BAB II

KEDUDUKAN KELEMBAGAAN BSSN DAN KEAMANAN SIBER NASIONAL

2.1. Kedudukan Kelembagaan Badan Siber dan Sandi Negara (BSSN) dalam Keamanan Siber Indonesia

Badan Siber dan Sandi Negara (BSSN) merupakan lembaga pemerintah Indonesia yang bertanggung jawab atas keamanan siber dan perlindungan informasi penting negara (Diskominfo, 2023). BSSN dibentuk melalui transformasi dari Lembaga Sandi Negara (Lemsaneg) yang didirikan pada 4 April 1946, serta penggabungan dengan Direktorat Keamanan Informasi dan Indonesia *Security Incident Response Team on Internet Infrastructure* (ID-SIRTII) dari Kementerian Komunikasi dan Informatika (Kemendikdasmen, 2018).

Pembentukan BSSN ditetapkan melalui Peraturan Presiden Nomor 53 Tahun 2017 dan kemudian diperbaharui dengan Peraturan Presiden Nomor 133 Tahun 2017 (BSSN, nd). Terdapat mandat utama BSSN untuk menyelenggarakan keamanan siber secara efektif dan efisien, yaitu dengan memanfaatkan, mengembangkan, serta mengonsolidasikan berbagai unsur yang berkaitan dengan keamanan siber. Dalam melaksanakan mandatnya, BSSN menjalankan sejumlah fungsi penting, antara lain merumuskan serta menetapkan kebijakan teknis di bidang keamanan siber dan persandian, sekaligus memastikan pelaksanaannya berjalan sesuai arah yang telah ditetapkan. Selain itu, BSSN juga berperan dalam menyusun norma, standar,

prosedur, dan kriteria terkait persandian yang menjadi acuan dalam pengelolaan informasi (Kemenko, 2017).

Fungsi lain yang tidak kalah strategis adalah memberikan bimbingan teknis, melakukan supervisi, serta mengoordinasikan pelaksanaan tugas dan pembinaan di seluruh unit organisasi yang berada di bawah naungannya. Di samping itu, BSSN juga bertanggung jawab atas pengelolaan barang milik negara yang menjadi kewenangannya, memberikan dukungan substantif bagi unit kerja internal, serta melakukan pengawasan terhadap pelaksanaan tugas di lingkungannya. Dengan fungsi-fungsi tersebut, BSSN diharapkan mampu menjaga keamanan siber nasional sekaligus memperkuat tata kelola persandian negara (Wibawana, 2022).

Berdasarkan peraturan BSSN No. 4 tahun 2018, dijelaskan bahwa visi BSSN adalah untuk menjadi lembaga yang tepercaya dalam menjaga keamanan siber dan persandian negara. Visi ini diwujudkan melalui sinergi dengan berbagai pemangku kepentingan, baik dari pemerintah, sektor swasta, maupun masyarakat, sehingga keamanan nasional dapat terjaga sekaligus mendukung pertumbuhan ekonomi nasional (Kemendikdasmen, 2018). Dalam rangka mewujudkan visi tersebut, BSSN mengembangkan sejumlah misi strategis.

Pertama, menjamin keamanan informasi yang mencakup sektor pemerintahan, infrastruktur informasi kritikal nasional, hingga ekosistem ekonomi digital. Kedua, membangun serta menerapkan tata kelola keamanan siber dan persandian yang komprehensif sehingga dapat menjadi pedoman bagi seluruh pemangku kepentingan. Ketiga, mendorong kemandirian teknologi di

bidang keamanan siber dan persandian dengan memfasilitasi pertumbuhan industri dalam negeri.

Keempat, mengembangkan sistem identifikasi, deteksi, mitigasi, hingga pemulihan terhadap ancaman atau serangan siber agar respons terhadap insiden lebih terkoordinasi. Kelima, menumbuhkan budaya keamanan digital sebagai nilai yang melekat di masyarakat dengan membiasakan penggunaan internet yang aman dan nyaman. Terakhir, mengoptimalkan sumber daya manusia serta sarana pendukung melalui pembelajaran berkelanjutan, disertai tata kelola organisasi yang transparan dan akuntabel (Kemendikdasmen, 2023).

Dengan demikian, BSSN juga memiliki tanggung jawab strategis dalam menangani kasus kejahatan siber, contohnya adalah persoalan kebocoran data yang semakin marak terjadi di Indonesia. Fenomena ini perlu ditelaah lebih dalam karena tidak hanya mencerminkan adanya celah dalam sistem keamanan teknologi, tetapi juga menunjukan adanya tantangan dalam tata kelola perlindungan data masyarakat.

2.2. Dinamika Kasus Kebocoran Data yang Terjadi di Indonesia

2.2.1. Kebocoran Data dalam Konteks Global

Pada era revolusi digital yang telah melaju pesat, Teknologi Informasi dan Komunikasi (TIK) telah menjadi pondasi utama untuk mengiringi berbagai aktivitas manusia modern. Mulai dari aspek sosial, ekonomi, layanan publik, pendidikan hingga tata kelola pemerintahan yang saat ini telah terdigitalisasi. Sehingga interaksi antara individu maupun sistem berlangsung lebih cepat, efisien, dan dapat melampaui batas geografis. Kehadiran *cyberspace* juga tidak lagi hanya digunakan untuk

media komunikasi, tetapi telah berevolusi menjadi wadah untuk melengkapi kehidupan sehari-hari. Perubahan ini tentunya telah melahirkan banyak tantangan yang harus dihadapi dunia (Siburian, 2024).

Salah satu tantangan paling nyata yang dihadapi Indonesia dalam keamanan siber adalah perlindungan terhadap privasi dan data pribadi seseorang. Hal ini seringkali dipandang remeh, padahal realitasnya memberikan dampak yang sangat merugikan. Salah satu kejahatan terhadap data pribadi seseorang adalah kebocoran data, dalam konteks global kebocoran data sangat berhubungan dengan pembobolan data. Kebocoran data terjadi ketika data pribadi, rahasia, atau sensitif tidak sengaja terekspos ke internet serta situs yang tidak aman, sehingga seorang peretas dapat mengakses, mencuri, atau bahkan menjual kembali data tersebut kepada pihak yang tidak berwenang, Sehingga kebocoran data bisa terjadi akibat kelalaian individu atau *human error*, serta terlambatnya peningkatan keamanan sistem dan regulasi yang membuat lemahnya proses proteksi mengenai privasi dan data pribadi (Silalahi et al, 2023, 615).

Berdasarkan tulisan yang berjudul *"The PII Problem: Privacy and a New Concept of Personally Identifiable Information"* oleh Paul M. Schwartz dan Daniel J. Solove, kebocoran data dipandang sebagai salah satu kegagalan dalam perlindungan data pribadi. Sehingga menimbulkan risiko terhadap privasi individu maupun keamanan suatu organisasi (Schwartz & Solove, 2011). Kemudian Menurut *National Institute of Standards and Technology* (NIST), kebocoran data merupakan insiden yang

mengakibatkan pengungkapan data kepada pihak yang tidak berwenang (NIST, 2020).

Data yang bocor bisa meliputi informasi identitas individu seperti nama, alamat, nomor identitas, data keuangan, hingga data kesehatan, maupun informasi strategis milik suatu institusi. Kebocoran data tidak hanya menimbulkan risiko kerugian material seperti penipuan dan pencurian identitas, tetapi juga dapat merusak kepercayaan publik terhadap lembaga yang menyimpan atau mengelola data tersebut (LPPM, 2024).

2.2.2. Tantangan Sistemik Keamanan Siber: Kasus dan Dampak Kebocoran Data di Indonesia

Dalam kurun waktu lima tahun terakhir, Indonesia berulang kali dihadapkan pada kasus-kasus kejahatan siber, salah satunya adalah kebocoran data yang bersifat masif dan merugikan. Menurut laporan dari Databoks, terdapat berbagai sektor yang terdampak oleh kejahatan siber, mulai dari sektor administrasi pemerintahan, keuangan, kesehatan, hingga transportasi yang digunakan masyarakat dalam kehidupan sehari-hari, dan sektor yang paling banyak mengalami serangan kejahatan siber adalah sektor administrasi pemerintahan (Ahdiat, 2024).

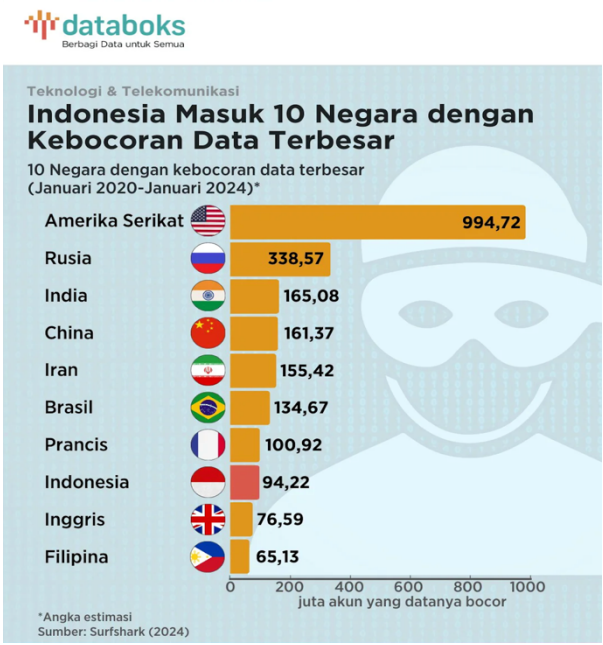
Kemudian mengutip dari laporan BSSN pada tahun 2023, terdapat 103 dugaan insiden kebocoran data yang terdeteksi di Indonesia. Sedangkan sektor yang paling banyak menjadi target serangan adalah sektor administrasi pemerintahan, dengan akumulasi sebanyak 69% atau terdapat 71 dugaan insiden yang telah terjadi (Ahdiat, 2024). Kondisi ini menunjukkan bahwa data yang dikelola oleh lembaga pemerintahan

memiliki kerentanan yang cukup tinggi dibandingkan sektor-sektor lainnya, baik karena tingginya nilai strategis informasi yang tersimpan maupun karena lemahnya sistem pengelolaan dan pengamanan data.

Berdasarkan laporan berita Kompas, pada tahun 2021 telah terjadi kebocoran data yang berasal dari BPJS Kesehatan yang merugikan sekitar 279 juta pengguna, kemudian data tersebut diperjual belikan dengan seharga 0,15 *bitcoin* yang setara dengan Rp 84,4 juta di forum daring *Raid Forums* (Gewati, 2021). Mengacu pada jurnal yang ditulis oleh Sabila dan Atman, perhatian publik telah memuncak setelah terjadinya kasus kebocoran data besar-besaran oleh aktor anonim *Bjorka* pada Agustus tahun 2022. Salah satu kasusnya telah menyebabkan bocornya 26 juta data riwayat pencarian pengguna milik PLN, dan diperjualbelikan di *Breached Forums* (Sabila dan Atman, 2025).

Kasus lainnya yang diakibatkan oleh *Bjorka* adalah kasus kebocoran data pada data pelanggan kartu SIM, yang menyebabkan bocornya 1,3 miliar data sensitif masyarakat yang mencakup nomor telepon, NIK, tanggal registrasi dan nama operator. Dugaan yang terjadi bahwa data tersebut diambil secara ilegal dari sistem pemerintah, termasuk Kementerian Komunikasi dan Informatika (Kominfo), dan data yang telah bocor dijual di forum gelap senilai USD 50.000 (Sabila dan Atman, 2025). Kemudian pada tahun 2023 terjadi kebocoran data dari data paspor yang diduga sebanyak 34 juta data pengguna (Panrb, 2023). Dan tahun 2024 terdapat kebocoran data dari Nomor Pokok Wajib Pajak (NPWP) sebanyak 6 juta data pengguna (CNBC, 2024).

Selain itu, telah terjadi kasus kebocoran data besar yang terjadi pada pertengahan Juni 2024. Kejahatan ini menargetkan Pusat Data Nasional Sementara (PDNS) yang melumpuhkan ratusan layanan publik. Serangan tersebut mengakibatkan lumpuhnya sistem penting, termasuk layanan keimigrasian di bandara, serta mengganggu operasional sekitar 210 hingga 282 instansi pemerintah (DTrust, 2025).



Gambar 2. 1 Grafik 10 negara dengan kasus kebocoran data terbesar di dunia

Sumber: Databoks, 2024

Akumulasi dari beragam peristiwa kebocoran data tersebut kemudian menjadikan Indonesia termasuk dalam jajaran negara dengan tingkat insiden kebocoran data terbesar di dunia. Bahkan, menurut catatan yang dihimpun sepanjang periode Januari 2020 hingga Januari 2024, Indonesia tercatat menduduki peringkat kedelapan secara global, dengan total sekitar 94,22 juta akun yang menjadi korban kebocoran data (Databoks, 2024). Kemudian menurut laporan dari *Goodstats* pada tahun

2024, Indonesia menempati peringkat ke tiga sebagai negara denga kasus kebocoran data terbanyak di ASEAN, dengan jumlah 21 juta kasus kebocoran data yang terjadi (Alfathi, 2025).

Melihat dari maraknya kasus kebocoran data yang terjadi di Indonesia dalam beberapa tahun terakhir, maka kerugian yang ditimbulkan tidak dapat dipandang sebagai persoalan teknis semata. Fenomena ini telah berkembang menjadi isu sosial, ekonomi, dan hukum yang secara langsung berdampak pada masyarakat luas. Oleh karena itu, penting untuk mengkaji lebih lanjut berbagai bentuk kerugian yang dialami masyarakat akibat kebocoran data, baik dari sisi material maupun nonmaterial.

Berdasarkan dari insiden kebocoran data yang terjadi, salah satunya pada PDNS tahun 2024 yang telah menimbulkan berbagai kerugian yang signifikan bagi masyarakat. Dampak yang muncul tidak hanya terbatas pada aspek teknis, tetapi juga mencakup kerugian ekonomi, sosial, psikologis, serta turunnya kepercayaan terhadap pemerintah dan penyelenggara sistem elektronik. Toding Bua dan Idris (2025) menjelaskan bahwa kebocoran data membuka peluang besar bagi pelaku kejahatan siber untuk melakukan tindak kriminal seperti pemerasan, penipuan daring, dan penyalahgunaan identitas. Masyarakat yang datanya bocor menjadi rentan terhadap pencurian identitas, peretasan akun keuangan, serta penyebaran data pribadi di forum gelap (Bua dan Idris, 2025,108).

Kemudian ditambah dengan kerugian ekonomi yang menjadi salah satu dampak paling nyata dari insiden kebocoran data. Pada insiden kebocoran data PDNS, pelaku serangan dilaporkan menuntut tebusan

sebesar 8 juta dolar AS**,** atau setara dengan Rp131 miliar, sebagai syarat pemulihan data yang dienkripsi. Lebih jauh lagi, analisis ekonomi memperkirakan bahwa gangguan operasional PDN yang berlangsung selama sekitar dua belas hari telah menyebabkan kerugian ekonomi nasional mencapai lebih dari Rp6,3 triliun akibat terhentinya berbagai layanan publik dan administratif yang bergantung pada sistem tersebut (Harris, 2024).

Dari sisi sosial dan psikologis, masyarakat mengalami peningkatan rasa cemas, tidak aman, dan kehilangan kepercayaan terhadap pemerintah sebagai pengelola data pribadi mereka (Iswenda, 2024). Kemudian menurunnya persepsi keamanan data dapat memengaruhi perilaku kepatuhan warga negara, seperti kepatuhan pajak dan partisipasi dalam program digitalisasi. Hilangnya rasa percaya ini berpotensi menghambat proses transformasi digital nasional, karena masyarakat menjadi enggan menggunakan layanan publik berbasis teknologi (Bua dan Idris, 2025,101).

Berdasarkan pernyataan pakar kemanan siber dari *Ethical Hackers Indonesia,* korban kebocoran data juga berpotensi mengalami kehilangan dana akibat penipuan daring (*phishing*) maupun penggunaan ilegal data finansial mereka (BBC, 2024). Hal ini menunjukkan bahwa kebocoran data tidak hanya menimbulkan kerugian individual, tetapi juga kerugian sistemik yang berdampak pada stabilitas ekonomi digital nasional.

Dampak dan kerugian yang sangat besar akibat insiden kebocoran data tersebut mencerminkan urgensi bagi pemerintah dan seluruh pemangku kepentingan untuk memperkuat kebijakan dan regulasi serta program untuk memperkuat perlindungan data pribadi. Dalam konteks ini,

keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam upaya memperkuat tata kelola keamanan data nasional serta memberikan landasan hukum yang lebih jelas dalam mencegah dan menanggulangi insiden serupa di masa mendatang.

2.2.3. Kerangka Regulasi Nasional: Undang Undang Perlindungan Data Pribadi

Indonesia telah memiliki regulasi mengenai kebocoran data yang diatur melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pada pasal 1, tertulis bahwa data pribadi merupakan data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik melalui sistem elektronik maupun non-elektronik (BPK, 2022).

Prinsip yang ada dalam UU PDP telah menjadi dasar dalam memproses data pribadi. Prinsip yang tertulis mencakup, akuntabilitas, transparansi, keamanan, kemudian persetujuan dari subjek data sebelum dilakukan proses data. Kemudian hak subjek data dalam UU PDP, yaitu individu yang datanya dikumpulkan dan di proses memiliki hak bahwa data tersebut digunakan secara transparan dan bertanggug jawab oleh pengelola data (Syailendra, 2025).

Individu juga memiliki hak untuk mengajukan keberatan jika data tersebut diproses untuk tujuan yang tidak sesuai dengan persetujuan awal. Walaupun UU PDP tidak menyebutkan definisi khusus tentang istilah

kebocoran data, fenomena ini dipahami sebagai bentuk kegagalan perlindungan data pribadi, di mana informasi diakses, digunakan, atau diungkapkan tanpa persetujuan pemiliknya (ELA, 2022).

Pasal 41 UU PDP mengatur kewajiban bagi pengendali data untuk memberitahukan kepada subjek data secara tertulis paling lambat tiga kali dua puluh empat jam setelah insiden kebocoran diketahui. Apabila kewajiban ini tidak dipenuhi, pengendali data dapat dikenai sanksi administratif berupa teguran, penghentian sementara kegiatan pemrosesan data, hingga pencabutan izin (Komdigi, 2022).

Selain itu, UU PDP juga mengatur sanksi pidana berupa hukuman penjara hingga tujuh tahun dan denda maksimal enam miliar rupiah bagi pihak yang menyalahgunakan data pribadi. Dengan demikian, kebocoran data dapat dipahami sebagai peristiwa yang bersifat multidimensional, karena tidak hanya terkait dengan aspek teknis seperti serangan siber, tetapi juga menyangkut aspek hukum dan etika dalam pengelolaan data pribadi (Komdigi, 2022).

Upaya penanggulangan kebocoran data tidak hanya bergantung pada regulasi nasional semata, tetapi juga diikuti dengan penguatan kapasitas dan kesadaran keamanan digital pada masyarakat. Dalam hal inilah peran BSSN sebagai lembaga yang menaungi masalah keamanan siber menjadi signifikan melalui program literasi keamanan digital yang ditujukan untuk memperkuat ketahanan siber nasional.

2.3 Literasi Keamanan Digital: Sejarah, Pengertian dan Kaitannya dengan BSSN

2.3.1. Sejarah Literasi Keamanan Digital

Literasi keamanan digital mulai berkembang seiring meningkatnya penggunaan internet pada tahun 1990-an. Pada tahun ini, keamanan siber telah memasuki fase baru dan membuat keterhubungan jaringan global sekaligus memunculkan beragam ancaman digital yang baru. Hal ini juga membuat pelaku kejahatan siber semakin berkembang dengan memanfaatkan celah dalam perangkat lunak maupun sistem untuk melakukan akses ilegal, mencuri informasi, serta mengacaukan aktivitas operasional (Maryville University, 2024).

Disusul pada dekade 2000-an, kasus pencurian identitas (*identity theft*) dan kebocoran data pribadi mulai menjadi hal yang sering terjadi kepada masyarakat. Melihat semakin masifnya kasus kejahatan siber yang terjadi di dunia global, maka literasi digital kemudian berkembang ke arah keamanan digital. Edukasi publik tidak lagi sebatas kemampuan teknis, tetapi juga keterampilan melindungi privasi, mengelola kata sandi, dan menghindari ancaman daring seperti *phishing* maupun *malware* (Kepnet, 2025).

Menurut UNESCO dalam *A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2* (2018), bahwa literasi digital merupakan kemampuan untuk mengakses, mengelola, memahami, mengintegrasikan, mengkomunikasikan, mengevaluasi, dan menciptakan informasi secara aman dan tepat melalui teknologi digital untuk

berpartisipasi dalam kehidupan ekonomi dan sosial. Literasi digital juga bukan hanya kemampuan dalam mengoperasikan perangkat digital, tetapi mencakup dimensi kognitif, sosial, dan etis (UNESCO, 2018).

Sejalan dengan itu, *European Union Agency for Cybersecurity* ENISA juga telah menegaskan bahwa literasi keamanan digital menjadi kunci untuk meningkatkan ketahanan masyarakat terhadap serangan siber. Uni Eropa telah menginisiasi *Insafe Network* dan kampanye *Safer Internet Day* untuk mengedukasi publik mengenai penggunaan internet yang aman (EC, 2025). Amerika Serikat pun mengintegrasikan literasi keamanan digital dalam strategi internasional keamanan sibernya sebagai upaya memperkuat diplomasi siber dan ketahanan global.

Sementara di level multilateral yaitu Perserikatan Bangsa-Bangsa, mengembangkan *Global Digital Compact* yang bertujuan menciptakan ekosistem digital yang aman, inklusif, dan berbasis hak asasi manusia (UN, 2024). Berbagai inisiatif global tersebut memperlihatkan bahwa literasi keamanan digital bukan hanya urusan nasional semata, melainkan juga bagian dari tata kelola siber internasional. Literasi keamanan digital dipahami sebagai instrumen strategis untuk menekan risiko kejahatan siber, memperkuat kepercayaan publik pada transformasi digital, serta menjaga stabilitas ruang siber global.

2.3.2. Literasi Keamanan Digital dalam Program BSSN: #JagaRuangSiber

Selain adanya literasi keamanan digital di tingkat global, Indonesia juga turut mengembangkan program serupa melalui BSSN. Salah satu

kampanye yang menjadi fokus utama BSSN adalah #JagaRuangSiber yang diluncurkan pada tahun 2022. Kampanye ini merupakan gerakan edukasi publik yang dirancang untuk meningkatkan kesadaran dan keterampilan masyarakat dalam menjaga keamanan aktivitas digital sehari-hari. Seperti penggunaan internet yang bijak, aman dan etis. Tujuan dibentuknya kampanye ini adalah untuk menciptakan lingkungan digital yang positif, aman dan sehat untuk menekan risiko kejahatan siber pada masyarakat. Maka dari itu, salah satu langkah yang diambil BSSN dalam merespons masalah kejahatan siber adalah dengan meningkatkan kapasitas SDM, sehingga mampu untuk menghadapi ancaman serta pengelolaan insiden siber (Diskominfo, 2022).

Kehadiran kampanye #JagaRuangSiber juga merupakan respon terhadap semakin maraknya kasus kejahatan siber di Indonesia, khususnya kebocoran data yang menimpa sektor publik maupun swasta. Fakta ini membuktikan bahwa persoalan keamanan siber tidak hanya disebabkan oleh lemahnya infrastruktur teknologi, tetapi juga oleh kurangnya kesadaran individu dalam mengelola dan melindungi informasi pribadi. Oleh karena itu, program literasi keamanan digital yang dikembangkan BSSN berfungsi sebagai upaya preventif untuk membangun budaya keamanan digital di masyarakat, sekaligus memperkuat ketahanan siber nasional.

Inisiatif literasi keamanan digital melalui kampanye #JagaRuangSiber tidak berdiri sendiri, melainkan menjadi bagian dari penerapam kerangka kerja sama internasional dengan ASEAN *Cybersecurity Cooperation Strategy* (2021–2025). Dengan menekankan

pentingnya peningkatan kapasitas masyarakat untuk menghadapi ancaman siber lintas batas.

2.4. ASEAN *Cybersecurity Cooperation Strategy* (ACCS): Sejarah dan Pengertiannya

ASEAN merupakan organisasi kerjasama regional yang terdiri dari negara-negara di Asia Tenggara yang didirikan pada 8 Agustus 1967 di Bangkok, Thailand. ASEAN terbentuk melalui deklarasi Bangkok yang didasari dari faktor sejarah, serta persamaan nasib yang telah dilalui negara-negara di Asia Tenggara setelah perang dunia II (Keling, 2011, 169). Karena hal ini, kawasan Asia Tenggara menggerakkan inisiasi untuk menciptakan rasa aman dan saling percaya dan mendorong kerjasama pembangunan kawasan. Seiring berjalannya waktu, keanggotaan ASEAN bertambah menjadi sepuluh negara dengan bergabungnya Brunei Darussalam, Vietnam, Laos, Myanmar dan Kamboja (Ulyana, 2025).

Pada Deklarasi Bangkok, tujuan pembentukan ASEAN adalah untuk meningkatkan pertumbuhan ekonomi, kemajuan sosial, perkembangan kebudayaan negara-negara anggota, serta memajukan perdamaian antara negara-negara anggota. Tujuan-tujuan tersebut tentunya tidak mudah untuk dicapai, maka dari itu ASEAN juga memiliki beberapa prinsip, yaitu; persamaan kedudukan dalam keanggotaan *(equality)*, musyawarah *(consensus and consultation)*, kepentingan bersama *(common interest)*, dan saling membantu *(solidarity)* (Purwandoko, 2012, 112).

Kemudian pada tahun 2003 terbentuk sebuah kesepakatan pada *Bali Chord II* yang menetapkan pembentukan tiga pilar utama ASEAN. Tiga pilar

tersebut yaitu, *economy community* (AEC)*, socio cultural community* (ASCC)*,* dan *political-security community* (APSC)*,* masing-masing pilar ini terbentuk untuk menangani isu-isu yang berbeda (Najmasani, 2023). ASEAN *Political Security Community* (APSC) telah dibentuk berdasarkan kerja sama serta solidaritas selama 40 tahun, lahirnya salah satu pilar ASEAN ini diawali pada tahun 1997 oleh para pemimpin ASEAN yang kemudian mengusulkan visi ASEAN 2020 untuk menciptakan masyarakat yang stabil, damai serta sejahtera (APSC Blueprint, nd).

APSC dibentuk untuk meningkatkan kerja sama politik dan keamanan antara negara-negara anggota ASEAN, dengan tiga tujuan utamanya adalah untuk mewujudkan masyarakat yang berbasis aturan dan nilai-nilai bersama, membentuk kawasan yang kohesif, aman dan stabil, serta meningkatkan peran ASEAN dalam dunia yang semakin maju dan terintegrasi. Fokus APSC adalah untuk menyelesaikan permasalahan tradisional dan non tradisional, salah satunya adalah kejahatan siber yang merupakan suatu hal yang tidak bisa dihindari oleh masyarakat terutama negara-negara anggota ASEAN (Kemlu, 2015).

Kemudian, untuk lebih memberikan fokus ASEAN dalam menindaklanjuti ancaman siber, mereka memperkenalkan strategi ASEAN *Cybersecurity Cooperation Strategy* (ACCS). Strategi ini sudah muncul pada tahun 2010 dan kemudian diperkenalkan dalam forum *Telecommunications and Informations Technology Ministers Meeting* (TELMIN) dan ASEAN *Ministerial Conference on Cybersecurity* (AMCC) (ACCS, nd).

ACCS merupakan sebuah *roadmap* kerjasama regional untuk mencapai tujuan yang sama, tujuan tersebut adalah untuk menciptakan keamanan dan perlindungan pada dunia siber di negara-negara anggota ASEAN. ACCS memiliki dua periode utama, periode pertama yaitu 2017-2020 dan periode kedua 2021-2025. Masing-masing periode memiliki fokus yang sedikit berbeda dalam menangani isu kejahatan siber, karena periode kedua diciptakan untuk menyempurnakan draf periode pertama yang sudah berjalan (Ramadhan, 2023).

ASEAN *Cybersecurity Cooperation Strategy* (ACCS) 2017-2020 memiliki fokus pada peningkatan kerjasama antar *Computer Emergency Response Team* (CERT) di negara-negara anggota ASEAN yang bertujuan untuk memperkuat respons negara anggota terhadap insiden siber yang sedang terjadi, menyediakan pelatihan dan program peningkatan kapasitas bagi tim keamanan siber di negara anggota, kemudian meningkatkan koordinasi kepada sesama negara anggota untuk saling bertukar informasi, dan membangun kerjasama internasional dengan negara mitra seperti Jepang dan China untuk meningkatkan kapasitas serta informasi terkait ancaman siber (ACCS, nd).

ASEAN *Cybersecurity Cooperation Strategy* (ACCS) 2021-2025 memiliki sedikit perbedaan dengan ACCS sebelumnya, karena periode kedua hanya menambahkan sesuai dengan perkembangan digitalisasi yang terjadi pada lima tahun terakhir serta melanjuti apa yang sudah dilaksanakan pada ACCS periode pertama. Maka fokus pada ACCS periode 2021-2025 adalah memperluas fokus dengan menekankan pentingnya pengembangan ekosistem keamanan siber yang komprehensif.

Selain melanjutkan kerja sama antar 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, nd).

Bab ini telah memaparkan gambaran umum mendorong urgensi literasi keamanan digital di Indonesia melalui BSSN. Inti temuan Bab II adalah respons terhadap kebocoran data telah berevolusi dari upaya teknis menjadi strategi peningkatan kesadaran dan kapasitas sumber daya manusia (SDM). Hal ini dicontohkan melalui kampanye #JagaRuangSiber milik BSSN di Indonesia yang menggunakan literasi keamanan digital sebagai elemen kunci ketahanan siber nasional. Serta sejalan dengan pilar *capacity building* dalam ASEAN *Cybersecurity Cooperation Strategy* (ACCS) 2021–2025.

Dengan demikian, Bab II telah menunjukan gambaran umum terkait kelembagaan BSSN serta literasi keamanan digital melalui kampanye #JagaRuangSiber sebagai salah satu respons preventif dari kasus kebocoran data, dan sebagai penerapan terhadap draf ACCS. Kemudian bab III akan berfokus pada analisis mendalam mengenai peran BSSN dalam implementasi kampanye #JagaRuangSiber kepada masyarakat sebagai penerapan indikator yang ada didalam draf ACCS.