BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi telah membawa perubahan besar dalam berbagai aspek kehidupan manusia. Sejak kemunculan komputer pertama hingga era digital saat ini, telah memunculkan tantangan baru berupa kejahatan siber yang mengancam individu, perusahaan, bahkan negara (Irwansyah, 2021). Kejahatan siber atau *cybercrime* merupakan suatu tindakan kejahatan dan vektor yang terus berkembang. Kejahatan ini dilakukan dengan menggunakan media internet atau *cyberspace*, yaitu ruang elektronik dalam jaringan komputer yang berfungsi sebagai alat komunikasi secara *online* (Ketaren, 2016). Metode untuk menyerang *cyberspace* juga semakin beragam, seperti peretasan, kebocoran data, *phising, cybertheft, cyberfraud, ransomware,* bahkan *cyber warfare* (Komdigi, 2023).

Salah satu kejahatan siber yang memiliki urgensi tinggi adalah kebocoran data. Berdasarkan Paul M. Schwartz dan Daniel J. Solove, melihat kebocoran data sebagai kejahatan yang terjadi ketika suatu data atau informasi yang sensitif dan rahasia seperti data pribadi tidak sengaja terungkap dan bisa diakses oleh pihak manapun ataupun *hacker* (Solove, 2011). Salah satu faktor yang menjadi penyebab kebocoran data adalah *human error,* akibat kurangnya literasi keamanan siber sehingga sedikitnya kesadaran terhadap penggunaan sandi yang lemah dan jarang diperbarui, tidak mengaktifkan autentikasi dua faktor, serta korban tertipu *phising* (Humaira, 2024).

Menurut *Computer Security Incident Response Team* (CSIRT), Indonesia telah terdaftar sebagai salah satu negara dengan kasus kebocoran data paling

banyak di dunia pada tahun 2024 (CSIRT, 2024). Kemudian berdasarkan *Cisco's 2024 Cybersecurity Readiness Index* hanya terdapat 12% organisasi atau perusahaan Indonesia yang sudah siap untuk melawan ancaman siber yang akan datang (Threestayanti, 2024). Kasus ini sudah terjadi dari beberapa tahun terakhir, salah satu kebocoran data terbesar yang terjadi di Indonesia adalah pada Pusat Data Nasional (PDN).

Kasus ini telah menimbulkan dampak serius, baik secara langsung maupun jangka panjang. Salah satu dampak paling nyata adalah kerugian finansial untuk menghadapi biaya pemulihan serta denda administratif. Mengutip dari laporan *News Data Financial Tools*, Indonesia mengalami kerugian sebanyak Rp 1,2 triliun dan masih terus bertambah akibat serangan siber pada Pusat Data Nasional (PDN) (Laoli, 2024). Kemudian dari sisi hukum, kebocoran data juga dapat memicu implikasi hukum karena telah melakukan pelanggaran terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (MK RI, 2023).

Kondisi tersebut telah menunjukan bahwa ancaman kebocoran data di Indonesia merupakan isu serius. Maka dari itu, dibutuhkan penanganan sistematis dan berkelanjutan kepada masyarakat. Salah satu cara untuk mencegah kebocoran data adalah dengan memberikan literasi keamanan digital, yang perlu dilakukan secara berkala agar masyarakat bisa mengenali potensi ancaman dan tidak melakukan kesalahan yang bisa membahayakan data (Antara, 2022). Karena pada dasarnya negara memiliki tanggung jawab utama untuk memastikan keamanan ruang siber nasional sebagai bagian dari perlindungan terhadap warga negara.

Di Indonesia, peran tersebut dimiliki oleh Badan Siber dan Sandi Negara (BSSN). BSSN dibentuk berdasarkan Peraturan Presiden Nomor 53 Tahun 2017 yang kemudian diperkuat melalui Peraturan Presiden Nomor 133 Tahun 2017, sebagai respons atas meningkatnya kompleksitas ancaman siber di tingkat nasional dan global. BSSN juga terbentuk melalui transformasi dari Lamsaneg (Lembaga Sandi Negara) serta penggabungan dengan Direktorat Keamanan Informasi dan Indonesia *Security Incident Response Team on Internet Infrastructure* (ID-SIRTII) dari Kementerian Komunikasi dan Informatika (Kompas, 2017). Pembentukan BSSN menandai konsolidasi fungsi keamanan siber dan persandian negara ke dalam satu lembaga yang terintegrasi, sehingga negara memiliki institusi khusus yang bertanggung jawab dalam menjaga kedaulatan siber (Komdigi, 2020).

BSSN berperan dalam merumuskan dan menetapkan kebijakan teknis keamanan siber nasional, melakukan deteksi dan respons terhadap insiden siber, membangun sistem perlindungan infrastruktur informasi vital, serta melakukan pembinaan dan peningkatan kapasitas sumber daya manusia di bidang keamanan siber (Komdigi, 2020). Salah satu literasi keamanan digital yang sudah berjalan berasal dari strategi yang dibentuk oleh Badan Siber dan Sandi Negara (BSSN) sesuai dengan peraturan BSSN nomor 3 tahun 2021 (Hasani, 2023, 1).

Literasi keamanan digital tersebut merupakan kampanye #JagaRuangSiber, berupa edukasi untuk meningkatkan kesadaran dan pemahaman dalam menjaga keamanan dan etika terhadap penggunaan teknologi digital secara aman dan bertanggungjawab. Pendekatan kampanye ini bersifat humanistik, dengan target utama adalah masyarakat umum. BSSN juga menyediakan konten edukatif melalui media sosial seperti Instagram, TikTok, dan YouTube untuk menjangkau audiens

yang lebih luas dan pemberian edukasi secara tatap muka (Diskominfo, 2022). Kampanye ini juga sejalan dengan fungsi BSSN untuk bertanggung jawab atas keamanan siber dan perlindungan informasi penting negara.

Selain adanya insisasi dari lembaga domestik, Indonesia sudah lama bergabung dan bekerjasama dengan organisasi regional yaitu *Association of Southeast Asian Nations* (ASEAN) untuk memperkuat pertahanan digitalnya. Salah satu pilar ASEAN adalah ASEAN *Political Security Community* (APSC), yang bertujuan untuk menyelesaikan permasalahan tradisional dan non tradisional contohnya kejahatan siber (APSC Blueprint, n.d.).

Kemudian inisiatif penting dibawah pilar ini adalah ASEAN *Cybersecurity Cooperation Strategy* (ACCS) yang merupakan sebuah *roadmap* kerjasama regional. ACCS diperkenalkan dalam forum *Telecommunications and Informations Technology Ministers Meeting* (TELMIN) dan ASEAN *Ministerial Conference on Cybersecurity* (AMCC). ACCS berfungsi untuk mencapai tujuan yang sama dan menciptakan keamanan dan perlindungan pada dunia siber di negara-negara anggota ASEAN. ACCS memiliki dua periode utama, periode pertama 2017-2020 dan periode kedua 2021-2025 (ACCS, n.d.).

ACCS 2021-2025 memiliki fokus dengan menekankan pentingnya pengembangan ekosistem keamanan siber yang komprehensif. Selain melanjutkan kerja sama antar *Computer Emergency Response Team* (CERT), strategi ini juga menyoroti pengembangan pendidikan dan pelatihan keamanan siber, peningkatan kesadaran publik, serta kolaborasi dengan sektor swasta dan komunitas internasional. Kemudian penguatan infrastruktur kritis, pengembangan standar keamanan, dan implementasi kebijakan yang mendukung pencegahan ancaman

siber sebelum terjadi. Strategi ini mengakui peran penting sektor swasta dalam ekosistem keamanan siber, maka terdapat dorongan untuk meningkatkan kolaborasi antara pemerintah, industri, dan akademisi dalam mengembangkan solusi keamanan siber yang inovatif dan efektif (ACCS, n.d.).

Berdasarkan dari penjelasan ACCS periode kedua, ditemukan kesinambungan dari isi draf ACCS dengan kampanye #JagaRuangSiber yang merupakan bentuk *policy transfer* dari ASEAN. Sehingga penelitian ini akan melihat bagaimana peran BSSN terhadap kampanye #JagaRuangSiber sebagai penerapan dari draf ACCS untuk meningkatkan keamanan siber kepada masyarakat.

1.2. Perumusan Masalah

Berdasarkan latar belakang yang sudah peneliti uraikan di atas, maka rumusan masalah yang penulis rumuskan adalah:

Bagaimana implementasi kampanye #JagaRuangSiber oleh Badan Siber dan Sandi Negara (BSSN) untuk meningkatkan literasi keamanan digital sebagai penerapan ASEAN *Cybersecurity Cooperation Strategy* (ACCS)?

1.3. Tujuan Penelitian

Penelitian ini memiliki dua tujuan yang ingin dicapai, yakni sebagai berikut:

1.3.1 Tujuan Umum

Penelitian ini bertujuan untuk menganalisis peran Badan Siber dan Sandi Negara (BSSN) dalam kampanye #JagaRuangSiber untuk meningkatkan literasi keamanan digital kepada masyarakat, sebagai salah satu respons dari maraknya kasus kebocoran data yang terjadi di Indonesia. Kemudian sebagai bagian dari

penerapan strategi keamanan siber regional ASEAN, yaitu ASEAN *Cybersecurity Cooperation Strategy* (ACCS).

1.3.2 Tujuan Khusus

a. Menganalisis peran BSSN dalam kampanye #JagaRuangSiber yang di tujukan kepada masyarakat.
b. Melihat bentuk transfer kebijakan BSSN terhadap *ASEAN Cybersecurity Cooperation Strategy* (ACCS) periode 2021–2025.

1.4. Kegunaan Penelitian

1.4.1 Kegunaan Akademis

Penelitian ini diharapkan dapat memberikan kontribusi teoritis bagi pengembangan kajian di bidang keamanan siber dan hubungan penelitian ini juga digunakan untuk menambah literatur mengenai keterkaitan antara strategi regional seperti ACCS dengan implementasinya dalam konteks nasional oleh lembaga seperti BSSN. Selain itu, penelitian ini juga dapat menjadi dasar bagi mahasiswa dan akademisi untuk mengembangkan kajian lanjutan mengenai peran negara dan institusi dalam menghadapi tantangan digital era moderen.

1.4.2 Kegunaan Praktis

Secara praktis, hasil penelitian ini diharapkan dapat menjadi masukan strategis bagi BSSN dalam mengevaluasi dan menyempurnakan program literasi keamanan digital yang ditujukan kepada masyarakat. Penelitian ini juga berguna dalam meningkatkan kesadaran akan pentingnya penguatan budaya keamanan siber, serta sebagai pedoman dalam merancang kebijakan internal terkait perlindungan data. Selain itu, temuan

dari penelitian ini juga dapat menjadi acuan bagi ASEAN dalam menilai efektivitas strategi ACCS di negara anggotanya, khususnya Indonesia.

1.5. Kerangka Pemikiran Teoritis

1.5.1. *Review Literatur*

Terdapat empat bacaan atau penelitian terdahulu yang menjadi acuan penulis dalam penelitian ini. Penelitian sebelumnya yang sudah meneliti isu kejahatan siber di indonesia yang mengeluarkan *output* untuk memberikan pemahaman mendalam terkait pertahanan siber kepada ASN sebagai bentuk implementasi dari ACCS secara tidak langsung, antara lain yaitu: Pertama, yakni penelitian yang berjudul "Analisis Kebijakan Siber Indonesia terkait ASEAN *Cybersecurity Cooperation Strategy* (ACCS) Tahun 2019-2022" oleh M. Rafly Ramdhan yang dutulis pada tahun 2023. Penelitian ini menganalisis keterkaitan kebijakan siber nasional dengan strategi ACCS yang disusun oleh ASEAN, dan mendapatkan hasil bahwa kebijakan yang dibentuk ASEAN seperti APSC *Blueprint* serta ACCS periode 2017–2020 dan 2021–2025, memberikan arah dan kerangka kerja yang membantu Indonesia dalam menangani kejahatan siber. Kemudian penelitian ini menyimpulkan bahwa strategi ACCS memberikan kontribusi signifikan terhadap upaya Indonesia dalam memperkuat sistem keamanan siber nasional (Ramadhan, 2023).

Penelitian kedua yang menjadi referensi penelitian ini adalah "*Analyzing the Impication of* ASEAN *Cybersecurity Cooperation Strategy* (ACCS) 2021-2025 *in Indonesia Cyber Regulations*" oleh Naylah R. A. Matondang pada tahun 2025. Hasil dari penilitian ini menunjukkan bahwa

implementasi ACCS di Indonesia memberikan dampak nyata terhadap peningkatan regulasi keamanan siber nasional. Hal ini ditunjukkan dengan meningkatnya jumlah regulasi yang dikeluarkan oleh Badan Siber dan Sandi Negara (BSSN) dari 15 regulasi pada periode sebelum 2021, menjadi 38 regulasi pada periode 2021–2025. Penelitian ini menyimpulkan bahwa implementasi ACCS mendorong Indonesia untuk memperkuat kerangka regulasi nasional, terutama pada aspek koordinasi kebijakan siber regional, sekaligus menunjukkan komitmen negara terhadap kerja sama multilateral dalam menghadapi tantangan siber kawasan (Matondang, 2025).

Penelitian ketiga adalah "Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah" oleh Naylawati Bahtiar tahun 2022 dalam jurnal *Development Policy and Management Review* menyoroti kondisi darurat kebocoran data pribadi di Indonesia, khususnya yang terjadi di sektor instansi pemerintahan. Penelitian ini menekankan bahwa lemahnya regulasi dan infrastruktur keamanan digital di tingkat lembaga pemerintahan menjadi penyebab utama maraknya insiden kebocoran data. Penelitian ini juga mengungkap bahwa tidak hanya infrastruktur teknologi yang lemah, namun sumber daya manusia yang mengelola sistem digital, termasuk ASN, masih memiliki tingkat kesadaran dan kompetensi yang rendah dalam perlindungan data pribadi (Bahtiar, 2022).

Penelitian keempat "Indonesia Cakap Digital Melalui Kegiatan Literasi Digital Bagi Seluruh Aparatur Sipil Negara (ASN)" oleh Mudji Estiningsih pada tahun 2023 dalam *Melati Journal of Management and Accounting Studies*, hasil penelitian menunjukkan bahwa kegiatan literasi

digital bagi ASN sangat penting dalam mendukung program transformasi digital pemerintahan. Penelitian ini menekankan bahwa ASN harus memiliki pemahaman digital yang matang, termasuk dalam hal etika digital, keamanan data, serta penggunaan platform digital untuk pelayanan publik yang efektif. Literasi digital dipandang sebagai pondasi utama untuk menciptakan birokrasi yang adaptif dan tangguh dalam menghadapi ancaman siber (Estiningsih, 2023).

Penelitian kelima *"Data Breaches in Government Institutions and Society and Their Impacts on National Security in Indonesia"* oleh Rahmadiah Josina Ukas tahun 2025. Menjelaskan hasil penelitian bahwa kebocoran data di Indonesia memberikan dampak yang sangat berbahaya bagi keamanan nasional. Penelitian ini juga menyimpulkan bahwa meskipun Indonesia telah memiliki UU PDP, implementasinya masih menghadapi kendala signifikan karena kurangnya transparansi, akuntabilitas, dan rendahnya tingkat literasi digital masyarakat. Di tingkat regional, Indonesia berupaya mengatasi ancaman ini melalui implementasi *ASEAN Cybersecurity Cooperation Strategy* (ACCS) 2021-2025. Sebagai solusi, penulis menekankan perlunya peningkatan pertahanan teknis seperti autentikasi multi-faktor, penegakan hukum yang lebih tegas dan kaku terhadap pelaku kebocoran data, serta penguatan literasi digital untuk membangun kepercayaan publik (Ukas, 2025).

Penelitian keenam berjudul "Peran ASEAN melalui ACCS dalam Menangani Kejahatan Siber di Indonesia" oleh Jonathan Manurung tahun 2024, memberikan hasil penelitian bahwa BSSN berperan

mengimplementasikan ACCS melalui pilar pengembangan kapasitas, penyelarasan kebijakan, dan pertukaran informasi teknis via ASEAN-CERT. Namun, evaluasi strategi nasional menunjukkan bahwa efektivitas langkah BSSN masih terhambat oleh lemahnya koordinasi antarlembaga, keterbatasan anggaran, serta kesenjangan kompetensi SDM jika dibandingkan dengan Singapura dan Malaysia. Oleh karena itu, sinergi antara regulasi UU PDP dan program literasi digital yang masif menjadi kunci utama yang direkomendasikan untuk memperkuat ketahanan siber nasional dan kedaulatan data Indonesia di tingkat regional (Manurung, 2024).

Berdasarkan beberapa tinjauan pustaka tersebut dapat dilihat bahwa *gap* atau kebaruan dari penelitian ini terletak pada isi penelitian yang memiliki fokus untuk mengulik bagaimana peran BSSN dalam menjalankan kampanye #JagaRuangSiber kepada masyarakat sebagai salah satu respons dari maraknya kasus kebocoran data di Indonesia. Serta melihat bagaimana penerapan BSSN dari draf ACCS 2021-2025, karena isi dari draf periode kedua tersebut memberikan acuan untuk membentuk serta memberikan pengembangan pendidikan dan pelatihan keamanan siber dan peningkatan kesadaran publik yang sejalan dengan tujuan program literasi keamanan digital.

1.5.2. *Policy Transfer Theory*

Dalam upaya memahami dinamika kebijakan domestik yang terinspirasi oleh kebijakan regional atau internasional, teori *policy transfer* memberikan kerangka analisis yang relevan dan aplikatif. Teori ini

dikembangkan untuk menjelaskan bagaimana kebijakan, program, institusi, atau praktik tertentu yang berasal dari satu sistem pemerintahan dapat memengaruhi atau diadopsi oleh sistem lain.

Menurut pemikiran Dolowitz dan Marsh (2000), mereka menekankan bahwa *policy transfer* bukan sekadar peniruan mekanis, tetapi merupakan proses aktif dan kompleks yang melibatkan pemilihan elemen kebijakan tertentu untuk diadaptasi ke dalam konteks yang berbeda. Proses ini dapat melibatkan berbagai aktor, termasuk pemerintah, lembaga publik, organisasi internasional, hingga lembaga swadaya masyarakat (Dolowitz & Marsh, 2000).

Why Transfer? Continuum Want To. . . . . Have To			Who Is Involved in Transfer?	What Is Transferred?		From Where		Degrees of Transfer	Constraints on Transfer	How To Demonstrate Policy Transfer	How Transfer leads to Policy Failure
Voluntary	Mixtures	Coercive			Past	Within-a Nation	Cross-National				
esson rawing Perfect tionality)	Lesson Drawing (Bounded Rationality)	Direct Imposition	Elected Officials	Policies (Goals) (content) (instruments)	Internal	State Governments	International Organizations	Copying	Policy Complexity (Newspaper) (Magazine) (TV) (Radio)	Media	Uniformed Transfer
	International Pressures		Bureaucrats Civil Servants	Programs	Global	City Governments	Regional State Local Governments	Emulation	Past Policies	Reports	Incomplete Transfer
	(Image) (Consensus) (Perceptions)									(Commissioned) (uncommissioned)	
	Externalities	Pressure Groups	Institutions			Local Authorities		Mixtures	Structural Institutional	Conferences	Inappropriate Transfer
	Conditionality	Political Parties	Ideologies					Inspiration	Feasibility	Meetings/ Visits	
	(Loans) (Conditions Attached to Business Activity)								(Ideology) (cultural proximity) (technology) (economic) (bureaucratic)		
	Obligations	Policy Entrepreneurs/ Experts	Attitudes/ Cultural Values						Language	Statements (written) (verbal)	
			Consultants Think Tanks Transnational Corporations Supranational Institutions	Negative Lessons			Past Relations				

Gambar 1. 1 *Policy Transfer Framework*

Sumber: Dolowitz dan Marsh, 2000

Framework dari teori ini digunakan untuk menganalisis dalam bentuk apa kebijakan di transfer, kemudian aktor apa saja yang terlibat, batasan pada melakukan transfer kebijakan dan hasil dari transfer kebijakan yang mengarah kepada kegalalan atau keberhasilan. Berdasarkan tulisan yang berjudul *Learning from Abroad: The Role of Policy Transfer in*

Contemporary Policy Making, dijelaskan bahwa *Policy transfer* terbagi ke dalam beberapa bentuk berdasarkan sejauh mana paksaan atau tekanan eksternal terlibat dalam proses adopsi kebijakan. Salah satu bentuk yang paling umum dalam kerja sama internasional adalah *voluntary transfer*, yakni proses adopsi kebijakan secara sukarela tanpa adanya tekanan atau kewajiban formal.

Dalam *voluntary transfer*, aktor domestik secara aktif dan sadar memilih untuk mengadopsi atau menyesuaikan kebijakan tertentu karena dianggap sesuai dengan kebutuhan lokal, memiliki nilai guna atau mampu menjawab tantangan kebijakan yang dihadapi. Tidak ada unsur pemaksaan atau sanksi, dan keputusan transfer terjadi karena adanya persepsi positif terhadap keberhasilan atau kesesuaian kebijakan tersebut di konteks asalnya (Dolowitz & Marsh, 2000).

1.6. Operasionalisasi Konsep

1.6.1. Definisi Konseptual

1.6.1.1. *Cybersecurity Capacity Maturity Model for Nations*

Dalam menghadapi tantangan keamanan digital yang kian kompleks, negara-negara di dunia dituntut untuk membangun kapasitas keamanan siber secara menyeluruh dan berkelanjutan. Konsep *Cybersecurity Capacity Maturity Model for Nations* (CMM) oleh *Global Cyber Security Capacity Centre* (GCSCC) di University of Oxford, muncul sebagai kerangka strategis yang menekankan pentingnya pengembangan kapasitas individu, kelembagaan, dan sistem untuk meningkatkan ketahanan siber suatu negara.

Kemudian konsep ini memiliki 5 dimensi sebagai alat analisisnya, yaitu *Cybersecurity Policy and Strategy, Cyber Culture and Society*, *Cybersecurity Education, Training, and Skills, Legal and Regulatory Frameworks, Standards, Organizations, and Technologies* (*Global Cyber Security Capacity Centre*, 2015). Masing-masing dimensi mencerminkan aspek penting dari sistem keamanan siber yang saling terhubung dan mempengaruhi.

CMM digunakan untuk membantu negara-negara dalam menilai dan mengembangkan kapasitas keamanan siber nasional mereka secara menyeluruh**.** Model ini juga telah digunakan secara luas oleh berbagai negara di dunia sebagai pedoman dalam memperkuat ketahanan siber mereka. Tujuan CMM adalah memberikan pemahaman yang komprehensif mengenai posisi suatu negara dalam hal kesiapan dan kemampuan menghadapi ancaman di ruang siber. Dengan demikian, CMM dapat membantu negara melihat kekuatan, kelemahan, serta peluang pengembangan kapasitas siber yang ada, baik dari sisi kebijakan, pendidikan, masyarakat, hukum, hingga teknologi (GCSCC, 2015).

1.6.1.2 *Human Security*

Setelah terjadinya perang dingin, pandangan mengenai keamanan telah berubah. Sebelumnya keamanan berhubungan dengan militer, pertahanan teritorial dan konflik. Sedangkan pasca perang dingin, pandangan mengenai keamanan berubah menjadi masalah kemanusiaan (Fakhrul, 2022). Berdasarkan tulisan dari Rita Floyd, *Human security* merupakan konsep keamanan manusia yang memandang individu sebagai

penerima semua masalah keamanan, dan manusia berpusat untuk mengenali berbagai ancaman terhadap masyarakat. Kemudian *human security* melibatkan perlindungan terhadap ancaman non-militer seperti bencana alam, perubahan iklim, kemiskinan, hingga kesejahteraan sosial (Floyd, 2007).

Pemikiran mengenai konsep *human security* pertama kali diperkenalkan pada tahun 1994 oleh *Human Development Report* UNDP. Laporan tersebut menjelaskan bahwa konsep akan keamanan harus berubah dari keamanan negara menjadi keamanan kepada manusia. *United Nations Development Program* (UNDP) memperkenalkan konsep *human security* sebagai *"freedom from fear and freedom from want"* (Bryan, 2026). Kemudian konsep *human security* ditujukan untuk perlindungan dan pemberdayaan manusia. Artinya melindungi individu dari ancaman yang ada, kemudian memberdayakan mereka untuk menghadapi tantangan dari isu keamanan yang semakin kompleks. Konsep ini juga melengkapi konsep keamanan negara dengan perlindungan terhadap hak asasi manusia. Kemanan bukan hanya mencakup perlindungan terhadap ancaman fisik individu, tetapi juga perlindungan terhadap hak-hak dasar individu (UNDP, 1994).

Secara konseptual, *human security* menurut UNDP merupakan pendekatan keamanan yang menempatkan individu sebagai *referent object* utama dalam studi keamanan. Berbeda dengan pendekatan keamanan tradisional yang berfokus pada perlindungan negara dari ancaman militer, *human security* menekankan perlindungan manusia dari berbagai ancaman

yang dapat mengganggu kelangsungan hidup, martabat, dan kesejahteraan mereka.

1.6.2. Definisi Operasional

1.6.2.1. *Cybersecurity Capacity Maturity Model for Nations*

CMM memberikan pendekatan yang komprehensif dan sistematis dalam mengevaluasi kapasitas keamanan siber suatu negara berdasarkan lima dimensi utama. Dengan menggunakan CMM, tantangan tidak hanya dilihat dari sisi teknis atau kebijakan semata, tetapi juga mencakup indikator yang berbeda-beda.

Gambar 1. 2 Dimensi dalam konsep CMM

Sumber: Gcscc, 2015

Berdasarkan dari gambar diatas, CMM terdiri atas lima dimensi utama yang mewakili aspek-aspek dari kapasitas keamanan siber suatu negara, yaitu:

a. *Cybersecurity Policy and Strategy* digunakan untuk mengevaluasi kemampuan suatu negara dalam merumuskan dan melaksanakan kebijakan serta strategi keamanan siber nasional.

b. *Cyber Culture and Society* merupakan dimensi untuk mengukur tingkat kesadaran, pemahaman, dan sikap masyarakat terhadap risiko siber, serta bagaimana budaya digital terbentuk dalam suatu negara.
c. *Building cybersecurity knowladge and capabilities* merupakan alat evaluasi ketersediaan dan efektivitas program pelatihan, pendidikan formal, dan pengembangan keahlian di bidang keamanan siber bagi seluruh pemangku kepentingan termasuk pemerintah, sektor swasta, dan masyarakat umum.
d. *Legal and Regulatory Frameworks,* dimensi ini menilai apakah suatu negara memiliki kerangka hukum dan peraturan yang memadai untuk mengatur dan menegakkan keamanan siber, termasuk regulasi tentang kejahatan siber serta perlindungan data.
e. *Standards, Organizations, and Technologies* membahas penerapan standar keamanan siber, kesiapan infrastruktur teknologi, dan penggunaan sistem atau produk teknologi yang aman dan mutakhir untuk melindungi individu maupun infrastruktur penting.

1.6.2.2. Human Security

Konsep *human security* terbagi menjadi 7 kelompok, yaitu *economic security*, *food security*, *health security*, *environmental* security, *personal security*, *community security*, kemudian *political security* (UNDP, 1994). *Personal security* dipahami sebagai kondisi di mana individu terlindungi dari berbagai ancaman terhadap keselamatan, integritas, dan martabat pribadinya. UNDP menekankan bahwa keamanan tidak hanya berkaitan dengan ancaman militer, tetapi juga ancaman yang dapat mengganggu

kehidupan sehari-hari individu. Dengan demikian, *personal security* menempatkan individu sebagai subjek utama yang harus dilindungi dari segala bentuk gangguan yang membahayakan rasa aman dan hak dasarnya (UNDP, 1994). Dengan demikian, *human security* dapat dipahami sebagai kerangka keamanan yang berorientasi pada perlindungan hak, keselamatan, dan kesejahteraan individu dari ancaman militer maupun non-militer dalam sistem global yang saling terhubung.

1.7 Argumen Penelitian

Peran Badan Siber dan Sandi Negara (BSSN) dalam kampanye #JagaRuangSiber merupakan bentuk penerapan terhadap ASEAN *Cybersecurity Cooperation Strategy* (ACCS) periode 2021–2025, khususnya terdapat *policy transfer* pada aspek peningkatan kesadaran publik dan penguatan kapasitas masyarakat. Implementasi kampanye ini lahir sebagai respons terhadap maraknya kasus kebocoran data di Indonesia. Karena kasus ini telah menimbulkan ancaman terhadap individu. Berdasarkan perspektif *human security*, kondisi ini menempatkan individu sebagai subjek yang rentan terhadap penyalahgunaan data dan menimbulkan kerugian finansial. Kemudian ancaman siber tidak hanya bersumber dari kerentanan teknis, tetapi juga dari rendahnya literasi keamanan digital masyarakat. Melalui kampanye #JagaRuangSiber, peran BSSN difokuskan melalui dimensi *cyber culture and society* dan *Building cybersecurity knowladge and capabilities* dari *Cybersecurity Capacity Maturity Model* (CMM). Dari dimensi tersebut, BSSN berperan dalam membangun *awareness* mengenai pentingnya perlindungan data pribadi, mengenalkan berbagai bentuk ancaman siber, serta mendorong

perubahan perilaku digital yang lebih aman dan bertanggung jawab. Dengan demikian, kampanye ini tidak hanya mencerminkan keselarasan Indonesia dengan agenda keamanan siber regional ASEAN, tetapi juga menjadi instrumen preventif untuk memperkuat kemampuan masyarakat dalam melindungi data mereka sendiri sebagai bagian dari upaya meningkatkan ketahanan siber nasional.

1.8. Metode Penelitian

Penelitian ini menggunakan metode kualitatif, sebagaimana dijelaskan dalam tulisan Abdul Nasution bahwa penelitian kualitatif digunakan untuk memahami dan menjelaskan suatu fenomena sosial yang tidak bisa diukur dengan angka atau kuantitatif. Penelitian ini lebih menekankan pada pemahaman makna, pengalaman, serta kondisi yang terjadi di lapangan yang berbeda dengan metode kuantitatif dengan menggunakan data statistik.

Penelitian kualitatif mengandalkan data mentah dari hasil wawancara, observasi atau dokumen serta menggunakan teori yang sudah ada untuk membantu menjelaskan temuan di lapangan (Nasution, 2023, 6). Alasan dipilihnya metode ini adalah karena mampu menggali informasi secara mendalam dan menyeluruh**,** terutama dalam memahami argumen, data, dan konteks yang kompleks. Selain itu, pendekatan ini memungkinkan peneliti untuk menyusun deskripsi yang detail dan menjelaskan hasil penelitian secara menyeluruh. Dengan demikian, tujuan utama dari penelitian ini adalah untuk memberikan gambaran yang objektif dan menyeluruh mengenai peran BSSN dalam melaksanakan program literasi keamanan digital kepada kepada masyarakat.

1.8.1. Tipe Penelitian

Penelitian ini menggunakan pendekatan deskriptif kualitatif**,** yaitu metode penelitian yang bertujuan untuk menggambarkan secara sistematis dan mendalam suatu fenomena sosial berdasarkan data kualitatif. Penelitian deskriptif kualitatif tidak menggunakan data statistik atau angka, tetapi lebih menekankan pada pemahaman terhadap konteks, proses, serta makna dari suatu peristiwa atau kebijakan (Sugiyono, 2022, 3).

Pendekatan ini dipilih karena sesuai untuk mengkaji peran BSSN dalam program literasi keamanan digital sebagai penerapan ACCS periode 2021–2025**.** Melalui pendekatan ini, peneliti dapat mengeksplorasi data dari dokumen, wawancara, dan observasi secara mendalam, sehingga menghasilkan pemahaman yang utuh terhadap fenomena yang diteliti.

1.8.2. Situs Penelitian

Penelitian ini menggunakan situs penelitian sebagai sumber data sebagai cara untuk menjawab rumusan masalah. Dalam penelitian ini, data primer diperoleh dari hasil wawancara dengan lembaga atau individu terkait, sedangkan data sekunder berasal dari sumber ilmiah. Data utama dalam penelitian ini menggunakan hasil wawancara dengan BSSN sebagai lembaga yang membentuk progam literasi keamanan digital. Kemudian wawancara dengan Diskominfo Belitung sebagai penerima dan penyalur program literasi keamanan digital dari BSSN, dan wawancara dengan NGO yang bernama ADIGSI untuk melihat bagaimana pandangan pengamat siber dalam keberjalanan kampanye ini.

Selain itu, pengambilan data sekunder berasal dari sumber yang tersedia dan dapat diakses seperti buku, jurnal, publikasi akademik, media berita, situs web, hingga laporan resmi. Oleh karena itu, tulisan ini merajuk karya-karya dari penelitian terdahulu, sumber resmi dari ASEAN, ACCS Periode 2021-2025, APSC *Blue Print*, BSSN dan media berita terkemuka.

1.8.3. Subjek Penelitian

Subjek penelitian berkaitan dengan individu atau lembaga terkait yang mampu memberikan data yang tepat untuk mendukung studi penelitian. Titik fokus penelitian ini adalah BSSN sebagai lembaga yang membentuk program literasi keamanan digital dan masyarakat sebagai penerima program.

1.8.4. Jenis Data

Berdasarkan cara memperoleh data, penelitian ini menggunakan dua jenis data yaitu primer dan sekunder. Data primer dapat menunjukan informasi yang diperoleh dari individu atau lembaga terkait yang diikuti dengan keaslian, objektivitas, serta bagaimana data tersebut dapat diandalkan untuk membentuk dasar dan menjawab rumusan masalah.

Pengumpulan data primer dilakukan dengan cara wawancara dan survei, sehingga penelitian ini dapat memberikan data faktual dan tepat untuk mendukung argumen penelitian. Sebaliknya, data sekunder didapatkan tidak langsung dari subjek penelitian atau sampel primer, data ini juga berfungsi sebagai sumber tambahan untuk memperkuat data primer yang diperoleh. Penggabungan kedua tipe data akan memberikan keragaman data dalam upaya penelitian ini (Nasution, 2023, 6)

1.8.5. Sumber Data

Sumber data penelitian ini adalah sumber primer dan sekunder. Sumber data primer didapatkan dari hasil wawancara dengan BSSN, Diskominfo Belitung, dan ADIGSI. Selanjutnya data sekunder didapatkan melalui buku, jurnal, karya ilmiah, situs, hingga laporan resmi yang relevan dengan penelitian ini. Dengan demikian sumber data primer dan sekunder yang telah didapatkan akan ditelaah dan dikaji lebih dalam kemudian disajikan dalam bentuk narasi.

1.8.6. Teknik Pengumpulan Data

Penelitian ini menggunakan teknik pengumpulan data *library research* atau studi kepustakaan dan wawancara. Studi kepustakaan mencakup strategi dalam pengumpulan data yang melibatkan pengambilan informasi dan data dari berbagai sumber yang tersedia. Studi ini juga akan memanfaatkan materi dari domain perputakaan, arsip serta sumber *online* (Zed, 2014.). Dengan memanfaatkan data yang ditemukan pada sumber sekunder, penelitian ini dapat secara efektif dalam melakukan analsis.

Selanjutnya, metodologi yang dipilih untuk pengumpulan data melibatkan wawancara dengan narasumber terkait. Wawancara digambarkan sebagai interaksi atau dialog antara dua individu, terdapat pewawancara yang mengajukan pertanyaan spesifik kepada orang yang diwawancarai untuk mendapatkan informasi atau jawaban dari pertanyaan yang diberikan. Data serta informasi dari hasil wawancara akan ditafsirkan dan dianalsis dengan cermat. Integrasi wawancara bertujuan untuk

melengkapi dan memperkaya data utama terhadap penelitian ini, dan mendapatkan data yang lebih substantif.

1.8.7. Analisis dan Interpretasi Data

Analisis dan interpretasi data dalam penelitian ini dilakukan secara kualitatif. Analisis data kualitatif dipahami sebagai proses pemilahan, pengorganisasian, dan penafsiran data yang diperoleh dari wawancara, dokumentasi, dan observasi, dengan tujuan untuk membangun pemahaman yang mendalam terhadap fenomena yang diteliti (Sugiyono, 2022, 133). Kemudian penelitian ini menggunakan pendekatan analisis yang selaras dengan teori yang diangkat. Menurut Mills, pendekatan yang selaras secara metodologis memungkinkan peneliti membangun atau memanfaatkan kerangka teoretis untuk menafsirkan situasi atau hasil tertentu. Apabila hasil temuan sejalan dengan teori, maka dapat disimpulkan adanya hubungan yang logis antara konteks empiris dengan kerangka konseptual yang digunakan (Mills et al., 2010, 62-63). Penelitian ini akan menelaah bagaimana proses adopsi kebijakan regional ACCS oleh BSSN melalui program literasi digital, serta sejauh mana implementasi pelaksanaannya.

Selanjutnya Interpretasi data kualitatif dalam penelitian ini dilakukan dengan mengaitkan temuan-temuan dominan dari lapangan dengan konsep dan teori yang digunakan. Hasil analisis akan dijabarkan dalam bentuk tema-tema utama yang mencerminkan dinamika implementasi kebijakan, tantangan dan keberhasilan yang dihadapi dalam pelaksanaan program literasi siber kepada masyarakat. Melalui proses ini, data yang terkumpul akan disusun secara sistematis dan dikaji secara kritis

agar dapat mengungkap tantangan dan keberhasilan pelaksanaan program literasi keamanan digital oleh BSSN dalam kerangka ACCS 2021–2025.

1.8.8. Kualitas Data *(goodness criteria)*

Penelitian ini memiliki kualitas data yang tinggi karena didukung oleh sumber data primer dan sekunder. Hasil wawancara yang akan dilakukan dengan BSSN dan individu yang sudah mengikuti program literasi keamanan digital berfungsi sebagai elemen penting dari data primer. Selain itu, data sekunder juga penting untuk meningkatkan kualitas data dalam penelitian ini, seperti publikasi, karta ilmiah, situs dan media berita terkemuka. Dengan demikian, penelitian ini mencapai kualitas data empiris dan teoritis yang penting untuk menjelaskan tantangan dan keberhasilan terhadap program literasi keamanan digital oleh BSSN.