

Judul Skripsi:

KERJASAMA BADAN SIBER DAN SANDI NEGARA (BSSN) DAN DEPARTEMEN OF FOREIGN AFFAIRS AND TRADE (DFAT) DALAM MENINGKATKAN KEAMANAN SIBER INDONESIA MELALUI PROGRAM SHARE INFORMATION AND BEST PRACTICE TAHUN (2019-2022)

Tugas Akhir Skripsi ini di ajukan untuk memenuhi persyaratan dalam memperoleh gelar sarjana
Hubungan Internasional

Nama: Amanda Rich Margareth Bakara

NIM: 1910412055



**HUBUNGAN INTERNASIONAL
ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS PEMBANGUNAN NASIONAL
"VETERAN" JAKARTA**

PENGESAHAN SKRIPSI

Skripsi ini diajukan oleh:

Nama : Amanda Rich Margareth Bakara

NIM : 1910412055

Program Studi : SI Hubungan Internasional

Judul Skripsi : KERJA SAMA BADAN SIBER DAN SANDI NEGARA (BSSN) DAN DEPARTEMEN OF FOREIGN AFFAIRS AND TRADE (DFAT) DALAM MENINGKATKAN KEAMANAN SIBER INDONESIA MELALUI PROGRAM SHARE INFORMATION AND BEST PRACTICE TAHUN (2019-2022)

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar sarjana pada Program Studi Hubungan Internasional. Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Pembangunan Nasional Veteran Jakarta

Pembimbing I



(Dr.Mansur,M.Si.)

Penguji I



(Dr.Nurmasari Situmeang,M.Si.)

Penguji II



(I Nyoman Aji Suadhana Rai,MIR)

Kepala Program Studi
Hubungan Internasional



(Wiwiek Rukmi Dwi A.,S.IP,M.Si)

Ditetapkan di : Jakarta

Tanggal Ujian : 16 January 2024

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar:

Nama : Amanda Rich Margareth Bakara
NIM : 1910412055
Program Studi : S1 Hubungan Internasional

Bilama di kemudian hari ditemukan ketidaksesuaian dengan pernyataan ini maka, saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Bekasi, January 2024

Yang menyatakan,



(Amanda Rich Margareth Bakara)

SURAT PERSETUJUAN PUBLIKASI ILMIAH

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta,
saya yang bertandatangan dibawah ini:

Nama : Amanda Rich Margareth Bakara

NIM : 1910412055

Fakultas : Ilmu Sosial dan Ilmu Politik

Program Studi : Hubungan Internasional

Judul Skripsi : KERJA SAMA BADAN SIBER DAN SANDI NEGARA (BSSN) DAN
DEPARTEMEN OF FOREIGN AFFAIRS AND TRADE (DFAT) DALAM
MENINGKATKAN KEAMANAN SIBER INDONESIA MELALUI PROGRAM SHARE
INFORMATION AND BEST PRACTICE TAHUN (2019-2022)

Dengan ini saya menyatakan bahwa saya menyetujui untuk:

1. Memberikan hak saya bebas royalti kepada Perpustakaan UPNVJ atas Penelitian karya ilmiah saya demi pengembangan ilmu pengetahuan.
2. Memberikan hak menyimpan, mengalih mediakan atau mengalih formatkan, mengolah pangkalan data (database), mendistribusikan, serta menampilkan dalam bentuk softcopy untuk kepentingan akademis kepada perpustakaan UPNVJ, tanpa perlu meminta izin dari saya selama tetap mencantumkan nama saya sebagai Peneliti/pencipta.
3. Bersedia dan menjamin untuk menanggung secara pribadi tanpa melibatkan pihak perpustakaan UPNVJ dari semua bentuk tuntutan hukum yang timbul atas pelanggaran hak cipta dalam karya ilmiah ini.

Demikian pernyataan ini saya buat dengan sebenar-benarnya dan semoga digunakan sebagaimana mestinya.

Dibuat di : Bekasi

Pada tanggal : 17 January 2024

Yang menyatakan,



(Amanda Rich Margareth Bakara)

**PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK
KEPENTINGAN AKADEMIS**

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Amanda Rich Margareth Bakara

NIM : 1910412055

Fakultas : Ilmu Sosial dan Ilmu Politik

Program Studi : S1 Hubungan Internasional

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

**KERJA SAMA BADAN SIBER DAN SANDI NEGARA (BSSN) DAN
DEPARTEMEN OF FOREIGN AFFAIRS AND TRADE (DFAT) DALAM
MENINGKATKAN KEAMANAN SIBER INDONESIA MELALUI
PROGRAM SHARE INFORMATION AND BEST PRACTICE TAHUN
(2019-2022)**

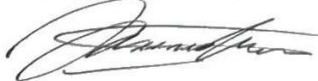
Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini. Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya:

Dibuat di : Bekasi, January 2024

Pada tanggal : 17 January 2024

Yang menyatakan,



(Amanda Rich Margareth Bakara)

**KERJA SAMA BADAN SIBER DAN SANDI NEGARA (BSSN) DAN
DEPARTEMEN OF FOREIGN AFFAIRS AND TRADE (DFAT) DALAM
MENINGKATKAN KEAMANAN SIBER INDONESIA MELALUI
PROGRAM SHARE INFORMATION AND BEST PRACTICE TAHUN (2019-2022)**

ABSTRAK

Keamanan siber diartikan sebagai usaha untuk menjamin pencapaian dan pemeliharaan keamanan data dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkup ruang siber. Terutama munculnya fenomena pandemi Covid 19 yang terjadi di periode 2019 hingga 2022 yang menjadikan peluang ancaman dan kejahatan siber meningkat secara drastis, melihat kondisi tersebut berbagai negara berusaha meningkatkan keamanan sibernya, termasuk Indonesia melakukan kerja sama dengan Australia. ok pelaksanaannya, kerjasama ini diwakili oleh Badan Siber dan Sandi Negara (BSSN) dari Indonesia dan Departemen Foreign Affairs and Trade (DFAT) dari Australia melalui program share information and best practice. Penulis menganalisis menggunakan teori kerjasama bilateral dan keamanan siber. Metode penelitian deskriptif kualitatif digunakan untuk menganalisis bentuk kerjasama yang ada antara Badan Siber dan Sandi Negara (BSSN) dengan

Departemen Foreign Affairs and Trade (DFAT) melalui program share information and best practice yang didasarkan pada MoU antara keduanya negara di bidang keamanan siber tahun 2018. Ada beberapa kegiatan yang dihasilkan dari kerjasama tersebut yaitu; Cyber Boot Camp, Kebijakan Cyber ASPI (Institut Kebijakan Strategis Australia). Lokakarya, Koneksi Bisnis Cyber: Austrade dan AustCyber di dunia digital ekonomi, dan Dialog Kebijakan Siber. Hasil dari penelitian ini membuktikan bahwa kerjasama yang di lakukan antara Badan Siber dan Sandi Negara (BSSN) dengan Departemen Foreign Affairs and Trade (DFAT) melalui program share information and best practice yang didasarkan pada MoU merupakan salah satu faktor meningkatnya keamanan siber di Indonesia.

Kata kunci: Keamanan siber, Badan Siber dan Sandi Negara, Departemen Foreign Affairs and Trade (DFAT) , Share Information and Best Practice.

ABSTRACT

Cybersecurity is defined as an effort to ensure the achievement and maintenance of data security and user assets against relevant security risks within the scope of cyberspace. Especially the emergence of the Covid 19 pandemic phenomenon that occurred in the period 2019 to 2022 which made the opportunity for cyber threats and crimes increase drastically, seeing these conditions various countries are trying to improve their cybersecurity, including Indonesia in cooperation with Australia. In its implementation, this cooperation is represented by the State Cyber and Crypto Agency (BSSN) from Indonesia and the Department of Foreign Affairs and Trade (DFAT) from Australia through the share information and best practice program. The author analyzes using the theory of bilateral cooperation and cybersecurity. The descriptive qualitative research method is used to analyze the form of cooperation that exists between the State Cyber and Crypto Agency (BSSN) and the Department of Foreign Affairs and Trade (DFAT) through the share information and best practice program based on the MoU between the two countries in the field of cybersecurity in 2018. There are several activities resulting from the collaboration, namely; Cyber

Boot Camp, ASPI (Australian Strategic Policy Institute) Cyber Policy, Workshop, Cyber Business Connection: Austrade and AustCyber in the digital economy, and Cyber Policy Dialogue. The results of this study prove that the cooperation between the National Cyber and Crypto Agency (BSSN) and the Department of Foreign Affairs and Trade (DFAT) through the share information and best practice program based on the MoU is one of the factors increasing cyber security in Indonesia

Keywords: *Cyber Security, Cyber Policy of the National Cyber and Crypto Agency, Department of Foreign Affairs and Trade (DFAT), Share Information and Best Practice.*

KATA PENGANTAR

Penulis menyampaikan rasa hormat dan terima kasihnya kepada Yesus Kristus yang selalu menjadi pendukung dan sahabatnya sepanjang hidupnya. Atas kebaikan dan berkah-Nyalah penulis dapat menyelesaikan skripsi yang berjudul “Kerjasama antara Badan Siber dan Sandi Negara (BSSN) dan Departemen Luar Negeri dan Perdagangan (DFAT) untuk memperbaiki keadaan di Indonesia. Keamanan siber melalui program Share Informaton and Best Practice periode 2019-2022”. Penelitian ini bertujuan untuk memenuhi beberapa persyaratan untuk memperoleh gelar sarjana pada Fakultas Hubungan Internasional Universitas Pembangunan Negeri “Veteran” Jakarta. Selain itu, penulis berharap penulisan skripsi ini dapat memperluas pengetahuan bagi pembaca khususnya mahasiswa hubungan internasional. Selama proses penulisan skripsi ini, penulis banyak menemui kesulitan dan hambatan tapi atas usaha dan kemampuan maksimal yang Tuhan berikan kepada penulis serta bantuan dan dukungan semua pihak, maka penulisan skripsi ini dapat terselesaikan.

Dalam kesempatan ini peneliti juga mengucapkan terima kasih yang sebesar- besarnya kepada orang tua peneliti atas kasih sayang, doa serta dukungan moril dan materiil yang diberikan kepada penulis palsu. Terima kasih atas segala pancaran cinta dan doa yang selalu mengiringi setiap langkah penulis. Selain peran penting sebagai instruktur, Bapak Dr. Mansur, Mas Dairatul Ma`arif dan Ibu Nurmasari atas kesabaran dan kesediaannya memberikan bimbingan selama penyusunan karya ilmiah ini. Akhir kata, peneliti berharap kepada seluruh pembaca karya ilmiah ini agar karya ilmiah ini dapat bermanfaat bagi dunia akademis dan dunia praktik khususnya untuk penelitian yang berkaitan dengan kolaborasi di bidang keamanan siber. Penulis masih memiliki banyak kesenjangan dalam pengetahuan dan pengalamannya. Topik yang disebutkan dalam skripsi ini maupun dalam penulisannya masih mempunyai banyak kesenjangan. Oleh karena itu, penulis dengan senang hati menerima berbagai masukan dari para pembaca berupa kritik dan saran yang bersifat membangun demi perbaikan penulisan skripsi di masa yang akan datang.

Bekasi, July 2023

Amanda Rich Margareth Bakara

DAFTAR ISI

HALAMAN PENGESAHAN	i
ABSTRAK	v
ABSTRACT	vii
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
BAB I PENDAHULUAN	1
I.1 Latar Belakang Masalah	1
I.2 Rumusan Masalah	11
I.3 Tujuan Penelitian	12
I.4 Manfaat Penelitian	12
1.4.1 Manfaat Praktis	13
1.4.2. Manfaat Akademis	13
I.5 Sistematika Penulisan	13
BAB II TINJAUAN PUSTAKA	15
II.1 Konsep Dan Teori Penelitian	15
II.1.1 Kerjasama Bilateral	15
II.1.2 Keamanan Siber	18
II.1 Kerangka Pemikiran	21
BAB III METODE PENELITIAN	25
III.1 Objek Penelitian	25
III.2 Jenis Penelitian	25
III.3 Teknik Pengumpulan Data	27
III.4 Sumber Data	28
III.5 Teknik Analisis Data	29
III.6 Tabel Rencana Waktu	30
BAB IV	31
GAMBARAN UMUM KEAMANAN SIBER INDONESIA DAN AUSTRALIA	31
IV.1 Kondisi Ruang Keamanan Siber Indonesia dan Australia	31

IV.1.1 Ruang Keamanan Siber di Indonesia	31
IV.1.2 Ruang Keamanan Siber di Australia	41
IIV.2 Faktor Kerjasama Keamanan Siber Indonesia dan Australian	46
IV.2.1 Perang Siber Antara Indonesia dan Australia	46
IV.2.2 Faktor Sumber Daya Manusia	51
IV.2.3 Faktor Strategi Keamanan Siber Indonesia dan Australia	53
IV.3 MoU BSSN dan DFAT	57
BAB V KERJA SAMA BADAN SIBER DAN SANDI NEGARA (BSSN) DAN DEPARTEMEN OF FOREIGN AFFAIRS AND TRADE (DFAT) DALAM ATKAN KEAMANAN SIBER INDONESIA MELALUI PRORAM SHARE INFORMATION AND BEST PRACTICE DATA KEJAHATAN SIBER DI INDONESIA	61
V.1 Data kejahatan siber di Indonesia	61
V.2 Komitmen Bersama Dalam Best Practice and Share Information	65
V.2.1 Komitmen bersama dalam Share Information	65
V.2.2 Komitmen Bersama Dalam Best Practice	65
V.3 Implementasi Program Share Information	66
V.4 Implementasi Program Best Practice	67
BAB VI	77
PENUTUP	77
VI.1 Kesimpulan	77
VI.2 Saran	78
DAFTAR PUSTAKA	79
DAFTAR LAMPIRAN	83

DAFTAR TABLE

Tabel 2.1 tabel jumlah dan jenis kejahatan siber 61

DAFTAR GAMBAR

Gambar 1 jumlah Serangan Siber January-Agustus Tahun 2019-2020	6
Gambar 1.1 kerjasama Indonesia dengan Australia dalam keamanan siber	68
Gambar 1.2 Pelatihan Jaga Keamanan Siber Nasional ke Kementerian,TNI.	71
Gambar 1.3 pelatihan generasi muda terhadap keamanan siber	72

BAB I PENDAHULUAN

I.1 LATAR BELAKANG

Selama beberapa dekade belakangan ini pertumbuhan serta perkembangan teknologi informasi dan komunikasi telah memberikan pengaruh baik, perkembangan tersebut telah memberikan dampak terhadap pertumbuhan ekonomi global dan memberikan dampak terhadap persaingan, produktivitas, dan keikutsertaan warga negara dalam jumlah yang lebih tinggi. Akan tetapi, adanya beberapa tantangan yang berhubungan dengan ancaman dalam keamanan siber dikarenakan masyarakat, pengusaha, dan instansi pemerintahan sebagian besar terkoneksi dan terhubung di dunia digital, maka dari itu dibutuhkannya perhatian dalam mengembangkan keamanan siber (*cyber security*) yang lebih ketat. Terutama melihat kondisi dalam periode 2019-2022 yakni selama masa pandemi covid 19 yang menyebabkan berubahnya sebagian besar pola interaksi sosial manusia baik dalam bidang perekonomian, pendidikan dan seluruh aspek pola kehidupan masyarakat. Dengan demikian munculnya beberapa sebutan baru yang muncul dalam aspek sosial masyarakat seperti seminar online, bekerja dari rumah (*work from home*), layanan kesehatan online, pembelajaran jarak jauh (*school from home*), serta kegiatan belanja online pun semakin meningkat. Meskipun dengan adanya perubahan pola kehidupan masyarakat global secara online telah memberikan kemudahan bagi kehidupan manusia, perubahan ini dapat menimbulkan risiko seperti terjadinya kegagalan sistem akibat serangan malware, penipuan belanja online, pencurian data, pemalsuan data, aktivitas matamata (*phishing*) bahkan gangguan dalam konferensi video (serangan zoom).

Kejahatan yang terjadi di Indonesia semenjak adanya pandemi Covid 19 ini meningkat sangat pesat dikarenakan pola kehidupan masyarakat yang berubah menjadi serba online yang dimana penggunaan internet di Indonesia pun meningkat sehingga ancaman ancaman siber di Indonesia mengalami peningkatan sangat drastis, dan Indonesia pun merupakan salah satu negara terbesar di Asia Tenggara yang dimana Indonesia memiliki potensi dalam politik regional serta ekonomi. Banyaknya aktifitas serta akses dalam bidang politik, ekonomi dan pertahanan negara dilakukan melalui jaringan sistem internet, sehingga ancaman keamanan siber pun menjadi hal yang serius bagi negara Indonesia. Keamanan siber merupakan kebutuhan nyata dan mendesak karena dampaknya berpotensi merusak atau mengganggu kehidupan, negara, bahkan seluruh dunia. Sehingga dengan adanya peluang ancaman siber di Indonesia dan Indonesia pun masih membutuhkan keamanan siber yang mumpuni sehingga dalam meningkatkan keamanan siber di Indonesia, dibutuhkan nya campur tangan dan kerjasama dari negara lain salah satunya dengan negara Australia.

Keamanan siber didasarkan pada MoU tanggal 31 Agustus 2018. BSSN dan DFAT bekerjasama di banyak bidang seperti berbagi informasi dan praktik terbaik, peningkatan kapasitas dan peningkatan konektivitas, teknis ekonomi digital, dan kejahatan siber. Kerjasama antara kedua negara, khususnya di bidang keamanan siber, tentunya merupakan salah satu hal yang membantu mencegah dan menghalangi kejahatan siber. Kerja sama yang terjalin antara Banda Siber dan Sandi Negara atau BSSN (sebagai perwakilan Indonesia) dan Departemen Luar Negeri dan Perdagangan atau DFAT (perwakilan Australia) untuk memperkuat Keamanan Siber merupakan salah satu strategi internasional Indonesia untuk mencegah kejahatan siber. Duta Besar Australia Tobias Feakin memuji sejumlah kegiatan yang telah dilakukan, termasuk program pelatihan online, dimana program ini memberikan kesempatan kepada peserta program untuk berdiskusi dan berbagi pengalaman mengenai permasalahan keamanan siber yang ada.

Menurut pandangan penulis, kegiatan serta kerjasama yang telah penulis paparkan diatas menjadi suatu kesuksesan antara negara Indonesia dan juga Australia dalam kepentingan meningkatkan keamanan siber (*cybersecurity*) yang telah dilakukan melalui bagan BSSN dan dibantu oleh DFAT. Dengan adanya kerjasama serta kegiatan tersebut menunjukkan adanya peningkatan terhadap komitmen Indonesia terhadap keamanan siber (*cyber security*) .

Bukti bahwa keberhasilan kerjasama bilateral antara Indonesia dan Australia bisa di lihat dari GCI pada tahun 2018 yang hal tersebut membawa keuntungan untuk Indonesia, menurut penulis kerja sama yang terjalin antara Indonesia dan Australia pada bidang keamanan siber ini mampu meningkatkan hubungan antara Indonesia dengan Australia kehubungan yang lebih baik dan dekat. Dan memang sudah semestinya juga bahwa negara negara yang memiliki keterbatasan dalam keamanan dan pertahanan siber membutuhkan kerjasama dengan negara negara yang memiliki potensi yang lebih baik dan mumpuni untuk membantu meningkatkan keamanan siber serta pertahanan siber.

Fungsi BSSN selama ini telah terlaksanakan dengan memberikan pembinaan kepada komunitas keamanan siber. Pembinaan yang diberikan BSSN di wujudkan dalam kegiatan Membangun Komunitas dan Berbagi Informasi di Sektor Ekonomi Digital dihadiri oleh Para Pejabat Tinggi dari BSSN, Bais TNI, Bareskrim Polri, BIN, dan komunitas keamanan siber. Kegiatan ini bertujuan untuk mengoordinasikan kegiatan fungsional dalam rangka kerja sama, koordinasi, sinergi, dan berbagi informasi.

Tahapan dalam peningkatan keamanan siber juga menjadikan sebuah tolak ukur dan praktek terbaik (Best Practices and Benchmark) dengan

menerapkan praktik-praktik terbaik dalam bidang keamanan siber di wilayah ASEAN, Asia, dan seluruh dunia.

Perubahan gaya hidup warga negara Indonesia di masa wabah Covid-19 yang semakin tergantung pada internet turut berkontribusi terhadap meningkatnya jumlah perusahaan penyerang siber yang hampir semuanya bekerja dari rumah. Adanya data laporan dari Badan Siber Nasional (BSSN) selama periode Januari hingga Desember 2020 mencatat adanya peningkatan serangan siber di Indonesia selama pandemi Covid-19, mencapai 495,3 juta serangan yang berjenis pencurian data melalui perangkat lunak berbahaya (malware)¹ (Pusat Operasi Keamanan Siber Nasional, 2021). Pada tanggal 10 Desember 2020 pun tercatat adanya anomali trafik tertinggi dengan jumlah mencapai 7.311.606 anomali. Menurut data dari ² (Pusiknas Polri, 2022) Serangan terbanyak terjadi Pada bulan Maret 2020, terjadi total 22 insiden siber yang berkaitan dengan pandemi COVID-19.

Mengingat tingginya serangan yang terjadi, diperlukan tata kelola yang baik dalam ruang siber yang mengarah pada aspek keamanan untuk membantu memenuhi kebutuhan serta mendapatkan kepercayaan masyarakat. Saat ini, penyelesaian permasalahan di ruang siber Indonesia masih belum terpadu dan belum sepenuhnya terintegrasi dengan baik sehingga tata kelolanya masih bersifat parsial. Hal ini dapat menjadi ancaman bagi ketahanan dan keamanan siber masyarakat, korporasi, bagan, dan penyelenggara pelayanan publik yang tentunya dapat berdampak secara strategis atau sistemik serta dapat memengaruhi stabilitas negara, sehingga bagi penulis pun dampak dari fenomena ini juga dapat di katakan sebagai ancaman dalam aspek Ideologi, Politik, Ekonomi, Sosial, Budaya,

Pertahanan, dan Keamanan yang disingkat sebagai IPOLEKSOSBUDHANKAM. Dengan tingginya penggunaan internet di Indonesia ini bisa dilihat bahwa resiko terhadap keamanan siber terhadap kejahatan kejahatan siber pun begitu besar, adanya penggunaan internet yang tinggi pun menjadikan

¹ Pusat Operasi Keamanan Siber Nasional. (2021). Laporan Tahunan Hasil Monitoring Keamanan Siber 2020.

² Pusiknas Polri. (2022). Kejahatan Siber Di Indonesia Naik Berkali-Kali Lipat. 82 https://Pusiknas.Polri.Go.Id/Detail_Artikel/Kejahatan_Siber_Di_Indonesia_Naik_Berkali-Kali_Lipat

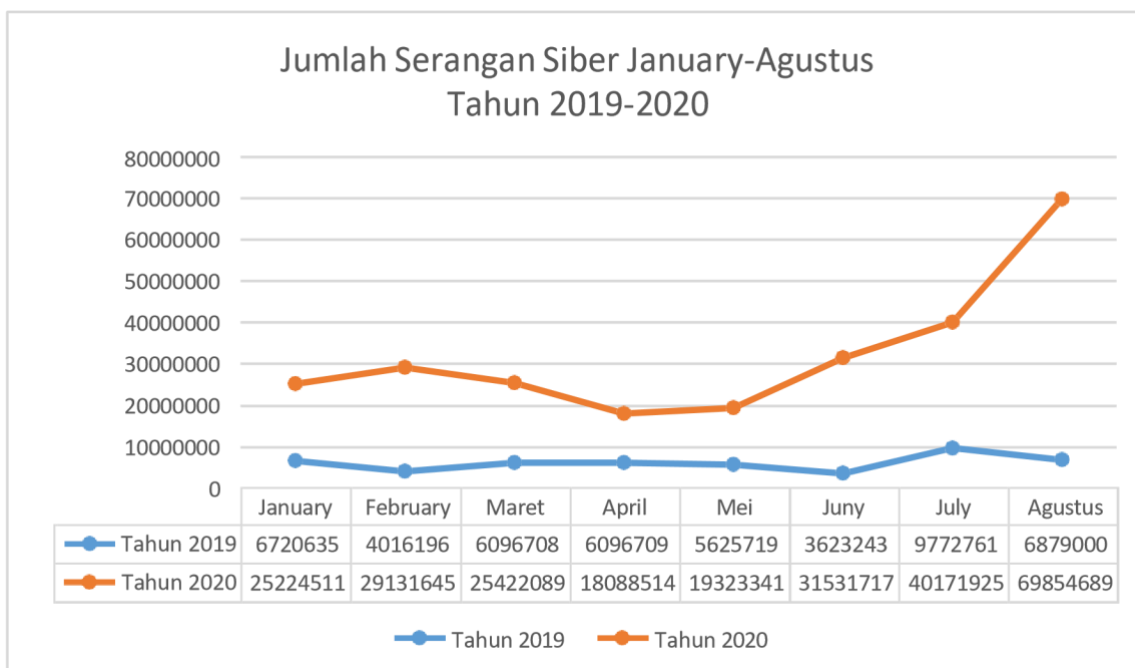
kurangnya perlindungan yang mumpuni terhadap keamanan siber di Indonesia dikarekan menurut Data GCI 2020 mengatakan bahwa Indonesia berada pada peringkat 24 dalam bidang keamanan siber jauh berada dibawah Singapura maupun Malaysia yang berada pada posisi 4 dan 5, sehingga Indonesia membutuhkan tindakan dalam meningkatkan keamanan siber salah satunya melakukan kerjasama dengan negara yang memiliki potensi keamanan dan pertahanan siber yang mumpuni, maka dari itu menurut penulis dibutuhkan fokus dalam meningkatkan keamanan dan pertahanan siber salah satu caranya melakukan kerjasama dengan negara lain untuk meningkatkan keamanan siber serta pertahanan siber Indonesia. Menurut laporan Naval Criminal Investigative Service atau disingkat NCSI juga menyatakan bahwa lemahnya regulasi pada perundang undangan di Indonesia, maka dari itu dibutuhkan kehadiran suatu negara untuk membantu mengintegrasikan secara terpadu pengelolaan bidang siber dengan mutlak untuk mengurangi ancaman pada aspek aspek kehidupan berbangsa dan bernegara³ (Hootsuite, 2021).

Novel Ariyadi, Director of Cyber Security at BDO Indonesia pun menyatakan bahwa situs pemerintah rentan terhadap serangan karena sistem keamanannya hanya diperhatikan pada saat layanan publik tersedia, yaitu hanya selama jam kerja. Hal ini terjadi dikarenakan bahwa kurangnya kesiapsiagaan serta penjagaan yang mumpuni sehingga situs pemerintahan pun mudah untuk diretas yang seharusnya untuk mencegah peretasan situs pemerintah oleh oknum yang tidak bertanggung jawab membutuhkan penjagaan yang mumpuni. Dengan fenomena serangan siber yang begitu tinggi bisa dilihat bahwa penulis melihat kurangnya tata kelola keamanan siber di instansi pemerintah karena masih banyaknya kejahatan siber di Indonesia terutama kebocoran data, pencurian data dan masih banyaknya *phising* yang ditemukan, dengan kondisi tersebut maka diperlukannya SDM yang kompeten untuk mengatasi ancaman yang terjadi.

Informasi dari Kementerian Komunikasi dan Informatika (Kominfo) juga menunjukkan bahwa pemanfaatan internet di Indonesia mengalami kenaikan sekitar 40 persen selama masa pandemi. Peningkatan tersebut

³ Hootsuite. (2021). Digital Global Overview Report 2021. <https://Techsauce.Co/Tech-And-Biz/Digital-2021-Overview-Report>

disebabkan oleh kebijakan jarak sosial yang memaksa orang untuk melakukan pekerjaan, pembelajaran, dan aktivitas lainnya dari rumah dengan menggunakan internet. Pusat penggunaan internet juga berpindah dari lingkungan kantor ke daerah perumahan. Ini akan mempengaruhi masa depan Indonesia dalam menghadapi pandemi Covid19. Selain itu juga adanya penggunaan internet di daerah terpencil yang meningkat sebesar 23 persen.



Gambar 1.1 umlah Serangan Siber January-Agustus Tahun 2019-2020

(Sumber: <https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi>)

Dari gambar diatas, Berdasarkan laporan BSSN (Badan Siber dan Sandi Negara), Indonesia mengalami hampir 190 juta percobaan serangan siber dari bulan Januari hingga Agustus tahun lalu, meningkat lebih dari empat kali lipat jika dibandingkan dengan periode yang sama pada tahun 2019 yang hanya mencapai 39 juta. Meskipun telah memasuki tahun 2021, serangan siber di Indonesia belum menunjukkan tanda-tanda mereda menurut beberapa pihak ⁴ (Kurniawan, 2020). Aksi peretas menggunakan keresahan masyarakat sebagai celah dalam melakukan dan memulai aksi

⁴ Kurniawan, F. (2020). Kerugian Serangan Siber Tahun 2021 Diprediksi RP 84.000 Triliun.

kejahatannya dengan memberikan berbagai serangan, mulai dari phishing hingga ransomware, yang menyebabkan masyarakat yang memanfaatkan layanan e-commerce seperti Tokopedia dan insiden kebocoran data 1,2 juta pengguna situs Bhinneka. Kaspersky mengungkapkan bahwa pandemi COVID-19 berpotensi meningkatkan gelombang kemiskinan yang dapat memicu tindakan kriminal, termasuk serangan siber.

Terkait dengan kondisi keamanan siber di Indonesia dalam artikel (Ramadhan, 2022) menjelaskan bahwa Indonesia merupakan urutan ketiga pengguna internet terbanyak di Asia dan urutan keempat di dunia yang menjelaskan bahwa Banyaknya pengguna internet di Indonesia serta imbas pandemi Covid-19 yang lebih mengedepankan pola interaksi secara daring menguatkan urgensi Indonesia untuk lebih memperkuat keamanan siber nasional. Serta seperti yang dikatakan (Bruijn.H & Janssen.M , 2017) bahwa penggunaan internet untuk mendukung aktivitas masyarakat sehari-hari sangat berkontribusi terhadap peningkatan risiko serangan dunia maya yang dimana masyarakat sangat bergantung pada fasilitas dalam bentuk digital. Tidak semua perusahaan terbiasa bekerja dari rumah, adanya ketergantungan masyarakat terhadap koneksi secara online serta infrastruktur jaringan digital. Sehingga bagi penulis hal ini patut mendapatkan perhatian mengingat Program Pengembangan Siber dan Sandi Negara merupakan program kunci yang terkait langsung dengan tingkat keamanan siber di Indonesia. Kemudian terdapat tren kenaikan anomali trafik siber di Indonesia yang didominasi oleh infeksi malware. Perlu diperhatikan bahwa tingginya persentase gangguan berupa malware ini merupakan suatu pertanda bahwa aktivitas ratusan juta pengguna internet di Indonesia memiliki risiko infeksi maupun pencurian informasi . Kenyataannya, monitoring keamanan siber di Indonesia masih terpusat di Indonesia bagian Barat atau lebih spesifik masih terpusat di Pulau Jawa dan masih terdapat beberapa provinsi yang belum sama sekali memiliki bentuk kerja sama monitoring keamanan siber oleh BSSN, masih banyak terjadinya kasus

peretasan pada situs Pemerintah pada tahun 2021. Diharapkan BSSN dapat meningkatkan keamanan siber di Indonesia agar kasus peretasan yang terjadi tidak semakin meningkat pada tiap tahunnya.

Berhubungan dengan Analisis akibat wabah Pandemi Covid 19 di Indonesia dilihat dari sudut pandang keamanan siber ada karya dari (Martanto Dwi Saksomo Hadi, Pujo Widodo, Resmanto Widodo Putro, 2020) yang menjelaskan bahwa Wabah pandemi Covid-19 memberikan dampak yang sangat meluas dan diperlukan nya waktu yang lama untuk masyarakat bangkit dari kerusakan akibatnya. Di sisi lain, Covid-19 juga telah memicu serangan siber yang sangat besar yang memengaruhi kehidupan masyarakat. Serta juga dengan karya (Martanto Dwi Saksomo Hadi, Pujo Widodo, Resmanto Widodo Putro, 2020) membahas akibat wabah Covid-19 di Indonesia dari perspektif keamanan siber. Wabah Covid- 19 mempunyai pengaruh yang merata dan memerlukan masa yang panjang untuk pulih. Selain itu, terdapat peningkatan yang signifikan dalam serangan siber di dunia maya yang dipakai oleh kelompok kriminal siber. Kelompok kejahatan siber terdiri dari kelompok cyber dependent crime dan kelompok cyber enabled crime. Kelompok cyber dependent crime melakukan kejahatan yang hanya dapat dilakukan di dunia maya melalui TIK, seperti peretasan, pencurian data elektronik, serangan denial of service distributed (DDOS), dan penyebaran malware. Sedangkan kelompok cyber enabled crime merupakan model kejahatan tradisional yang meningkat ukuran dan cakupannya melalui TIK, seperti penipuan online dan pencurian data pribadi melalui phishing. Peningkatan drastis serangan siber di dunia maya yang memanfaatkan situasi saat ini, di mana para pemimpin negara harus membuat keputusan sulit untuk menentukan masa depan mereka dalam melawan Covid-19. Keadaan masyarakat sangat tertekan, banyaknya berita bohong yang tersebar di dunia maya membuat masyarakat resah, ini situasi yang agak sulit akibat ditutupnya kegiatan usaha. Sehingga penulis melihat dengan fenomena Covid19 yang terjadi sangat mempengaruhi penyerangan dan memberikan peluang yang tinggi terhadap kejahatan siber di karenakan selama

pandemi Covid 19 adanya perubahan sosial terhadap kehidupan sehari-hari masyarakat.

Adanya jurnal (Budiman, 2017) yang menjelaskan mengenai optimalisasi badan siber dan sandi negara tempat Badan Siber dan Sandi Negara (BSSN) resmi dibentuk berdasarkan Keputusan Presiden Nomor 53 Tahun 2017 tentang Badan Siber Nasional tertanggal 19 Mei 2017. Dalam aturan ini, pembentukan BSSN didasarkan pada fakta bahwa keamanan siber merupakan salah satu bidang administrasi yang harus ditingkatkan dan diperkuat guna meningkatkan pertumbuhan ekonomi dan keamanan nasional. Pembentukan BSSN bertujuan untuk mengubah Badan Sandi Negara menjadi Badan Siber dan Sandi Negara, sehingga kebijakan dan program pemerintah di bidang keamanan siber dapat dijalankan dengan baik. Seperti yang tertulis dalam artikel (Hidayat Chusnul Chotimah, 2019) tentang Manajemen Keamanan Siber dan Diplomasi Siber Indonesia di bawah lembaga Badan Siber dan Sandi Negara yang mengangkat perdebatan ini dan menyatakan bahwa BSSN adalah salah satu pelaksana dari diplomasi siber Indonesia⁵. Badan badan tersebut bekerja sama secara bilateral dengan beberapa negara seperti Australia, United Kingdom, Netherlands dan Amerika Serikat. Pada saat yang sama, Indonesia juga turut ikut serta di tingkat regional dalam ASEAN Cyber Security and Cybercrime Cooperation dan ASEAN Capacity Program (ACCP). Tindakan diplomasi tersebut dilakukan guna menjaga keamanan dan kedaulatan siber di Indonesia, dengan BSSN ikut terlibat sebagai lembaga siber nasional. Sebagai upaya mengantisipasi berbagai ancaman kejahatan keamanan siber di Indonesia, Badan Siber dan Sandi Negara (BSSN) didirikan sebagai model lembaga siber untuk menjaga keamanan nasional⁶ (BSSN, 2019). Terlebih lagi, sebagai salah satu negara yang sedang berkembang, Indonesia memiliki jumlah penduduk terbesar di dunia dan menjadi salah satu negara dengan penggunaan

⁵ Hidayat Chusnul Chotimah. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. *Jurnal Politica* Vol.10 No. 2. Dapat diakses melalui <https://doi.org/10.22212/jp.v10i1.1447>

⁶ Biro Hukum Dan Humas BSSN. (2019). BSSN Selenggarakan Community Building And Information Sharing Sektor Ekonomi Digital. <https://Bssn.Go.Id/BssnSelenggarakan-Community-Building-And-Information-SharingSektorEkonomi-Digital/>

internet terbesar di dunia.. Pasal lain mengenai tata kelola BSSN dibahas juga dalam artikel (Ahmad Budiman, 2017) yang menjelaskan bahwa badan hukum yang meliputi Badan Sandi Negara sebagai pendahulu berdirinya BSSN dibentuk dengan Keputusan Presiden No 103 Tahun 2001 tentang status, tugas, tugas, wewenang, susunan organisasi dan tata kerja lembaga negara non kementerian (LPND) yang ditugaskan untuk melaksanakan tugas administrasi di bidang persandian sesuai dengan ketentuan peraturan perundang-undangan.

Dalam artikel (Marina Christmartha, Rudy A. G. Gultom, Sovian Aritonang, 2020), dibahas mengenai signifikansi sumber daya manusia dalam sektor keamanan siber di Indonesia. Rencana strategi kebijakan peningkatan tenaga kerja siber nasional sangat penting untuk menunjang pertahanan negara menghadapi risiko serangan siber yang kian meningkat. Meskipun terdapat instansi khusus yang menangani persoalan keamanan siber yaitu Badan Siber dan Sandi Negara (BSSN) namun masyarakat Indonesia masih kekurangan sumber daya manusia dalam bidang siber, baik secara kuantitatif maupun kualitatif dan kualitas. Hal ini menandakan bahwa diperlukan upaya yang lebih besar untuk mengembangkan SDM siber nasional, oleh karena itu artikel ini juga membahas cara-cara peningkatan SDM siber nasional yaitu: Mengkaji lebih lanjut kompetensi pelaksana cybersecurity nasional untuk mendukung keberhasilan implementasi pengembangan tenaga cybersecurity, mengingat kompetensi pelaksana dalam menghasilkan analisis kebutuhan tenaga cybersecurity yang memadai masih belum lengkap. Dan juga tertulis karya (Rosidah, 2009) yang mengataka bahwa Pengetahuan mengenai situasi keamanan siber dan kejahatan siber beserta peran masing-masing institusi juga dibutuhkan untuk menghindari tumpang tindih dalam pelaksanaan fungsi pengembangan sumber daya manusia siber nasional. Meningkatkan kolaborasi dengan entitas swasta lainnya, terutama untuk mencapai pengembangan sumber daya manusia siber nasional yang optimal.⁷

⁷ Rosidah, A. T. S. (2009). Manajemen Sumber Daya Manusia. Graha Ilmu.

Menurut Kaspersky(Cakrawala, 2021)., keamanan siber merupakan sebuah praktik untuk melindungi komputer, server, perangkat mobile, sistem elektronik, jaringan, dan data dari serangan jahat. Keamanan siber juga memerlukan tata kelola dan strategi dalam proses nya⁸ yang di mana juga hal ini tertulis di dalam artikel (Infantono, 2021) yang menjelaskan beberapa cara dalam penguatan strategi cyber security di indonesia yakni:

Capacity Building, Pembentukan Undang-Undang Khusus tentang Tindak Pidana Siber , Peningkatan Sumber Daya Manusia dan Kerjasama. Tapi dibalik fenomena ini penulis melihat masalah keamanan jaringan sangat rumit dan kompleks, sehingga diperlukan pendekatan multidimensi. Oleh karena itu menerapkan prinsip multistakeholder sangat penting untuk meningkatkan tata kelola keamanan jaringan. Tanpa kerja sama dan kolaborasi antar pemangku kepentingan (dari organisasi layanan publik hingga sektor swasta, akademisi, dan masyarakat sipil), mengatasi masalah keamanan siber yang sulit, sepihak, dan tidak lengkap akan terus berlanjut. Mekanisme yang komprehensif diperlukan untuk menjustifikasi keputusan dan mencerminkan serta mempertimbangkan kepentingan Negara dan mereka yang terkena dampak.

I.2 RUMUSAN MASALAH

Dalam laporan Pusat Operasi Keamanan Siber Nasional (Pusopkamsinas) BSSN periode Januari hingga Desember 2020, tercatat bahwa selama pandemi Covid-19 terjadi peningkatan insiden keamanan siber di Indonesia, maka perlunya penanganan yang tepat dalam meningkatkan keamanan siber di Indonesia, dengan berbagai cara BSSN melakukan strategi dalam meningkatkan keamanan siber di Indonesia salah satu nya adalah dengan melakukan kerjasama dengan negara australia yang dimana kerjasama ini di lakukan dikarenakan australia merupakan negara yang maka dari itu BSSN melakukan kerjasama nya dengan australia dalam peningkatkan infrastruktur serta sumber daya manusia yang berperan dalam keamanan siber di Indonesia

⁸ Cakrawala. (2021). Apa Itu Cyber Security? Mengapa Cyber Security Kini Makin Penting? Infokomputer.Grid.Id.
<https://infokomputer.grid.id/read/122710604/apa-itu-cybersecurity-mengapa-cyber-security-kini-makin-penting?page=all>

yaitu BSSN karna dengan ada nya infrastruktur serta sumber daya manusia yang mumpuni maka keamanan siber di Indonesia mampu meningkat, Terkait penjelasan di atas, penulis merumuskan masalah dalam bentuk pertanyaan penelitian sebagai berikut: **bagaimana kerjasama BSSN dan DFAT dalam upaya meningkatkan keamanan siber di Indonesia melalui program share information and best practice pada masa pademi tahun 2019-2022 ?**

I.3 TUJUAN PENELITIAN

Dengan mengacu pada latar belakang dan rumusan masalah yang telah diuraikan di atas, penelitian ini memiliki tujuan yaitu dapat menjadi referensi mengenai proses kerjasama dalam peningkatan keamanan siber di indonesia yang dilakukan kerjasama BSSN dengan australia melalui program berbagi informasi dan pelatihan terbaik dalam meningkatkan infrastruktur serta sumber daya manusia yang mumpuni dalam peningkatan keamanan siber di indonesia Melalui penelitian ini, dapat menjadi acuan bagi pemangku kepentingan di sektor siber keamanan dalam peningkatan keamanan siber di indonesia melalui program berbagi informasi dan pelatihan terbaik serta memperkaya pembahasan penelitian hubungan internasional khususnya di bidang keamanan siber terkait isu keamanan siber yang berkembang di Indonesia melalui program berbagi informasi dan pelatihan terbaik.

I.4. MANFAAT PENELITIAN

Penelitian ini diharapkan memberikan manfaat secara akademis maupun praktis, diantaranya adalah:

I.4.1 Manfaat Praktis

Hasil penelitian ini akan menjadi tolak ukur dan sumber data untuk kajian lebih lanjut yang berhubungan dengan keamanan siber di Indonesia.

I.4.2 Manfaat Akademis

Diharapkan kajian ini bermanfaat dalam memikirkan teori-teori hubungan internasional yang telah dipelajari dalam kaitannya dengan keamanan siber dan memberikan wawasan baru bagaimana upaya peningkatan keamanan siber di

Indonesia dilakukan kerjasama dengan Australia melalui program berbagi informasi dan pelatihan terbaik.

I.5 SISTEMATIKA PENULISAN

BAB I: PENDAHULUAN

Bab ini akan membahas pengenalan penelitian meliputi dasar dasar, rumusan masalah, pertanyaan penelitian, tujuan penelitian, kepentingan penelitian dan sistem penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab kedua, penulis akan menjelaskan konsep dan teori sesuai topik yang dibahas sehingga dapat dijelaskan jawaban dan hasil dari rumusan masalah. Konsep dan teori juga dapat dikembangkan berdasarkan penelitian. Penulis kemudian juga akan membuat kerangka kerja yang merupakan garis besar dari penelitian ini, sehingga menghasilkan jawaban dan hasil dari penelitian ini.

BAB III : METODE PENELITIAN

Pada bab ketiga ini penulis memaparkan tentang objek penelitian, terutama terhadap permasalahan yang berkaitan dengan objek penelitian. penulis juga menjelaskan jenis pencarian yang digunakan untuk mengambil hasil pencarian. Selain itu juga akan dijelaskan metode pengumpulan data, sumber data, analisis data, dan jadwal penelitian.

BAB IV : GAMBARAN UMUM KEAMANAN SIBER DI INDONESIA DAN KEAMANAN SIBER AUSTRALIA

Pada bab keempat ini, penulis akan memaparkan gambaran umum kamanan siber yang ada di indonesia serta juga gambaran umum keamanan siber di australia.

**BAB V : IMPLEMENTASI KERJASAMA BSSN DAN DFAT DALAM
MENINGKATKAN KEAMANAN SIBER INDONESIA MELALUI
PROGRAM SHARE INFORMATION AND BEST PRACTICE TAHUN
2019-2022**

Pada bab ke lima ini penulis akan memamparkan mengenai implementasi kerjasama yang dilakukan oleh badan siber dan sandi negaa (BSSN) dengan departemen of foreign affairs and trade (DFAT) dalam meningkatkan keamanan siber indonesia melalui program share information and best practice selama periode 2019-2022

BAB VI : KESIMPULAN DAN SARAN

Bab ini akan menjadi kesimpulan dan saran dari penelitian yang dilakukan oleh penulis. Bab ini merupakan kesimpulan dan saran dari masalah penelitian dan pertanyaan yang diperoleh dari BAB I, II, III, IV, dan V.

DAFTAR PUSTAKA

BAB II TINJAUAN PUSTAKA

II.1 KONSEP DAN TEORI PENELITIAN

Dalam penelitian ini, konsep dan teori dibutuhkan sebagai landasan untuk menjawab temuan penelitian. Konsep dan teori dapat memberikan suatu kerangka pemikiran bagi kebutuhan penelitian ini.

II.1.1 Kerjasama Bilateral

Hubungan antar negara telah berlangsung sejak lama dan terus berkembang hingga saat ini. Adanya kebutuhan yang tidak mampu dipenuhi sendiri membuat suatu negara berusaha berhubungan dengan negara lain dalam konsep hubungan kerjasama yang saling menguntungkan. Di era globalisasi yang semakin mendistorsi batas ini sistem interaksi antar negara menjadi semakin terintegrasi karena globalisasi membentuk suatu pola interaksi yang terbuka dan saling bergantung satu sama lainnya sehingga saat ini banyak negara yang melakukan kerjasama.

Kerjasama bilateral mengacu pada hubungan antara satu negara dengan negara lain untuk tujuan tertentu dan secara umum mengacu pada saling mempengaruhi antara kedua negara. Dalam kolaborasi, tidak hanya negara yang menjadi aktor satu-satunya, namun entitas lain seperti perusahaan, lembaga, dan organisasi internasional juga bisa dilibatkan. Dalam kondisi sistem internasional yang anarkis seperti ini, suatu negara membutuhkan negara lain untuk memenuhi kebutuhannya dan mewujudkan kepentingan nasionalnya.

Karena suatu negara pada dasarnya tidak bisa berdiri sendiri tanpa bantuan negara lain. Kolaborasi merupakan upaya untuk memadukan sudut pandang demi mencapai kepentingan bersama yang ingin dicapai. Robert O. Keohane dan Robert Axelrod menjelaskan situasi tiga dimensi yang memungkinkan negara-negara untuk bekerja sama, yaitu Kebersamaan

kepentingan, jumlah pelaku dan bayangan masa depan Kesamaan kepentingan dan tujuan menjadi faktor utama yang mempengaruhi.

menciptakan hubungan kerjasama karena hal ini memungkinkan kerjasama dapat berjalan dengan lancar dan efisien serta membuahkan hasil yang memuaskan bagi kedua belah pihak.

Kemudian muncul jumlah aktor atau jumlah pihak yang terlibat dalam kerjasama tersebut. Dalam hal ini, negara harus memperhitungkan jumlah pihak yang terlibat agar tidak terjadi pembelot dan parasit dalam hubungan kerjasama. Strategi yang efektif diperlukan ketika membangun hubungan kerjasama adalah timbal balik⁹ (Saudi, 2016).

Negara yang terjalin dalam kerjasama harus bisa mengetahui apakah ada pihak di dalamnya yang memiliki kemungkinan menghambat kerjasama, memberikan pembalasan dan sanksi terhadap negara yang menjadi penghambat tersebut.

Terakhir, bagaimana bayangan masa depan mengenai kerja sama dicapai dapat menciptakan prospek yang baik di masa depan atau tidak, Suatu negara akan cenderung melakukan kerjasama jika hasil kerjasamanya membawa manfaat jangka panjang. Teori kerjasama telah digunakan secara luas, terutama dalam literatur hubungan internasional, yang memperdebatkan bagaimana kerjasama dapat muncul dan bertahan dalam sistem internasional yang anarkis. Definisi umum kerjasama terjadi ketika aktor menyesuaikan perilaku mereka dengan preferensi aktual atau yang diharapkan dari pihak lain (Axelrod/Keohane 1985: 226). Oleh karena itu, kepentingan para aktor sangat menentukan proses kerja sama, karena jika ditemukan perbedaan yang tidak sehat atau bahkan tidak terselesaikan maka hal ini dapat menimbulkan konflik. (Paulo, 2014). Definisi kerjasama tersebut memuat dua elemen penting. Pertama, asumsi bahwa perilaku setiap aktor diarahkan untuk mencapai beberapa tujuan bersama. Kedua, definisi tersebut mengasumsikan bahwa kerjasama harus memberikan keuntungan bagi aktor yang terlibat meskipun

⁹ Saudi, A. (2016). KEJAHATAN SIBER TRANSNASIONAL DAN STRATEGI PERTAHANAN SIBER INDONESIA. Universitas Riaria.

keuntungannya tidak sama besar tetapi yang ditekankan disini adalah timbal baliknya. Aktor yang terlibat dalam kerjasama disini harus membantu aktor lainnya dengan menyesuaikan kebijakan mereka untuk memastikan bahwa kerjasama dapat menghasilkan keuntungan, terlebih mampu mencerminkan kepentingannya (Helen Milner, 1992).

Dalam upaya meningkatkan keamanan siber, Indonesia harus memperkuat perannya dalam memajukan kerjasama internasional. Hal ini meliputi dukungan terhadap kesepakatan bersama yang telah disetujui oleh ITU, yaitu organisasi utama dalam menciptakan lingkungan siber yang aman bagi pemerintah, masyarakat, dan bisnis. Selain itu, Indonesia juga dapat mengembangkan kerjasama dengan negara anggota ITU lainnya yang memiliki kemampuan IT yang lebih baik untuk memperkuat sumber daya manusia, melindungi pengguna dari kemungkinan kejahatan dunia maya, dan meningkatkan pemanfaatan internet untuk informasi¹⁰ (Sunyoto, 2015).

Penulis akan menggunakan pendekatan teori kerjasama Robert Axelrod dan Robert O. Keohane untuk menjabarkan hal-hal yang berkaitan dengan realisasi kerjasama yang dilakukan antara Indonesia dengan australia dalam kerjasamanya meningkatkan sumber daya manusia serta infrastruktur keamanan siber di Indonesia ¹¹(Simamora, 2004) . Dengan menggunakan teori kerjasama ini penulis bertujuan untuk menjelaskan situasi dimensional yang memungkinkan Indonesia dan australia melakukan kerjasama terkait permasalahan tersebut.

II.1.2 Keamanan Siber

Keamanan siber memiliki dua kata kunci: keamanan dan siber. Membahas siber berarti berbicara tentang informasi, koneksi (telekomunikasi, jaringan), port (komputer, perangkat, pengguna) dan berbicara tentang relevansi, penggunaan atau koneksi dengan komputer, jaringan dan Internet. Selain itu, keamanan sering kali dikaitkan dengan perlindungan properti dan aset.

¹⁰ Sunyoto, D. (2015). Penelitian Sumber Daya Manusia. Buku Seru.

¹¹ Simamora, H. (2004). Manajemen Sumber Daya Manusia. YKPN Jakarta.

Keamanan melindungi aset, melindungi komputer, jaringan, program dan data dari akses, modifikasi atau penghancuran yang tidak disengaja atau tidak sah, dan melindungi informasi dan sistem dari serangan dunia maya. Seperti yang diungkapkan (Fathika Anjani Firman 2018: 32) Keamanan siber melibatkan seluruh hal yang terkait dengan pemantauan, pengawasan, dan pengendalian komputer dengan ketat, serta memperjuangkan hak asasi fundamental . keamanan siber merupakan usaha untuk menjamin pencapaian dan pemeliharaan keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkup ruang siber (Fathika Anjani Firman, 2018: 33).

Berinisiatif mencari cara untuk mencapai kesepakatan yang mengikat kewajiban hukum tentang keamanan siber di tingkat internasional. Namun, karena belum adanya kesepakatan internasional tentang keamanan siber, penguatan perlindungan keamanan siber nasional sangat dibutuhkan. Menurut Handrini (2014), keamanan siber telah menjadi hal yang penting untuk semua negara di seluruh dunia sejak teknologi informasi dan komunikasi digunakan dalam berbagai bidang kehidupan¹². Seiring dengan peningkatan penggunaan teknologi informasi dan komunikasi, risiko dan ancaman penyalahgunaan teknologi informasi dan komunikasi juga meningkat dan menjadi lebih kompleks¹³ (Barrinha, A. & Renard, 2017). Sampai saat ini belum ada perjanjian internasional yang mengikat mengenai keamanan siber, sehingga Indonesia sebagai negara harus Kerja sama internasional lainnya yang terkait dengan pengembangan keamanan siber adalah dalam rangka peningkatan kapasitas keamanan siber dalam hal infrastruktur, infrastruktur dan pengembangan kapasitas personel di bidang keamanan siber baik secara bilateral antara kedua negara maupun di tingkat regional atau internasional. Selain itu, penguatan kerjasama di bidang teknologi informasi dan keamanan siber diharapkan dapat memberikan peluang untuk

¹² Handrini, A. (2014). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Politica*, 5(1).

¹³ Barrinha, A., & Renard, T. (2017). Cyber-Diplomacy: The Making Of An International Society In The Digital Age. *Global Affairs*, 3(4–5), 353–364. <https://doi.org/10.1080/23340460.2017.1414924>

pengembangan dalam industri komunikasi baru terkait teknologi informasi di Indonesia sebagai bagian dari strategi pertumbuhan industri Karma.

Menurut buku *Cyber Security Policy Guidebook* oleh (Bayuk et al., 2012), keamanan siber adalah keamanan yang dimodifikasi yang terkait dengan segala sesuatu yang dilindungi di dunia maya. Secara umum, cybersecurity mengacu pada cara orang, proses, dan teknologi digunakan untuk mencegah, mendeteksi, dan memperbaiki kerusakan pada kerahasiaan, integritas, dan ketersediaan informasi di dunia digital.¹⁴

Dalam bukunya *Cyber Security: Essential Principles to Secure Your Organization*, Calder, 2020 menjelaskan bahwa cybersecurity adalah bagian dari keamanan informasi dan sama dengan keamanan informasi. Keamanan informasi adalah hal biasa, cybersecurity berfokus pada pendekatan tertentu terhadap informasi elektronik (termasuk aspek fisik penyimpanan informasi tersebut).¹⁵

Dalam rangka pertahanan, diperlukan strategi pengembangan bakat di bidang keamanan siber yang terintegrasi dan terkoordinasi. Saat ini, konsep pertahanan siber yang diterapkan oleh Departemen Pertahanan dan TNI masih bersifat sektoral dan belum dikelola dengan baik, seperti yang dijelaskan oleh Eris Herryanto pada tahun 2011. Untuk meningkatkan keterampilan keamanan siber, diperlukan program pelatihan yang bekerja sama dengan tim Pusat Operasi Pertahanan Siber. Selain itu, penting untuk memberikan edukasi kepada masyarakat tentang perlunya keamanan di dunia maya dan cara mencegah kejahatan siber. Perlu juga mengembangkan keterampilan SDM yang dapat menangani masalah keamanan siber.

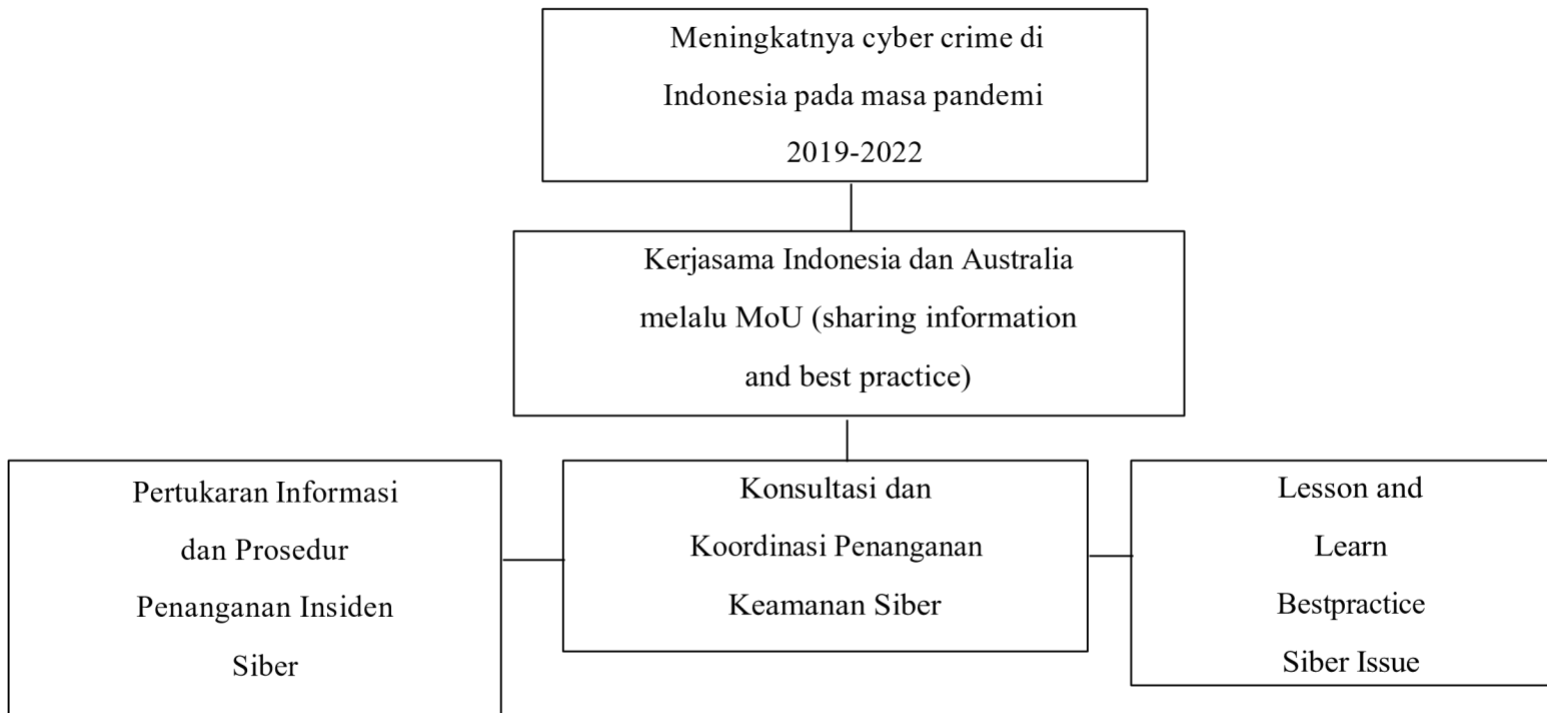
Dengan demikian penulis bisa melihat pada penjelasan bahwa bagaimana konsep keamanan siber memanfaatkan manusia, prosedur, serta teknologi untuk mengidentifikasi, mendeteksi, mencegah, melindungi, menangani, dan

¹⁴ Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber Security Policy Guidebook*. In *Cyber Security Policy Guidebook*. John Wiley And Sons, Inc. <https://doi.org/10.1002/9781118241530>

¹⁵ CALDER, A. (2020). *Cyber Security: Essential Principles To Secure Your Organisation*. In *Cyber Security: Essential Principles To Secure Your Organisation*. IT Governance Publishing Ltd. <https://doi.org/10.2307/J.Ctv10crcbg>

memulihkan kerahasiaan, integritas, dan ketersediaan data digital (elektronik) yang rusak atau terkena serangan keamanan siber, yang dikarenakan keamanan siber yang lemah dapat menciptakan ketegangan di antara negara-negara dan mengganggu stabilitas keamanan, menciptakan pengaruh sosial, ekonomi, dan lingkungan, serta mengganggu hubungan antar negara.

II.2 Kerangka Pemikiran



Gambar 1. Kerangka Pikiran

Di era globalisasi teknologi mengalami kemajuan yang sangat pesat dalam melakukan komunikasi dan memberikan informasi. Teknologi menghilangkan batas-batas wilayah dan waktu dalam menghubungkan manusia. Kecepatan perkembangan yang ada tentunya perlu disertai pemilihan hukum yang dapat berlaku dalam sengketa multi-yuridiksi ¹⁶(Saefullah, 2002). Dalam menghadapi perkembangan tersebut tentunya terdapat ancaman dan tantangan. Salah satu kejahatan yang dapat terjadi dan berkembang di Indonesia adalah *cybercrime*. Sehingga untuk menangani kasus tersebut diperlukan aturan agar keharmonisan

sosial tetap terjaga. Salah satu contoh kejahatan siber yang sering terjadi yaitu pada kebutuhan *e-banking* dan *e-commerce*. Tindak kejahatan yang terjadi antara lain berupa penipuan, penggelapan, peretasan, perusakan sistem

¹⁶ Saefullah, N. T. S. (2002). Yurisdiksi Sebagai Upaya Penegakan Hukum Dalam Kegiatan Cyberspace. In In Cyber Law: Suatu Pengantar.). Pusat Studi Cyber Law UNPAD.

komputer, dan lainnya yang banyak belum terjangkau oleh undang-undang¹⁷ (Richiyanti, 2020).

Cybercrime merupakan tindakan kriminal yang memanfaatkan kecanggihan teknologi sebagai alat dalam membantu kejahatan yang dilakukan. *Cybercrime* termasuk kedalam perbuatan yang melanggar hukum dan memberikan ancaman bagi tatanan teknologi informasi seperti akses ilegal yang dilakukan baik pada komputer maupun perangkat yang memiliki akses internet¹⁸ (Richiyanti, 2020). Dalam upaya mencegah terjadinya kejahatan siber atau *cybercrime* setiap negara membentuk sebuah badan atau lembaga yang memiliki tugas khusus untuk menangani hal tersebut. Lembaga merupakan tatanan permainan yang berlaku dalam masyarakat atau formalnya merupakan aturan-aturan yang disusun sesuai dengan tujuan dibentuknya¹⁹ (North, 1990). Untuk mengatur kejahatan siber yang bermunculan, Indonesia menciptakan BSSN sebagai lembaga atau institusi siber.

Upaya yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN) salah satunya adalah dengan pengadaan MOU Indonesia-Australia *Cyber Cooperation*. Fokus yang dilakukan dalam penelitian ini terdapat pada paragraf 2 yang membahas tentang kesepakatan kerjasama antar wilayah negara. Sesuai dengan latar belakang, rumusan masalah, dan tujuan yang telah disebutkan maka penelitian ini akan fokus pada kerjasama yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN) dan Australia dalam upaya meningkatkan keamanan siber di Indonesia pada tahun 2019-2022. Berdasarkan tujuan penelitian yang akan dilakukan maka penelitian dimulai dengan menganalisis kerjasama yang dilakukan BSSN dan Australia selama pandemic 2019-2022. Setelah itu peneliti akan fokus pada MOU antara Indonesia dan Australia terkait *Cyber Cooperation* terutama pada paragraf ke dua dengan fokus kerjasama antar wilayah. Setelah itu analisis dilakukan dengan melihat bagaimana kejahatan siber yang terjadi selama tahun 2019-2022 di Indonesia.

¹⁷ Richiyanti, S. (2020). Pengaruh Dan Penanganan Cybercrime Dalam Perkembangan Teknologi Informasi. KODIFIKASI, 2(2), 46–56.

¹⁸ Richiyanti, S. (2020). Pengaruh Dan Penanganan Cybercrime Dalam Perkembangan Teknologi Informasi. KODIFIKASI, 2(2), 46–56. ¹⁹ North, D. C. (1990). *Institutions, Institutional Change And Economic Performance*. Cambridge University Press.

Adapun langkah selanjutnya dengan menganalisis bagaimana upaya yang dilakukan untuk meningkatkan infrastruktur keamanan siber dan SDM keamanan siber yang ada di Indonesia dengan adanya peningkatan yang dilakukan melalui program share information and best practice ini peneliti melihat bagaimana peningkatan yang terjadi berdasarkan fakta yang ada.

Dengan melihat kerangka diatas bahwa adanya juga peraturan perundang undangan yang mendukung akannya keamanan siber nasional Indonesia:

- 1) Berdasarkan Peraturan Presiden (Perpres) Nomor 47 tahun 2023 tentang Strategi Keamanan Siber Nasional (SKSN) dan Manajemen Krisis Siber (MKS), ruang lingkup pengaturan meliputi SKSN dan MKS. Tujuan Perpres tersebut antara lain mewujudkan keamanan siber, melindungi ekosistem perekonomian digital nasional, meningkatkan kekuatan dan kapabilitas keamanan siber yang andal dan berdaya tangkal, dan mengutamakan kepentingan nasional dan mendukung terciptanya ruang siber global yang terbuka, aman, stabil dan bertanggung jawab. Fokus area yang diatur termasuk tata kelola manajemen risiko, kesiapsiagaan dan ketahanan, penguatan perlindungan infratraktur informasi vital, kemandirian kriptografi nasional, peningkatan kapabilitas, kapasitas, dan kualitas, kebijakan keamanan siber dan kerja sama internasional.
- 2) Berdasarkan Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital yang bertujuan untuk melindungi keberlangsungan penyelenggaraan IIV secara aman, mencegah terjadinya gangguan, kerusakan, dan/atau kehancuran pada IIV akibat serangan siber, serta meningkatkan kesiapan dalam menghadapi insiden siber dan mempercepat pemulihan dari insiden siber dimana BSSN berperan sebagai koordinator dan melibatkan 8 (delapan) kementerian sebagai penanggung jawab sektor IIV di bidang administrasi pemerintahan, Energi dan Sumber Daya Manusia, transportasi, Teknologi Informasi dan

Komunikasi, Pangan, keuangan, pertahanan, dan kesehatan serta sektor IIV lainnya yang ditetapkan Presiden. Adapun pengaturan ruang lingkup didalamnya meliputi identifikasi sektor IIV dan IIV, penyelenggaraan perlindungan IIV, pembinaan dan pengawasan penyelenggaraan perlindungan IIV, dan koordinasi penyelenggaraan perlindungan IIV.

BAB III

METODE PENELITIAN

III.1 OBJEK PENELITIAN

Menurut (Arikunto, 1998) Fokus penelitian adalah hal yang menjadi perhatian utama dalam suatu penelitian. Menurut Supranto (2000), objek penelitian terdiri dari sekelompok elemen seperti individu, kelompok organisasi, atau barang yang akan dijadikan objek penelitian. Oleh karena itu, objek penelitian merupakan inti dari penelitian agar memiliki arah yang jelas. Objek penelitian juga dapat dilihat dari judul penelitian yang mencerminkan masalah penelitian yang akan diteliti. Adapun objek penelitian ini meliputi: (1) apa saja kerjasama yang dilakukan antara BSSN dengan australia dalam meningkatkan keamanan siber di indonesia melalui program berbagi informasi dan pelatihan terbaik (2) apa pengaruh yang diberikan australia untuk indonesia dalam kerjasamanya dalam meningkatkan keamanan siber di Indonesia (3) apakah dengan kerjasama ini keamanan siber di indonesia meningkat melalui program berbagi informasi dan pelatihan terbaik.

III.2 JENIS PENELITIAN

Penelitian terdiri dari 2 (dua) jenis, yakni kuantitatif dan kualitatif. Studi Ilmu Hubungan Internasional seiring dengan perkembangan isu, dapat diteliti dengan dua jenis penelitian tersebut. Dalam penelitian kualitatif, penulis akan mendeskripsikan, interpretasi, menerjemahkan, memahami makna dari suatu fenomena. Dalam (Merriam, 2009) terdapat beberapa ciri pokok dalam penelitian kualitatif, diantaranya:

1. Berfokus pada mencari arti dan pemahaman.
2. Peneliti merupakan instrumen atau alat utama.
3. Mengaplikasikan metode induksi dalam menganalisis data.

4. Hasil penelitian disajikan dalam bentuk deskripsi, uraian kata-kata, dan didukung oleh gambar.
5. Desain penelitian yang fleksibel terhadap situasi penelitian yang sedang berlangsung.

Suatu penelitian akan dipertanyakan keilmiahannya. Penelitian dapat dikatakan ilmiah selama mengikuti aturan penelitian. Dengan melakukan aturan penelitian, maka kredibilitas penelitian tersebut dapat sah dalam suatu ilmu pengetahuan. Penelitian kualitatif dalam menjaga keilmiahannya perlu dilakukan dengan aturan-aturan tertentu, diantaranya:

- 1) Menjaga netralitas.
- 2) Adanya keterlibatan yang memadai sepanjang penelitian dan di lokasi pengumpulan data.
- 3) Deskripsi yang memupuni dan kaya akan data.

Poerwandari (1998) menegaskan bahwa penelitian kualitatif bertujuan untuk memahami fenomena secara mendalam dengan mengumpulkan dan menganalisis data dalam bentuk deskriptif, seperti transkrip wawancara, catatan lapangan, gambar, foto, rekaman video, dan sebagainya. Metode penelitian ini digunakan untuk memperoleh pemahaman yang lebih baik terhadap realitas yang kompleks dan tidak dapat diukur secara kuantitatif.

Penulis memilih jenis penelitian deskriptif kualitatif yang merupakan jenis dari penelitian kualitatif. Tujuannya adalah untuk menggambarkan fakta, situasi dan fenomena atau kejadian pada topik yang sedang dibahas. Deskriptif kualitatif menyajikan data yang bersangkutan dengan situasi yang sedang terjadi. Dalam penelitian kualitatif, peneliti diharapkan memiliki pengetahuan yang luas karena merupakan hal penting dalam penelitian, sehingga bisa memproses informasi, menganalisis dan membangun apa yang diteliti agar lebih terlihat dan bermakna. Oleh karena itu, peneliti menggunakan jenis penelitian deskriptif kualitatif untuk menjelaskan fenomena yang terjadi, yakni proses bagaimana kerjasama antara Australia dengan BSSN dalam meningkatkan keamanan siber di Indonesia.

III.3 TEKNIK PENGUMPULAN DATA

Dalam suatu penelitian kualitatif, kelengkapan data yang dihasilkan sangat mempengaruhi kredibilitas penelitian. Penelitian kualitatif memiliki triangulation data yang dihasilkan dengan tiga metode, yakni interview, observasi, dan telaah dokumen (document records). Dalam teknik mengumpulkan data, juga melibatkan kegiatan pendukung lainnya seperti penciptaan rapport, pemilihan informan, pengumpulan data dari informan, pengumpulan data pendukung dan pencatatan data.

Menurut (Faisal, 1990), dengan penciptaan rapport akan terjalin hubungan saling percaya antara peneliti dengan pihak yang akan diteliti. Kemudian, pemilihan informan perlu dilakukan secara purposif didasarkan pada elemen-elemen yang sesuai dengan kebutuhan penelitian. Jika peneliti menganggap bahwa informasi yang didapatkan sudah cukup, maka tidak perlu melanjutkan untuk membuat sample baru. Pemilihan informan sangat penting, menurut (Subadi, 2006) ada tiga tahap dalam pemilihan informan (1) Seleksi awal informan, baik untuk diwawancarai maupun diamati, (2) Seleksi informan tambahan untuk memperoleh informasi yang lebih luas dan mengejar ragam informasi yang mungkin tersedia, (3) Menghentikan seleksi informan apabila tidak ada informasi baru yang muncul.

Dalam penelitian ini, penulis akan menggunakan teknik pengumpulan data dengan menggunakan wawancara terstruktur dan telaah dokumen. Penulis akan melakukan wawancara terstruktur dengan menetapkan pertanyaan yang akan diajukan. Kemudian, metode dokumentasi dapat membantu penulis untuk menemukan data atau fakta yang tersimpan dalam bentuk arsip, hasil rapat, jurnal, dan sebagainya. Penulis akan melakukan wawancara dengan Kementerian dan Lembaga terkait, diantaranya:

1. Sulistyono (Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia)

Selain melakukan interview dengan kementerian dan lembaga terkait, penulis juga akan memperkokoh data dari dokumen dan internet. Hal itu dilakukan agar deskripsi hasil yang penulis sajikan dapat memperkaya tulisan dan data yang diperoleh.

III.4 SUMBER DATA

Penelitian ini didukung oleh berbagai sumber data, sebagaimana digariskan oleh penulis terhormat Arikunto (2006) dan Lofland (sebagaimana dikutip dalam Moleong, 2007). Menurut Arikunto, sumber data mengacu pada subjek dari mana data dapat dikumpulkan. Sementara itu, Lofland mengemukakan bahwa penelitian kualitatif mengandalkan kata-kata dan tindakan sebagai sumber primer, dengan data tambahan yang berasal dari dokumen dan sumber lain. Untuk penelitian ini, sumber data telah dikategorikan menjadi dua kelompok yang berbeda, yakni:

- A. Sumber data primer, yakni terkait kegiatan yang dilakukan dalam kerjasama antara australia dengan BSSN dalam meningkatkan keamanan siber di indonesia, kemudian hasil yang didapatkan dari kerjasama tersebut keujtungan ataupun perubahan dalam keamanan siber di indonesia. Kemudian data primer mengenai bentuk kerjasama yang dilakukan australia dengan indonesia dalam menyikapi ancaman siber yang ada di indonesia serta hasil yang diperoleh dari pertemuan-pertemuan internasional yang membahas keamanan siber di indonesia dengan australia.
- B. Sumber data sekunder, yakni berupa informasi pendukung seperti jurnal, dokumen, catatan, berita, dan sumber pendukung lainnya yang kredibel mengenai peningkatan keamanan siber. Selain itu sebagai data pendukung, penulis juga akan melihat bagaimana peluang ancaman siber di indonesia lebih besar atau tidak, lalu kebijakan dan ketentuan yang ditetapkan oleh BSSN dalam meningkatkan keamanan siber di indonesia.

III.5 TEKNIK ANALISIS DATA

Teknik analisis data dalam penelitian ini yakni berupa data yang berbentuk kata-kata yang akan disusun dalam struktur klasifikasi. Data dalam penelitian

didukung oleh wawancara dan telaah dokumen. Menurut (Miles & Huberman, 1994), ada beberapa tahapan proses setelah pengumpulan data, diantaranya:

III.5.1 Data Reduction (Reduksi Data)

Dalam proses reduksi data, data yang diperoleh akan dirangkum dan dipilah pokok-pokoknya. Hal tersebut dilakukan agar fokus pada hal-hal yang penting secara tema penelitian dan pola. Reduksi data akan mempermudah penulis untuk memberi gambaran dan mengumpulkan data- data selanjutnya. Parafrase juga dilakukan agar penelitian mengikuti gaya penulisan peneliti. Tahapan reduksi data sudah penulis lakukan sejak memilih topik penelitian dengan menemukan pokok permasalahan dari penelitian ini, yakni bagaimana kerjasama antara BSSN dengan australia dalam meningkatkan keamanan siber di indonesia . Selanjutnya, penulis akan mereduksi data di pembahasan setelah melakukan proses wawancara dengan informan dan memberikan data pendukung berupa telaah dokumen, jurnal terkait, website kementerian dan lembaga, serta berita. Penulis mengelompokkan sesuai dengan sub-bahasan yakni mulai dari keamanan siber di indonesia itu sendiri, hingga proses kerjasama Indonesia dengan Australia untuk meningkatkan keamanan siber . Data dan informasi yang akan penulis peroleh akan disajikan dalam kata-kata atau deskripsi, grafik, tabel dan kutipan.

III.5.2 Data Display (Penyajian Data)

Penyajian data yang dilakukan setelah proses reduksi data. Dalam penelitian kualitatif, (Miles & Huberman, 1984) penyajian data yang dilakukan adalah berupa teks naratif. Penyajian data yang akan dilakukan penulis adalah per subbab pembahasan agar data yang disajikan lebih fokus. Kemudian, penyajian data juga didukung dengan tabel, grafik dan gambar terkait topik penelitian agar memudahkan penulis dan pembaca dalam memahami substansi penelitian mengenai kerjasama antara australia dengan BSSN dalam meningkatkan keamanan siber di indonesia tahun 2019-2022.

III.5.3 Penarikan Kesimpulan dan Verifikasi Data

Data yang sudah penulis peroleh dalam mendukung penelitian akan diuji keabsahan datanya melalui validasi data. Penulis akan menggunakan

teknik triangulasi untuk memvalidasi data penulis. Teknik triangulasi untuk meningkatkan pemahaman penulis tentang fakta dan data yang diperoleh. Triangulasi data merupakan sebuah gabungan dari beberapa metode untuk mengkaji keterkaitan antar isu melalui membandingkan informasi dengan informasi lainnya melalui sumber berbeda. Proses ini akan dilakukan penulis dengan membandingkan data primer yakni hasil wawancara dan sekunder yang diperoleh dari kementerian dan lembaga terkait dengan jurnal, telaah dokumen, berita dan portal website resmi pemerintah. Triangulasi yang dilakukan penulis guna mencegah adanya bias, sehingga data yang diperoleh adalah valid.

Proses penarikan kesimpulan yang dilakukan penulis dapat berupa deskripsi mengenai kegiatan kerjasama yang dilakukan untuk meningkatkan keamanan siber di Indonesia. Tahapan penarikan kesimpulan dilakukan selama proses penelitian berlangsung. Kesimpulan yang dilakukan akan diverifikasi melalui data yang sudah diperoleh sesuai dengan topik penelitian. Penarikan kesimpulan akan menjawab rumusan penelitian ini atau tidak, karena isu yang dibahas dan rumusan masalah dalam suatu penelitian kualitatif bersifat sementara dan akan terus berkembang atau pun mengalami perubahan selama penelitian berlangsung. Oleh karena itu, kemungkinan munculnya penambahan data akan ada sampai penelitian selesai.

III.6 TABEL RENCANA WAKTU

no	Uraian kegiatan	(Bulan)Tahun 2022			(bulan)Tahun 2023						(bulan) Tahun 2024		
		1 0	1 1	1 2	3	4	5	6	7	8	1	2	3
1	Pengumpulan outline	X											
2	Penyusunan proposal		X	X	X	X							
3	Bimbingan proposal		X	X	X	X							
4	Sidang proposal						X						
5	Revisi proposal							X					
6	Bimbingan skripsi							X	X	X			
7	Pengumpulan data							X	X	X			
8	Analisis data							X	X	X			
9	Penyusunan hasil penelitian							X	X	X			
10	Sidang skripsi										X		

BAB IV

GAMBARAN UMUM KEAMANAN SIBER INDONESIA DAN AUSTRALIA

IV.1 Kondisi Ruang Keamanan Siber Indonesia dan Australia

IV.1.1 Ruang Keamanan Siber Indonesia

Keamanan Siber di Indonesia telah mengalami perubahan dan peningkatan yang signifikan dari masa ke masa. Sementara itu, cikal bakal perkembangan siber di Indonesia tidak terlepas dari peristiwa awal kemerdekaan Indonesia, tepatnya 4 April 1946. Sebelum melihat sejarah keamanan siber di Indonesia, penting nya memahami dulu apa itu keamanan siber. Menurut National Cyber and Cryptocurrency Authority, keamanan siber adalah serangkaian upaya yang ditujukan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi dan semua komponen dan fasilitas pendukungnya di tingkat nasional, yang bersifat interdisipliner.

Sejalan dengan perkembangan teknologi global saat ini. Kejahatan siber memerlukan perhatian dan keseriusan dalam mengembangkan keamanan siber di setiap negara, termasuk Indonesia. Saat ini Indonesia berada dalam situasi yang mendesak untuk meningkatkan kapasitas keamanan sibernya karena tingkat kejahatan siber yang sangat mengkhawatirkan. Berbeda dengan jenis kejahatan lainnya, pola pikir holistik diperlukan untuk mempraktikkan keamanan siber. Berdasarkan permasalahan tersebut, Dewan Teknologi Informasi dan Komunikasi Nasional Indonesia berupaya mencari solusi agar keamanan siber dapat terjaga sepenuhnya di Indonesia dengan peningkatan kejahatan jaringan yang sangat pesat. Seperti pada Program Reformasi Birokrasi ke-9 dan Nawacita ke-5, pembangunan keamanan siber nasional sangat erat kaitannya dengan pembangunan pemerintahan yang bersih, efisien, demokratis, dan amanah. Oleh karena itu, penulis akan menyusun kajian mengenai perkembangan keamanan siber

nasional di Indonesia. Pertama-tama kita harus memahami sejarah keamanan siber untuk memahami bagaimana perlindungan data berevolusi dari eksperimen sederhana. Sejalan dengan data statistik saat ini, hal ini menunjukkan bahwa popularitas keamanan siber akan terus meningkat, dengan semakin mahirnya para penjahat siber dalam menggunakan strategi dan metode terkini untuk melakukan serangan siluman menggunakan teknologi baru seperti AI (Kecerdasan Buatan), teknologi blockchain. dan mesin penambangan (ML).

Hasil analisis data sistem manajemen lalu lintas siber ID-SIRTII mengungkapkan, kejadian serangan di dunia maya mencapai sejuta kasus, yang disebabkan oleh kelemahan sistem dan aplikasi yang tidak diketahui. Institusi negara juga tidak kebal terhadap serangan kejahatan siber, dengan sebanyak 2.138 serangan yang menyasar situs web pemerintah Indonesia antara tahun 1998 hingga 2009. Banyak terjadi perang siber di seluruh dunia dan bahkan pada tahun 2017 terjadi serangan siber virus WannaCry 2.0 atau WannaCry yang dengan cepat menyebar dan menginfeksi semua negara di dunia. Hal ini tentu membuat Indonesia semakin khawatir terhadap permasalahan keamanan siber yang berkaitan dengan keamanan nasional.

Sejalan dengan pesatnya dampak sistem jaringan global dan perkembangan teknologi internet di Indonesia, hal ini semakin meningkatkan kerentanan keamanan informasi organisasi terhadap ancaman siber. Bagi para pengambil keputusan di era inovasi informasi saat ini, serangan siber merupakan sebuah tantangan tersendiri. Peningkatan kejahatan menggunakan teknologi informasi telah diamati sejak tahun 2003, seperti kejahatan kartu (penipuan kartu kredit), skimming ATM dan EDC (awal tahun 2010), hacking, phishing (penipuan perbankan online), malware (virus/worm/trojan/bots), kelompok mafia dunia maya, pornografi, perjudian online, kejahatan internasional, perdagangan narkoba, terorisme, pencucian uang, perdagangan manusia, underground economy) (IDSIRTII/CC, 2017).

Sebagai acuan pemerintah dalam penegakan hukum keamanan siber di Indonesia, maka Pemerintah mengeluarkan beberapa peraturan perundang-undangan. Selain itu yang menjadi rujukan undang-undang adalah kesadaran yang paling penting dan relevan meningkatkan kesadaran akan keamanan siber di semua tingkatan termasuk pemerintah, industri dan masyarakat sipil mulai dari anak sekolah, pemuda, orang tua, pekerja hingga pakar keamanan, anggota dewan dan komisaris serta pegawai negeri.

Laporan National Cyber Index (NCIS) yang terbaru mengatakan bahwa Indonesia berada di peringkat 84 dengan skor keamanan siber 38,96. NCIS menggunakan 12 komponen dalam pembuatan laporan ini, mulai dari pengembangan kebijakan keamanan siber hingga perlindungan informasi pribadi dan pemberantasan kejahatan siber. Laporan NCIS menunjukkan bahwa Indonesia menduduki peringkat tiga terbawah dalam peringkat keamanan siber sehingga menunjukkan bahwa keamanan siber Indonesia masih sangat rendah dibandingkan negara-negara G20. Indonesia hanya lebih unggul dari Meksiko dan Afrika Selatan, sedangkan Meksiko dan Afrika Selatan tidak terpaut jauh dari segi poin.

Global Cyber Security Index (GCI) merupakan kegiatan survei International Telecommunication Union (ITU) dalam mengukur upaya keamanan siber negara-negara anggota ITU. Tujuan dari GCI adalah memberikan bantuan kepada negara-negara untuk mengidentifikasi peluang meningkatkan keamanan siber guna memperkuat komitmen komunitas internasional terhadap keamanan siber di seluruh dunia. Penilaiannya akan didasarkan pada lima pilar.

- 1) Legal, namun sudah memiliki lembaga hukum dan kerangka keamanan siber.
- 2) Teknis. Hal ini dinilai dari keberadaan institusi teknis dan penerapan teknologi.
- 3) Institusionalisme. Diukur melalui koordinasi pembuat kebijakan dan pengembangan strategi keamanan siber.

- 4) Pengembangan kapasitas. Diukur melalui penelitian dan pengembangan, program pelatihan, profesional dan karyawan bersertifikat.
- 5) Kolaborasi. Hal ini diukur dengan adanya kemitraan, kerangka kolaboratif, dan jaringan berbagi informasi.

KAMI (Indeks Keamanan Informasi) versi 3.1 adalah alat untuk mengukur tingkat penerapan standar dari keamanan siber, serta tingkat penerapan dan pemantauan pengendalian keamanan informasi. Indeks KAMI dikembangkan oleh Kementerian Informasi dan Komunikasi. Tujuan dari alat penilaian ini bukan untuk menganalisis kelayakan atau efektivitas bentuk keamanan yang ada, melainkan untuk memberikan wawasan kepada manajemen organisasi mengenai tingkat kesiapan (kelengkapan dan kelengkapan) informasi tertentu dalam kerangka kerahasiaan. Alat penilaian Indeks KAMI dikelola oleh personel yang berwenang dan bertanggung jawab langsung dalam mengelola keamanan informasi di seluruh organisasi yang dipimpinnya. Penilaian Indeks KAMI mencakup lima bagian tematik: Manajemen Keamanan Informasi, Manajemen Risiko Keamanan Informasi, Kerangka Keamanan Informasi, Aset Manajemen Keamanan Informasi, dan Teknologi Informasi. Sebelum melakukan penilaian kuantitatif, terlebih dahulu harus dilakukan proses pengklasifikasian jenis-jenis sistem elektronik.

Standar keamanan siber Indonesia dibuat pada tahun 2009, masing-masing berisi spesifikasi teknis dan persyaratan yang harus diikuti saat membuat sistem manajemen keamanan jaringan (ISMS). Standar ini tidak bergantung pada produk TI dan persyaratan manajemen risiko dan bertujuan untuk memastikan bahwa fitur keamanan yang dipilih dapat melindungi sumber daya informasi terhadap berbagai risiko dan memberikan kepercayaan Stakeholder terhadap tingkat keamanan informasi. Pengembangan standar Proses pendefinisian, penerapan, pengoperasian, pemantauan, peninjauan, pemeliharaan, dan peningkatan SMKI. Pentingnya pendekatan proses untuk mendorong pengguna sistem keamanan siber adalah :

- a) Memahami persyaratan keamanan informasi organisasi dan kebutuhan akan kebijakan dan tujuan keamanan informasi.
- b) Penerapan dan penggunaan pengendalian manajemen risiko keamanan informasi sehubungan dengan risiko bisnis umum organisasi.
- c) Memantau dan mengkaji efektivitas dan efisiensi SMKI.
- d) Perbaikan berkelanjutan berdasarkan pengukuran tingkat pencapaian tujuan.

Berikut adalah fungsi dan kategori bersama dengan pengidentifikasi dan pendefinisian yang unik, yaitu :

- 1) Identifikasi: meningkatkan pemahaman organisasi untuk mengelola risiko keamanan siber terhadap sistem, aset, informasi, dan kemampuan;
- 2) Perlindungan: pengembangan dan penerapan langkah-langkah perlindungan yang diperlukan untuk memastikan penyediaan layanan infrastruktur penting;
- 3) Deteksi: meningkatkan dan menetapkan langkah-langkah yang tepat untuk mendeteksi insiden keamanan siber;
- 4) Respon: meningkatkan dan menerapkan langkah-langkah yang tepat untuk insiden keamanan siber yang teridentifikasi
- 5) Pemulihan: meningkatkan dan menerapkan langkah-langkah yang tepat untuk mempertahankan rencana yang kuat dan memulihkan operasi atau layanan yang terganggu oleh insiden keamanan siber.

Hasil penilaian keamanan siber bagi negara-negara yang sudah memiliki program dan sedang mengembangkan program keamanan siber namun belum melaksanakannya yaitu negara-negara yang baru memulai komitmennya terhadap keamanan siber (ITU, 2017). Di tingkat nasional, Kementerian Komunikasi dan Informatika telah membuat Indeks Keamanan Informasi atau indeks KAMI. Indeks KAMI adalah suatu aplikasi yang berguna untuk menilai kematangan, tingkat realisasi penerapan SNI dan pedoman di

bidang manajemen keamanan sistem informasi instansi pemerintah. Penilaian dilakukan terhadap berbagai aspek penerapan keamanan informasi dengan serangkaian pembahasan yang memenuhi seluruh aspek keamanan yang ditetapkan dalam standar ,yaitu:

- 1) Manajemen perlindungan data
- 2) Manajemen risiko keamanan informasi
- 3) Kerangka keamanan informasi
- 4) Pengelolaan sumber daya informasi
- 5) Teknologi dan keamanan informasi
- 6) Peran TIK dalam penilaian produk indeks KAMI
2017

Bidang dengan nilai tertinggi standar ini adalah teknologi keamanan informasi. Sementara itu, nilai manajemen risiko keamanan informasi meningkat pada tahun 2017, dan nilai rata-ratanya tidak terlalu rendah. Area dengan nilai rata-rata terendah dalam daftar benchmark KAMI tahun 2017 adalah framework keamanan informasi. Saat ini indeks KAMI telah diedit oleh Badan Sibernetika dan Sandi Negara (BSSN), berdasarkan kriteria SNI ISO/IEC 27007, terkait dengan beberapa aspek:

- 1) Manajemen
- 2) Manajemen risiko
- 3) Kerangka kerja
- 4) Manajemen aset
- 5) Aspek teknologi

Lemahnya keamanan dsiber di Indonesia berasal dari kurangnya undang-undang terkait keamanan siber, yang menyebabkan kebingungan di kalangan warga negaranya. Dunia siber melintasi batas-batas, perbatasan dan bahkan batas individu, yang dapat menciptakan konflik dan perselisihan antar anggota masyarakat. Badan Siber dan Sandi Negara yang disingkat BSSN merupakan

representasi peran pemerintah dalam pengelolaan dunia maya nasional Indonesia.

Menurut laporan GCI 2020 yang dirilis pada tahun 2021 oleh ITU, badan khusus PBB yang berbasis di Jenewa, Swiss, indeks keamanan siber Indonesia menempati peringkat ke-24 dari 194 negara, naik dari peringkat ke-41 pada tahun 2018. Indonesia menempati peringkat keenam di Asia- Pasifik. regional dan ketiga di kawasan ASEAN setelah Singapura dan Malaysia. ITU adalah organisasi internasional yang dibentuk untuk menstandarisasi dan mengatur berita dan komunikasi internasional.

Menurut laporan National Cyber Security Index (NCSI) terbaru, negara ini berada di peringkat 83 dari 160 negara di seluruh dunia.

Berikut beberapa kejahatan yang sering terjadi di Indonesia sebagai berikut:

Penipuan Phising

Seperti namanya, phishing dapat diartikan sebagai “umpan” bagi penyerang untuk memberikan identitas dan informasinya. Banyak orang tidak menyadari bahwa mereka adalah korban penipuan phishing karena penyerang pandai berkomunikasi dengan “mengaitkan” korban dengan pertanyaan-pertanyaan yang menipu.

Peretasan

Peretasan merupakan upaya memasuki sistem komputer seseorang tanpa izin. Beberapa aktivitas peretas termasuk membobol sistem dan mencuri data pribadi dan keuangan.

Cyber Stalking

Cyber stalking adalah penggunaan Internet atau teknologi lain untuk menguntit atau mengintimidasi korban. penguntit juga akan melakukan sesuatu terhadap korbannya secara berulang, yang selain membuat korban merasa tidak nyaman, juga akan membahayakan nyawa korban.

Cyber Bullying

Cyber bullying penindasan atau pelecehan terhadap kelompok atau individu lain secara online melalui Internet atau teknologi lainnya. Hal ini sering terjadi di kolom komentar berbagai jejaring sosial.

Penulis melihat bahwa ketika terjadi peretasan dan pencurian data, penipuan phishing, peretasan cyber stalking, cyber bullying, yang terpenting adalah menilai dan menemukan sumber kerentanan yang dapat dieksploitasi para pelaku cyber crime. Oleh karena itu, fokusnya bukan lagi pada klarifikasi atau pembelaan diri, tetapi pada peningkatan infrastruktur, pengembangan teknologi, dan yang terpenting, pada perlindungan para profesional. Para pelaku cyber crime akan terus hadir sampai kita mampu memperbaikinya. Insiden phishing, kehilangan data pribadi online, dan serangan ransomware sering terjadi di seluruh dunia. Klarifikasi, penyangkalan, dan menyalahkan pihak lain tidak akan mencegah serangan. Yang paling penting, kita harus menemukan cara untuk mengurangi kerentanan pada keamanan siber kita sendiri.

Penulis juga meyakini bahwa keamanan siber adalah salah satu cara untuk membangun peradaban. Maka sikap yang jujur, integritas, dan profesionalitas dibutuhkan agar bisa terus mengembangkan cyber security tersebut. Serangan dunia maya biasanya dilakukan untuk kepentingan material, yaitu mencari ruang yang paling lemah. Jika kita menyadari bahwa pemrograman cyber security adalah cara untuk meningkatkan kualitas untuk masa yang akan datang.

Dalam uraian sebelumnya, kita dapat melihat adanya kelemahan yang dimiliki oleh Indonesia dalam keamanan siber, penulis juga bisa memberikan pandangan agar keamanan siber di Indonesia dapat di tingkatkan dengan beberapa strategi yang dapat dilakukan oleh Indonesia seperti Menyiapkan daftar proyek-proyek infrastruktur nasional yang penting dan bekerja sama secara terbuka dengan seluruh pemangku kepentingan dan perusahaan yang bergerak di bidang proyek tersebut. Disamping itu harus dibarengi dengan penyelenggaraan pelatihan manajemen krisis di tingkat nasional dengan partisipasi seluruh pemangku kepentingan dalam rangka persiapan yang matang

dan menyeluruh untuk menangani insiden siber. Menciptakan dan membangun masyarakat yang responsif dan memperkuat kemampuan untuk melindungi kepentingan nasional di dunia maya.

IV.1.2 Ruang Keamanan Siber di Australia

Pusat Keamanan Siber Australia didirikan pada tahun 2014, menggantikan Pusat Operasi Keamanan Siber, yang juga dikelola oleh Direktorat Sinyal Australia. Konsisten dengan rekomendasi tinjauan independen tahun 2017 terhadap komunitas intelijen Australia yang dipimpin oleh Michael L'Estrange dan Stephen Merchant, Perdana Menteri Malcolm Turnbull mengumumkan bahwa peran Pusat Keamanan Siber Australia akan ditingkatkan dan penguatan Penasihat Khusus Perdana Menteri program .Keamanan siber Alastair MacGibbon akan mengambil tanggung jawab sebagai kepala pusat Direktorat Sinyal Australia, yang didirikan sebagai badan hukum. Menurut Pusat Keamanan Siber Australia, laporan kejahatan siber meningkat hampir 13% pada tahun 2020-2021 dibandingkan tahun sebelumnya.

Pertumbuhan anggaran keamanan siber dalam beberapa tahun terakhir menunjukkan betapa seriusnya Australia. ACSC mulai beroperasi pada tahun 2014 sebagai kemitraan antar instansi pemerintah. Sejak saat itu, dan sebagai bagian dari Tinjauan Intelijen Independen tahun 2017, Pemerintah Australia telah mengidentifikasi kebutuhan untuk memberikan peningkatan kemampuan keamanan siber serta satu titik saran dan dukungan keamanan siber. Pada tanggal 1 Juli 2018, ketika ASD menjadi badan hukum, keahlian keamanan siber Pemerintah Australia dari Tim Tanggap Darurat Komputer Australia dan Badan Transformasi Digital dialihkan ke ACSC. Tujuan ACSC adalah untuk meningkatkan keamanan siber Australia dengan memantau ancaman siber. ACSC memberikan konsultasi keamanan siber kepada individu, bisnis, dan operator infrastruktur penting.

Australia berada di peringkat ke-4 di dunia setelah Inggris, Amerika Serikat, dan Kanada. Peringkat Australia meningkat dari peringkat keempat menjadi peringkat kedua berkat investasi berkelanjutan dalam reformasi pemerintahan dan penerapan Strategi Keamanan Siber 2016. Strategi internasional pertama Australia telah dipublikasikan dalam Tinjauan Intelijen Independen tahun 2017. Sejumlah rekomendasi memperkuat keamanan siber Australia perlindungan posisinya – termasuk memperluas kewenangan Australian Cyber Security Centre (ACSC) sebagai otoritas keamanan siber nasional dan merinci peran keamanan siber informasi ACSC.

Saat ini, organisasi-organisasi Australia menjadi sasaran para aktor siber negara yang canggih. Operasi-operasi ini menargetkan organisasi-organisasi Australia di berbagai sektor, termasuk semua tingkat pemerintahan, industri, organisasi kebijakan, pendidikan, kesehatan, penyedia layanan penting dan pemangku kepentingan lainnya. Menurut perkiraan Canberra, serangan siber terhadap bisnis dan rumah tangga Australia telah menimbulkan kerugian hingga 29 miliar dolar Australia atau setara dengan Rp302,5 triliun.

Jumlah ini menyumbang sekitar 1,5% PDB Australia.

Canberra hendak menganggarkan pertahanan siber senilai 1,6 miliar dollar Australia untuk 10 tahun ke depan. Hal itu dilakukan untuk menghindari pembengkakan kerugian akibat serangan siber.

Dalam sebuah makalah diskusi yang diterbitkan pada awal September 2021 oleh Canberra disebutkan bahwa 2,3 miliar dollar Australia atau sekitar Rp 24 triliun telah dicuri oleh penjahat siber dari warga Australia pada 2017.

Para peretas semakin berupaya mengambil keuntungan dari situasi pandemi COVID-19, secara aktif menyerang orang-orang yang rentan dan layanan kesehatan untuk memata-matai mereka serta mencuri uang dan data sensitif.

Jumlah serangan ransomware meningkat sekitar 15%, dan sektor kesehatan merupakan sektor terbesar kedua yang mengalami serangan siber. Ransomware adalah jenis malware yang bertujuan untuk memblokir akses ke sistem komputer hingga uang tebusan dibayarkan. Perangkat lunak ini bekerja dengan mengenkripsi data korban, dan peretas sering kali memberikan kuncinya dengan imbalan pembayaran mata uang kripto senilai jutaan dolar. Kebijakan inti untuk keamanan siber Australia terdapat 3 kebijakan inti yaitu:

- 1) Meningkatkan dan menyelaraskan kerangka peraturan
- 2)Memperkuat strategi keamanan siber internasional Australia
- 3)Sistem pemerintahan yang aman

Ada pula beberapa serangan terhadap keamanan siber di Australia yakni:

Serangan Siber Scott Morrison

Pada Juni 2020, pemerintahan Perdana Menteri Scott Morrison mengalami serangan dunia maya. Menariknya, serangan tersebut merupakan tindakan yang disponsori negara. Artinya, serangan tersebut tidak hanya ditujukan kepada perdana menteri namun juga terhadap pemerintah dan sektor-sektornya secara keseluruhan, seperti layanan kesehatan, pendidikan, dan banyak lainnya.

Karena serangan tersebut disponsori negara dan menyasar sektor pemerintah, alasan mereka melakukan serangan tersebut tidak jelas. Apakah mencari data untuk digunakan sebagai pengaruh di masa depan? Apakah mereka hanya mengawasi Australia? Kita mungkin tidak akan pernah tahu.

Apa pun masalahnya, serangan ini berarti bahwa bahkan organisasi tertinggi pun bisa menjadi korban serangan siber, oleh karena itu keamanan siber harus diprioritaskan.

Meningkatnya Kerentanan

Alasan sederhana mengapa langkah-langkah keamanan siber harus diterapkan adalah karena bisnis di Australia punya uang untuk dicuri. Karena negara ini memiliki perekonomian yang sehat dan hanya menggunakan teknologi terkini, maka negara ini akan selalu menghadapi risiko.

Ancaman semakin meningkat selama pandemi COVID-19 karena sebagian besar perusahaan beralih ke sistem kerja jarak jauh. Ketakutan dan kecemasan yang bertambah terhadap virus corona semakin meningkatkan serangan sejak penjahat dunia maya memanfaatkannya untuk keuntungan mereka.

Sebaliknya, bisnis kecil hanya dapat menerapkan keamanan siber pada tingkat yang lebih rendah. Oleh karena itu, usaha kecil dan menengah (UKM) terancam. Berbeda dengan bisnis besar yang menerapkan langkah-langkah keamanan siber yang ekstensif, mereka hanya bisa melakukan banyak hal, dan hal tersebut masih belum cukup untuk menjaga keamanan mereka.

Diplomasi siber Australia dengan Indonesia menggunakan strategi peningkatan kapasitas untuk saling memperkuat 55 cybersecurity kedua pihak, Australia melakukan peningkatan kapasitas untuk Indonesia dengan membuat program kerjasama peningkatan kesadaran dan pelatihan. Pada peningkatan kesadaran, Australia melakukan Cyber Policy Dialogue dengan Indonesia yang dimana program Cyber Policy Dialogue ini dilakukan sebanyak 3 kali. Cyber Policy Dialogue merupakan upaya Australia dalam meningkatkan kesadaran dan kapasitas Indonesia dalam meningkatkan cybersecurity dan peluang siber. Dalam Cyber Policy Dialogue I dilakukan dialog percakapan mengenai isu-isu siber, ancaman siber, kebijakan dan strategi, serta pentingnya perkembangan siber regional dan internasional. Lalu dalam Cyber Policy Dialogue II Australia dan Indonesia membahas masing-masing kepentingan dan kepentingan bersama mereka dalam internet yang terbuka, bebas dan aman yang mendukung sistem keamanan negara dalam ranah siber dan pertumbuhan ekonomi digital, Cyber Policy Dialogue II menghasilkan MoU kesepakatan untuk melanjutkan kerjasama dalam urusan siber. Cyber Policy Dialogue III dilakukan setelah adanya Cyber Bootcamp, pada dialog ini Australia menjelaskan akan pentingnya mekanisme siber internasional dan regional dalam membangun ruang siber yang aman. Cyber Policy Dialogue ini berperan penting dalam saling membangun kesadaran dan kapasitas Australia dan Indonesia. Pada pelatihan Australia melakukan pelatihan terhadap Indonesia melalui Cyber Bootcamp, Program Cyber Bootcamp dirancang dalam menyatukan

keterampilan dan keahlian yang saling melengkapi dari seluruh pemerintah, akademisi dan sektor swasta untuk memberikan program pelatihan yang komprehensif, holistik 56 dan inovatif kepada Indonesia. Cyber Bootcamp merupakan program intensif selama dua minggu di Australia dimana dalam kegiatan ini perwakilan Indonesia mengikuti pelatihan, workshop, kunjungan lokasi industri, dan dialog dengan lembaga pemerintah Australia. Dengan adanya program ini Australia berharap Indonesia dapat mengimplementasikan pelatihan dan pembelajaran dalam menangani isu-isu siber nasional yang akan berkontribusi untuk cybersecurity yang kuat bagi kawasan regional. Sehingga dapat disimpulkan bahwa upaya Australia dalam meningkatkan cybersecurity melalui diplomasi siber dengan Indonesia merupakan langkah yang sangat penting, hal ini demikian karena Indonesia merupakan mitra internasional yang cocok dalam penerapan Australia's International Cyber Engagement Strategy 2017 untuk meningkatkan cybersecurity nasional maupun regional dan peluang siber lainnya.

Penulis melihat akan adanya serangan keamanan siber di Australia, untuk keamanan siber di Australia ini pun menjadi ancaman serius karena dapat mencuri data, baik data pribadi maupun lainnya. Tidak seorang pun ingin data pribadi bocor secara terbuka, jadi kita harus proaktif dalam menggunakan langkah-langkah keamanan siber. Semakin aman data kita, semakin kita merasa aman menggunakan komputer

IV.2 Faktor kerjasama Keamanan Siber Indonesia dan Australia

IV.2.1 Perang siber antara Indonesia dan Australia

Melihat fenomena serangan dan kejahatan yang dialami oleh Indonesia dan Australia khususnya perang antara pelaku cyber Indonesia dan Australia pada bulan November 2013. Saat itu, saling serang antar website pun tak terhindarkan sehingga membuat hubungan kedua negara semakin harmonis.

Perang siber dimulai pada tahun 2009 dengan rumor bahwa agen intelijen

Australia telah menguping Presiden Susilo Bambang Yudhoyono (SBY) dan beberapa anggota kabinetnya. Informasi ini terungkap berdasarkan dokumen yang dibocorkan oleh mantan pejabat Kementerian. Edward Snowden dari Badan Keamanan Nasional (NSA). Dokumen yang bocor menyatakan bahwa badan intelijen Australia mengincar Presiden SBY, istrinya, Wakil Presiden Boediono, dan beberapa menteri lainnya. Bocoran tersebut juga mengtakan model ponsel yang digunakan masing-masing sasaran, termasuk diagram "audio event" Presiden SBY. yang juga merupakan mitra dagang yang sangat penting bagi Australia. Indonesia Di bawah pemerintahan Presiden Yudhoyono, Indonesia telah berpartisipasi dengan Australia dalam sejumlah forum regional utama untuk mencari kerja sama guna memerangi isu-isu seperti perdagangan manusia, pencucian uang, serangan teroris dan bentuk-bentuk korupsi lainnya. Pada akhirnya, negara dan individu tidak jauh berbeda. Negara tidak bisa hidup sendiri dan membutuhkan negara lain untuk mewujudkan cita-citanya, Oleh karena itu, keinginan untuk membangun hubungan antar bangsa sering disebut dengan hubungan internasional (Jackson dan Sorensen, 2005).

Begitu juga dengan Australia dan Indonesia tentunya saling membutuhkan sebagai negara, apalagi jika Indonesia dan Australia saling berdekatan dalam hubungan terkait lainnya. Meski hubungan kedua negara sempat berfluktuasi tergantung perimbangan kekuatan antar negara, namun hubungan tetap harmonis sejak Indonesia mendeklarasikan kemerdekaan pada tahun 1945.. Namun seiring berjalannya waktu, kedua belah pihak kerap menghadapi perbedaan pemahaman dalam berbagai isu, termasuk konfrontasi Indonesia-Malaysia, kasus Timor timur , dan konflik separatis Papua. masalah dan permasalahan umum lainnya yang dapat menimbulkan konflik antar negara. Meski demikian, kedua tetangga tersebut tetap bisa menyelesaikan masalah tersebut dengan baik tanpa konflik.

Pandangan penulis terhadap fenomena yang terjadi antara Indonesia dan Australia merupakan adanya relasi yang memang sudah lama dan mengalami pasang surut yang dimana selain kedua negara tersebut memiliki relasi dalam

kerjasama kedua negara inipun mengalami peperangan siber antara kedua nya yang dimana relasi yang di alami kedua negara tersebut pun mengalami bentrokan karena ada nya peperangan siber yang terjadi antara Indonesia dengan Australia,yang dimana peperangan itu terjadi dengan adanya Penyadapan dua negara, penyadapan lintas batas negara, sebenarnya sudah berlangsung lama. Dengan kemajuan teknologi, penyadapan sudah menjadi hal biasa di telepon seluler, website, internet, gadget frekuensi, satelit, dan alat teknologi lainnya, sehingga penyadapan sering dilakukan untuk tujuan negatif¹⁹(Sujadmiko, 2014). Pelanggaran terhadap UU No.2. Nomor 36 Tahun 1999 tentang Telekomunikasi dan UU Digital yang dengan jelas di langgar oleh Australia berdasarkan atas kepentingan diplomatik yang akan memberikan kekebalan berdasarkan hukum yang berlaku saat ini. Penyadapan yang dilakukan Australia jelas melanggar UU Telekomunikasi dan Digital 36 Tahun 1999. Informasi dan Transaksi Elektronik November 2008. Perlakuan memalukan ini diterapkan Australia berdasarkan kepentingan diplomatik (dalam undang-undang saat ini dianggap impunitas atau impunitas). Namun kenyataannya hal tersebut melanggar hukum Republik Indonesia dan hukum internasional.

Tindakan intersepsi yang dilakukan tentunya menimbulkan kerugian yang besar bagi pihak Indonesia yang menjadi korban dari tindakan intersepsi tersebut. Kerugian yang paling dapat diperkirakan adalah terbongkarnya rahasia negara, khususnya mengenai politik luar negeri yang ditempuh negara Indonesia. Ketika Australia menerima data dari Indonesia, kita dapat memperkirakan bahwa Australia akan lebih mudah membaca dan memprediksi kebijakan yang akan diterapkan oleh Indonesia. Australia berpendapat bahwa selain hukum dalam negeri Indonesia, hal ini melanggar hubungan internasional dan ketentuan perjanjian internasional tahun 1961 (Konvensi Wina tentang Hubungan Diplomatik) yang disetujui oleh Indonesia, Australia, dan negara

¹⁹ Sujadmiko, Bayu. (2014). PENYADAPAN LINTAS NEGARA KEDAULATAN DITINJAU DARI HUKUM INTERNASIONAL. https://www.researchgate.net/publication/305462455_PENYADAPAN_LINTAS_NEGARAKEDAULATAN_DITINJAU_DARI_HUKUM_INTERNASIONAL/citation/download

lain. Ini adalah subkultur yang memberontak terhadap sistem yang sudah mapan, dan bagi sebagian peretas, nasionalisme dan persekutuan masyarakat adalah hal yang penting.

Karena yang menjadi sasaran penyadapan ini adalah tokoh-tokoh penting di Indonesia, maka tidak berlebihan jika dikatakan bahwa masyarakat Indonesia, termasuk para hacker Indonesia, sangat marah. Ini adalah data dari kantor negara yang diblokir oleh Australia.

Perang hacker antara Indonesia dan Australia tidak terlepas dari sentimen nasionalis masing-masing negara. Keduanya percaya bahwa negaranya benar dan harus dilindungi olehnya. Jika menyangkut benar dan salahnya suatu negara, yang terpenting adalah melindungi negara tersebut. Sebelumnya, hacker digambarkan sebagai aktor non-negara yang berperan dalam hubungan internasional. Saat ini, pelaku serangan di dunia siber tidak hanya melakukan kejahatan demi keuntungan finansial, namun juga kelompok teroris dan hacktivist yang berkonten politik kuat. Anonimitas serangan siber juga menciptakan peluang bagi aktor negara untuk melakukan serangan siber jika diperlukan²⁰ (Chandra, 2018). Penyadapan tersebut memicu respons dari para peretas Indonesia, yang segera melancarkan serangan terhadap sejumlah situs web Australia, baik swasta maupun pemerintah, yang tampaknya merugikan Australia. Di antara puluhan website yang diserang hacker Indonesia, terdapat website strategis pemerintah, yaitu situs intelijen dan kepolisian. Peretas Indonesia melintasi batas negara dan mengikuti pola yang tidak sistematis, sehingga sulit dideteksi. Hal ini terbukti ketika pemerintah Indonesia dan Australia mengakhiri konflik akibat penyadapan beberapa pejabat, namun peretas tetap melancarkan perang siber.

Dari fenomena diatas penulis bisa memberikan pandangan yang dimana Kelompok yang sejak awal melakukan penyerangan, bahkan sebelum pemerintah pusat memberikan tanggapan, yaitu Anonymous Indonesia

²⁰ Yudha, Chandra. 2018. Penguatan kerjasama cybersecurity: keniscayaan untuk ASEAN. Majalah masyarakat ASEAN. kemenlu

(Anonindo), terus melakukan penyerangan meski terjadi dialog antar pemerintah. Padahal itu merupakan kejahatan terhadap pemerintah Australia dan sektor swasta. Pikirkan tentang serangan itu. Mengenai apakah hacker apakah mereka penjahat atau bukan, masih perlu dilakukan verifikasi mengenai penelitian hubungan internasional apakah hacker tergolong aktor non-negara dalam kategori organisasi kriminal transgender (kejahatan federal) atau tidak. Hal ini perlu diidentifikasi karena aktor negara dapat terlibat atau memfasilitasi peretas dalam perang siber. Masih belum ada data yang jelas apakah pemerintah Indonesia menggunakan peretas dalam konflik penyadapan ini. Namun terlihat jelas bahwa pemerintah Indonesia mengabaikan dan seolah-olah mengambil keuntungan dari munculnya peretas dalam konflik penyadapan ini.

Penulis melihat perang siber antara peretas Indonesia dan Australia menunjukkan bagaimana perangkat lunak komputer telah menjadi alat yang dapat menghancurkan suatu negara. Perjuangan Australia melawan peretas setelah penyadapan pejabat pemerintah Indonesia membuktikan peran penting dunia maya dalam politik. Dalam konteks ini, penelitian hubungan internasional menunjukkan bahwa hacker merupakan aktor non-negara dalam hubungan internasional.

Dalam melaksanakan upaya pertahanan siber, Kementerian Pertahanan dan TNI mempunyai dua kepentingan utama. Kami berupaya melindungi seluruh sistem elektronik dan jaringan informasi di lingkungan kami. Kami berkomitmen untuk mendukung koordinasi keamanan siber di bidang lain jika diperlukan. Penting untuk dapat mengembangkan dan menerapkan kebijakan yang menjadi dasar atau referensi bagi seluruh aktivitas pertahanan siber, termasuk pengembangan kebijakan, operasional, dan koordinasi. Kebutuhan tersebut perlu dipenuhi dalam bentuk peraturan, pedoman, pedoman teknis, dan bentuk kebijakan lain yang dapat menjamin kelancaran operasional pertahanan siber.

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. 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. Teknologi dan infrastruktur pendukung Teknologi dan infrastruktur pendukung yang komprehensif diperlukan untuk melaksanakan pertahanan siber yang lebih efektif, serta peralatan dan fasilitas untuk melaksanakan operasi pertahanan siber. Teknologi dan infrastruktur pendukungnya harus dicapai melalui penelitian dan pengembangan serta tahap persiapan selanjutnya, serta pengembangan, adaptasi dan/atau peningkatan teknologi dan infrastruktur tersebut agar dapat dimanfaatkan sebaik-baiknya. Teknologi dan infrastruktur yang tersedia di Indonesia untuk mendukung pertahanan siber bersifat umum dan spesifik dan terus meningkat.

IV.2.2 Faktor Sumber Daya Manusia

Salah satu faktor pendukung dalam meningkatkan keamanan siber adalah melalui 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 pertahanan siber. Sumber daya manusia ini dapat diperoleh melalui program rekrutmen, pembinaan dan

pemisahan tugas sesuai 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 kepekaan 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, sebagaimana 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 Indonesia 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.

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 sebagai cyber law yang mengatur segala bentuk tindakan cybercrime, melainkan hanya perumpamaan

terhadap pasal-pasal dari kebijakan hukum yang berkaitan dengan teknologi informasi secara umum.

Berdasarkan Roadmap Pembinaan SDM Keamanan Siber dan Sandi 2020-2024, peluang karir di bidang keamanan siber dengan daya saing terbesar pada SDM dengan fokus keamanan jaringan. Sebagai informasi bahwa telah ada publikasi Peta Okupasi Nasional Fungsi Keamanan Siber untuk dapat menjadi rujukan dalam pengembangan standar kompetensi, penyelenggaraan aktivitas sertifikasi kompetensi berbasis skema okupasi, pengembangan kurikulum pendidikan, pemetaan profil kebutuhan dan ketersediaan serta pembuatan berbagai modul berbasis kompetensi. BSSN dengan Kementerian/Lembaga terkait telah menghasilkan beberapa standar kompetensi kerja nasional Indonesia (SKKNI) bidang keamanan siber dan telah terbentuk lembaga sertifikasi profesi (LSP) BSSN untuk menjawab berbagai peluang karir SDM di bidang keamanan siber di tahun-tahun mendatang. Digitalisasi dapat berjalan dengan baik dengan adanya keamanan didalamnya.

IV.2.3 Faktor strategi Keamanan Siber Indonesia dan Australia

Indonesia menganggap Australia sebagai negara dengan ruang kondisi keamanan siber yang baik. Hal ini terlihat jelas dari Strategi Keamanan Siber Australia yang diterbitkan pada bulan April 2016. Strategi Keamanan Siber Australia dirancang untuk meningkatkan konektivitas bagi warga Australia untuk terhubung dengan orang-orang di seluruh dunia melalui dunia maya. Bukti dari pertumbuhan ini adalah 90% warga Australia aktif menggunakan internet, mayoritas warga Australia menggunakan internet satu hari dalam seminggu, dan 84% usaha kecil Australia memiliki akses ke internet. Strategi Keamanan Siber Australia mencakup lima tema aksi untuk tahun 2020. Kelima topik aksi tersebut adalah Kemitraan Siber Nasional, Pertahanan Siber yang Kuat, Tanggung Jawab dan Dampak Global, Pembangunan dan Inovasi, serta Pemanfaatan Siber yang Efektif. Penerapan masing-masing program yang tertuang dalam Strategi Keamanan Australia mempunyai keuntungan tersendiri.

Untuk membangun jaringan siber nasional, Australia akan melaporkan perkembangan strategi yang diterapkan, mengadakan pertemuan rutin dengan para pemimpin keamanan siber, membentuk badan yang mengawasi keamanan siber Australia dan mendirikan Pusat Pengembangan Keamanan Siber, Australia. Badan ini dikenal dengan nama Cyber Security Centre (CSC) dan mendanai penelitian terkait keamanan siber yang berdampak pada pembangunan ekonomi Australia. Selain meningkatkan konektivitas internet nasional, Australia juga memperkuat pertahanan sibernya dalam pembicaraan keamanan siber. Dengan latar belakang ini, pemerintah Australia telah mengembangkan pendekatan berlapis untuk mengidentifikasi dan mengatasi ancaman dunia maya yang muncul. Pendekatan hierarki ini memiliki tiga bagian yang saling terkait: Tingkat pertama adalah Cyber Australia - Australia dengan informasi rahasia tentang aspek kritis cyber praktik keamanan dengan mitra dengan mitra. Tingkat kedua adalah Pusat Ancaman Siber Bersama. Tingkat ini mencakup pemerintah, dunia usaha, dan peneliti Australia. Lapisan ini lebih fokus pada keamanan informasi sensitif terkait ancaman di dunia maya. Saat ini, lapisan ketiga adalah Portal Berbagi Ancaman Siber Online, sebuah portal online yang mencakup organisasi yang berbagi informasi ancaman dan hasil analisis ancaman siber. Strategi Australia ini juga menunjukkan bahwa Australia telah berupaya memperkenalkan kesadaran keamanan siber di kalangan masyarakat untuk mengatasi ancaman siber. Tanggung jawab global terhadap keamanan siber menjadi prioritas Australia sebagai bentuk akuntabilitas untuk mengurangi jumlah kejahatan siber di seluruh dunia. Saat ini, banyak sekali potensi kolaborasi. Dua tren yang menonjol dalam bagian ini adalah pembentukan asosiasi internasional untuk memerangi kejahatan dunia maya, dengan fokus pada kawasan Indo-Pasifik;

Sementara itu, Australia juga mengundang untuk peningkatan kapasitas siber di kawasan Indo-Pasifik melalui kemitraan publik-swasta dan mengumumkan strategi untuk mengatasi masalah internet global dan memastikan semua negara memiliki internet yang terbuka, gratis, dan aman.

Menciptakan pertumbuhan dan keterlibatan secara online. Dalam hal ini sangat mungkin terjadi. Untuk pengembangan dan inovasi, Australia mendirikan Pusat Pengembangan Keamanan Siber dengan sektor swasta untuk mengoordinasikan Jaringan Inovasi Keamanan Siber Nasional, yang memelopori penelitian dan inovasi keamanan siber. Selain itu, pemerintah Australia telah mendirikan pusat akademik keunggulan siber di beberapa universitas untuk meningkatkan literasi internet di kalangan angkatan kerja. Selain itu, terdapat kebutuhan mendesak untuk bekerja sama dengan sektor swasta dan internasional untuk meningkatkan kesadaran keamanan siber di seluruh masyarakat. Dua poin yang disebutkan di atas merupakan langkah yang diambil pemerintah Australia untuk menciptakan pengguna internet yang terinformasi.

Dari uraian kemampuan Australia di bidang keamanan siber di atas, penulis dapat menyimpulkan bahwa Australia dapat menjadi modal bagi perkembangan keamanan siber secara global. Hal ini dapat dilihat dari banyak sudut pandang. Meskipun demikian, Australia sangat inovatif dalam memberikan solusi terhadap tantangan-tantangan Internet global dengan mengembangkan strategi inklusif mengenai masalah-masalah Internet global dan mempromosikan Internet yang terbuka, bebas dan aman. Pertumbuhan dan akses Internet untuk semua negara. Perkembangan keamanan siber, jika berhasil dikembangkan, merupakan wadah bisnis baru bagi negara.

Di dunia bisnis adanya peningkatan sebesar 38% per tahun. Masalah-masalah serius ini memerlukan lebih banyak investasi nasional dalam pelatihan keamanan siber dan pengembangan alat. Pengeluaran keamanan siber di kawasan Asia-Pasifik diperkirakan mencapai \$22 miliar pada tahun 2020 memberikan Australia peluang untuk mengembangkan industri keamanan sibernya. Keamanan siber dirancang tidak hanya untuk melindungi negara dan komunitas bisnis, namun juga memungkinkan setiap individu melindungi diri mereka sendiri secara online. Faktanya, kemajuan keamanan siber Australia

bukanlah yang terbaik di dunia. Australia saat ini berada di peringkat kesembilan dalam hal pass rush. Saat ini, dalam hal pelanggan keamanan siber, Australia berada di peringkat kedelapan dengan 15 pelanggan, tertinggal dari negara terdepan, Amerika Serikat, dengan 827 pelanggan. Namun, Australia, meski bukan yang terbaik, masih merupakan peluang kerja sama bagi Indonesia mengingat beberapa hal. aspek. Pertama, Indonesia merupakan tetangga terdekat Australia, sehingga keamanan regional menjadi perhatian utama bagi negara-negara di kawasan. Kedua, meski bukan yang terbaik di dunia, perkembangan Internet di Australia dapat mengimbangi kekurangan perkembangan Internet di Indonesia yang fokus pada Internet. Penjelasan di atas menunjukkan kelemahan Indonesia dalam bidang pengembangan Internet sebagai berikut:

- 1) belum mempunyai peringkat kerentanan dan prioritas pada sektor infrastruktur.
- 2) Literatur terkait internet di Indonesia masih membingungkan; 3) kurangnya motivasi Indonesia untuk meningkatkan kesadaran masyarakat terhadap ancaman siber.
- 4)Penguatan kemampuan respon siber difokuskan pada sektor militer
- 5)Kemampuan internet tidak merata

Penulis berpendapat bahwa Indonesia dapat memperoleh manfaat dari kerja sama dengan Australia, dan ada tiga titik lemah yang dapat diperbaiki melalui kerja sama tersebut.

Kelemahan 1 dan 2 dapat dimanfaatkan melalui kehadiran Australian Academic Centre of Cyber excellence dari pusat penelitian ini akan membantu Indonesia menetapkan prioritas infrastrukturnya. sektor ini, memfasilitasi persiapan tindakan pencegahan lainnya,dengan perencanaan dan penentuan prioritas yang tepat, Indonesia diharapkan dapat menciptakan dokumen strategis yang lebih efektif dan mudah diterapkan ketika serangan siber terjadi. Kelemahan selanjutnya saat ini tidak bisa diatasi dengan pertukaran informasi

dengan negara mitra kerjasama Namun ini adalah masalah yang bisa diselesaikan di Indonesia.

IV.3 MoU BSSN dan DFAT

Kesepakatan yang di lakukan oleh Pemerintah Republik Indonesia dan Pemerintah Australia untuk memperkuat kerja sama di bidang keamanan siber melalui penandatanganan Memorandum of Understanding (MOU) pada kunjungan resmi Perdana Menteri Australia ke Istana Bogor pada Jumat 31 Agustus 2018. Djoko Setiadi, Direktur Badan Keamanan Siber Nasional (BSSN) dan Tobias Feakin, Duta Besar Australia untuk Masalah Siber, menandatangani MoU tersebut di hadapan Presiden di kantor pusat departemen Australia. Kementerian Dalam Negeri dan Perdagangan Luar Negeri. Perdana Menteri Indonesia Joko Widodo dan Perdana Menteri Australia Scott Morrison.

Menciptakan jaringan nasional dan internasional merupakan salah satu dari tujuan utama BSSN dalam menciptakan keamanan siber Penandatanganan MoU yang dilakukan merupakan bukti prioritas yang bertujuan untuk meningkatkan hubungan dan memberikan kerangka kerja sama di bidang keamanan siber. MoU juga Melaksanakan berbagai kegiatan yakni:

- a) pertemuan bilateral antara BSSN dengan DFAT dan Kedutaan Besar Australia di Jakarta serta Ambassador Australia untuk Urusan Siber dan Teknologi Kritis yang membahas isu keamanan siber.
- b) Berbagi praktik terbaik dalam penyusunan Strategi Keamanan Siber Nasional antar negara.
- c) Penyelenggaraan berbagai bentuk peningkatan kapasitas SDM Keamanan Siber seperti Australia Cyber Bootcamp dan SANS Training.

BSSN bukanlah organisasi baru Melainkan merupakan penggabungan dari lembaga keamanan pemerintah sebelumnya, seperti Badan Sandi Negara (Lemsaneg) dan Direktorat Keamanan Informasi, Direktorat Aplikasi Informasi, dan Kementerian Komunikasi. BSSN didirikan untuk melaksanakan fungsi pemerintahan yang berkaitan dengan keamanan siber dan pengamanan kata sandi, membantu Presiden dalam sosialisasi undang- undang dan melaksanakan seluruh tugas dan fungsi di bidang sandi di Lemsaneg dan pengamanan sandi, informasi, jaringan dan infrastruktur telekomunikasi di Lemsaneg. Kementerian Informasi dan Komunikasi. BSSN mempunyai tugas melaksanakan fungsi pemerintahan di bidang keamanan siber dan sandi untuk membantu Presiden dalam menjalankan pemerintahan.

Dalam melaksanakan fungsi tersebut, BSSN menyelenggarakan fungsi sebagai berikut:

- 1) Menyusun dan menerbitkan pedoman teknis di bidang keamanan jaringan dan password;
- 2) Melaksanakan bimbingan teknis di bidang keamanan jaringan dan password;
- 3) Mengembangkan norma, standar, proses dan kriteria di bidang enkripsi;
- 4) Melaksanakan pelatihan teknis dan supervisi di bidang sandi;
- 5) Mengkoordinasikan pelaksanaan tugas, memberikan bimbingan dan dukungan administratif kepada seluruh bagian organisasi di lingkungan BSSN;
- 6) Pengelolaan kekayaan negara menjadi tanggung jawab BSSN;
- 7) Memberikan dukungan menyeluruh kepada seluruh komponen organisasi di lingkungan BSSN
- 8) Memantau pelaksanaan tugas di lingkungan BSSN.

Departemen Luar Negeri dan Perdagangan (DFAT) bekerja dengan mitra internasional dan negara-negara lain untuk mengatasi tantangan global,

meningkatkan peluang perdagangan dan investasi, melindungi peraturan internasional, menjaga stabilitas kawasan dan membantu warga Australia di luar negeri. DFAT mengelola kehadiran internasional Australia, jaringan yang terdiri lebih dari 120 kedutaan, komisi tinggi, konsulat jenderal, dan kantor perwakilan di lima benua. Kami mempekerjakan lebih dari 6.000 orang, termasuk orang Australia dan luar negeri. anggota ini termasuk diplomat, negosiator, dan pejabat konsuler. dan konsultan yang mengembangkan dan menerapkan kebijakan luar negeri, perdagangan dan pembangunan atas nama Australia dan warga Australia. DFAT merupakan badan yang mewakili Australia dalam kerja sama keamanan siber dengan BSSN.

Melalui MoU ini, Indonesia dan Australia dapat mewujudkan kepentingan bersama untuk saling memperkuat hubungan persahabatan kedua negara berdasarkan prinsip kesetaraan dan timbal balik.

Indonesia dan Australia akan bekerja sama di berbagai bidang, antara lain: berbagi informasi dan praktik terbaik; meningkatkan kapasitas dan memperkuat koneksi; serta kerja sama di bidang ekonomi digital; dan di bidang manajemen kejahatan dunia maya.

Setelah MoU ini, BSSN menjadi lembaga utama Kementerian Luar Negeri dan Perdagangan untuk Republik Indonesia dan Australia.

Adanya juga 4 bagian poin dalam MoU yang di lakukan Indonesia dan Australia

- a) Berbagi Informasi dan Praktik Terbaik, berupa sharing session dengan E-Safety Commissioner.
- b) Pembangunan Kapasitas dan Mempererat Hubungan melalui berbagai pelatihan, simposium, dan kegiatan peningkatan kapasitas lainnya.

- c) Ekonomi Digital, berupa pelibatan pada berbagai forum seperti Australia-Indonesia Digital Forum di Jakarta dan Australia Embassy Jakarta Digital Month.
- d) Kejahatan Siber, berupa peningkatan kapasitas SDM
Keamanan Siber termasuk investigasi dan digital forensik

Pada tulisan ini penulis mengambil salah satu program kerjasama MoU yaitu pada poin pertama :

Best Practice and Share Information:

- a) Peserta akan melakukan pertukaran informasi mengenai undang-undang dan perundang-undangan, strategi dan kebijakan siber nasional, serta prosedur manajemen insiden siber
- b) Peserta akan berkonsultasi dan berkoordinasi mengenai respon insiden siber dan informasi ancaman siber, terutama apabila insiden siber mempunyai dampak langsung terhadap Peserta
- c) Peserta akan berbagi pandangan, pengalaman, pembelajaran dan praktik terbaik mengenai isu-isu siber serta risiko dan peluang yang ditimbulkan oleh isu-isu teknologi siber yang muncul yang memiliki kapasitas untuk secara signifikan meningkatkan atau menimbulkan risiko terhadap keamanan nasional.

Penulis berharap melalui MoU ini, dapat terjalin kerjasama antara Indonesia dengan Australia di bidang keamanan siber dalam rangka menciptakan keamanan nasional maupun kawasan, khususnya di Indonesia dan Australia.

BAB V

KERJA SAMA BADAN SIBER DAN SANDI NEGARA (BSSN) DAN DEPARTEMEN OF FOREIGN AFFAIRS AND TRADE (DFAT) DALAM ATKAN KEAMANAN SIBER INDONESIA MELALUI PRORAM SHARE INFORMATION AND BEST PRACTICE DATA KEJAHATAN SIBER DI INDONESIA

V.1 DATA JENIS KEJAHATAN SIBER INDONESIA

Laporan NCSI sangat penting jika kita melihat realita yang terjadi di Indonesia. Berdasarkan laporan masyarakat bulanan hasil pemantauan keamanan siber bulan Agustus 2022 yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN), terdapat 44.776.891 anomali lalu lintas yang terjadi di Indonesia sepanjang Agustus 2022. Anomali siber adalah pola keamanan yang menyimpang dari pola siber normal dan terjadi dengan cara yang tidak masuk akal, yang mungkin merupakan tanda serangan dunia maya (Huo, *et al.*, 2019).

Tabel 2.1 tabel jumlah dan jenis kejahatan siber

Jenis Anomali	Jumlah
Malware	24.448.343
Trojan Activity	8.362.317
Information Leak	7.084.332
Exploit	1.644.543
APT	387.307
Web Application Attack	343.510
Information Gathering	177.510
Denial of Service	50.115
Others	2.278.914

(sumber: <https://cfds.fisipol.ugm.ac.id/id/2023/03/28/>)

Laporan BSSN menunjukkan bahwa, selain trafik yang luar biasa tinggi, banyak email phishing yang terjadi di Indonesia sepanjang Agustus 2022. Email phishing meniru identitas orang atau organisasi yang berwenang melalui email, sehingga data sensitif seperti ID pengguna, kata sandi, dan lainnya diminta dan disalahgunakan. Laporan BSSN menunjukkan 6.342 kasus email phishing pada Agustus 2022. Email phishing ini sebagian besar berisi dokumen dengan ekstensi.pdf. Topik yang digunakan termasuk keamanan siber, urgensi pembayaran, dan bukti pembayaran, antara lain. Terakhir, laporan BSSN mengungkapkan berapa banyak website yang dihack di Indonesia. Sepanjang Agustus 2022, 148 situs web telah diserang oleh pihak ketiga. Situs web diretas termasuk situs pemerintah, lembaga penegakan hukum, dan lainnya. Sebanyak 62 situs, situs pemerintah daerah, 54 situs pendidikan, dan 19 situs penegakan hukum adalah situs yang paling banyak diserang. Banyaknya peretasan website, email phishing, dan trafik menunjukkan bahwa sistem keamanan siber Indonesia masih sangat lemah dalam menghadapi serangan siber yang dapat membahayakan pemerintahan dan jaminan sosial. Tabel di atas menunjukkan bahwa penulis menemukan beberapa penyebab sistem keamanan siber Indonesia yang lemah. Adanya juga Tren kejahatan yang masih terjadi antara lain:

- 1) *Data Breaches* : Data akan terus menjadi perhatian utama bagi organisasi di seluruh dunia. Data saat ini memiliki nilai jual, sehingga dapat menjadi target yang potensial.
- 2) *APT/State-Sponsored Cyber Warfare* : Serangan siber yang didukung badan pemerintah atau organisasi besar lain dengan tujuan untuk memperoleh akses tidak sah ke jaringan komputer target dan tetap tidak terdeteksi untuk jangka waktu yang lama.
- 3) *IoT with 5G Network : The New Era of Technology and Risks* : Teknologi baru yang masih perlu dilakukan penelitian untuk menutupi celah keamanan tersebut.
- 4) *Mobile is the New Target* : Perkembangan *mobile* yang signifikan menjadikannya target baru serangan.

- 5) *Rise of Automotive Hacking* : Teknologi otomotif menjadi target baru serangan siber.
- 6) *Targeted Ransomware* : Ransomware yang dapat melakukan penyanderaan terhadap data terdampak.
- 7) *Cloud is Also Potentially Vulnerable* : Cloud menjadi target serangan dengan semakin berkembangnya industri jaringan.
- 8) *Potential of Artificial Intelligence (AI)* : AI dapat digunakan untuk melakukan serangan siber.
- 9) *Insider Threats* : *Cyber security awareness* sangat dibutuhkan untuk menghindari serangan siber yang diakibatkan oleh *human error*.
- 10) *Automation and Integration* : Keamanan bagian otomatisasi dan integrasi menjadi perhatian pada saat pengembangan aplikasi web.

Pertama dan terpenting, undang-undang yang berlaku saat ini tidak cukup untuk mengawasi aktivitas yang terjadi di dunia maya. Hingga saat ini, Indonesia hanya memiliki dua undang-undang yang mengatur aktivitas siber: Undang-undang Nomor 1 dan Peraturan Pemerintah Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang telah diubah oleh Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik . Undang-undang tentang Perlindungan Data Pribadi Nomor 19 Tahun 2016 dan Nomor 27 Tahun 2022 Meskipun terdapat undang-undang turunan, kedua undang-undang tersebut jelas tidak cukup untuk mengatur lalu lintas jaringan di Indonesia. Tidak dapat diatur hanya dengan UU ITE dan UU PDP karena kejahatan dunia maya terus berkembang seiring dengan perkembangan internet. Indonesia membutuhkan undang-undang tambahan yang mengatur kejahatan internet.

Kedua, Indonesia memiliki infrastruktur teknologi informasi yang terbatas untuk mendukung keamanan siber. Infrastruktur teknologi yang memadai diperlukan untuk menghadapi tantangan yang muncul dari kemajuan informasi teknologi selama Revolusi Industri Keempat. Sayangnya, pemerintah saat ini lebih memprioritaskan pembangunan infrastruktur fisik daripada infrastruktur

TI (Sembiring, 2022). Hal ini terlihat dari fakta bahwa belum meratanya distribusi infrastruktur teknologi informasi antara kota dan daerah terpencil.

Ketiga, tingkat keterampilan digital masyarakat Indonesia masih terbilang sangat rendah. Laporan Keterampilan Digital terbaru tahun 2021 oleh Direktur Aplikasi Telematika (Ditjen Aptika) menunjukkan bahwa tingkat keterampilan digital masyarakat Indonesia adalah 3,49. Jumlah ini meningkat 3,46 dibandingkan tahun sebelumnya. Namun, jika dilihat lebih dekat, skor keamanan digital turun secara signifikan dari 3,24 menjadi 3,10. Tiga poin di atas menunjukkan bahwa tingkat keamanan digital di Indonesia masih sangat rendah.

Menurut penulis, terdapat cara untuk mengatasi permasalahan keamanan siber di Indonesia. Upaya itu harus dilakukan dengan partisipasi seluruh pemangku kepentingan digital, termasuk masyarakat, operator sistem energi, dan pemerintah. Dari sudut pandang masyarakat, kita sebagai pengguna internet perlu terus menyempurnakan bahasa digital kita. Hal ini dapat dicapai dengan menjadi lebih proaktif saat menggunakan Internet, memfilter informasi dengan memeriksa ulang sebelum membagikannya, dan melindungi kata sandi dan data sensitif lainnya. Untuk mencapai hal tersebut, operator sistem elektronik yang menyimpan data pengguna harus memperkuat sistem keamanan sibernya. Hal ini untuk menghindari situs web yang datanya dapat disusupi atau diretas pihak yang tidak bertanggung jawab. Saat ini, pemerintah sebagai regulator harus menjamin keamanan aktivitas di dunia online dengan mengeluarkan undang-undang yang mengatur aktivitas online secara ketat. Tujuannya adalah untuk menjamin integritas hukum dengan memastikan bahwa kejahatan yang dilakukan oleh seseorang di dunia siber dapat dihukum. Untuk memperkuat keamanan siber, semua pemangku kepentingan harus bekerja sama untuk memenuhi tanggung jawab mereka masing-masing. Dengan cara ini, dunia siber menjadi tempat yang aman bagi semua pihak.

V.2 KOMITMEN BERSAMA DALAM SHARE INFORMATION AND BEST

PRACTICE

Dalam rangka kerjasama yang dilakukan oleh Indonesia dan Australia melalui MoU yang telah disepakati bersama munculnya juga komitmen komitmen bersama dalam program Share Information, yakni :

V.2.1 Komitmen Bersama Dalam Share Information

1. BSSN sebaiknya segera membentuk forum (*Clearing House*) untuk berbagi informasi terkait ancaman siber.
2. Mekanisme Praktik berbagi informasi keamanan siber yang perlu diterapkan:
 - a) Rapat intensif (setiap enam bulan atau setiap tahun).
 - b) Portal/website didedikasikan untuk pertukaran informasi.
 - c) Adanya Pusat Pertukaran Informasi.
 - d) Menjadi titik kontak nasional untuk mengelola insiden keamanan (*Cyber Center*).

V.2.2 Komitmen Bersama Dalam Best Practice

1. Berkolaborasi dengan industri dan pakar untuk mengembangkan panduan teknis mengenai praktik terbaik dalam menangani insiden keamanan siber.
2. Pemberian pendidikan dalam bentuk workshop, seminar dan lain-lain.
3. Berkoordinasi dan berkomunikasi dengan pihak terkait, seperti CERT di negara lain, lembaga penegak hukum, atau pihak lain, untuk mengelola insiden keamanan siber.
4. BSSN wajib mendukung otoritas/sektor terkait dengan pelatihan tanggap insiden keamanan siber (*cyber workout*) yang dilaksanakan minimal setahun sekali.
5. Berbagai kegiatan seperti dialog siber, workshop penerapan hukum internasional di dunia siber, pelatihan penanganan insiden siber dan kecerdasan buatan, pelatihan penanganan kejahatan siber dan penyalahgunaan mata uang kripto, program beasiswa pendidikan untuk jenjang magister dan doktoral juga di Australia serta program pertukaran informasi dan Best Practices terkait

implementasi strategi keamanan siber nasional dan penerapan sebelas standar siber untuk perilaku pemerintah yang bertanggung jawab di dunia siber telah terbukti sangat bermanfaat dan patut ditingkatkan serta dilanjutkan dalam perjanjian kerja sama di masa depan.

V.3 IMPLEMENTASI PROGRAM SHARE INFORMATON

Berbagi informasi keamanan siber dapat diterapkan dalam suatu organisasi atau sekelompok organisasi, seperti Pusat Berbagi dan Analisis Informasi (ISAC), dalam konteks penerapan strategi pertahanan terhadap serangan siber. Penerapan berbagi informasi keamanan siber terbagi dalam berbagai bidang utama: Energi, Kesehatan, Transportasi, Keuangan, Transportasi, dan banyak lagi. Pertukaran informasi dapat dilakukan melalui pertemuan tatap muka melalui konferensi video atau konferensi. Anda juga dapat berkomunikasi dengan platform kolaboratif melalui jaringan intranet. Anda juga dapat menggunakan alamat email khusus anggota untuk berkomunikasi. Informasi yang dibagikan dapat mencakup ancaman siber, kerentanan siber, insiden siber, respons dan mitigasi siber, praktik terbaik, intelijen ancaman siber, dan informasi terkait siber lainnya. Informasi tersebut sebaiknya digunakan dalam klasifikasi informasi, salah satunya adalah dengan menggunakan protokol candlestick. Pembagian informasi keamanan siber memerlukan kerjasama antar aktor yang melibatkan model organisasi, manajemen kepercayaan, dan insentif. Manajemen berbagi informasi keamanan siber berfokus pada sumber daya manusia, manusia, proses, dan teknologi. Penelitian ini menggunakan referensi dari *Cybersecurity Framework* dan MITRE *Build a Information Sharing Ecosystem Type Based Use*. Menurut *Traffic Light Protocol* (TLP), ada empat klasifikasi informasi: merah (tersembunyi), kuning (dilindungi), hijau (dibatasi untuk masyarakat), putih (informasi publik atau publik)

V.4 IMPLEMENTASI PROGRAM BEST PRACTICE

Best practice merupakan salah satu program kerjasama yang di lakukan Indonesia dan Australia dalam pelatihan terbaik untuk meningkatkan keamanan

Indonesia, tidak hanya adanya pelatihan di dalam negeri saja tetapi di butuhkan nya juga pelatihan terbaik antar negara untuk menciptakan dan melahirkan kualitas ketahanan keamanan siber di negaranya, seperti adanya mengukur pelaksanaan kursus pelatihan bagi para profesional, khususnya kursus pelatihan dan pelatihan bagi para profesional di bidang Internet. BSSN diharapkan dapat mempertahankan dan meningkatkan program pelatihan keamanan siber dalam rangka meningkatkan keterampilan dan pengalaman profesional di bidang keamanan siber berdasarkan kemajuan ICT dan ancaman siber serta memenuhi kebutuhan organisasi dalam penerapan keamanan siber. Di Indonesia tujuan Indeks Pendidikan dan Kurikulum Nasional adalah untuk mengukur upaya pemerintah dalam mendukung pengembangan program pendidikan dan kurikulum pendidikan di dunia maya. Meski berstatus GCI merah, Indonesia sudah mulai mengembangkan program pelatihan dan kurikulum pendidikan di bidang keamanan siber di tingkat SMK dan perguruan tinggi.



Gambar 1.1 kerjasama Indonesia dengan Australia dalam keamanan siber

Pembahasan pada gambar di atas didasarkan pada Rencana Aksi Kemitraan Komprehensif Indonesia-Australia (2020-2024) yang ditandatangani oleh Menteri Luar Negeri kedua negara, dan merupakan upaya berkelanjutan kedua negara untuk meningkatkan hubungan bilateral dan saling pengertian mengenai isu keamanan siber. 10 Februari 2020 Para peserta menyampaikan keprihatinan mendalam mengenai peningkatan insiden keamanan siber dan dampaknya, termasuk aktivitas kejahatan siber yang dilakukan oleh pihak-pihak yang mencari keuntungan dari situasi pandemi COVID-19 saat ini. Peserta dari kedua negara sepakat mengenai perlunya kerja sama internasional untuk mencegah dan memerangi kejahatan dunia maya yang mengancam perdamaian dan keamanan internasional. Para peserta menekankan pentingnya mekanisme internasional dan regional, termasuk Kelompok Ahli Pemerintahan Perserikatan Bangsa-Bangsa (UN GGE) dan Kelompok Kerja Terbuka bilateral (OEWG), untuk membangun ruang Internet yang lebih baik. Australia dan India telah menyatakan komitmen mereka untuk mematuhi laporan UN GGE tahun 2010, 2013 dan 2015 dan untuk mendorong dunia maya yang damai dan stabil berdasarkan interpretasi mereka terhadap hukum internasional dan Pasal 11 Peraturan Pemerintah. Pernyataan ini menunjukkan komitmen berkelanjutan lembaga penegak hukum Indonesia dan Australia dalam memerangi kejahatan dunia maya.

Atas dasar Australia merupakan negara tetangga Indonesia, penghormatan atas kedaulatan nasional negara masing-masing, non intervensi atas urusan domestik dan saling menguntungkan serta kerja sama di bidang keamanan siber dengan Australia tetap berdasarkan pada politik luar negeri Indonesia, yaitu bebas aktif. Oleh karena itu, BSSN sangat terbuka dengan adanya kerja sama dengan negara lain sepanjang memenuhi prinsip 4 aman yaitu:

- a. Politis, tidak bertentangan dengan kebijakan nasional, khususnya politik luar negeri Indonesia,
- b. Yuridis, tidak bertentangan dengan ketentuan peraturan perundang-undangan,
- c. Teknis, tidak bertentangan dengan kebijakan teknis

Kementerian/Lembaga di Indonesia, dan

- d. Security, bukan merupakan suatu penyelundupan hukum.

Selain itu, kapabilitas Australia yang lebih unggul dibandingkan Indonesia serta kebutuhan Indonesia untuk memperkuat kapasitas dan kapabilitas keamanan siber nasional dengan belajar dari pemerintah Australia. Indonesia dan Australia berkeinginan untuk bersama-sama menjaga keamanan siber dalam rangka CBM kedua negara dengan membawa kepentingan nasional negara masing-masing untuk dapat menciptakan *mutual trust* diantara kedua negara.

Para peserta menekankan pentingnya penegakan hukum dalam negeri yang kuat dan kompeten, serta kemitraan internasional yang melibatkan pemerintah, organisasi internasional, serta organisasi bisnis dan industri digital.. Australia dan India juga berkomitmen untuk bekerja sama dalam sejumlah forum untuk membangun kepercayaan dan kapasitas, termasuk Seri Aksi Keamanan ICT Forum Regional ASEAN. Menurut penulis, diskusi dalam pertemuan ini akan menjadi kesempatan untuk meninjau Memorandum of Understanding (MoU) Indonesia-Australia on Cyber Cooperation tahun 2018, serta hasil positif dari diskusi dan pertukaran best practice yang terbaik. dan mendukung pengembangan teknologi. termasuk kolaborasi online. .Lihat Para peserta sepakat untuk terus bekerja sama memperkuat kekuatan keamanan siber nasional dan regional dan sepakat untuk memperpanjang MoU untuk dua tahun ke depan.



Gambar 1.2 Pelatihan Jaga Keamanan Siber Nasional ke Kementerian, TNI, dan Polri

Badan Keamanan Siber dan Sandi Negara (BSSN) memberikan pelatihan kepada 45 peserta yang berasal dari kementerian, organisasi, pemerintah daerah, TNI dan Polri mengenai optimalisasi keamanan siber untuk menjaga keamanan siber nasional. Melalui pelatihan ini, para peserta mampu mengelola dan memperkuat kolaborasi dan sinergi untuk mewujudkan implementasi keamanan siber dalam skala nasional. Pelatihan ini tidak hanya memberikan pengetahuan baru tetapi juga membentuk karakter peserta agar lebih siap menghadapi tantangan masa depan. Pelatihan berlangsung pada tanggal 9 Februari 2023. Peserta kegiatan memperoleh pengetahuan dan pemahaman mendalam tentang keamanan

Siibe. Beberapa materi yang diberikan antara lain Kali Linux untuk

Penetration Testing, Cybersecurity Awareness/Basics, Vulnerability Assessment Analyst, Basic Penetration Testing, dan Basic Web Application Security. melatih peserta untuk lebih mengembangkan pengetahuan dan

keterampilannya di bidang keamanan siber. dengan terus belajar, pelatihan ini berharap dapat membangun sistem keamanan siber yang andal dan dapat melindungi data penting dari ancaman siber.



Gambar 1.3 pelatihan generasi muda terhadap keamanan siber

Melalui Fresh Graduate Academy (FGA), salah satu program DTS, pelatihan keamanan siber Mastercard Academy 2.0 akan berkontribusi pada kumpulan keterampilan digital pemerintah pada tahun 2022 sebanyak 200.000 orang. Pelatihan ini bertujuan untuk memberikan informasi dan komunikasi kepada pekerja muda Indonesia, masyarakat dan pejabat pemerintah melalui pelatihan intensif dan sertifikasi internasional di bidang keterampilan dan kompetensi, produk, pengetahuan SDM di bidang teknologi dan keamanan siber.

Program pendidikan online diharapkan dapat memberikan kesempatan kepada peserta untuk memperoleh keterampilan internet dan berpartisipasi dalam penghargaan internasional di bidang keamanan siber. Peserta akan menerima pelatihan intensif selama enam minggu tentang sumber daya Linux+

dan Keamanan+, kemudian mengakses sertifikasi dan jalur karier untuk memperluas peluang karier mereka di bidang TI dan keamanan siber. program ini bertujuan untuk memperkuat dan menemukan kembali sektor digital untuk memenuhi kebutuhan sumber daya manusia yang akan memasuki dunia Industri 4.0 melalui aliansi tripartit antara pemerintah, industri dan universitas. Pelatihan yang ditawarkan adalah kesempatan untuk memperoleh sertifikasi internasional keamanan siber dan Comptia Linux dalam dua bulan.

Cyber Boot Camp

Cyber Boot Camp merupakan program dari DFAT yang dimana program ini merupakan bentuk kerjasama Australia dengan negara-negara mitra di seluruh Indo-Pasifik untuk meningkatkan keamanan siber. Didirikan pada tahun 2016, Cyber cooperation ini menjadi pemeran penting dalam mendukung pertumbuhan ekonomi global dan pembangunan berkelanjutan, melindungi keamanan nasional dan mendorong stabilitas internasional. Penyelenggaraan Cyberboot Camp, CSIRO Data 4 Development (D4D) Fellowship Program for Indonesia Civil Servants, webinar terkait isu keamanan siber dan pelatihan SANS Institute yaitu bidang:

- a) *Practical Open-Source Intelligence;*
- b) *Hacker Tools, Techniques and Incident Handling;*
- c) *Web App Penetration Testing and Ethical Hacking;*
- d) *Implementing and Auditing Security and Frameworks and Controls.*

ASPI (Australian Strategic Policy Institute) cyber policy workshop

ASPI bertujuan untuk menyelenggarakan workshop bagi negara-negara mitra di bidang keamanan siber dan Australia mengenai perilaku pemerintah dalam keamanan siber. ASPI juga akan bekerja sama dengan BSSN untuk meningkatkan analisis ancaman siber, keterlibatan dalam isu kebijakan siber, dan koordinasi antarlembaga. Melalui program ini kebijakan siber ASPI, Indonesia yang masih membutuhkan langkah-langkah manajemen risiko yang memadai di bidang keamanan siber, sebaiknya memperkuat analisisnya

terhadap ancaman siber yang masih terjadi di Indonesia. Manajemen risiko adalah bagian penting dari strategi. Dengan manajemen risiko dan menghitung anggaran yang dibutuhkan.

Cyber Business Connection: Austrade mendorong keamanan siber dalam ekonomi digital.

Kunjungan perusahaan keamanan siber Australia ke Indonesia yang diselenggarakan oleh Austrade menunjukkan beberapa solusi yang dapat dilakukan bagi perusahaan di ekonomi digital. Grup ini mencakup perusahaan dan sistem perlindungan data, enkripsi dan pengujian. Kunjungan tersebut, yang diselenggarakan bersama oleh perusahaan bisnis

AustCyber dan Austrade, mempertemukan para pemimpin dan bisnis dari Australia dan India pada tanggal 8 Januari 2019. Selain rencana untuk mengembangkan sektor ekonomi digital, seperti seiring berkembangnya penggunaan sertifikat digital untuk perdagangan impor dan ekspor, melalui kegiatan jaringan bisnis online tersebut, Indonesia yang dianggap oleh Australia sebagai negara dengan potensi ekonomi digital terbesar bersiap menghadapi digital. usia dan ancamannya.

Dialog ketiga tentang kebijakan siber (Third Cyber Policy Dialogue)

Dialog Kebijakan Siber yang ketiga baru saja dilaksanakan pada tanggal 2 September 2020. Acara tersebut dipandu oleh Hinsa Hasibuan, CEO BSSN, dan delegasi Australia dipimpin oleh Duta Besar Bidang Siber, Dr. Dipimpin oleh Dr. Tobias Bikini. Dialog Kebijakan Siber merupakan acara tahunan menyusul perjanjian bilateral antara Presiden Republik Indonesia dan Perdana Menteri Australia pada tahun 2017. Dialog kebijakan siber bertujuan untuk memperkuat kerja sama di bidang keamanan siber dan kerja sama kedua negara dalam pertukaran informasi, praktik terbaik siber, energi untuk pembangunan, peningkatan ekonomi digital, dan pemberantasan kejahatan siber.

Analisis kerjasama BSSN dan DFAT dalam pengembangan keamanan siber

Eratnya hubungan dan kerjasama bilateral antara Indonesia dan Australia di dasarkan pada Partnership Agreement Kerja sama bilateral dapat terjadi setelah kedua negara menandatangani persetujuan (agreement) yang dijadikan sebagai acuan, yang dimana kerjasama ini didasarkan pada Memorandum of Understanding (MOU) pada kunjungan resmi Perdana Menteri Australia ke Istana Bogor pada Jumat 31 Agustus 2018, yang didukung oleh sifat komplementaritas sumber daya dan keunggulan yang dimiliki masing-masing negara, di samping proses kemajuan keamanan siber di kedua negara yang sangat baik hingga membuka peluang kerjasama di dalam sektor keamanan siber semakin terbuka lebar. Selain itu, kedua negara juga secara aktif saling mendukung di berbagai forum baik regional maupun internasional seperti pelatihan pelatihan, adanya forum pertemuan, di bentuk nya berbagai kegiatan untuk pelatihan dan berbagi informasi, dan lain sebagainya. Letak geografis antara Indonesia dan Australia yang dekat juga menjadikan salah satu faktor pendorong mempermudah kerjasama bilateral ini. Kerjasama ini juga tercipta karena kedua negara saling memahami untuk meningkatkan kemajuan konektivitas dan sistem informasi, terkait dengan meningkatnya kemarahan dan kekerasan serta kebencian terhadap keamanan nasional. Oleh karena itu, kedua negara berharap dapat mendorong penggunaan Internet secara terbuka, bebas dan aman, untuk mendorong pertumbuhan ekonomi dan melindungi keamanan nasional dan stabilitas global. Kerjasama kedua negara mencakup kerjasama di bidang keamanan siber yang tidak hanya bertujuan untuk meningkatkan kemampuan Internet, namun juga meningkatkan posisi Indonesia dalam indeks keamanan siber global (ITU) International Telecommunication Union. Sebuah survei yang dilakukan oleh ITU untuk menilai komitmen negara-negara anggota terhadap keamanan siber. Tujuan GCI adalah membantu negara-negara mengembangkan praktik keamanan siber mereka di seluruh dunia dengan membantu negara-negara mengidentifikasi area yang perlu ditingkatkan di Internet. Penulis berharap melalui MoU ini dapat terjalin kerja sama antara

Indonesia dan Australia di bidang keamanan siber untuk menciptakan keamanan nasional dan regional khususnya di Indonesia dan Australia.

Dari data diatas penulis melihat bahwa dengan adanya pelatihan terbaik dalam negara maupun antar negara yang di lakukan Indonesia untuk meningkatkan keamanan siber nya terbukti berhasil melahirkan dan meningkatkan kualitas Sumber Daya Manusia dalam keamanan siber Indonesia itu sendiri dengan adanya pertemuan dialog yang saling memberikan pemahaman terhadap isu-isu keamanan siber antara Indonesia dengan Australia, lalu adanya pelatihan keamanan dalam militer yang dapat memperluas wilayah lingkup keamanan siber di Indonesia itu sendiri dan dengan adanya seminar untuk lulusan baru yang dimana dengan adanya seminar dan pelatihan pelatihan untuk lulusan baru dapat juga memperbaharui kondisi lingkup keamanan siber yang lebih baru dengan kualitas terbaru dan dengan pelatihan terbaik juga, yang dimana analisa terhadap pelatihan terbaik dan berbagi informasi ini telat memberikan keuntungan bagi kedua negara dilihat dari hasil wawancara yang di lakukan penulis dengan bapak sigit selaku direktur BSSN yang mengatakan bahwa Australia dapat terus memfasilitasi program peningkatan kapasitas SDM di bidang keamanan siber tidak hanya bagi BSSN, namun

Kementerian/Lembaga terkait lain, bahkan akademisi, komunitas dan masyarakat. Sedangkan BSSN dapat berbagi pandangan kebijakan keamanan siber nasional dan informasi perkembangan lanskap keamanan siber Indonesia.

VI. PENUTUP

VI.1 KESIMPULAN

Penulis menyimpulkan bahwa kerja sama yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN) dan Department of Foreign Affairs and Trade (DFAT) melalui program Share Information and Best practice yang didasarkan pada MoU merupakan salah satu program kerjasama yang dilaksanakan Indonesia dan Australia dalam bidang keamanan siber. Terkait implementasi strategi peningkatan keamanan siber melalui berbagai komitmen dan kegiatan yang disepakati bersama seperti Pertukaran informasi melalui pertemuan tatap muka, pertemuan melalui platform kolaboratif, adanya pelatihan dan kurikulum pendidikan di bidang keamanan siber di tingkat SMK dan perguruan tinggi, pelatihan kepada 45 peserta yang berasal dari kementerian, organisasi, pemerintah daerah, TNI dan Polri, serta pelatihan Fresh Graduate Academy (FGA) pelatihan keamanan siber Mastercard Academy 2.0 telah terbukti efektif serta hasil kerjasama yang dilakukan oleh BSSN dan DFAT pun menjadi salah satu faktor yang mendorong peningkatan keamanan siber di Indonesia.

Melalui kerjasama yang terjalin diantara Indonesia dan Australia ini tentunya berhasil meningkatkan komitmen Indonesia terhadap cyber security karena hal ini sejalan dengan poin ke-5 dari ITU yakni cooperation, meningkatnya keterampilan serta kesadaran Indonesia dalam hal cyber security, menjadi salah satu faktor terhadap kenaikan posisi Indonesia dalam peringkat keamanan siber.

Adanya faktor faktor yang mendorong kerjasama antara Indonesia dan Australia yakni: sumber daya soft power Australia, Kredibilitas politik Australia, keuntungan dari Indonesia dan Australia sebagai negara demokratis, dan kelangsungan hidup politik dari masing-masing pemimpin. Dengan demikian, keempat faktor ini faktor ini menyebabkan kedua negara mempertahankan hubungan baik mereka hubungan baik mereka melalui kerja sama keamanan siber.

VI.2. SARAN

Penulis melihat bahwa fenomena yang muncul terhadap keamanan siber Indonesia perlu meningkatkan kemampuan dan stabilitas teknologinya dalam konteks pembangunan dan pembangunan regional. Indonesia juga perlu memetakan sektor-sektor utama infrastrukturnya yang rentan terhadap ancaman siber. Indonesia tidak hanya perlu meningkatkan keamanan siber di tingkat militer untuk menjadikan wilayah Indonesia lebih aman dari ancaman siber, namun juga perlu meningkatkan kesadaran masyarakat terhadap ancaman siber. Indonesia perlu mengembangkan dokumen yang lebih komprehensif dan praktis untuk mengatasi ancaman siber. Upaya Indonesia dalam meningkatkan keamanan siber dilakukan melalui kerja sama dengan mitra dialog Indonesia, termasuk Australia, yang merupakan negara dengan kapabilitas dan kemampuan siber yang lebih besar. Dengan ditandatanganinya Nota Kesepahaman antara Indonesia dan Australia, penulis berharap kerjasama kedua negara melalui MoU ini dapat memberikan kontribusi bagi masa depan keamanan siber di Indonesia dan Australia dalam jangka panjang

DAFTAR PUSTAKA

- Australian Govt. (2020). *Fraud Control* | Australian Government Department Of Foreign Affairs And Trade. Website.
<https://www.dfat.gov.au/about-us/corporate/fraud-control>
- Badan Siber dan Sandi Negara, Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019, 6-8.
- Barrinha, A., & Renard, T. (2017). Cyber-Diplomacy: The Making Of An International Society In The Digital Age. *Global Affairs*, 3(4–5), 353–364.
<https://doi.org/> <https://doi.org/10.1080/23340460.2017.1414924>
- Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). Cyber Security Policy Guidebook. In *Cyber Security Policy Guidebook*. John Wiley And Sons, Inc.
<https://doi.org/10.1002/9781118241530>
- Biro Hukum Dan Humas BSSN. (2019). *BSSN Selenggarakan Community Building And Information Sharing Sektor Ekonomi Digital*. <https://bssn.go.id/bssn-selenggarakan-community-building-and-information-sharing-sektor-ekonomi-digital/>
- BSSN. (2019). *ASEAN-JAPAN Online Cyber Exercise*.
<https://bssn.go.id/asean-japan-online-cyber-exercise/>
- Cakrawala. (2021). *Apa Itu Cyber Security? Mengapa Cyber Security Kini Makin Penting?* Infokomputer.Grid.Id.
<https://infokomputer.grid.id/read/122710604/apa-itu-cyber-security-mengapa-cyber-security-kini-makin-penting?page=all>

CALDER, A. (2020). *Cyber Security: Essential Principles To Secure Your Organisation*. In *Cyber Security: Essential Principles To Secure Your Organisation*. IT Governance Publishing Ltd. <https://doi.org/10.2307/J.Ctv10crebg>

D, Margisa. (2020). Kerja Sama Badan Siber Dan Sandi Negara (Bssn) Indonesia Dengan Department Of Foreign Affairs And Trade (DFAT). *Jurnal FISIP*, 2– 4.

FIRST. "TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 1.0." <https://www.first.org/tlp/> (diakses 25 Desember 2023)

Gautama, H. (2014). *Penerapan Cyber Security*.
Kemhub RI.
[Http://kemhubri.dephub.go.id/pusdatin/%0Afiles/Materi/Penerapan_Cyber security.Pdf](http://kemhubri.dephub.go.id/pusdatin/%0Afiles/Materi/Penerapan_Cyber_security.Pdf)

Hamali, A. Y. (2016). *Pemahaman Manajemen Sumberdaya Manusia*. Center For Academic Publishing Servive.

Handrini, A. (2014). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Politica*, 5(1).

Hidayat Chusnul Chotimah. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. *Jurnal Politica* Vol.10 No. 2. Dapat diakses melalui <https://doi.org/10.22212/jp.v10i1.1447>

Hootsuite. (2021). *Digital Global Overview Report 2021*.
<https://techsauce.co/tech-and-biz/digital-2021-overview-report>

Iskandar, Z. A. (2020). CYBER DIPLOMACY: MENUJU MASYARAKAT INTERNASIONAL YANG DAMAI DI ERA DIGITAL. *Padjadjaran Journal Of International Relations*, 317–320.

- Kompas.Com. (2019). *RI Rugi Rp 478,8 Triliun Akibat Serangan Siber, DPR Siapkan RUU KKS Halaman All - Kompas.Com.*
<https://Nasional.Kompas.Com/Read/2019/08/12/13454311/Ri-Rugi-Rp-4788-Triliun-Akibat-Serangan-Siber-Dpr-Siapkan-Ruu-Kks?Page=All>
- Kurniawan, F. (2020). *Kerugian Serangan Siber Tahun 2021 Diprediksi RP 84.000 Triliun.*
<https://Tekno.Sindonews.Com/Read/284040/207/KerugianSerangan-Siber-Tahun-2021-Diprediksi-Rp84000-Triliun1609240357>
- L. Ulinuha, *Evaluasi Pengelolaan Keamanan Jaringan di ITS Dengan Menggunakan Standar Indeks Keamanan Informasi (KAMI) Kemenkominfo RI, Surabaya: Sistem Informasi ITS, 2013*
- Maulia Jayantina Islami, “Tantangan Dalam Implementasi Strategi Keamanan Siber nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index”
Jurnal Masyarakat Telematika dan Informasi Volume: 8 No. 2 (Oktober – Desember 2017) Hal. 139
- Nicholas Westcott. (July 2008). *Digital Diplomacy: The Impact of the Internet on International Relations*. Research Report 16, hlm 14.
- North, D. C. (1990). *Institutions, Institutional Change And Economic Performance*.
Cambridge University Press.
- Penjelasan Sekretaris Jenderal Kementerian Pertahanan Marsdya TNI Eris Herryanto Pada Seminar Nasional Keamanan Infrastruktur Internet Yang Diselenggarakan Indonesia Security Incident Response Team On Internet Infrastruktur (ID-SIRTI) Di Universitas Pertah. (2011).*
- Pusat Operasi Keamanan Siber Nasional. (2021). *Laporan Tahunan Hasil Monitoring Keamanan Siber 2020.*
- Pusiknas Polri. (2022). *Kejahatan Siber Di Indonesia Naik Berkali-Kali Lipat.*

https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

Richiyanti, S. (2020). Pengaruh Dan Penanganan Cybercrime Dalam Perkembangan Teknologi Informasi. *KODIFIKASI*, 2(2), 46–56.

Rosidah, A. T. S. (2009). *Manajemen Sumber Daya Manusia*. Graha Ilmu.

Saefullah, N. T. S. (2002). Yurisdiksi Sebagai Upaya Penegakan Hukum Dalam Kegiatan Cyberspace. In *In Cyber Law: Suatu Pengantar*.). Pusat Studi Cyber Law UNPAD.

Saudi, A. (2016). *KEJAHATAN SIBER TRANSNASIONAL DAN STRATEGI PERTAHANAN SIBER INDONESIA*. Universitas Riaria.

S. Ghernaouti-Hélie, *Cybersecurity Guide for Developing Countries*, (Geneva: International Telecommunication Union, 2009) Hal. 18.

Simamora, H. (2004). *Manajemen Sumber Daya Manusia*. YKPN Jakarta.

Sujadmiko, Bayu. (2014). PENYADAPAN LINTAS NEGARA KEDAULATAN DITINJAU DARI HUKUM INTERNASIONAL. https://www.researchgate.net/publication/305462455_PENYADAPAN_LINTAS_NEGARAKEDAULATAN_DITINJAU_DARI_HUKUM_INTERNASIONAL/citation/download

Sunyoto, D. (2015). *Penelitian Sumber Daya Manusia*. Buku Seru.

T. D. K. Informasi, "*Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik*," Jakarta, Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika, 2012, pp. 34 – 58

Yudha, Chandra. 2018. Penguatan kerjasama cybersecurity:keniscayaan untuk ASEAN. *Majalah masyarakat ASEAN.kemenlu*

DAFTAR LAMPIRAN

Lampiran persetujuan sidang proposal

LEMBAR PERSETUJUAN SIDANG PROPOSAL / SUP


Skripsi diajukan oleh:
 Nama : Aminda Rch. Margareth Balara
 NIM : 1910412055
 Program Studi : Hubungan Internasional
 Judul Skripsi : Kerjasama Badan Siber dan Sandi Negara (BSSN) Dan Australia
 Dalam Meningkatkan Keamanan Siber Indonesia Melalui Program Share
 Information and Best Practice Tahun 2021-2022

Telah berhasil melakukan bimbingan minimal 4X dihadapan dosen pembimbing diterima sebagai bagian persyaratan untuk melakukan sidang **proposal atau seminar usulan penelitian** yang diperlukan untuk memperoleh gelar Sarjana, pada Program Studi Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Pembangunan Nasional "Veteran" Jakarta.

Pembimbing I


 (Dr. Mansur, M.Si.)

Pembimbing II


 (Dzikrul Wafiq)

Ditetapkan di : Jakarta

Lampiran tanda tangan pernyataan A1



A1.1

SURAT PERNYATAAN

Yang bertandatangan dibawah ini

NAMA : Amanda Rich Margareth Bakara
PEMBIMBING I : Dr. Mansur, M.Si.
PEMBIMBING II : Daifatul Maarif, S.Pd., MA.

Menyatakan bahwa bersedia / (tidak bersedia *) menjadi pembimbing Skripsi, mahasiswa :

NAM A : Amanda Rich Margareth Bakara
NIM : 1910912055
PROGRAM STUDI : Hubungan Internasional
KONSENTRASI : Keamanan dan Kerjasama dibidang Cyber Crime
JUDUL SKRIPSI : Kerjasama Badan Siber dan Sandi Negara (BSSN) dan
Asuransi Dalam Meningkatkan Keamanan Siber Indonesia Melalui
Program Secure Information and Best Practice Tahun 2019-2022

Demikian Surat Pernyataan ini saya buat, agar dapat dipergunakan sebagaimana mestinya.

Jakarta, 22 Februari 2023.

Pembimbing I,

Dr. Mansur, M.Si.

Jakarta, 27 February 2023.

Pembimbing II,

DAIFATUL MAARIF

Lampiran tanda tangan A2

Kontrak Penulisan Skripsi

Saya yang bertanda tangan dibawah ini menyatakan dengan sungguh-sungguh akan melaksanakan proses pembimbingan skripsi secara tertib, terfokus dan menyelesaikan penulisan skripsi selambat-lambatnya enam bulan, terhitung sejak penandatanganan kontrak ini

Jakarta, Rabu 7 Desember 2022


Pembimbing Utama: [Signature]
(Dr. Marni M.Si)

Yang Menyatakan: [Signature]
(Amanda Ruch Maryam Ralawa)

Ketua Program Studi: [Signature]
(Dr. Widiarta Satrio M.Si)

Hakikat Penulisan Skripsi

1. Penulisan Skripsi pada hakikatnya adalah kegiatan ilmiah untuk melatih mahasiswa berpikir tertib, logis dan metodis
2. Penulisan Skripsi pada hakikatnya adalah kewajiban akademis yang penyelesaiannya menjadi tanggung jawab penuh mahasiswa
3. Jalin Komunikasi pembimbingan yang intensif dengan pembimbing anda untuk kecepatan dan ketepatan penulisan skripsi
4. Skripsi merupakan karya ilmiah hasil penelitian mandiri yang terbebas dari tindakan plagiat
5. Segala bentuk plagiarisme dalam penulisan skripsi merupakan pelanggaran akademik dan akan dikenai sanksi sesuai aturan yang berlaku


KARTU BIMBINGAN SKRIPSI

JADWAL BIMBINGAN	Pemb. Utama	Har / Pukul
	Pemb. Pendamping	Har / Pukul
Nama	Amanda Ruch Maryam Ralawa	
NIM	1910917995	
Program Studi	Hubungan Internasional / S1	
Konsentrasi	Hubungan Internasional	
Telepon / HP	08215621671	
Pembimbing Utama	Dr. Marni M.Si	
Pembimbing Pendamping		
Judul	: Ketersediaan beasiswa S1 dan S2 di negara asing dan Pergerakan pada Trade (KCA) dalam meningkatkan kemampuan S1 dan S2 melalui program Keahlian S1 dan S2 pada tahun 2022-2023	

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

Lampiran tanda tangan perbaikan proposal

LEMBAR PERBAIKAN
HASIL SIDANG PROPOSAL
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

Nama : Amanda Ruch Maryam Ralawa
NIM : 1910917995
Judul : Ketersediaan beasiswa S1 dan S2 di negara (ISS) dan Pergerakan of Pergerakan pada Trade (KCA) dalam meningkatkan kemampuan S1 dan S2 melalui Program Short Information and Best Practice Indonesia Melalui Program Short Information and Best Practice
Tanggal Ujian :
Penguji 2 : Dr. Marni M.Si


No.	Catatan Perbaikan	Status Perbaikan	Tanda Tangan dan Tanggal Pengajuan Revisi
1.	Perbaikan Penulisan latar belakang	Sudah diperbaiki	<u>[Signature]</u>
2.	Perbaikan Penulisan literatur review dan kerangka pemikiran	Sudah diperbaiki	<u>[Signature]</u>
3.	Perbaikan Penulisan narasi dan navigasi page	Sudah diperbaiki	<u>[Signature]</u>
4.			

LEMBAR PERBAIKAN
HASIL SIDANG PROPOSAL
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

Nama : Amanda Ruch Maryam Ralawa
NIM : 1910917995
Judul :
Tanggal Ujian :
Penguji 1 : Dr. Marni M.Si

No.	Catatan Perbaikan	Status Perbaikan	Tanda Tangan dan Tanggal Pengajuan Revisi
1.	Bab I = Perbaikan Permisian dan data sesuai uraian tahun	acc	<u>[Signature]</u>
2.	Bab II = Perbaikan teori dan Gambar uraian	acc	<u>[Signature]</u>
3.	Bab III = Perbaikan isi dan Bab IV Konsep Perencanaan	acc	<u>[Signature]</u>
4.			

Lampiran surat riset dan hasil wawancara



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
Jalan Rumah Sakit Fatmawati, Pondok Labu, Jakarta Selatan 12450
Telepon 021 - 7656971, Fax. 021 - 7656904
Laman : www.uprvj.ac.id, e-mail uprvj@uprvj.ac.id

Nomor : 719 /UN61/RS/FISIP/2023
Hal : Permohonan Riset

18 Agustus 2023

Yth. Bapak Irjen. Pol. Dono Indarto, S.I.K., M.H.
Badan Siber dan Sandi Negara (BSSN)
Jl. Harsono RM No.70, RT.2/RW.4, Ragunan, Ps. Minggu, Kota Jakarta Selatan,
Daerah Khusus Ibukota Jakarta 12550


Berkaitan dengan program pemerintah di bidang Pendidikan dalam mewujudkan keterkaitan dan kesepadanan (*link and match*) antara pendidikan dengan dunia usaha, maka Fakultas Ilmu Sosial dan Ilmu Politik (FISIP) UPN "Veteran" Jakarta mewajibkan mahasiswa yang akan menyelesaikan studinya mengikuti Riset di instansi pemerintah maupun swasta.

Oleh karena itu kami mengajukan untuk dapat kiranya mahasiswa/i kami melaksanakan Riset di Badan Siber dan Sandi Negara (BSSN) yang Bapak/Ibu pimpin.

Adapun mahasiswa/i yang kami maksud adalah:

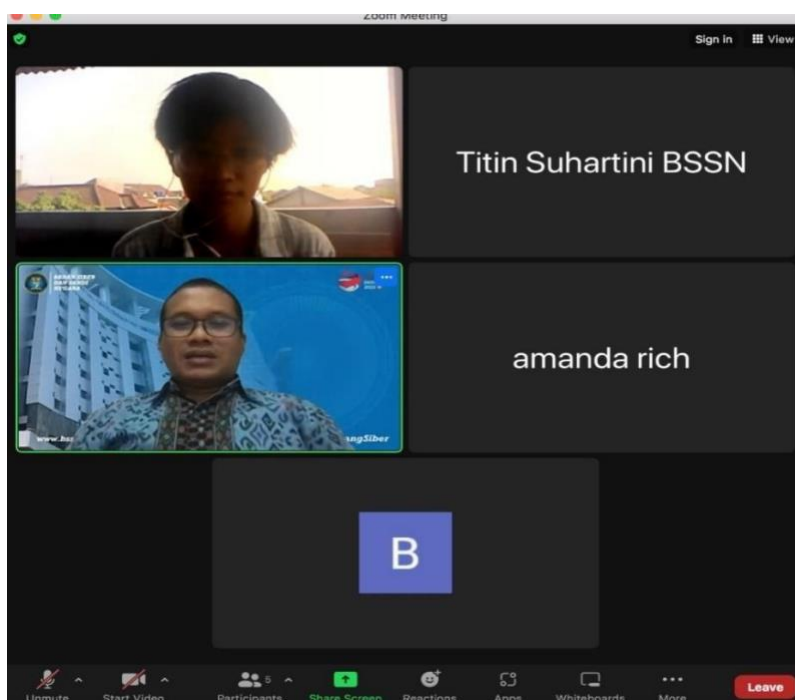
Nama : Amanda Rich Margareth Bakara
N I M : 1910412055
Program Studi : S1 Hubungan Internasional
Alamat : PTI Khusus Blok J5 Nomor 1, Bekasi Timur Cipete Raya, 17510
Telepon / Hp : 085173021621
Judul : Kerja Sama Badan Siber dan Sandi Negara (BSSN) dan Departemen Of Foreign Affairs And Trade (DFAT) Dalam Meningkatkan Keamanan Siber Indonesia Melalui Program Share Information And Best Practice Tahun (2019-2022)

Demikian permohonan ini Kami sampaikan atas perhatian dan kerjasama yang baik diucapkan terima kasih.



a.n. DEKAN
Wakil Dekan Bidang Akademik
Fitria Wuningtyas
NIK. 216121191

Tembusan:
- Dekan



Hasil wawancara

Narasumber: Direktur Strategi Keamanan Siber dan Sandi, BSSN

Angle Wawancara

Pada topik wawancara ini, narasumber diharapkan dapat membahas mengenai:

- kondisi ancaman siber sebelum, selama, dan sesudah pandemi dalam lingkup nasional dan internasional
- pentingnya kerjasama indonesia-australia dalam meningkatkan keamanan siber di indonesia
- kondisi BSSN dan DFAT selaku pemeran dalam kerjasama ini - penerapan best practice and share information:
 - a) apa saja kegiatan yang telah di lakukan, yang sedang di lakukan, dan yang akan di lakukan
 - b) bagaimana cara penerapan yang di lakukan dan yang berperan dalam penerapannya
 - c) dampak dan manfaat yang di dapat dari penerapan yang dilakukan

daftar pertanyaan:

1. Apa yang dilakukan oleh Indonesia dalam meningkatkan keamanan siber dalam periode 2018 sebelum pandemik dan juga saat periode pandemik tahun 2019?

Tanggapan :

- Sebelum pandemik COVID19, BSSN telah berupaya melakukan literasi dan edukasi keamanan siber kepada Kementerian/Lembaga dengan berbagai bentuk program kegiatan peningkatan kesadaran keamanan siber pada berbagai sektor, pembentukan regulasi di bidang keamanan siber, penguatan teknologi keamanan siber dan berbagai program kegiatan lainnya.
- Paska pandemik COVID19, BSSN lebih meningkatkan berbagai jenis program kegiatan peningkatan kesadaran keamanan siber yang lebih luas

hingga masyarakat/publik dalam rangka mendorong terciptanya ruang siber yang aman dan bertanggungjawab.

2. Bentuk kerjasama apa saja yang di lakukan oleh Indonesia dan Australia dalam meningkatkan keamanan siber dan mengurangi ancaman siber di kedua negara tersebut?

Tanggapan:

- Berbagi Informasi dan Praktik Terbaik, berupa sharing session dengan E- Safety Commissioner.
- Pembangunan Kapasitas dan Mempererat Hubungan melalui berbagai pelatihan, simposium, dan kegiatan peningkatan kapasitas lainnya.
- Ekonomi Digital, berupa pelibatan pada berbagai forum seperti Australia- Indonesia Digital Forum di Jakarta dan Australia Embassy Jakarta Digital Month.
- Kejahatan Siber berupa peningkatan kapasitas SDM Keamanan Siber termasuk investigasi dan digital forensik.

3. Bentuk kerjasama apa yang dilakukan BSSN dan DFAT dalam kerjasamanya sebagai badan perwakilan dalam keamanan siber?

Tanggapan D11:

- Melaksanakan pertemuan bilateral antara BSSN dengan DFAT dan Kedutaan Besar Australia di Jakarta serta Ambassador Australia untuk Urusan Siber dan Teknologi Kritis yang membahas isu keamanan siber.
- Berbagi praktik terbaik dalam penyusunan Strategi Keamanan Siber Nasional antar negara.
- Penyelenggaraan berbagai bentuk peningkatan kapasitas SDM Keamanan Siber seperti Australia Cyber Bootcamp dan SANS Training.

4. Dengan adanya kerjasama yang telah dilakukan BSSN dan DFAT dalam keamanan siber apakah ada perubahan terhadap tingkat keamanan siber di kedua Negara tersebut?

Tanggapan:

Ada, berdasarkan hasil GCI tahun 2018 dan 2020 yaitu Indonesia semula berada pada peringkat 41 menjadi 24. Sedangkan Australia semula peringkat 10 menjadi 12.

5. Mengapa indonesia memilih bekerjasama dengan negara australia dalam meningkatkan keamanan siber?

Tanggapan:

Pertimbangan GCI yang berada diatas peringkat yang diperoleh Indonesia, Australia memiliki strategi keamanan siber nasional yang dinamis dan menjadi salah satu rujukan bagi Indonesia dalam menyusun Strategi Keamanan Siber Nasional. Saling mendukung di Kawasan dan Australia merupakan negara tetangga Indonesia.

6. Pendapat dan tanggapan terhadap kerjasama yang di lakukan indonesia (BSSN) dan australia (DFAT) melalui best practice and share information?

Tanggapan:

Dengan adanya salah satu area kerja sama yaitu Berbagi Informasi dan Praktik Terbaik menunjukkan bahwa BSSN dan DFAT memiliki fokus yang sama untuk dapat saling berbagi informasi dan praktik terbaik dalam berbagai isu yang terkait dengan keamanan siber. Dalam mempertimbangkan kerja sama bilateral yang memegang salah satu prinsip *mutual beneficial*, diharapkan area kerja sama ini menghasilkan keuntungan bagi kedua belah pihak dalam peningkatan kapasitas keamanan siber nasional masing-masing negara.

7. Dalam MoU, program best practice and share information merupakan salah satu pilar dari kerjasama, lalu bagaimana kualitas dari pemeran keamanan siber sebelum adanya program ini?

Tanggapan:

Sebelum adanya area kerja sama ini tentunya kami hanya dapat memperoleh informasi dari sumber terbuka dan memiliki keterbatasan informasi, lain halnya jika telah memiliki kerja sama memiliki keuntungan dapat saling bertukar informasi dengan lebih mudah dan cepat ketika dibutuhkan.

8. Dalam isu keamanan siber, terutama mengenai ancaman siber yang terjadi, apa yang bisa Australia bagikan dengan Indonesia? dan juga Indonesia untuk Australia?

Tanggapan:

Australia dapat terus memfasilitasi program peningkatan kapasitas SDM di bidang keamanan siber tidak hanya bagi BSSN, namun Kementerian/Lembaga terkait lain, bahkan akademisi, komunitas dan masyarakat. Sedangkan BSSN dapat berbagi pandangan kebijakan keamanan siber nasional dan informasi perkembangan lanskap keamanan siber Indonesia.

9. Bagaimana Anda melihat Keamanan Siber sebagai karier di tahun-tahun mendatang?

Tanggapan:

Berdasarkan Roadmap Pembinaan SDM Keamanan Siber dan Sandi 2020- 2024, peluang karir di bidang keamanan siber dengan daya saing terbesar pada SDM dengan fokus keamanan jaringan. Sebagai informasi bahwa telah ada publikasi Peta Okupasi Nasional Fungsi Keamanan Siber untuk dapat menjadi rujukan dalam pengembangan standar kompetensi, penyelenggaraan aktivitas sertifikasi kompetensi berbasis skema okupasi, pengembangan kurikulum pendidikan, pemetaan profil kebutuhan dan ketersediaan serta pembuatan berbagai modul berbasis kompetensi. BSSN

dengan Kementerian/Lembaga terkait telah menghasilkan beberapa standar kompetensi kerja nasional Indonesia (SKKNI) bidang keamanan siber dan telah

terbentuk lembaga sertifikasi profesi (LSP) BSSN untuk menjawab berbagai peluang karir SDM di bidang keamanan siber di tahun-tahun mendatang. Digitalisasi dapat berjalan dengan baik dengan adanya keamanan didalamnya.

10. Tren keamanan siber manakah yang akan memiliki dampak terbesar dalam lima tahun ke depan?

Tanggapan:

Ancaman siber yang masih menjadi tren antara lain:

- 11) *Data Breaches* : Data akan terus menjadi perhatian utama bagi organisasi di seluruh dunia. Data saat ini memiliki nilai jual, sehingga dapat menjadi target yang potensial.
- 12) *APT/State-Sponsored Cyber Warfare* : Serangan didukung badan pemerintah atau organisasi besar lain dengan tujuan untuk memperoleh akses tidak sah ke jaringan komputer target dan tetap tidak terdeteksi untuk jangka waktu yang lama.
- 13) *IoT with 5G Network : The New Era of Technology and Risks* : Teknologi baru yang masih perlu dilakukan penelitian untuk menutupi celah keamanan tersebut.
- 14) *Mobile is the New Target* : Perkembangan *mobile* yang signifikan menjadikannya target baru serangan.
- 15) *Rise of Automotive Hacking* : Teknologi otomotif menjadi target baru serangan siber.
- 16) *Targeted Ransomware* : Ransomware yang dapat melakukan penyanderaan terhadap data berdampak.
- 17) *Cloud is Also Potentially Vulnerable* : Cloud menjadi target serangan dengan semakin berkembangnya industri jaringan.

- 18) *Potential of Artificial Intelligence (AI)* : AI dapat digunakan untuk melakukan serangan siber.

19) *Insider Threats* : *Cyber security awareness* sangat dibutuhkan untuk menghindari serangan siber yang diakibatkan oleh *human error*.

20) *Automation and Integration* : Keamanan bagian otomatisasi dan integrasi menjadi perhatian pada saat pengembangan aplikasi web.

11. Menurut anda seberapa penting peran badan badan seperti BSSN dan badan siber lainnya dalam ruang lingkup keamanan siber?

Tanggapan :

Bagaimana perkembangan kajian teori Sangat penting karena BSSN tidak dapat bekerja sendiri dalam menjaga ruang siber yang aman sehingga membutuhkan sinergitas dengan para pemangku kepentingan untuk bersama-sama membangun dan meningkatkan kapasitas dan kapabilitas dalam rangka penguatan keamanan siber nasional agar tidak menimbulkan dampak kerugian yang lebih besar.

12. dan praktik empiris Keamanan Siber selama ini?

Tanggapan :

Sebelum menyusun kebijakan di bidang keamanan siber, BSSN berupaya melakukan penyusunan naskah akademik terlebih dahulu untuk mengkaji urgensi kebijakan yang akan disusun dan melakukan uji publik. Oleh karenanya, penting untuk dapat mengkaji dengan pendekatan teoritis dan praktis untuk menghasilkan rumusan kebijakan yang dapat diimplementasikan oleh berbagai pemangku kepentingan.

13. Bagaimana pengaturan mengenai Keamanan Siber dalam ketentuan peraturan perundang-undangan yang ada?

Tanggapan:

UU ITE yang berkaitan dengan keamanan siber, berbagai Peraturan Presiden, Peraturan Pemerintah, Peraturan BSSN, dan peraturan teknis lainnya. Dikarenakan keamanan siber merupakan *crosscutting issues* sehingga keamanan siber diatur pada berbagai peraturan yang saling terkait bahkan pada sektor lain seperti ekonomi, pertahanan, pemerintahan (sistem pemerintah berbasis elektronik), TIK, publik (pelindungan data pribadi), dan seterusnya. Peraturan diharapkan saling menguatkan dan tidak kontradiktif.

14. Apa saja pelatihan dan workshop dalam penanggulangan insiden keamanan siber yang dilakukan antara Indonesia dan Australia?

Tanggapan:

Penyelenggaraan Cyberboot Camp, CSIRO Data 4 Development (D4D) Fellowship Program for Indonesia Civil Servants, webinar terkait isu keamanan siber dan pelatihan SANS Institute yaitu bidang:

- *Practical Open-Source Intelligence;*
- *Hacker Tools, Techniques and Incident Handling;*
- *Web App Penetration Testing and Ethical Hacking;*
- *Implementing and Auditing Security and Frameworks and Controls.*

15. Apa yang melatar belakangi kerjasama australia dan indonesia mengapa kedua negara tersebut bekerjasama?

Tanggapan :

- Atas dasar Australia merupakan negara tetangga Indonesia, penghormatan atas kedaulatan nasional negara masing-masing, non intervensi atas urusan domestik dan saling menguntungkan serta kerja sama di bidang keamanan siber dengan Australia tetap berdasarkan pada politik luar negeri Indonesia, yaitu bebas aktif. Oleh karena itu, BSSN sangat terbuka dengan adanya kerja sama dengan negara lain sepanjang memenuhi prinsip 4 aman yaitu:

- e. Politis, tidak bertentangan dengan kebijakan nasional, khususnya politik luar negeri Indonesia,
 - f. Yuridis, tidak bertentangan dengan ketentuan peraturan perundang-undangan,
 - g. Teknis, tidak bertentangan dengan kebijakan teknis Kementerian/Lembaga di Indonesia, dan
 - h. Security, bukan merupakan suatu penyelundupan hukum.
- Selain itu, kapabilitas Australia yang lebih unggul dibandingkan Indonesia serta kebutuhan Indonesia untuk memperkuat kapasitas dan kapabilitas keamanan siber nasional dengan belajar dari pemerintah Australia.
 - Indonesia dan Australia berkeinginan untuk bersama-sama menjaga keamanan siber dalam rangka CBM kedua negara dengan membawa kepentingan nasional negara masing-masing untuk dapat menciptakan *mutual trust* diantara kedua negara.

Lampiran tanda tangan persetujuan sidang skripsi


LEMBAR PERSETUJUAN SIDANG SKRIPSI

Skripsi diajukan oleh:

Nama : Amanda Rizka Margaretha Ramadani
NIM : 1910417055
Program Studi : Hubungan Internasional
Judul Skripsi : Kerjasama Badan Siber dan Sandi Negara (BSSN) dan Departement of Foreign and Trade (DFAT) Dalam Menghadapi Keamanan Siber Indonesia Melalui Program Secure Information and Best Practice Team (2019-2022)

Telah berhasil melakukan bimbingan minimal **6X** dihadapan dosen pembimbing diterima sebagai bagian persyaratan untuk melakukan sidang **SKRIPSI** yang diperlukan untuk memperoleh gelar Sarjana, pada Program Studi Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Pembangunan Nasional "Veteran" Jakarta.

Pembimbing I


(Dr. Mansur, M.Si.)

Ditetapkan di : Jakarta
Tanggal Ujian :

RIWAYAT HIDUP

Nama : Amanda Rich Margareth Bakara Tempat/Tanggal Lahir : Jakarta, 16 April 2000 Jenis Kelamin: Perempuan Agama : Kristen Protestan Kewarganegaraan: Indonesia Alamat: Perumahan PTI Khusus Blok J5 Nomor 1, Cipete Raya, Mustikajaya, Bekasi, 17510 No. Telp : 085173021621 Email : amandarichmrg@gmail.com

Nama Orang Tua :

1) Ayah : Bisker M Bakara 2) Ibu : Budiaty Malau

PENDIDIKAN TERAKHIR 1) SD Santa Lusia Bojong Menteng (Bekasi Timur, Bekasi) 2) SMP Santa Lusia Bojong Menteng (Bekasi Timur, Bekasi) 3) SMA Marsudirini Bekasi (Kemang Pratama, Bekasi)