BAB 1

PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, kemajuan teknologi informasi dan komunikasi telah menciptakan perubahan baru yang mengubah cara kita berinteraksi, bekerja, dan hidup. Internet menjadi tulang punggung masyarakat global, memfasilitasi pertukaran informasi, perdagangan, dan komunikasi antar negara. Mirip dengan teknologi komputer dan internet, komputer dan internet berkontribusi pada pembentukan dunia maya. Kata "*cyberspace*" pertama kali diperkenalkan pada tahun 1984 oleh William Gibson dalam novelnya Neuromancer (Murray, 2007). Namun, bersamaan dengan manfaatnya, kita juga dihadapkan pada tantangan yang tidak dapat terhindarkan.

Indonesia saat ini menduduki populasi internet terbesar keempat di dunia, yang dimana menjadi target empuk bagi pelaku kejahatan siber. Seiring dengan perkembangan teknologi informasi dan penetrasi internet yang semakin meluas, negara ini menghadapi ancaman serius dari serangan siber. Pada tahun 2023, tercatat 86.342 kasus serangan siber, meningkat 12,6% dibandingkan tahun sebelumnya. Serangan ini tidak hanya menyasar sektor pemerintah, tetapi juga sektor swasta, seperti disrupsi layanan publik yang mengganggu, seperti gangguan pada layanan kesehatan dan pendidikan, dapat mempengaruhi akses masyarakat terhadap layanan dasar yang penting. (bssn.go.id)

Dalam konteks globalisasi dan interkoneksi yang semakin erat di era digital, memperkuat kerjasama bilateral dalam keamanan siber bukan hanya menjadi kebutuhan, tetapi juga merupakan kewajiban bagi Indonesia sebagai bagian dari komunitas internasional. Melalui upaya bersama dengan mitra seperti Australia, Indonesia dapat membangun fondasi yang kokoh dalam menghadapi tantangan keamanan siber masa depan dan menjaga kedaulatan digital negara serta kepentingan nasionalnya.

Indonesia merupakan anggota yang aktif dalam berbagai forum PBB, termasuk dalam Konferensi Anggota PBB tentang Kejahatan Transnasional Terorganisir yang telah menetapkan lima kejahatan baru yang harus mendapat perhatian, termasuk kejahatan siber yang dapat terjadi antar negara. Dari sisi Indonesia sendiri, tergolong rentan terhadap kejahatan tersebut dikarenakan letaknya yang strategis dan masyarakatnya yang banyak dan beragam. Sehingga, Pemerintah Indonesia melakukan upaya pencegahan dengan menaruh perhatian khusus terhadap kejahatan lintas negara baru dan berkembang yang telah ditetapkan, serta mengintensifkan kerjasama internasional untuk melindungi kepentingan dan kedaulatan nasional Indonesia. Dalam hal ini, Indonesia mengupayakan peningkatan keamanan siber dengan cara bekerjasama dengan negara lain, baik melalui kerjasama bilateral maupun regional. (Rosy, 2020)

Ancaman siber ini terlihat sangat menakutkan bagi masyarakat dan menjadi penghambat kemajuan bangsa di era digital. Tak heran, pemerintah Indonesia tak tinggal diam. Berbagai upaya dilakukan untuk meningkatkan pertahanan siber nasional, seperti menerbitkan regulasi terkait keamanan siber, membentuk

Lembaga khusus seperti Badan Siber dan Sandi Negara (BSSN), dan tidak ketinggalan untuk meningkatkan kapasitas sumber daya manusia di bidang keamanan siber melalui pendidikan dan pelatihan. (bssn.go.id)

Namun, upaya ini tak cukup jika ditempuh sendirian. Dalam era yang gejolak dan kompleks, kesadaran akan pentingnya kerjasama internasional semakin meningkat. Menghadapi ancaman siber yang semakin canggih dan meresahkan membutuhkan pendekatan yang inklusif dan kolaboratif. Oleh karena itu, langkah-langkah koordinasi antarnegara dan pertukaran informasi yang efektif menjadi esensial dalam menjaga kedaulatan digital dan melindungi kepentingan nasional.

Maka dari itu, Indonesia perlu terus memperkuat kerjasama antar negara dalam menghadapi tantangan keamanan siber, dengan membangun kemitraan strategis yang memungkinkan pertukaran pengetahuan dan pengalaman untuk meningkatkan ketahanan siber nasional.

Serangan *cyber* yang semakin tumbuh dan menjadi ancaman keamanan nasional, sehingga pemerintah membentuk badan untuk melindungi warganya dan menjaga kedaulatan negara khususnya di ranah *cyber*. Melalui peraturan presiden nomor 53 tahun 2017, Badan Cyber dan Sandi Negara (BSSN) dibentuk sebagai organisasi pemerintahan (badan) yang bertanggung jawab untuk membidangi *cyber* nasional danberfungsi menentukan kebijakan *cyber security* nasional dengan peran dan kerjasamaantara pemerintah, sektor swasta serta masyarakat. (bssn.go.id)

Ketersediaan data sensitif dan infrastruktur kritis menjadi daya tarik bagi para pelaku kejahatan siber untuk melakukan berbagai jenis serangan, mulai dari

pencurian data pribadi hingga gangguan terhadap layanan publik. Menyadari hal ini, Pemerintah Indonesia telah mengambil langkah-langkah untuk meningkatkan keamanan siber nasional, seperti menerbitkan regulasi, membentuk lembaga khusus (BSSN), dan meningkatkan kapasitas SDM**.**

Kejahatan siber dapat mengganggu dan menjadi ancaman bagi keamanan nasional suatu negara dikarenakan saat ini banyak negara yang sudah mengkoneksikan data-data dan kontrolnya terhadap beberapa sektor melalui internet atau daring (*online*). Karena luasnya jenis kejahatan siber yang dapat terjadi di internet, hingga kini belum ada klasifikasi dan pengertian pasti dari kejahatan siber itu. Namun, kejahatan siber saat ini telah mendapatkan perhatian internasional sebagai salah satu kejahatan transnasional.

Indonesia pernah menjalin kerjasama dengan beberapa negara yaitu, pertama bekerja sama dengan Singapura, kedua negara telah menandatangani *Memorandum of Understanding* (MoU) tentang Kerjasama Keamanan Siber pada tahun 2016. MoU ini bertujuan untuk meningkatkan kerjasama dalam bidang pertukaran informasi, pengembangan kapasitas, dan penelitian keamanan siber. (bssn.go.id)

Kemudian Amerika Serikat Indonesia dan Amerika Serikat memiliki *Cyber Dialogue* yang diselenggarakan secara berkala untuk membahas isu-isu keamanan siber dan bertukar informasi. Kedua negara juga bekerja sama dalam bidang pelatihan dan pengembangan kapasitas untuk meningkatkan kemampuan personel keamanan siber. (treaty.kemlu.go.id, 2018)

Kemudian juga kerja sama dengan Jepang, Indonesia dan Jepang memiliki MoU tentang Kerjasama Keamanan Siber yang ditandatangani pada tahun 2019. MoU ini bertujuan untuk meningkatkan kerjasama dalam bidang pertukaran informasi, pengembangan kapasitas, dan penelitian keamanan siber.

Selanjutnya Australia, Indonesia dan Australia memiliki MoU tentang Kerjasama Keamanan Siber yang ditandatangani pada tahun 2018. MoU ini bertujuan untuk meningkatkan kerjasama dalam bidang pencegahan dan penanggulangan *cybercrime*, serta pengembangan kapasitas personel keamanan siber. (dfat.gov.au, 2018)

Australia pun menghadapi tantangan serupa. Pada tahun 2022, terjadi 13,5 juta serangan siber di Australia, meningkat 35% dibandingkan tahun sebelumnya. Kedua negara memiliki hubungan bilateral yang kuat, termasuk dalam bidang keamanan siber. Kerjasama Indonesia dan Australia telah terjalin dalam berbagai bidang, seperti pertukaran informasi dan *best practices* tentang ancaman siber terbaru dan strategi untuk mengatasinya, pelatihan dan pengembangan kapasitas SDM di bidang keamanan siber melalui pelatihan dan *workshop*, penyelenggaraan forum dialog dan konsultasi untuk membahas isu-isu keamanan siber dan mencari solusi bersama, kerjasama dalam penanganan insiden siber untuk menangani serangan siber yang besar dan kompleks. (Danny Tran, 2023)

Indonesia memilih Australia sebagai mitra JCCP (*Joint Cyber Community Program*) karena beberapa alasan, pertama karena (kedekatan geografis dan budaya) Australia adalah negara tetangga dengan kesamaan budaya dan sejarah,

memudahkan kerjasama dan komunikasi. Kedua (kepentingan bersama) Indonesia dan Australia memiliki kepentingan bersama dalam memerangi cybercrime dan menjaga stabilitas kawasan Indo-Pasifik. Ketiga (keahlian Australia) Australia memiliki keahlian dan pengalaman luas di bidang keamanan siber yang dapat membantu Indonesia meningkatkan kemampuannya. Keempat (komitmen Australia) Australia telah menunjukkan komitmennya untuk membantu Indonesia dalam meningkatkan keamanan siber. Terakhir (kerjasama yang sudah ada) Indonesia dan Australia telah memiliki kerjasama erat di berbagai bidang, termasuk keamanan siber, dan JCCP merupakan kelanjutan dari kerjasama tersebut. (Kedutaan Besar Australia, 2019)

Keamanan siber di Indonesia masih menghadapi beberapa tantangan yaitu (Kurangnya Kesadaran Masyarakat) Banyak masyarakat belum sadar akan pentingnya keamanan siber, sehingga mudah menjadi korban cybercrime. (Kurangnya Infrastruktur) Infrastruktur keamanan siber di Indonesia belum memadai, membuat negara lebih rentan terhadap serangan siber. (Kekurangan Tenaga Ahli) Indonesia masih kekurangan tenaga ahli keamanan siber yang qualified, sehingga sulit membangun sistem keamanan siber yang kuat. (Hukum dan Regulasi Lemah) Hukum dan regulasi terkait keamanan siber masih lemah, sehingga penegakan hukum terhadap cybercrime menjadi sulit. (Elva A, 2021)

Pemerintah Indonesia telah mengambil langkah-langkah untuk mengatasi tantangan ini, seperti (Meningkatkan Kesadaran Masyarakat) Melakukan berbagai program untuk meningkatkan kesadaran masyarakat tentang pentingnya keamanan siber. (Membangun Infrastruktur) Membangun infrastruktur keamanan siber yang

lebih kuat. (Mengembangkan Tenaga Ahli) Mengembangkan program pendidikan dan pelatihan untuk menghasilkan tenaga ahli keamanan siber yang *qualified*. (Memperkuat Hukum dan Regulasi) Memperkuat hukum dan regulasi terkait keamanan siber. (Elva A, 2021)

Meskipun masih banyak tantangan, Indonesia terus berusaha untuk meningkatkan keamanan sibernya. Keanggotaan Indonesia dalam JCCP Indo-Australia diharapkan dapat membantu Indonesia dalam mencapai tujuan ini.

Salah satu bentuk kerjasama konkrit adalah *Joint Cyber Community Program* (JCCP) yang diluncurkan pada tahun 2018. JCCP bertujuan untuk meningkatkan kesadaran dan pemahaman tentang keamanan siber di kedua negara, memperkuat pertukaran informasi dan *best practices* tentang keamanan siber, meningkatkan kapasitas SDM di bidang keamanan siber, mendorong kerjasama dalam penanganan insiden siber.

Kerjasama JCCP diharapkan dapat menjadi langkah signifikan dalam meningkatkan keamanan siber di Indonesia dan Australia. Program ini berpotensi memberikan dampak positif seperti meningkatnya kesadaran masyarakat, kapasitas SDM yang lebih mumpuni, serta koordinasi dan kolaborasi yang lebih erat dalam menghadapi ancaman siber.

Indonesia dan Australia menjalin kerjasama dalam program *Joint Cyber Community Program* (JCCP) pada tahun 2018, data hacking di Indonesia mengalami peningkatan yang cukup signifikan.

Berikut beberapa contohnya,

Tahun 2018, Kebocoran data 106 juta pengguna *e-commerce* Bukalapak, Kebocoran data 51 juta pengguna Grab, Serangan *ransomware* Petya melanda sejumlah perusahaan dan instansi pemerintah. Tahun 2019, Kebocoran data 91 juta pengguna Bhinneka.com, Kebocoran data 2,3 miliar pengguna Google+, Serangan *ransomware* GandCrab melanda sejumlah perusahaan dan instansi pemerintah.

Tahun 2020. Kebocoran data 96 juta pengguna Tokopedia, Kebocoran data 26 juta pengguna Brizzi, Serangan *ransomware* Maze melanda sejumlah perusahaan dan instansi pemerintah, Peretasan Situs Web Universitas Indonesia, Data Pengguna Tokopedia Bocor di Dark Web, Website DPR RI Down dan Berganti Nama, Situs Web Tempo Down, Penyerangan Terhadap Website Sekretariat Kabinet RI.

Tahun 2021, 2022, 2023, Peretasan Terhadap *Website* BPJS Kesehatan, Kebocoran Data Asuransi Jiwa BRI Life, Serangan DDoS pada Layanan Perbankan, Kasus Penipuan Online, Serangan *Ransomware* pada Bank Syariah Indonesia (blog.privy.id, 2024)

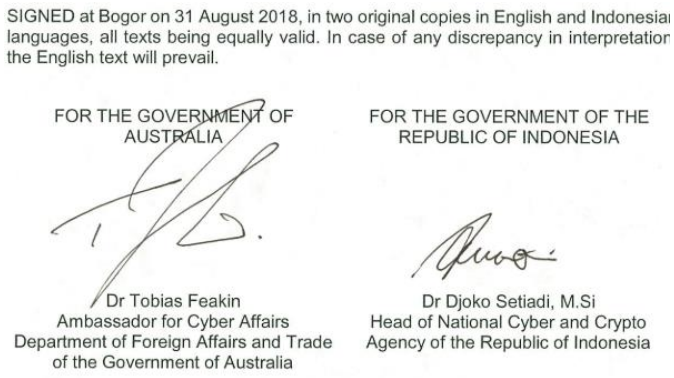
Indonesia dalam JCCP Indo-Australia memiliki potensi untuk meningkatkan keamanan data di Indonesia. Namun, penting untuk mempertimbangkan dengan cermat risiko potensial yang terkait dengan keanggotaan ini. Pemerintah Indonesia harus memastikan bahwa ada kerangka kerja yang jelas untuk transparansi, akuntabilitas, dan perlindungan data sebelum bergabung dengan JCCP. (Nuzulia, A, 2022)

Meskipun berbagai upaya telah dilakukan, Australia masih menghadapi beberapa tantangan dalam mewujudkan keamanan siber yang optimal. Keterbatasan sumber daya, kompleksitas teknologi yang terus berkembang, dan perubahan taktik para pelaku kejahatan siber menjadi tantangan yang perlu diatasi secara berkelanjutan**.** Australia berkomitmen untuk membangun lingkungan digital yang aman dan terpercaya. Melalui investasi berkelanjutan, peningkatan kapasitas SDM, dan kerjasama internasional, Australia berupaya menjadi benteng yang tangguh terhadap serangan siber di era digital.

Dalam konteks ini, kerjasama antar negara seperti *Joint Cyber Community Program* antara Indonesia dan Australia memainkan peran penting dalam melindungi kedua negara dari ancaman siber yang semakin kompleks dan beragam. Melalui pertukaran informasi, pelatihan, dan kerjasama teknis, kedua negara berupaya untuk meningkatkan kesiapsiagaan dan respons terhadap ancaman keamanan siber, serta membangun ekosistem keamanan siber yang kokoh dan terpercaya.

Joint Cyber Community Program ditandatangani melalui MoU pada tanggal 31 Agustus 2018 di Bogor oleh BSSN dan *DFAT.* Indonesia memilih Australia sebagai mitra dalam *Joint Cyber Community Program* (JCCP) karena beberapa alasan. Pertama, Australia memiliki komitmen kuat untuk memerangi *cybercrime* dan telah mengembangkan program-program yang efektif dalam hal ini. Kedua, Australia memiliki keahlian teknis yang mumpuni di bidang *cybersecurity*. Ketiga, Australia memiliki hubungan yang baik dengan Indonesia, termasuk dalam bidang keamanan siber. Kerjasama antara Indonesia dan Australia dalam JCCP diharapkan dapat

meningkatkan kapasitas kedua negara dalam memerangi *cybercrime* dan melindungi infrastruktur siber mereka. (dfat.gov.au, 2018)


SIGNED at Bogor on 31 August 2018, in two original copies in English and Indonesia languages, all texts being equally valid. In case of any discrepancy in interpretatior the English text will prevail.

FOR THE GOVERNMENT OF AUSTRALIA

Dr Tobias Feakin
Ambassador for Cyber Affairs
Department of Foreign Affairs and Trade
of the Government of Australia

FOR THE GOVERNMENT OF THE REPUBLIC OF INDONESIA

Dr Djoko Setiadi, M.Si
Head of National Cyber and Crypto
Agency of the Republic of Indonesia

Gambar 1.1 Tanda Tangan MoU

Salah satu contoh nyata kerjasama keamanan siber Indonesia-Australia adalah *Cyber Boot Camp*. Program ini merupakan bagian dari *Cyber Cooperation Program* yang diinisiasi oleh *Department of Foreign Affairs and Trade* (DFAT) Australia. *Cyber Boot Camp* memberikan pelatihan dan pembelajaran kepada para ahli dan profesional di bidang keamanan siber dari Indonesia. Pelatihan ini mencakup berbagai topik, seperti analisis forensik digital, respon insiden siber, dan kriptografi. Program ini telah berhasil meningkatkan kapasitas SDM di bidang keamanan siber di Indonesia. Para peserta pelatihan mendapatkan pengetahuan dan keahlian yang baru untuk dapat lebih efektif dalam memerangi *cybercrime*. (bssn.go.id)

Meskipun data hacking di Indonesia masih terjadi, program JCCP telah memberikan dampak positif dalam meningkatkan keamanan siber di kedua negara.

Kerjasama dan kolaborasi antar lembaga *cyber security* perlu terus ditingkatkan untuk memerangi *cybercrime* secara efektif.

Pada penelitian ini, terdapat beberapa bahan acuan dari penelitian terdahulu yang dapat dijadikan sebagai rujukan, pertama, penelitian yang dibuat oleh Monica Romauly Weu dari Universitas Komputer Indonesia, Bandung pada tahun 2020 mengenai "Kerjasama Pemerintah Indonesia Dan Pemerintah Kerajaan Inggris Dalam Bidang Keamanan Siber". Dalam penelitian ini menganalisis tentang kerjasama bilateral antara Indonesia dan Inggris untuk meningkatkan keamanan siber di kedua negara dan memperkuat pertahanan kolektif terhadap ancaman siber global. Kerjasama ini penting karena kedua negara menghadapi berbagai ancaman siber, dan kerjasama dapat membantu mereka mengatasi ancaman tersebut melalui pertukaran informasi, pengembangan kapasitas, dan operasi bersama.

Penelitian yang dibuat oleh Afifah Fidina Rosy dari Sebelas Maret University pada tahun 2020 mengenai "Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional Di Bidang Keamanan Siber". Dalam penelitian ini menganalisis tentang upaya Indonesia dalam meningkatkan keamanan nasional di bidang keamanan siber melalui kerjasama internasional. Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif ini menggunakan proses dari pengolahan data. Persamaan antara judul "Kerjasama internasional Indonesia: memperkuat keamanan nasional di bidang keamanan siber" dan analisis "Kerjasama Cyber Security Indonesia Dan Australia Melalui *Joint Cyber Community Program*" terletak pada penekanan pada penguatan keamanan nasional di bidang keamanan siber melalui kerjasama internasional**.** Perbedaannya terletak

pada ruang lingkupnya, untuk yang pertama kerjasamanya internasional yang dimana berarti kerjasama dengan banyak negara, sedangkan yang peneliti buat kerjasama dengan satu negara yaitu Australia. Kekurangan penelitian adalah judulnya kurang spesifik, seperti hanya menyebutkan kerjasama internasional dan tidak diketahui siapa mitra atau partner kerjasamanya.

Penelitian yang dibuat oleh Muhamad Rizki Hapizon, Khairur Rizki, Mahmuluddin dari Universitas Mataram, NTB, Indonesia pada tahun 2022 mengenai "Analisis Kerjasama *Cyber Security* Indonesia-Australia Dalam Menangani Kejahatan Siber Di Indonesia". Dalam penelitian ini menganalisis bagaimana kerjasama keamanan siber antara Indonesia dan Australia untuk menangani kejahatan siber di Indonesia, dengan fokus pada bentuk, ruang lingkup, tujuan, peran masing-masing negara, dan dampaknya. Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif ini menggunakan proses dari pengolahan data. Persamaannya adalah sama-sama meneliti kerjasama keamanan siber antara Indonesia dan Australia, dan fokus pada upaya kedua negara dalam memperkuat keamanan siber Indonesia dan memerangi kejahatan siber di wilayah tersebut. Perbedaannya adalah cakupan analisisnya lebih luas, meneliti berbagai aspek kerjasama *cyber security* Indonesia dan Australia secara menyeluruh, sedangkan yang peneliti buat cakupannya berfokus pada program kerjasama *Joint Cyber Community Program* (JCCP). Kekurangan penelitian ini tidak mencakup semua aspek kerjasama *cyber security* Indonesia-Australia, seperti program dan kegiatan yang dilakukan, peran aktor non-negara, dan dampak kerjasama terhadap keamanan siber di kawasan. fokus pada kerjasama formal antar pemerintah, dan

tidak mempertimbangkan kerjasama informal antar sektor swasta atau masyarakat sipil dan tidak memberikan detail yang cukup tentang program dan kegiatan kerjasama yang dilakukan, seperti tujuan, implementasi, dan hasil yang dicapai.

Penelitian yang dibuat oleh Hegar Krisnaduta dari Universitas Pasundan Bandung pada tahun 2019 mengenai "Kerjasama Indonesia-Australia di Bidang Keamanan dalam Mengatasi *Cyber Crime* di Indonesia melalui *Program Cyber Policy Dialogue*". Dalam penelitian ini menganalisis berbagai aspek kerjasama *cyber security* Indonesia-Australia yang dilakukan melalui program *Cyber Policy Dialogue* (CPD). Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif ini menggunakan proses dari pengolahan data. Persamaannya adalah membahas berbagai topik yang terkait dengan kerjasama *cyber security* Indonesia-Australia, memahami kerjasama *cyber security* Indonesia Australia dan untuk meningkatkan kerjasama. Perbedaannya adalah terletak pada fokus penelitiannya yaitu fokus pada program *Cyber Policy Dialogue* (CPD), yang merupakan forum dialog dan kerjasama antar pemerintah Indonesia dan Australia, sedangkan yang peneliti buat fokus pada program *Joint Cyber Community Program* (JCCP), yang merupakan program pelatihan dan pengembangan kapasitas untuk meningkatkan kemampuan *cyber security* kedua negara. Kekurangan penelitian ini adalah hanya memberikan deskripsi tentang kerjasama *cyber security* Indonesia-Australia, dan tidak melakukan analisis kritis terhadap efektivitas dan keberhasilan kerjasama tersebut.

Terakhir, penelitian dari Ujang Priyono, Yoedhi Swastanto, Budi Pramono dari Universitas Pertahanan Republik Indonesia pada tahun 2023 mengenai *Cyber*

Diplomacy (*A Perspective From Indonesia -Australia Cyber Cooperation*). Dalam penelitian menganalisis kerjasama *cyber security* antara Indonesia dan Australia dari sudut pandang Indonesia. Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif ini menggunakan proses dari pengolahan data. Persamaannya adalah membahas tentang kerjasama *cybersecurity* antara Indonesia dan Australia, dan bertujuan untuk memahami kerjasama *cybersecurity* Indonesia-Australia dan untuk meningkatkan kerjasama tersebut di masa depan. Untuk perbedaannya analisisnya lebih fokus pada aspek diplomatik kerjasama *cybersecurity*, seperti dialog, negosiasi, dan pembangunan kepercayaan, sedangkan yang peneliti lebih fokus pada aspek program JCCP, seperti tujuan, implementasi, dan hasil yang dicapai.

Berdasarkan latar belakang yang telah diuraikan di atas, maka peneliti tertarik untuk melakukan penelitian dengan judul :

"**KERJASAMA INDONESIA DAN AUSTRALIA MELALUI JOINT CYBER COMMUNITY PROGRAM UNTUK MENINGKATKAN KEAMANAN SIBER DI INDONESIA"**

Penelitian ini tentunya didukung oleh Mata Kuliah pada Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Komputer Indonesia, sebagai berikut :

1. Cyber Security

   Mata kuliah *Cyber Security* dalam Hubungan Internasional (HI) membahas tentang ancaman keamanan siber yang dihadapi oleh negara-

negara di dunia dan bagaimana negara-negara tersebut bekerja sama untuk mengatasinya.

2. Hubungan Internasional Di Asia Tenggara

   Mata kuliah ini membahas tentang politik regional di kawasan Asia Tenggara, termasuk kerjasama antar negara di berbagai bidang, seperti keamanan, ekonomi, dan sosial budaya. Kerjasama *cybersecurity* Indonesia-Australia dapat menjadi salah satu contoh kerjasama regional di bidang keamanan.

3. Studi Keamanan Internasional

   Mata kuliah ini membahas tentang studi kasus kerjasama internasional di berbagai bidang, seperti keamanan, ekonomi, dan lingkungan. Kerjasama *cybersecurity* Indonesia-Australia dapat menjadi salah satu contoh studi kasus kerjasama internasional di bidang keamanan.

1.1 Rumusan Masalah

Dari latar belakang tadi terdapat beberapa rumusan masalah penelitian sebagai berikut:

1.1.1 Rumusan Masalah Makro

Mengacu pada latar belakang yang sudah disampaikan di atas, peneliti merumuskan masalah sebagai berikut**: "Bagaimana Kerjasama Indonesia dan Australia Melalui Joint Cyber Community Program (JCCP) dalam meningkatkan keamanan siber di Indonesia?".**

1.1.2 Rumusan Masalah Mikro

Dalam penelitian ini masalah yang akan dibahas tentu akan berkembang seiring dengan waktu, hubungan variabel dengan variabel lain akan berkembang dan berhubungan menjadi suatu masalah yang akan diteliti. Maka, identifikasi masalah pada penelitian ini sebagai berikut :

1. Apa kendala kerjasama Indonesia dan Australia melalui JCCP untuk meningkatkan keamanan siber di Indonesia?
2. Bagaimana strategi kerjasama yang diterapkan JCCP?
3. Bagaimana hasil kerjasama Indonesia dan Australia melalui JCCP untuk menangani ancaman keamanan siber di Indonesia?

1.2 Batasan Masalah

Penelitian ini akan memfokuskan diri pada analisis kerjasama keamanan siber yang diterapkan oleh pemerintah Indonesia dan Australia melalui *Joint Cyber Community Program*. Fokus utama penelitian adalah pada kerjasama keamanan siber Indonesia dan Australia yang telah diimplementasikan atau diusulkan oleh kedua negara untuk menghadapi ancaman siber di era digital melalui *Joint Cyber Community Program*. Penelitian ini mengambil batas waktu 2018-2024. Alasannya karena kerjasama ini terjalin dan terbentuk pada tahun 2018, lalu 2024 karena program ini masi terus berjalan sampai hari ini dan kerjasama ini bersifat berkelanjutan. Penelitian ini tidak akan membahas aspek teknis keamanan siber, tetapi akan berfokus pada evaluasi kerjasama Indonesia dan Australia yang dilakukan melalui program tersebut. Selain itu, batasan penelitian tidak mencakup

analisis aspek hukum atau regulasi yang terkait dengan keamanan siber, melainkan akan difokuskan pada aspek kebijakan dan strategis dalam mengatasi ancaman siber melalui kerjasama lintas negara yang terwujud dalam *Joint Cyber Community Program.*

1.4 Maksud Dan Tujuan Penelitian

1.4.1 Maksud

Maksud dalam penelitian ini adalah mengetahui bagaimana terjadinya kerjasama *cyber security* Indonesia dan Australia melalui *Joint Cyber Community Program.*

1.4.2 Tujuan Penelitian

Penelitian bertujuan untuk:

1. Menganalisis kendala program kerjasama JCCP dalam pelaksanaannya di Indonesia.
2. Menganalisis strategi kerjasama apa yang diterapkan JCCP.
3. Menganalisis hasil kerjasama JCCP untuk menangani ancaman keamanan siber di Indonesia

1.5 Kegunaan Penelitian

1.5.1 Kegunaan Teoritis

Penelitian ini bertujuan untuk memberikan pemahaman yang mendalam tentang kerjasama *cyber security* antara Indonesia dan Australia melalui *Joint Cyber Community Program*, khususnya dalam konteks kebijakan keamanan siber. Dengan fokus pada analisis kerjasama antar negara ini, penelitian ini akan

membahas program kerjasama yang telah diimplementasikan atau diusulkan oleh kedua negara untuk mengatasi ancaman siber di era digital melalui *Joint Cyber Community Program.*

1.5.2 Kegunaan Praktis

1. Bagi Peneliti

   Sebagai syarat untuk penyelesaian tugas akhir untuk kelulusan di jurusan Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Komputer Indonesia. Selain itu penelitian ini sangat barmanfaat bagi peneliti sebagai buah karya ilmiah. Mengetahui perspektif, ilmu dan keterampilan baru di mana para pemimpin nasional mempengaruhi kebijakan luar negeri negara dalam pemenuhan kepentingan nasional.

2. Bagi Program Studi

   Diharapkan penelitian ini bisa dijadikan sebagai bahan kajian bagi mahasiswa ilmu hubungan internasional lain agar bisa memahami dan mempernudah penelitian selanjutnya mengenai *cyber security*.