BAB V

ANALISIS

5.1. Strategi Indonesia dalam Menangani Cybercrime Berdasarkan Hukum Negara

Akibat dari maraknya kasus *cybercrime* yang terus meningkat setiap tahunnya di Indonesia tentu memberikan dampak negatif di berbagai aspek kehidupan terutama aspek keamanan negara. Tindak pidana *cybercrime* terbukti dapat merugikan korban dalam jumlah yang banyak, terutama dalam hal keuangan, baik pribadi maupun perekonomian negara. Sebagian dari para korban memang ada yang mengikhlaskan perihal tindak kejahatan yang sudah terjadi dengan tidak melaporkannya ke pihak yang berwajib, namun bukan berarti hal tersebut tidak menjadi sebuah 'perhatian' baru untuk negara dan lembaga-lembaga nasional maupun internasional lainnya.[1] Salah satu penyebab dari tingginya angka kejahatan dalam *cyberspace* di Indonesia adalah lemahnya hukum dan kebijakan yang berlaku dalam hal pengamanan dan penanganan kasus *cybercrime* ini. Hal ini juga dipertambah dengan kecilnya kemungkinan penangkapan pelaku serta kemajuan teknologi yang terus berkembang pesat yang akan terus memberikan kemudahan bagi para pelaku dalam melakukan aksi kejahatannya.

Dalam subjeknya, *cybercrime* tidak hanya sebuah perdebatan politik dan hukum, dasar penelitian untuk teknologi, sosiologis maupun ekonomi, namun juga masalah yang menyangkut semua orang dan tidak dapat dipahami jika hanya

[1] Dista Amalia Arifah. Kasus Cybercrime di Indonesia. *Jurnal Bisnis dan Ekonomi*, *18*(2). 2011. Hlm. 189-190

berdasar pada satu perspektif atau dilihat dari satu dimensi tunggal saja. Hanya dengan melalui pendekatan interdisipliner terhadap fenomena *cybercrime* yang dapat memahami apa saja yang diperlukan guna melakukan tindakan pencegahan dan memberikan respon aktif yang tepat. Tantangan dalam memerangi *cybercrime* secara efektif juga pasti membutuhkan posisi politik yang kuat guna menyatukan badan-badan publik dan swasta serta dapat memobilisasikan mereka untuk dapat bekerjasama baik secara nasional maupun internasional. Sejatinya, dalam menanggulangi *cybercrime* harus dengan menggunakan pendekatan yang sesuai dengan sumber serangan yang sedang dihadapi. Beberapa bentuk penanggulangan kasus *cybercrime* agar tidak semakin marak terjadi diantaranya dengan melakukan:[2]

1. **Penanganan siber** (*cyber defense*), sebagai upaya dalam menangani segala bentuk serangan *cyber* yang dapat menyebabkan terjadinya gangguan pada setiap kegiatan.
2. **Penanganan hukum** *(cyber law*), sebagai dasar tindakan dan peringatan yang dilakukan melalui koordinasi aparat keamanan negara apabila diketahui telah terjadi tindak kejahatan siber (*cybercrime*).
3. **Serangan balik siber** (*cyber counter-attack*), dijadikan sebagai suatu tindakan menyerang balik sumber serangan kejahatan agar dapat menimbulkan efek jera bagi para pelaku kejahatan.

[2] Kementerian Pertahanan Indonesia. Pedoman Pertahanan Siber. *Jakarta: Kemhan RI*. 2014

Dalam melakukan upaya pertahanan siber, Kementerian Pertahanan dan Tentara Nasional Indonesia memiliki dua kepentingan utama, yakni Pertama; berupaya untuk melindungi semua sistem elektronik dan jaringan informasi di lingkungan, dan Kedua; berupaya untuk mendukung koordinasi keamanan siber di sektor lain sesuai dengan kebutuhan. Adapun beberapa aspek yang perlu diperhatikan berdasar dari dua kepentingan sebelumnya guna memperlancar upaya pertahanan siber, diantaranya:[3]

1. **Kebijakan**

   Sangat penting untuk dapat mengembangkan dan menerapkan kebijakan-kebijakan yang akan menjadi dasar atau acuan bagi segala kegiatan pertahanan siber, termasuk pengembangan, operasi dan koordinasi. Kebutuhan ini perlu diwujudkan dalam bentuk regulasi, kebijakan, petunjuk teknis dan bentuk kebijakan lainnya yang dapat memastikan kegiatan *cyber defence* berjalan dengan baik. Saat ini rancangan kebijakan pertahanan siber di Indonesia sudah mulai disusun dan akan terus dikembangkan serta diimplementasikan pada tahap berikutnya. Kebijakan ini juga dimaksudkan untuk membantu pemerintah mempersiapkan, mengembangkan, melatih dan mengoperasikan pertahanan siber di masa depan.

[3] *Ibid*. Hlm. 15-17

2. **Kelembagaan**

Diperlukannya lembaga yang kuat dan efektif untuk dapat melaksanakan segala tugas dan kegiatan terkait pertahanan siber dengan mengacu pada kebijakan yang telah ditetapkan. Hal ini termasuk dalam struktur organisasi, pembagian tugas dan kompetensi, serta mekanisme kerja dan kontrol. Saat ini, kelembagaan di Indonesia terbilang masih mendukung teknologi informasi umum dan tidak mendukung persyaratan pertahanan siber yang lebih spesifik. Namun, adapun langkah-langkah yang telah diambil untuk membentuk badan pertahanan siber yang terdiri dari penambahan tugas dan fungsi pertahanan siber ke dalam struktur yang sudah ada.

3. **Teknologi dan Infrastruktur Pendukung**

Sebagai peralatan dan fasilitas untuk melakukan kegiatan pertahanan siber, diperlukannya teknologi dan infrastruktur pendukung yang lengkap guna dapat melaksanakan pertahanan siber secara lebih efektif dan efisien. Teknologi dan infrastruktur pendukung ini harus dicapai melalui sebuah penelitian pengembangan dan langkah-langkah persiapan selanjutnya, serta pembentukan, adaptasi dan/atau peningkatan teknologi dan infrastruktur yang dapat digunakan secara optimal. Teknologi dan infrastruktur pendukung yang tersedia di Indonesia saat ini bersifat

umum dan khusus untuk mendukung pertahanan siber dan masih dalam proses penyempurnaan.

4. Sumber Daya Manusia

Departemen sumber daya manusia adalah salah satu faktor terpenting dalam memastikan bahwa pertahanan siber dapat diterapkan sesuai dengan kebijakan atau pedoman yang telah ditetapkan. Pengetahuan dan keterampilan pertahanan siber tertentu perlu diperoleh dan dipelihara seiring dengan berkembangnya persyaratan pertahanan siber. Sumber daya manusia ini dapat diperoleh melalui program rekrutmen, pembinaan dan pemisahan terkait dengan peraturan yang berlaku. Di Indonesia saat ini sudah memulai persiapan penyediaan Sumber Daya Manusia dalam rangka dukungannya terhadap pertahanan siber, namun hal ini baru sebuah persiapan awal yang berupa program *awareness* dan peningkatan tentang pengetahuan serta keterampilan di bidang keamanan informasi. Dalam mengimplementasikan pertahanan siber di masa depan tentu akan membutuhkan program peningkatan SDM yang jauh lebih besar dan substansial.

Aspek dan kepentingan tersebut diatas merupakan upaya-upaya pemerintah dalam menghadapi ancaman *cybercrime* terutama dalam keamanan nasional yang tertuang dalam Peraturan Kementerian Pertahanan Nomor 82 Tahun 2014 tentang pedoman pertahanan siber. Peraturan tersebut merupakan satu-satunya peraturan

yang menjelaskan definisi dari keamanan siber. Keamanan siber nasional mencakup kerahasiaan, integritas, ketersediaan informasi dan segala upaya dalam melindungi lembaga-lembaga pendukung dari adanya serangan siber pada tingkat nasional. Segala macam bentuk perkataan dan tindakan dari pihak-pihak yang mengancam pertahanan, kedaulatan serta keutuhan wilayah akan dianggap sebagai sebuah serangan siber. Namun, peraturan ini hanya berlaku untuk pengembangan kemampuan pertahanan siber yang ada di dalam lingkup militer dan hanya akan dilaksanakan oleh Kementerian Pertahanan dan Tentara Nasional Indonesia. Sedangkan untuk bentuk ancaman siber yang bersifat non-militer, akan direferensikan kepada peraturan atau kebijakan hukum lainnya.[4]

Sejatinya terdapat dua jenis hukum pada setiap negara, yakni undang-undang dan kasus. Undang-undang sendiri merupakan jenis hukum yang telah disahkan oleh seorang legislator baik di negara bagian ataupun pemerintah negara. Sedangkan kasus merupakan hukum yang sebagaimana seorang hakim mencari fakta dan telah menafsirkannya pada hukum perundang-undangan dalam tindakan pengadilan yang sebenarnya.[5] Akan tetapi, di Indonesia belum memiliki kebijakan dan Undang-undang khusus atau *cyber law* yang mengatur segala bentuk tindakan *cybercrime,* melainkan hanya perumpamaan terhadap pasal-pasal dari kebijakan hukum yang berkaitan dengan teknologi informasi secara umum.

---

[4] Noor Halimah Anjani. *Op.cit.* Hlm. 4

[5] Peter Stephenson and Keith Gilbert. *Investigating Computer-Related Crime*. Florida: CRC Press. 1999.

Kebijakan hukum tersebut tertuang dalam beberapa pasal yang ada di dalam Kitab Undang-undang Hukum Pidana (KUHP). Terkhusus untuk kasus kejahatan penipuan online, pemerasan ataupun pengancaman, pasal-pasal yang dikenakan diantaranya adalah Pasal 378, 368 dan 369 KUHP. Pasal 378 KUHP mengatur tentang segala macam tindakan penipuan dengan maksud untuk mengambil keuntungan sendiri atau orang lain dengan menipu, merangkai kebohongan dan membuat orang lain menyerahkan sesuatu barang kepadanya akan dikenakan sanksi pidana penjara maksimal empat tahun. Pasal 368 KUHP mengatur tentang tindakan pemerasan dengan mengancam kekerasan agar dapat memberikan seluruh atau sebagian barang yang orang tersebut atau orang lain punya akan dikenakan sanksi pidana penjara maksimal sembilan bulan. Sedangkan Pasal 369 KUHP mengatur tentang segala bentuk ancaman pencemaran baik secara lisan maupun tulisan akan dikenakan sanksi pidana penjara maksimal empat tahun.[6]

Melalui pasal-pasal hukum pidana tersebut, para pelaku tindakan *cybercrime* akan dikenakan sanksi hukuman dengan melihat tingkatan kejahatan yang dilakukannya terlebih dahulu. Namun selain itu, ada pula Undang-undang khusus yang mengatur tentang Informasi dan Transaksi Elektronik (ITE) yakni UU ITE No.11 Tahun 2008 dan/atau telah diubah menjadi UU No.19 Tahun 2016. Ini menjadi Undang-undang paling utama yang akan dijadikan aturan dasar dalam menangani segala kasus *cybercrime* yang terjadi di Indonesia, khususnya pada Pasal 27 sampai 37 yang mengatur tentang perbuatan yang dilarang. Undang-

[6] Mahkamah Agung. *KUHP (Kitab Undang-undang Hukum Pidana): Buku Kesatu*. 2021. Diakses melalui <https://jdih.mahkamahagung.go.id> pada 3 Juni 2022

undang tersebut berisi aturan-aturan untuk beberapa jenis pelanggaran kejahatan atau tindak pidana yang dapat mengancam sistem komputer atau elektronik lain serta memberikan perlindungan hukum terhadap isi sistem elektronik dan transaksi elektronik. Namun, Undang-undang ini tidak mencakup aspek-aspek penting dari keamanan siber seperti infrastruktur informasi dan jaringan serta sumber daya manusia yang memiliki keahlian di bidang keamanan siber.[7]

Lebih lanjut, adapun aturan yang terkandung pada UU ITE terkait tindakan penipuan online telah diatur dalam Pasal 28 ayat 1 yang mengatakan bahwa *"Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik"* akan dikenakan sanksi hukum pidana penjara maksimal enam tahun dan/atau membayar denda maksimal satu miliar rupiah sebagaimana telah diatur dalam Pasal 45 ayat 2. Sedangkan untuk tindakan pemerasan diatur dalam Pasal 27 ayat 4 yang mengatakan bahwa *"Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman"* akan dikenakan sanksi hukum pidana penjara maksimal enam tahun dan/atau membayar denda maksimal satu miliar rupiah sebagaimana telah diatur dalam Pasal 45 ayat 1. Serta Pasal 29 yang mengatur tindakan pengancaman dikatakan bahwa *"Setiap orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi"* akan

[7] Noor Halimah Anjani. *Loc.Cit.*

dikenakan sanksi hukum pidana penjara paling lama dua belas tahun dan/atau membayar denda maksimal dua miliar rupiah sebagaimana telah diatur dalam Pasal 45 ayat 3.[8]

Secara khusus, di Indonesia sendiri telah memiliki kebijakan yang telah diinisiasi sejak tahun 2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet yang kemudian direvisi dengan Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMINFO/10/2010 yang kemudian diperbarui lagi menjadi No.29/PER/M.KOMINFO/12/2010. Salah satu yang diatur dalam kebijakan tersebut ialah dengan dibentuknya ID-SIRTII, yang merupakan kepanjangan dari *Indonesia Security Incident Response Team on Internet Infrastructure*. ID-SIRTII merupakan tim yang ditugaskan oleh KOMINFO untuk membantu pengawasan keamanan jaringan telekomunikasi berbasis protokol internet.[9] Tugas dan fungsi dari dibentuknya ID-SIRTII ialah untuk melakukan pemantauan, pendeteksian dini, peringatan dini terhadap ancaman dan gangguan jaringan. Selain itu juga berkoordinasi dengan beberapa pihak terkait baik di dalam atupun luar negeri dalam menjalankan tugas pengamanan jaringan telekomunikasi.

Pada 2019, Pemerintah juga mengeluarkan sebuah peraturan teknis yang tertuang dalam Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Peraturan Pemerintah ini

[8] Dewan Perwakilan Rakyat Republik Indonesia. Undang-undang Republik Indonesia Nomor 11 Tahun 2008. Diakses melalui <https://www.dpr.go.id> pada 3 Juni 2022
[9] Handrini Ardiyanti. *Op.Cit*. Hlm. 99

didasari oleh UU ITE Tahun 2016 terkait penyelenggaraan *cybersecurity* pada sistem dan transaksi elektronik. Dalam PP No.71 Tahun 2019 memuat aturan yang lebih kuat mengenai perlindungan data dan informasi pribadi serta autentikasi *website* untuk menghindari adanya laman *web* palsu yang berujung penipuan. Selain itu, dalam peraturan tersebut juga ditekankan bagi pemerintah untuk dapat mencegah terjadinya kerugian bagi masyarakat umum dari penyalahgunaan informasi dan transaksi elektronik, serta perlunya menyusun strategi keamanan siber nasional. Namun akibat terbatasnya cakupan UU ITE dan PP No.71 Tahun 2019, membuat pemerintah Indonesia kurang memberikan respon aktif atas ancaman siber yang terus meningkat dan berkembang, terutama terhadap infrastruktur penting pemerintah.[10]

5.2. Strategi Australia Dalam Menangani Cybercrime

Sama halnya seperti Indonesia, Australia juga menjadi negara pengguna internet paling tinggi di kawasan Oceania. Berdasarkan data per 31 Desember 2020, Australia telah mencapai 21,711 juta jiwa yang menggunakan internet dan teknologi informasi dari total populasi sebanyak 25,788 juta jiwa atau ada sekitar 84,2% dari seluruh penduduk di Australia telah menggunakan internet pada setiap kegiatan hariannya. Dengan sama-sama memiliki banyak pengguna internet aktif yang akan terus berkembang, menjadikan Australia juga sebagai negara dengan potensi terkena ancaman *cyber* yang cukup tinggi. Umumnya pada sektor bisnis atau *e-commerce* serta *website* resmi pemerintah Australia yang kerap dijadikan salah satu target utama serangan. Hal tersebut tentu menjadi suatu perhatian khusus

[10] Noor Halimah Anjani. *Loc.Cit.*

bagi Australia untuk memerangi tindakan *cybercrime* yang terjadi di negaranya. Dengan menerapkan berbagai kebijakan untuk melindungi aset di dalam *cyberspace*, *cybersecurity* tentu menjadi salah satu kebijakan terpenting bagi Pemerintah Australia.

Upaya pertahanan yang dilakukan oleh organisasi maupun lembaga pemerintah merupakan suatu tanggung jawab negara dalam memelihara infrastruktur nasional. Utamanya, hal-hal yang bergantung pada kegiatan komando dan operasional. Namun, dalam hal keamanan *cyber*, bentuk pertahanan saja bukanlah sebuah otoritas utama.[11]Perlu adanya peningkatan kesadaran akan risiko dari praktik *cyber* yang lemah, karena hal tersebut akan menjadi kunci untuk memastikan bahwa *cybersecurity* merupakan bagian dari prioritas seluruh negara. Selain karena dampak serangan *cyber* yang dapat tertuju pada sektor bisnis maupun individu, ada pula potensi gangguan yang dapat ditimbulkan oleh serangan *cyber* tersebut terhadap kepercayaan Australia terhadap teknologi informasi dan komunikasi baik secara individu ataupun kelompok.

Cybersecurity ini harus dilihat sebagai sebuah upaya kolektif bagi negara karena tidak ada suatu organisasi yang dapat mengatasi semua masalah dengan satu teknologi dan memenuhi semua harapannya. Disisi lain, Australia juga membagi tugas terkait penanganan *cybersecurity* secara horizontal antara Pemerintah Federal dan Negara Bagian. Karena itu, Pemerintah Australia akhirnya menciptakan

[11] Desmond Ball. *An Australian Cyber-warfare Centre; In Australia and Cyber-warfare*, Australia: ANU Press. 2011, Hlm. 121

beberapa peran yang berbeda-beda guna menangani *cybersecurity* di negaranya, diantaranya yakni:[12]

- **Peran pertama** adalah peran yang dilakukan oleh Pemerintah Federal Australia dengan empat tanggung jawab yakni membuat, menerapkan dan menegakkan hukum, aturan dan kebijakan terkait *cybersecurity*. Kemudian, perlunya berkontribusi pada setiap *cybersecurity* global guna meningkatkan koordinasi dan kolaborasi dalam menghadapi ancaman *cyber*. Selain itu kita juga perlu menyediakan kebijakan publik yang dapat digunakan sebagai alat untuk menyelidiki aktivitas kejahatan dunia maya. Terakhir, dengan memberikan referensi, rekomendasi dan keterampilan operasional untuk mengidentifikasi dan mendeteksi adanya ancaman *cyber*.
- **Peran kedua** adalah peran yang dilakukan oleh negara serta wilayah pemerintah. Pada prinsipnya, memiliki misi yang sama dengan pemerintah federal. Perbedaannya hanya pada pemerintah negara bagian dan teritorial hanya terfokus pada anggota dari wilayah mereka saja. Di sebagian yurisdiksi, *cybersecurity* untuk pribadi maupun perusahaan merupakan masalah utama bagi departemen kepolisian setempat. Departemen kepolisian ini lebih terfokus pada identifikasi, penyelidikan dan penuntutan pada para pelaku *cybercrime*. Tentu hal tersebut menjadi sebuah tanggung jawab yang lebih besar bagi pemerintah negara bagian dan teritorial, terlebih

[12] P.D. Persadha, A.A. Waskita & S. Yazid. *Op.cit.* Hlm. 147-148

pada proses memberikan edukasi kepada masyarakat terutama para remaja dan anak-anak terkait bahaya ancaman *cyber* serta cara mengatasinya.

- **Peran ketiga** adalah peran yang dilakukan oleh ISP (*Internet Service Provider*). Hal ini dikarenakan peran dan tanggung jawabnya yang cukup penting dalam menyediakan layanan internet dan jalur komunikasi yang aman bagi penggunanya untuk setiap kegiatan transaksi baik yang legal maupun ilegal. Salah satu langkah spesifik yang telah dilakukan oleh ISP terkait *cybersecurity* adalah dengan menolak situs web yang berisi konten yang tidak pantas seperti pelecehan anak. Mereka juga kerap melakukan identifikasi, memberikan informasi serta memberikan dukungan dan rekomendasi untuk perbaikan perangkat lunak berbahaya yang dapat mempengaruhi komputer.
- **Peran keempat** adalah peran yang dilakukan oleh pemilik dan pengelola sistem ICT (*Information and Communication Technology*), baik untuk individu maupun perusahaan. Kelompok ini berperan penting karena dapat menerapkan sistem *cybersecurity* dalam fasilitasnya. Jika masing-masing dari mereka telah berhasil menerapkan sistem *cybersecurity* yang kuat, maka perangkat lunak berbahaya sekalipun tidak akan dengan mudah menyebar dan merusak ke seluruh sistem.

Selain beberapa lembaga dan kelompok tersebut diatas, Australia juga memiliki lembaga organisasi lainnya yang dirancang khusus untuk menjaga *cybersecurity* negara. Salah satunya adalah *Australian Cyber Security Centre (*ACSC) bersama *Australian Signals Directorate* yang hadir untuk memimpin upaya Pemerintah Australia dalam menjaga *national cybersecurity.* Kedua lembaga ini didirikan guna mengintegrasikan kemampuan *cybersecurity* yang berada di seluruh Pemerintahan Australia, meningkatkan ketahanan *cyber* komunitas Australia serta membantu menjadikan Australia sebagai negara paling aman untuk terhubung secara online. ACSC sendiri merupakan pusat kolaborasi sektor swasta dan publik yang menjadikannya tempat berbagi informasi tentang *cybersecurity* guna mencegah, menanggapi sekaligus meminimalisirkan adanya ancaman bahaya *cyber* terhadap warga Australia. Lembaga ini juga kerap memberikan saran dan dukungan untuk perekonomian secara keseluruhan, termasuk infrastruktur penting dan sistem kepentingan nasional, federal, negara bagian, lokal, usaha kecil dan menengah, pendidikan tinggi, organisasi nirlaba serta komunitas Australia.

Lebih spesifik lagi, ACSC memiliki strategi dalam berperan untuk; Merespon ancaman dan *cybersecurity* sebagai Australia's *Computer Emergency Response Team* (CERT); Berkolaborasi dengan sektor swasta dan publik untuk berbagi informasi terkait ancaman serta meningkatkan keamanan; Bekerja sama dengan pemerintah, industri dan masyarakat guna meningkatkan kesadaran akan *cybersecurity*; serta Memberikan informasi, saran dan bantuan *cybersecurity*

kepada semua masyarakat Australia.[13] Strategi tersebut tentu menjadi keputusan yang sangat ditunggu oleh masyarakat, karena setidaknya Australia telah mendapatkan kembali visi yang jelas dan telah memperbarui jalur yang jauh lebih relevan. Adapun hasil strategi yang telah dipartisi menjadi enam portofolio berbeda, yakni: Pertahanan, Jaksa Agung, Industri, Inovasi dan Ilmu, Pengetahuan, Urusan Luar Negeri dan Perdagangan, Pendidikan dan Pelatihan.

Hingga pada April 2016, Strategi *cybersecurity* Australia baru akhirnya diterbitkan. Strategi ini dirancang guna mengatasi beberapa masalah yang terus-menerus terjadi terutama dalam hal kepemimpinan. Secara jelas Departemen Perdana Menteri, Departemen Kejaksaan Agung dan Kabinet diidentifikasi sebagai 'pusat kebijakan'. Strategi ini juga akan ikut membantu meningkatkan investasi di CERT Australia dengan mengakui kontribusi yang dibuat oleh pihak CERT. Hal yang dimaksud diantaranya yakni; menciptakan 'Duta *cyber*' baru guna mengadvokasi internet yang terbuka, bebas dan aman; Mengusulkan pusat baru untuk berbagi informasi atau berkolaborasi dengan bisnis dan komunitas riset; serta merelokasi ACSC untuk meningkatkan keterlibatan dengan sektor swasta. Australia memandang bahwa dari seluruh langkah-langkah strategi tersebut dapat meningkatkan kebijakan dan operasi yang sama.[14] Kini Australia berfokus pada strategi *cyber policy dialogue* yang menjunjung tinggi nilai-nilai Australia dalam menciptakan masa depan *cyberspace* yang terbuka, bebas dan aman. Dengan

[13] Australian Government: *Australian Signals Directorate*. Cyber Security. Diakses melalui, <https://www.asd.gov.au> pada 3 Juni 2022

[14] Frank Smith, & Graham Ingram. Organising cyber security in Australia and beyond. *Australian Journal of International Affairs*, *71*(6), 642-660, 2017. Hlm.13

dirancangnya penunjukkan ‘Duta *cyber*’ juga dipandang dapat memberikan bantuan yang cukup pesat dalam meningkatkan profil dan pengaruh Australia dalam *global dialogue* perihal norma-norma dunia maya.

Selain membuat lembaga khusus penanganan *cybersecurity*, Australia juga memiliki beberapa landasan hukum pidana terkait dengan pelanggaran komputer dan/atau penyelenggaraan komputer layaknya Indonesia. Namun, tidak ada Undang-undang khusus yang mengatur segala macam tindak *cybercrime*, melainkan hanya sebuah Undang-undang dasar yang mengatur kejahatan terkait pelanggaran *cybercrime* atau segala hal yang dapat mengancam kerusakan, gangguan sistem komputer maupun elektronik lainnya. Peraturan tersebut tertuang dalam Australia *Criminal Code* 1995 (Undang-undang KUHP 1995) khususnya pada bagian 10.7 Pasal 477-478 tentang pelanggaran komputer serius dan pelanggaran komputer lainnya. Pasal 477.2 mengatur tentang segala macam tindakan pemodifikasian data ilegal yang menyebabkan penurunan nilai dan dengan sengaja merusak akses data yang disimpan akan dikenakan sanksi pidana maksimal sepuluh tahun penjara. Pasal 478.1 mengatur tentang tindakan pelanggaran akses ilegal, memodifikasi dan pembatasan data akan dikenakan sanksi pidana maksimal dua tahun penjara. Pasal 478.3 mengatur tentang kepemilikan atau kendali kontrol data dengan maksud untuk melakukan perusakan sistem komputer dan/atau memegang kendali data untuk digunakan kembali oleh orang tersebut atau orang lain akan dikenakan hukum pidana maksimal tiga tahun penjara.

Karena luasnya peraturan Undang-undang yang dimiliki Australia terhadap serangan sistem komputer dan elektronik lainnya menjadikan Australia

memberikan tugas yang berbeda-beda pada setiap lembaga maupun kelompok guna dapat menangani *cybersecurity.* Pemerintah Federal yang ditugaskan untuk memegang tanggung jawab dalam membuat aturan,undang-undang dan kebijakan terkait *cybersecurity* untuk seluruh negara bagian. Sedangkan tugas untuk Pemerintah Negara Bagian diberikan tanggung jawab untuk dapat melaksanakan dan menegakkan segala aturan-aturan, hukum serta kebijakan yang telah dibuat.

5.3. Implementasi Program *Cyber Policy Dialogue* Terhadap Penanganan Kasus Penipuan Online di Indonesia

Upaya Indonesia dalam menangani kasus *cybercrime* atau kejahatan dunia maya yang masuk kedalam kategori tindak kejahatan pidana memang terbilang sudah cukup baik. Pemerintah Indonesia menciptakan landasan perlindungan hukum bagi setiap masyarakat yang menjadi korban sekaligus pihak yang dirugikan atas tindak kejahatan tersebut. Diberlakukannya beberapa pasal yang terkandung dalam Undang-undang Republik Indonesia (UU RI) dan Kitab Undang-Undang Hukum Pidana (KUHP) menjadi salah satu upaya Indonesia dalam menangani kasus *cybercrime*. Selain dengan menerapkan hukum-hukum pidana tersebut, Indonesia juga kerap melakukan upaya lainnya guna meminimalisir kasus serta meningkatkan keamanan negara dari bahaya *cybercrime*.

Kerjasama internasional menjadi pilihan Indonesia dalam merealisasikan salah satu strategi BSSN yang menjadi satu-satunya lembaga organisasi khusus penanganan segala bentuk tindakan *cybercrime* di Indonesia. Strategi BSSN yang dimaksud adalah dengan melakukan pendekatan dan menjalin kerjasama terhadap

lembaga-lembaga yang relevan guna mengoptimalkan upaya dan kinerja BSSN. Kerjasama tersebut tidak hanya akan dilakukan dengan instansi pemerintahan saja, namun juga dengan pihak lainnya seperti universitas, lembaga penelitian, komunitas dan/atau organisasi masyarakat yang relevan dengan segala hal tentang ruang dunia maya (*cyberspace*) serta teknologi dan informasi, baik di Indonesia maupun di luar negeri.[15] Sejalan dengan strategi tersebut, Indonesia diketahui menjalin kerjasama dengan Australia dalam hal menjaga keamanan siber atau *cybersecurity*.

Keduanya sepakat untuk menjalankan kerjasama dalam bidang hukum dan keamanan dikarenakan adanya peningkatan interkonektivitas pada sistem informasi yang diduga dapat memberikan dampak negatif berupa ancaman kesejahteraan masyarakat dan keamanan negara. Dalam pandangan teori kerjasama internasional, Indonesia dan Australia terlihat memiliki kepentingan dan tujuan yang sama dalam bidang hukum dan keamanan nasional. Setiap negara pasti akan selalu mengutamakan kepentingan nasionalnya masing-masing, namun tidak jarang pula ada negara-negara yang merasa tidak mampu dalam mewujudkan kepentingannya tersebut. Maka dari itu, diperlukannya suatu kerjasama internasional guna dapat merealisasikan kepentingan nasionalnya dengan mudah.

Oleh karenanya, tindakan yang diputuskan Indonesia dan Australia merupakan salah satu tindakan yang tepat untuk dilakukan, mengingat kepentingan dan tujuan dari kedua negara yang sama-sama ingin memperkuat sistem keamanan

[15] BSSN. Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018 – 2019. 2018. Hlm.39

negara dalam menghadapi ancaman *cybercrime* yang memungkinkan mengalami peningkatan di era serba digital ini. Selain itu, kesepakatan dalam membuat MoU ini juga di dasari oleh prinsip-prinsip kesetaraan dan timbal balik yang diharap akan memberikan kontribusi baik yang saling menguntungkan serta memelihara hubungan persahabatan antar kedua negara. Ketika hendak memutuskan untuk meningkatkan perlindungan keamanan, tentu perlu diimbangi dengan besarnya risiko yang akan di hadapi. Dalam *cybersecurity*, beberapa risiko yang sangat erat kaitannya adalah tentu dengan pemrosesan informasi, sistem komputer, alat telekomunikasi dan segala hal yang berkaitan dengan penggunaan internet.

Namun adapula risiko yang perlu diperhatikan, seperti risiko dalam hal keuangan atau biaya yang diperlukan untuk menunjang langkah-langkah keamanan yang diinginkan. Minimal, suatu organisasi harus dapat mengidentifikasi apa saja aset yang akan dilindungi beserta dengan alasannya. Risiko sendiri sejatinya dapat diartikan sebagai bahaya yang dapat diantisipasi dengan mengukur kemungkinan kerusakan dan kerugian yang diakibatkannya kelak. Hal ini dikarenakan terbentuknya suatu strategi pasti akan bergantung pada kendala aktual dan sumber daya organisasi, keuangan, manusia dan teknis yang dimiliki. Maka dari itu, langkah-langkah yang hendak diambil oleh suatu negara atau organisasi haruslah efektif dan mencerminkan keseimbangan antara kinerja dan efektivitas biaya guna dapat mencapai strategi yang dituju dengan baik.[16]

[16] Solange Ghernaouti-Helie. *Op.cit.* Hlm 362-363

Berdasarkan MoU yang telah disepakati ada beberapa rencana kegiatan yang akan dilaksanakan guna mewujudkan keamanan bagi masing masing negara dari ancaman siber, salah satunya dengan diadakannya *cyber policy dialogue*. Program *dialogue* ini sejatinya merupakan suatu forum diskusi antara anggota peserta perwakilan Indonesia dan Australia dalam meningkatkan strategi *cybersecurity*. Hal ini juga menjadi salah satu upaya bagi kedua negara untuk menunjang keberlangsungan kegiatan-kegiatan praktik yang hendak dilakukan selama masa kerjasama berlangsung. *Cyber policy dialogue* ini diadakan setiap tahun sejak penandatangan MoU dengan saling bertukar pandangan serta mengevaluasi hasil kegiatan kerjasama yang telah dijalankan oleh pihak BSSN dan DFAT sebagai ketua pelaksana dari masing-masing negara.

Jika di analisis dengan kasus *cybercrime* yang terjadi di Indonesia, utamanya pada tahun 2018 hingga 2020, program *cyber policy dialogue* ini cukup memberikan hasil yang positif dalam menunjang kinerja Indonesia, khususnya bagi Polri dan BSSN dalam menangani kasus *cybercrime*. Akan tetapi, program *cyber policy dialogue* ini memang tidak memberikan implementasinya secara langsung pada setiap kasus *cybercrime* yang terjadi di Indonesia. Melainkan, hanya dengan memberikan kebebasan dalam pembentukan pengaturan pelaksanaan tertulis yang dapat ditentukan bersama. Hal tersebut sebagaimana yang dijelaskan pada MoU Indonesia dan Australia dalam kerjasama *cyber*, yakni pada *paragraph* 5 tentang *Implementing Arrangements* yang berbunyi:[17]

[17] *Memorandum of Understanding Between The Government of The Republic of Indonesia and The Government of Australia on Cyber and Emerging Cyber Technology Cooperation.*

1. *Relevant institutions of the participants may arrange between themselves the establishment of implementing arrangements, or other mutually determined written arrangements, under this MoU.*
2. *The arrangements mutually determined upon by the relevant institutions of the participants will serve to implement the scope of cooperation.*
3. *The establishment, finalization and implementation of the arrangement under this MoU will be coordinated and by consent of the respective focal points as stipulated in Term 4 of this MoU.*

Para anggota peserta *cyber policy dialogue* berpendapat bahwa pentingnya untuk menjalin kerjasama internasional, baik yang melibatkan pemerintah, organisasi internasional, industri perusahaan di bidang teknologi serta peran lembaga penegak hukum negara yang mampu menangani suatu tindak kejahatan yang dapat merugikan berbagai pihak.[18] Jika ada suatu tindak kejahatan yang terjadi pada masyarakat disuatu negara, pastinya akan ada peran dari lembaga penegak hukum yang tidak lepas untuk berupaya membantu menyelesaikan permasalahan tersebut. Seperti halnya yang dilakukan oleh Kepolisian Negara Republik Indonesia (Polri) bersama dengan Kepolisian Federal Australia (AFP). Keduanya ikut andil dalam program kerjasama peningkatan *cybersecurity* melalui penegakan hukum, pengembangan sumber daya manusia dan peralatan serta praktik pelatihan penanganan kasus *cybercrime*.

[18] Dhiyanka Magrisa. *Op.cit.* Hlm. 8

Hubungan Polri dan AFP berawal dari kerjasama yang dilakukannya sejak 2002 dengan berfokus pada penanganan kasus kejahatan terorisme dan kejahatan transnasional. Akan tetapi, hingga kini keduanya masih menjalin hubungan baik serta memperluas cakupan perlindungan dari kejahatan termasuk *cybercrime.* Terbukti dengan dibangunnya gedung *Transnational Crime Coordination Centre* (TNCC) dan laboratorium *Cybercrime Investigations Satellite* (CCIS). Hal ini sejalan dengan salah satu langkah strategi dalam lingkup kerjasama yang telah disepakati oleh Indonesia dan Australia di dalam MoU tentang *sharing information*. TNCC berperan sebagai tempat pengumpulan analisis dan pertukaran informasi dan/atau dengan kata lain, TNCC ini dijadikan sebagai sebuah jaringan informasi antara Polri dan AFP dalam menangani *cybercrime* dan kejahatan transnasional lainnya. Sedangkan laboratorium CCIS ditujukan untuk mendeteksi pendanaan jaringan teroris yang selama ini diterima dengan baik. Polisi kemudian dapat menggunakan satelit tersebut untuk melacak dan mendeteksi adanya jaringan teroris di suatu tempat berdasarkan cara komunikasi yang biasa dilakukan melalui email atau SMS.[19]

Walaupun Indonesia telah melakukan kerjasama dengan Australia dalam hal penanganan cyber, kasus-kasus *cybercrime* yang terjadi di Indonesia nantinya akan tetap diawasi dan ditangani langsung oleh pihak Kepolisian RI. Hanya saja, pihak Kepolisian RI kini telah mendapatkan bantuan 'pengetahuan' mengenai *cybersecurity* guna mempermudah Indonesia menghadapi berbagai macam kasus

[19] Indri Noviyanti & Ahmad Jamaan. Kerjasama Kepolisian Negara Republik Indonesia Dan Kepolisian Federal Australia Menanggulangi Cybercrime di Indonesia. J*urnal Online Mahasiswa (JOM) Bidang Ilmu Sosial dan Ilmu Politik*, *1*(2), 2014. Hlm:7

cybercrime. Hal tersebut merupakan buah hasil dari program *cyber policy dialogue* yang memutuskan untuk menjalin pelatihan bersama antara Polri dan AFP. Mengenali dan mengevaluasi macam-macam bentuk kejahatan *cyber* menjadi salah satu contoh latihan dasar yang harus dimiliki oleh Kepolisian sebagai aktor pertama yang akan langsung berkaitan dengan berbagai kasus kejahatan di negara. Berdasarkan data laporan masyarakat atas kasus *cybercrime* yang terjadi di Indonesia, kasus penipuan online terbukti menjadi yang paling tertinggi dan sering terjadi hingga terus meningkat di setiap tahunnya. Penipuan online yang dimaksud dalam hal ini ialah jual beli online melalui *e-commerce* yang kerap dilakukan para pelaku untuk merampas hak orang lain (uang ataupun barang). Akibat kerugian besar yang didapat oleh korban, menjadikan masalah ini dapat ditindak lanjuti oleh pihak kepolisian karena kategorinya yang masuk ke dalam tindak pidana.

Dalam upayanya, pihak Kepolisian RI sendiri telah mengeluarkan anggaran hingga mencapai 43,53 miliar rupiah untuk menangani tindak pidana siber pada tahun 2020. Anggaran tersebut digunakan untuk mencapai stabilitas dan keamanan politik melalui perlindungan hak-hak professional, proporsional dan bertanggung jawab serta dukungan hak asasi manusia, khususnya di bidang keamanan *cyber*. Hasil dari kerjasama Polri dan AFP juga menjadikan Australia memberikan bantuan dana kepada Indonesia. Sebagaimana yang dijelaskan oleh Perdana Menteri Australia Scott Morrison, bantuan dana yang diberikan kepada Indonesia mencapai hingga 1,35 miliar dolar Australia atau setara dengan 13,3 triliun rupiah untuk

jangka waktu 10 tahun kedepan dalam upaya meningkatkan pertahanan keamanan *cyber* di Indonesia.[20]

Lebih lanjut lagi, kerjasama Indonesia dan Australia juga direalisasikan dengan memberikan dukungan berbasis teknologi bagi para anggota Kepolisian RI. Dukungan tersebut berupa berbagi pengetahuan atau ilmu tentang bagaimana cara menindaklanjut kasus-kasus *cybercrime*, yang mana pada awalnya Polri belum memiliki pengalaman bekerja dengan teknologi terbarui. Pada sektor sumber daya manusia dalam bentuk pelatihan atau *best practice*, Polri dan AFP memberikan pelatihan intensif kepada hakim, para pejabat serta aparat hukum negara lainnya guna dapat menangani *cybercrime* yang terjadi khususnya di Indonesia. Bantuan-bantuan tersebut jelas memberikan kemudahan bagi Polri dalam melakukan langkah-langkah investigasi ilmiah terhadap *cybercrime.*

Hingga pada tahun 2020 menjadi tahun dimana semua negara mengalami pandemi covid-19, termasuk Indonesia dan Australia. Dampak yang ditimbulkan tentu langsung kepada perekonomi negara yang menjadi lemah namun tinggi tingkat kebutuhannya. Karena hal itu pula menjadikan kasus cybercrime tetap memiliki angka yang tinggi terutama pada sektor jual beli online. Para peserta anggota *cyber policy dialogue* juga ikut menyatakan kepedulian yang mendalam terhadap meningkatnya frekuensi kejahatan dan aktivitas *cyber* yang dilakukan oleh para pelaku dengan terus memanfaatkan dan mengeksploitasi situasi pandemi covid-19

[20] Julkifli Sinuhaji. "Australlia Habiskan Dana Rp 13,3 Triliun Demi Keamanan Siber". *pikiranrakyat.com*. 30 Juni 2020. Diakses melalui, < https://www.pikiran-rakyat.com> pada 15 Juli 2022

hanya untuk keuntungan diri sendiri. Karenanya, kedua negara dirasa masih sangat perlu untuk terus menciptakan koordinasi internasional yang tepat guna dapat mencegah dan meminimalisir segala bentuk aktivitas *cyber* berbahaya agar tidak merusak perdamaian dan keamanan internasional.