Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan *Cyber Espionage* Pada Era *Society* 5.0

Hamdan Mustameer

Universitas Pembangunan Nasional Veteran Jawa Timur, hamdanmusta.02@gmail.com

Abstract

The era of Society 5.0 is a condition of society that is required to solve various challenges and social problems by utilizing various innovations that were born in the era of the Industrial Revolution 4.0 such as the Internet on Things, Big Data, Artificial Intelligence, and robots to improve the quality of human life. The new things in Era Society 5.0 should not change law enforcement based on decision-making, the freedom of legal institutions in deciding cases, the professionalism of the apparatus, and public transparency. The rapidity of this era in entering the country during the Covid-19 pandemic, triggering cybercrimes that use new tools such as virus spread, and cracking. One of the crimes that the state is vulnerable to is Cyber Espionage. This crime is an act of espionage that takes advantage of advances in technology and information. As a state of law, Indonesia is required to have policies that regulate Cyber Espionage actions while still paying attention to aspects of international law so that law enforcement in Indonesia can run smoothly. To find out the readiness of Indonesian law in facing the threat of Cyber Espionage, we write this article with normative juridical research with three approaches, conceptual approach, statutory approach, and comparative approach. The results of our research show that the national legal instruments in Indonesia are still limited to the Electronic Information and Transaction Law (ITE), Government Regulations regarding its implementation, Presidential Regulations on National Defense (Perpreshanneg), and the absence of policies that specifically regulate cyber crimes.

Keywords: *Cyber espionage*; society 5.0; national law; international law.

Abstrak

Era *Society* 5.0 adalah kondisi masyarakat yang dituntut menyelesaikan berbagai tantangan dan permasalahan sosial dengan memanfaatkan berbagai inovasi yang lahir pada era Revolusi Industri 4.0 seperti *Internet on Things* (internet untuk segala sesuatu), *Big Data* (data dengan jumlah yang besar), *Artificial Intelligence* (kecerdasan buatan), dan robot untuk meningkatkan kualitas kehidupan manusia. Hal-hal baru pada Era *Society* 5.0 seharusnya tidak mengubah penegakan hukum yang berlandaskan dengan pengambilan keputusan, kebebasan lembaga hukum dalam memutus perkara, profesionalisme aparat, dan transparansi publik. Pesatnya Era ini dalam memasuki negara pada Pandemi Covid-19, memicu kejahatan *cybercrime* yang menggunakan alat baru seperti penyebaran virus, dan cracking. Salah satu kejahatan yang rentan dialami oleh negara adalah *Cyber Espionage.* Kejahatan ini merupakan tindakan spionase yang memanfaatkan kemajuan teknologi dan informasi. Sebagai negara hukum, Indonesia diharuskan memiliki kebijakan yang mengatur tindakan *Cyber Espionage* dengan tetap memperhatikan aspek hukum internasional agar penegakan hukum di Indonesia bisa berjalan dengan lancar. Untuk mengetahui kesiapan hukum Indonesia dalam menghadapi ancaman *Cyber Espionage*, maka kami menulis artikel ini dengan penelitian yuridis normatif dengan tiga pendekatan yaitu pendekatan konseptual, pendekatan perundang-undangan, dan pendekatan perbandingan. Hasil penelitian kami menunjukkan bahwa instrumen hukum nasional di Indonesia masih terbatas pada Undang-Undang Informasi dan Transaksi Eletronik, Peraturan Pemerintah tentang penyelenggaraannya, Peraturan Presiden tentang Pertahanan Negara, dan belum adanya kebijakan yang mengatur tindak kejahatan siber secara khusus.

Kata Kunci: *Cyber Espionage*, Society 5.0, Hukum Nasional, Hukum Internasional

Jurnal
YUSTIKA
Media Hukum dan Keadilan
Fakultas Hukum Universitas Surabaya
Vol. 25 No. 01, July 2022
P-ISSN:1410-7724
E-ISSN: 2655-7479

1. Pendahuluan

Dunia telah mengalami empat revolusi industri yang telah memberikan perubahan peradaban secara signifikan. Revolusi pertama dimulai pada tahun 1750 yang diawali dengan mesin uap. Revolusi kedua ialah penemuan alat proses produksi massal di sekitaran tahun 1870. Revolusi ketiga diiringi dengan kemunculan komputer. Revolusi keempat adalah berkembangnya jaringan siber dan kecerdasan buatan. (Haqqi & Wijayati, 2019) Sampai saat ini revolusi keempat mulai bertransisi menjadi kelima. Perdana Menteri Jepang, Shinzo Abe mengemukakan konsep dari Era *Society* 5.0 dalam pidatonya di acara CeBUT pada tahun 2017.(Christiawan, 2021) Revolusi ini ditandai dengan munculnya solusi atas permasalahan Era Revolusi Industri 4.0 yang dimana banyak mesin berteknologi canggih bersaing dengan manusia.

Revolusi Era *Society* 5.0 diharapkan menyelesaikan permasalahan yang muncul pada era 4.0 dengan menjadikan manusia dan mesin saling berdampingan, dengan contoh layanan *e-commerce* dan layanan ojek online. Kedua usaha tersebut terbukti memberikan kesempatan manusia untuk bekerja dan tidak menghilangkan lapangan pekerjaan, bahkan memberikan kemudahan dalam pekerjaannya. Masa peralihan Era Industri 4.0 menuju Era *Society* 5.0 dipercepat dengan munculnya Pandemi Covid-19. Secara tidak langsung, era 5.0 telah mulai aktif ketika pemerintah memberlakukan pembatasan kegiatan fisik agar mencegah penularan virus Covid-19. Masyarakat mulai memanfaatkan teknologi sekitar yang kemudian menuntut masyarakat untuk memcahkan masalah secara kompleks, kritis dan kreatif. Menteri BUMN, Erick Thoir pernah mengatakan bahwa Era *Society* 5.0 menghasilkan banyak trasnformasi dan disrupsi digital bagi Indonesia. (Syahputra, 2021)

Digitalisasi memberikan dampak baik dan buruk kepada Indonesia karena kondisi penduduk yang padat dan mendapatkan bonus demografi pada tahun 2030-2035. Dampak baik dari lajunya perkembangan era 5.0 ini ialah menjadikan masyarakat dan pemerintah Indonesia serta pihak swasta untuk menyesuaikan perkembangan teknologi dan informasi digital. Sedangkan dampak buruk dari era 5.0 adalah meningkatnya ancaman kejahatan siber atau *cyber crime* dengan sasaran perseorangan bahkan suatu negara melalui dunia maya.

Istilah Cyber Crime pertama kali dikenalkan oleh William Gibson (1982) yang tertulis dalam novelnya dengan judul *Neuromancer* pada tahun 1984. Dalam novelnya terdapat istilah '*cyber space*' yang digambarkan dengan dunia maya yang terkoneksi dengan aktivitas komputer dan istilah '*cyber crime*' digambarkan dengan tindak kejahatan yang bertempat di dunia maya tersebut dan mengancam keamanan. (Wall, 2007) Indra Safitri berpendapat bahwa *Cyber Crime* adalah kejahatan yang berkaitan dengan penggunaan teknologi informasi sebagai media dan mencari celah keamanan sebuah sistem yang diakses oleh pengguna internet.(Wahid, 2005) Dalam perkembangannya, *cyber crime* berkembang secara pesat dengan modus yang beragam. Ragam yang dimaksud tidak hanya melibatkan pelaku individu, melainkan melibatkan negara sebagai pelakunya. Salah satu jenis *cyber crime* adalah *Cyber Espionage*.

Cyber Espionage atau spionase siber dapat dijelaskan dengan memaknai satu persatu kata *cyber* dan *espionage*. *Cyber* diartikan sebagai "dunia maya" yang menjadi media kejahatan itu berlangsung dan *espionage* atau spionase adalah upaya pengumpulan informasi yang dilakukan oleh individu atau negara.(Baker, 2003) Dengan ini *Cyber Espionage* dapat diartikan menjadi tindakan mencari informasi baik umum ataupun khusus ke sasaran yang diminta oleh pemerintah dan dijalankan oleh orang yang tidak berwenang dengan memanfaatkan ruang siber atau *cyber space*.

Praktik spionase antar negara lazim dilakukan dan dengan perkembangan zaman, sangat memungkinkan untuk melakukan spionase melalui komputer dan jaringan internet.

Kejahatan spionase pada era modern ini meminimalisir resiko untuk diketahui pihak sasaran. Kejahatan ini dapat merugikan dan mengganggu stabilitas keamanan dan pertahanan suatu negara. Salah satu kegiatan spionase asing yang telah terjadi di Indonesia adalah kasus spionase Australia dan Amerika Serikat terhadap Pemerintah Indonesia. Kasus ini diungkap oleh Kepala Badan Intelijen Negara (BIN), Marciano Norman yang menyatakan bahwa Australia telah melakukan penyadapan percakapan telepon kepada sejumlah pejabat Indonesia dalam kurun waktu 2007-2009. (Sudiarta, 2014)

Kasus tersebut mencerminkan kondisi persaingan global yang sangat mengkhawatirkan. Hal ini disebabkan oleh kemajuan teknologi informasi dan komunikasi pada era digital yang dapat disalahgunakan dan memperlihatkan kelemahan Indonesia sebagai target spionase dari segi instrumen hukumnya. Pasalnya, tindakan *Cyber Espionage* merupakan kejahatan transnasional yang megnhilangkan batas-batas negara (borderless) sehingga berdampak pada kedaulatan negara Indonesia, siapa saja dapat melakukannya tanpa dipengaruhi ruang dan waktu, sekaligus identitasnya tidak dapat diketahui dengan mudah. Sehingga Indonesia dengan instrumen hukum nasional dan hukum internasional perlu bersiap untuk menghadapi ancaman *Cyber Espionage.*

Penegakan hukum pada era 5.0 perlu memerhatikan keadilan sebagai landasan pengambilan keputusan, imparsialitas, independensi, profesionalisme lembaga penegak hukum dalam memutus perkara, dan melibatkan partisipasi publik. Hal ini karena era 5.0 menempatkan manusia sebagai pusat aktivitas yang menyeimbangkan antara keuntungan ekonomi dengan solusi-solusi masyarakat. Hal ini dapat dicapai melalui penggunaan integrasi yang tinggi, baik *cyberspace* maupun *physical space*.

Berdasarkan permasalahan di atas, ditemukan rumusan masalah yang akan dibahas dalam artikel ini, (1.) Bagaimana Cyber Espionage Menjadi Ancaman Pertahanan Dan Keamanan Pada Era Society 5.0?; (2.) Bagaimana Instrumen Hukum Internasional dalam Menghadapi Ancaman Cyber Espionage?; (3.) Bagaimana Kesiapan Indonesia Dalam Penegakan Hukum Terhadap Cyber Espionage Pada Era Society 5.0?

2. Metode Penelitian

Penelitian ini menggunakan metode yuridis normatif yang menggunakan bahan-bahan kepustakaan sebagai sumbernya dan melalui tiga pendekatan yaitu pendekatan konseptual, pendekatan perbandingan, dan pendekatan perundang-undangan. Bahan sumber penelitian ini terdiri dari bahan hukum primer dan sekunder. Bahan hukum primer adalah bahan hukum yang terdiri dari peraturan perundang-undangan dan putusan-putusan hakim yang dijadikan sebagai yurisprudensi. Bahan hukum sekunder adalah bahan hukum berupa publikasi tentang hukum seperti buku literatur, jurnal hukum, dan penelitian hukum terkait dengan penelitian yang diambil.

3. Hasil Penelitian dan Pembahasan

3.1. *Cyber Espionage* sebagai Ancaman Pertahanan dan Keamanan Pada Era Society 5.0

Cyber Espionage meruapakan perkembang dari metode spionase secara konvensional. Tindakan spionase secara konvensional lazim dilakukan sejak masa perang. Pengertian spionase dari Kamus Besar Bahasa Indonesia (KBBI) adalah penyelidikan secara diam-diam terhadap data ekonomi dan militer negara lain; segala hal yang berkaitan dengan spion; tindakan mata-mata: penangkapan dua orang wakil atase militer di atas dugaan. Teknik spionase sering digunakan dalam

Jurnal Yustika
Vol. 25 No. 01, Jul 2022

sebagai suatu strategi untuk memenangkan peperangan. Hal ini sejalan dengan pendapat ahli strategi perang dari Cina, Sun Tzu yang mengatakan bahwa puncak dari kemenangan adalah memenangkan peperangan tanpa adanya pertempuran.(Purna Nugraha, 2017) Penggunaan spionase sebagai tipu daya perang dan sebagai upaya memperoleh informasi mengenai musuh diperbolehkan apabila kita merujuk pada Pasal 24 Konveni Den Haag. Dilanjut pada Pasal 25 dan Pasal 29 bahwa seorang yang mencari informasi rahasia di daerah operasi dilakukan dengan diam-diam dilarang untuk menyerang atau mengebom kota-kota, pemukiman dan bangunan vital. Salah satu konvensi yang mengatur kegiatan spionase adalah *Hague Convention* IV 1907 yang mengatur kegiatan spionase dalam Pasal 29, dapat dipahami bahwa seorang tentara dapat dikatakan melakukan spionase ketika memasuki wilayah musuh dengan penyamaran dan tujuan mereka ialah mencari informasi musuh dan menyampaikan informasinya kepada pengirimnya.

Pada masa pasca perang atau masa damai, spionase masih sering digunakan untuk kepentingan nasional dan menyusun strategi pertahanan nasional suatu negara. Tindakan spionase ini masih dilakukan dengan mengirim seorang intelijen, memanfaatkan seorang diplomatik ke negara sasaran, bahkan meretas sistem negara. Negara yang pernah menjadi sasaran spionase adalah Prancis dan Jerman yang diaktori oleh Amerika Serikat. Beberapa kasus spionase di masa damai ini adalah kasus seorang intelijen Brazil yang bernama Abin, dia melakukan spionase dalam kurun waktu tahun 2003 sampai tahun 2004 serta kasus Ryan Fogle, seorang diplomat Amerika serikat yang dipulangkan oleh Pemerintah Rusia setelah diketahui melakukan spionase. (Pratiwi & Correia, 2020) Indonesia juga pernah menjadi korban spionase pada tahun 1982, dimana Kolonel Sergei Egorof yang kala itu bertugas sebagai asisten pertahanan kedutaan Soviet di Jakarta tertangkap pihak yang berwenang karena terlibat dalam jual beli dokumen rahasia Indonesia yakni peta Hidrografi Laut Banda.(Sudiro & Marton, 2017)

Pesatnya perkembangan teknologi komputer dan internet dimanfaatkan sebagai media spionase. Tallin Manual 2.0 yang merupakan panduan spionase siber atau *Cyber Espionage* untuk pemegang kebijak dan ahli hukum internasional menjelaskan bahwa tindakan ini dilakukan dengan sembunyi-sembunyi dan menggunakan kemampuan siber untuk mengumpulkan informasi.(Michael, 2013) Pemanfaatan siber sebagai media *Cyber Espionage*, menjadikan kejahatan ini termasuk dalam *cyber crime*. Definisi kejahatan siber dijelaskan oleh *Organization for Economic Cooperation Development* (OECD) adalah setiap perbuatan tidak etis atau tidak sah berupa pengaksesan data atau transmisi data.(Sinaga, 2010) Bentuk dari *cyber crime* diklasifikasikan oleh Dikdik M. Arief dan Elisatris Gultom berupa :(Dikdik & Gultom, 2005)

1. *Unauthorized Access to Computer System and Service;*
2. *Data forgery;*
3. *Illegal contents;*
4. *Cyber Espionage;*
5. *Cyber Sabotage and Exstortion;*
6. *Infringement of privacy*
7. *Offense Against Intellectual property;*

Disebut secara khusus *Cyber Espionage* adalah kejahatan siber. Pada prakteknya, *Cyber Espionage* dilakukan perorangan atau kelompok atas permintaan pemerintah yang ditujukan untuk mencuri informasi rahasia dengan menggungkan Teknik peretasan (hacking) dan penyebaran virus kepada komputer atau sistem internet

suatu lembaga swasta atau negara. Sebagai contoh adalah Cozy Bear yang merupakan kelompok peretas (hacker) yang berasosiasi dengan agen intelijen negara Rusia. Kelompok yang berfokus pada sektor militer, pemerintahan, energi, diplomatik dan telekomunikasi ini telah melakukan *Cyber Espionage* terhadap pihak komersial dan pemerintah di Jerman, Uzbekistan, Kora Selatan, dan Amerika Serikat, termasuk Departemen Luar Negeri dan Gedung Putih pada tahun 2014.(Baumgartner, 2015) Pada Juli 2020, Cozy Bear dituduh oleh lembaga keamanan siber *National Cyber. Security Centre* (NCSC), *National Security Agency* (NSA), dan *Cyber Security Education* (CSE) telah mencoba mencuri data tentang vaksin dan perawatan untuk virus Covid-19 yang sedang dikembangkan di Inggris, Amerika Serikat, dan Kanada.(HSToday, 2020)

Meskipun korban dari kejahatan *Cyber Espionage* ini mendominasi negara maju dan memiliki keamanan digital, bukan berarti negara berkembang seperti Indonesia tidak akan menjadi sasaran *Cyber Espionage*. Kaspersky Lab yang merupakan perusahaan antivirus mengungkapkan bahwa di Asia Tenggara ada kelompok yang diduga menjalankan *Cyber Espionage*. Negara Indonesia termasuk pemerintahan, departemen pertahanan, departemen intelijen, institusi diplomatik dan perusahaan telekomunikasi menjadi sasaran kelompok APT ini. Metode penyerangan *Cyber Espionage* ini melalui serangan virus yang mencuri email atau dokumen yang kemudian hasil tersebut dikirim ke pengirimnya.(Baezner, 2018) Faktor utama yang menjadikan ancaman dunia maya ialah geopolitik dan ekonomi dan Indonesia salah satu negara di Asia Tenggara yang beraneka ragam etnis, pandangan politik dan pembangunan ekonomi.

3.2. Instrumen Hukum Internasional dalam Menghadapi Ancaman *Cyber Espionage*

Cyber Espionage masih menjadi pembahasan yang baru dalam hukum internasional, sehingga belum ada aturan khusus yang mengatur mengenai kejahatan siber ini.(D. Wallace, 2019) Dalam melakukan kejahatan ini, hacker memanfaatkan *cyber space* dalam mengakses data dan menyalin datanya. *Cyber space* yang mencakup jaringan komputer dan internet dapat menghilangkan yurisdiksi negara dalam penegakan hukum apabila dilakukan dari negara yang berbeda. Mengenai hal ini, dalam penegakan hukum dengan kondisi seperti ini diperlukannya instrumen hukum yang dapat mengakomodir dari hukum-hukum yang berada di negara lain. Prof. Rebecca Wallace mendefinisikan bahwa aturan yang dapat mengatur perilaku antarnegara termasuk masyarakat dan organsiasi internasional ialah hukum internasional.(R. Wallace, 1993)

Pada saat ini, hukum internasional berkembang menjadi kebijakan luar negeri yang menjadi akar hukum dan legitimasinya terletak pada dinamika yang dialami oleh-negara-negara. Sumber hukum internasional yang menjadi pertimbangan pengadilan tertuang pada Pasal 38 ayat (1) Statuta Mahkamah Internasional yakni:

1. Traktat-traktat internasional yang diakui oleh negara peserta dalam traktat tersebut;
2. Kebiasan internasional, termasuk *opinio juris* yang telah diakui oleh masyarakat olehinternasional;
3. Prinsip-prinsip umum hukum;
4. Keputusan-keputusan pengadilan dan doktrin para sarjana yang terkemuka dari berbagai negara dijadikan sumber.

Berdasarkan pasal tersebut, perbuatan *Cyber Espionage* akan diuji melalui sumber hukum internasional. Pengujian dimulai dari traktat sampai dengan doktrin para sarjana yang dapat berimplikasi terhadap *Cyber Espionage*.

Pertama, adanya kekosongan hukum yang mengatur *Cyber Espionage* secara khusus sehingga negara-negara telah mengatur tindakan *Cyber Espionage* ke dalam hukum

Jurnal Yustika
Vol. 25 No. 01, Jul 2022

nasionalnya. (Michael, 2013) Meski demikian, terdapat instrumen hukum yang membahas mengenai tindakan kejahatan spionase, khususnya pada masa perang. Spionase dalam peperangan sering digunakan sebagai suatu strategi untuk memenangkan peperangan. Pasal 24 Konvensi Den Haag menyatakan bahwa diperkenankan menggunakan tipu daya perang dan penggunaan cara-cara untuk mendapatkan informasi yang berkaitan dengan musuh. Niccolo Machiavelli, seorang diplomat dan politikus Italia berpendapat bahwa melakukan tipu daya dalam peperangan dianggap lumrah dan setiap kawan adalah musuh, sehingga orang tidak segan untuk menipu dan kekerasan dengan sesamanya. (Machiavelli, 2015) Mengenai status agen spionase yang tertangkap, diatur dalam pasal 30 dan 31 Konvensi Den Haag, yakni agen spionase yang tertangkap musuh ketika menjalankan tugasnya tidak dapat dihukum tanpa adanya putusan pengadilan dan agen spionase yang telah kembali pada pasukannya lalu ditangkap oleh musuh, maka diperlakukan sebagai penjahat perang sehingga tidak bertanggungjawab atas tindakan spionase sebelumnya.

Kemudian terdapat *Vienna Convention* 1961 yang melarang tindakan spionase dalam menjalin hubungan diplomatik. Pejabat diplomat yang mewakili negara pengirim menjalankan tugas sesuai dengan perjanjian yang telah disetujui oleh negara penerima. Tugas diplomat pada umumnya ialah mewakili negara pengirim, mendapatkan informasi, memajukan dan mempertahankan kepentingan nasional, dan pengambilan keputusan. Artikel 3 (1) *Vienna Convention* 1961 menyebutkan "*Ascertaining, by all lawfull means, conditions and developments in the receiving state and reporting thereon to the government of the sending state*" bahwa pejabat diplomat dapat melaporkan segala perkembangan dan kondisi Negara penerima kepada Negara pengirim dengan cara yang sah. Namun, pencarian informasi dengan spionase tidak dibenarkan dalam hukum internasional karena dianggap dapat mengganggu kedaulatan negara penerima dan hubungan diplomatik antara negara pengirim dan penerima. Tertuang dalam Resolusi Majelis Umum Perserikatan Bangsa-Bangsa (PBB) tentang *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations* No. 2625 Tahun 1970, menegaskan bahwa setiap negara yang melakukan hubungan kerjasama dengan negara lain harus didasari dengan itikad baik .

Selain itu, terdapat aturan yang mengatur kejahatan siber ialah *Convention on Cybercrime.* Konvensi yang telah disahkan di Budapest, telah diratifikasi negara-negara mulai 23 November 2001. Konvensi ini mengharmonisasi hukum nasional negara, secara materil dan formil, termasuk organisasi internasional yang menandatangani konvensi ini. *Convention on Cybercrime* berisi ketentuan yang mengatur kewenangan masin-masing negara anggota untuk mengadopsi ketentuan-ketentuan dalam konvensi ini ke dalam hukum nasionalnya, baik berupa pedoman atau sanksi yang dapat diberikan atas pengaksesan informasi secara tidak sah. Dalam konteks pedoman atau sanksi, konvensi ini mengatur proses ekstradisi dan bantuan hukum yang dapat diperoleh pelaku. *European Convention on Cybercrime* (ECC) yang merupakan aturan mengenai kejahatan siber yang mengikat negara-negara Uni Eropa. Konvensi ini mencakup perbuatan mengakses data secara tidak sah yang merupakan metode dalam *Cyber Espionage*.

Kedua, belum ada kebiasaan internasional dan *opinion juris* sebagai legalitas tindakan *Cyber Espionage* yang dapat dibenarkan oleh hukum internasional. Pada dasarnya, hanya kebiasaan yang diterima sebagai hukum oleh masyarakat

internasional dan tidak setiap kebiasaan merupakan sumber hukum internasional. Kebiasaan internasonal harus memenuihi dua unsur yaitu, praktek umum negara-negara dan praktek tersebut diterima oleh negara-negara sebagai hukum. Sebagai bukti bahwa kebaisaan hukum internasional berlaku, negara-negara harus menaati kewajiban yang mengikat negara bersangkutan (Schwarzenberger, 1967)

Salah satu penyelesaian kasus internasional yang menjadikan kebiasaan internasional menjadi sumber hukumnya adalah kasus *Anglo-Norwegian Fisheries* yang telah diselesaikan melalui Mahkamah Internasional. Sengketa antara Norwegia dan Inggris ini adalah perbedaan penetapan garis pangkal laut di antara kedua negara. Inggris berpendapat penetapan garis pangkal oleh Norwegia yang ditarik dari selat menyalahi hukum internasional, karena penarikan tersebut seharusnya dari daratan yang kering dan Inggris merasa dirugikan karena Norwegia dapat mengeksploitasi wilayah selat tersebut yang kaya akan sumber daya perikanan. Sedangkan Norwegia, menganggap bahwa penetapan garis pangkal laut tersebut merupakan hasil sesuai dengan dekrit raja, sehingga telah sesuai dengan hukum internasional. Kemudian, menurut Norwegia penetapan pangkal laut sudah menjadi hukum kebiasaan di Norwegia sejak abad XVII dan menjadi sumber mata pencaharian nelayan-nelayan norwegia. Selain itu, selat yang dimaksud masih memiliki hubungan teritorial dengan darat Norwegia yang menjadikannya wilayah kedaulatan dan kondisi geografis Norwegia yang berupa pegunungan dan pantai yang berkarang mendukung anggapan bahwa selat tersebut termasuk sebagi daratan. Berdasarkan jawaban Norwegia atas gugatan Inggris mengenai penetapan garis pangkal laut, Mahkamah Internasional memenangkan Norwegia.(Green, 1952)

Ketiga, Tindakan *Cyber Espionage* melanggar tiga asas hukum internasional yaitu kedaulatan negara, non-internvensi dan pelaku non-negara atau *non-state actor*.

1. Kedaulatan Negara

Max Huber mendefinisikan kedaulatan sebagai suatu kemerdekaan suatu negara dalam hubungan internasional, sehingga negara tersebut berhak menjalankan pemerintahannya dengan mengesampingkan negara lain.(Delerue, 2020) *United Nations Group of Governmental Experts on Development* (UN GGE 2013) menyatakan bahwa kedaulatan negara dan norma serta prinsip internasional menyesuaikan dari keberlakuan kedaulatan suatu negara terkait tindakan teknologi informasi komunikasi. Berdasarkan pernyataan dari UN GGE tersebut dapat disimpulkan bahwa asas kedaulatan negara dan norma internasional juga berlaku terhadap ruang siber.

Metode pelaksanaan *Cyber Espionage* yang tercakup dalam operasi ruang siber diklasifikasikan menjadi dua. Pertama, *Cyber Espionage* yang dioperasikan dari luar wilayah kedaulatan negara sasaran atau *remote-Cyber Espionage*. Pakar hukum internasional, seperti Prof. Michael Schmitt menyatakan bahwa tindakan tersebut bukan suatu pelanggaran atas kedaulatan negara, tetapi metode dan pelaksanaan tersebut dapat menjadikan tindakan itu sebagai pelanggaran suatu kedaulatan negara. (Michael, 2017) Kedua, tindakan *Cyber Espionage* yang dapat berdampak terhadap kedaulatan negara adalah ketika tindakan tersebut dilakukan di dalam wilayah yurisdiksi negara sasaran. Keberadaaan agen di dalam wilayah yurisdiksi negara lain dan menjalankan operasi spionase secara diam-diam serta dengan justifikasi yang jelas,

menjadikan agen tersebut sedang melanggar kedaulatan negara tersebut. (D. Wallace, 2019) Sehingga, tindakan *Cyber Espionage* dapat dikatakan melanggar asas kedaulatan negara dilihat dari metode pelaksanaannya dan pembuktiannya di depan hukum.

2. Non-intervensi

Non-intervensi merupakan suatu prinsip di mana negara tidak diperbolehkan untuk ikut campur dalam permasalahan negara lain, seperti penentuan sistem politik, masalah sosial, dan budaya kebijakan luar negeri suatu negara. (Jamnejad, 2009) Prinsip ini dilandasi dengan Pasal 2 Paragraf 7, Pasal 42, Pasal 51 *United Nations Charter* dan *United Nations General Assembly Resolution* 2625 XXV. Deklarasi tersebut menyatakan bahwa segala tindakan intervensi yang dapat merugikan negara sasaran merupakan suatu pelanggaran hukum internasional.

Pengumpulan data dan informasi dari negara lain yang dilakukan dalam *Cyber Espionage*, dapat dikatakan pelanggaran asas non intervensi ketika data yang terkumpul digunakan untuk melakukan persiapan atau rencana gabungan, maka seketika itu tindakan tersebut dapat dikatakan sebagai pelanggaran asas non intervensi ini.

3. Pelaku non negara

Pelaku yang melakukan peretasan terhadap negara lain atau perusahaan asing bukan sebuah tindakan spionase, tetapi diatur secara umum dalam hukum nasional. Namun, pelaku yang mengakses informasi rahasia negara lain atau bahkan meretasnya dengan instruksi pemerinta, maka terjadilah asas "*state responbility attributable to the state*" yakni negara bertanggungjawab terhadap segala perintahnya.(Kulesza, 2009)

Berdasarkan pengujian *Cyber Espionage* ke dalam sumber-sumber hukum internasional, dapat disimpulkan bahwa tindakan ini tidak diatur secara lugas tetapi dikualifikasikan sebagai pengaksesan data dan perolehan data secara tidak sah. Perolehan data dengan cara penyadapan data melanggar hak-hak individu yang berhak dilindungi data elektroniknya.

3.3. Kesiapan Indonesia Dalam Penegakan Hukum Terhadap Cyber Espionage Pada Era Society 5.0

Era *Society* 5.0 yang merupakan penyelesaian permasalahan dari pesatnya perkembangan teknologi yang dikhawatirkan akan mengurangi produktivitas manusia, juga dituntut harus bisa menegakan hukum yang lebih mengacu pada *human centric* dengan tujuan untuk menghormati hukum yang hidup di masyarakat (*living law*) dan penegakan hukum tidak semata terbatas pada norma perundang-undangan semata. Nilai-nilai *human centric* dapat berupa independensi, kebebasan lembaga penegak hukum dalam memutus perkara, profesionalisme aparat penegakan hukum, dan melibatkan partisipasi publik. Penegakan hukum termasuk norma dan nilai hukum yang melatarbelakangi norma tersebut harus diikuti dengan pemahaman para penegak hukum mengenai spirit hukum yang menjadi dasar peraturan hukum harus ditegakkan. (Muladi, 2002)

Penegakan hukum idealnya dilakukan menggunakan pendekatan sistem hukum. Sudikno Mertokusumo mendefinisikan sistem hukum sebagai suatu kesatuan yang terdiri dari unsur-unsur yang berinteraksi dan bekerja sama dalam mencapai tujuan kesatuan tersebut. (Mertokusumo, 1991) Dalam setiap sistem

hukum terdiri terdiri dari tiga subsistem yaitu substansi hukum (legal substance), struktur hukum (legal structure), dan budaya hukum (legal culture).(Friedman, 2001) Substansi hukum yang meliputi instrumen hukum Indonesia. Struktur hukum terdiri dari institusi penegak hukum termasuk kewenangan lembaga dan aparat hukum. Sedangkan budaya hukum berkaitan dengan perilaku masyarakat. Ketiga unsur ini memengaruhi keberhasilan penegakan hukum di suatu negara dan saling bersinergi satu dengan yang lain untuk mencapai tujuan penegakan hukum yaitu keadilan.

Dalam menguji kesiapan penegakan hukum Indonesia dan hukum Internasional terhadap *Cyber Espionage* bisa melalui prinsip manajemen organisasi dengan menggunakan pendekatan tiga subsistem hukum. Organisasi dalam hal ini pemerintah Indonesia dalam upaya menghadapi ancaman *Cyber Espionage*. Salah satu prinsip manajemen organisasi adalah *Planning, Organizing, Actuating,* dan *Controlling* (POAC) yang diperkenalkan oleh George R. Terry. (Terry, 1968) Prinsip POAC berisi tahapan dalam melaksanakan fungsi organisasi yang terdiri dari perencanaa, pengorganisasian, pengarahan, dan pengawasan.

1. *Planning*

Planning adalah sebuah tahapan seorang manajer untuk memutuskan visi misi, menetapkan pelaksanaan demi mencapai tujuan dengan membagi tanggung jawab untuk melaksanakan rencana tersebut kepada seseorang dan mengukur indikator keberhasilan dengan membandingkan tujuan. Penerapan prinsip *planning* dalam penegakan hukum dapat berupa mencari dan mengkaji pengaturan hukum nasional, termasuk hasil ratifikasi dari perjanjian internasional yang berkaitan dengan *Cyber Espionage* dan Menyusun rencana dalam penegakan hukumnya.

Dalam Kitab Undang-Undang Hukum Pidana (KUHP) di Indonesia, telah terdapat aturan mengenai kejahatan yang memanfaatkan jaringan komputer atau *cybercrime*. Ketentuan-ketentuan dalam KUHP yang berkaitan dengan *cyber crime* masih bersifat konvensional. Namun, *cyber crime* dapat diklasifikasi berdasarkan tingkat intensitas terjadinya kasus tersebut, yaitu:

a) Ketentuan tentang delik pencurian.
b) Ketentuan tentang tindakan memasuki atau melintasi wilayah orang lain.
c) Ketentuan tentang pembocoran rahasia.

Aturan dalam KUHP yang mengatur klasifikasi kasus tersebut dapat ditemukan dalam pasal 362 KUHP, 167 KUHP, 112-113 KUHP. Dalam menggunakan pasal tersebut, maka harus melalui pendekatan atau penafsiran hukum. Contoh penerapan penafsiran hukum adalah kasus pencurian aliran listrik. Yang dipermasalahkan dalam kasus ini adalah, apakah aliran listrik dapat ditafsirkan sebagai "barang" dan apakah dapat dikatakan tindakan tersebut sebagai "mengambil". Majelis Kehakiman Belanda telah memutuskan bahwa alitan listirk termasuk dalam barang dan dengan demikian terjadilah tindakan pengambilan sesuai yang diatur dalam Pasal 362 KUHP. Hal yang menjadi pertimbangan majelis kehakiman tersebut, bahwa maksud dari Pasal 362 adalah upaya perlindungan terhadap harta orang lain (Hoge Raad tabnggal 23 Mei 1921, W 10726, NJ 1921. 564).

Kemudian, mengenai ketentuan tentang memasuki atau melintasi wilayah orang lain. Dalam pasal 167 KUHP disebutkan bahwa upaya memasuki rumah,

Jurnal Yustika
Vol. 25 No. 01, Jul 2022

ruangan atau pekarangan tertutup, dengan cara yang tidak dibenarkan oleh nilai-nilai norma dan memberikan ancaman kepada pemilik rumah diancam pidana paling lama sembilan bulan dan dapat ditambah apabila diikuti dengan ancaman atau adanya kerja sama dalam melakukan aksinya. Apabila dikaitkan dengan *Cyber Espionage*, tempat yang menjadi kejahatan tersebut ialah dunia maya. Oleh karena itu, apabila melakukan penafsiran hukum terhadap pasal tersebut maka yang diarikan adalah tindakan atau perbuatan masuk melawan hukumnya.

Ketentuan lain yang berkaitan dengan tindak *Cyber Espionage* adalah perbuatan tersebut menjadikan bocornya data terutama data yang harus rahasia, maka ketentuan yang dapat diterapkan adalah Pasal 112, Pasal 113, dan Pasal 114 KUHP. Dimulai ancaman pidana paling lama satu tahun yaitu ketika seseorang lalai dalam menjalankan tugasnya sehingga surat atau benda rahasia dapat diketahui oleh pihak yang tidak berhak mengetahui sampai dengan ancaman pidana yang paling berat adalah ketika seseorang dengan sengaja memberikan informasi rahasia negara kepada negara lain diancam pidana penjara paling lama tujuh tahun.

Selain Kitab Undang-Undang Hukum Pidana, terdapat ketentuan lain yang berkaitan dengan *Cyber Espionage* yakni Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (UU Telkom). Undang-Undang ini dibentuk agar menjadi payung hukum bagi para aparat penegak hukum untuk menangkap dan menjerat pelaku kejahatan ini dibanding hanya mengandalkan KUHP sebagai sumber hukum dalam penyelesaian pelanggaran tindak pidana ini.

Dalam UU ITE terdapat Pasal 30 Ayat (2) yang mengatur ketentuan *Cyber Espionage* yang menyatakan bahwa seseorang yang sengaja mengakses komputer atau sistem elektronik dengan cara yang tidak sah untuk memperoleh informasi elektronik atau dokumen elektronik dikenai sanksi pidana penjara paling lama 7 (tujuh) tahun dan/ atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah). Ketentuan subjek dalam tindakan *Cyber Espionage* juga ditentukan dalam undang-undang ini, yang terdiri dari perorangan dan korporasi. Mengenai tindakan *Cyber Espionage* yang dilakukan oleh korporasi maka berakibat pada pidana yang dijatuhkan, hal ini tercantum pada pasal 52 Ayat (4) yang dapat dipahami ketika korporasi melakukan tindak *Cyber Espionage* maka dipidana dengan pidana pokok ditambah dua per tiga. Mengenai alat bukti dalam tindak pidana siber ini ditambahkan alat bukti berupa informasi atau dokumen elektronik.

Ketentuan yang mengatur tentang tindak pidana kejahatan di bidang telekomunikasi diatur dalam UU Telkom. Dalam Pasal 22 dan pasal 50 yang dapat dimaknai bahwa setiap orang dilarang mengakses atau memanipulasi jaringan computer atau telekomuikasi dan penyedia jasa. Pasal ini tidak secara tertulis menyampaikan bahwa *Cyber Espionage* masuk dalam rumusan pasalnya, tetapi mengatur perbuatan peretas yang melakukan spionase untuk mengintai atau menyadap data. Untuk memperkuat penegakan hukum terhadap aksi *Cyber Espionage*, Indonesia turut serta dalam Resolusi Anti Spionase PBB tanggal 5 November 2013.

2. *Organizing*

Organizing adalah seluruh proses pengelompokkan orang, alat, tugas, serta wewenang dan tanggung jawab untuk menciptakan organisasi yang dapat digerakkan sebagai suatu kesatuan dalam rangka pencapaian tujuan yang telah ditentukan. Penerapan tahap ini ialah memastikan sumber daya untuk menjalankan

rencana dan pembagian tugas yang spesifik, kepada instansi dan aparat penegak hukum.

Indonesia memiliki beberapa institusi yang berkaitan dengan ancaman *Cyber Espionage*, salah satunya adalah Kepolisian Negara Republik Indonesia (Polri). Polri merupakan komponen negara yang berperan untuk memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, serta memberikan perlindungan, pengayoman serta pelayanan kepada masyarakat demi terjaganya keamanan dalam negeri. Kekuatan militer yakni Tentara Nasional Indonesia (TNI) dan lembaga intelijen yakni Badan Intelijen Negara (BIN) dapat menghadapi ancaman *Cyber Espionage*. Badan Intelijen Negara (BIN) sebagai lembaga intelijen negara bertugas untuk mendeteksi secaara dini ancaman yang dapat mengganggu stabilitas pertahanan dan keamaann negara dan dalam hal ini berkoordinasi dengan TNI sebagai upaya mempertahankan negara melalui penjagaan ketat batas0batas geografis darisernangan negara menggunakan kekuatan militernya.

Selain itu, Indonesia telah menjadi anggota *International Telecommunication Union* (ITU) sejak 1949. Hal ini berdasarkan Keputusan Presiden Nomor 10 Tahun 1969 terkait Konvensi *International Telecommunication Union* di Montreux pada 1965. ITU merupakan organisasi internasional yang bergerak dalam bidang telekomunikasi dan berkaitan dengan Persatuan Bangsa-Bangsa (PBB).

3. *Actuating*

Actuating dalam prinsip manajemen organisasi merupakan upaya untuk merealisasikan rencana dengan mengarahkan dan memotivasi setiap karyawan sesuai dengan peran, tugas dan tanggung jawab. Penerapan prinsip *actuating* dalam penegakan hukum dapat ialah pemerintah mengarahkan instansi dan aparat penegak hukum untuk melaksanakan penegakan sesuai dengan hukum yang berlaku.

Landasan yang menjadikan Polri diharapkan dapat memberikan pengayoman dan perlindungan kepada masyarakat berkaitan dengan *Cyber Espionage* adalah Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia. Keberadaan militer dalam komponen pertahanan dan keamanan di Indonesia dilandasi dengan Pasal 3 Undang-Undang Nomor 34 Tahun 2004 Tentang Tentara Nasional Indonesia (TNI) yang menyatakan bahwa TNI berada di bawah perintah presiden dalam pengerahan kekuatan militer.

BIN memliki landasan hukum berupa Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara. Dalam pasal 4 disebutkan BIN berperan untuk melakukan upaya deteksi dan peringatan dini dalam mencegah, menangkal dan menanggulangi hakikat ancaman yang mungkin akan timbul dan membahayakan kepentingan dan keamanan nasional. Mengenai TNI yang juga berkoordinasi dengan BIN untuk memaksimalkan pertahanan dan keamanan negara disebutkan dalam Pasal 9. Kemudian, ITU dapat bekerja sama dengan Polri, TNI, ataupun BIN sebagai fasilitator dalam pembangunan keamanan untuk menghadapi ancaman siber, hal ini berdasarkan hasil di WSIS (*World Summit of Information Society*) tahun 2013. (International Telecomunication Union (ITU), 2015)

4. *Controlling*

Controlling merupakan tahap akhir dari setiap pelaksanaan rencana yang memastikan bahwa setiap tugas telah berjalan sesuai rencana dan menentukan rencana selanjutnya setelah melihat hasil dari pelaksanaan. Upaya Polri, TNI, BIN, dan ITU dalam menegakkan hukum terhadap Cyber Espionage perlu diawasi oleh

masing-masing satuan fungsi pengawas dari setiap Lembaga seperti Inspektorat Pengawasan Umum Polri, Inspektorat Jenderal TNI, Inspektorat Utama BIN, dan untuk Lembaga ITU dapat dilakukan pengawasan oleh PBB ataupun setiap negara anggota.

Dengan demikian, Indonensia dapat melakukan penegakan hukum terhadap *Cyber Espionage* dengan menggunakan perundang-undangan yang masih berlaku dan menjalankan institusi Polri, TNI, BIN serta mengajak kerja sama ITU.

4. Kesimpulan

Berdasarkan pembahasan di atas, maka dapat disimpulkan sebagai berikut, bahwa *Cyber Espionage* merupakan kejahatan siber yang mengancam stabilitas pertahanan dan keamanan negara-negara di dunia. Pada Era *Society* 5.0 tindak kejahatan ini menjadi sebuah celah bagi pelaku untuk menjalankan aksinya, terutama ke negara-negara yang memiliki keamanan digital yang rendah dan mengalami kekosongan hukum mengenai kegiatan *Cyber Espionage* pada masa damai. Dengan demikian, upaya preventif yang dapat dilakukan oleh setiap negara dalam menghadapi tindakan *Cyber Espionage* terhadap negaranya adalah meningkatkan keamanan digital dan membentuk instrumen hukum yang membahas mengenai kegiatan *Cyber Espionage* dan sanksinya secara khusus.

Kemudian, belum adanya instrumen hukum internasional yang mengatur secara khusus mengenai *Cyber Espionage*. Instrumen hukum yang ada saat ini hanya mencakup tindak kejahatan siber, spionase dalam masa perang dan damai. Mengingat tindakan ini melanggar asas kedaulatan negara, non-intervensi dan pelaku non-negara, maka diperlukan instrumen hukum internasional yang mengatur *Cyber Espionage*. Dengan demikian, negara-negara dapat meratifikasi instrumen tersebut ke dalam hukum nasionalnya.

Terakhir, Kesiapan Indonesia dalam penegakan hukum terhadap *Cyber Espionage* melalui metode manajemen organisasi POAC dan pendekatan tiga subsistem hukum dapat menggunakan perundang-undangan dan instansi yang telah ada. Namun, akan lebih baik jika Indonesia memiliki perundang-perundangan yang mengatur mengenai *Cyber Espionage* secara khusus agar tidak terjadi kekosongan hukum.

Daftar Referensi

Buku:

Delerue, F. (2020). Cambridge Studies in International and Comparative Law. In *Cyber Operations and International Law*. Cambridge University Press.

Dikdik, & Gultom, E. (2005). *Cyber Law: Aspek Hukum Teknologi Informasi*. Refika Aditama.

Friedman, L. (2001). *Hukum Amerika: Sebuah Pengantar* (diterjemahkan W. Basuki). Tatanusa.

Haqqi, H., & Wijayati, H. (2019). *Revolusi Industri 4.0 di Tengah Society 5.0: Sebuah Integrasi Ruang, Terobosan Teknologi, dan Transformasi Kehidupan di Era Disruptif*. Anak Hebat Indonesia.

Machiavelli, N. (2015). *The Art of war* (diterjemahkan E. S. Alkhatab & T. Setiawan). Narasi.

Mertokusumo, S. (1991). *Mengenal Hukum*. Liberty.

Michael, S. (2013). *Tallin Manual 2.0 International Applicable to Cyberwarfare*. Cambridge University Press.

Muladi. (2002). *Hak Asasi Manusia, Politik dan Sistem Peradilan Pidana*. Badan Penerbit Universitas Diponegoro.

Schwarzenberger, G. (1967). *A Manual of International Law* (Fifth Edition). Stevens and Sons Limited.

Sudiro, A., & Marton. (2017). The Suppression of Hijacking and Other Crimes Involving

Indonesian Aviation Activities. In *Indonesia, Aviation Laws and Regulations Applicable in* (p. 360). Rajagrafindo.

Sudiro, A., & Marton. (2017). The Suppression of Hijacking and Other Crimes Involving Indonesian Aviation Activities. In *Indonesia, Aviation Laws and Regulations Applicable in* (p. 360). Rajagrafindo.

Terry, G. (1968). *Principles of Management*. Richar D Erwin.

Wahid, A. (2005). *Kejahatan Mayantara (Cyber Crime)*. Refika Aditama.

Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

Wallace, D. (2019). Peeling Back the Onion of Cyber Espionage after Tallin 2.0. *Maryland Review*, *78*(2), 17.

Wallace, R. (1993). *Hukum Internasional* (B. Arumanadi (ed.)). IKIP Semarang Press.

Artikel Jurnal:

Baezner, M. (2018). *Hotspot Analysis: Use of cybertools in regional tensions in Southeast Asia*. *11*, 1–28.

Baker, C. (2003). Tolerance of International Espionage: A Functional Approach. *American University International Law Review*, 12.

Baumgartner, K. (2015). *The CozyDuke APT*. Securelist.

Green, L. (1952). The Anglo-Norwegian Fisheries Case, 1951 (I. C. J. Reports 1951, p. 116). *The Modern Law Review*, *15*(3), 373–377.

Jamnejad, M. (2009). The Principle of Non-Intervention. *Leiden Journal of International Law*, 2.

Kulesza, J. (2009). State Responsibility For Cyber-Attacks On International Peace and Security. *Polish Yearbook of International Law*, *XXIX*, 9.

Pratiwi, L. Y. E., & Correia, Z. F. M. (2020). HUKUM SIBER : PRAKTIK SPIONASE DALAM KEDAULATAN NEGARA DAN HUBUNGAN DIPLOMASI BERDASARKAN KETENTUAN HUKUM INTERNASIONAL. *Jurnal Pendidikan Kewarganegaraan Undiksha*, *8*(3), 206–218.

Purna Nugraha, A. (2017). Dukungan Indonesia Terhadap Resolusi Anti Spionase Perserikatan Bangsa-Bangsa. *Jurnal Hubungan Internasional*, 935.

Sinaga, O. (2010). Penanggulangan Kejahatan Internasional Cyber Crime di Indonesia. *Makalah Institut Pertanian Bogor*, 10.

Sudiarta, I. K. (2014). Pelanggaran Kedaulatan Negara Terkait Tindakan Spionase dalam Hubungan Diplomasi Internasional. *Kerthanegara*, *2*.

Haqqi, H., & Wijayati, H. (2019). *Revolusi Industri 4.0 di Tengah Society 5.0: Sebuah Integrasi Ruang, Terobosan Teknologi, dan Transformasi Kehidupan di Era Disruptif*. Anak Hebat Indonesia.

HSToday. (2020). *NSA Teams with NCSC, CSE, DHS CISA to Expose Russian Intelligence Services Targeting COVID-19 Researchers*. Homeland Security Today.

Jamnejad, M. (2009). The Principle of Non-Intervention. *Leiden Journal of International Law*, 2.

Kulesza, J. (2009). State Responsibility For Cyber-Attacks On International Peace and Security. *Polish Yearbook of International Law*, *XXIX*, 9.

Machiavelli, N. (2015). *The Art of war* (E. S. Alkhatab & T. Setiawan (eds.); 1st ed.). Narasi.

Mertokusumo, S. (1991). *Mengenal Hukum*. Liberty.

Michael, S. (2013). *Tallin Manual 2.0 International Applicable to Cyberwarfare*. Cambridge University Press.

Muladi. (2002). *Hak Asasi Manusia, Politik dan Sistem Peradilan Pidana*. Badan Penerbit Universitas Diponegoro.

Pratiwi, L. Y. E., & Correia, Z. F. M. (2020). HUKUM SIBER : PRAKTIK SPIONASE DALAM KEDAULATAN NEGARA DAN HUBUNGAN DIPLOMASI BERDASARKAN KETENTUAN HUKUM INTERNASIONAL. *Jurnal Pendidikan Kewarganegaraan Undiksha*, *8*(3), 206–218.

Purna Nugraha, A. (2017). Dukungan Indonesia Terhadap Resolusi Anti Spionase Perserikatan Bangsa-Bangsa. *Jurnal Hubungan Internasional*, 935.

Schwarzenberger, G. (1967). *A Manual of International Law* (Fifth Edit). Stevens and Sons Limited.

Sinaga, O. (2010). Penanggulangan Kejahatan Internasional Cyber Crime di Indonesia. *Makalah Institut Pertanian Bogor*, 10.

Sudiarta, I. K. (2014). Pelanggaran Kedaulatan Negara Terkait Tindakan Spionase dalam Hubungan Diplomasi Internasional. *Kerthanegara*, *2*.

Haqqi, H., & Wijayati, H. (2019). *Revolusi Industri 4.0 di Tengah Society 5.0: Sebuah Integrasi Ruang, Terobosan Teknologi, dan Transformasi Kehidupan di Era Disruptif*. Anak Hebat Indonesia.

HSToday. (2020). *NSA Teams with NCSC, CSE, DHS CISA to Expose Russian Intelligence Services Targeting COVID-19 Researchers*. Homeland Security Today.

Jamnejad, M. (2009). The Principle of Non-Intervention. *Leiden Journal of International Law*, 2.

Kulesza, J. (2009). State Responsibility For Cyber-Attacks On International Peace and Security. *Polish Yearbook of International Law*, *XXIX*, 9.

Machiavelli, N. (2015). *The Art of war* (E. S. Alkhatab & T. Setiawan (eds.); 1st ed.). Narasi.

Mertokusumo, S. (1991). *Mengenal Hukum*. Liberty.

Michael, S. (2013). *Tallin Manual 2.0 International Applicable to Cyberwarfare*. Cambridge University Press.

Muladi. (2002). *Hak Asasi Manusia, Politik dan Sistem Peradilan Pidana*. Badan Penerbit Universitas Diponegoro.

Pratiwi, L. Y. E., & Correia, Z. F. M. (2020). HUKUM SIBER : PRAKTIK SPIONASE DALAM KEDAULATAN NEGARA DAN HUBUNGAN DIPLOMASI BERDASARKAN KETENTUAN HUKUM INTERNASIONAL. *Jurnal Pendidikan Kewarganegaraan Undiksha*, *8*(3), 206–218.

Purna Nugraha, A. (2017). Dukungan Indonesia Terhadap Resolusi Anti Spionase Perserikatan Bangsa-Bangsa. *Jurnal Hubungan Internasional*, 935.

Schwarzenberger, G. (1967). *A Manual of International Law* (Fifth Edit). Stevens and Sons Limited.

Sinaga, O. (2010). Penanggulangan Kejahatan Internasional Cyber Crime di Indonesia. *Makalah Institut Pertanian Bogor*, 10.

Sudiarta, I. K. (2014). Pelanggaran Kedaulatan Negara Terkait Tindakan Spionase dalam Hubungan Diplomasi Internasional. *Kerthanegara*, *2*.

Artikel Internet:

Baezner, M. (2018). *Hotspot Analysis: Use of cybertools in regional tensions in Southeast Asia*. *11*, 1–28.

Baker, C. (2003). Tolerance of International Espionage: A Functional Approach. *American University International Law Review*, 12.

Baumgartner, K. (2015). *The CozyDuke APT*. Securelist.

Christiawan, R. (2021). *Tantangan Hukum Era GoTo*. Kontan. https://analisis.kontan.co.id/news/tantangan-hukum-era-goto-1

Delerue, F. (2020). Cambridge Studies in International and Comparative Law. In *Cyber Operations and International Law*. Cambridge University Press.

Dikdik, & Gultom, E. (2005). *Cyber Law: Aspek Hukum Teknologi Informasi*. Refika Aditama.

Friedman, L. (2001). *Hukum Amerika: Sebuah Pengantar* (W. Basuki (ed.); 2nd ed.). Tatanusa.

Green, L. (1952). The Anglo-Norwegian Fisheries Case, 1951 (I. C. J. Reports 1951, p. 116). *The Modern Law Review*, *15*(3), 373–377. https://www.jstor.org/stable/1091592

International Telecomunication Union (ITU). (2015). *Statistics confirm ICT revolution of the past 15 years*. ITU Releases 2015 ICT Figures. https://www.itu.int/net/pressoffice/press_releases/2015/17.aspx

Michael, S. (2017). *Respect for Sovereignty in Cyberspace*. Texas Law Review. https://texaslawreview.org/respect-sovereignty-cyberspace/

Syahputra, R. (2021). *Adaptasi Teknologi : Kunci Kemajuan Diri di Era Society 5.0*. Universitas Indonesia. https://www.ui.ac.id/adaptasi-teknologi-kunci-kemajuan-diri-di-era-society-5-0/