BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Dalam beberapa dekade terakhir, dunia tengah dihadapi oleh fenomena globalisasi yang kian marak terjadi dan disertai dengan kemajuan teknologi informasi dan komunikasi yang terus berkembang pesat. Globalisasi biasanya diidentikkan dengan istilah '*global village'* yakni kondisi yang membuat batas antar negara menjadi pudar karena teknologi dan informasi. Globalisasi menurut salah satu ahli yaitu Tomlinson menjelaskan bahwa globalisasi merujuk kepada perkembangan yang cepat dan mendalam pada jaringan hubungan dan ketergantungan yang menjadi ciri kehidupan sosial modern.[1] Pembicaraan mengenai globalisasi pastinya mengacu pada kemajuan kehidupan yang dicapai masyarakat beserta dengan berbagai dampak yang ditimbulkannya. Hal ini tentu sangat berpengaruh pada setiap aspek kehidupan manusia dan telah menjadi sebuah kebutuhan hidup yang tak terlepaskan baik untuk kehidupan manusia pribadi ataupun organisasi. Dengan terus berkembanganya teknologi informasi dari masa ke masa membuat semua masyarakat dapat dengan mudah mengakses internet dan menggunakan media sosial dimana pun dan kapan pun serta dapat membantu kehidupan manusia menjadi lebih dinamis.

Hadirnya internet sebagai bagian dari bentuk teknologi baru akibat arus globalisasi menyebabkan manusia tidak dapat terlepas dari perkembangan

[1] Mohammad Maiwan. Memahami Politik Globalisasi dan Pengaruhnya Dalam Tata Dunia Baru: Antara Peluang dan Tantangan. *Pamator Journal*, *7*(1), 2014. Hlm. 2

informasi dan komunikasi dalam setiap kegiatannya. Hal ini mengartikan bahwa hadirnya internet telah merubah cara dan pola interaksi masyarakat dalam bertukar informasi dan berkomunikasi, yang awalnya dilakukan dengan cara bertemu langsung atau mengirim surat, kini semua dapat lebih mudah dilakukan karena terbantu oleh adanya teknologi internet. Perkembangan teknologi informasi dan komunikasi yang terus meningkat pesat membuat segala sesuatu menjadi lebih mudah untuk dilakukan, baik dalam menerima ataupun memberikan data dan informasi kepada individu, kelompok sampai antar negara. Tidak hanya negara maju saja yang terus mengembangkan teknologi agar masyarakatnya dapat lebih mudah dan praktis dalam mengolah informasi ataupun data, tetapi negara berkembang pun juga terus berusaha untuk mengembangkan teknologi agar negaranya tidak tertinggal dalam arus globalisasi yang kian meningkat.

Internet membawa manusia pada suatu ruang atau dunia baru yang tercipta bernamakan *cyberspace*. *Cyberspace* diartikan sebagai tempat maya atau dunia maya untuk berkomunikasi dengan menggunakan jaringan sistem komputer atau internet. Tidak dapat dipungkiri, kemajuan teknologi ini tentu dapat memberikan dampak positif maupun negatif terhadap stabilitas dan keamanan suatu negara. Ketergantungan masyarakat terhadap teknologi dapat menjadikan masyarakat atau generasi yang kurang kreatif dalam menghadapi suatu persoalan dan cenderung kurang aktif dalam bersosialisasi. Kebebasan masyarakat dalam mengakses internet terutama dalam menyampaikan opini di media sosial tanpa menghiraukan risiko yang akan terjadi selanjutnya pada dirinya sendiri ataupun orang lain menjadi salah satu kasus penyalahgunaan dalam bermedia sosial. Dampak positif yang bisa

dirasakan ialah masyarakat bahkan sampai organisasi negara dapat dengan mudah berkomunikasi dan bertukar informasi yang membuat hubungan antar negara menjadi lebih mudah untuk dilakukan.

Pada sektor ekonomi, teknologi juga dapat dimanfaatkan oleh para pelaku bisnis dalam melakukan proses bisnisnya atau dalam melakukan transaksi online. Selain itu pada aspek kehidupan lainnya pun juga dapat ikut merasakan kemudahan atas teknologi informasi yakni seperti sektor pendidikan yang dapat mempermudah para murid dan guru dalam mencari bahan ajaran dan melakukan *video conference* atau sekolah daring. Terlebih pada masa pandemi yang telah berlangsung sejak awal tahun 2020 menjadikan banyak masyarakat yang menggunakan teknologi internet guna menunjang kebutuhannya dalam sekolah atau bekerja dari rumah. Selain itu pada sektor pariwisata, teknologi juga dapat memberikan kemudahan bagi masyarakat luas untuk mengetahui suatu tempat melalui situs atau website tertentu serta teknologi informasi dapat menjadi salah satu tempat untuk menyampaikan opini dan lain sebagainya.

Namun, ada pula dampak negatif yang timbul dan tidak jarang kita rasakan akibat tak terbatasnya masyarakat dalam mengakses internet. Banyak individu bahkan kelompok yang dengan sengaja menyalahgunakan perkembangan teknologi ini dengan berbagai macam kejahatan. Dampaknya pun tidak sedikit, contohnya seperti penipuan online, pencurian data, *hacking*, serangan ransomware, *skimming*, pemalsuan data, berita hoaks, ujaran kebencian, perjudian bahkan sampai teroris dunia maya (*cyber terrorism*). Semua contoh kasus tersebut merupakan kejahatan-kejahatan yang masuk dalam kategori kejahatan siber (*cybercrime*) dan kejahatan

siber ini juga merupakan bagian dari kejahatan transnasional (*transnational crime*). Secara lebih luas, *cybercrime* dikenal sebagai salah satu kejahatan atau tindakan ilegal yang dalam aksinya didukung oleh adanya teknologi komputer. Istilah *cybercrime* ini timbul karena adanya pemanfaatan teknologi internet dan tentu ini menjadi suatu ancaman yang serius bagi individu ataupun negara yang mengalaminya.

Dikarenakan kejahatan ini dilakukan dengan menggunakan teknologi sistem informasi dari jaringan komputer, maka secara langsung akan dapat menyerang teknologi sistem milik korban yang dituju. Berdasarkan dari motif kegiatannya, *cybercrime* dapat digolongkan kedalam beberapa jenis, seperti cybercrime murni, yang tindakannya berdasar pada kriminalitas; *cybercrime 'abu-abu'* atau kejahatan yang sulit untuk dibedakan apakah tindakan tersebut kriminal atau tidak*; cybercrime against person*, tindakan yang dilakukan dan dituju kepada orang lain dengan motif dendam yang bertujuan untuk mencemarkan nama baik korban; *cybercrime against property*, tindakan yang dilakukan pada hasil karya sesorang dengan menyebarkan, menduplikat hingga mengubahnya untuk tujuan pribadi yang umumnya berupa materi; dan *cybercrime against government*, tindakan yang menjadikan pemerintah sebagai objek utama.[2] Para pelaku kejahatan ini biasanya merupakan seorang individu atau kelompok yang ahli dalam menggunakan sistem informasi dan jaringan komputer sehingga mereka dapat dengan mudah melakukan aksi *cybercrime*.

[2] Eliasta Ketaren. Cybercrime, Cyber Space, dan Cyber Law. *Journal Times*, *5*(2), 2016. Hlm. 37

Adanya *cybercrime* yang dapat mengancam para pengguna internet dan media sosial di dunia termasuk Indonesia banyak disebabkan oleh adanya konten-konten negatif yang disebarkan oleh beberapa pihak yang tidak bertanggung jawab. Ancamannya sendiri dapat dimaknai sebagai usaha atau tindakan, baik yang berasal dari dalam maupun luar negeri dan berpotensi membahayakan keselamatan bangsa, kedaulatan Negara serta keutuhan wilayah Negara. Konsep ancaman tersebut dapat mencakup hal yang selalu berubah dan berkembang dari waktu ke waktu. *Cybercrime* memiliki cakupan yang luas serta dampak yang juga luas pada suatu Negara kawasan bahkan di dunia. *Cyber threat* atau ancaman siber kerap mengincar objek-objek vital di suatu Negara sehingga nantinya dapat menyebabkan kerugian besar yang harus ditanggung oleh berbagai pihak. Dampak yang dialami akibat adanya serangan *cyber* bisa berupa: penyalahgunaan informasi, pengendalian sistem secara remote, kerusuhan, ketakutan, kekerasan, kekacauan, konflik, gangguan fungsional ataupun kondisi merugikan lainnya yang dapat mengakibatkan kehancuran.[3] Ancaman-ancaman tersebut pastilah sangat berbahaya karena dapat mengintai di segala penjuru serta ke setiap celah yang mampu dimanfaatkan oleh para pelaku untuk melakukan kejahatan.

Cybercrime sendiri memiliki berbagai macam jenis yang berbeda. Umumnya kita dapat mengkategorikan beberapa potensi ancaman *cybercrime* diantaranya:[4] *online fraud*, *illegal content*, *cyber espionage*, *data forgery*, *carding*,

[3] Henike Primawanti, Sidik Pangestu. Diplomasi Siber Indonesia Dalam Meningkatkan Keamanan Siber Melalui Association Of Southeast Asian Nation (Asean) Regional Forum. *Global Mind*, *2*(2), 2020. Hlm.3

[4] *Ibid.*

cracking, unauthorized access to computer system and service, offense against intellectual property, cyber stalking, cyber terrorism and cybersquatting, and infringements of privacy. Namun, lebih rinci lagi *cybercrime* dapat dikelompokan menjadi dua kategori yakni;[5] Kejahatan Biasa (konvensional) yang dalam aksinya menggunakan komputer dan internet sebagai alat kejahatan; dan Kejahatan Baru yang menjadikan komputer dan internet serta perangkatnya sebagai sasaran objek *cybercrime*. Beberapa contoh kasus *cybercrime* yang marak terjadi di Indonesia ialah diantaranya; penipuan online, penyebaran konten provokatif, pornografi, akses ilegal, perjudian, pemerasan, pencurian data dan identitas pribadi, peretasan sistem elektronik, intersepsi ilegal, pengubahan tampilan situs, gangguan sistem serta manipulasi data.

Menurut data dari laporan Siber Polri,[6] ada beberapa kasus kejahatan yang sering terjadi di Indonesia. Namun, terdapat dua laporan tertinggi atas kasus *cybercrime* sejak tahun 2017-2020 yakni penipuan online (*online fraud*) dan penyebaran konten provokatif. Pada tahun 2017, kasus kejahatan penipuan online yang terdata ada sebanyak lebih dari 1.400 laporan, sedangkan kasus penyebaran konten provokatif sebanyak lebih dari 1.100 laporan. Di tahun 2018, data yang dilaporkan kian meningkat, angka laporan kasus penipuan online tercatat mencapai lebih dari 1.700 laporan dan penyebaran konten provokatif juga sebanyak 1.700 laporan. Di tahun 2019, angka kasus penipuan online tercatat sedikit menurun dari

[5] Abdullah Tulip, Nasriana & Akhamd Idris. Kerjasama Indonesia Dengan Negara Negara Tetangga Dalam Pemberantasan Kejahatan Transnasional. *Laporan Penelitian Makalah Lengkap*, (0200.3), 2011. Hlm. 53-54

[6] Direktorat Tindak Pidana Siber ialah satuan kerja yang berada di bawah naungan Bareskrim Polri yang bertugas dalam melakukan penegakan hukum terhadap kejahatan siber di Indonesia.

tahun sebelumnya, yakni ada sekitar 1.600 laporan atas kasus tersebut dan untuk kasus penyebaran konten provokatif tetap berada di angka sekitar 1.700 lebih laporan. Hingga akhirnya pada tahun 2020 data laporan kasus *cybercrime* terbilang cukup jauh lebih menurun dari tahun-tahun sebelumnya yakni, sekitar 600 laporan atas kasus penipuan online dan 1.000 laporan atas kasus penyebaran konten provokatif.[7] Data-data tersebut merupakan data tahunan atas laporan-laporan yang diberikan oleh masyarakat kepada Polri (Polisi Republik Indonesia) melalui portal *patrolisiber.id*. Dari selama kurun waktu empat tahun ke belakang, platform yang paling banyak mendapatkan pelaporan atas *cybercrime* ialah pada platform *messenger* yakni Whatsapp dengan lebih dari 5000 kasus karena platform tersebut terbilang paling banyak digunakan oleh masyarakat Indonesia dengan total kerugian yang disebabkan hingga mencapai lebih dari Rp 1 triliun.

Bahkan dalam masa pandemi *covid-19* tahun 2020, Indonesia mendapati beberapa kasus kejahatan baru yang dilakukan oleh para pelaku tidak bertanggung jawab, yakni dengan memanfaatkan masa pandemi untuk menjual barang serta alat kesehatan medis dan menaikkan harga jual diatas harga normal atau harga umum yang dipasarkan. Ada pula beberapa pihak yang dengan sengaja menimbun banyak alat-alat kesehatan tersebut sehingga menyebabkan kelangkaan di beberapa tempat dan menyulitkan masyarakat umum untuk mendapatkan barang tersebut. Karena hal itu banyak masyarakat yang mau tidak mau untuk membeli alat-alat kesehatannya dengan harga yang sangat tinggi karena kebutuhannya yang sangat

[7] Patroli Siber. "Statistics; Jumlah Laporan Polisi Yang Dibuat Masyarakat". Diakses melalui, <https://patrolisiber.id/statistic> pada 20 Desember 2021

mendesak. Selain itu juga makin banyak tersebarnya informasi hoaks atau konten penipuan tentang pandemi *covid-19* oleh beberapa pelaku yang kemudian ditangani oleh pihak kepolisian. Para pelaku tersebut dengan sengaja memanfaatkan serta mencoba mengambil keuntungan dari adanya kerentanan dan keterbatasan masyarakat dalam beraktifitas selama pandemi yang terjadi di Indonesia maupun dunia.

Cybercrime kerap dilakukan oleh para peretas (*hackers*) untuk dapat mencari keuntungan semata bagi individu ataupun kelompoknya. Kegiatan ini pun juga sama mudahnya untuk dilakukan dimanapun dan kapan pun. Target pelaku juga tidak hanya individu saja melainkan juga bisa menyerang pemerintahan negara yang menyebabkan keamanan negara ikut terancam. Maka dari itu, ancaman *cyber* ini sangat membutuhkan lebih banyak perhatian untuk dapat mengembangkan keamanan siber yang jauh lebih kuat pada setiap negara serta perlu adanya tindakan sebagai bagian dari upaya pencegahan aktivitas *cybercrime*. Keamanan siber atau *cybersecurity* sendiri terdiri dari praktik, tindakan ataupun upaya yang bertujuan untuk melindungi ekosistem *cyber* dan juga aset perkembangan perusahaan dan pengguna dari serangan yang berbahaya.[8] Salah satu bentuk upaya suatu negara dalam menjaga keamanannya ialah dengan terus memperkuat sistem *cybersecurity* itu sendiri. *Cybersecurity* merupakan suatu alat, kebijakan atau konsep keamanan yang dapat digunakan guna melindungi lingkungan *cyber* dan organisasi serta aset pengguna. Hal ini juga merupakan sebuah upaya guna memastikan pencapaian dan

[8] Noor Halimah Anjani. *Perlindungan Keamanan Siber Di Indonesia*. 2021. Hlm. 2

pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan *cyber*.[9]

Indonesia sebagai salah satu negara berkembang yang juga termasuk negara dengan jumlah pengakses internet terbanyak di dunia, menjadikannya tidak luput dari ancaman *cybercrime*. Namun, seiring dengan pesatnya penggunaan internet oleh masyarakat, Indonesia belum diimbangi dengan adanya *cybersecurity* yang memadai. Dasar hukum yang mengatur tentang *cybersecurity* di Indonesia juga hanyalah berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008 yang telah di revisi menjadi UU ITE Nomor 19 Tahun 2016. UU ITE memberikan perlindungan hukum bagi konten keamanan sistem elektronik dan transaksi elektronik. Namun, UU ITE tidak dapat mencakup aspek yang paling penting dalam *cybersecurity*, yakni dalam infrastruktur informasi dan jaringan serta sumber daya manusia dengan keahliannya di bidang *cybersecurity*.[10] Hal ini menjadikan legalitas hukum dalam penanganan *cybercrime* masih terbilang lemah, karena meskipun sudah ada peraturan perundang-undangan yang melarang segala bentuk *cybercrime* baik yang berupa penyerangan ataupun perusakan sistem elektronik ternyata masih banyak kasus-kasus *cybercrime* yang terjadi dan kurang mendapat perhatian atau sanksi tegas dari lembaga penegak hukum negara.[11]

Selain itu, Indonesia juga belum memiliki peraturan perundang-undangan atau kebijakan yang benar-benar mengatur secara khusus tentang *cybercrime*

---

[9] Handrini Ardiyanti. Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *5*(1), 2016. Hlm. 98

[10] Noor Halimah Anjani*. Op.Cit.* Hlm. 4

[11] Noor Halimah Anjani. *Op.Cit.* Hlm. 100

berserta penanganannya. Padahal bentuk kejahatan di dunia *cyber* semakin meningkat dan berkembang sangat cepat sehingga cukup sulit untuk ditangani sekalipun oleh aparat penegak hukum. Dengan belum terbentuknya sistem pertahanan yang terkoordinasi dan memadai menjadikan hal tersebut sebagai salah satu faktor bahwa Indonesia termasuk kedalam negara 'darurat *cyber*'.

Dibangunnya kerangka hukum *cybersecurity* di Indonesia berlandaskan dasar Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No.11 Tahun 2008, yang didalamnya telah diatur bagaimana mengoperasikan sistem elektronik yang disediakan baik oleh pihak swasta maupun pemerintah agar dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan dan keteraksesan informasi elektronik.[12] Selain itu juga ada Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No.82 Tahun 2012 serta surat edaran dan peraturan menteri. Seiring dengan terus meningkatnya ancaman *cyber* yang tumbuh menjadi sebuah ancaman keamanan nasional, menjadikan pemerintah Indonesia harus bersikap tegas dalam menanggulangi masalah tersebut. Diharapkan negara dapat membentuk suatu badan atau lembaga khusus untuk dapat melindungi masyarakatnya sekaligus menjaga kedaulatan negara khususnya dalam bidang *cybersecurity.*

Dalam responnya pada peristiwa tersebut, Indonesia pada tahun 2017 berdasarkan Peraturan Presiden membentuk Badan Siber dan Sandi Negara (BSSN)

[12] Hidayat Chusnul Chotimah. Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *10*(2), 2019 Hlm. 119

sebagai model institusi *cybersecurity* nasional.[13] Meskipun Indonesia telah mengeluarkan kebijakan tentang keamanan informasi melalui UU ITE untuk membangun pertahanan negara melalui *cybersecurity*, hal itu dirasa belum cukup jika hanya berlandaskan pada undang-undang saja. Indonesia memberikan kebijakan melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) dan perubahannya Peraturan Presiden Nomor 133 Tahun 2017 membentuk BSSN yang bertugas untuk melaksanakan *cybersecurity* secara efektif dan efisien dengan memanfaatkan, mengembangkan dan mengonsolidasikan semua unsur yang terkait dengan *national cybersecurity*. Hal ini dilakukan Indonesia guna menciptakan lingkungan *cyber* yang strategis dengan penyelenggaraan sistem elektronik yang aman, andal dan terpercaya serta dapat memajukan dan menumbuhkan ekonomi digital dengan meningkatkan daya saing inovasi *cyber*. Selain itu juga agar dapat membangun kesadaran dan kepekaan masyarakat negara terhadap ketahanan dan keamanan nasional dalam ruang *cyber*.

BSSN merupakan penguatan dari lembaga yang telah ada sebelumnya yakni Lembaga Sandi Negara dan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika. Dengan dibentuknya BSSN, maka seluruh pelaksanaan tugas dan fungsinya berada di bidang keamanan informasi, pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet dan keamanan jaringan serta infrastruktur telekomunikasi yang ada di Kementerian Komunikasi dan Informatika. BSSN menyusun strategi *cybersecurity* Indonesia sebagai acuan bersama untuk seluruh pemangku

[13] *Ibid*. Hlm. 116

kepentingan *national cybersecurity* dalam menyusun dan mengembangkan kebijakan *cybersecurity* di instansi masing-masing. Strategi itu sendiri merupakan alat untuk mencapai tujuan atau keunggulan bersaing dengan melihat faktor eksternal dan internal organisasi.[14] Hadirnya BSSN sebagai institusi *cyber* nasional di sini berperan dalam menjalin koordinasi dan kerjasama antara institusi dan pemangku kepentingan di bidang *cyber* di Indonesia yang meliputi *cybercrime, cyber defense, cyber diplomacy* dan Kementerian Komunikasi dan Informatika serta lembaga-lembaga lainnya. Tujuan dari strategi *cybersecurity* Indonesia ialah tercapainya ketahanan *cyber*, keamanan layanan publik, penegakan hukum *cyber*, budaya keamanan *cyber* dan *cybersecurity* pada ekonomi digital. Dengan adanya strategi ini diharapkan dapat menjadi salah satu fondasi kepercayaan dunia kepada Indonesia dalam berbagai forum keamanan siber internasional karena strategi *cybersecurity* Indonesia merupakan sumbangsih bangsa Indonesia dalam mendorong terciptanya perdamaian dunia.

Permasalahan lainnya ialah ada pada penanganan *cybersecurity* dalam kerangka pertahanan negara yang hingga kini masih bersifat sektoral. Dalam mengatasi *cybercrime*, Kementerian Pertahanan Keamanan membentuk Tim Kerja Pusat Operasi Dunia Maya (*Cyber Defence Operation Centre*) dengan tujuan untuk menjaga keamanan dan perlindungan internal (Kemhan) maupun keamanan dan perlindungan eksternal (Nasional) dalam dunia *cyber*. Pembentukan tim ini ditujukan untuk membangun sistem pertahanan semesta yang melibatkan seluruh

[14] Damar Apri Sudarmadi, Arthur Josias Simon Runturambi. Strategi Badan Siber Dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2), Hlm. 159

warga negara, wilayah dan sumber daya nasional lainnya untuk menegakkan kedaulatan negara, keutuhan wilayah dan keselamatan segenap bangsa dari ancaman *cyber*.[15] Selain itu Indonesia juga memiliki Direktorat Tindak Pidana Siber Bareskrim Polri (Dittipidsiber) yang merupakan satuan kerja yang dibawahi oleh Bareskrim Polri dan ditugaskan untuk melakukan penegakan hukum terhadap berbagai bentuk *cybercrime*. Namun secara umum, Dittipidsiber fokus dalam menangani dua kelompok *cybercrime* yakni kejahatan komputer (*computer crime*) atau kelompok kejahatan yang menggunakan komputer sebagai alat utama dalam menjalankan kejahatannya dan kejahatan yang berkaitan dengan komputer (*computer-related crime*) atau *cybercrime* yang menggunakan komputer sebagai alat bantu dalam menjalankan kejahatannya.

Dalam melakukan proses pembuktian, penanganan dan penindakan lanjutan terhadap setiap *cybercrime*, Dittipidsiber diimbangi dengan berbagai fasilitas infrastruktur dan sarana pendukung seperti *Laboratorium Digital Forensic* yang telah meraih ISO 17025:2018 sebagai laboratorium uji serta kalibrasi di bidang *Computer Forensic* yang telah memenuhi standar mutu khusus dalam hal manajerial dan teknis untuk keperluan pemeriksaan yang berupa barang bukti digital. Dittipidsiber juga terus menjalin kerjasama dengan berbagai instansi baik di dalam dan ataupun luar negeri. Hal itu dilakukan guna mempermudah terjalinnya koordinasi antar negara dalam mengatasi *cybercrime* yang bersifat transnasional dan terorganisir (*transnational crime*).[16] Kejahatan transnasional (*transnational*

[15] Handrini Ardiyanti. *Op.Cit.* Hlm. 101
[16] Patroli SIber. "Direktorat Tindak Pidana Siber Bareskrim Polri". Diakses melalui, <https://patrolisiber.id/about> pada 20 Desember 2021

crime) itu sendiri dapat dikelompokkan menjadi beberapa jenis kejahatan, misalnya terorisme, perdagangan manusia (*human trafficking*), pencucian uang, penyelundupan obat-obatan terlarang (narkoba) hingga kejahatan di dunia maya (*cybercrime*).

Selaras dengan Dittipidsiber, upaya lainnya yang dilakukan oleh Indonesia ialah dengan melakukan kerjasama internasional dengan organisasi regional maupun internasional ataupun menjalin kerjasama bilateral dengan negara-negara tetangga lainnya yang lebih kuat dan memadai dalam menjaga keamanan di bidang *cyber*. Kerjasama dianggap perlu dilakukan untuk dapat mempererat hubungan diplomasi antar negara sekaligus meningkatkan dan mengembangkan suatu bidang untuk menjaga stabilitas negara. Karena semua negara di dunia pastinya tidak dapat berdiri sendiri dalam memenuhi segala kebutuhannya terlebih lagi dalam usahanya untuk meningkatkan perkembangan negaranya. Berkaitan dengan alasan tersebutlah yang menjadikan kerjasama dengan negara lain disebut sebagai adanya saling ketergantungan antar dua negara yang sesuai dengan kebutuhannya masing-masing. Ini juga merupakan tanda dari perkembangan situasi hubungan internasional yang mana terus berkembangnya jalinan kerjasama internasional di berbagai aspek kehidupan. Kerjasama ini juga merupakan salah satu bentuk upaya suatu negara dalam meningkatkan kesejahteraan masyarakat dan bangsanya yang dilandasi dengan adanya prinsip saling percaya, menghormati dan menghargai.

Kerjasama internasional umumnya diartikan sebagai adanya hubungan yang dilakukan oleh dua negara atau lebih guna mencapai tujuan-tujuan tertentu atau untuk kepentingan negara-negara tersebut. Tujuan lainnya ialah juga sebagai upaya

agar suatu negara dapat menangani serta mencegah adanya konflik yang mungkin terjadi serta yang paling penting ialah atas kerjasama ini dipastikan dapat mempererat hubungan antar negara tersebut. Kerjasama ini dapat dijalankan baik dalam bidang ekonomi, politik, budaya, pendidikan sampai keamanan negara. Hubungan dan kerjasama internasional dapat muncul karena adanya suatu kebutuhan dari masing-masing negara serta tidak dimilikinya kemampuan dan potensi yang sama antar negara tersebut. Hal inilah yang menjadikan negara-negara sangat membutuhkan bantuan dari kemampuan negara lain agar bisa membantu segala kebutuhan yang diperlukannya. Hubungan kerjasama ini perlu untuk terus dijalankan dan dipelihara agar dapat berjalan sesuai dengan tujuan awal dan mendapatkan manfaat yang maksimal sehingga menciptakan hubungan damai antar negara-negara di dunia.[17]

Menurut K.J Holsti, kerjasama internasional didefinisikan sebagai: pandangan bahwa dua atau lebih dari kepentingan, nilai atau tujuan yang saling bertemu dan dapat menghasilkan sesuatu lalu dipromosikan atau dipenuhi kebutuhannya oleh semua pihak sekaligus; Pandangan atau harapan dari suatu negara bahwa kebijakan yang telah diputuskan oleh negara lainnya pastinya akan membantu negara tersebut untuk dapat mencapai kepentingan serta nilai-nilainya; Adanya sebuah persetujuan dari masalah-masalah tertentu antar dua negara atau lebih dalam rangka memanfaatkan adanya kesamaan kepentingan atau benturan kepentingan bersama; Aturan resmi atau tidak resmi perihal sebuah transaksi di

[17] Zulkifli. Kerjasama Ekonomi Internasional Sebagai Solusi Pengelolaan Kawasan Perbatasan Negara (Studi Kasus Indonesia). *Cano Ekonomos*, *3*(2), 2014. Hlm. 18-19

masa depan yang hendak dilakukan untuk melaksanakan persetujuan bersama; Menjalin transaksi antar negara untuk dapat memenuhi persetujuan mereka.[18] Namun, kerjasama juga tidak hanya bisa dilakukan oleh individual antar negara saja, melainkan juga bisa dilakukan oleh sekelompok organisasi ataupun lembaga internasional antar negara.

Dalam hal ini, kerjasama yang hendak dilakukan Indonesia diharap dapat memperkuat sistem pertahanan negara dalam menghadapi kejahatan-kejahatan transnasional yang dapat mengancam keamanan negara khususnya pada bidang *cyber*. Sebelumnya Indonesia telah melakukan kerjasama internasional dengan beberapa negara dan organisasi luar negeri seperti contohnya kerjasama dengan menjadi negara anggota ASEAN *Network Security Action Council*, menjadi anggota *International Telecommunication Union* (ITU), serta melakukan kerjasama bilateral dengan beberapa negara lain pada bidang *cybersecurity* seperti Jepang, Inggris dan negara-negara lainnya. Indonesia juga terbilang cukup aktif dalam program global *cybersecurity* agenda yang telah diluncurkan oleh *World Telecommunication and Information Society Day* di tahun 2007. Program tersebut merupakan bentuk kerjasama internasional yang memiliki tujuan agar dapat menciptakan strategi dan juga membentuk solusi guna meningkatkan keamanan negara dan kepercayaan masyarakat.[19]

Selain kerjasama dengan beberapa negara dan organisasi tersebut, Indonesia juga menjalin kerjasama dengan negara tetangga yakni Australia. Australia

[18] Kalevi Jaakko Holsti. *Politik Internasional: Kerangka untuk Analisis, Jilid 2*. Terjemahan M. Tahrir Azhari. Jakarta: Erlangga. 1988. Hlm. 143-144
[19] Handrini Ardiyanti. *Op.Cit*. Hlm. 101-102

diketahui memang telah menjalin kerjasama dengan Indonesia di berbagai bidang, seperti perdagangan, ekonomi, pariwisata, kesehatan, pendidikan sampai keamanan negara. Karena kondisi keamanan negara yang tengah mengancam Indonesia khususnya di bidang *cyber* menjadikan salah satu alasan Indonesia membentuk kerjasama dalam menjaga keamanan antar dua negara ini. Australia yang juga dikenal sebagai negara yang memiliki kekuatan *cybersecurity* cukup baik, menjadikan hal tersebut sebagai salah satu faktor bagi Indonesia untuk menjalin hubungan bilateral dalam meningkatkan strategi *cybersecurity*. Australia diketahui memiliki lima tema aksi dalam menyusun strategi keamanan siber yang berlaku hingga tahun 2020 yakni meliputi kemitraan *cyber* nasional, pertahanan *cyber* yang kuat, tanggung jawab global dan pengaruhnya, pengembangan dan inovasi serta penggunaan *cyber* yang cerdas. Beberapa kinerja Australia meliputi pelaporan mengenai perkembangan strategi, melakukan pertemuan rutin dengan para pimpinan kepentingan dalam keamanan *cyber*, membentuk sebuah lembaga yang bertanggung jawab serta sebagai pusat pengembangan *cybersecurity* Australia dan mendanai aktivitas penelitian terkait.[20]

1.2. Masalah Penelitian

Seiring perkembangan globalisasi dan kemajuan teknologi informasi menjadikan tantangan tersendiri bagi pemangku kebijakan pada era informasi. Maraknya ancaman *cybercrime* ini bisa berupa penipuan, aktivitas manipulasi data, kebocoran data, *money laundering*, serangan ransomware, *skimming*, bahkan

[20] Sofia Trisni, Rika Isnarti & Abdul Halim. Peningkatan Keamanan Siber ASEAN Melalui Kerja Sama Keamanan Siber Dengan Australia: Pusat Studi ASEAN Universitas Andalas. 2017.

sampai terorisme yang dapat mengancam keselamatan dari para pengguna media informasi. Perlu adanya kebijakan atau landasan keamanan dari setiap pemerintah atau organisasi di dunia yang dapat meretas *cybercrime* tersebut agar masyarakat merasa aman dan terlindungi ketika ingin mengakses dan menggunakan media sosial atau teknologi informasi lainnya.

Di Indonesia, kasus *cybercrime* kian terus meningkat sehingga menjadikan keamanan negara juga ikut terancam. Keadaan ini membuat pemerintah Indonesia harus bertindak tegas dalam menangani dan mencegah setiap aktifitas *cybercrime* yang mungkin terjadi dengan menegakkan hukum *cyber* di negara sehingga terciptanya *cybersecurity* yang baik dan kuat. *Cybersecurity* dapat digambarkan sebagai suatu kebijakan, pedoman, proses maupun tindakan yang diperlukan guna meminimalisir risiko pelanggaran dan pencurian dalam dunia maya. *Cybersecurity* juga dijadikan sebagai alat atau teknik dalam proses untuk melindungi segala aset yang ada dalam sistem informasi dan komputer. Melalui *cybersecurity*, pemerintah dituntut untuk siap mencegah dan mengamankan data serta mengawasi setiap aktivitas masyarakat di dunia internet.

Kejahatan transnasional ini pastinya tidak bisa ditangani sendiri oleh negara, maka dari itu suatu negara perlu menjalin hubungan atau kerjasama internasional dalam menangani kejahatan transnasional. Hendaknya, kerjasama ini dilakukan dengan negara lain yang lebih kuat dalam penanganan *cybercrime* agar terciptanya perjanjian serta kebijakan bersama guna menjaga keamanan negara. Hal ini tentu akan membuka peluang bagi Indonesia untuk dapat bangkit dan meminimalisir terjadinya berbagai kasus *cybercrime* yang jauh lebih mengancam

dan berbahaya. Bentuk kerjasama internasional atau hubungan bilateral yang dilakukan Indonesia bersama Australia dalam meningkatkan *cybersecurity* merupakan salah satu bentuk contoh aksi reaksi dari Indonesia terhadap maraknya kasus kejahatan siber yang mengancam keamanan negara maupun individu masyarakat. Bentuk kerjasama yang dilakukan ini salah satunya melalui program *Cyber Policy Dialogue* yang telah disepakati bersama sejak tahun 2018 hingga sekarang.

Berdasarkan latar belakang dan masalah penelitian yang telah dijelaskan sebelumnya, Indonesia dengan Australia sepakat untuk melakukan kerjasama pada bidang keamanan, terkhusus *cybersecurity* guna menangani ancaman *cybercrime* yang mungkin terjadi di kedua negara. Kedua negara sepakat untuk membuat MoU kerjasama pada bidang *cyber* dengan membentuk program *Cyber Policy Dialogue*. Maka dari itu penulis tertarik untuk membahas serta menganalisis topik tersebut dengan pertanyaan pokok yakni: **'Bagaimana implementasi program kerjasama *Cyber Policy Dialogue* dalam penanganan kasus penipuan online di Indonesia?'** selain itu penulis juga memiliki beberapa pertanyaan operasional, diantaranya:

1. Apa saja faktor yang membuat Indonesia hendak menjalin kerjasama internasional dengan Australia dalam menangani *cybercrime* ?
2. Bagaimana hasil implementasi cyber policy dialogue bagi Indonesia dalam menangani kasus penipuan online ?

1.3.Tujuan Penelitian

Sebagai upaya dalam memperoleh hasil dari penelitian yang hendak dilakukan oleh peneliti, maka perlu adanya penegasan dalam mencapai suatu tujuan dari hasil penelitian ini, yaitu :

1. Menganalisis dan mendeskripsikan bentuk kerjasama Indonesia dengan Australia dalam menangani *cybercrime* melalui program *Cyber Policy Dialogue.*
2. Menganalisis strategi Indonesia berdasarkan hasil dari implementasi program *Cyber Policy Dialogue.*

1.4. Manfaat Penelitian

Penelitian tentang Kerjasama *Cyber Security* Indonesia dengan Australia dalam Kasus Penipuan Online Melalui Program *Cyber Policy Dialogue* Tahun 2017-2020 ini diharap dapat memberikan manfaat secara teoritis untuk terus mengembangkan kerjasama internasional dan atau menjalin hubungan antar negara baik dalam level multilateral ataupun bilateral guna dijadikan sebagai salah satu solusi dalam mencegah dan menangani suatu kejahatan baik yang berupa kejahatan *domestic* ataupun kejahatan transnasional di suatu kawasan. Selain itu penelitian ini juga diharapkan dapat memiliki beberapa manfaat atau kegunaan bagi lingkungan sekitar, antara lain :

a. Bagi Penulis

Penelitian ini dilaksanakan guna memenuhi persyaratan tugas akhir untuk memperoleh gelar Sarjana Sosial di Universitas Nasional. Selain itu, penelitian ini juga dapat menambah pengetahuan serta wawasan peneliti dalam memahami

bentuk kerjasama Indonesia dengan Australia dalam menangani suatu masalah khususnya *cybercrime.*

b. Bagi Instansi Pendidikan

Penelitian ini memiliki manfaat untuk dapat memberikan pandangan serta informasi mengenai kejahatan dunia maya yang termasuk ke dalam suatu kelompok kejahatan transnasional atau kejahatan yang terorganisir serta bentuk hubungan kerjasama internasional antar Indonesia dan Australia dalam menangani keamanan negaranya dari ancaman *cybercrime* melalui program *Cyber Policy Dialogue.*

c. Bagi Masyarakat

Penelitian ini memiliki manfaat terhadap masyarakat untuk memberikan informasi dan pandangan pada suatu kejahatan yang terjadi di dunia maya, salah satunya penipuan online yang dapat mengancam masyarakat serta upaya penanganan dan pencegahan dari pembentukkan kebijakan yang dilakukan Indonesia bersama Australia dalam program *Cyber Policy Dialogue*.

1.5. Sistematika Penulisan

Guna memahami skripsi ini secara lebih jelas, maka materi yang disampaikan dalam tulisan ini dikelompokkan ke beberapa sub-bab dengan sistematika penyampaian sebagai berikut :

- **BAB I PENDAHULUAN** merupakan bab yang berisi tentang latar belakang masalah, masalah penelitian yang juga terdapat pertanyaan pokok dan beberapa pertanyaan operasional, tujuan penelitian, manfaat penelitian serta sistematika penulisan pada penelitian ini berdasarkan kasus yang akan penulis bahas.

- **BAB II TINJAUAN PUSTAKA** merupakan bab yang berisi tentang kerangka konseptual, *literature review* yang terdiri dari *review* teori dan konsep serta *review* penelitian terdahulu yang relevan guna mendukung penulis dalam melakukan penelitian.
- **BAB III METODE PENELITIAN** merupakan bab yang berisi tentang bentuk metodologi penelitian yang akan penulis gunakan, pendekatan penelitian, jenis penelitian, teknik pengumpulan data, teknik pemeriksaan keabsahan data serta teknik pengolahan data yang hendak penulis gunakan dalam menganalisa kasus ini.
- **BAB IV PEMBAHASAN** merupakan bab yang berisi tentang penjelasan dan tinjauan umum mengenai kasus-kasus kejahatan siber yang terjadi di Indonesia sejak 2018-2020 khususnya pada kasus penipuan online serta factor awal Indonesia berkerjasama dengan Australia.
- **BAB V ANALISIS** merupakan bab yang berisi tentang analisis dan deskripsi mengenai legalitas hukum di Indonesia dan Australia sebagai salah satu strategi *cybersecurity* negara, serta hubungan kerjasama bilateral Indonesia dengan Australia dalam meningkatkan *cybersecurity* melalui kebijakan program *Cyber Policy Dialogue* sejak tahun 2018-2020, yang mana penulis juga akan menganalisisnya jika diimplementasikan pada kasus penipuan online di Indonesia.
- **BAB IV PENUTUP** merupakan bab akhir dalam penulisan yang berisi sebuah kesimpulan dari hasil analisis penelitian guna menjawab pertanyaan pokok, operasional serta fokus masalah pada penelitian ini.