

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Transformasi digital yang semakin berkembang dalam penyelenggaraan pelayanan publik menjadikan sistem informasi pemerintah sebagai elemen strategis dalam tata kelola pemerintahan modern. Untuk menjamin keamanan, integritas, serta ketersediaan informasi tersebut, negara membutuhkan institusi yang memiliki mandat, sumber daya, dan koordinasi yang baik dalam mengelola keamanan siber nasional. Di Indonesia, mandat tersebut berada pada Badan Siber dan Sandi Negara (BSSN), yang telah ditetapkan melalui Perpres Nomor 53 Tahun 2017 dan diperkuat melalui Perpres Nomor 133 Tahun 2017 (Republik Indonesia, 2017a, 2017b). Kehadiran BSSN menegaskan arah pembentukan arsitektur pertahanan siber nasional, termasuk pengelolaan ancaman terhadap infrastruktur informasi vital dan platform digital pemerintah.

Namun, pada Oktober 2021, terjadi insiden peretasan berupa *defacement* pada situs Pusat Malware Nasional (Pusmanas), sebuah unit yang berada di bawah koordinasi BSSN. Dalam serangan tersebut, halaman resmi situs Pusmanas sempat diganti tampilannya oleh pelaku dengan menyisipkan pesan tertentu, yang menunjukkan adanya celah keamanan pada sistem *website* milik lembaga dengan fungsi utama pertahanan siber negara. Insiden ini kemudian menjadi perhatian publik karena menyerang lembaga yang justru bertugas menjaga keamanan dan kerahasiaan informasi milik negara. Serangan *defacement* dalam konteks ini tidak

hanya bersifat teknis, tetapi menunjukkan bentuk kompromi terhadap otoritas institusional negara dalam ruang digital (Badan Siber dan Sandi Negara, 2022).

Terjadinya insiden *defacement* di lembaga sebesar BSSN menimbulkan pertanyaan terkait kemampuan institusi tersebut dalam mengakses, mengelola, dan memproteksi infrastruktur yang menjadi bagian dari sistem nasional. Secara konseptual, sebuah lembaga keamanan siber seharusnya menerapkan standar keamanan yang lebih ketat dibanding lembaga lainnya, termasuk sistem pemantauan, audit keamanan berkala, pembaruan perangkat lunak, serta mitigasi kerentanan web. Namun, fakta bahwa *defacement* dapat terjadi kepada platform resmi BSSN menunjukkan adanya kerentanan pada aspek tata kelola keamanan teknologi informasi yang tidak hanya bersumber dari faktor teknis, tetapi juga dari manajemen risiko, koordinasi internal, hingga kapasitas sumber daya manusia. Kondisi tersebut sejalan dengan Adma et al. (2023) yang menunjukkan bahwa penguatan ketahanan siber Indonesia masih menghadapi tantangan pada aspek talenta digital, infrastruktur teknologi informasi dan komunikasi, sistem pengelolaan keamanan digital, serta keterbatasan pendanaan. (Adma et al., 2023).

Selain itu, serangan ini mengundang persoalan terkait tata kelola informasi publik. Situs Pusmanas memiliki fungsi strategis dalam memberikan publikasi dan edukasi terkait ancaman *malware*, basis pengetahuan, dan riset teknis keamanan. Ketika platform tersebut diretas dan diubah tampilannya, terdapat potensi gangguan terhadap kepercayaan publik terhadap fungsi penyuluhan dan edukasi digital pemerintah. Keamanan informasi bukan semata kondisi bebas ancaman, tetapi

menyangkut kepercayaan publik terhadap kemampuan negara melindungi data, sistem publik, dan kedaulatan digital.

Di sisi lain, insiden ini juga menyoroti lemahnya pendekatan respons insiden pemerintah. Tidak terdapat publikasi yang komprehensif terkait langkah penanganan, investigasi teknis, maupun prosedur pemulihan sistem pasca insiden. Kurangnya transparansi ini menimbulkan pertanyaan tambahan mengenai kesiapan struktur komando dan mekanisme krisis dalam menghadapi serangan terhadap institusi digital negara. Padahal, salah satu prinsip yang dianut dalam manajemen insiden siber adalah transparansi prosedural untuk menjaga akuntabilitas serta meningkatkan resiliensi sistem.

Melalui fenomena ini, menarik untuk menganalisis bagaimana peran BSSN dalam menangani insiden tersebut, baik dari perspektif teknis, kelembagaan, maupun kebijakan. Dengan menggunakan pendekatan studi kasus terhadap insiden *defacement* situs Pusmanas, penelitian ini dapat memetakan tahapan respons, mengidentifikasi kelemahan struktural dalam tata kelola keamanan siber, serta memberikan gambaran nyata mengenai kapasitas pertahanan digital negara. Penelitian ini tidak hanya relevan secara akademis, tetapi juga secara praktis, mengingat tingginya frekuensi ancaman peretasan terhadap situs pemerintah dan tingginya tuntutan terhadap keamanan digital yang profesional dan terstandarisasi (Nurhayati, 2023).



Grafik 1.1. Jumlah Serangan Siber yang terjadi di Indonesia
 (Sumber: AwanPintar.id, 2024)

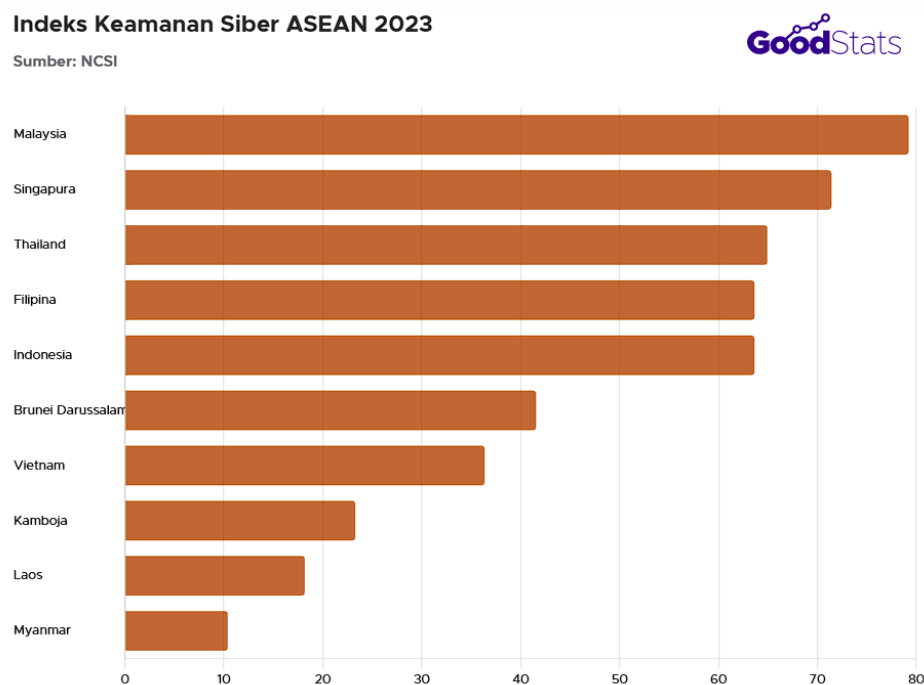
Melihat kondisi ini, sangat penting untuk melakukan kajian yang lebih mendalam mengenai situasi terkini, khususnya terkait dampak yang dirasakan masyarakat dan sektor-sektor penting. Di era digital yang semakin maju, risiko keamanan terus meningkat, dan serangan siber kerap menargetkan sektor-sektor vital seperti pemerintahan, perbankan, dan infrastruktur publik (Fikrie, 2024). Oleh karena itu, penelitian ini akan berfokus pada analisis permasalahan keamanan yang dihadapi Indonesia saat ini, terutama yang berhubungan dengan insiden-insiden

siber yang berpengaruh besar terhadap stabilitas dan operasional sektor-sektor tersebut.

Penelitian ini tidak hanya akan mengidentifikasi berbagai ancaman yang telah terjadi, tetapi juga menggali lebih dalam mengenai dampak jangka pendek dan jangka panjang dari serangan tersebut, termasuk hilangnya kepercayaan publik, kerugian finansial, serta implikasi bagi keamanan nasional. Dengan demikian, pemahaman yang lebih mendalam mengenai bagaimana ancaman siber mempengaruhi masyarakat dan institusi akan menjadi dasar dalam merumuskan strategi perlindungan dan mitigasi yang lebih baik di masa mendatang. Selain itu, penelitian ini juga akan membahas langkah-langkah yang dapat diambil oleh pemerintah, perusahaan, dan masyarakat untuk memperkuat perlindungan di era digital. Pemerintah diharapkan dapat memperkuat kebijakan dan regulasi yang ada, memastikan infrastruktur keamanan siber yang lebih tangguh, dan meningkatkan kesadaran publik terhadap pentingnya keamanan digital. Dari sisi perusahaan, penting bagi mereka untuk menginvestasikan lebih banyak sumber daya dalam teknologi keamanan dan memberikan pelatihan kepada karyawan untuk meningkatkan kesadaran akan ancaman siber. Masyarakat pun harus didorong untuk lebih memahami risiko yang muncul dari penggunaan teknologi, dan lebih aktif dalam melindungi data pribadi mereka.

Urgensi dari penelitian ini sangat penting, melihat pada kenyataannya yang semakin besar ketergantungan Indonesia terhadap teknologi digital di hampir semua sektor kehidupan mulai dari pemerintahan, layanan publik, kesehatan, pendidikan, hingga sektor ekonomi. Di tengah percepatan transformasi digital,

Indonesia justru dihadapkan pada lonjakan ancaman siber yang signifikan, seperti kebocoran data, *ransomware*, dan serangan terhadap infrastruktur kritis (Kementerian Komunikasi dan Informatika, 2024). Ancaman-ancaman ini tidak hanya mengganggu sistem operasional, tetapi juga berpotensi meruntuhkan kepercayaan masyarakat terhadap institusi negara, terutama jika data pribadi warga bocor atau layanan publik terganggu. Hal ini menciptakan risiko serius terhadap keamanan nasional, karena serangan siber dapat memberikan konsekuensi terhadap pertahanan dan keamanan negara (Hastri, 2021).

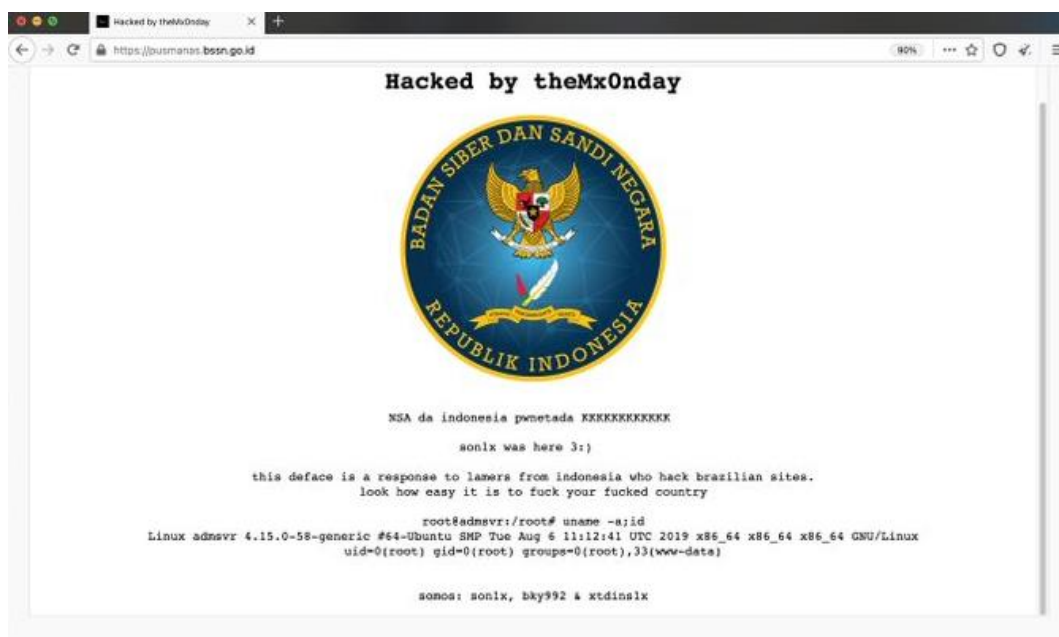


Grafik 1.2. Indeks Keamanan Siber ASEAN
(Sumber: Agnes Z Yonatan, 2023)

Berdasarkan Grafik 2. dari *Global Cybersecurity Index (GCI) 2024* yang dirilis oleh *International Telecommunication Union (ITU)*, Indonesia berhasil mencapai *Tier 1* (International Telecommunication Union [ITU], 2024), kategori

tertinggi yang menunjukkan komitmen kuat terhadap keamanan siber. Pencapaian ini menempatkan Indonesia sejajar dengan negara-negara seperti Amerika Serikat dan Jepang dalam hal keamanan siber. Di tingkat regional, menurut *National Cyber Security Index* (NCSI) 2023, Indonesia memperoleh skor 63,64 dari 100 poin, menempatkannya di posisi keempat di ASEAN setelah Malaysia, Singapura, dan Thailand (National Cyber Security Index [NCSI], 2023).

Penelitian ini diharapkan dapat menghasilkan rekomendasi strategis yang bermanfaat untuk memperkuat ketahanan siber di Indonesia, dengan fokus pada kolaborasi antara pemerintah, sektor swasta, dan masyarakat. Selain memberikan solusi jangka pendek, penelitian ini juga bertujuan untuk memberikan pandangan jangka panjang terkait pengembangan keamanan siber yang lebih efektif dan berkelanjutan, guna menghadapi tantangan-tantangan yang terus berkembang di masa depan.



Gambar 1.1. Web BSSN Selama di Retas oleh Hacker

Berikut adalah tampilan di web BSSN selama di hack oleh *Hacker* asal brazil ini, web ini *Suspend* oleh pihak BSSN untuk diperbaiki dan kejadian ini berlangsung selama 2 hari

1.2. Rumusan Masalah

Dari penjelasan latar belakang mengenai kesiapan keamanan siber di indonesia ini, maka telah dirumuskan permasalahan masalah (*Research Question*):

1. Bagaimana faktor implementasi kebijakan mempengaruhi efektivitas respons BSSN dalam kasus serangan Web *Defacement*?

1.3. Tujuan Penelitian

1.3.1. Tujuan Umum

Tujuan dari peneliti menulis untuk menjawab rumusan masalah, dengan menganalisis kondisi keamanan siber di Indonesia dengan memfokuskan pada insiden-insiden yang telah mempengaruhi sektor vital, seperti pemerintahan, dan infrastruktur publik. Peneliti juga mencari kekurangan dari keamanan siber dari negara Indonesia sehingga bisa mengusulkan strategi mitigasi jangka panjang untuk menghadapi tantangan keamanan siber di masa depan.

1.3.2. Tujuan Khusus

Penelitian ini bertujuan untuk mengkaji berbagai insiden keamanan siber yang telah mempengaruhi sektor-sektor vital di Indonesia, seperti pemerintahan, dan infrastruktur publik. Selain itu, penelitian ini juga bertujuan untuk mengidentifikasi berbagai kelemahan yang masih terdapat dalam sistem keamanan siber nasional. Berdasarkan temuan-temuan

tersebut, penelitian ini diharapkan dapat merumuskan strategi mitigasi jangka panjang yang relevan dan mampu menjawab tantangan keamanan siber yang terus berkembang di masa depan.

1.4. Manfaat Penelitian

1.4.1. Manfaat Akademis

Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan literatur dan kajian di bidang keamanan siber, khususnya dalam konteks negara berkembang seperti Indonesia. Dengan menganalisis ancaman, dampak, dan strategi mitigasi keamanan siber, penelitian ini akan menambah wawasan akademis dalam upaya membangun ketahanan siber yang lebih baik. Hasil penelitian ini juga dapat menjadi referensi bagi peneliti lainnya yang ingin mendalami topik keamanan siber, khususnya terkait kebijakan, regulasi, dan pengembangan infrastruktur keamanan di negara berkembang.

1.4.2. Manfaat Praktis

Bagi Pemerintah, Penelitian ini diharapkan dapat memberikan rekomendasi strategis yang bermanfaat bagi pemerintah Indonesia dalam memperkuat kebijakan dan regulasi di bidang keamanan siber, meningkatkan efektivitas perlindungan data publik, dan mengurangi resiko serangan siber yang berdampak pada pelayanan pemerintahan dan infrastruktur publik.

Bagi Perusahaan, Penelitian ini dapat membantu sektor swasta, khususnya perusahaan yang bergerak di bidang teknologi informasi dan

komunikasi, untuk lebih memahami ancaman keamanan siber yang dihadapi. Dengan rekomendasi yang diberikan, perusahaan dapat meningkatkan sistem keamanan internal, menerapkan pelatihan siber untuk karyawan, dan memperkuat infrastruktur digital mereka.

Bagi Masyarakat, Penelitian ini dapat meningkatkan kesadaran masyarakat terhadap pentingnya keamanan siber dalam kehidupan sehari-hari. Masyarakat diharapkan dapat lebih waspada terhadap ancaman siber dan memahami pentingnya menjaga data pribadi serta menerapkan langkah-langkah proteksi yang tepat.

1.5. Kerangka Pemikiran Teoritis

1.5.1. Literature Review

Dalam rangka mendukung pelaksanaan penelitian ini, penulis memerlukan sejumlah sumber referensi yang relevan dan kredibel guna memperkuat landasan teoritis serta mempertajam analisis terhadap isu yang diangkat. Penelitian ini berfokus pada efektivitas keamanan siber Indonesia dalam menghadapi serangan siber global, khususnya yang mengancam infrastruktur vital dan sulit dilacak asal usulnya. Oleh karena itu, kajian terhadap berbagai literatur terdahulu menjadi langkah awal yang penting untuk memahami sejauh mana kesiapan Indonesia dalam merespons dinamika ancaman siber yang semakin kompleks dan transnasional.

Tinjauan pustaka ini disusun dengan mempertimbangkan keterkaitannya terhadap rumusan masalah yang telah ditetapkan, terutama yang berhubungan dengan kapasitas kelembagaan, kerangka regulasi, kerja

sama internasional, serta kesadaran masyarakat dalam menghadapi risiko siber. Selain itu, penelusuran literatur juga bertujuan untuk mengidentifikasi ruang kosong (*research gap*) yang belum banyak dibahas dalam penelitian sebelumnya, seperti efektivitas implementasi kebijakan di tingkat lokal, tantangan koordinasi antar lembaga, dan rendahnya literasi digital di kalangan masyarakat umum. Dengan demikian, kajian pustaka ini tidak hanya menjadi pijakan konseptual, tetapi juga sebagai dasar untuk membangun argumen yang logis dan sistematis dalam pembahasan penelitian ini. Berikut akan diuraikan beberapa literatur terdahulu yang menjadi acuan utama dalam penyusunan penelitian ini.

Literatur pertama dari Rosy (2020) dalam penelitiannya membahas tentang kerjasama internasional Indonesia dalam memperkuat keamanan nasional melalui penguatan keamanan siber. Dengan menggunakan pendekatan teori Lykke yang memisahkan strategi menjadi unsur *ends*, *means*, dan *ways*, peneliti mengadaptasinya menjadi pendekatan 4T (*Tolerate, Treat, Transfer, Terminate*) untuk mitigasi risiko siber. Penelitian ini menggunakan metode kualitatif deskriptif berbasis tinjauan pustaka. Hasilnya menunjukkan bahwa kelemahan utama Indonesia berada pada regulasi dan rendahnya kesadaran masyarakat terkait keamanan siber. Penelitian ini menekankan pentingnya kerja sama internasional, peningkatan SDM di bidang siber, serta penguatan regulasi untuk menghadapi ancaman siber secara strategis.

Literatur terdahulu yang kedua yaitu dari Eko Budi (2021) mengkaji strategi penguatan keamanan siber Indonesia dalam konteks era *Society 5.0* yang penuh dengan perkembangan teknologi digital. Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan analitis melalui studi pustaka terhadap berbagai sumber sekunder. Hasil kajian menunjukkan bahwa Indonesia tengah berada dalam kondisi darurat keamanan siber, yang ditandai dengan maraknya serangan seperti kebocoran data pengguna dan peningkatan serangan ransomware selama pandemi. Peneliti menyoroti lemahnya pemahaman para penyelenggara negara tentang pentingnya keamanan siber serta ketiadaan dasar hukum yang kuat. Oleh karena itu, dibutuhkan strategi nasional yang komprehensif untuk memperkuat ketahanan siber.

Literatur ketiga dari Tamarell Vimy (2022) menganalisis kapasitas keamanan siber Indonesia dan pentingnya kerjasama internasional sebagai bagian dari strategi memperkuat keamanan nasional. Melalui metode kualitatif deskriptif berbasis studi pustaka, penelitian ini menunjukkan bahwa meskipun ancaman siber meningkat seiring perkembangan teknologi dan internet, kapasitas teknis dan regulasi di Indonesia masih perlu ditingkatkan. Sejak pembentukan BSSN, Indonesia mulai aktif menjalin kerjasama bilateral dengan negara seperti Belanda dan Inggris, serta multilateral melalui ASEAN dan ARF. Namun, kolaborasi internasional tersebut harus dibarengi dengan penguatan internal dalam bentuk pengembangan SDM dan kebijakan nasional yang kuat.

Literatur yang kelima berasal dari penulis yang bernama Vincha dan Satrio (2024) membahas dampak kehadiran teknologi 5G terhadap ketahanan siber Indonesia. Penelitian ini menggunakan pendekatan kualitatif eksploratif dengan teknik wawancara bersama pejabat BSSN dan pengamat keamanan siber, serta studi pustaka dari berbagai sumber seperti jurnal, berita, dan laporan. Hasil penelitian menunjukkan bahwa 5G menghadirkan tantangan baru karena kompleksitas jaringannya dan banyaknya perangkat yang terhubung, yang meningkatkan risiko serangan dari aktor negara maupun non-negara. Selain itu, sifat *dual-use* dari teknologi 5G menimbulkan dilema keamanan tersendiri. Oleh karena itu, diperlukan strategi keamanan siber yang adaptif, penguatan regulasi, peningkatan kapasitas SDM, dan perluasan kerjasama internasional untuk mengantisipasi ancaman yang bersifat global.

Penelitian selanjutnya dilakukan oleh Adma et al. (2023) yang membahas transformasi sistem pertahanan siber Indonesia dengan menempatkan BSSN sebagai poros utama dalam penguatan sistem pertahanan siber nasional. Penelitian tersebut menunjukkan bahwa penguatan ketahanan siber Indonesia masih menghadapi tantangan pada aspek talenta digital, infrastruktur teknologi informasi dan komunikasi, sistem pengelolaan keamanan digital, serta keterbatasan pendanaan. Penelitian ini relevan dengan kajian yang dilakukan karena menunjukkan bahwa efektivitas keamanan siber tidak hanya dipengaruhi oleh keberadaan institusi, tetapi juga oleh kapasitas kelembagaan dan sumber daya yang

dimiliki. Namun, penelitian Adma et al. lebih berfokus pada transformasi sistem pertahanan siber secara makro, sedangkan penelitian ini berfokus pada implementasi kebijakan dalam respons BSSN terhadap kasus spesifik web defacement Pusmanas tahun 2021. (Adma et al., 2023).

Simbolon et al. (2021) mengkaji kejahatan siber dalam penyelenggaraan perdagangan berbasis sistem elektronik serta kebutuhan akan koordinasi antar kementerian dan lembaga dalam pengamanan ruang siber. Penelitian tersebut menunjukkan bahwa ancaman siber yang bersifat multidimensional membutuhkan koordinasi lintas lembaga dan kejelasan pembagian kewenangan agar kebijakan keamanan dapat diimplementasikan secara efektif. Penelitian tersebut relevan dengan penelitian ini karena memperkuat pentingnya koordinasi kelembagaan dalam implementasi keamanan siber. Perbedaannya, penelitian Simbolon et al. berfokus pada keamanan dalam perdagangan berbasis sistem elektronik, sedangkan penelitian ini mengkaji implementasi kebijakan pada lembaga keamanan siber melalui kasus Pusmanas. (Simbolon et al., 2021).

Kelima jurnal yang ditinjau memberikan gambaran komprehensif mengenai upaya Indonesia dalam memperkuat keamanan nasional melalui keamanan siber. Jurnal pertama membahas pentingnya *capacity building*, regulasi tindak pidana siber, dan penguatan SDM di era *Society 5.0*. Jurnal kedua menyoroti peran diplomasi siber dan kerja sama internasional dalam memperkuat infrastruktur dan pertukaran informasi. Jurnal ketiga mengulas

peran Badan Siber dan Sandi Negara (BSSN) sebagai koordinator utama kebijakan dan kerja sama keamanan siber nasional.

Berdasarkan literatur terdahulu, kajian mengenai keamanan siber Indonesia telah banyak membahas penguatan kapasitas kelembagaan, pengembangan sistem pertahanan siber, koordinasi antarinstansi, serta dampak cybercrime terhadap keamanan nasional. Namun, masih terbatas penelitian yang secara spesifik mengkaji kesenjangan antara standar kebijakan atau regulasi keamanan siber dengan implementasinya pada tingkat institusi melalui studi kasus konkret. Oleh karena itu, penelitian ini berfokus pada kasus web defacement situs Pusmanas tahun 2021 untuk melihat sejauh mana kebijakan keamanan siber diterjemahkan ke dalam proses pencegahan, respons, pemulihan, dan evaluasi BSSN.

1.5.2. Crisis Management Theory

Crisis Management Theory merupakan teori yang menjelaskan bagaimana suatu organisasi atau institusi mengelola suatu krisis secara sistematis untuk meminimalkan dampak yang ditimbulkan serta memulihkan kondisi organisasi setelah krisis terjadi. Menurut Ian I. Mitroff, krisis bukan merupakan peristiwa yang terjadi secara tiba-tiba, melainkan suatu proses yang memiliki tahapan tertentu sehingga dapat diantisipasi dan dikelola melalui mekanisme manajemen krisis yang tepat. Oleh karena itu, keberhasilan suatu organisasi dalam menghadapi krisis tidak hanya diukur dari kemampuannya menyelesaikan permasalahan ketika krisis

berlangsung, tetapi juga dari kesiapan dalam melakukan pencegahan sebelum krisis terjadi serta evaluasi setelah krisis berakhir.

Dalam konteks keamanan siber, teori ini relevan karena serangan siber, termasuk web *defacement*, merupakan bentuk krisis yang dapat mengganggu keberlangsungan operasional organisasi, menurunkan kredibilitas institusi, serta mengurangi kepercayaan publik terhadap kemampuan pemerintah dalam melindungi sistem elektronik nasional. Oleh karena itu, respons terhadap insiden keamanan siber memerlukan pendekatan yang terstruktur agar dampak yang ditimbulkan dapat diminimalkan sekaligus menjadi dasar perbaikan kebijakan di masa mendatang.

Dalam kerangka Crisis Management Theory, penanganan kasus *defacement* dapat dianalisis melalui empat tahapan utama, yaitu *pre-crisis stage*, *acute crisis stage*, *chronic stage*, dan *resolution stage*. Tahap pertama, *pre-crisis stage*, merupakan fase pencegahan yang bertujuan mengurangi kemungkinan terjadinya krisis. Pada tahap ini organisasi dituntut untuk melakukan identifikasi risiko (*risk assessment*), pemetaan aset digital yang bersifat kritis, audit keamanan secara berkala, *vulnerability assessment*, *penetration testing*, pemantauan lalu lintas jaringan (*network monitoring*), serta penyusunan dan pengujian Standard Operating Procedure (SOP) penanganan insiden siber. Selain itu, peningkatan kapasitas sumber daya manusia melalui pelatihan keamanan siber dan simulasi penanganan insiden (*cyber drill*) juga menjadi bagian penting dalam membangun kesiapsiagaan

organisasi. Dalam penelitian ini, tahap *pre-crisis* digunakan untuk menganalisis sejauh mana kesiapan BSSN dalam mengantisipasi ancaman terhadap situs Pusat Malware Nasional sebelum insiden *defacement* terjadi.

Tahap kedua adalah *acute crisis stage*, yaitu fase ketika krisis sedang berlangsung dan memerlukan respons yang cepat, tepat, dan terkoordinasi. Fokus utama pada tahap ini adalah membatasi dampak serangan agar tidak menyebar ke sistem lain, menjaga keberlangsungan layanan, serta memberikan informasi yang akurat kepada publik. Dalam konteks kasus Pusmanas, indikator yang dianalisis meliputi kecepatan respons BSSN dalam mendeteksi serangan, tindakan isolasi terhadap sistem yang terdampak, aktivasi BSSN-CSIRT dalam melakukan penanganan insiden, proses investigasi awal terhadap sumber serangan, serta strategi komunikasi publik yang dilakukan BSSN selama penanganan krisis. Efektivitas respons pada tahap ini menjadi salah satu indikator utama dalam menilai kemampuan institusi mengendalikan dampak insiden keamanan siber.

Tahap ketiga adalah *chronic stage*, yaitu fase ketika kondisi krisis mulai terkendali, tetapi proses penanganan masih terus berlangsung. Pada tahap ini organisasi melakukan investigasi digital forensik untuk mengidentifikasi penyebab terjadinya insiden, celah keamanan yang berhasil dieksploitasi, metode serangan yang digunakan pelaku, serta potensi dampak lanjutan terhadap sistem lainnya. Selain itu, dilakukan pula proses pemulihan layanan (*system recovery*), peningkatan keamanan sistem, pembaruan perangkat lunak, serta evaluasi terhadap efektivitas respons yang

telah dilakukan. Dalam penelitian ini, tahap *chronic stage* digunakan untuk menilai bagaimana BSSN melakukan proses pemulihan dan penguatan sistem setelah insiden *defacement* berhasil dikendalikan.

Tahap terakhir adalah *resolution stage*, yaitu fase penyelesaian krisis ketika sistem telah kembali beroperasi secara normal dan organisasi melakukan evaluasi menyeluruh terhadap keseluruhan proses penanganan krisis. Hasil evaluasi tersebut umumnya menjadi dasar dalam penyempurnaan kebijakan, pembaruan SOP, peningkatan standar keamanan informasi, penguatan koordinasi antarinstansi, serta penyusunan strategi mitigasi guna mencegah terulangnya insiden serupa. Dalam konteks penelitian ini, tahap *resolution stage* digunakan untuk menganalisis apakah insiden *defacement* terhadap situs Pusmanas mendorong adanya perubahan kebijakan, peningkatan tata kelola keamanan siber, maupun langkah-langkah perbaikan yang dilakukan oleh BSSN setelah krisis berakhir.

Berdasarkan penjelasan tersebut, *Crisis Management Theory* digunakan sebagai indikator analisis untuk mengevaluasi efektivitas respons BSSN terhadap insiden *defacement* situs Pusat Malware Nasional tahun 2021. Melalui empat tahapan manajemen krisis, penelitian ini tidak hanya menilai tindakan BSSN saat krisis berlangsung, tetapi juga mengidentifikasi tingkat kesiapsiagaan sebelum krisis, efektivitas proses pemulihan setelah krisis, serta berbagai pembelajaran yang dihasilkan guna memperkuat tata kelola keamanan siber nasional.

1.6. Operasionalisasi Konsep

1.6.1. Definisi Konseptual

Definisi konseptual merupakan penjelasan mengenai makna suatu konsep berdasarkan teori atau literatur yang menjadi landasan penelitian (Nindita, 2023). Dalam penelitian ini, konsep utama yang digunakan adalah keamanan siber (cyber security) dan manajemen krisis (crisis management).

Keamanan siber didefinisikan sebagai serangkaian upaya yang dilakukan untuk melindungi sistem komputer, jaringan, perangkat, serta data dari berbagai bentuk ancaman siber seperti peretasan (hacking), malware, ransomware, phishing, maupun bentuk serangan siber lainnya yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Dalam konteks penelitian ini, keamanan siber dipahami sebagai kemampuan suatu institusi, khususnya Badan Siber dan Sandi Negara (BSSN), dalam menjaga keamanan sistem elektronik pemerintah dari berbagai ancaman yang dapat mengganggu keberlangsungan layanan digital negara. Selain konsep keamanan siber, penelitian ini juga menggunakan *Crisis Management Theory* sebagai kerangka analisis utama. Menurut Ian I. Mitroff, manajemen krisis merupakan suatu proses sistematis yang dilakukan organisasi dalam mengantisipasi, merespons, memulihkan, dan mengevaluasi suatu krisis agar dampak yang ditimbulkan dapat diminimalkan. Teori ini membagi proses manajemen krisis ke dalam empat tahapan utama, yaitu *pre-crisis stage*, *acute crisis stage*, *chronic stage*, dan *resolution stage*. Keempat tahapan tersebut digunakan untuk menjelaskan

bagaimana suatu organisasi mempersiapkan diri sebelum krisis terjadi, melakukan respons saat krisis berlangsung, melaksanakan proses pemulihan, serta melakukan evaluasi guna mencegah terulangnya krisis di masa mendatang.

1.6.1.1. *Crisis Management Theory*

Crisis Management Theory merupakan kerangka yang digunakan untuk memahami bagaimana suatu organisasi mempersiapkan diri, menghadapi, mengendalikan, dan memulihkan kondisi setelah terjadinya suatu krisis. Manajemen krisis tidak hanya berkaitan dengan tindakan yang dilakukan ketika krisis berlangsung, tetapi merupakan suatu proses yang mencakup kondisi sebelum, selama, dan setelah krisis. Dalam proses tersebut, organisasi dituntut untuk memiliki kemampuan dalam mengenali potensi ancaman, mempersiapkan respons, mengambil tindakan ketika krisis terjadi, serta melakukan evaluasi dan pembelajaran setelah krisis berakhir.

Dalam penelitian ini, *Crisis Management Theory* digunakan untuk memahami proses penanganan krisis keamanan siber yang terjadi pada situs Pusat Malware Nasional (Pusmanas). Teori ini digunakan karena insiden web *defacement* tidak hanya dapat dilihat sebagai permasalahan teknis, tetapi juga sebagai suatu kondisi krisis yang membutuhkan kesiapan, respons, pemulihan, dan evaluasi dari organisasi yang terdampak. Untuk melihat proses tersebut secara lebih sistematis, penelitian ini menggunakan empat tahapan dalam

manajemen krisis, yaitu *pre-crisis stage*, *acute crisis stage*, *chronic stage*, dan *resolution stage*.

1.6.1.2. *Pre-Crisis Stage*

Pre-Crisis Stage merupakan tahap yang berlangsung sebelum suatu krisis terjadi. Tahap ini berkaitan dengan kondisi kesiapan organisasi dalam menghadapi kemungkinan munculnya krisis serta berbagai upaya yang dilakukan untuk mencegah atau mengurangi dampak dari ancaman yang berpotensi terjadi. Pada tahap ini, organisasi melakukan proses persiapan dan pengenalan terhadap berbagai risiko yang dapat mengganggu aktivitas maupun fungsi organisasi.

Dengan demikian, *Pre-Crisis Stage* menggambarkan bagaimana suatu organisasi mempersiapkan diri sebelum menghadapi kondisi krisis. Tahap ini menjadi bagian penting dalam manajemen krisis karena tingkat kesiapan sebelum krisis dapat memengaruhi kemampuan organisasi dalam memberikan respons ketika suatu ancaman benar-benar terjadi.

1.6.1.3. *Acute Crisis Stage*

Acute Crisis Stage merupakan tahap ketika suatu krisis telah terjadi dan organisasi harus memberikan respons secara langsung terhadap kondisi tersebut. Tahap ini ditandai dengan munculnya situasi yang membutuhkan tindakan cepat untuk mengendalikan krisis dan mencegah meluasnya dampak yang ditimbulkan. Pada

tahap ini, organisasi berada dalam kondisi yang membutuhkan proses pengambilan keputusan dan tindakan untuk menangani situasi yang sedang berlangsung.

Dalam konteks manajemen krisis, *Acute Crisis Stage* menjadi tahapan yang berfokus pada penanganan langsung terhadap krisis. Kemampuan organisasi dalam merespons kondisi tersebut menjadi penting karena tindakan yang dilakukan pada tahap ini menentukan bagaimana krisis dapat dikendalikan sebelum memasuki proses penanganan dan pemulihan lebih lanjut.

1.6.1.4. *Chronic Stage*

Chronic Stage merupakan tahap setelah kondisi krisis mulai dapat dikendalikan dan organisasi memasuki proses penanganan lanjutan. Tahap ini berkaitan dengan proses pemulihan, investigasi, serta pemahaman terhadap penyebab dan dampak yang ditimbulkan oleh krisis. Organisasi pada tahap ini tidak lagi hanya berfokus pada penghentian krisis, tetapi mulai melakukan upaya untuk mengembalikan kondisi organisasi dan memahami berbagai faktor yang berkaitan dengan terjadinya krisis.

Tahap *chronic* juga menjadi bagian dari proses pembelajaran organisasi karena hasil dari investigasi dan pemulihan dapat memberikan pemahaman mengenai kelemahan yang terdapat dalam proses penanganan sebelumnya. Dengan demikian, tahap ini

menjadi penghubung antara penanganan krisis dengan proses evaluasi dan penyelesaian krisis secara menyeluruh.

1.6.1.5. *Resolution Stage*

Resolution stage merupakan tahap akhir dalam proses manajemen krisis ketika kondisi krisis telah berhasil diselesaikan dan organisasi mulai kembali menjalankan aktivitasnya secara normal. Pada tahap ini, perhatian organisasi tidak hanya diarahkan pada pemulihan kondisi, tetapi juga pada evaluasi terhadap keseluruhan proses penanganan krisis yang telah dilakukan.

Tahap resolution juga berkaitan dengan proses pembelajaran dari pengalaman krisis. Hasil evaluasi dapat digunakan oleh organisasi untuk memahami kekurangan dalam penanganan krisis serta melakukan perbaikan agar organisasi memiliki kesiapan yang lebih baik dalam menghadapi kemungkinan krisis di masa mendatang. Dengan demikian, berakhirnya suatu krisis tidak hanya ditandai dengan kembalinya kondisi organisasi seperti semula, tetapi juga dengan adanya proses pembelajaran yang dapat meningkatkan kemampuan organisasi dalam menghadapi krisis berikutnya.

1.6.2. Definisi Operasional

Definisi operasional merupakan penjabaran mengenai bagaimana suatu konsep digunakan sebagai alat analisis dalam penelitian. Dalam penelitian ini, konsep manajemen krisis dioperasionalkan berdasarkan empat tahapan dalam *Crisis Management Theory* yang digunakan untuk

menganalisis respons Badan Siber dan Sandi Negara (BSSN) terhadap insiden *defacement* situs Pusat Malware Nasional (Pusmanas) tahun 2021.

Operasionalisasi konsep dilakukan melalui indikator-indikator sebagai berikut.

Tahapan Crisis Management Theory	Indikator Operasional
<i>Pre-Crisis Stage</i>	Identifikasi risiko, audit keamanan sistem, vulnerability assessment, penetration testing, monitoring sistem, kesiapan SOP, kesiapan sumber daya manusia, serta upaya mitigasi sebelum insiden terjadi.
<i>Acute Crisis Stage</i>	Kecepatan respons BSSN, isolasi sistem yang terdampak, aktivasi BSSN-CSIRT, investigasi awal, koordinasi antarinstansi, serta komunikasi publik selama penanganan insiden.
<i>Chronic Stage</i>	Proses digital forensik, identifikasi penyebab serangan, pemulihan sistem (<i>system recovery</i>), peningkatan keamanan infrastruktur, serta evaluasi terhadap efektivitas penanganan insiden.
<i>Resolution Stage</i>	Evaluasi pasca-insiden, pembaruan SOP, penyempurnaan kebijakan keamanan siber, peningkatan kapasitas SDM, serta penerapan <i>lessons learned</i> untuk mencegah terulangnya insiden serupa.

Tabel 1.1. Indikator Operasional Crisis Management Theory

Berdasarkan indikator tersebut, penelitian ini menganalisis efektivitas respons BSSN terhadap insiden *defacement* situs Pusat Malware Nasional melalui setiap tahapan manajemen krisis. Dengan demikian, operasionalisasi konsep tidak hanya digunakan untuk menggambarkan

tindakan yang dilakukan BSSN selama penanganan insiden, tetapi juga untuk menilai sejauh mana setiap tahapan dalam *Crisis Management Theory* telah diterapkan dalam praktik.

1.6.2.1. Crisis Management Theory

Crisis Management Theory merupakan konsep yang digunakan dalam penelitian ini untuk menjelaskan bagaimana suatu institusi mengelola sebuah krisis, termasuk krisis yang berkaitan dengan keamanan siber, mulai dari fase sebelum krisis terjadi hingga fase pemulihan sepenuhnya. Secara konseptual, teori ini memandang krisis bukan sebagai peristiwa tunggal yang berdiri sendiri, melainkan sebagai sebuah proses berkelanjutan yang terdiri atas beberapa tahapan yang saling berkaitan satu sama lain. Dalam penelitian ini, *Crisis Management Theory* dioperasionalkan melalui empat tahapan utama, yaitu *Pre-Crisis Stage*, *Acute Crisis Stage*, *Chronic Stage*, dan *Resolution Stage*.

Pre-Crisis Stage dioperasionalkan sebagai tahap kesiapan institusi sebelum krisis terjadi, yang tercermin dari ada atau tidaknya sistem deteksi dini, kegiatan monitoring risiko secara berkala, serta kesiapan prosedur operasional standar dalam menghadapi potensi ancaman. *Acute Crisis Stage* dioperasionalkan sebagai tahap ketika krisis sedang berlangsung, yang diukur melalui kecepatan dan ketepatan tindakan awal yang diambil institusi, seperti isolasi sistem yang terdampak dan pelacakan sumber ancaman. *Chronic Stage*

dioperasionalkan sebagai tahap pemulihan dan investigasi, yang dilihat dari proses penelusuran penyebab krisis secara mendalam serta langkah perbaikan yang dilakukan terhadap sistem yang terdampak. Sementara itu, *Resolution Stage* dioperasionalkan sebagai tahap akhir dari siklus krisis, yang ditandai dengan pulihnya kondisi secara menyeluruh serta munculnya pembelajaran institusional berupa kebijakan atau prosedur baru sebagai hasil evaluasi. Keempat tahapan ini menjadi kerangka acuan utama dalam menganalisis efektivitas respons BSSN terhadap insiden *defacement* yang menjadi fokus penelitian ini.

1.6.2.2. *Pre-Crisis Stage*

Pre-Crisis Stage dioperasionalkan sebagai tahap yang digunakan untuk melihat kesiapan dan upaya pencegahan BSSN sebelum terjadinya insiden web *defacement*. Pada tahap ini, penelitian melihat berbagai tindakan yang menunjukkan bagaimana BSSN mempersiapkan diri dalam menghadapi potensi ancaman siber. Hal tersebut dapat dilihat melalui adanya kebijakan dan regulasi keamanan siber, mekanisme identifikasi dan pemantauan ancaman, pengelolaan kerentanan sistem, penerapan standar keamanan, serta kesiapan prosedur dalam menghadapi insiden keamanan siber.

Dalam penelitian ini, informasi mengenai kondisi BSSN sebelum insiden Pusmanas kemudian digunakan untuk melihat

apakah terdapat mekanisme pencegahan dan kesiapsiagaan yang telah diterapkan sebelum web *defacement* terjadi. Dengan demikian, tahap pre-crisis tidak digunakan untuk melihat apakah BSSN berhasil atau gagal secara langsung, tetapi untuk menggambarkan bagaimana bentuk kesiapan dan pencegahan yang dimiliki BSSN sebelum munculnya krisis.

1.6.2.3. *Acute Crisis Stage*

Acute Crisis Stage dioperasionisasikan sebagai tahap yang digunakan untuk melihat respons BSSN ketika insiden web *defacement* terjadi. Pada tahap ini, penelitian berfokus pada tindakan yang dilakukan setelah adanya indikasi atau konfirmasi serangan terhadap situs Pusmanas. Informasi yang diamati mencakup respons awal terhadap insiden, tindakan pengamanan terhadap sistem yang terdampak, upaya membatasi dampak serangan, proses identifikasi awal terhadap insiden, serta koordinasi yang dilakukan dalam proses penanganan.

Tahap ini juga digunakan untuk melihat bagaimana BSSN mengambil tindakan dalam menghadapi kondisi krisis yang sedang berlangsung. Oleh karena itu, sumber data sekunder yang memuat kronologi kejadian, pernyataan resmi lembaga, pemberitaan mengenai respons BSSN, maupun dokumen terkait penanganan insiden digunakan untuk menggambarkan proses respons pada tahap acute crisis. Dengan demikian, tahap ini memberikan gambaran

mengenai bagaimana BSSN menghadapi dan mengendalikan insiden ketika krisis berlangsung.

1.6.2.4. *Chronic Stage*

Chronic Stage dioperasionisasikan sebagai tahap yang digunakan untuk melihat proses penanganan lanjutan setelah kondisi awal dari insiden berhasil dikendalikan. Pada tahap ini, penelitian melihat proses investigasi terhadap insiden, identifikasi penyebab dan kerentanan sistem, proses pemulihan sistem yang terdampak, serta tindakan perbaikan yang dilakukan setelah serangan terjadi.

Informasi mengenai proses investigasi dan pemulihan digunakan untuk melihat bagaimana BSSN menangani konsekuensi dari web *defacement* setelah fase krisis akut. Selain itu, tahap ini juga digunakan untuk melihat apakah terdapat proses evaluasi terhadap kelemahan sistem yang memungkinkan terjadinya insiden. Dengan demikian, *Chronic Stage* dalam penelitian ini menggambarkan bagaimana BSSN menangani dampak insiden dan melakukan proses pemulihan setelah kondisi krisis mulai terkendali.

1.6.2.5. *Resolution Stage*

Resolution Stage dioperasionisasikan sebagai tahap yang digunakan untuk melihat proses penyelesaian dan pembelajaran setelah insiden web *defacement* berakhir. Pada tahap ini, penelitian melihat tindakan yang dilakukan setelah sistem kembali berfungsi, termasuk evaluasi terhadap penanganan insiden, pembaruan atau

perbaikan kebijakan, penyempurnaan prosedur keamanan, peningkatan kapasitas keamanan siber, serta langkah-langkah yang dilakukan untuk mengurangi kemungkinan terjadinya insiden serupa di masa mendatang.

Tahap resolution juga digunakan untuk melihat sejauh mana pengalaman dari insiden Pusmanas dapat menjadi pembelajaran bagi BSSN dalam meningkatkan kesiapan menghadapi ancaman siber berikutnya. Oleh karena itu, data mengenai kebijakan setelah insiden, perubahan prosedur, evaluasi kelembagaan, maupun upaya penguatan sistem keamanan dapat digunakan untuk menggambarkan tahap resolusi. Dengan demikian, tahap ini menunjukkan bagaimana BSSN menyelesaikan krisis sekaligus memanfaatkan pengalaman tersebut sebagai dasar untuk meningkatkan kesiapsiagaan terhadap ancaman di masa mendatang.

1.7. Argumen Penelitian

Penelitian ini berargumen bahwa insiden web defacement pada situs Pusmanas tahun 2021 menunjukkan adanya implementation gap antara standar keamanan siber yang telah dirumuskan melalui regulasi dengan penerapannya pada tingkat institusi. Implementation gap tersebut tidak dipahami sebagai ketiadaan kebijakan, melainkan sebagai kesenjangan antara tuntutan normatif regulasi dengan bukti penerapan kebijakan dalam proses pencegahan, penanganan, pemulihan, dan evaluasi insiden.

Pada aspek pencegahan, Peraturan BSSN Nomor 8 Tahun 2020 telah memberikan kerangka sistem pengamanan dalam penyelenggaraan sistem elektronik, tetapi terjadinya defacement menunjukkan bahwa masih terdapat kerentanan pada sistem yang dapat dieksploitasi. Pada aspek penanganan insiden, Peraturan BSSN Nomor 10 Tahun 2020 telah mengatur Tim Tanggap Insiden Siber, tetapi informasi mengenai penerapan mekanisme kelembagaan tersebut dalam kasus Pusmanas masih terbatas. Sementara itu, Peraturan BSSN Nomor 4 Tahun 2021 mengatur evaluasi kinerja dan perbaikan berkelanjutan keamanan informasi SPBE, tetapi bukti mengenai evaluasi pasca-insiden dan pembelajaran kelembagaan yang secara spesifik dihasilkan dari kasus Pusmanas belum terlihat secara kuat.

Dengan demikian, implementation gap dalam penelitian ini terlihat pada ketidaksejajaran antara standar yang ditetapkan dalam regulasi dengan bukti implementasi yang dapat diidentifikasi pada kasus Pusmanas, terutama pada aspek pencegahan, dokumentasi proses respons, serta evaluasi dan perbaikan pasca-insiden.

1.8. Metode Penelitian

1.8.1. Tipe Penelitian

Metodologi atau metode penelitian adalah langkah-langkah sistematis yang digunakan untuk menyelidiki dan menelusuri suatu masalah dengan pendekatan ilmiah secara teliti dan cermat. Tujuannya adalah untuk mengumpulkan, mengolah, menganalisis data, serta menarik kesimpulan secara objektif, guna memecahkan suatu masalah atau menguji hipotesis

untuk menghasilkan pengetahuan yang bermanfaat bagi kehidupan manusia. Konsep yang paling cocok untuk menjawab penelitian ini adalah apa, bagaimana, dan mengapa. Konsep ini cocok untuk digunakan dalam penelitian ini karena mencakup seluruh aspek dalam kejahatan siber, mulai dari bagaimana cara negara lain dalam menangani ancaman siber, apa tindakan negara untuk kedepannya dan mengapa kita perlu mencegah kejahatan siber terjadi di tanah air ini.

1.8.2. Situs Penelitian

Dalam konteks penelitian kejahatan siber ini, lembaga pemerintahan, perusahaan teknologi, institusi keamanan siber, atau sektor publik dan swasta di Indonesia yang rentan terhadap serangan merupakan situs yang cocok dalam penelitian ini. Penelitian ini juga bisa dilakukan pada negara-negara yang memiliki kebijakan keamanan siber yang efektif guna untuk dibandingkan dengan kondisi Indonesia.

1.8.3. Subjek Penelitian

Dalam penelitian kualitatif berbasis studi kepustakaan (*library research*), subjek penelitian tidak berupa individu atau narasumber yang diwawancarai, melainkan berbagai dokumen dan literatur yang relevan dengan fokus penelitian. Oleh karena itu, subjek penelitian ini meliputi dokumen resmi Badan Siber dan Sandi Negara (BSSN), peraturan perundang-undangan mengenai keamanan siber, laporan tahunan BSSN, jurnal ilmiah nasional maupun internasional, buku akademik, artikel ilmiah, laporan lembaga internasional, serta publikasi media yang kredibel.

mengenai insiden *defacement* situs Pusat Malware Nasional (Pusmanas) tahun 2021. Seluruh dokumen tersebut dianalisis untuk memperoleh pemahaman mengenai respons BSSN terhadap insiden tersebut serta implementasi kebijakan keamanan siber nasional di Indonesia.

1.8.4. Jenis Data

Penelitian ini menggunakan data sekunder sebagai sumber utama penelitian. Data sekunder diperoleh melalui studi kepustakaan (*library research*) dengan menelaah berbagai sumber ilmiah yang relevan dengan topik penelitian. Sumber tersebut meliputi jurnal ilmiah nasional dan internasional, buku, laporan resmi Badan Siber dan Sandi Negara (BSSN), laporan organisasi internasional, dokumen kebijakan pemerintah, peraturan perundang-undangan, artikel ilmiah, serta pemberitaan media yang memiliki kredibilitas tinggi. Data-data tersebut digunakan untuk menganalisis respons BSSN terhadap insiden *defacement* situs Pusat Malware Nasional (Pusmanas) tahun 2021 berdasarkan perspektif *Crisis Management Theory*.

1.8.5. Sumber Data

Sumber data dalam penelitian ini sepenuhnya berasal dari data sekunder yang diperoleh melalui studi kepustakaan (*library research*). Data dikumpulkan dari berbagai literatur yang berkaitan dengan keamanan siber, seperti jurnal ilmiah nasional dan internasional, buku referensi, laporan tahunan Badan Siber dan Sandi Negara (BSSN), laporan lembaga internasional seperti ITU, regulasi pemerintah mengenai keamanan siber,

dokumen resmi negara, serta artikel berita dari media yang kredibel. Selain itu, penelitian juga memanfaatkan penelitian terdahulu yang relevan sebagai bahan perbandingan untuk memperkuat analisis mengenai implementasi kebijakan keamanan siber nasional dan respons BSSN terhadap insiden *defacement* situs Pusmanas.

1.8.6. Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan melalui studi kepustakaan (*library research*) dengan menggunakan metode *literature review*. Peneliti mengumpulkan berbagai sumber data sekunder yang relevan, seperti jurnal ilmiah, buku, laporan resmi Badan Siber dan Sandi Negara (BSSN), laporan lembaga internasional, dokumen kebijakan pemerintah, peraturan perundang-undangan, serta artikel berita dari media yang kredibel. Seluruh literatur yang diperoleh kemudian diseleksi berdasarkan relevansi, kredibilitas, dan keterkaitannya dengan fokus penelitian.

Setelah proses pengumpulan dilakukan, setiap sumber dianalisis secara sistematis untuk mengidentifikasi informasi mengenai kronologi insiden *defacement* situs Pusat Malware Nasional (Pusmanas), respons yang dilakukan oleh BSSN, implementasi kebijakan keamanan siber nasional, serta berbagai faktor yang mempengaruhi efektivitas penanganan insiden tersebut. Teknik *literature review* digunakan untuk membandingkan berbagai temuan dari penelitian terdahulu dan dokumen resmi sehingga diperoleh pemahaman yang komprehensif mengenai objek penelitian.

1.8.7. Analisis dan Interpretasi Data

Analisis data dalam penelitian ini dilakukan secara kualitatif dengan pendekatan deskriptif-analitis. Seluruh data yang diperoleh melalui studi kepustakaan diklasifikasikan berdasarkan tema-tema yang berkaitan dengan fokus penelitian, seperti kronologi insiden *defacement*, respons Badan Siber dan Sandi Negara (BSSN), implementasi kebijakan keamanan siber nasional, serta faktor-faktor yang mempengaruhi efektivitas penanganan insiden.

Tahapan analisis dilakukan melalui proses reduksi data, penyajian data, dan penarikan kesimpulan. Selanjutnya, data yang telah diklasifikasikan dianalisis menggunakan *Crisis Management Theory* untuk mengevaluasi tahapan penanganan krisis yang dilakukan BSSN, mulai dari pre-crisis, acute crisis, *Chronic Stage*, hingga *Resolution Stage*. Selain itu, hasil analisis kemudian diinterpretasikan untuk menjelaskan hubungan antara respons institusi, implementasi kebijakan, dan penguatan tata kelola keamanan siber nasional.

1.8.8. Kualitas Data

Kualitas data dalam penelitian kualitatif tidak diukur melalui uji validitas kuantitatif, melainkan melalui kriteria seperti kredibilitas, otentisitas, dan keterkaitan data dengan realitas sosial yang diteliti. Dalam paradigma interpretif (konstruktivis), data dinilai berkualitas jika mampu merepresentasikan pengalaman dan persepsi para pelaku sosial secara otentik. Sementara dalam pendekatan kritis, kualitas data juga ditentukan

oleh sejauh mana analisis mempertimbangkan konteks historis, sosial, budaya, ekonomi, dan politik dari objek penelitian yang dikenal dengan istilah *historical situatedness*. Selain itu, peneliti juga memperhatikan aspek *transferability* (apakah temuan dapat diterapkan pada konteks lain), *dependability* (konsistensi data dan analisis), serta *confirmability* (objektivitas dan transparansi peneliti). Dengan memenuhi prinsip-prinsip tersebut, data yang diperoleh dapat memberikan dasar yang kuat bagi kesimpulan dan rekomendasi penelitian.