(2023), 1 (5): 178–191 Kultura 2985-5624
Jurnal Ilmu Hukum, Sosial, dan Humaniora

Penegakan Hukum dalam Era Society 5.0: Cyber Espionage dalam Sorotan Hukum Nasional dan Internasional

Sita Amelia Salsabilla[1)], Kenisha Andiani[2)], Asmak Ul Hosnah[3)].
Fakultas Hukum Universitas Pakuan, Jalan Pakuan No. 1 Bogor 16143, Indonesia [123]
Alamat e-mail : sitamelias8@gmail.com [1], kenishadiani@gmail.com [2],
asmak.hosnah@unpak.ac.id [3]

Correspondence
Email: No. Telp:
Submitted: 13 December 2023 Accepted: 22 December 2023 Published: 23 December 2023

ABSTRACT

The threat of Cyber Espionage, or cyber espionage, has evolved rapidly along with technological advancements in the Society 5.0 Era. In this paper, we discuss the evolution from conventional espionage to cyber espionage, and its impact on national defense and security. Cyber Espionage involves the use of cyber technology to steal confidential information, and is often classified as a cyber crime. This means that the existence and increasing threat of Cyber Espionage requires serious attention in the context of national policies and international cooperation. In the era of Society 5.0, data protection and cybersecurity are crucial to maintaining a country's sovereignty and security.

Keyword : Cyber Espionage, Spionase Siber, Kejahatan Siber, Society 5.0, Keamanan Siber.

ABSTRAK

Ancaman Cyber Espionage, atau spionase siber, telah berkembang pesat seiring dengan kemajuan teknologi dalam Era Society 5.0. Dalam tulisan ini, kami membahas evolusi dari spionase konvensional ke spionase siber, serta dampaknya terhadap pertahanan dan keamanan negara. Cyber Espionage melibatkan penggunaan teknologi siber untuk mencuri informasi rahasia, dan seringkali tergolong sebagai kejahatan siber. Artinya, keberadaan dan peningkatan ancaman Cyber Espionage memerlukan perhatian serius dalam konteks kebijakan nasional dan kerja sama internasional. Di era Society 5.0, perlindungan data dan keamanan siber menjadi sangat penting untuk menjaga kedaulatan dan keamanan suatu negara.

Kata kunci: Cyber Espionage, Spionase Siber, Kejahatan Siber, Society 5.0, Keamanan Siber.

Pendahuluan

Selama beberapa dekade terakhir, telah terjadi empat revolusi industri yang memberikan dampak besar terhadap masyarakat. Revolusi pertama terjadi pada tahun 1750, bertepatan dengan munculnya mesin uap yang mengubah wajah industri. Revolusi kedua terjadi sekitar tahun 1870 dengan penemuan alat-alat produksi massal yang mengguncang ekonomi dan masyarakat. Revolusi ketiga datang bersamaan dengan kemunculan komputer, membawa kemajuan teknologi yang tak terhentikan. Revolusi keempat, yang sedang berlangsung, ditandai oleh perkembangan jaringan siber dan kecerdasan buatan, menghadirkan era di mana mesin canggih bersaing dengan manusia (Haqqi & Wijayati, 2019).

Namun, saat ini, kita melihat pergeseran menuju revolusi yang lebih besar lagi, yakni transisi dari Era Revolusi Industri 4.0 ke Era Society 5.0. Dalam pidatonya di acara CeBUT tahun 2017, Shinzo Abe, Perdana Menteri Jepang, secara visioner memperkenalkan gagasan Society 5.0 (Christiawan, 2021). Society 5.0 merupakan perubahan fundamental dalam cara kita berinteraksi dengan teknologi, lingkungan, dan satu sama lain.

Era Society 5.0 bermaksud mengatasi berbagai tantangan yang muncul dalam konteks Revolusi Industri. Munculnya Era 4.0 melibatkan integrasi manusia serta mesin, sehingga menciptakan terjalinnya hubungan sinergis yang saling menguntungkan. Sebagai contoh,

layanan e-commerce serta layanan ojek online adalah contoh nyata bagaimana manusia dan teknologi dapat berjalan beriringan. Kedua inovasi ini tidak hanya memberikan lapangan kerja, tetapi juga memudahkan kehidupan sehari-hari bagi masyarakat. Peralihan dari Era Industri 4.0 ke Era Society 5.0 dipercepat oleh pandemi COVID-19, yang mendorong penerapan teknologi untuk menjaga jarak sosial dan mengatasi tantangan baru. Masyarakat mulai mengandalkan teknologi untuk memecahkan masalah yang kompleks, kritis, dan kreatif, mengejar inovasi demi bertahan (Syahputra, 2021).

Era Society 5.0 membawa perubahan besar bagi Indonesia. Digitalisasi telah memberikan dampak positif dan negatif bagi negara ini, terutama mengingat perkembangan teknologi yang pesat dan bonus demografi yang akan datang pada tahun 2030-2035. Dampak positifnya adalah kemampuan masyarakat dan pemerintah Indonesia untuk beradaptasi dengan teknologi dan informasi digital. Namun, ada juga dampak negatif, terutama dalam bentuk meningkatnya ancaman kejahatan siber atau cyber crime, yang bisa merugikan individu, perusahaan, bahkan negara melalui dunia maya.

Ungkapan “cyber crime” pertama kali diperkenalkan oleh William Gibson pada tahun 1982 dalam novelnya "Neuromancer" yang diterbitkan pada tahun 1984. Gibson memperkenalkan istilah "cyber space" untuk menggambarkan dunia maya yang terhubung dengan aktivitas komputer serta "cyber crime" untuk merujuk pada tindakan kriminal yang terjadi di dunia maya serta mengancam keamanan (Wall, 2007). Cyber crime mengacu pada aktivitas kriminal yang memanfaatkan teknologi informasi sebagai sarana untuk mengidentifikasi kerentanan dalam sistem yang dapat diakses internet (Wahid, 2005). Seiring berjalannya waktu, cyber crime telah berkembang dengan pesat, ditandai dengan beragamnya modus operandi, yang beberapa di antaranya melibatkan negara sebagai pelakunya. Jenis cyber crime baru yang semakin menonjol ialah Cyber Espionage.

Cyber Espionage, atau spionase siber, mengacu pada mengurai kata demi kata. "Cyber" merujuk pada dunia maya yang menjadi tempat kejahatan ini terjadi, sementara "espionage" mengacu pada pengumpulan informasi yang disengaja serta sistematis oleh seseorang atau badan pemerintah (Baker, 2003). Cyber Espionage, mengacu pada aktivitas yang dilaksanakan di dunia maya oleh individu atau kelompok yang tidak berwenang dengan maksud mendapatkan informasi yang dibutuhkan, baik bersifat umum atau khusus, atas nama pemerintah.

Dalam dunia yang semakin terhubung dan terdigitalisasi, praktik spionase antar negara semakin canggih. Informasi yang dikumpulkan secara diam-diam dapat digunakan untuk kepentingan negara, dan targetnya seringkali tidak menyadari bahwa mereka sedang diawasi. Salah satu contoh nyata adalah kasus spionase yang dilaksanakan oleh Australia serta Amerika Serikat terhadap Pemerintah Indonesia. Pengungkapan kejadian ini diungkapkan Marciano Norman, Direktur Badan Intelijen Negara (BIN), yang mengemukakan Australia pernah terlibat dalam penyadapan panggilan telepon yang melibatkan otoritas Indonesia selama periode 2007-2009 (Sudiarta, 2014).

Kasus ini memperlihatkan ancaman serius yang dihadapi oleh negara-negara dalam persaingan global saat ini. Perkembangan teknologi informasi serta komunikasi pada era digital memungkinkan praktik spionase melalui komputer dan jaringan internet, yang sangat sulit dideteksi. Selain itu, tindakan Cyber Espionage melibatkan pelaku yang dapat beroperasi tanpa terpengaruh oleh batasan geografis, ruang, atau waktu, yang membuatnya menjadi ancaman yang sulit ditangani.

Untuk menghadapi ancaman Cyber Espionage, penegakan hukum harus mempertimbangkan prinsip-prinsip seperti keadilan, imparsialitas, independensi, dan profesionalisme dalam pengambilan keputusan serta melibatkan partisipasi publik. Era Society 5.0 mengedepankan sentralitas kemanusiaan dalam upayanya, sehingga memerlukan

keseimbangan yang harmonis antara keunggulan ekonomi serta resolusi kemasyarakatan. Tujuan ini dapat dicapai melalui integrasi yang luas, termasuk ranah digital (cyberspace) serta ranah fisik (physical space).

Metode Penelitian

Riset ini menerapkan metodologi yuridis normatif, dengan memanfaatkan literatur sebagai sumber utama serta mencakup tiga pendekatan berbeda: konseptual, komparatif, serta perundang-undangan. Bahan riset meliputi sumber hukum primer serta sekunder. Dokumen hukum primer mencakup peraturan perundang-undangan serta keputusan pengadilan, yang berfungsi sebagai komponen dasar yurisprudensi. Sementara bahan hukum sekunder melibatkan publikasi ilmiah seputar aspek hukum, seperti buku, jurnal, serta riset terkait yang relevan dengan fokus riset ini. Dengan pendekatan ini, penelitian bertujuan untuk memberikan wawasan mendalam mengenai topik yang diteliti, menjembatani aspek konseptual, perbandingan, dan aspek perundang-undangan serta memanfaatkan sumber daya literatur yang relevan dalam analisisnya.

Hasil dan Pembahasan

Hukum Nasional dan Hukum Internasional

Istilah "hukum nasional" mengacu pada kerangka kerja hukum yang mengatur kegiatan serta hubungan di suatu negara atau wilayah tertentu. Ini mencakup berbagai aspek, mulai dari hukum pidana, hukum perdata, hukum kontrak, hukum lingkungan, hingga hukum pajak. Tujuan utama hukum nasional adalah memberikan panduan yang jelas mengenai apa yang diperbolehkan serta dilarang dalam masyarakat. Ini menciptakan kerangka kerja yang mengatur hak dan kewajiban individu, perusahaan, dan pemerintah.

Hukum nasional biasanya didefinisikan dan disusun dalam bentuk peraturan, undang-undang, dan keputusan pengadilan. Hukum ini berlaku di seluruh yurisdiksi negara dan berfungsi sebagai alat untuk menyelesaikan konflik, menjaga ketertiban sosial, dan menjalankan kebijakan pemerintah.

Hukum Internasional ialah disiplin hukum yang mengatur berbagai tindakan yang terjadi di tingkat internasional. Awalnya, definisi hukum internasional hanya berkaitan dengan perilaku serta interaksi negara-negara berdaulat. Namun, seiring dengan berjalannya waktu dan semakin kompleksnya pola hubungan internasional, cakupan hukum internasional berkembang menjadi lebih luas. Saat ini, ranah hukum internasional tidak hanya mencakup kerangka kerja serta perilaku organisasi internasional, namun juga mencakup perusahaan multinasional serta individu dalam beberapa kasus.

Hukum internasional, juga dikenal sebagai hukum antar negara, yakni kumpulan peraturan, konsep, serta perjanjian yang mengatur interaksi antara berbagai entitas di panggung global. Ini mencakup negara-negara, organisasi internasional, dan dalam beberapa situasi tertentu, individu dan perusahaan multinasional. Konsep hukum internasional juga mencerminkan sejarah panjang di mana norma dan peraturan yang mengatur hubungan antarnegara telah berkembang.

Hukum internasional berperan penting dalam pemeliharaan perdamaian serta keamanan dalam skala dunia, serta dalam memfasilitasi kerjasama internasional dalam berbagai bidang seperti perdagangan, HAM, serta lingkungan. Dalam pembahasan selanjutnya, kita akan menyelami berbagai aspek hukum internasional, termasuk sumber hukum, perkembangan sejarahnya, serta peran dan tantangan yang dihadapi dalam era modern.

Hukum nasional mengacu pada kerangka hukum yang berlaku di suatu negara atau yurisdiksi tertentu. Landasan hukum ini mencakup beragam aspek, mulai dari hukum pidana yang mengatur pelanggaran kriminal hingga hukum perdata yang berkaitan dengan sengketa sipil antara individu. Selain itu, hukum kontrak mengatur perjanjian antara pihak-pihak yang berkontrak, hukum lingkungan menjaga keseimbangan alam, dan hukum pajak mengatur kewajiban pajak. Tujuan utama dari hukum nasional adalah memberikan panduan yang jelas kepada masyarakat tentang apa yang diperbolehkan serta apa yang dilarang. Hal ini menciptakan kerangka kerja yang mengatur hak dan kewajiban individu, perusahaan, serta pemerintah.

Hukum nasional sering kali didefinisikan dan diatur dalam bentuk peraturan, undang-undang, dan keputusan pengadilan. Hukum ini berlaku di seluruh wilayah negara dan berperan sebagai alat untuk menyelesaikan konflik, menjaga ketertiban sosial, dan menjalankan kebijakan pemerintah. Landasan hukum nasional merupakan tulang punggung sistem hukum dalam suatu negara, memastikan bahwa keadilan dan ketaatan terhadap hukum dijaga.

Hukum Internasional ialah disiplin hukum yang mengatur berbagai tindakan yang terjadi di tingkat internasional. Awalnya, definisi hukum internasional hanya berkaitan dengan perilaku serta interaksi negara-negara berdaulat. Namun, seiring berjalannya waktu dan semakin kompleksnya hubungan internasional, cakupan hukum internasional berkembang menjadi lebih luas. Saat ini, ranah hukum internasional tidak hanya mencakup kerangka kerja serta perilaku organisasi internasional, namun juga mencakup perusahaan multinasional serta individu dalam beberapa kasus.

Hukum internasional, yang sering disebut hukum antar bangsa atau hukum antar negara, mencakup serangkaian aturan, prinsip, dan konvensi yang mengatur hubungan antara berbagai entitas di tingkat internasional. Entitas tersebut termasuk negara-negara, organisasi internasional, dan dalam beberapa situasi tertentu, individu dan perusahaan multinasional. Konsep hukum internasional mencerminkan sejarah panjang di mana norma dan peraturan yang mengatur hubungan antarnegara telah berkembang.

Hukum internasional berperan penting dalam pemeliharaan perdamaian serta keamanan dalam skala dunia. Ini berperan sebagai alat untuk mengatasi konflik antarnegara, memfasilitasi kerjasama internasional dalam berbagai bidang seperti perdagangan, hak asasi manusia, dan lingkungan. Hukum internasional memainkan peran penting dalam menjembatani negara-negara untuk bekerja sama dalam mengatasi tantangan global, termasuk isu-isu perubahan iklim dan perdagangan internasional. Dalam era modern, hukum internasional menghadapi berbagai tantangan, seperti ketegangan geopolitik dan isu-isu hak asasi manusia. Dengan demikian, pemahaman yang mendalam tentang hukum internasional menjadi semakin penting untuk menjaga stabilitas dan kerjasama internasional di abad ke-21. Dalam pembahasan selanjutnya, kita akan menjelajahi berbagai aspek hukum internasional, termasuk sumber hukum, perkembangan sejarahnya, serta peran dan tantangan yang dihadapinya dalam era modern.

Cyber Espionage

Dalam era globalisasi yang didorong oleh teknologi informasi, masalah cyber crime telah menjadi isu penting dalam konteks keamanan jaringan komputer dan informasi. Cyber crime terkait erat dengan penggunaan internet sebagai komoditas utama, di mana informasi menjadi aset berharga yang memerlukan kehandalan dalam penyediaan layanan agar tidak

mengecewakan konsumennya. Dalam upaya memahami cyber crime, ada beberapa definisi yang diberikan oleh berbagai sumber.

Indra Safitri mengemukakan cyber crime mencakup aktivitas kriminal yang memanfaatkan teknologi informasi tanpa batasan, seringkali mengandalkan manipulasi teknis tingkat lanjut yang memerlukan langkah-langkah keamanan yang kuat serta keandalan informasi yang diakses serta dikirim oleh pengguna internet. Ini mendeskripsikan karakteristik yang melekat pada aktivitas kriminal yang terjadi di dunia digital, yang semakin berkembang seiring dengan pesatnya kemajuan teknologi informasi. Cyber crime melibatkan aktivitas yang dilakukan dengan duduk di depan komputer dan sering kali terkait dengan penggunaan teknologi tanpa batasan.

Berlandaskan Kepolisian Inggris, cyber crime mencakup semua bentuk aktivitas yang mencakup penggunaan jaringan komputer dengan maksud kriminal, sering kali dengan mengeksploitasi kemudahan teknologi digital. Hal ini menggambarkan sifat kejahatan yang berbasis teknologi tinggi dan penggunaan teknologi digital untuk kegiatan kriminal.

Dalam era globalisasi yang didorong oleh teknologi informasi, masalah cyber crime telah menjadi isu penting dalam konteks keamanan jaringan komputer dan informasi. Cyber crime adalah jenis kejahatan yang tumbuh seiring dengan perkembangan pesat internet sebagai komoditas utama. Internet telah menjadikan informasi sebagai aset berharga yang memerlukan keandalan dalam penyediaan layanan agar tidak mengecewakan konsumennya.

Dalam upaya memahami cyber crime, berbagai sumber memberikan definisi yang bervariasi. Indra Safitri mengemukakan cyber crime mencakup aktivitas kriminal yang memanfaatkan teknologi informasi tanpa batasan, seringkali mengandalkan manipulasi teknis tingkat lanjut yang memerlukan langkah-langkah keamanan yang kuat serta keandalan informasi yang diakses serta dikirim oleh pengguna internet. Cyber crime mencerminkan sifat kejahatan di dunia maya yang berkembang seiring perkembangan teknologi informasi. Aktivitas kejahatan ini seringkali dilakukan oleh individu yang duduk di depan komputer dan terkait dengan penggunaan teknologi tanpa batasan.

Berlandaskan Kepolisian Inggris, cyber crime mencakup semua bentuk aktivitas yang mencakup penggunaan jaringan komputer dengan maksud kriminal, seringkali dengan mengeksploitasi kemudahan teknologi digital. Hal ini menggambarkan sifat kejahatan yang sangat bergantung pada teknologi tinggi dan penggunaan teknologi digital untuk melakukan kegiatan kriminal. Dengan kata lain, cyber crime melibatkan aktivitas kejahatan yang memanfaatkan infrastruktur teknologi komputer untuk mencapai tujuan kriminal, termasuk pencurian data, penipuan online, dan serangan terhadap sistem komputer.

Penting untuk memahami sifat kompleks cyber crime karena perkembangan teknologi terus berlanjut. Ini memerlukan upaya yang lebih besar dalam mencegah dan melawan kejahatan ini, termasuk kerja sama internasional, pengembangan kebijakan cyber security, dan peningkatan kesadaran masyarakat terhadap risiko yang terkait dengan penggunaan internet. Dengan pemahaman yang lebih baik tentang cyber crime, kita dapat memitigasi ancaman terhadap keamanan jaringan komputer dan informasi, sehingga masyarakat global dapat terus mengakses dan memanfaatkan teknologi informasi tanpa takut menjadi korban kejahatan digital.

Perkembangan teknologi informasi telah mengubah paradigma definisi cyber crime, di mana awalnya fokus pada perangkat keras komputer, seperti komputer pribadi. Namun, seiring dengan kemunculan internet, fokus definisi cyber crime telah bergeser menjadi aktivitas yang

dapat terjadi dalam dunia siber melalui sistem informasi yang dipergunakan. Ini mencerminkan perkembangan teknologi informasi yang telah mengintegrasikan aspek-aspek berbeda dari telekomunikasi, media, dan informatika menjadi satu kesatuan. Pertumbuhan aplikasi internet telah memunculkan berbagai kegiatan kriminal, yang secara kolektif dikenal sebagai Cyber crime, yang mencakup berbagai jenis kejahatan serta metode operasi yang difasilitasi oleh pemakaian aplikasi internet.

Secara umum, cyber crime mencakup beberapa jenis kegiatan kriminal yang secara khusus menargetkan komputer, jaringan komputer, serta mereka yang memanfaatkan sistem tersebut. Cyber crime dapat diklasifikasikan ke dalam dua kategori berbeda, yakni dalam lingkup terbatas serta konteks yang lebih luas. Dalam interpretasi sempit, cyber crime mencakup kejahatan yang ditujukan terhadap sistem komputer. Namun dalam interpretasi yang lebih luas, cyber crime mencakup pelanggaran yang menargetkan sistem atau jaringan komputer, serta pelanggaran yang menmanfaatkan komputer sebagai sarananya. Secara umum, cyber crime mencakup serangkaian aktivitas kriminal yang secara khusus menargetkan komputer, jaringan komputer, serta pemakainya. Selain itu, ini mencakup jenis perilaku kriminal konvensional yang dilaksanakan dengan penggunaan komputer.

Dalam konteks perkembangan teknologi informasi serta internet, pemahaman yang mendalam tentang cyber crime sangat penting dalam upaya menjaga keamanan jaringan komputer dan informasi. Cyber crime dapat memiliki dampak yang serius terhadap individu, perusahaan, dan masyarakat secara keseluruhan. Oleh karena itu, langkah-langkah untuk mengatasi cyber crime dan meningkatkan keamanan jaringan komputer menjadi sangat relevan dalam era digital ini. Dengan pemahaman yang kuat tentang sifat dan jenis cyber crime, kita dapat mengembangkan strategi yang lebih efektif dalam melindungi diri dari ancaman di dunia maya.

Era Society 5.0

Era Society 5.0 ialah perpanjangan dari evolusi teknologi yang telah mempengaruhi masyarakat sejak zaman primitif. Konsep ini muncul sebagai respons terhadap gejolak disrupsi yang disebabkan oleh Revolusi Industri 4.0 pada tahun 2019. Era Society 5.0 memiliki visi besar, yaitu mengarahkan kita untuk memanfaatkan kemajuan teknologi guna mempermudah aktivitas manusia. Dalam konteks ini, Society 5.0 dapat dipahami sebagai penyempurnaan dari generasi-generasi sebelumnya, mulai dari Era 1.0 hingga Era 4.0.

Era 1.0 menggambarkan masa ketika manusia hidup sebagai pemburu dan mengenal tulisan. Era 2.0 ditandai dengan perkembangan pertanian dan pertanian, sedangkan Era 3.0 adalah masa ketika manusia mulai mengenal industri serta memanfaatkan mesin dalam kehidupan sehari-hari. Era 4.0, yang merupakan periode yang mendahului Society 5.0, menghadirkan revolusi teknologi komputer dan internet, yang secara luas dimanfaatkan dalam berbagai aspek kehidupan.

Konsep Society 5.0 lahir di Jepang dengan gagasan utama "Harus memanusiakan manusia dengan teknologi." Meskipun ada evolusi dari Era 4.0 ke Era Society 5.0, perubahan tersebut tidak menciptakan perbedaan yang besar. Sebaliknya, Era Society 5.0 lebih fokus pada penggunaan yang lebih efektif dan optimal dari teknologi yang telah ada dalam Era Revolusi Industri 4.0. Prinsip utamanya adalah menghubungkan masyarakat, benda, sistem, dan elemen-

elemen lainnya secara virtual dan memproses data dengan menerapkan kecerdasan buatan (Artificial Intelligence).

Pada Era Society 5.0, praktik yang berbeda dari Revolusi Industri 4.0 terlihat dalam cara data dan informasi dikelola. Di Era Society 5.0, informasi yang terkumpul dari berbagai sumber, termasuk Internet of Things (IoT), Big Data, kecerdasan buatan, serta robot, tidak hanya dianalisis oleh manusia. Sebaliknya, data ini diolah dan dimengerti oleh sistem kecerdasan buatan (AI), yang kemudian menghasilkan solusi yang optimal. Hal ini membuka peluang untuk mencapai tingkat efisiensi yang jauh melampaui kapasitas manusia dalam mengolah dan menginterpretasikan data.

Visi utama dari Society 5.0 ialah bahwa masyarakat yang hidup di era ini diharapkan mampu mengatasi berbagai permasalahan dan tantangan dengan memanfaatkan kemajuan teknologi yang telah ada. Terobosan besar dalam teknologi, seperti Internet of Things (IoT), Artificial Intelligence (kecerdasan buatan), Big Data (data besar), serta robot, diharapkan dapat membantu mengatasi berbagai masalah yang mungkin sulit dipecahkan dalam Era 4.0. Dengan menggabungkan teknologi dan kecerdasan buatan, Society 5.0 bertujuan untuk menciptakan solusi yang lebih efisien dan lebih cerdas dalam berbagai aspek kehidupan, mulai dari layanan kesehatan hingga manajemen lingkungan.

Society 5.0 ialah refleksi dari bagaimana teknologi terus mengubah cara kita hidup dan berinteraksi. Dengan visi untuk "memanusiakan" teknologi, era ini mengejar pencapaian kehidupan yang lebih baik melalui pemanfaatan inovasi teknologi. Namun, dalam upaya menuju Society 5.0, penting untuk mempertimbangkan aspek-aspek seperti etika, privasi, dan keamanan, agar teknologi dapat digunakan dengan cara yang bertanggung jawab dan berkelanjutan. Dengan demikian, Era Society 5.0 membawa harapan serta masalah baru dalam masyarakat yang semakin terhubung dan terdigitalisasi.

Era Society 5.0 ialah sebuah konsep yang menggambarkan perpanjangan dari evolusi teknologi yang telah memengaruhi masyarakat sejak zaman primitif hingga Revolusi Industri 4.0 pada tahun 2019. Era Society 5.0 muncul sebagai respons terhadap gejolak disrupsi yang disebabkan oleh kemajuan teknologi. Visi utamanya adalah mengarahkan kita untuk memanfaatkan teknologi guna mempermudah aktivitas manusia dan "memanusiakan manusia dengan teknologi." Dalam konteks ini, Society 5.0 dapat dipahami sebagai penyempurnaan dari generasi-generasi teknologi sebelumnya, mulai dari Era 1.0 hingga Era 4.0.

Era 1.0 menggambarkan masa ketika manusia hidup sebagai pemburu dan mengenal tulisan. Era 2.0 ditandai dengan perkembangan pertanian, sedangkan Era 3.0 adalah masa ketika manusia mulai mengenal industri serta memanfaatkan mesin dalam kehidupan sehari-hari. Era 4.0, yang mendahului Society 5.0, menghadirkan revolusi teknologi komputer dan internet, yang telah mendalam dalam berbagai aspek kehidupan manusia.

Konsep Society 5.0 pertama kali muncul di Jepang serta bertujuan untuk menghubungkan masyarakat, benda, sistem, dan elemen-elemen lainnya secara virtual. Era Society 5.0 lebih berfokus pada penggunaan yang lebih efektif dan optimal dari teknologi yang telah ada dalam Era Revolusi Industri 4.0. Prinsip utamanya ialah menggabungkan teknologi seperti Internet of Things (IoT), Artificial Intelligence (kecerdasan buatan), serta Big Data untuk memproses data dengan tingkat efisiensi yang tinggi.

Pada Era Society 5.0, cara data dan informasi dikelola berbeda dari Revolusi Industri 4.0. Informasi yang terkumpul dari berbagai sumber, termasuk IoT, Big Data, kecerdasan

buatan, dan robot, tidak hanya dianalisis oleh manusia. Data ini diolah dan dimengerti oleh sistem kecerdasan buatan (AI), yang kemudian menghasilkan solusi yang optimal. Hal ini membuka peluang untuk mencapai tingkat efisiensi yang jauh melampaui kapasitas manusia dalam mengolah dan menginterpretasikan data.

Visi utama dari Society 5.0 ialah bahwa masyarakat yang hidup di era ini diharapkan mampu mengatasi berbagai permasalahan dan tantangan dengan memanfaatkan kemajuan teknologi. Terobosan besar dalam teknologi, seperti IoT, kecerdasan buatan, Big Data, dan robot, diharapkan dapat membantu mengatasi berbagai masalah yang mungkin sulit dipecahkan dalam Era 4.0. Dengan menggabungkan teknologi dan kecerdasan buatan, Society 5.0 bertujuan untuk menciptakan solusi yang lebih efisien dan lebih cerdas dalam berbagai aspek kehidupan, mulai dari layanan kesehatan hingga manajemen lingkungan.

Society 5.0 adalah refleksi dari bagaimana teknologi terus mengubah cara kita hidup dan berinteraksi. Dengan visi untuk "memanusiakan" teknologi, era ini mengejar pencapaian kehidupan yang lebih baik melalui pemanfaatan inovasi teknologi. Namun, dalam upaya menuju Society 5.0, penting untuk mempertimbangkan aspek-etika, privasi, dan keamanan, agar teknologi dapat digunakan dengan cara yang bertanggung jawab dan berkelanjutan. Era Society 5.0 menghadirkan peluang serta hambatan dalam masyarakat yang semakin terhubung serta bergantung pada teknologi digital. Era ini menumbuhkan kecenderungan masyarakat terhadap gaya hidup terkemuka yang ditandai dengan peningkatan efisiensi serta keterhubungan, tetapi juga mewajibkan kita untuk bersama-sama menjaga agar kemajuan teknologi berjalan seiring dengan kepentingan manusia dan masyarakat pada umumnya.

Ancaman yang Berkembang terhadap Pertahanan dan Keamanan di Era Society 5.0

Cyber Espionage mewakili evolusi modern dari metode mata-mataan konvensional. Mata-mataan konvensional telah menjadi praktik umum sejak masa perang. Kamus Besar Bahasa Indonesia (KBBI) mendefinisikan spionase sebagai penyelidikan secara diam-diam terhadap data ekonomi serta militer negara asing, segala hal yang terkait dengan spionase, dan tindakan mata-mata: tindakan teknis mata-mata. Teknik mata-mataan konvensional sering digunakan sebagai strategi untuk mendapatkan keuntungan dalam peperangan, sejalan dengan pandangan ahli strategi perang Tiongkok Sun Tzu, yang meyakini bahwa puncak kemenangan terletak pada kemampuan meraih kemenangan dalam suatu konflik tanpa harus melaksanakan pertarungan fisik (Purna Nugraha, 2017). Pemakaian spionase sebagai strategi peperangan serta sebagai sarana untuk mengumpulkan informasi intelijen tentang musuh diperbolehkan sesuai dengan Pasal 24 Konvensi Den Haag. Lebih lanjut, diatur dalam Pasal 25 serta 29 bahwa mereka yang mengejar bahan rahasia di dalam wilayah operasi dilarang keras melakukan tindakan agresi seperti penyerangan atau pengeboman pusat kota, desa, serta infrastruktur penting. Konvensi Den Haag IV tahun 1907 adalah salah satu konvensi yang mengatur aktivitas spionase. Pasal 29 konvensi ini menyiratkan bahwa seorang prajurit dapat dianggap terlibat dalam spionase saat mereka memasuki wilayah musuh dengan menyamar dengan tujuan mengumpulkan informasi musuh dan mengirimkannya kepada pihak pengirim.

Selama periode setelah konflik bersenjata atau masa damai, spionase terus sering diterapkan guna memajukan kepentingan nasional serta merumuskan kebijakan pertahanan nasional suatu negara. Tindakan spionase melibatkan pengerahan agen intelijen, penggunaan staf diplomatik dalam negara target, serta bahkan meretas sistem negara. Terutama, Prancis dan Jerman telah menjadi target spionase yang dilakukan oleh Amerika Serikat. Pada masa

damai, beberapa kasus spionase yang mencolok mencakup kegiatan agen intelijen Brasil bernama Abin dari tahun 2003 hingga 2004 dan kasus Ryan Fogle, seorang diplomat Amerika Serikat yang repatriasi oleh pemerintah Rusia setelah terungkap terlibat dalam spionase (Pratiwi & Correia, 2020). Indonesia juga telah melihat contoh spionase. Salah satu insiden penting terjadi pada tahun 1982, ketika Kolonel Sergei Egorof, yang menjabat sebagai kepala asisten pertahanan di Kedutaan Besar Soviet di Jakarta, ditangkap karena partisipasinya dalam perdagangan gelap bahan-bahan rahasia Indonesia, antara lain Peta Hidrografi Laut Banda (Sudiro & Marton, 2017).

Kemajuan pesat teknologi komputer serta internet telah diterapkan sebagai sarana untuk terlibat dalam kegiatan spionase. Manual Tallinn 2.0, sebuah sumber daya komprehensif yang dirancang untuk para pembuat kebijakan serta pakar hukum internasional, menjelaskan sifat rahasia dari spionase dunia maya, yakni operasi rahasia yang dilaksanakan dengan menggunakan kemampuan dunia maya untuk memperoleh informasi sensitif (Michael, 2013). Penggunaan dunia maya sebagai platform untuk melakukan Cyber Espionage mengklasifikasikan perilaku ini sebagai salah satu jenis kejahatan siber. Organisasi Kerja Sama Ekonomi dan Pembangunan (OECD) mendefinisikan kejahatan siber sebagai tindakan tidak etis atau ilegal yang melibatkan akses tidak sah ke sistem komputer atau transmisi data (Sinaga, 2010). Kejahatan siber lebih lanjut diklasifikasikan oleh Dikdik M. Arief serta Elisatris Gultom sebagai Akses Tidak Sah ke Sistem Komputer dan Layanan, Pemalsuan Data, Isi Tidak Sah, Cyber Espionage, Sabotase dan Ekstorsi Cyber, Pelanggaran Privasi, dan Pelanggaran Hak Kekayaan Intelektual (Dikdik & Gultom, 2005).

Cyber Espionage secara khusus diidentifikasi sebagai kejahatan siber. Dalam penerapan praktisnya, Cyber Espionage dilaksanakan oleh individu atau kelompok di bawah arahan pemerintah, dengan maksud mendapatkan data sensitif secara ilegal melalui penggunaan metodologi peretasan serta penyebaran virus komputer di dalam sistem komputer atau jaringan internet entitas swasta atau pemerintah. Salah satu contohnya ialah kelompok peretas yang dikenal sebagai Cozy Bear, yang telah dikaitkan dengan entitas intelijen Rusia. Kelompok ini berfokus pada bidang militer, pemerintahan, energi, diplomatik, serta telekomunikasi, serta telah terlibat dalam kegiatan Cyber Espionage yang menargetkan berbagai entitas seperti perusahaan serta badan pemerintah di Jerman, Uzbekistan, Korea Selatan, serta Amerika Serikat. Khususnya, pada tahun 2014, operasi mereka termasuk menyusup ke Departemen Luar Negeri dan Gedung Putih (Baumgartner, 2015). Pada bulan Juli 2020, tuduhan dibuat oleh National Cyber Security Center (NCSC), National Security Agency (NSA), serta Cyber Security Education (CSE) terhadap Cozy Bear, mencoba mencuri data terkait vaksin dan perawatan Covid-19 yang sedang dikembangkan di Inggris, Amerika Serikat, serta Kanada (HSToday, 2020).

Meskipun kebanyakan korban Cyber Espionage adalah negara maju dengan tindakan keamanan digital yang canggih, itu tidak berarti bahwa negara berkembang seperti Indonesia kebal terhadap ancaman tersebut. Kaspersky Lab, sebuah perusahaan antivirus ternama, baru-baru ini mengungkapkan adanya kelompok yang dicurigai terlibat dalam aktivitas Cyber Espionage di kawasan Asia Tenggara. Negara Indonesia, termasuk lembaga pemerintahan, departemen pertahanan, departemen intelijen, lembaga diplomatik, serta perusahaan telekomunikasi, telah menjadi sasaran serangan yang ditargetkan oleh organisasi APT tersebut. Serangan Cyber Espionage di Indonesia melibatkan penggunaan virus untuk mencuri email atau dokumen, yang kemudian dikirimkan kepada para penyerang (Baezner, 2018).

Faktor utama yang berkontribusi pada lanskap ancaman siber adalah geopolitik dan ekonomi. Indonesia, dengan keragaman etnis, pandangan politik, dan pembangunan ekonominya, adalah bagian dari Asia Tenggara dan oleh karena itu tidak kebal terhadap ancaman berkembangnya Cyber Espionage. Dalam era Society 5.0, di mana teknologi sangat terintegrasi dalam kehidupan sehari-hari, kebutuhan akan langkah-langkah keamanan siber dan pertahanan yang kokoh lebih penting daripada sebelumnya untuk melindungi kepentingan nasional dan menjaga informasi rahasia dari pelaku siber yang jahat.

Instrumen Hukum Internasional dalam Menghadapi Ancaman Cyber Espionage

Cyber Espionage merupakan topik relatif baru dalam hukum internasional, dan hingga saat ini belum terdapat peraturan khusus yang mengaturnya. Dalam aktivitas Cyber Espionage, para peretas memanfaatkan ruang siber untuk mengakses dan menyalin data. Ruang siber, termasuk jaringan komputer serta internet, mempunyai kapasitas untuk melemahkan kewenangan yurisdiksi negara dalam bidang penegakan hukum, terutama ketika serangan bersumber dari negara lain. Untuk mengatasi tantangan seperti ini, diperlukan instrumen hukum yang dapat mengakomodasi tindakan tersebut, sejalan dengan hukum-hukum yang berlaku di negara-negara terkait. Profesor Rebecca Wallace mengungkapkan istilah "hukum internasional" mengacu pada peraturan yang mengatur perilaku suatu negara, termasuk interaksi antar negara serta masyarakat serta organisasi internasional (R. Wallace, 1993).

Saat ini, evolusi hukum internasional sangat terkait dengan kebijakan luar negeri yang diambil oleh suatu negara, serta asal usulnya dapat ditelusuri kembali ke dinamika unik yang dihadapi oleh masing-masing negara. Beragam sumber hukum internasional sebagai bahan pertimbangan pengadilan serta pakar hukum dituangkan dalam Pasal 38 ayat (1) Statuta Mahkamah Internasional. Ketentuan ini menyebutkan sumber-sumber hukum internasional diantaranya:

1.Perjanjian internasional yang telah mendapat pengakuan dari semua negara peserta.
2.Kebiasaan internasional, termasuk pendapat juris yang diakui masyarakat internasional.
3.Prinsip-prinsip hukum yang menyeluruh.
4.Sumber mencakup keputusan pengadilan serta doktrin para akademisi terkemuka yang berasal dari berbagai negara.

Pasal ini memperlihatkan pemeriksaan terhadap aktivitas Cyber Espionage akan dilaksanakan melalui penggunaan sumber daya hukum internasional, termasuk perjanjian serta perspektif akademisi berpengaruh, yang dapat membentuk perlakuan terhadap Cyber Espionage.

Pertama, kurangnya undang-undang Cyber Espionage yang jelas telah menakibatkan pemerintah mengambil tindakan berlandaskan peraturan dalam negeri. Meskipun begitu, beberapa instrumen hukum membahas kejahatan spionase, terutama dalam konteks perang. Spionase ialah taktik perang yang umum diterapkan. Pasal 24 Konvensi Den Haag, sebagai contoh, memperbolehkan penggunaan tipu daya perang dan metode lain untuk mengumpulkan informasi musuh. Niccolo Machiavelli, seorang diplomat serta politisi Italia, menganjurkan penipuan dalam pertempuran serta melihat semua pihak sebagai musuh. Pasal 30 serta 31 Konvensi Den Haag mengklaim pelaku spionase yang ditangkap dalam konflik bersenjata tidak dapat dihukum tanpa adanya putusan pengadilan, sementara agen yang kembali ke pasukan mereka dan kemudian tertangkap oleh musuh dianggap sebagai penjahat perang.

Spionase diplomatik dilarang berlandaskan Konvensi Wina 1961. Diplomat dari negara pengirim mengikuti kesepakatan negara penerima. Meskipun tugas diplomat adalah

mendapatkan informasi dan melindungi kepentingan nasional, spionase untuk tujuan ini melanggar hukum internasional karena dapat merusak kedaulatan serta hubungan diplomatik negara penerima. Resolusi Majelis Umum PBB tentang Deklarasi Prinsip-Prinsip Hukum Internasional mengenai 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 menekankan itikad baik dalam hubungan internasional.

Di samping itu, ada peraturan yang mengatur kejahatan siber dalam Konvensi tentang Kejahatan Siber. Konvensi ini, yang telah disepakati di Budapest dan diratifikasi oleh sejumlah negara sejak 23 November 2001, berusaha mengharmonisasi hukum nasional dalam hal kejahatan siber, baik dalam aspek materiil maupun formil, dan mengatur kerja sama internasional dalam penegakan hukum. Konvensi ini memberi wewenang kepada negara-negara anggota untuk mengintegrasikan isinya ke dalam undang-undang nasional mereka, termasuk pedoman atau konsekuensi atas akses informasi yang tidak sah. Perjanjian ini mengatur ekstradisi serta bantuan hukum penjahat dunia maya dalam kerangka pedoman serta hukuman. European Convention on Cybercrime (ECC), yang mengikat Uni Eropa menangani akses data terlarang, sebuah taktik Cyber Espionage yang sering dilaksanakan.

Kedua, tidak ada kebiasaan atau penilaian hukum internasional yang melegitimasi Cyber Espionage. Prinsip-prinsip kebiasaan internasional harus memenuhi dua elemen: praktik umum di suatu negara diakui sebagai hukum oleh komunitas internasional. Beberapa tradisi bukan merupakan hukum internasional, dan pengakuan oleh negara-negara terhadap kewajiban yang mengikat adalah bukti utama keberlakuan kebiasaan internasional (Schwarzenberger, 1967).

Sebagai contoh, Kasus Anglo-Norwegian Fisheries ialah kasus internasional yang mengatur kebiasaan internasional. Norwegia dan Inggris menyelesaikan perselisihan garis dasar maritim mereka di Mahkamah Internasional. Inggris menuduh Norwegia melanggar hukum internasional dengan menarik garis pangkal laut dari selat, sehingga memberikan Norwegia kesempatan untuk mengeksploitasi sumber daya perikanan yang kaya di selat tersebut. Norwegia, di sisi lain, berpendapat bahwa tindakan tersebut telah sesuai dengan hukum internasional. Hasil akhirnya, Mahkamah Internasional memenangkan Norwegia (Green, 1952).

Ketiga, tindakan Cyber Espionage menentang tiga prinsip hukum internasional utama: kedaulatan negara, non-intervensi, dan pelaku non-negara atau non-state actor.

1. Kedaulatan Negara: Kedaulatan negara adalah hak suatu negara untuk menjalankan pemerintahannya tanpa campur tangan negara lain. Prinsip ini memungkinkan negara-negara untuk mengejar kebijakan dan kepentingan nasional mereka tanpa intervensi eksternal (Max Huber, 1929). United Nations Group of Governmental Experts on Development (UN GGE 2013) mengemukakan kedaulatan negara dan norma serta prinsip internasional harus berlaku dalam konteks teknologi informasi dan komunikasi. Oleh karena itu, asas kedaulatan negara serta norma internasional juga relevan dalam ruang siber. Metode pelaksanaan Cyber Espionage, terutama yang dilakukan dari luar wilayah negara sasaran, menciptakan potensi pelanggaran kedaulatan negara. Meskipun tindakan semacam itu mungkin tidak selalu melanggar kedaulatan negara secara langsung, cara pelaksanaannya dapat membuatnya menjadi pelanggaran (Michael N. Schmitt, 2017).
2. Non-Intervensi: Prinsip non-intervensi melarang negara-negara untuk campur tangan dalam urusan internal negara lain, seperti penentuan sistem politik, masalah sosial, serta

budaya, serta kebijakan luar negeri suatu negara (Jamnejad, 2009). Prinsip ini didasarkan pada Pasal 2 Paragraf 7, Pasal 42, Pasal 51 dari Piagam PBB, serta Resolusi Majelis Umum PBB No. 2625 tahun 1970. Tindakan mengumpulkan data serta informasi dari negara lain dalam konteks Cyber Espionage dapat dianggap sebagai pelanggaran terhadap prinsip non-intervensi, terutama ketika data tersebut dimanfaatkan untuk alasan yang merugikan negara sasaran.

3. Pelaku Non-Negara: Peretas yang menargetkan pemerintah atau perusahaan asing biasanya bukan agen negara atau tidak disponsori negara. Dalam banyak kasus, pelaku siber adalah individu atau kelompok independen yang bertindak atas kepentingan pribadi atau finansial. Namun, ketika pelaku tersebut diinstruksikan atau didukung oleh pemerintah, maka negara tersebut dapat bertanggung jawab atas tindakan tersebut (Kulesza, 2009). Setelah melaksanakan analisis terhadap sumber-sumber hukum internasional, dapat disimpulkan bahwa pengaturan kegiatan ini tidak secara tegas diatur dalam kerangka hukum internasional. Namun, tindakan seperti ini dapat diklasifikasikan sebagai akses ilegal ke data serta perolehan data yang tidak sah. Oleh karena itu, perlu mempertimbangkan prinsip-prinsip hukum internasional yang ada, seperti kedaulatan negara, non-intervensi, dan tanggung jawab pelaku non-negara, guna memastikan perlindungan hak dan keamanan di dunia siber

Kesimpulan

Secara keseluruhan, isu Cyber Espionage merupakan tantangan serius dalam hukum internasional yang belum memiliki regulasi khusus. Tindakan ini memanfaatkan ruang siber untuk mengakses dan mencuri data, yang melibatkan sejumlah aspek hukum internasional. Meskipun belum ada aturan yang secara tegas mengatur Cyber Espionage, prinsip-prinsip hukum internasional seperti kedaulatan negara, non-intervensi, serta tanggung jawab pelaku non-negara menjadi relevan. Sumber hukum internasional seperti traktat internasional, Konvensi tentang Kejahatan Siber, dan hukum kebiasaan menjadi dasar dalam menilai tindakan Cyber Espionage. Perlindungan hak dan keamanan di ruang siber perlu menjadi perhatian utama dalam menghadapi ancaman ini dan mengembangkan instrumen hukum yang relevan.

Referensi

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 (Edisi Kelima). Stevens and Sons Limited.

Sudiro, A., & Marton. (2017). The Suppression of Hijacking and Other Crimes Involving Indonesian Aviation Activities. Dalam Indonesia, Aviation Laws and Regulations Applicable in (hlm. 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.

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.

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

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

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/