BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi merupakan hal yang tidak dapat dihindari dari tiap era, perkembangan teknologi sendiri sangat diperlukan bagi umat manusia karena dengan adanya penggunaan teknologi semua pekerjaan manusia dapat terbantu dalam kesehariannya. Teknologi telah memberikan dampak yang besar bagi keberlangsungan hidup manusia. Teknologi sendiri terdapat bermacam macam variasi yang terbagi dalam beberapa bidang, dalam beberapa bidang tersebut teknologi juga memiliki dampak masing masing sesuai kegunaan dan penggunanya. Akan tetapi tidak semua perkembangan dan penggunaan teknologi memiliki dampak positif, teknologi juga dapat menjadi hal yang negatif. Teknologi komputer dan internet telah membuat adanya *cyberspace*, Istilah *cyberspace* pertama kali muncul pada tahun 1984 oleh William Gibson dalam novel Neuromancer (Murray, 2007). Dalam *cyber space* pengguna komputer dapat berkomunikasi tanpa menunjukkan identitas dan tanpa dibatasi oleh wilayah bahkan lintas negara (transnasional) (Nugraha, 2013). Dengan begitu *cyber space* membuat lahirnya kejahatan kejahatan baru yaitu *cybercrime*, *cyber attack*, *cyber espionage*, hingga *cyberterrorism.*

Seiring perkembangan zaman dan globalisasi membuat meningkatnya penyalahgunaan *cyberspace*, saat ini kejahatan dalam dunia siber sangat berpotensi merusak pertahanan negara. Negara negara didunia telah menganggap kejahatan yang lahir karena *cyber space* sebagai ancaman nasional maupun internasional, hal ini dikarenakann ancaman serangan siber akan terus berkembang mengikuti perkembangan teknologi informasi. Seperti yang diketahui bahwa saat ini pengguna komputer didunia telah meningkat pesat, menurut data *World Bank* dalam ITU (*International Telecommunication Union*) misalnya porsi pengguna internet di dunia adalah sekitar 49% populasi pada tahun 2017. Porsi tersebut meningkat pesat dibandingkan tahun 2000 yang hanya sekitar 6,7%. Lalu menurut *Internet World Stats* akan ada porsi pengguna internet dunia sebesar 64.2% populasi pada tahun 2021, adapun jumlah populasi yang diperkirakan tersebut adalah lebih dari 5 miliar (Cakrawala, 2021). Tak hanya itu ancaman siber akan terus meningkat dan berkembang sesuai dengan perkembangan teknologi dan penggunanya, dengan meningkatnya pengguna internet maka jumlah serangan juga meningkat. Menurut *Deep Instinct* misalnya, Jumlah serangan siber menggunakan *malware* mengalami peningkatan sebesar 358% pada tahun 2020 dibandingkan tahun 2019. Sementara dalam serangan siber menggunakan *ransomwarwe* meningkat sebanyak 435% pada tahun 2020 dibandingan tahun 2019 (Cakrawala, 2021). Penguatan *cybersecurity* saat ini sangat penting karena perkembangan teknologi informasi dan penggunanya yang telah berkembang pesat, penguatan *cybersecurity* tersebut akan meningkatkan pertahanan negara dan kepentingan nasional lainnya.

Australia saat ini merupakan salah satu negara yang sangat fokus dalam menanggapi kejahatan siber, Australia telah mengalami berbagai macam serangan siber yang terjadi, sejak tahun 2011 serangan siber di Australia terus meningkat. Lebih dari 5000 insiden serangan siber yang direspon oleh Australian Signals Directorate (ASD) sejak tahun 2011 – 2017 (ACSC, 2017). Serangan siber di Australia sendiri memiliki berbagai macam bentuk serangan yang terdiri dari beberapa tipe serangan yaitu *Cyber attack*, *Cyber espionage*, *Cybercrime*, *Cyber terrorism*. Selain dalam menanggapi serangan siber, Australia juga melihat *cyberspace* sebagai kepentingan nasionalnya.

Australia telah membentuk badan pertahanan siber negara yang disebut *Australian Cyber Security Centre (ACSC)*. Selain itu juga *The Department of Foreign Affairs and Trade* (DFAT) Australia juga ikut *improve* atau berpartisipasi dalam ranah *cyber security*. DFAT (*Department of Foreign Affairs and Trade*) Australia merupakan departemen pemerintahan Australia yang bertugas untuk memajukan kepentingan Australia dan warganya dalam skala internasional, DFAT mengelola hubungan luar negeri dan kebijakan perdagangan. Saat ini DFAT melihat dunia siber sebagai hal yang mempengaruhi semua aspek hubungan internasional, DFAT menganggap bahwa *cyberspace* dapat mempengaruhi keamanan nasional, keamanan ekonomi, perlindungan Hak Asasi Manusia, hingga pembangunan berkelanjutan (SDGs) (DFAT, 2017). Bagi Australia *cyberspace* merupakan prioritas kebijakan luar negeri, Australia akan terlibat dalam keamanan *cyberspace* dalam nasional maupun internasional.

Dalam pembangunan *cybersecurity*, Australia melakukan pendekatan atau strategi yaitu diplomasi siber. Australia tidak dapat bertindak sendiri dalam menangani ancaman *cyberspace*, kerjasama internasional diperlukan untuk menciptakan peluang agar terciptanya *cybersecurity* yang kuat. Menurut Australia siber saat ini memiliki kapasitas untuk meningkatkan atau membahayakan kepentingan nasional negara, oleh karena itu Australia berpendapat bahwa keterlibatan Australia dalam siber internasional akan mencapai tujuan *cybersecurity* Australia (Government, 2020).

Dalam upaya Australia untuk meningkatkan *cybersecurity*, Australia membuat program yaitu *Cyber Cooperation Program* pada tahun 2016. *Cyber Cooperation Program* merupakan Program yang memainkan peran penting dalam mendukung keterlibatan siber internasional untuk memperjuangkan internet yang terbuka, bebas, dan aman dalam melindungi keamanan nasional dan stabilitas internasional (Government, 2017). Selain itu *Cyber Cooperation Program* merupakan salah satu implementasi dari kebijakan strategi Australia dalam bidang Cyber yaitu *Australia's International Cyber Engagement Strategy.* Dalam kebijakan tersebut Australia melakukan pendekatan diplomasi siber dengan negara negara lain, salah satunya Indonesia. Pendekatan ini merupakan hal yang menarik karena Australia pernah berkonflik dengan Indonesia dalam ranah siber pada tahun 2013. Australia bekerja secara kolaboratif dengan mitra Internasional dan membantu negara negara di kawasan dalam meningkatkan kapasitas untuk mengatasi *cybercrime* yang bertujuan meningkatkan pencegahan dan penindakan kejahatan siber di seluruh dunia

(Government, 2017). Diplomasi siber Australia dengan Indonesia dalam melalui *cyber cooperation program* merupakan langkah strategi Australia dalam meningkatkan *cybersecurity*, Indonesia merupakan partner strategis Australia karena selain fakta letak geografis yang dimiliki Indonesia, Indonesia juga dianggap mampu untuk membantu Australia dalam menciptakan stabilitas siber regional. Australia melakukan pendekatan pertama kali dengan mengajak Indonesia dalam *Cyber Policy Dialogue* pada kamis 4 mei 2017, dialog tersebut diselenggarakan dengan semangat kolaborasi, keterbukaan, dan tujuan bersama dalam mengatasi isu isu siber. Kedua negara menegaskan akan berkomitmen terhadap internet yang terbuka, bebas, dan aman untuk pertumbuhan ekonomi dan inovasi serta memperdalam kerja sama dalam menghadapi ancaman *cyber space*. Kedua negara kembali bertemu pada *Cyber Policy Dialogue* kedua yaitu pada tahun 2018, dalam pertemuan tersebut kedua negara sepakat untuk melanjutkan kerjasama dalam bidang siber, ekonomi digital, dan keamanan siber. Kedua negara telah menyepakati *Memorandum of Understanding* (MoU) tentang kerjasama siber.

Maka dari itu, penulisan ini akan membahas bagaimana upaya Australia dalam memperkuat cybersecurity melalui *Cyber Cooperation Program* dengan Indonesia, jangka waktu kedua negara adalah 2017 – 2020 dimana jangka waktu tersebut merupakan periode dialog dan program kerjasama dalam ranah siber Australia – Indonesia

Penelitian ini akan penulis kaitkan dengan beberapa karya ilmiah terdahulu ataupun beberapa data yang berkaitan dengan penelitian ini sehingga akan membantu

penulis dalam melakukan penelitian. Adapun karya ilmiah dan data yang penulis maksud adalah sebagai berikut :

Jurnal Milik Dhiyanka Magrisa dengan judul : " KERJA SAMA BADAN SIBER DAN SANDI NEGARA (BSSN) INDONESIA DENGAN *DEPARTMENT OF FOREIGN AFFAIRS AND TRADE (DFAT)* AUSTRALIA DALAM PENGEMBANGAN *CYBER SECURITY* " tahun 2020. Jurnal ini membahas bentuk kerjasama yang dilakukan Australia dengan Indonesia dalam pengembangan *cybersecurity* di Indonesia, sedangkan penelitian ini akan membahas implementasi awal diplomasi siber antara Australia dengan Indonesia hingga terjadinya program kerjasama.

Skripsi milik Shafira Quranul dengan judul : " KERJASAMA INDONESIA DENGAN AUSTRALIA DALAM PENANGANAN KASUS PENIPUAN ONLINE MELALUI PROGRAM CYBER POLICY DIALOGUE TAHUN 2018-2020 '' tahun 2022. Skripsi tersebut membahas implementasi cyber policy dialogue dalam penanganan kasus penipuan online, sedangkan penelian ini akan lebih berfokus dalam alur implementasi diplomasi siber Australia dan Indonesia dalam Cyber Cooperation Program.

Dari tinjauan pustaka tersebut dapat ditemukan titik persamaan dan perbedaan dengan yang peneliti teliti. Dalam titik persamaannya adalah dimana sama sama

membahas akan peningkatan *cyber security*, sedangkan penelitian ini akan membahas alur implementasi diplomasi siber Australia dengan Indonesia dalam Cyber Cooperation Program.

1.2 Rumusan Masalah

Mengangkat tentang analisis upaya Australia dalam penguatan *cyber security* melalui *Cyber Cooperation Program* dengan Indonesia, berdasarkan latar belakang yang telah diuraikan maka rumusan masalah dari penulisan ini adalah " **Bagaimana implementasi diplomasi siber Australia dengan Indonesia dalam *Cyber Cooperation Program* tahun 2017 - 2020?** "

1.3 Tujuan Penelitian

1. Mengetahui upaya Australia dalam meningkatkan cybersecurity negara Australia
2. Mengetahui mekanisme Diplomasi siber Australia – Indonesia
3. Mengetahui program kerjasama kedua negara dalam Cyber Cooperation Program

1.4 Kerangka Pemikiran

1.4.1 Cybersecurity

Menurut Handrini Ardiyanti *Cyber security* merupakan konsep keamanan, alat kebijakan, perlindungan keamanan, pedoman, tindakan dan praktik dalam melindungi lingkungan *cyber* (Ardiyanti, 2016). *Cyber security* negara merupakan tindakan negara dalam melindungi negaranya dalam ranah cyber, dalam hal ini negara bertindak tegas dengan membuat undang undang atau kebijakan dalam negeri maupun luar negeri yang bertujuan untuk melindungi masyarakat atau negaranya dalam ranah *cyber*. *Cyber security* sendiri juga merupakan upaya dalam mencapai pemeliharaan sifat keamanan organisasi terhadap *Global cyber security*. *Global cyber security* sendiri merupakan keamanan *cyber* di lingkungan global karena *cyber* sendiri bersifat luas yang dimana tidak hanya dialami satu negara tetapi semua negara yang ada dilingkungan global, *Global cyber secu*rity dibangun untuk menciptakan dunia yang aman terhadap kejahatan *cyber.*

Cyber security sendiri lebih lanjut dimaknai sebagai mekanisme dalam melindungi atau meminimalkan gangguan kerahasiaan, integritas, dan ketersediaan informasi (Ardiyanti, 2016). Mekanisme ini harus bisa melindungi ketiga hal tersebut dari *cyber attack* ataupun *cyber crime*, negara akan melakukan beberapa cara agar dapat melindungi ketiga hal tersebut. Negara akan membuat beberapa strategi dengan motif tertentu dalam perlindungan siber, seperti contohnya negara akan membuat beberapa kebijakan dalam negeri dengan menerapkan undang undang dalam ranah siber agar terjaganya gangguan kerahasiaan, integritas, maupun informasi yang valid dalam negeri. Selanjutnya negara juga akan memikirkan cara seperti membuat kebijakan luar

negeri ataupun berdiplomasi dengan negara negara lain agar negara dapat mengatasi maupun meminimalisir *cyber attack* ataupun *cyber crime* karena pada *Global cyber security* dibangun atas lima bidang kerja yang dimana kerjasama internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*) termasuk didalamnya (Makarim, 2013)

Penulis menggunakan konsep *cybersecurity* karena penulis meyakini konsep *cybersecurity* dapat membantu dalam menjawab rumusan masalah dalam penulisan ini.

1.4.2 Diplomasi

Diplomasi menurut Earnest Satow, kata diplomasi pertama kali disebutkan dalam Bahasa Inggris yang menunjukkan artian keahlian dan keberhasilan dalam melakukan hubungan internasional dan perundingan (Satow, 1917). Teori diplomasi adalah praktek pelaksanaan hubungan antarnegara melalui perwakilan resmi, diplomasi juga merupakan teknik operasional untuk mencapai kepentingan nasional di luar batas wilayah negara (Plano & Olton, 1979). Pada intinya diplomasi merupakan alat bagi negara untuk mencapai kepentingan nasionalnya dalam dunia internasional, dengan adanya diplomasi negara dapat menerapkan strateginya untuk tercapainya tujuan. Hedley Bull mengatakan bahwa:

" *Diplomacy is the behavior of relations between countries and other entities in world politics that are expressed by official agents and in a peaceful manner* " (Bull, 1995)

dari pernyataan diatas menjelaskan bahwa menurut Bull diplomasi adalah proses negosiasi dalam hubungan internasional yang dilakukan secara damai, fitur yang mendasar dari diplomasi yaitu pendekatan tanpa penggunaan kekerasan untuk merekonsiliasi kepentingan kepentingan di antara para aktor internasional, terutama negara (Hamonangan & Assegaff, 2020)

Terdapat 5 fungsi utama dalam diplomasi menurut Hedley Bull yang dikutip Barrinha dan Renard (Barrinha & Renard, 2017). Yang pertama adalah untuk memfasilitasi komunikasi dalam politik dunia, dalam hubungan internasional komunikasi antar negara merupakan hal yang sangat penting dalam melakukan kerjasama atau konflik, komunikasi tersebut berguna untuk penyampaian kepentingan tiap tiap negara. Yang kedua yaitu untuk menegosiasikan perjanjian, kerjasama antar negara akan menghasilkan perjanjian dan dalam perjanjian tersebut tiap negara berhak bernegosiasi untuk kepentingan nasionalnya, negosiasi sangat perlu dilakukan karena dalam kerjasama tiap negara pasti ingin mencapai solusi menang - menang dan solusi tersebut bisa didapatkan dalam negosiasi. Lalu yang ketiga adalah untuk mengumpulkan informasi dan intelijen dari negara lain, dalam diplomasi selain untuk mencapai kepentingan nasional tiap negara juga menginginkan informasi dari negara lain, informasi tersebut berguna untuk penerapan strategi agar tercapainya kepentingan nasional. Yang keempat yaitu untuk menghindari atau menimalkan gesekan dalam hubungan internasional, diplomasi merupakan alat komunikasi dalam dunia hubungan internasional, jika terdapat konflik internasional maka diplomasi merupakan cara

komunikasi agar menimalkan gesekan atau konflik. Dan yang kelima adalah untuk melambangkan keberadaan masyarakat dalam negara, diplomasi selain berguna untuk komunikasi dalam hubungan internasional juga berguna untuk alat penunjuk identitas nasional dalam dunia internasional.

1.4.1.1 Diplomasi Siber

Dalam ranah diplomasi, diplomasi dibagi menjadi bermacam macam bidang. Salah satunya adalah diplomasi siber, dalam hubungan internasional saat ini *cyberspace* telah menjadi fokus yang signifikan dan topik ini menjadi arus utama yang membuat aktor aktor global telah mengeluarkan kebijakan luar negerinya sebagai langkah dalam meningkatkan keamanan dalam dunia siber ataupun meningkatkan peluang dalam dunia siber. Diplomasi siber sendiri terbagi menjadi tiga definisi yaitu yang pertama sebagai upaya komunikasi, negosiasi, hingga pengumpulan informasi dari negara lain. Lalu yang kedua yaitu diplomasi siber sebagai alat kepentingan nasional dalam dunia siber, seperti yang diketahui dalam *cyberspace* rentan sekali kejahatan kejahatan yang terjadi sehingga beberapa negara menggunakan diplomasi siber sebagai penawaran gagasan kepentingan nasional dalam ranah siber. Lalu yang ketiga adalah diplomasi siber sebagai pengamanan pertahanan dalam ranah siber melalui diplomasi, kejahatan siber rentan terjadi dalam jangkauan transnasional sehingga beberapa negara melakukan diplomasi siber kepada negara lain agar saling meningkatkan keamanan negara dalam *cyberspace* (Hamonangan & Assegaf, 2020) .

Diplomasi siber saat ini sangat penting dalam memperkuat *cybersecurity*, hal ini dijelaskan oleh Gady dan Austin

> " *Because of high levels of cross-border connectivity in the cyber world, new approaches for cybersecurity must factor in the international dimension. Thus, instead of exclusively focus-ing on cyber defense or cyber war, it is also important to begin to develop cyber diplomacy.Few governments have even thought about the diplomatic dimension of cybersecurity, andthey certainly haven't developed diplomatic strategies commensurate with the threat.* '' (Gady & Austin, 2010).

Gady dan Austin menjelaskan bahwa tingkat konektivitas lintas batas yang tinggi di dunia siber membuat adanya pertimbangan untuk fokus dalam *cyber defense* atau *cyber war*, selain itu juga penting untuk memulai mengembangkan diplomasi siber. Beberapa pemerintahan dunia telah memikirkan akan dimensi diplomasi dalam *cybersecurity*, dalam pengembangan tersebut dibutuhkan adanya strategi diplomatik.

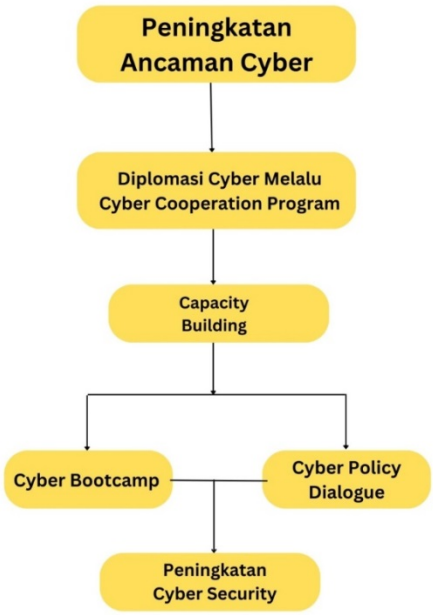
Salah satu strategi yang dilakukan dalam diplomasi siber adalah peningkatan kapasitas, Peningkatan kapasitas dalam diplomasi siber telah berkembang dalam dekade terakhir. Konsep pembangunan kapasitas siber dalam konteks keamanan internasional pertama kali diperkenalkan dalam laporan *UN Group of Governmental Expert* (GGE) tahun 2010. Peningkatan kapasitas menjadi pilar utama diplomasi siber dengan tujuan yang jelas yaitu memperkuat kerangka hukum nasional, menciptakan dan memperkuat tanggap aksi, pelatihan, dan peningkatan kesadaran (Pawlak, 2022). Selain itu, diplomasi bilateral dalam lingkungan siber menawarkan negara negara dengan kapasitas diplomasi siber potensi untuk membentuk koalisi negara negara yang berpikiran sama melalui percakapan tertutup dan identifikasi nilai nilai dan

kepentingan bersama. Mereka juga dapat menciptakan peluang kerja sama dan pengembangan kapasitas antara dua negara atau lebih, serta memajukan kepercayaan dan keyakinan dalam domain di mana sulit untuk memahami kepentingan dan kemampuan negara lain (CybertechAccord, 2021)

Konsep pembangunan kapasitas sendiri menurut Grindle (1997) *capacity building* menjadi serangkaian strategi yang ditujukan untuk meningkatkan efisiensi, efektivitas dan responsivitas, maka *capacity building* tersebut harus memusatkan perhatian kepada dimensi: pengembangan sumber daya manusia, penguatan organisasi, dan reformasi kelembagaan. Dalam konteks pengembangan sumber daya manusia, perhatian diberikan kepada pengadaan atau penyediaan personel yang profesional dan teknis. Kegiatan yang dilakukan antara lain pendidikan dan latihan (training), pemberian gaji/upah, pengaturan kondisi dan lingkungan kerja dan sistim rekruitmen yang tepat (Grindle, 1997).

Berdasarkan definisi dan penjelasan diatas penulis menggunakan teori dan konsep diplomasi siber karena pendekatan Australia dalam meningkatkan *cybersecurity* melalui *Cyber Cooperation Program* dengan Indonesia menggunakan praktik diplomasi, lebih tepatnya diplomasi siber dengan strategi yang digunakan yaitu *capacity building*.

1.5 Sintesa Pemikiran



Gambar 1.5 Sintesa Pemikiran

Berawal dari adanya peningkatan ancaman cyber, Australia melakukan berbagai usaha untuk mencapai keamanan dan kepentingan nasionalnya dalam bidang siber. Australia melakukan inisiasi dalam peningkatan *cybersecurity* dengan membuat kebijakan yaitu *Australia's International Cyber Engagement Strategy.* Kebijakan tersebut diimplementasikan dengan pembuatan program *Cyber Cooperation Program* yang dimana program ini akan mengajak kerjasama negara negara di Indo-pasifik untuk meningkatkan kapasitas dalam bidang siber agar terciptanya keamanan cyberspace.

Australia melakukan diplomasi siber dengan Indonesia untuk mengimplementasikan Cyber Cooperation Program. melalui Diplomasi siber,

Australia dan Indonesia dengan membuat program kerja dalam bidang peningkatan kapasitas siber.

1.6 Argumen Utama

Berdasarkan data data dan pemikiran yang telah dianalisis sebelumnya, maka penulis menyimpulkan argumen utama penelitian yang menyatakan bahwa kerjasama Australia dengan Indonesia dalam bidang siber melalui upaya diplomasi siber memiliki tujuan bagi Australia yaitu tercapainya penguatan *cybersecurity* Australia dan keamanan nasionalnya. Diplomasi siber antara Australia dengan Indonesia diimplementasikan kedalam *Cyber Cooperation Program* Australia - Indonesia.

Dalam diplomasi siber untuk memperkuat *cybersecurity* dan mendorong stabilitas internasional dalam *cyberspace*, Australia melakukan strategi pembangunan kapasitas yang dimana Australia akan membantu Indonesia untuk melatih dan meningkatkan kesadaran Indonesia dalam siber. Peningkatan kapasitas yang dilakukan Australia terhadap Indonesia terbentuk dalam beberapa program kerja yaitu *Cyber Booth Camp* dan *Cyber Policy Dialogue*. Dengan pembangunan kapasitas yang dilakukan Australia terhadap Indonesia akan membantu Australia dalam memperkuat *cybersecurity* negaranya, hal ini dikarenakan *cybersecurity* bersifat luas yang dimana tidak hanya dialami satu negara tetapi semua negara maka Australia akan membantu meningkatkan kapasitas Indonesia agar tercapainya stabilitas siber internasional yang merupakan tujuan peningkatan *cybersecurity* Australia.

1.7 Metode Penelitian

1.7.1 Tipe Penelitian

Tipe penelitian ini adalah deskriptif. penelitian deskriptif adalah penelitian yang dilakukan untuk mengetahui nilai variabel mandiri, baik satu variabel atau lebih (independen) tanpa membuat perbandingan, atau menghubungkan antara variabel satu dengan variabel lain (Sugiyono, 2014)

1.7.2 Jangkauan Penelitian

Untuk membatasi penelitian yang akan dijelaskan, jangkauan penelitian dalam judul“ Analisis Upaya Australia Dalam Penguatan *Cybersecurity* Melalui *Cyber Cooperation Program* Dengan Indonesia Tahun 2017 – 2020 ’’ penulis membatasi batasan waktu selama 3 tahun dalam periode waktu 2017 - 2020 karena pada tahun 2017 merupakan awal adanya *cyber policy dialogue* antara Australia dengan Indonesia, dan pada tahun 2018 merupakan tahun penandatanganan MoU sedangkan 2019 hingga 2020 merupakan tahun program kerja kedua negara yang telah disepakati dalam MoU.

1.7.3 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini penulis akan melakukan pengumpulan data dalam wujud data sekunder yang dimana penulis menghimpun

refrensi dan sumber data berupa jurnal, buku, laporan penelitian, dan media elektronik yang berhubungan terkait dengan penelitian.

1.7.4 Teknik Analisis Data

Teknik analisis data dalam penelitian ini penulis menggunakan data data terkait kerjasama bilateral dalam bidang *cybersecurity* Australia - Indonesia dengan didasari pendekatan kualitatif. Analisis data dilakukan dengan maksud mempertajam fokus pengamatan atau kebenaran data serta memperdalam pokok pokok permasalahan yang diteliti. Data yang dikumpulkan melalui buku, jurnal, penelitian, laporan, media pemerintahan resmi, dan juga situs internet yang relevan terkait penelitian ini.

1.8 Sistematika Penelitian

Sistematika penelitian penelitian ini ditulis secara sistematis yang terdiri dari beberapa bab yaitu :

BAB I : Memuat Pendahuluan, Latar Belakang Masalah, Tinjauan Pustaka, Rumusan Masalah, Tujuan Penelitian, Kerangka Pemikiran, Sintesa Pemikiran, Argumen Utaman, dan Metode Penelitian.

BAB II : **Strategi Peningkatan Cybersecurity Australia 2017 – 2020**

2.1 Strategi Peningkatan Cybersecurity Australia Melalui Australia's International Cyber Engagement Strategy 2017

2.1.1 Cyber Cooperation Program