MEMBANGUN PERTAHANAN DAN KEAMANAN SIBER NASIONAL INDONESIA GUNA MENGHADAPI ANCAMAN SIBER GLOBAL MELALUI *INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE* (ID-SIRTII)

BUILDING INDONESIA'S NATIONAL CYBER DEFENSE AND SECURITY TO FACE THE GLOBAL CYBER THREATS THROUGH INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE (ID-SIRTII)

Adi Rio Arianto[1] dan Gesti Anggraini[2]

Universitas Pembangunan Nasional Veteran Jakarta dan
Universitas Satya Negara Indonesia
(arianto.adirio@gmail.com & gestianggra92@gmail.com)

Abstrak – Terbentuknya "*Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII)" merupakan langkah taktis dari Kementerian Komunikasi dan Informatika Republik Indonesia guna mewujudkan stabilitas informasi, perlindungan siber, dan segala bentuk ancamannya. Studi ini mendalami pentingnya ID-SIRTII dalam mencegah ancaman siber global. Hasil studi menemukan bahwa ancaman siber di Indonesia sangat kompleks, melihat variasi dari aktor, motif, dan targetnya. Kompleksitas ini dapat dijelaskan melalui empat aspek berikut, yaitu: (1) berangkat dari studi Geometripolitika, fungsionalisme siber berada dalam dua domain, yaitu "fungsionalisme siber untuk tujuan politik tingkat tinggi (geometrik militer)" berupa formulasi dan aktivasi kekuasaan Siber guna menghadapi Perang Siber Global (PSG), Perang Geometri Antarbangsa (PGA), dan kompleksitas terbentuknya Negara Maya atau Pemerintahan Siber; dan "fungsionalisme siber untuk tujuan politik tingkat normal (geometrik sipil)" berupa perlindungan aktivitas sipil di dunia maya; (2) guna mencegah kejahatan siber, implementasi kebijakan ID-SIRTII terintegrasi dengan peran strategis institusi siber nasional; (3) guna menghadapi Ancaman Siber Global, implementasi kebijakan ID-SIRTII perlu terintegrasi dengan institusi siber regional dan global; dan (4) berangkat dari "fungsionalisme siber" dan untuk menciptakan suatu strukturalisme Pertahanan dan Keamanan Siber Nasional Indonesia, sudah saatnya Indonesia membentuk Angkatan Siber sebagai pelengkap dari Angkatan Darat, Agkatan Laut, dan Angkatan Udara.

Kata Kunci: pertahanan, keamanan, siber, *ID-SIRTII*, angkatan siber

Abstract – *The establishment of the "Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII)" is a tactical step by the Indonesian Ministry of Information and Communcation to ensure the stability of national information regarding cyber protection and all forms of threats. This study explores the urgency of ID-SIRTII to prevent global cyber threats. The study found that cyber*

[1] Dosen Departemen Ilmu Hubungan Internasional, Universitas Pembangunan Nasional Veteran Jakarta, dan Koordinator Keamanan Internasional HI FISIP UPNVJ, kepakaran dalam bidang Strategi, Pertahanan, dan Keamanan Internasional.

[2] Mahasiswa Konsentrasi Strategi dan Keamanan Internasional, Program Studi Ilmu Hubungan Internasional, Universitas Satya Negara Indonesia, Jakarta.

threats in Indonesia is very complex, seeing the variations of actors, motives, and targets (civil or military purpose). This complexity can be explained through the following four aspects, namely: (1) by understanding of Geometripolitic studies in cyber, there are at least two domains that can be reached, namely "the using of cyber for high-politics purposes (military)" by formulating and activating of Cyberpower to face the Global Cyber War(PSG), Wold Geometri War (PGA), and the forming of "Siber State or Siber Government"; and "the use of cyber for low-politics purposes (civil)" by the protecting of civil activities in cyberspace; (2) in order to prevent the spread of national cyber crime, the implementation of the ID-SIRTII policy is integrated with the national siber institutions; (3) in order to prevent the Global Cyber Threat, the implementation of ID-SIRTII policies needs to be strengthened and well-integrated with the regional and global cyber institutions; and (4)considering of the two "functionalism of cyber" also to form a structuralism of Indonesian National Defense and Security system in the cyber sector, nowdays Indonesia needs to build a Cyber Force as a complement to the Army, Navy, and Air Force.

Keywords: *defense, security,cyber, ID-SIRTII, cyberforce*

Pendahuluan: Indonesia dan Kompleksitas Ancaman Siber

Lingkungan Strategis Abad ke-21 menjadi bagiandari Era Horizontal (Horizontalisasi) atau "Globalinium", dimana keamanan informasi (data: aktual dan elektronik) menjadi sangat sulit dikendalikan yang berefek pada kemanan Siber dan Nuklir.[3] Dalam Studi Keamanan Internasional, istilah Era Horizontal (Horizontalisasi) atau "Globalinium" diperkenalkan oleh Adi Rio Arianto dalam karyanya "Keamanan Siber Menuju Perang Geometri Antarbangsa: Geometripolitika dan Arsitektur Keamanan Dunia Era Horizontal Abad ke-21." Menurut Arianto melalui konsep Geometripolitika, keamanan informasi adalah bagian dari Keamanan Siber, sebab metode dan cara-cara mengamankan informasi adalah bagian dari Keamanan Siber yang menginduk pada Kajian Keamanan Internasional (KKI).[4]

Berkenaan dengan ancaman abad ke-21, pandangan Raden Mas Jerry Indrawan dan Efriza perlu disimak, dimana ancaman abad ke-21 bersifat *intangible* (tidak terlihat) seperti ancaman ideologi berupa terorisme dan radikalisme yang berimplikasi pada bela negara dan keamanan nasional khususnya di Indonesia.[5] Dalam situasi ini, ancaman *intangible* beririsan dengan ancaman siber karena sama-sama tidak bisa diraba oleh fisik, namun efeknya bisa dirasakan. Brascomb mengemukakan bahwa informasi berfungsi layaknya aliran darah bagi tubuh manusia.[6] Sehingga, ancaman terhadap Informasi adalahancaman terhadap Siber, dan ancaman terhadap Siber sudah pasti mengancam Keamanan

[3] Adi Rio Arianto, "Keamanan Siber Menuju Perang Geometri Antarbangsa: Geometripolitika dan Arsitektur Keamanan Dunia Era Horizontal Abad 21", Prosiding Konvensi Nasional Asosiasi Ilmu Hubungan Internasional Indonesia VII (VENNAS AIHII VII), 2016, hlm. 18-20.

[4] *Ibid.*

[5] Raden Mas Jerry Indrawan dan Efriza, "Bela Negara Sebagai Metode Pencegahan Ancaman Radikalisme di Indonesia", *Jurnal Pertahanan dan Bela Negara*, Universitas Pertahanan Indonesia, Nomor 3, Volume 7, Desember 2017, hlm. 1-2

[6] Anne W. Brascomb, *Toward A Law of Global Communication Network*, (USA: Longman, 1986), hlm.1.

Siber Nasional diikuti dengan ancaman terhadap Keamanan Siber Gobal. Dengan demikian, ancaman terhadap Keamanan Siber Global adalah ancaman total terhadap Keamanan Internasional.

Berkenaan dengan Keamanan Siber Global, internet menyebabkan manusia terintegrasi dengan aktivitas dunia maya. Internet telah menyebabkan terjadinya satu lompatan besar dalam kinerja umat manusia. Internet tidak bebas nilai, oleh karena itu Siber pun tidak bebas nilai saat bersentuhan dengan politik yang berujung pada pembentukan kekuasaan. Teknologi akan menjadi efektif jika kita memberi perhatian strategis pada kegunaan teknologi yang disesuaikan dengan nilai-nilai masyarakat yang terikat dengan peraturan nasional yang melindungi masyarakat guna menghindari dampak negatif yang ditimbulkannya. Dengan demikian, siber mutlak untuk dikontrol.

Indonesia terus memperkuat jalur lalulintas informasi di dunia maya secara efektif. Pengguna internet di Indonesia mencapai 82 juta orang, menempatkan Indonesia pada peringkat ke-8 di dunia sebagai pengguna aktif internet.[7] Jumlah pengguna tersebut tidak berbanding lurus dengan tingkat keamanannya, sebab Indonesia berada dalam situasi yang lemah keamanan sibernya. Akibatnya, medorong kejahatan siber di ranah sipil berupa peretasan data kartu debit nasabah bank akibat penyusupan ke sistem pengamanan kartu nasabah. Di ranah strategis (militer), Indonesia lemah dalam membentengi lalu lintas informasi. Munculnya kasus spionase, intelijen, *hacking,* dan lain-lain, menunjukkan minimnya dominasi (kuasa) Indonesia dalam mengontrol lalu lintas informasi dalam menghadapi perang siber. Ini menjadi catatan buruk terhadap keamanan siber di Indonesia.

Selain itu, berdasarkan laporan *Akamai* yang mengungkap bahwa kejahatan internet di Indonesia meningkat dua kali lipat. Angka ini menempatkan Indonesia di posisi pertama negara berpotensi menjadi target *hacker*, menggantikan Tiongkok.[8] Laporan tersebut menyebutkan bahwa Indonesia menyumbang 38 persen dari total sasaran trafik *hacking* di internet sesuai dengan hasil investigasi dari 175 negara, dan Indonesia berada dalam posisi pertama tingkat kejahatan sibernya.[9] Berdasarkan pada laporan David Belson dari Akamai *Research*, kecepatan akses internet tidak selalumenimbulkan potensi kejahatan internet yang mengancam Indonesia.[10] Namun demikian, kerugian yang disebabkan karena tindak kejahatan dengan memanfaatkan dunia Siber di Indonesia menurut data CIA mencapai 1,20% dari tingkat kerugian akibat

[7] Untuk informasi lebih lanjut dapat dilihat pada "Kemkominfo: Pengguna Internet di Indonesia Capai 82 Juta", dalam http://kominfo.go.id/index.php/content/detail/3980/Kemkominfo%3A+Pengguna+Internet+di+Indonesia+Capai+82+Juta/0/berita_satker#.U9G405R_tfs, diakses pada 24 Oktober 2018.

[8] Akamai, "The State of The Internet Report", Dokumen Americas Highlights, Second Quarter 2013.

[9] *Ibid.*

[10] "Ketika Hacker Lebih Menakutkan Ketimbang Teroris", dalam http://m.news.viva.co.id/news/read/507480-ketika-hacker-lebih-menakutkan-ketimbang-teroris, diakses pada 17 Oktober 2018.

Tabel 1. Perkiraan Kerugian Akibat Kejahatan Siber: Perbandingan Dunia dan Indonesia

	Global	Indonesia
GDP* :	USD 71,620 bn	USD 895 bn
Percent of global GDP*:		1,20 %
Cost of** :		
Genuine Cyber Crime:	USD 3,457 m	USD 43 m
Transitional Cyber Crime:	USD 46,600 m	USD 582 m
Cyber Criminal Infrastructure:	USD 24,840 m	USD 310 m
Traditional Crimes Cecoming Cyber	USD 150,200 m	USD 2,748 m

Sumber: DAKA Advisory, "Meeting the cyber security challenge in Indonesia An analysis of threats and responses A report from DAKA advisory", 2018, hlm. 21, dalam http://dakaadvisory.com/wp-content/uploads/DAKAIndonesia-cyber-security-2013-web-version.pdf, diakses pada 22 Oktober 2018 .

Kejahatan Siber yang terjadi di dunia, sebagaimana terlihat dalam tabel 1.

Tabel di atas menunjukkan perkiraan kerugiaan akibat Kejahatan Siber di Indonesia, yaitu USD 895 milyar yang artinya mencapai 1,20% dari total keseluruhan perkiraan kerugian akibat kejahatan siber global,yaitu USD 71,620 milyar. Dalam tataran kebijakan, Kejahatan Siber berbeda dalam penanganannya. Pemerintah dapat mengendalikan dan menerapkan hukum didalam wilayah kedaulatan negaranya. Berbeda dengan aktivitas siber yang lokasinya dapat berubah sewaktu-waktu, bahkan hanya dapat dibayangkan.[11] Menurut Menthe dalam "*Jurisdiction in Cyberspace: A Theory of International Space*", mengemukakan bahwa berkenaan dengan ruang internet, penentuan pilihan hukum dan yurisdiksi telah mengakibatkan berbagai pemikiran tentang bagaimana mendekati permasalahan akibat dari penempatan internet sebagai ruang internasional keempat sama seperti antartika, luar angkasa, dan samudera.[12] Berbeda dengan Arianto, yang menempatkan internet (*netika*) sebagai ruang geometri karena kemampuannya dalam membentuk dominasi (kuasa) berupa "keamanan dan kekuasaan siber" yang lebih kompleks, bersifat geometris, dan tak terbatas.[13]

Berdasarkan berbagai pandangandi atas, maka diperlukan banyak kajian mendalamguna memahami kompleksitas ancaman siber di level nasional Indonesia, terutama dalam rangka memahamiragam aktor, motif, dan targetnya, serta tujuannya yang bisa mengarah pada aktivitas sipil atau militer. Pemahaman ini diarahkan untuk menjawab empat aspek berikut, yaitu: (1) bagaimana langkah taktis Indonesia guna mendukung pertahanan dan keamanan siber nasional; (2) guna mencegah meluasnya

[11] Elizabeth Longworth, "The Possibilities for legal framework for cyberspace- Including New Zealand Perspective", dalam Theresa Fuentes et.al (editor), *The International Dimesions of Cyberspace Law: Law of Cyberspace Series,* Vol.1, (Aldershot: Ashgate Publishing Limited, 2000), hlm.14.

[12] D. Menthe, "Jurisdiction in Cyberspace: A Theory of International Space", *Michigan Telecommunications and Technology Law Review*, 23 April 1998, hlm. 59.

[13] Adi Rio Arianto, 2016 ,*op.cit*, hlm. 20-21.

kejahatan siber nasional, bagaimana peran strategis ID-SIRTII serta kerja sama ID-SIRTI dengan tim atau institusi siber di level nasional; (3) guna menghadapi Ancaman Siber Global, apa langkah-langkah yang seharusnya ditempuh oleh ID-SIRTII sebagai tim khusus dalam mengontrollalu lintas informasi di dunia maya, termasuk peran kerja sama ID-SIRTII dengan lembaga keamanan siber di tingkat regional dan global. (4) seberapa urgen bilamana Indonesia menghadirkan "Angkatan Siber" guna menciptakan suatu strukturalisme Pertahanan dan Kemanan Siber Nasional Indonesia sebagai pelengkap dari Angkatan Darat, Angkatan Laut, dan Angkatan Udara.

Fungsionalisme Siber: Tujuan Politik Tingkat Tinggi (Geometrik Militer) Vs. Tujuan Politik Tingkat Normal (Geometrik Sipil)

Untuk mengetahui kompleksitas dari ruang siber, kita perlu memahami lebih mendalam mengenai bentuk-bentuk pemanfaatan "(matra) siber" sebagai sebab utama hadirnya ruang siber lalu mencoba menelaah akibat yang dihasilkan atas pemanfaatan ruang tersebut. Hal ini boleh kita sebut sebagai fungsionalisme siber. Untuk itu, "fungsionalisme siber" perlu dikaji sebagai suatu filsafat keseimbangan, kekuatan, dan keamanan membentuk suatu "kekuasan atas ruang siber" guna menunjang berbagai bentuk pemikiran tentang usaha manusia memahami efek "sebab" dan efek "akibat" atas pemanfaatan ruang siber terhadap aktivitas umat manusia. Berikut adalah konsep-konsep utama dalam melihat fungsionalisme siber, yaitu: Geometripolitika, Telematika, Multimedia, dan Net (Netika).

Pertama, konsep Geometripolitika. Konsep Geometripolitika dikenal sebagai "Teorema Arianto" yang menemukan hubungan strategis antara: keseimbangan, kekuatan, dan keamanan sebagai unsur-unsur strategis pembentuk kekuasaan dengan melibatkan matra siber yang meliputi : *matra* (sebagai wilayah maya berbentuk siber), *netika* (jalur konektifitas lalulintas elektronik), *data* (sekumpulan informasi berbasis maya atau elektronik), *pengguna* (aktor-aktor fungsionalisme siber), dan *kuasa* (dominasi atas akses data dan kompleksitasnya). Kelima unsur ini adalah syarat terbentuknya fungsionalisme siber untuk membentuk kekuasaan siber (geometrik). Konsep Geometripolitika, melihat dunia sebagai suatu kompleksitas kekuasaan yang dikelompokkan kedalam delapan matra, yaitu: darat, laut, udara, bawah tanah, siber, galaksi, ruang hampa, dan khatulistiwa. Adapun, suatu proses politik yang melibatkan "mengikutsertakan" seluruh matra di atas, termasuk dalam hal ini, matra siber untuk membentuk suatu "kekuasaan internasional" disebut dengan istilah "geometripolitik" atau Cabang Ilmu "Geometripolitika" melampaui Cabang Ilmu Politika, Geopolitika, dan Astroplitika.[14]

[14] Adi Rio Arianto, "Cyber Security: Geometripolitika dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21", *Jurnal Power In International Relations*, Universitas Potensi Utama, Vol. 1, No.2, Februari 2017, hlm. 110-112.

Awalnya, kekuasaan dibentuk oleh politik yang didominasi oleh basis fisik. Geometripolitika memperluas basis "kekuasaan" menjadi lima basis, yaitu: basis fisik (material), metafisik (metafisikal), psikologik (psikologikal), ideasionik (ideasional), dan geometrik (geometrikal). Kekuasaan dapat dibentuk melalui "geografi" menghasilkan Geopolitik, lalu melampaui geografi menembus ruang "luar angkasa" menghasilkan Astropolitik. Akhirnya, Geometripolitika memunculkan basis keempat dan kelima sebagai akibat hadirnya matra maya yang melahirkan "kekuasaan atas sesuatu" di dunia maya, yaitu basis "ideasionik" dan "geometrik."

Politik didominasi oleh basis fisik yang terbatas untuk mencapai kekuasaan. Sedangkan, Geopolitik mengoptimalkan basis fisik "geografi" yang juga terbatas untuk memperluas kekuasaan. Adapun, Astropolitik berusaha mengembangkan basis metafisik ruang luar angkasa yang tidak terbatas dengan cara penguasaan atas ekplorasi ruang angkasa untuk tujuan kekuasaan. Dengan berkembangnya ruang lingkup keamanan dan kekuasaan, maka ancamannya pun ikut berkembang sejalan dengan kemajuan teknologi. Kemajuan teknologi ini turut mempengaruhi perluasan fungsionalisme siber yang melibatkan *matra*, *netika*, *data*, *pengguna*, dan *kuasa* atas informasi di dunia maya. Dengan demikian, konsep Geometripolitika adalah suatu konsep kekuasaan yang melampaui konsep Politika, Geopolitika, dan Astropolitika sebagai konsep final yang mencoba memetakkan secara rinci hubungan antara keseimbangan, kekuatan, dan keamanan melampaui basis fisik (material), metafisik (metafisikal), psikologik (psikologikal) dengan cara memunculkan basis "ideasionik" dan basis "geometrik" sebagai pelengkap keempat dan kelima. Adapun, basis "ideasionik" dan "geometrik" berusaha menjelaskan terbentuknya kekuasaan di dunia maya. Basis fisik adalah bangunan kuasa yang dibentuk oleh objek fisik yang nyata, dapat disentuh, dan terbatas. Basis metafisik adalah bangunan kuasa yang ditopang oleh abstraksi kausalitas. Adapun, basis psikologik ialah abstraksi suasana kebatinan yang mengandung efek kuasa. Selanjutnya, basis ideasionik yaitu kontrol terhadap ide tak terbatas guna mendukung kuasa atas suatu abstraksi. Adapun, basis geometrik ialah bangunan kuasa maya tak terbatas yang terbentuk akibat fungsionalisme siber melampaui kekuasaaan aktualnya.

Basis geometrik memiliki efek pada semua basis di atas, maka muncullah dua ruang lingkup geometrik, yaitu (1) Dimensi Geometri Terbatas (DGT), dan (2) Dimensi Geometri Tidak Terbatas (DGTT). Dimensi Geometri Terbatas adalah dimensi keamanan yang bersifat fisik, dapat disentuh oleh manusia, dan sifatnya terbatas karena dapat dijangkau oleh fisikal manusia dan dapat dipandang melalui mata telanjang. Dimensi ini meliputi: ruang darat, laut, udara, dan bawah tanah. Sedangkan, Dimensi Geometri Tidak Terbatas adalah dimensi keamanan dan kekuasaan yang bersifat

geometrik dan tidak terbatas, karena keberadaannya tidak dapat diraba oleh fisik, namun efeknya secara metafisik, psikologik, dan ideasionik dapat dibayangkan dan membentuk keamanan dan keamanan atas suatu objek. Dimensi ini meliputi: siber, yang sama kongruennya dengan ruang hampa, galaksi (luar angkasa), dan ruang khatulistiwa.

Dari sini, fungsionalisme siber dapat dipetakan secara akurat. Siber menjadi satu dari delapan medan keamanan dan kekuasaan dunia yang tergabung ke dalam Dimensi Geometri Tidak Terbatas (DGTT). Dengan demikian, melalui gagasan Geometripolitika dapat didefinisikan bahwa, "siber adalah matra maya berbentuk geometris dan tak terbatas yang berisi sekumpulan dataelektronik yang tersimpan dan terhubung oleh *netika* atau jaringan komputerik dan sibernetik yang dalam fungsionalismenya membentuk kuasa (dominasi) atas pembuatan, penghilangan, distribusi, kecepatan, percepatan, perlambatan, variasi, dan volume data." Sifat alamiah Siber adalah geometris dan tidak terbatas, karena keberadaannya tidak dapat diraba oleh fisik, namun efeknya secara metafisik, psikologik, dan ideasionik dapat dibayangkan dan membentuk keamanan dan kekuasaan atas suatu objek. Siber bersifat geometris karena siber tidak dapat disentuh namun dapat dibentuk dan diabstraksikan melalui kuasaatas lalu lintas datanya. Adapun, siber bersifat tak terbatas karena siber tidak dapat dibatasi oleh apapun, termasuk negara dan organisasi, kecuali oleh batas fungsionalisme siber itu sendiri, yaitu kemampuan melakukan eksplorasi ruang siber adalah batasnya. Dengan demikian, atas sifat-sifat siber yang geometris dan tak terbatas, dapat ditarik suatu kesimpulan, "siber adalah ruang fatamorgana sebagai refleksi dari objek aktualnya.

Fungsionalisme siber merefleksikan kekuasaan akibat terhubungnya seluruh basis fisik (material), metafisik (metafisikal), psikologik (psikologikal), ideasionik (ideasional), dan geometrik (geometrikal)." Sehingga, dapat didefinisikan bahwa "Keamanan Siber adalah kemampuan untuk menciptakan perlindungan secara geometris dan tak terbatas terhadap segala aktivitas matra maya, perlindungan terhadap segala informasi strategis berupa transformasi data aktual menjadi data elektronik yang tersimpan dan terhubungoleh suatu netika atau jaringan komputerik dan sibernetik membentuk lalu lintas informasi, dan perlindungan terhadap kualitas lalu lintas informasi berupa pengadaaan, penghilangan, distribusi, kecepatan, percepatan, perlambatan, variasi, dan volume data." Keamanan siber berusaha untuk menciptakan situasi dimana aktor siber berada dalam kondisi aman termasuk terdapatnya perlindungan terhadaplingkungan (*matra*), organisasi dan infrastruktur (*netika*), aset (*data*), aktor siber (*pengguna*),dan dominasi atas informasi di dunia maya (*kuasa*). Organisasi, infrakstuktur, dan aset pengguna siber dapat berupa keberadaan perangkat yang terhubung dengan

komputer dan internet, meliputi: program, aplikasi, layanan, telekomunikasi, dan data informasi yang dikirimkan dan disimpan dalam lingkungan maya, yaitu ruang siber.

Fungsionalisme siber lebih strategis jika dihubungkan dengan pembentukan "kekuasaan di dunia maya". Fungsionalisme siber, yaitu segala bentuk pemanfaatan ruang siber untuk berbagai tujuan, termasuk mengejar kekuasaan tak terbatas atas siber. Dalam konsep Geometripolitika, fungsionalisme siber menghasilkan kuasa atas dunia maya, disebut dengan istilah "geometrik". Efek geometrik dapat mendorong berbagai aktivitas strategis dalam dunia sipil dan kemiliteran, seperti: mendorong Perang Siber Global (PSG), Perang Geometri Antarbangsa (PGA), dan terbentuknya Negara Maya atau Pemerintahan Siber. "Perang Siber Global" adalah perang yang terjadi akibat bertemunya fungsionalisme ruang siber untuk tujuan kuasa (geometrik militer) guna mendukung perang di dunia maya yang efek geometriknya masih dalam tataran dunia maya. Sedangkan, "Perang Geometri Antarbangsa" adalah Perang yang mengkombinasikan seluruh matra (DGT dan DGTT) dengan teknologi siber dan teknologi nuklir dimana perang di matra siber akan menjadi pemantik untuk memulai perang aktual di dunia sesungguhnya.[15] Adapun, "Negara Maya atau Negara Siber, yaitu kedaulatan yang ditopang oleh suatu kekuasaan geometris "geometrik" tak terbatas di dunia maya akibat fungsionalisme siber secara terstruktur oleh aktor sekelas negara atau tak terbatas yang berkepetingan membentuk kekuasaan atas data elektronik secara total. Inilah Kekuasaan Siber, suatu Pemerintahan Siber." Konsep Negara Maya hadir akibat evolusi dari seluruh basis kuasa, yaitu: basis fisik (material), metafisik (metafisikal), psikologik (psikologikal), ideasionik (ideasional), dan basis geometrik (geometrikal). Fungsionalisme siber dapat membentuk kedaulatan maya.

Pada akhirnya, dalam tataran kebijakan negara, konsep Geometripolitika membagi fungsionalisme siber menjadi dua domain utama, yaitu: pertama, "fungsionalisme siber untuk politik tingkat tinggi (geometrik militer)" yaitu pemanfaatan ruang siber yang mengarah pada penguasaan dan mengamankan aktivitas militer yang berujung pada Perang Siber. Pemanfaatan ini jauh lebih rumit karena melibatkan instrument militer. Jika tidak dikendalikan dengan baik, dapat menghambat aksi kemiliteran. Fungsionalisme siber untuk geometrik militer dapat berupa pemanfaatan ruang siber untuk menciptakan, menangkal, dan melindungi berbagai serangan terhadap infrastruktur siber yang terhubung dengan teknologi nuklir, teknologi pembangkit listrik nasional, teknologi kemaritiman, teknologi penerbangan dan antariksa, serta penyerangan terhadap seluruh fasilitas negara yang terkoneksi dengan teknologi siber yang mengarah pada dukungan perang siber. Kedua, "fungsionalisme siber untuk politik tingkat normal (geometrik sipil)" yaitu pemanfaatan siber yang mengarah pada

[15] Adi Rio Arianto, 2016, *op.cit,* hlm. 20.

penguasaan dan mengamankan aktivitas masyarakat sipil di ruang siber. Jika terjadi penyalahgunaan terhadap fungsionalitas ini, berpotensi munculnya kejahatan siber seperti serangan terhadap fasilitas internet sipil: website, dan lain-lain, jebolnya akun nasabah bank, pencurian data untuk motif ekonomi, penyebaran identitas pribadi, kejahatan terhadap aktivitas sosial media, dan lain-lain. Jadi, fungsionalisme ruang siber mesti dikontrol secara akurat dan komprehensif dengan melibatkan geometrik militer dan geometrik sipil.

Berlanjut pada konsep berikutnya yaitu telematika. Telematika atau "*the new hybrid of technology*" muncul karena perkembangan teknologi siber yang membuat perkembangan teknologi telekomunikasi dan informatika terhubung dengan baikatau disebut dengan istilah "konvergensi" (perpaduan). Perpaduan teknologi telekomunikasi, media, dan informasi mendorong penyelenggaraan sistem elektronik berbasis siber yang kemudian di kenal dengan istilah "*net*." Konsep tentang perpaduan ini terus berkembang mengikuti kemajuan teknologi siber pada akhir Abad ke-20 dan memasuki awal Abad ke-21 disebut dengan istilah "Era Horizontal (Horizontalisasi)" dengan hadirnya revolusi kegiatan industri di sektor siber yang bertalian dengan efek teknologi senjata nuklir.

Dampak konvergensi secara sosial telah dirasakan positif dan negatifnya.[16] Kejahatan siber adalah salah satu dampak negatifnya. Kejahatan siber memerlukan perhatian besar, termasuk Indonesia. Selanjutnya para praktisi menyebut media dalam telematika tersebut dengan istilah *multimedia*. Berkembangnya infrastruktur sistem telekomunikasi diikuti dengan kemajuan sistem informasi yang mampumengarahkan masyarakat untuk masuk dalam suatu ruang baru, yaitu ruang maya atau siber.[17] William Gibson dalam karyanya "*Neuromancer*", melihat lebih mendalam integrasi antara komputer dengan aktivitas manusia.[18]

Selanjutnya, dalam karya Ronald Thompson dan William Cats Barril "*Information Technology and Management*" berkenaan dengan keamanan ruang siber, terdapat beberapa hal yang harus diperhatikan dalam usaha mengolah sumber-sumber teknologi informasi. Pengelolaan tersebut meliputi: (1) perangkat lunak seperti sistem dan aplikasi dan perangkat keras infrastruktur teknologi informasi, (2) manajemen isi dari informasi, (3) telekomunikasi dan jaringan internet, dan (4) internet dan perdagangan dunia maya melalui ruang internet.[19] Sementara, untuk pengorganisasian terkait dengan penggunaan sistem teknologi informasi setidaknya ada empat hal utama yang harus diperhatikan yaitu: sistem informasi,

[16] Pusat Teknologi Informasi dan Komunikasi Badan Pengkajian dan Penerapan Teknologi (BPPT), *Kajian Konvergensi Teknologi Informasi dan Komunikasi*, (Jakarta: Pusat Teknologi Informasi dan Komunikasi BPPT, 2007), hlm. 3

[17] M. Arsyad Sanusi, *Hukum Teknologi dan Informasi*, (Bandung: Tim Kemas Buku, 2005), hlm.92-93.

[18] John Vivian, *Teori Komunikasi Massa*, (Jakarta: Kencana, 2008), hlm. 264.

[19] Ronald Thompson & William Cats Barril, *Information Technology and Management*, (New York: Mc Graw Hill, 2003), hlm. 29.

kompetisi organisasi, sistem informasi dan pengambilan keputusan organisasi, dan pengorganisasian penggunaan suatu sistem informasi.

Sistem informasi mesti terintegrasi, teknologi informasi dibangun berbasis sistem yang dirancang untuk dapat mendukung kerja, manajemen dan pengambilan keputusan dalam organisasi. TIK adalah salah satu komponen paling penting dalam pengembangan sistem informasi.[20] Pengelolaan sumber daya sistem informasi adalah permasalahan selanjutnya terkait dengan tantangan pengembangan TIK. Ada empat kunci utama yang harus diperhatikan yaitu: pengelolaan sumber daya sistem informasi haruslah ditempatkan sebagai proses manajemen bisnis, pembangunan sistem informasi, sumber daya ekternal sistem informasi, dan manajemen sumber daya informasi.Dalam membangun sistem keamanan siber, berikut hal-hal yang mesti diperhatikan: (1) kepastian hukum berupa Undang-Undang Kejahatan Siber; (2) teknis dan tindakan prosedural termasuk pengguna akhir dan bisnis pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak; (3) struktur organisasi guna menghindari tumpang tindih; (4) pendidikan pengguna berupa kampanye publik dan komunikasi terbuka ancaman kejahatan siber terbaru; (5) kerja sama internasional dalam upaya mengatasi ancaman Siber.[21]

[20] *Ibid*, hlm. 200-203.

[21] Handrini Ardiyanti, "*Cyber-Security* dan Tantangan Pengembangannya di Indonesia", *JurnalPolitica,* Vol. 5, No. 1 , Juni 2014, hlm. 108.

Parameter Pertahanan dan Keamanan Siber Nasional Indonesia: Peran ID-SIRTII dan Institusi Siber Lingkup Nasional

Situasi keamanan siber Indonesia berada dalam tahap yang berbahaya dan kritis. Hal ini sebagai akibat dari meningkatnya lalu lintas informasi global yang melewati dan masuk kedalam sistem jaringan informasi nasional Indonesia. Melihat Indonesia berada pada posisi pertama dengan target *hacker*, menggantikan Tiongkok, maka arus informasi tersebut semakin sulit dikendalikan. Hal ini mendorong kejahatan siber global yang dapat mengarah pada kelumpuhan sistem informasi nasional jika tidak dikontrol. Situasi ini perlu mendapat perhatian besar.

Untuk mencegah memburuknya pertahanan dan keamanan siber, diperlukan kepastian Hukum Kebijakan Keamanan Siber. Pada tahun 2007 dikeluarkan Peraturan Menteri Komunikasi dan Informatika No.26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet, dan direvisi Peraturan Menteri Komunikasi dan Informatika No.16/PER/M.KOMINFO/10/2010, lalu diperbaharui lagi dengan Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMINFO/12/2010. Peraturan inisebagai landasan ID-SIRTII.ID-SIRTII ditugaskan untuk: (1) melakukan pemantauan, pendeteksian awal, peringatan dini terhadap ancaman jaringan internet, (2) berkoordinasi dengan pihak dalam

danluar negeri gunameningkatkan keaamanan jaringan diinternet, (3) mengoperasikan dan mengembangkan sistem database ID-SIRTII, (4) menyusun katalog pemanfaatan jaringan, (5) memberikan layanan atas ancaman dan keamanan telekomunikasi yang berbasis protokol internet, (6) menjadi *contact point* dengan lembaga dalam pemanfaatan jaringan telekomunikasi, dan (7) menyusun program kerja keamanan jaringan telekomunikasi yang berbasis internet.[22]

Selain ID-SIRTII, berikut adalah beberapa lembaga dan organisasi yang menangani persoalan internet, keberadaannya setingkat nasional baik formal maupun non-formal yang sudah ada di Indonesia, diantaranya: Dewan Teknologi Informasi dan Komunikasi atau Dewan TIK (dibentuk tahun 2006), *Indonesia Security Incident Response Team On Internet and Infrastructure / Coordination Center* (ID-SIRTII/CC, dibentuk tahun 2007), *Indonesia Computer Emergency Response Team* (ID-CERT, dibentuk tahun 1998), *Computer Security Incident Response Team*(CSIRT, dibentuk tahun 1998), *Indonesia Telecommunications User Group* (IDTUG, dibentuk tahun 2004). Organisasi di atas bekerja secara sektoral dalam menangani kejahatan siber, dan tidak berfokus pada kepentingan nasional Indonesia. Oleh karena itu, perlu kesamaan visi dalam melihat fungsionalime siber sekaligus merumuskan suatu strukturalisme pertahanan dan keamanan siber.

Kerangka hukum Keamanan Siber di Indonesia dibangun berdasarkan atas dasar UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012 serta surat edaran menteri dan peraturan menteri. Terkait dengan upaya menjamin kepastian hukum dalam pengembangan Keamanan Siber telah dilakukan antara lain dengan melaksanakan serangkaian program yang sudah mulai berjalan diantaranya: menginisiasi peraturan perundangundangan yang terkait dengan Keamanan Siber seperti UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012, menyusun kerangka nasional Keamanan Siber. Legalitas penanganan kejahatan Siber masih lemah meskipun ada peraturan perundangundangan yang melarang bentuk penyerangan atau perusakan sistem elektronik. Belum terdapat peraturan perundang-undangan yang mengatur secara khusus Kejahatan Siber dan penanganan Kejahatan Siber. Hal ini melihat efek geometris dan tak terbatasnya siber, sehingga sulit ditangani.

Terdapat masalah dalam pembangunan Keamanan Siber: (1) Lemahnya pemahaman negara atas

[22] Pasal 9 Peraturan Menteri Komunikasi dan Informatika No. 29/PER/M.KOMINFO/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M. Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

keamanan siber yang memerlukan pembatasan layanan yang servernya berada di luar negeri dan diperlukan adanya pengunaan *secured system*, (2) Legalitas penanganan penyerangan di dunia Siber, (3)Pola kejadian Kejahatan Siber sangat cepat sehingga sulit ditangani, (4)Tata kelola kelembagaan Keamanan Siber nasional, (5) Rendahnya kesadaran akan adanya ancaman serangan siber internasional yang dapat melumpuhkan infrastruktur vital suatu negara, (6) Masih lemahnya industri kita dalam memproduksi dan mengembangkan perangkat keras atau *hardware* terkait dengan teknologi informasi yang merupakan celah yang dapat memperlemah pertahanan dalam dunia Siber.[23] Hal ini diarahkan untuk dan perlu diangkat guna mendukung kesamaan persepsi dan visi dalam melihat fungsionalisme siber sekaligus untuk merumuskan suatu strukturalisme pertahanan dan keamanan siber nasional.

Penanganan kejahatan Siber yang masih parsial dan tersebar serta belum adanya koordinasi yang baku dalam penanganan masalah Keamanan Siber. Rendahnya *awarenees* atau kesadaran akan adanya ancaman Siber yang berdampak melumpuhkan infrastruktur vital contohnya adalah sistem radar penerbangan di bandara internasional Soekarno Hatta yang beberapa kali mengalami gangguan. Tidak menutup kemungkinan Serangan Siber menyerang infrastruktur vital negara seperti itu. Terkait dengan kebijakan Keamanan Siber di Indonesia diperlukan sebuah kebijakan yang mengatur berbagai elemen terkait Keamanan Siber dalam kebijakan-kebijakan yang mengatur tentang sistem teknologi informasi komunikasi yang digunakan. Hal tersebut meliputi adanya pengaturan dokumen standar sebagai acuan dalam menjalankan seluruh proses yang terkait dengan keamanan informasi dan standar infrastruktur yang sesuai dengan standar internasional dalam menghadapi Perang Siber. Standar infrastruktur tersebut adalah adanya perimeter *defense* yang memadai, *network monitoring system*, *system information and event management* yang berfungsi memonitor berbagai kejadian di jaringan terkait dengan insiden keamanan, serta *network security assement* yang berperan sebagai *control* dan *measurement* keamanan.

Kerjasama dalam Menghadapai Ancaman Siber Global : ID-SIRTII dan Institusi Siber Lingkup Regional dan Global

Dengan hadirnya ID-SIRTII, setidaknya Indonesia mampu mengontrol ancaman siber dari tingkat nasional hingga tingkat global terutama dalam mengontrol kualitas informasi. Jika tidak seperti itu, maka ada kemungkinan muncul ancaman siber dari berbagai kondisi. Salah satu fakta menunjukkan Kejahatan Siber di Indonesia cukup mengkhawatirkan. Data CIA yang menyebutkan kerugian yang disebabkan karena tindak kejahatan dengan memanfaatkan maupun di dunia

[23] Hasyim Gautama, "Penerapan *Cyber Security*", dalam http://kemhubri.dephub.go.id/pusdatin/files/materi/Penerapan_Cybersecurity.pdf, diakses pada 17 Oktober 2018.

Siber di Indonesia telah mencapai 1,20% dari tingkat kerugian akibat Kejahatan Siber yang terjadi di dunia. Penanganan Kejahatan Siber sangat berbeda dengan penangganan kejahatan lainnya sebab ruang lingkupnya yang tidak terbatas.

Selanjutnya, butuh pemikiran yang kompleks untuk membangun keamanan siber. Oleh karena itu, setidaknya ada beberapa halyang mesti diangkat yaitu: pertama, bagaimana kebijakan Keamanan Siber yang sudah berjalan sebelum dan sesudah berdirinya ID-SIRTII. Kedua, bagaimana tingkat keamanan siber setelah implementasi kebijakan Keamanan Siber dijalankan oleh Indonesia. Kebijakan Keamanan Siber yang telah dijalankan di Indonesia telah diinisiasi sejak tahun 2007 dengan dibentuknya ID-SIRTII yaitu Tim yang ditugaskan Menteri Komunikasi dan Informatika RI untuk membantu pengawasan keamanan jaringan telekomunikasi berbasis protokol internet.

Guna mendukung keamanan informasi, kerjasama regional dan global dapat dilakukan oleh ID-SIRTII berdasarkan Pasal 9 Peraturan Menteri Komunikasi dan Informatika No.29/ PER/M.KOMINFO/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi. Dalam pasal ini, terdapat poin pentingberkaitan dengan kerjasama ID-SIRTII dengan berbagai lembaga guna mendukung keamanan siber guna mencegah ancaman siber global yang termaktub dalam poin kedua dan keenam: "…(2) berkoordinasi dengan pihak-pihak terkiat didalam maupun luar negeri dalam menjalankan tugas pengamanan jaringan telekomunikasi berbasis protokol internet, dan …(6) menjadi *contact point* dengan lembaga terkait dalam pengamanan jaringan telekomunikasi berbasis internet."

Dalam menjalankan perannya, ID-SIRTI setidaknya dapat bekerjasama dengan lembaga siber regional dan internasional, yaitu: pertama, di level regional terdapat organisasi APCERT (*Asia Pacific Computer Emergency Response Team*). Berdirinya APCERT diinisiasi oleh *Indonesia Computer Emergency Response Team* (ID-CERT), *Japan Computer Emergency Response Team* (JP-CERT), dan *Australia Computer Emergency Response Team* (AusCERT). Salah satu peran APCERT adalah menjadi "mediator" negara anggota yang mengalami gangguan terhadap lalu lintas internet dan infrastrukturnya. Kedua, di level internasional terdapat organisasi ITU (*International Telecommunication Union*) di bawah struktur Perserikatan Bangsa-Bangsa (PBB). Kerjasama Indonesia dengan ITU pernah terealisasi dalam kasus *The Five Eyes,* yaitu suatu penyadapan yang dilakukan oleh AS, Inggris, Australia, Kanada, dan Selandia Baru dalam menyadap jaringan komunikasi kabel laut, satelit, dan saluran komunikasi global. Penyadapan oleh *The Five Eyes* adalah kasus siber paling genting karena menyasar telekomunikasi dari tokoh-tokoh penting Indonesia, yaitu Presiden Susilo Bambang Yudhoyono dan kabinetnya. Ini berbahaya dan termasuk

pelanggaran intelijen, karena aksinya mengemuka di ranah publik dunia.

Kerangka hukum Keamanan Siber di Indonesia saat ini dibangun atas dasar UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012 serta Surat Edaran Menteri dan Peraturan Menteri. Namun demikian, terdapat permasalahan terkait dengan pembangunan Keamanan Siber yang tangguh diantaranya adalah: lemahnya pemahaman penyelenggara negara atas keamanan siber yang memerlukan pembatasan layanan yang servernya berada di luar negeri, dan diperlukan adanya pengunaan *secured system;* belum adanya legalitas yang memadai terhadap penanganan serangan siber; tata kelola kelembagaan Keamanan Siber secara nasional yang masih parsial dan tersebar serta tidak adanya koordinasi yang baku dalam penanganan masalah Keamanan Siber.

Penangganan keamanan siber harus terintegrasi secara kuat dan melibatkan berbagai lembaga seperti: intelijen, penegak hukum, pertahanan dan keamanan baik itu Kementerian Pertahanan dan TNI serta pemerintah sebagai pengatur, dalam hal ini diwakili oleh Kominfo dan Lembaga Sandi Negara yang kini bertranformasi menjadi Badan Siber dan Sandi Negara (BSSN). Guna menyikapi kejahatan siber yang semakin kompleks, sudah sewajarnyajika Indonesia menempatkan matra siber dalam konteks "pertahanan dan Keamanan Nasional" dengan cara menghadirkan: (1) pembangunan basis strukturalnya seperti diciptakannya suatu Angkatan Siber melengkapi Angkatan Darat, Angkatan Laut, dan Angkatan Udara; (2) pembangunan basis infrastrukturnya seperti diperkuatnya satelit khusus untuk pertahanan dan keamanan siber, termasuk didalamnya; (3) memantau protokol kerja lalu lintas Siber yang secara hukum masuk dalam wilayah Indonesia, namun secara teknikalnya dikontrol oleh sejumlah provider telekomunikasi pemilik kuasa dari teknologi dimana alat tersebut dibeli, teknologi asing.

Strukturalisme Pertahanan dan Keamanan Nasional Indonesia di Sektor Siber: Angkatan Siber

Wacana lahirnya Angkatan Siber melengkapi Angkatan Darat, Angkatan Laut, dan Angkatan Udara perlu disikapi secara positif dan serius. Ini adalah tantangan pemerintah Indonesia guna menghadirkan suatu sistem pertahanan dan keamanan siber yang handal dan berkualitas. Selain tantangan struktural, tantangan lainnya ke depan dalam pengembangan kebijakan Keamanan Siber adalah sifat dari ancaman Siber yang "geometris dan tak terbatas" membuat penanganannya tidak hanya menjadi tanggungjawab dari TNI, Polri, Kemhan, serta Kemenkominfo. Salah satu strategi menarik yang patut dicermati dalam menghadapi ancaman siber global diantaranya adalah upaya serius pemerintah dalam bertugas

menangani keamanan siber secara nasional yang didukung oleh sektor swasta dan masyarakat danmembuat dan menerapkan program manajemen risiko untuk siber guna melindungi infrastruktur telekomunikasi dan siber dari situasi kritis. Sektor swasta dan masyarakat memiliki tugas untuk membangun dan memelihara sistem keamanan Siber.

Pada akhirnya, berangkat dari dua domain "fungsionalisme siber" di atas sekaligus untuk menciptakan suatu strukturalisme Pertahanan dan Keamanan Nasional Indonesia di sektor siber, sudah saatnya Indonesia membentuk Angkatan Siber sebagai pelengkap dari Angkatan Darat, Angkatan Laut, dan Angkatan Udara. Angkatan Siber akan menjadi bagian dariformasi struktural di tubuh Tentara Nasional Indonesia (TNI) dengan mengembangkan strategi nasional dalam membangun Keamanan Siber di Indonesia ke depan. Selain itu, Angkatan Siber di-visi-kan untuk menyelesaikan dan mendukung perkembangan teknologi informasi yang tidak hanya di ranah militer, tetapi juga menjangkau ranah sipil dalam membangunKeamanan Siber nasional dan global. Tugas-tugas yang diemban oleh Angkatan Siber diharapkan mampu menjadi pusat kontrol atas sistem informasi nasional, kompetisi organisasi informasi, pengambilan keputusan organisasi informasi, danfungsionalisme sistem informasi dalam dua domain dimaksud dengan bekerjasama dengan institusi siber lainnya.

Kesimpulan

Melihat kemajuan teknologi siber di seluruh dunia, Indonesia nampaknya menjadi salah satu aktor paling penting dalam tata lalu lintas informasi siber masa depan. Saat ini Indonesia berada di posisi pertama negara berpotensi menjadi target*hacker*, menggantikan Tiongkok. Hadirnya fungsionalisme siber sebagai arena politik internasional, Indonesia perlu mempersiapkan agenda besar guna mendukung pertahanan dan keamanan siber nasional untuk mencegah ancaman siber global, baik di ranah sipil maupun ranah militer yang mengarah pada "Perang Siber Global (PSG)" atau dengan istilah lebih kompleks "Perang Geometri Antarbangsa (PGA)." Selain itu, melanjutkan kajian Geometripolitika yang menghasilkan suatu kekuasaan siber atas pelibatan matra siber dalam kekuasan dengan istilah "geometrik", maka kita juga akan bergelut dengan kehadiran "Negara Maya atau Pemerintahan Siber." Hal ini mengingat bahwa kekuasaan juga dapat dibentuk di ruang siber yang ditopang oleh suatu kedaulatan siber. Setidaknya, dengan dibentuknya"*Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII)", Indonesia Indonesia telah merespons sesuai dengan ketersediaan SDM dan SDA.

Dalam mencegah ancaman siber global, studi ini pada akhirnya menemukan bahwa ancaman siber di Indonesia sangat kompleks, melihat variasi dari aktor, motif, dan targetnya. Kompleksitas ini dapat dijelaskan melalui empat aspek

berikut, yaitu: (1) berangkat dari studi Geometripolitika, fungsionalisme siber berada dalam dua domain, yaitu "fungsionalisme siber untuk tujuan politik tingkat tinggi (geometrik militer)" berupa formulasi dan aktivasi kekuatan Siber guna menghadapi Perang Siber Global (PSG), Perang Geometri Antarbangsa (PGA), dan kompleksitas terbentuknya "Negara Maya atau Pemerintahan Siber"; dan "fungsionalisme siber untuk tujuan politik tingkat normal (geometrik sipil)" berupa perlindungan segala aktivitas sipil di dunia maya; (2) guna mencegah meluasnya kejahatan siber, implementasi kebijakan ID-SIRTII mesti terintegrasi dengan peran strategis institusi siber nasional; (3) guna menghadapi Ancaman Siber Global, implementasi kebijakan ID-SIRTII perlu terintegrasi dengan institusi siber regional dan global; dan (4) berangkat dari dua "fungsionalisme siber" di atas sekaligus untuk menciptakan suatu struktur Pertahanan dan Keamanan Siber Nasional Indonesia, sudah saatnya Indonesia membentuk Angkatan Siber Nasional sebagai pelengkap dari Angkatan Darat, Angkatan Laut, dan Angkatan Udara. Angkatan Siber di-visi-kan untuk menyelesaikan dan mendukung perkembangan teknologi informasi yang tidak hanya di ranah militer, tetapi juga menjangkau ranah sipil dalam membangun Keamanan Siber nasional dan global.

Keempat hal di atas setidaknya dapat menjadi salah satu indikator untuk memahami kesiapan Indonesia dalam menhadapai berbagai macam kemungkinan berkenaan dengan dunia Internasional Abad ke-21 yang didominasi oleh teknologi siber. Dengan demikian, Indonesia kini menjadi salah satu aktor paling utama dalam pembentukan arsitektur keamanan dunia di Era Horizontal Abad ke-21. Indonesia perlu mendukung Globalinium dan Horizontalisasi Dunia yang menempatkan siber sebagai salah satu matra strategis abad ke-21. Dengan demikian, masa depan Keamanan Siber Global akan banyak bergantung kepada Indonesia.

Daftar Pustaka

Buku

Brascomb, Anne W. 1986. *Toward A Law of Global Communication Network*. USA: Longman.

Longworth, Elizabeth. 2000. "The Possibilities for legal framework for cyberspace-Including New Zealand Perspective". Dalam Theresa Fuentes et.al (editor). *The International Dimesions of Cyberspace Law: Law of Cyberspace Series*. Vol.1. Aldershot: Ashgate Publishing Limited.

Pusat Teknologi Informasi dan Komunikasi Badan Pengkajian dan Penerapan Teknologi (BPPT). 2007. *Kajian Konvergensi Teknologi Informasi dan Komunikasi*. Jakarta: Pusat Teknologi Informasi dan Komunikasi BPPT.

Jurnal

Arianto, Adi Rio. 2017. "Cyber Security: Geometripolitika dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21". *Jurnal Power In International Relations*. Universitas Potensi Utama. Vol. 1. No.2. Februari.

Ardiyanti, Handrini. 2014. "*Cyber-Security* dan Tantangan Pengembangannya di Indonesia". *Jurnal Politica.* Vol. 5. No. 1 . Juni.

Indrawan, Raden Mas Jerry dan Efriza. 2017. "Bela Negara Sebagai Metode Pencegahan Ancaman Radikalisme di Indonesia". *Jurnal Pertahanan dan Bela Negara*. Universitas Pertahanan Indonesia. Vol. 7.No. 3. Desember.

Menthe, D. 1998. "Jurisdiction in Cyberspace: A Theory of International Space". *Michigan Telecommunications and Technology Law Review*. 23 April.

Sanusi, M. Arsyad. 2005. *Hukum Teknologi dan Informasi*. Bandung: Tim Kemas Buku.

Vivian, John. 2008.*Teori Komunikasi Massa*. Jakarta: Kencana.

Thompson, Ronald & William Cats Barril. 2003. *Information Technology and Management*. New York: Mc Graw Hill.

Makalah

Arianto, Adi Rio. 2016. "Keamanan Siber Menuju Perang Geometri Antarbangsa: Geometripolitika dan Arsitektur Keamanan Dunia Era Horizontal Abad 21". Prosiding Konvensi Nasional Asosiasi Ilmu Hubungan Internasional Indonesia VII (VENNAS AIHII VII).

Akamai. 2013. "The State of The Internet Report". Dokumen Americas Highlights. Second Quarter.

Peraturan Menteri

Pasal 9 Peraturan Menteri Komunikasi dan Informatika No. 29/PER/M. KOMINFO/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M. Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

Website

Gautama, Hasyim, "Penerapan *Cyber Security*", dalam http://kemhubri.dephub.go.id/pusdatin/files/materi/Penerapan_Cybersecurity.pdf, diakses pada 17 Oktober 2018.

"Kemkominfo: Pengguna Internet di Indonesia Capai 82 Juta", dalam http://kominfo.go.id/index.php/content/detail/3980/Kemkominfo%3A+Pengguna+Internet+di+Indone sia+Capai+82+Juta/0/berita_satker#.U9G405R_tfs, diakses pada 24 Oktober 2018.

"Ketika Hacker Lebih Menakutkan Ketimbang Teroris", dalam http://m.news.viva.co.id/news/read/507480- ketika-hacker-lebih-menakutkan-ketimbang-teroris, diakses pada 17 Oktober 2018.