Volume 18 Nomor 2, Halaman 194-215
Istinbath : Jurnal Hukum
ISSN : Print 1829-8117 – Online 2527-3973

Tripartite Collaborative Institutions: Skema Konvergensi Institusi Untuk Mewujudkan Ketahanan Siber Indonesia

Fradhana Putra D., Dedi Joansyah P., Sahril Wildani, Ana Laela Fatikhatul C., Alfiah Yustiningrum, Dinda Fefty M P
Fakultas Hukum, Universitas Jember, Jember, Indonesia
E-mail : dfradhana@gmail.com

Abstract

Cybercrime is a crime that is carried out systematically to damage or destroy computer networks, and will automatically have an impact on important data stored on the computer network. This article is written using a normative legal research method, with data sources in the form of primary legal materials and secondary legal materials, understood using a conceptual approach and a statute approach, then the data is analyzed qualitatively through deductive thinking. From the results of the research, it is known that the weakness of technical and non-technical infrastructure related to the network and information systems of a country is one of the reasons of cyber crime. So we need a defense concept that can overcome these weaknesses. The concept of cyber defense with tripartite collaborative institutions can be used as an option to strengthen cyber defense. With a system of cooperation between the Ministry of Defense, Kominfo, and BSSN. The Ministry of Defense focuses on cyber threats from abroad, the Ministry of Communication and Information focuses on cyber threats from within the country, while BSNN focuses on coordination, prevention, and handling of cyber crimes.

Keywords: *Cyberspace, Cyberattack, Convergence, Tripartite Colaboration*

Abstrak

Kejahatan siber (cybercrime) adalah tindak kejahatan yang dilakukan secara sistematis dengan tujuan merusak atau menghancurkan jaringan komputer, dan secara otomatis akan berdampak pada data penting yang tersimpan pada jaringan komputer tersebut. Artikel ini merupakan tulisan dengan metode penelitian hukum normatif, dengan sumber data berupa bahan hukum primer dan bahan hukum sekunder, dipahami menggunakan *conseptual approach* dan *statute approach*, lalu data dianalisa secara kualiatif dengan cara berpikir deduktif. Dari hasil penelitain diketahui bahwa lemahnya infrastruktur teknis dan non-teknis berhubungan dengan sistem jaringan dan informasi dari suatu Negara, menjadi salah satu penyebab terjadinya

kejahatan siber. Sehingga dibutuhkan suatu konsep pertahanan yang dapat mengatasi kelemahan tersebut. Konsep pertahanan siber dengan *tripartite collaborative institutions* dapat dijadikan opsi guna memperkuat pertahanan siber. Dengan sistem kerjasama antara Kemenhan, Kominfo, dan BSSN. Kementerian Pertahanan fokus pada ancaman siber dari luar negeri, Kementerian Komunikasi dan Informasi fokus pada ancaman siber dari dalam negeri, sedangkan BSNN fokus pada koordinasi, pencegahan, dan penanganan terhadap tindak pidana siber.

Kata kunci: *Cyberspace, Serangan Siber, Konvergensi, Kolaboaris Tripartite.*

Istinbath: Jurnal Hukum
Website : http://e-journal.metrouniv.ac.id/index.php/istinbath/index

Received : 2021-07-16| Published : 2021-12-30.

Pendahuluan

Dunia siber yang saling terhubung dan terus berkembang, memberi banyak kemudahan sekaligus menjadi salah satu isu prioritas dunia internasional. Tingkat pemanfaatan dunia siber, berbanding lurus dengan kerentanan akan ancaman serangan siber, atau yang biasa disebut dengan *cyber attack.*[1] Terdapat banyak sekali bentuk *cyber attack*, mulai dari *skimming, human trafficking, terrorism, malware, cracking, hacking, money laundering, phising, cracking, underground economy* dan lain sebagainya.[2] Kerentanan tersebut juga mengancam Indonesia sebagai bagian dari komunitas dunia internasional.

[1] Florian J. Egloff and Max Smeets, "Publicly Attributing Cyber Attacks: A Framework," *Journal of Strategic Studies*, March 10, 2021, 1–32, https://doi.org/10.1080/01402390.2021.1895117.

[2] Marko Milanovic and Michael N. Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic," *Journal of National Security Law & Policy (JNSLP)* 11, no. 1 (2021): 247–82.

Badan Siber dan Sandi Negara (BSSN) mencatat bahwa dalam kurun waktu Januari-Juli 2021, telah terjadi 741 kasus *cyberattack.*[3] Selain itu, *Kaspersky Security Network* (KSN) juga mencatat bahwa terdapat 18.488.946 ancaman internet di dunia maya pada komputer partisipan anonim KSN di Indonesia.[4] Bahkan di tahun 2021 ini, pernah terjadi peretasan yang mengakibatkan data vaksinasi Presiden Joko Widodo bisa bocor di publik.[5] Dengan adanya fakta-fakta tersebut, maka ancaman serangan siber tidak dapat dipandang sebelah mata.

Ancaman serangan siber telah menjadi pertaruhan kedaulatan sebuah bangsa. Infrastruktur negara dalam bidang teknologi dan informasi wajib senantiasa diorientasikan sebagai salah satu upaya menjaga kedaulatan bangsa.[6] Sehingga sudah semestinya perlindungan dan keamanan operasional siber merupakan hal yang paling mendasar guna menghadapi derasnya arus teknologi dan informasi. Bagi suatu negara, keamanan siber menjadi pilar yang fundamental sebagai bentuk antisipasi dari adanya pengaruh teknologi yang dapat menimbulkan tindak kejahatan lintas batas.[7]

Teknologi yang menghubungkan manusia dan negara dengan tanpa batas, tetapi sangat rentan akan serangan siber. Sebagai negara terus maju dalam menjadi tergantung pada teknologi dan jaringan yang lebih luas, taruhannya keamanan juga meningkat.[8] Oleh karena demikian, *cyber attack* dapat menyerang kedaulatan negara, khususnya dalam hal data informasi rahasia negara. Terlebih, pada era perkembangan teknologi dan informasi; pola interaksi dalam *cyber space* seringkali dilakukan, mengingat *cyberspace* memiliki *power* dengan memberikan keleluasaan seseorang

[3] Alviansyah Pasaribu, "BSSN Catat 741 Juta Kali Serangan Siber Periode Januari-Juli 2021," antaranews.com, 2021, https://www.antaranews.com/berita/2347446/bssn-catat-741-juta-kali-serangan-siber-periode-januari-juli-2021.

[4] Noer Qomariah Kusumawardhani, "Ancaman Siber Di Indonesia Meningkat," republika.co.id, 2021, https://republika.co.id/berita/trendtek/internet/qxkbqh368/ancaman-siber-di-indonesia-meningkat.

[5] Markus Junianto Sihaloho, "Sertifikat Vaksinasi Jokowi Bocor, Pakar: Keamanan Siber Kita Lemah," beritasatu.com, 2021, https://www.beritasatu.com/digital/822641/sertifikat-vaksinasi-jokowi-bocor-pakar-keamanan-siber-kita-lemah.

[6] David Omand, "Natural Hazards and National Security: The COVID-19 Lessons," *PRISM* 9, no. 2 (2021): 1–19.

[7] Yelena Biberman, "The Technologies and International Politics of Genetic Warfare," *Strategic Studies Quarterly* 15, no. 3 (2021): 6–33.

[8] Marios Panagiotis Efthymiopoulos*, A Cyber-Security Framework for Development, Defense and Innovation at NATO*, Journal of Innovation and Entrepreneurship, 2019, hlm 16

untuk melakukan sesuatu.[9] Sehingga, *cyberspace* tidak memiliki standar kekuatan tersendiri; sangat susah menentukan mengenai baik atau buruknya suatu tindakan dalam dunia virtual. Tak ayal, muncul berbagai tingkat perilaku ilegal di dunia maya atau *cyber space* dapat dimacamkan seperti kejahatan dunia maya, *cyber terrorism*, dan *cyber war*.

Meskipun begitu, *cyberspace* menjadi salah satu bentuk kemajuan teknologi siber sekaligus menjadi instrumen primer dari *cyberpower*. Kemajuan teknologi siber dipengaruhi oleh sebuah *maxim* bahwa 'teknologi adalah pedang bermata dua';[10] oleh karena, di samping teknologi memiliki andil dalam pembangunan peradaban manusia melalui berbagai kemudahannya, teknologi juga berpotensi menjadi media yang efektif untuk melakukan tindak kejahatan.[11] *Pertama,* teknologi mendorong perkembangan intelektualitas sumber daya manusia dengan berbagai upaya akademik; misalnya publikasi artikel jurnal, makalah, web-seminar, deseminasi, dan lain sebagainya –yang tersedia di *cyberspace*-. Sehingga, faset teknologi mendorong upaya pemerataan informasi dan ilmu pengetahuan bagi masyarakat. *Kedua,* kecanggihan teknologi dimanfaatkan oleh beberapa oknum untuk melakukan tindak kejahatan lintas batas yang dapat menyebabkan kerugian materiil maupun non-materiil.

Kondisi paradoks di atas dapat direfleksikan sebagaimana yang disampaikan oleh Soerjono Soekanto,[12] bahwa perubahan-perubahan di bidang kemasyarakatan akan berbanding lurus dan beriringan dengan perkembangan teknologi. Kemajuan teknologi sebagai bagian dari perkembangan masyarakat justru melahirkan enigma baru yaitu *cybercrime*. Kejahatan siber (*cybercrime*) dapat menyebabkan disfungsionalitas infrastruktur teknologi publik, sehingga dapat mengakibatkan kerugian negara sekaligus meresahkan masyarakat. Oleh karena itu, diperlukan suatu skema yang bersifat konvergensif sebagai upaya kolaborasi dan kerjasama antara lembaga pemerintah terhadap upaya pengamanan infrastruktur sistem dan jaringan negara. Hal ini dilakukan agar pelaksanaan keamanan siber dapat dilakukan secara efisien dan efektif dengan mengembangkan, memanfaatkan, mengkoordinasikan, mengkonsolidasikan, seluruh

[9] Jeffrey M. Erickson, "The Cyber Defense Review: Cybersecurity within a Pandemic Environment," *The Cyber Defense Review* 6, no. 2 (2021): 9–14.

[10] Sergio Castro, "Towards the Development of a Rationalist Cyber Conflict Theory," *The Cyber Defense Review* 6, no. 1 (2021): 35–62.

[11] Castro.

[12] Castro.

elemen keamanan siber. Namun, pilar-pilar kewenangan setiap lembaga perlu diperhatikan agar tidak terjadi tumpang tindih dan benturan kewenangan dalam penerapan penegakan hukum siber.

Dengan demikian, penelitian hukum ini memiliki dua isu hukum. *Pertama*, Bagaimana dinamika perkembangan *cyberspace* dan *cybercrime*? *Kedua*, Bagaimana implementasi *Tripartite Collaborative Institutions* sebagai strategi Konvergensi dalam mempertahankan ketahanan siber Indonesia? Penelitian hukum ini bertujuan menganalisa perkembangan *cybercrime* sebagai bagian dari era *cyberspace*; sekaligus memberikan satu bentuk konsepsi melalui pendekatan *tripartite* atas institusi negara untuk menjaga ketanahan siber di Indonesia.

Metodelogi Penelitian

Penelitian ini adalah penelitian hukum normatif; sehingga, penelitian dilakukan dengan berbagai upaya guna mencapai kebenaran koherensi dengan menghubungkan hasil identifikasi atas keselerasan antara peraturan-peraturan yang berlaku dengan norma-norma dan/atau prinsip-prinsip hukum yang berlaku di masyarakat.[13] Penelitian ini bertujuan mengkaji enigma dan dinamika keberadaan kejahatan siber dengan berbagai motifnya; sekaligus untuk memberikan konsep tripartit dalam strategi konvergensif sebagai salah satu upaya mempertahankan ketahanan siber nasional. Pendekatan yang digunakan dalam penelitian ini adalah pendekatan konseptual dan pendekatan peraturan perundang-undangan. Bahan hukum yang digunakan terdiri dari bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer yang digunakan adalah peraturan perundang-undangan yang berhubungan dengan kejahatan siber. Sedangkan bahan hukum sekunder yang digunakan adalah artikel jurnal, buku-buku hukum, dan lain sebagainya. Kedua bahan hukum tersebut diinventarisir oleh peneliti melalui studi kepustakaan agar mendapatkan preskripsi atas isu hukum yang dibahas. Kemudian, peneliti menggunakan analisa data menggunakan pola deduksi untuk menjelaskan berbagai norma Peraturan yang berkaitan dengan isu hukum terlebih dahulu kemudian menjelaskan tentang fakta hukum kemudian. Analisa data tersebut disusun secara sistematis, teratur, logis, saksama, dan dideskripsikan secara holistik dan

[13] Peter Mahmud Marzuki, *Penelitian Hukum: Edisi Revisi*, 13th ed. (Jakarta: KENCANA, 2017).

rinci. Dengan demikian, pola penalaran tersebut disusun secara sistematis sehingga tercapai suatu kesimpulan dari isu hukum yang dikaji.

Pembahasan

Eksistensi Cyberattack sebagai Cybercrime: Enigma dan Dinamika

Tidak ada definisi yang pasti terkait *cybercrime*.[14] Bahkan, tindakan *cybercrime* dapat dicirkan dengan istilah yang berbeda-beda, misalnya *computer-crime*, *network intrusion*, *internet security*, *network intusion*, dan lain sebagainya, khususnya termasuk definisi pula dalam peraturan perundang-undangan dan kebijakan pada suatu negara maupun organisasi internasional.[15] *The Prevention of Crime and the Treatment of Offenders* 1990 sebagai hasil dari Konggres Perserikatan Bangsa-Bangsa memberikan makna *cybercrime* dalam dua term.[16] *Pertama*, *cybercrime* sebagai *computer crime*. Maknanya, *cybercrime* adalah tindakan ilegal berupa serangan yang menyasar sistem keamanan dan data yang diproses pada suatu computer. *Kedua*, *cybercrime* sebagai *computer related crime.* Artinya, *cybercrime* adalah perbuatan illegal yang menganggu dan/atau merusak terhadap hal-hal yang berhubungan dengan sistem jaringan atau komputer. Di sisi lain, *cybercrime* dapat dimengerti sebagai segala tindakan yang menyasar pada serangan terhadap sistem, jaringan, dan data; dengan memanfaatkan kecanggihan teknlogi internet.

Cybercrime merupakan hambatan utama terhadap pelaksanaan *e-governance* dan *e-government* di negara berkembang. Oleh karena itu, pemerintah memiliki peran penting dalam mengembangkan mekanisme kontrol yang diimplementasikan dalam bentuk undang-undang, menetapkan kebijakan yang tepat, fasilitas pelengkap, khususnya yang memengaruhi sektor telekomunikasi, infrastruktur lain, dan modal manusia. Terlebih, *cybercrime* sebagai bagian dari kejahatan yang berbasis pada perkembangan teknologi secara teknis dilakukan dengan adanya kolaborasi pelaku

[14] Hassan Younies and Tareq Na'el Al-Tawil, "Effect of Cybercrime Laws on Protecting Citizens and Businesses in the United Arab Emirates (UAE)," *Journal of Financial Crime* 27, no. 4 (May 25, 2020): 1089–1105, https://doi.org/10.1108/JFC-04-2020-0055.

[15] Vasiliy Laptev and Vladimir Fedin, "Legal Awareness in a Digital Society," *Russian Law Journal* 8, no. 1 (March 27, 2020): 138–57, https://doi.org/10.17589/2309-8678-2020-8-1-138-157.

[16] Lisa J. Sotto, *Privacy and Cybersecurity Law Deskbook*, 2021st ed. (New York: Wolters Kluwer Law & Business, 2020).

lintas negara dengan target yang berada di suatu yurisdiksi lain.[17] Kejahatan siber merupakan kejahatan yang berbasis teknologi serta pelaksanaannya dapat dilaksanakan secara sistematis. Di tinjau dari motifnya, *cybercrime* dikategorikan dalam lima motif.

Pertama, cybercrime merupakan suatu bentuk perbuatan melawan hukum yang dilakukan karena murni kriminalitas. Pada motif ini, internet dijadikan sebagai media untuk melakukan kejahatan terhadap berbagai *user* atau *tools* dari komputer lain. Seringkali, tindakan kejahatan yang dilakukan termasuk dalam kategori *cybercrime* murni yaitu *carding*, *spamming*, penyebaran material bajakan, dan lain sebagainya. *Kedua, cybercrime* merupakan *cryptic crime*. Oleh sebab, identifikasi suatu tindakan pada *cyberspace* membutuhkan usaha yang komprehensif dan elaboratif. Sehingga, cukup sulit menentukan apakah tindakan tersebut termasuk tindakan kriminal atau bukan. Misalnya, terdapat akun sosial media yang memiliki profil yang sama dengan seseorang yang pada faktanya ada. Padahal, orang tersebut bukanlah orang yang sebenarnya; dia menggunakan profil orang lain agar seluruh tindakan di sosial media seakan-akan digambarkan sebagai tindakan yang dilakukan oleh orang yang mereka manfaatkan. *Ketiga*, *cybercrime* sebagai kejahatan terhadap kehormatan individu. Maknanya, *cybercrime* juga tidak jarang dilakukan untuk merusak kehormatan manusia atau mendelegitimasi keberadaan seseorang di dunia internet dengan melakukan berbagai tindakan yang menyasar pada pornografi, *cyberstalking*, kesalahan, privasi, dan lain sebagainya. *Keempat*, *cybercrime* sebagai kejahatan terhadap hak cipta atau hak milik seseorang. Lumrahnya, tindakan ini dilakukan dengan mengubah, memasarkan, menggandakan, mengganti suatu hak cipta; agar dapat menghasilkan keuntungan pribadi. *Kelima, cybercrime* terhadap pemerintah. Kejahatan ini dapat dilakukan dengan berorientasi pada penyerangan infrastruktur pemerintah untuk merusak segala sistem yang dimiliki oleh pemerintah, sehingga seluruh data intelijen dan data rahasia negara dapat di dikuasai oleh *cybercrimer*.

Cyber attacks adalah upaya untuk ‘merusak’ atau ‘menghancurkan’ jaringan komputer atau perangkat internet lainnya.[18] Makna ‘merusak’ dari aktivitas tersebut yakni dapat mengubah, mengacaukan, menipu, menurunkan kualitas sistem atau

[17] Keith B. Alexander and Jamil N. Jaffer, “COVID-19 and the Cyber Challenge,” *The Cyber Defense Review* 6, no. 2 (2021): 17–28.

[18] Milanovic and Schmitt, “Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic.”

jaringan komputer. Sedangkan, makna 'menghancurkan' yaitu aktivitas tersebut dapat memberhentikan program yang ada di dalam suatu sistem komputer secara paksa. *Cyber attacks* inilah yang dapat mencuri identitas seseorang maupun informasi keuangan suatu perusahaan. Bahkan, dengan meretas *website* pemerintah, serangan ini dapat menyebabkan lenyapnya data pribadi warga negara.[19] Aktivitas tersebut dapat berkisar manakala komputer seseorang termuat oleh virus, hingga dapat berdampak lebih besar yakni sepert arti diretasnya sistem jaringan perusahaan multinasional guna mendapatkan pengetahuan orang dalam serta mencuri informasi keuangan dari pelanggan serta perusahaan itu sendiri.

Aktivitas *cyber attacks* meruapakan salah satu bentuk kehatan non-kekerasan yang tentunya melanggar prinsip non-intervensi dari suatu pihak.[20] *Cyber attacks* bukanlah masalah teknis; karena kerusakan yang diakibatkan olehnya berkaitan dengan gangguan terhadap hak dan kepentingan orang, organisasi, maupun pemerintah suatu negara sekalipun. Serangan tersebut sering menargetkan berbagai unsur infrastruktur yang vital yaitu e-aset, sistem, bagian dari sistem, hal-hal yang berfungsi sebagai aspek penunjang masyarakat modern, seperti jaringan transportasi atau jaringan pemerintah, dan perusakan dapat menimbulkan dampak bagi kondisi stabilitas suatu negara. Sehingga, hal tersebut berakibat pada hilangnya data rahasia atau adanya perubahan data rahasia tersebut, bahkan terjadinya kebocoran data rahasia maupun informasi lainnya. Secara prinsip, aktivitas *cyber attacks* menjuru pada akses ilegal ke sistem informasi, memberikan gangguan kepada sistem, dan mencuri data yang melindungi integritas sistem komputer secara ilegal.[21] *Cyber attacks* dapat diklasifikasikan dalam dua kategori, yakni *denial of service* (DoS) *attacks* dan *deception attacks.*[22]

Cyber attacks yang dilakukan menggunakan teknik DoS memiliki ciri khas, yakni adanya botnet. Nantinya, botnet akan membanjiri *host* yang terhubung ke internet dengan jutaan permintaan informasi palsu, yang dapat menyebabkan sementara waktu

---

[19] Nori Katagiri, "Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks," *Journal of Cybersecurity* 7, no. 1 (February 16, 2021): 1–9, https://doi.org/10.1093/cybsec/tyab009.

[20] Jeffrey M. Erickson, "The Cyber Defense Review: Looking Forward," *The Cyber Defense Review* 6, no. 1 (2021): 9–16.

[21] Marie Baezner, "Cybersecurity in Switzerland: Challenges and the Way Forward for the Swiss Armed Forces," *Connections* 19, no. 1 (2020): 63–72.

[22] Andrew J. Grotto and Martin Schallbruch, "Cybersecurity and the Risk Governance Triangle," *International Cybersecurity Law Review* 2, no. 1 (June 24, 2021): 77–92, https://doi.org/10.1365/s43439-021-00016-9.

atau tanpa batas dapat menghentikan atau menangguhkan suatu layanan dari sistem komputer. Sedangkan, tingkat kerusakan pada *deception attacks* lebih mengarah pada konsekuensi yang lebih serius, karena serangannya mengkompromikan integritas dan autisitas data yang lebih *soft* dan tersembunyi. Berdasarkan tipikalnya, *deception attacks* sendiri terbagi atas data *replay attacks* dan *FDI attacks*.[23] Data *replay attacks* adalah suatu bentuk serangan yang menitikberatkan pada data pengukuran atau perintah kontrol yang telah dikirimkan melalui jaringand dengan mengakibatkan suatu program layaknya sengaja diputar ulang maupun ditunda, yang juga akan menghasilkan efek yang mirip dengan penundaan acak yang telah terinduksi dengan jaringan. Sedangkan *FDI attacks* adalah serangan yang dilakukan dengan menyuntikkan data palsu ke dalam suatu pengontrol jaringan, yang ditunjukkan dengan munculnya kesalahan sensor maupun kesalahan aktuator pada suatu sistem komputer.

Serangan siber bukan hanya mencakup perilaku yang melanggar hukum; tetapi juga mencakup perilaku yang dianggap tidak pantas atau amoral. Banyak kasus terjadi menunjukkan bukan karena ada perilaku kriminal baru, melainkan ada cara baru untuk melakukan perilaku yang ada. Maka dari itu, saat ini *cyber attacks* dipecah menjadi dua kategori berdasarkan tekniknya; yakni serangan sintaksis dan serangan semantik.[24] Serangan sintaksis ini berkaitan dengan serangan yang dilakukan terhadap perangkat lunak yang mencakup virus, malware, dan lain sebagainya. Sedangkan serangan semantik adalah serangan yang menggunakan modifikasi serta penyebaran informasi yang benar dan salah. Maksudnya, suatu informasi yang didapat secara ilegal itu dimodifikasi untuk menutupi jejak dari pemilik informasi tersebut, kemudian dilakukanlah penyebaran informasi kepada publik. Secara tidak langsung, serangan siber merupakan tingkatan serangan kinetik di dunia fisik, yang digunakan sebagai pengganti kekerasan konvensional dengan mencapai tujuan yang sama tanpa menimbulkan resiko yang sama dengan penyerang.[25] Ironisnya, saat ini sulit bagi negara untuk menilai ruang lingkup *cyber attacks* atau mencari tahu siapa yang bertanggung

[23] William Steingartner, Darko Galinec, and Andrija Kozina, "Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model," *Symmetry* 13, no. 1 (2021): 1–25.

[24] Sharngan Aravindakshan, "Cyberattacks: A Look at Evidentiary Thresholds in International Law," *Indian Journal of International Law* 59, no. 1–4 (February 17, 2021): 285–99, https://doi.org/10.1007/s40901-020-00113-0.

[25] Steven David Brown, "Hacking for Evidence: The Risks and Rewards of Deploying Malware in Pursuit of Justice," *ERA Forum* 20, no. 3 (February 6, 2020): 423–38, https://doi.org/10.1007/s12027-019-00571-z.

jawab atas aktivitas tersebut. Kesulitan itu didasarkan pada alasan suatu negara yang takut melanggar hukum perang apabila menindaklanjuti adanya aktivitas serangan *cyber*.

Adanya *cyber attacks* yang mengganggu jaringan informasi serta infrastruktur prinsipil dalam suatu negara dapat berdampak pada pertahanan nasional, mengganggu komando dan kontrol sosial, serta melemahkan kemauan politik dari suatu negara.[26] *Cyber attack* mengalami peningkatan dalam skala dan keparahan yang lebih berdampak, yang berbanding terbalik dengan kualitas jaringan sistem, dan layanan *cyber* suatu negara untuk mendukung kegiatan operasional negara. Sehingga, data-data yang bersifat prnisipal tetap rentan terhadap pencurian, spionase, gangguan, dan penghancuran.[27] Para pelaku kegiatan tersebut memiliki beragam motivasi. Lazimnya, mereka berhasil untuk mencapai suatu bentuk reputasi yang paling tinggi, kepuasan diri, memperkaya diri, dan memperoleh keuntungan non uang lainnya.

Terdapat beberapa alasan adanya serangan siber; yaitu: (1) serangan siber diharapkan menciptakan rasa takut pada individu kelompok atau masyarakat; (2) serangan siber dapat menimbulkan kerusakan yang spektakuler; dan (3) menciptakan kerugian finansial yang cukup besar. Sebagian besar serangan dunia maya pada perangkat komputasi, atau pada jaringan yang menghubungkannya, akan sesuai dengan pola tertentu. Serangan ini memerlukan beberapa bentuk akses ke sistem yang ditargetkan melalui perangkat aplikasi atau jaringan yang biasanya diikuti oleh semacam eksploitasi data.[28] Serangan siber dilakukan dalam sepersekian detik, sementara alat pencegahan dan deteksi otomatis yang dapat beroperasi pada kecepatan komputer tergantung pada cepat lambatnya pengambilan keputusan dari manusia.[29] Sehingga, kecepatan serangan *cyber* dengan tingkat kecepatan manusia, khsususnya daya operasionalnya, tidaklah selaras. Ancaman *cyber attack* dalam berbagai aspeknya menuntut adanya penyelenggaraan negara di era digital yang berdasarkan pada orientasi pengamanan sekaligus pengelolaan pada bidang siber sebagai wujud

[26] Egloff and Smeets, "Publicly Attributing Cyber Attacks: A Framework."

[27] Peter J Phillips and Gabriela Pohl, "Disinformation Cascades, Espionage & Counter-Intelligence," *The International Journal of Intelligence, Security, and Public Affairs* 22, no. 2 (October 20, 2020): 1–14, https://doi.org/10.1080/23800992.2020.1834311.

[28] Mark Johnson, *Crime Security and Digital Intelligence*, (New York : Routledge, 2016), hlm. 70.

[29] Nawa Raj Pokhrel et al., "Cybersecurity: A Predictive Analytical Model for Software Vulnerability Discovery Process," *Journal of Cyber Security Technology* 5, no. 1 (January 2, 2021): 41–69, https://doi.org/10.1080/23742917.2020.1816647.

langkah strategis untuk mencapai tujuan bangsa dan menjaga kedaulatan bangsa.[30] Dengan demikian, solusi pemerintah dalam mengantisipasi dan mengelola derasnya teknologi informasi membutuhkan kolaborasi dari berbagai pihak; sehingga, aspek skema yang dirancang dapat dilakukan dengan optimal, salah satunya dengan terbitnya Perpes Nomor 53 tahun 2017 yang selanjutnya disempurnakan dengan Perpres Nomor 133 tahun 2017; sebagaimana diubah terakhir kali dengan Perpres Nomor 28 tahun 2021 mengenai pembentukan Badan Siber dan Sandi Negara (BSSN). Langkah strategis tersebut adalah upaya negara untuk menjaga kedaulatan ruang siber negara melalui tata kelola pengamanan yang kuat. Perpres tersebut juga menegaskan bahwa ruang siber merupakan kesatuan yang utuh dari wilayah Negara Kesatuan Republik Indonesia (NKRI) yang tidak terpisahkan dengan wilayah lainnya, yaitu darat, laut dan udara. Terlebih, penguatan di bidang keamanan siber adalah wujud usaha pemerintah untuk melahirkan keamanan nasional. Sehingga, hadirnya lembaga pemerintah non Kementerian yang berada di bawah dan bertanggung jawab kepada Presiden ini menjadi pilar untuk menjamin keberlangsungan dan terselenggaranya.

Tripartite Collaborative Institutions: Sebuah Strategi Konvergensif

Pemanfaatan teknologi dan informasi yang sedang berkembang dan digunakan sebagai media menunjang kehidupan masyarakat memiliki konsekuensi kewajiban untuk menjadi bagian dari norma.[31] Oleh sebab, apabila hal tersebut –perkembangan digitalisasi–tidak diatur dalam suatu bentuk norma hukum, maka muncul berbagai masalah mengenai pertentangan aspek moralitas dengan dampak dari modernisasi.[32] Dengan demikian, tak salah apabila Bo Zhao menyatakan terdapat tiga faktor yang mendorong perubahan pada suatu profesi pada masa modernisasi;[33] yaitu teknologi informasi, liberalisasi, dan tantangan kapitalisme. Sementara itu, teknologi informasi melahirkan berbagai teknologi kecerdasan buatan yang dapat berfungsi dalam

[30] Bora Ly and Romny Ly, "Cybersecurity in Unmanned Aerial Vehicles (UAVs)," *Journal of Cyber Security Technology* 5, no. 2 (April 3, 2021): 120–37, https://doi.org/10.1080/23742917.2020.1846307.

[31] Tejas N. Narechania and Erik Stallman, "Internet Federalism," *Harvard Journal of Law & Technology* 34, no. 2 (2021): 548–618.

[32] Jan Oster, "Code Is Code and Law Is Law—the Law of Digitalization and the Digitalization of Law," *International Journal of Law and Information Technology* 29, no. 2 (July 3, 2021): 101–17, https://doi.org/10.1093/ijlit/eaab004.

[33] Bo Zhao, "Seeking Legal Boundaries of Digital Home in the IOT Age: A Conceptual Reflection," *European Journal of Law and Technology* 12, no. 1 (2021): 1–29.

implementasi instrumen hukum suatu negara. Alasannya, penggunaan teknologi kecerdasan buatan melahirkan suatu bentuk transformasi pada layanan dan tata kelola mengenai kebutuhan hukum masyarakat. Kemajuan teknologi yang berbanding lurus dengan perkembangan keilmuan hukum sejatinya berdasarkan pada sebuah *maxim* hukum yang disampaikan oleh Satjipto Rahardjo bahwa Hukum untuk manusia, bukan manusia untuk hukum.[34]

Istilah hukum dapat dikategorikan dalam dua pemaknaan, yaitu hukum objektif dan hukum subjektif.[35] Pengertian dari hukum objektif adalah bangunan peraturan yang mengatur pola interaksi dan pola hubungan antar sesama masyarakat; sedangkan, hukum subjektif memberikan pengertian bahwa terdapat hak dan atau kewenangan yang diperoleh manusia berdasarkan hukum objektif. Maka dari itu, konsep hukum progresif memberikan orientasi bahwa hukum yang bergerak wajib senantiasa mengikuti perkembangan zaman sekaligus menjadi jalan keluar untuk menjawab segala masalah yang berkembang di dalam masyarakat, serta mampu menjadi di sarana pelayanan bagi masyarakat dengan memperhatikan aspek nilai-nilai moralitas dan sumber daya manusia yang ada, baik itu dari sisi masyarakat itu sendiri dan atau dari aparat penegak hukum.[36] Gagasan hukum progresif sebagaimana dikemukakan oleh Satjipto Rahardjo memiliki hubungan erat dengan strategi konvergensi hukum dalam menghadapi kemajuan teknologi. *Oxford Advanced Learner's Dictionary* mendefinisikan konvergensi sebagai "*to move towards and meet at the same place*" dan "*to become similar or the same*" atau dapat dikatakan dengan 'mengumpul dan berpadu'. Term konvergensif pada aspek bidang telekomunikasi dimaknai sebagai kemampuan dari jaringan yang menyasar pada kemampuan bekerjanya berbagai jenis layanan yang dapat menyatukan perangkat secara bersamaan dari suatu konsumen. Bukan hanya itu, konvergensi dimaknai sebagai penyelenggaraan aktivitas sistem-jaringan yang dilakukan oleh suatu entitas dengan kemampuan teknologi yang sama; yang berasal dari dua dan/atau beberapa entitas lainnya.

[34] Satjipto Rahardjo, *Membedah Hukum Progresif* (Jakarta: Penerbit Buku Kompas, 2006).
[35] Satjipto Rahardjo, *Penegakan Hukum Progresif* (Jakarta: Penerbit Buku Kompas, 2010).
[36] Satjipto Rahardjo, *Hukum Progresif: Sebuah Sintesa Hukum Indonesia* (Yogyakarta: Genta Publishing, 2009).

Pada perspektif hukum, konsep konvergensi seringkali dikaitkan dengan paradigma hukum terhadap perkembangan teknologi.[37] Oleh sebab, kajian hukum memberikan dua kategorisasi mengenai aspek skema konvergensi, yakni konvergensi formal dan konvergensi fungsional; sebagaimana yang diungkapkan oleh Ugo Mattei dan Luca G. Pes.[38] Pandangan konvergensi formal memberikan suatu jalan pemikiran bahwa suatu institusi atau lembaga yang memiliki kewenangan yang sama, wajib saling melengkapi dan berkaborasi untuk mengatur suatu format hukum. Konvergensi formal menekankan pada faset efektivitas dan efisiensi dari suatu lembaga negara agar dapat berfungsi secara optimal dalam melaksanakan wewenang dan tugas nya. Sedangkan konvergensi fungsional menekankan pada adanya aspek cepat dan berkelanjutan dalam melakukan suatu kebijakan atau perkembangan teknologi yang berdampak luas bagi masyarakat. Pada konvergensi fungsional ini yang ditekankan adalah aspek aturan dari suatu tatanan hukum untuk ditaati masyarakat. Pada penelitian ini, lebih diorientasikan pada aspek konvergensi formal untuk menghadapi kerentanan serta berbagai kekhawatiran akan keamanan siber nasional.

Keamanan bukan hanya gagasan untuk bebas dari bahaya, seperti yang umumnya dipahami, tetapi dikaitkan dengan kehadiran musuh negara.[39] Kekhawatiran yang wajib segera ditemukan jalan keluarnya adalah apabila terdapat musuh negara yang memiliki kemampuan canggih melihat beberapa kelemahan dalam dunia siber yang dimiliki oleh negara kita. Terlebih, rencana serangan tersebut memang menargetkan beberapa infrastruktur vital dikarenakan infrastruktur tersebut dianggap merupakan titik pusat yang menjalankan sistem komando dan kontrol, pusat pengelolaan logistik, pusat perencanaan dari seluruh sumber daya suatu negara. *Cyber attacks* biasanya dapat dideteksi sangat lambat, sangat sulit dilacak dan seringkali tidak dapat dilihat secara terpisah, karena pada dasarnya serangan dunia maya menjadi semakin canggih dan cerdas yang telah ditunjang dengan meningkatnya tingkat jaringan

[37] Bertrand Crettez, Bruno Deffains, and Olivier Musy, "On the Dynamics of Legal Convergence," *Public Choice* 156, no. 1/2 (2013): 345–56.

[38] Ugo Mattei and Luca G. Pes, *Civil Law and Common Law: Toward Convergence?* (Oxford University Press, 2008), https://doi.org/10.1093/oxfordhb/9780199208425.003.0015.

[39] Monesh Kumar and Puru Lekhi, "Cyber Security: An Emerging Role of Law in the Field of Cyber Crime," *National Journal of Cyber Security Law* 4, no. 1 (2021): 26–35.

sistem melalui IT.[40] Oleh karena itulah, harus dapat dipastikan keamanan jaringan komunikasi di masa yang akan datang.

Cara yang radikal untuk menghadapi serangan dunia maya adalah memutuskan semua koneksi domain di dunia maya. Masalahnya, hal ini berdampak akan menghapus suatu negara dari dunia modern; oleh karena, pada saat ini negara-negara dipaksa untuk terlibat dalam domain dunia maya, baik itu preferensi, prioritas, seember maupun kemampuan secara nasional. Cara radikal kedua yakni melakukan spionase dunia maya yang berfungsi untuk menyeimbangkan informasi guna mencapai titik keuntungan. Maknanya, negara kita dapat mengetahui rencana buruk dari beberapa pihak baik itu orang pribadi maupun negara lain yang yang ingin melakukan serangan siber terhadap negara kita. Tentunya, hal ini dilakukan apabila terdapat beberapa indikasi yang dilakukan oleh pihak; terutama oleh negara lain. Saluran informasi yang baru membawa peluang baru untuk mendapatkan informasi yang baru pula. Agar berhasil melawan *cyber attack*, bahkan menggunakan beberapa cara radikal di atas; perlu adanya kerjasama yang antar semua pemangku kepentingan pula, mulai dari berbagai Kementerian dalam pemerintahan, produsen teknologi, operator jaringan, dan penyedia layanan guna mengembangkan sistem agar dapat mendeteksi serangan pada tahap awal dan memastikan keamanan akan pertukaran informasi. Oleh sebab itu, perlu adanya *tripartite collaborative institutions* antara BSSN, Kementerian Pertahanan, dan Kementerian Komunikasi dan Informasi. Hal tersebut merupakan salah satu bentuk optimalisasi dari para *stakeholder* yang berwenang di Indonesia guna menghadapi serangan dunia maya.

Tripartite collaborative institutions merupakan implementasi dari konsepsi konvergensi formal yang diharapkan berfungsi dapat memberikan aspek penunjang atas efisiensi serta efektivitas masing-masing tugas dan kewenangan lembaga. *Tripartite collaborative institution* adalah cermin adanya pembangunan infrastruktur ketahanan negara. Pembangunan infrastruktur bukan hanya alutista semata; akan tetapi, kualitas operasional dan manajemen koordinasi dari para pemangku kepentingan merupakan hal yang sangat mendasar untuk menciptakan ketahanan dan kekuatan bangsa yang maju. Pembangunan tersebut digunakan agar nantinya apabila terdapat serangan *cyber* oleh suatu pihak; maka, bangsa Indonesia dapat pulih dengan cepat serta dapat bertahan,

[40] Egloff and Smeets, "Publicly Attributing Cyber Attacks: A Framework."

bahkan menghancurkannya. *Tripartite collaborative institutions* adalah strategi optimalisasi aspek koordinasi yang diharapkan dapat lebih memberikan kekuatan antar lembaga negara. Fungsi koordinasi antar lembaga negara merupakan hal primer yang patut untuk dilakukan. Hal ini dikarenakan keamanan bukan merupakan masalah teknis, tetapi masalah yang kompleks yang berkaitan dengan hukum ekonomi dan sosial.[41] Di samping itu, kita harus mengenali batasan dari keamanan itu sendiri; apakah yang perlu dilindungi merupakan hak publik maupun privat.

Apabila sesuatu yang merupakan bagian privat dari warga negara, maka harus mendapatkan persetujuan dari warga negara bersangkutan.[42] Selanjutnya, keamanan memang membutuhkan uang sebagai dasar pembangunan infrastruktur; tetapi, keamanan juga membutuhkan waktu kenyamanan, kemampuan, kebebasan, dan lain sebagainya yang tidak mungkin dapat dilakukan hanya satu lembaga negara saja. Ancaman terkait kerahasiaan, ketersediaan integritas, ketahanan; maka, masing-masing memerlukan respon yang berbeda yang tentunya membutuhkan sinergitas antara lembaga negara untuk saling memperkuat satu sama lain. Pada *tripartite collaborative institution,* Kementerian Pertahanan lebih berfokus pada ancaman siber dari luar negeri, Kementerian Komunikasi dan Informasi lebih berfokus pada ancaman siber dari dalam negeri. Sedangkan, BSSN lebih berfokus pada taraf koordinasi serta pencegahan dan penanganan terhadap tindak pidana siber. Hal ini dimaksudkan agar tidak terjadi benturan kepentingan serta tumpang tindih kewenangan antar institusi; apabila terjadi, akan menimbulkan ketidak-efektifan serta ketidakefisienan dari pelaksanaan tugas dan wewenang. Di samping itu, pembagian ini berfungsi agar nantinya apabila terjadinya problematika siber; dapat teratasi dengan baik oleh lembaga yang memiliki spesialisasi masing-masing.

Tripartite collaborative institutions dapat membuat kerangka kerja strategis sebagai salah satu pedoman untuk menentukan cara mengalahkan musuh, dengan menganalisa tujuan, cara, dan sarana. Perlunya persamaan visi misi guna memperkuat ketahanan negara sangat diperlukan. Hal ini didasarkan bahwa ketiga lembaga tersebut akan memiliki tingkat standarisasi yang sama akan tujuan dari ketahanan bangsa.

[41] Catherine Friend et al., "Fighting Cybercrime: A Review of the Irish Experience," *International Journal of Cyber Crimology* 14, no. 2 (2020): 383–99, https://doi.org/10.5281/zenodo.4766527.

[42] Information Resources Management Association, *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications*, 1st ed. (Pennsylvania: IGI Global, 2019).

Kerangka kerja tersebut merumuskan fase-fase penanganan serangan siber yang terdiri dari tiga fase, yakni:

1. Fase sebelum insiden serangan siber (*before cyber attack*)
2. Fase ketika terjadinya insiden serangan siber (*during cyber attack)*
3. Fase setelah terjadinya insiden serangan siber (*after cyber attack*)

Di samping mempertegas kedaulatan negara, adanya kolaborasi ini; wajib memberikan jaminan perlindungan dan keamanan kepada warga masyarakat. Kolaborasi antara lembaga ini bahkan dapat merancang serangan layaknya layanan intelijen khusus untuk melakukan pengintaian serta penyebaran serangan terhadap musuh, dan menguji peralatan alutista secara fisik maupun nonfisik, yang tergantung pada target yang akan dituju. Resistensii terhadap serangan siber wajib kita pahami dengan cara memodifikasi prinsip perang secara fisik dengan paradigma baru yang kita hadapi saat ini

Pada perspektif sebelum insiden serangan siber atau dapat dikatakan strategi pencegahan *cyber attacks*, ketiga pemangku kepentingan tersebut harus memberikan suatu strategi yang didasarkan pada tiga hal. *Pertama*, kemampuan, *tripartite collaborative institutions* mampu memiliki sarana dan atau dasar hukum guna mempengaruhi perilaku seseorang menjadi lebih peduli, khsuus pada operasional dunia maya. *Kedua*, kredibilitas, yakni kolaborasi ketiga lembaga tersebut mampu memberikan legitimasi bahwa tindakan-tindakan yang sebenarnya dapat diikuti oleh masyarakat luas. *Ketiga*, komunikasi, yakni segala hal yang disampaikan oleh *tripartite collaborative institutions* dapat diterima secara luas oleh masyarakat. Kemudian, pada fase manakala terjadinya insiden serangan siber (*during cyber attack),* tripatrit ini dapat melakukan degradasi dunia maya. Maknanya, *tripatrite collaboration institution* dapat melakukan operasi pemaksaan untuk menyabot jaringan atau sistem dari pihak lain apabila benar-benar telah sedang terjadi serangan siber yang dilakukan oleh *attackers.* Hal ini dilakukan guna memberikan ‘gertakan’ represif berupa peretasan sistem milik pelaku. Di samping itu, peretasan tersebut dapat memberikan identitas informasi atas pihak yang telah melakukan serangan siber. Apabila serangan tersebut berasal dari luar negeri, maka Kementerian Pertahanan harus memberikan tindakan tegas berdasarkan hukum internasional. Sedangkan, apabila serangan tersebut berasal dari dalam negeri, maka Kementerian Komunikasi dan Informasi dapat melacak lokasi melalui *IP Adress* pengguna.

Pada dasarnya, membatasi konektivitas yang dapat dampak kurangnya kerentanan resiko serangan siber terhadap suatu sistem nasional, memiliki implikasi yakni mengurangi kemampuan masyarakat untuk menggunakannya secara bebas. Meskipun begitu, adanya kolaborasi ini diharapkan dapat lebih mengendalikan jenis lalu lintas internet; terutama pada saluran kabel internet bawah laut. Maka dari itu, pada aspek pertahanan *cybe*r, utamanya manakala setelah terjadinya insiden serangan siber; *tripartite collaborative institutions* wajib melibatkan proses deteksi analisis serta sinkronisasi. Sehingga bentuk pertahanan ini merupakan serangkaian perbuatan yang melibatkan musuh sebelum dan selama insiden *cyber*. Dengan mempertahankan seluruh komponen *tripartite collaborative institutions* yang kuat, maka serangkaian operasi yang dilakukan pada berbagai saluran sangat memungkinkan untuk dapat mengatasi musuh. Tentunya, tak lupa untuk dilakukan evaluasi secara menyeluruh oleh *stakeholder* terkait. Evaluasi yang paling primer yang dapat dilakukan oleh kolaborasi ini adalah terkait kerahasiaan privasi warga negara. Pada dunia digital, informasi memiliki nilai.[43] Melindungi informasi dengan demikian sangatlah penting, tidak hanya rasa internal dan data pribadi yang sensitif harus dijaga; tetapi, data transaksional hubungan perusahaan atau individu juga tidak kalah penting. Untuk itu, dengan adanya kolaborasi triparit dari beberapa lembaga ini, dapat menunjang alat teknis seperti enkripsi dan kontrol akses untuk menciptakan kerahasiaan yang holistik.

. *Tripartite collaborative institutions* dalam pelaksanaanya dapat melakukan beberapa hal. *Pertama*, dibentuklah suatu divisi khsusus yang dapat secara spesifik untuk menyerang sistem yang sangat spesifik pula. *Kedua*, dengan adanya kolaborasi tripatrit ini diharapkan memiliki kemampuan yang luas untuk meretas semua jenis sistem yang berkaitan dengan tugas pokok dan fungsi masing-masing lembaga. Misalnya, apabila dianggap dapat memberikan dampak negatif pada stabilitas dunia maya nasional, Kementerian Pertahanan dapat meretas semua jenis sistem yang berasal dari luar negeri yang telah masuk ke Indonesia. *Ketiga*, kolaborasi ini dapat menangani suatu jenis serangan yang menimbulkan kerugian finansial dan strategis negara. *Keempat*, kolaborasi dari ketiga lembaga ini dapat menunjukkan kemampuannya untuk mengumpulkan informasi rahasia dari para pelaku serangan *cyber*, dan kemudian

[43] Mark Burdon, *Digital Data Collection and Information Privacy Law* (New York: Cambridge University Press, 2020).

menyimpan beberapa hal yang prinsipil dan kemudian menyerahkan atau menampilkannya kepada publik. Tentunya, berbagai hal yang ditampilkan kepada publik tidaklah menyeluruh. Adanya unsur publikasi ini guna memenuhi asas transparansi. *Kelima*, diharapkan dengan adanya kolaborasi ini maka negara mampu untuk mengatur operasi informasi cyber secara lebih komprehensif. Apabila penyebaran informasi yang berada di dunia maya terakumulasi dengan baik oleh instansi yang berwenang; maka, dampak-dampak negatif seperti halnya hoaks, ujaran kebencian, pencurian data informasi, dan lain sebagainya, tidak akan terjadi kembali.

Serangan balik terhadap *cyber attackers* dapat menurunkan operasi angkatan bersenjata apabila *cyber attackers* bergantung pada jaringan komersial serta penyedia layanan dan internet secara ilegal dan bersifat kontinu.[44] Aset penting negara yang harus dilindungi terhadap serangan siber internal dan eksternal dapat dicapai dengan melakukan pendekatan ketahanan yang melibatkan seluruh pembangunan infrastruktur, agar kedaulatan negara dapat ditegakkan secara seutuhnya. Kemampuan *cyber defence* harus selalu ditingkat sembari mengembangkan kebijakan umum yang revolusioner.[45] Kemudian, dengan adanya *tripartite collaborative institutions* dapat mengembangkan bersama sumber daya industri dan teknologi untuk keamanan siber. Pembangunan infrastruktur siber ini juga diperlukan untuk membangun kepercayaan masyarakat terhadap institusi negara. Segala infrastruktur lini pertahanan baik udara, darat, laut dan artileri segalanya wajib dipandu oleh sistem komputer serta secara otomatis menjadikan amunisi yang ada dapat menyesuaikan dengan penerbangan berdasarkan pembaruan *Global Positioning System*.[46] Tentunya, sistem komputasi serta operasional ini dikuasai oleh *tripartite collaborative institutions,* khususnya Kementerian Pertahanan sebagai speasialisasi dalam bidang pertahanan. Pada konteks ini, Kementerian Komunikasi dan Informasi dapat memberikan orientasi terkait adanya indikasi serangan siber yang dapat menganggu jaringan telekomunikasi dan komputasi. Selanjutnya, BSSN dapat memberikan informasi terkait bagian sistem virtual perthanan mana saja yang masih rentan untuk menghadapi serangan siber. Dengan demikian, masing-masing lembaga

[44] Martti Lehto dan Pekka Neittaanmaki, *Cyber Security: Analytics, Technology and Automation*, (Cham: Springer, 2015), hlm. 8.

[45] Nobuo Hayashi, *Military Necessity: The Art, Morality and Law of War* (New York: Cambridge University Press, 2020).

[46] Glen E. Howard and Matthew Czekaj, *Russia's Military Strategy and Doctrine* (Washington: Jamestown Foundation, 2019).

dapat ‘mengisi’ satu sama lain guna menguatkan ketahanan serta menegaskan kedaulatan bangsa.

Hubungan eksternal dengan negara mitra pandang sebagai proyek strategi keamanan jangka panjang serta upaya untuk mengatasi ketidak setaraan kekuatan antar negara.[47] Untuk itulah, diperlukan strategi politik diplomatik yang bertujuan untuk mempengaruhi sesama negara secara terstruktur dan sistematis, yang utamanya dilakukan oleh Kementerian Pertahanan. Hal ini merupakan salah satu cara untuk menggabungkan ancaman kekuatan, serta utilitas dari negara mitra. Hal ini berfungsi untuk menegosiasikan kompromi yang nantinya dapat menimbulkan keuntungan secara bersamaan dalam pengelolaan ancaman *cyber* serta kerjasama terkait pertahanan antar bangsa. Kementerian Komunikasi dan Informasi juga dapat memberikan andil besar seperti memberikan evaluasi ketahanan siber nasional kepada Kementerian Pertahanan, berupa data-data terkait penanganan kasus siber secara nasional, metode penanganan kasus siber secara nasional, dan lain sebagainya. Diplomasi yang mengandung bujukan positif inilah yang secara khusus akan menimbulkan suatu kerjasama yangg menghasilkan pencegahan bersama terhadap serangan *cyber*. Di samping itu, bangsa kita dapat memahami bagaimana negara mitra menggunakan strategi *cyber* serta bagaimana melakukan pencegahan serangan siber. BSSN juga memiliki andil penting, yakni memberikan masukan apa saja yang perlu dibahas serta dilakukan Kementerian Pertahanan dengan negara mitra. Masalah yang sampai saat ini masih belum jelas dari serangan siber adalah kurangnya data statistik yang konkret tentang pelanggaran *cyber* secara nasional maupun internasional.[48] Hal ini mengakibatkan jalannya evaluasi tidak maksimal, sehingga lembaga negara tidak dapat mendeteksi secara keseluruhan titik lemah dari sistem siber nasional. BSSN disini melakukan pendekatan proaktif melakukan pengadaan bukti yang diperlukan untuk penuntutan. Bahkan, menghargai pelaku yang bertanggung jawab atas serangan siber yang dilakukan dengan insentif ekonomi merupakan salah satu bentuk dari strategi desain proaktif.[49]

Di samping itu, BSSN bekerja sama dengan Kementerian

[47] Mario O'Neill, Ken Swinton dan Aaron Winter, *New Challenges for the EU Internal Security Strategy*, (Cambridge: Cambridge Scholars Publishing, 2013), hlm. 6.

[48] Mohamed Chawki, *et al*., *Cybercrime, Digital Forensics and Jurisdiction*, (Cham: Springer, 2015), hlm. 6.

[49] D. Frank Hsu dan Dorothy Marinucci, *Advances in Cyber Security: Technology, Operations, and Experiences*, (New York: Fordham Univ Press, 2013), hlm. 48.

Komunikasi dan Informatika melakukan pengumpulan data, mengintegrasikan sistem pencatatan pelanggaran, melakukan penegakan hukum, transfer data rahasia kepada *tripartit collaboration institutions*, serta analisa resiko serangan *cyber*. Hal tersebut dikarenakan keamanan dunia maya dibangun berdasarkan analisis ancaman siber. Bahkan, struktur dan elemen strategi keamanan siber serta program implementasinya didasarkan pada hasil analisa tersebut. Kolaborasi ketiga institusi ini juga dapat melahirkan bersama suatu pedoman pendidikan yang dirancang guna mengubah perilaku dari pengguna internet di Indonesia harus dimaksimalkan. Hal ini dikarenakan pengguna dunia maya wajib mengetahui pentingnya manajemen konfigurasi dan perbaikan suatu sistem, resiko dari dunia maya, keamanan dari dunia maya, dan daya guna positif dari dunia maya. Pemerintah juga perlu memiliki *cyber student volunteer*, guna menunda aspek publisitas serta sosialisasi akan resiko dan daya fungsi dari dunia *cyber*. Bahkan, pemerintah dapat menawarkan beasiswa kepada masyarakat yang tertarik untuk menjadi *student volunteer*. Beasiswa tersebut dapat berupa beasiswa sekolah maupun beasiswa mitra, yakni adanya timbal balik yang dilakukan oleh penerima beasiswa kepada Kementerian terkait.

Kesimpulan

Dinamika kejahatan siber dalam berbagai motif memberikan kewajiban suatu negara untuk memperkuat tata kelola infrastruktur lembaga negara yang berhubungan dengan bidang siber. Oleh sebab, orientasi kejahatan siber mengarah pada perusakan sistem dan jaringan milik negara; sehingga, dapat berpotensi mencuri atau membocorkan data rahasia milik negara. Dengan demikian, di Indonesia; tata kelola kelembagaan BSSN dalam menangani ancaman serangan siber/ cyber attack sudah sepantasnya membuat koordinasi yang utuh dan penuh dengan lembaga terkait. Skema konvergensif melalui *tripartite collaborative institutions* antara BSSN, Kementerian Pertahanan, dan Kementerian Komunikasi dan Informasi dimaksudkan agar ketiga lembaga tersebut tidak saling tumpang tindih kewenangan yang dapat menghambat upaya penegakan hukum siber; bilamana dalam menangani tindak pidana atau kejahatan Siber. Selain itu, optimalisasi koordinasi kewenangan ketiga lembaga tersebut diharapkan bahwa ketiga lembaga tersebut dapat lebih efektif dan efisien dalam menjalankan tugas dan kewenangannya untuk megantisipasi bahkan melakukan

penindakan terhadap kejahatan siber. Pada penerapannya, Kementerian Pertahanan lebih berfokus pada ancaman siber dari luar negeri, Kementerian Komunikasi dan Informasi lebih berfokus pada ancaman siber dari dalam negeri, sedangkan BSNN memiliki konsentrasi pada taraf koordinasi serta pencegahan dan penanganan terhadap tindak pidana siber.

Daftar Pustaka

Alexander, Keith B., and Jamil N. Jaffer. "COVID-19 and the Cyber Challenge." *The Cyber Defense Review* 6, no. 2 (2021): 17–28.

Aravindakshan, Sharngan. "Cyberattacks: A Look at Evidentiary Thresholds in International Law." *Indian Journal of International Law* 59, no. 1–4 (February 17, 2021): 285–99.

Association, Information Resources Management. *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications*. 1st ed. Pennsylvania: IGI Global, 2019.

Baezner, Marie. "Cybersecurity in Switzerland: Challenges and the Way Forward for the Swiss Armed Forces." *Connections* 19, no. 1 (2020): 63–72.

Biberman, Yelena. "The Technologies and International Politics of Genetic Warfare." *Strategic Studies Quarterly* 15, no. 3 (2021): 6–33.

Brown, Steven David. "Hacking for Evidence: The Risks and Rewards of Deploying Malware in Pursuit of Justice." *ERA Forum* 20, no. 3 (February 6, 2020): 423–38.

Burdon, Mark. *Digital Data Collection and Information Privacy Law*. New York: Cambridge University Press, 2020.

Castro, Sergio. "Towards the Development of a Rationalist Cyber Conflict Theory." *The Cyber Defense Review* 6, no. 1 (2021): 35–62.

Crettez, Bertrand, Bruno Deffains, and Olivier Musy. "On the Dynamics of Legal Convergence." *Public Choice* 156, no. 1/2 (2013): 345–56.

Egloff, Florian J., and Max Smeets. "Publicly Attributing Cyber Attacks: A Framework." *Journal of Strategic Studies*, March 10, 2021, 1–32. https://doi.org/10.1080/01402390.2021.1895117.

Erickson, Jeffrey M. "The Cyber Defense Review: Cybersecurity within a Pandemic Environment." *The Cyber Defense Review* 6, no. 2 (2021): 9–14.

———. "The Cyber Defense Review: Looking Forward." *The Cyber Defense Review* 6,

no. 1 (2021): 9–16.

Friend, Catherine, Lorraine Bowman Grieve, Jennifer Kavanagh, and Marek Palace. "Fighting Cybercrime: A Review of the Irish Experience." *International Journal of Cyber Crimology* 14, no. 2 (2020): 383–99.

Grotto, Andrew J., and Martin Schallbruch. "Cybersecurity and the Risk Governance Triangle." *International Cybersecurity Law Review* 2, no. 1 (June 24, 2021): 77–92.

Hayashi, Nobuo. *Military Necessity: The Art, Morality and Law of War*. New York: Cambridge University Press, 2020.

Howard, Glen E., and Matthew Czekaj. *Russia's Military Strategy and Doctrine*. Washington: Jamestown Foundation, 2019.

Katagiri, Nori. "Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks." *Journal of Cybersecurity* 7, no. 1 (February 16, 2021): 1–9.

Kumar, Monesh, and Puru Lekhi. "Cyber Security: An Emerging Role of Law in the Field of Cyber Crime." *National Journal of Cyber Security Law* 4, no. 1 (2021): 26–35.

Kusumawardhani, Noer Qomariah. "Ancaman Siber Di Indonesia Meningkat." republika.co.id, 2021.

Laptev, Vasiliy, and Vladimir Fedin. "Legal Awareness in a Digital Society." *Russian Law Journal* 8, no. 1 (March 27, 2020): 138–57.

Ly, Bora, and Romny Ly. "Cybersecurity in Unmanned Aerial Vehicles (UAVs)." *Journal of Cyber Security Technology* 5, no. 2 (April 3, 2021): 120–37.

Marzuki, Peter Mahmud. *Penelitian Hukum: Edisi Revisi*. 13th ed. Jakarta: KENCANA, 2017.

Mattei, Ugo, and Luca G. Pes. *Civil Law and Common Law: Toward Convergence?* Oxford University Press, 2008.

Milanovic, Marko, and Michael N. Schmitt. "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." *Journal of National Security Law & Policy (JNSLP)* 11, no. 1 (2021): 247–82.

Narechania, Tejas N., and Erik Stallman. "Internet Federalism." *Harvard Journal of Law & Technology* 34, no. 2 (2021): 548–618.

Omand, David. "Natural Hazards and National Security: The COVID-19 Lessons." *PRISM* 9, no. 2 (2021): 1–19.

Oster, Jan. "Code Is Code and Law Is Law—the Law of Digitalization and the Digitalization of Law." *International Journal of Law and Information Technology* 29, no. 2 (July 3, 2021): 101–17.

Pasaribu, Alviansyah. “BSSN Catat 741 Juta Kali Serangan Siber Periode Januari-Juli 2021.” antaranews.com, 2021.

Phillips, Peter J, and Gabriela Pohl. “Disinformation Cascades, Espionage & Counter-Intelligence.” *The International Journal of Intelligence, Security, and Public Affairs* 22, no. 2 (October 20, 2020): 1–14..

Pokhrel, Nawa Raj, Netra Khanal, Chris P. Tsokos, and Keshav Pokhrel. “Cybersecurity: A Predictive Analytical Model for Software Vulnerability Discovery Process.” *Journal of Cyber Security Technology* 5, no. 1 (January 2, 2021): 41–69.

Rahardjo, Satjipto. *Hukum Progresif: Sebuah Sintesa Hukum Indonesia*. Yogyakarta: Genta Publishing, 2009.

———. *Membedah Hukum Progresif*. Jakarta: Penerbit Buku Kompas, 2006.

———. *Penegakan Hukum Progresif*. Jakarta: Penerbit Buku Kompas, 2010.

Sihaloho, Markus Junianto. “Sertifikat Vaksinasi Jokowi Bocor, Pakar: Keamanan Siber Kita Lemah.” beritasatu.com, 2021.

Sotto, Lisa J. *Privacy and Cybersecurity Law Deskbook*. 2021st ed. New York: Wolters Kluwer Law & Business, 2020.

Steingartner, William, Darko Galinec, and Andrija Kozina. “Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model.” *Symmetry* 13, no. 1 (2021): 1–25.

Younies, Hassan, and Tareq Na’el Al-Tawil. “Effect of Cybercrime Laws on Protecting Citizens and Businesses in the United Arab Emirates (UAE).” *Journal of Financial Crime* 27, no. 4 (May 25, 2020): 1089–1105..

Zhao, Bo. “Seeking Legal Boundaries of Digital Home in the IOT Age: A Conceptual Reflection.” *European Journal of Law and Technology* 12, no. 1 (2021): 1–29.