siber, khususnya untuk masalah-masalah ancaman keamanan nasional. Pemerintahan Obama saat itu malah mampu membawa ruang siber ke dalam domain kebijakan nasional AS melalui aturan UU Patriot tadi. Kebijakan berorientasi ke

27 Solange Ghernaoui, *Cyber Power: Crime, Conflict and Security in Cyberspace* (Lausanne: EPFL Press, 2013): 126.

28 Tikk-Ringas, *The Emerging Global*, 155-156.

29 William H. Boothby, *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors* (The Hague: TMP Asser Press, 2014), 223.

30 NATO CCDCOE, “Cyber Definitions,” NATO CCDCOE, tanpa tanggal, diakses 12 Februari 2019, <https://ccdcoe.org/cyber-definitions.html>

siber (*cyber-centered public policy*) melahirkan *US Cyber Command* yang merupakan bagian dari angkatan bersenjata AS, diluar angkatan darat, laut, dan udara. Komando Siber lahir dari kesadaran Departemen Pertahanan AS yang menyatakan bahwa ruang siber adalah medan perang yang kelima, setelah darat, laut, udara, dan ruang angkasa. Keputusan ini merupakan jawaban dari banyaknya insiden pencurian data dan teknologi militer AS.

Dijadikannya ruang siber sebagai matra perang keempat (darat, laut, udara, dan ruang siber) cukup beralasan, karena semua negara pasti ingin meningkatkan kemampuan untuk mengamankan diri dari serangan musuh. Kemajuan pesat teknologi informasi dan komunikasi dewasa ini akan menjadi landasan penting bagi pengembangan doktrin militer di masa mendatang. Dengan demikian teknologi informasi dan komunikasi akan sangat mempengaruhi perubahan strategi militer. Selanjutnya, Israel diketahui mempunyai sebuah unit khusus bernama Unit 8200 yang mempunyai spesialisasi *cyber warfare* dibawah *Israel Defense Forces* (IDF). Salah satu catatan keberhasilan yang fenomenal dari unit ini adalah ketika Unit 8200 berhasil menghentikan operasi radar senjata anti pesawat udara Suriah. Bahkan serangan *worm* Stuxnet terhadap sistem komputer fasilitas nuklir Iran pada awal tahun 2011 ini disebut-sebut merupakan hasil kerja dari unit ini.³¹

Saat ini Indonesia pun mulai mengarahkan corong meriamnya ke arah pertempuran dunia maya. Kementerian Pertahanan menyikapi perang dunia maya ini dengan mulai aktif menggelar seminar maupun lokakarya yang melibatkan Kementerian/ LPNK, Perguruan Tinggi, Pakar dan pihak lainnya untuk merumuskan sistem teknologi informasi terpadu dalam menghadapi perang teknologi informasi melalui dunia maya, yang dikemas dalam konsep Sistem Pertahanan

31 Soewardi, "Perlunya Pembangunan Sistem Pertahanan Siber", 33.

Dunia Maya. Pada tanggal 23 Oktober 2012 menteri pertahanan telah membentuk Tim Kerja Pertahanan Dunia Maya, yang diketuai oleh Dirjen Pothan Kemhan dan beranggotakan unit terkait pada Satuan Kerja Kementerian Pertahanan, serta narasumber dari Kementerian/ LPNK, perguruan tinggi, para pakar maupun tokoh masyarakat dunia maya, dimana tim kerja ini secara garis besar bertugas merumuskan *roadmap* strategi nasional pertahanan negara yang berkaitan dengan ancaman siber, serta menyiapkan pembentukan organisasi pertahanan siber berskala nasional (*National Cyber Defense*). Demikian juga TNI, dalam konteks yang lebih luas dan modern, kedaulatan suatu bangsa pada saat ini tidak hanya dalam ruang lingkup tanah, air dan udara, tetapi juga memasuki kedaulatan di ruang siber, di mana TNI juga harus memainkan peranan yang signifikan.³²

Serangan siber tanpa menghadirkan kekuatan militer secara fisik di negara lawan telah menjadi tren baru dalam perang modern di abad-21. Karenanya, Indonesia harus segera mempersiapkan kekuatan *cyber army* atau prajurit siber yang terdiri dari individu-individu terampil serta ahli dalam *cyber warfare*, yang dituangkan dalam konsep pembangunan nasional pertahanan siber sebagai garda terdepan dalam menjawab tantangan perang siber. Dengan terbentuknya *National Cyber Defense* (saat ini bernama Badan Siber dan Sandi Negara/BSSN), diharapkan pembangunan kapasitas nasional dalam rangka meningkatkan ketahanan nasional terhadap berbagai ancaman dari ranah siber akan dapat lebih ditingkatkan. Namun di sisi lain, pembangunan infrastruktur perlu juga segera direalisasikan secara terintegrasi, khususnya di lingkungan Kemhan/TNI maupun lembaga negara lainnya. Kemampuan yang telah ada saat ini (lahirnya BSSN) dapat dianggap sebagai modal dasar dalam rangka penyiapan konsep dan pembangunan awal

32 *Ibid*, 34-35.

atau tulang punggung pertahanan siber yang komprehensif, mengingat sejauh ini pembangunan konsep pertahanan siber memang masih bersifat sektoral atau belum menyeluruh sebagai satu kesatuan.³³

Oleh karena itu, masalah-masalah keamanan dan pertahanan terkait juga dengan kebijakan-kebijakan yang dibuat di ranah politik oleh negara. Ancaman terhadap keamanan negara, baik ancaman militer maupun non-militer, seperti ancaman siber misalnya, adalah bagian dari kajian *cyberpolitics* juga. Negara perlu memahami bahwa ranah siber saat ini, selain penuh dengan kesempatan, tetapi juga penuh tantangan dan ancaman. Negara harus hadir di ruang siber, tidak hanya dalam membentuk regulasi, tetapi juga mengawasi dan siap bertindak jika ada penyelewengan, terlebih ancaman terhadap keamanan dan pertahanan. Hadirnya BSSN sebagai lembaga negara setingkat kementerian adalah jawaban dari pentingnya *cyberpolitics* dalam pengelolaan masalah keamanan dan pertahanan di Indonesia.

Kesimpulan

Perkembangan teknologi informasi telah menciptakan sebuah “ruang baru” yang bersifat artifisial dan maya. Ruang baru ini telah mengalihkan berbagai aktivitas manusia, seperti politik, sosial, ekonomi, budaya dan spiritual dari dunia nyata ke dunia maya yang dikenal dengan dunia tanpa batas. Apapun yang dapat dilakukan di dunia nyata, sekarang dapat dilakukan dalam bentuk artifisialnya di ruang siber. Ruang siber menciptakan sebuah kehidupan yang mungkin nantinya sebagian besar akan dibangun seluruhnya oleh model kehidupan yang dimediasi secara mendasar oleh teknologi. Ruang siber yang terbentuk oleh jaringan komputer dan informasi yang terhubung secara global telah menawarkan bentuk-bentuk komunitasnya sendiri (*cyber*

community), bentuk realitasnya (*virtual reality*), dan bentuk “ruang-nya” sendiri (*cyberspace*).

Terkait keamanan dan pertahanan siber, ruang siber merupakan ruang virtual yang terbentuk dari hasil penyatuan antara manusia dan teknologi. Oleh sebab itu, ada banyak terminologi dan interpretasi yang dihubungkan dengan konsep keamanan dan pertahanan siber. Hal ini menyebabkan, konsep keamanan dan pertahanan siber tidak lagi hanya menyentuh wilayah teknologi tapi telah menjadi ancaman terhadap keamanan nasional (sekuritisasi). Atas dasar itulah, keamanan siber saat ini dilihat sebagai bagian dari kebijakan yang dibuat oleh sektor keamanan negara, yang tidak lagi menggunakan kekuatan bersenjata (*use of force*), namun cara-cara non-koersif lainnya.

Kebijakan keamanan siber digunakan untuk menghadapi risiko ekonomi dan kebebasan sipil, spionase, termasuk serangan militer atau teroris, yang kesemuanya dilakukan melalui medium internet. Menggunakan perspektif mazhab Kopenhagen terkait sekuritisasi, apapun yang membentuk ancaman terhadap sebuah kelompok, entitas yang memiliki nilai-nilai tertentu, cara hidup, atau ideologi, dapat dikategorikan sebagai masalah keamanan. Spektrum ancaman di era *cyberpolitics* ini berkembang menjadi sangat luas.

Politik siber sangat terkait dengan ruang siber. *Cyberpolitics* adalah sebuah terminologi yang diciptakan, berkaitan dengan interaksi manusia (politik) yang meliputi kegiatan-kegiatan, seperti siapa mendapat apa, kapan, dan bagaimana, yang dimungkinkan untuk terjadi melalui ranah ruang siber sebagai sebuah arena baru pertarungan dengan pengandai-andaian dan realitanya sendiri.

Penulis melihat di masa depan, *Cyberpolitics* akan menjadi ranah dalam berinteraksi politik di masa depan. Semua *stakeholder* bidang politik akan menggunakan medium siber

33 *Ibid*, 35.

untuk mengejar kepentingannya masing-masing, baik untuk memilih maupun dipilih. Ruang siber akan menjadi jembatan antara dunia nyata dengan *constructive reality*, di mana politik akan menjadi “pihak” yang mengambil banyak keuntungan darinya. Realita ini membuat cakupan dari ilmu politik menjadi sangat luas, sehingga menawarkan perspektif baru dalam memahaminya. Untuk itu, penulis merekomendasikan bahwa kajian-kajian yang membahas tentang konsep *cyberpolitics* mulai lebih banyak dibahas dan diteliti di kalangan akademisi-akademisi ilmu politik, agar perpaduan antara ilmu politik dengan TI ke depannya dapat semakin memperkaya khazanah keilmuan masing-masing.

DAFTAR PUSTAKA

- Boothby, William. H. *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors*. The Hague: TMP Asser Press, 2014.
- Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge: MIT Press, 2012.
- Vestberg, Hans. “Ericsson CEO to Shareholders: 50 Billion Connections 2020.” *Ericsson*, 13 April 2010. Diakses 7 Februari 2019. <http://www.ericsson.com/thecompany/press/releases/2010/04/1403231>.
- Fenz, Stefan. *Cyberspace Security: A Definition and A Description of Remaining Problems*. University Vienna and Institute of Government & European Studies, 2005.
- Ghernaoui, Solange. *Cyber Power: Crime, Conflict and Security in Cyberspace*. Lausanne: EPFL Press, 2013.
- Huldt, Bo, dkk (ed). *The Emerging Global Security Environment*. Vasteras: The Swedish National Defense College, 2013.
- Moelong, Lexy. *Metode Penelitian Kualitatif*. Bandung: Remaja Rosdakarya. 2001.
- Munir, Nudirman. *Pengantar Hukum Siber Indonesia*. Depok: Rajawali Press. 2017.
- Nasrullah, Rulli. *Komunikasi Antarbudaya di Era Budaya Siber*. Jakarta: Kencana, 2014.
- NATO CCDCOE. “Cyber Definitions.” NATO CCDCOE, tanpa tanggal. Diakses 12 Februari 2019. <https://ccdcoe.org/cyber-definitions.html>.
- Nawawi, Hadari. *Metode Penelitian Bidang Sosial*. Yogyakarta: Gadjah Mada University Press, 1997.
- Sayuti, Solatun Dulah. *Komunikasi Pemasaran Politik*. Bandung: Remaja Rosdakarya, 2014.
- Soewardi, Bagus Artiadi, *Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia, Media Informasi Ditjen Pothan Kemhan*, Maret 2013.
- Triwahyuni, Dewi dan Tine Agustin Wulandari. “Strategi Keamanan Cyber Amerika Serikat.” *Jurnal Ilmu Politik dan Komunikasi Universitas Komputer Indonesia*, Vol. 6, No. 1 (Juni 2016): 110.