# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Skripsi ini menganalisis strategi Indonesia dalam memerangi *cyber attack* melalui Badan Siber dan Sandi Negara (BSSN). Tujuannya adalah untuk mengevaluasi efektivitas strategi tersebut dan memberikan masukan bagi pengembangan sekuritisasi siber di masa depan. Penelitian ini menggunakan teori sekuritisasi Barry Buzan untuk mengkaji bagaimana BSSN mengkonstruksikan *cyber attack* sebagai ancaman dan merumuskan strategi untuk mengatasinya.

Skripsi ini juga membahas konsepsi, data, dan indikasi ancaman siber yang telah terjadi di Indonesia. Penelitian ini diharapkan dapat memberikan kontribusi yang signifikan bagi pemahaman tentang strategi Indonesia dalam memerangi *cyber attack*. Selain itu, hasil penelitian ini juga diharapkan dapat membantu pemerintah dalam meningkatkan keamanan siber nasional. Dengan demikian, penelitian ini memiliki nilai yang sangat penting dalam konteks keamanan siber di Indonesia.

Siber dalam perspektif hubungan internasional adalah sebuah ruang digital tanpa batas. Ruang ini merupakan arena baru bagi interaksi antar negara yang tidak dibatasi oleh wilayah fisik. Ruang ini memiliki karakteristik unik seperti aksesibilitas yang mudah, anonimitas, dan kecepatan tinggi. Karakteristik ini mendorong munculnya berbagai aktor non-negara yang memperumit dinamika keamanan tradisional dan menantang sistem keamanan yang ada (Triwibowo, 2023: 1-3).

Siber memiliki potensi untuk meningkatkan kerja sama antar negara dalam berbagai bidang, seperti ekonomi, pendidikan, dan budaya. Namun, hal tersebut juga menghasilkan potensi untuk digunakan sebagai alat untuk melakukan kejahatan, seperti pencurian data, *cyber attack*, dan propaganda. Oleh karena itu, siber merupakan isu penting dalam hubungan internasional yang membutuhkan kerja sama dan regulasi global untuk menjamin keamanan dan stabilitas internasional (Madu, 2018: 1).

Terbukanya berbagai potensi yang dihasilkan oleh siber yang mempunyai kemungkinan menghadirkan ancaman siber, oleh karena itu diperlukan adanya keamanan siber. Keamanan siber dipahami sebagai fenomena yang muncul sebagai tanggapan terhadap era globalisasi yang semakin terkait erat dengan teknologi informasi. Dalam konteks ini, negara-negara di seluruh dunia menghadapi tantangan yang serius terkait dengan keamanan siber, yang menjadi fokus utama dalam kebijakan nasional dan internasional (Moenardy, 2021: 1-2).

Indonesia, sebagai negara yang terus mengalami pertumbuhan signifikan dalam penggunaan internet, tidak bisa mengabaikan dampaknya terhadap keamanan siber. Penggunaan internet yang meluas telah membawa perubahan besar dalam berbagai aspek kehidupan di Indonesia. Melalui ranah siber, negara ini terlibat dalam berbagai aktivitas modern. Aktivitas ini mencakup transaksi bisnis hingga komunikasi antar individu, yang semakin mengandalkan teknologi digital.

Selain itu, perkembangan teknologi informasi dan komunikasi telah membuka peluang baru. Peluang ini termasuk peningkatan efisiensi dalam sektor publik dan swasta. Namun, ini juga membawa tantangan baru dalam bentuk

ancaman siber. Oleh karena itu, penting bagi Indonesia untuk memperkuat langkah-langkah keamanan siber. Langkah-langkah ini harus mencakup kebijakan, regulasi, dan teknologi yang tepat untuk melindungi infrastruktur digital nasional. (Ramadhan, 2022: 3).

Ancaman siber yang dihadapi Indonesia sangatlah beragam. Peretasan data, serangan siber politik, pencurian identitas, dan penyebaran berita palsu adalah beberapa contoh serangan yang kerap muncul dan memiliki potensi merusak. Dengan infrastruktur kritis yang semakin terhubung dengan internet, seperti sistem keuangan dan jaringan listrik, negara ini rentan terhadap serangan yang dapat mengganggu stabilitas ekonomi dan sosialnya.

Pada tahun 2017 saja, terdapat lebih dari 200 juta serangan siber yang menargetkan Indonesia (BSSN, 2023). Oleh karena itu, keamanan siber menjadi prioritas utama dalam agenda kebijakan pemerintah (Kim et al., 2023: 2). Perkembangan teknologi informasi telah membawa dampak yang signifikan pada masyarakat Indonesia. Seiring dengan masuknya teknologi informasi ke dalam masyarakat, ancaman siber telah menjadi semakin mendalam dan mendesak. Sejarah perkembangan ancaman siber di Indonesia mencerminkan interaksi kompleks antara faktor-faktor domestik dan internasional. Faktor-faktor ini mencakup kebijakan pemerintah, kemajuan teknologi, dan dinamika politik dalam dan luar negeri.

Dalam kerangka ilmu hubungan internasional, ancaman siber merupakan topik yang semakin berkembang dan signifikan. Dampak dari ancaman siber tidak hanya terbatas pada aspek keamanan nasional, tetapi juga mempengaruhi politik

dan ekonomi negara. Interaksi kompleks antara berbagai aktor dalam dan luar negeri telah membentuk latar belakang yang kompleks untuk pemahaman tentang ancaman siber di Indonesia.

Ancaman siber di Indonesia telah menjadi perhatian yang signifikan dalam beberapa tahun terakhir. Negara ini telah mengalami berbagai insiden siber, termasuk serangan yang dilakukan oleh aktor negara dan non-negara. Salah satu insiden penting adalah kerusuhan rasial pada tahun 1998, dimana Indonesia harus memerangi peretas dari Tiongkok dan Taiwan (Margiansyah, 2020: 4). Insiden-insiden ini menyoroti sifat ancaman siber yang bersifat transnasional dan perlunya kerja sama internasional untuk mengatasinya.

Indonesia telah menyadari sifat ancaman terorisme siber yang canggih dan berbahaya. Salah satu contoh kasus yang pernah dialami adalah unit Kopassus 81 berperan penting dalam menangani terorisme siber dan mendukung upaya pertahanan negara (Uksan et al., 2023: 4). Hal ini menyoroti pentingnya mengintegrasikan pasukan keamanan dan mengembangkan strategi untuk melawan ancaman siber dalam konteks internasional.

Kebijakan dan kerja sama siber pemerintah Indonesia menghadirkan situasi yang kompleks. Identifikasi ancaman dan perumusan kebijakan dipengaruhi oleh faktor domestik dan internasional. Hal ini menunjukkan sifat kompleks dari ancaman siber dan perlunya pendekatan komprehensif yang mempertimbangkan dinamika hubungan internasional.

Selain terorisme siber, Indonesia juga menghadapi ancaman perang siber. Aktor negara dan non-negara memiliki kemampuan siber yang dapat digunakan

untuk menargetkan infrastruktur penting negara dan keamanan nasional. Hal ini menekankan perlunya Indonesia untuk meningkatkan kemampuan pertahanan sibernya dan menetapkan strategi yang efektif untuk melawan ancaman perang siber. Pada tahun 2020, terdapat lebih dari 50 insiden perang siber yang menargetkan infrastruktur kritis Indonesia (Moenardy, 2021: 5).

Dampak ancaman siber tidak hanya mencakup masalah keamanan. Serangan siber juga dapat menimbulkan dampak ekonomi, khususnya terkait dengan investasi asing. Memastikan lingkungan siber yang aman sangat penting untuk menarik dan mempertahankan investasi asing di Indonesia. Pada tahun 2019, terjadi serangan ransomware WannaCry yang menyerang instansi dan beberapa bagian aspek pemerintahan Indonesia sehingga menyebabkan nilai kerugian ekonomi akibat serangan siber di Indonesia mencapai USD 34,2 juta (Listyowati et al., 2022: 3).

Dari perspektif hubungan internasional, revolusi siber menimbulkan tantangan terhadap teori dan tata negara. Para pengambil keputusan seringkali menyoroti ancaman siber, namun analisis sistematis dari perspektif studi keamanan internasional dinilai masih kurang. Hal ini menyoroti perlunya penelitian dan kolaborasi komprehensif di antara para akademisi dan pembuat kebijakan untuk :mengatasi ancaman siber secara efektif (Madu, 2018: 3).

Ancaman siber di Indonesia memiliki akar sejarah yang panjang, dan seiring dengan perkembangan teknologi informasi telah menjadi isu yang semakin serius. Pada awal sejarahnya, internet hadir di Indonesia pada akhir tahun 1980-an, namun saat itu penggunaannya masih terbatas pada akademisi dan pemerintah. Ancaman

siber pada periode ini masih sangat terbatas, dan fokus utamanya adalah pada aspek teknis jaringan. Selama tahun 2000-an, seiring dengan perkembangan jaringan dan internet di Indonesia, muncul peluang baru bagi serangan siber. Penjahat siber mulai mengincar data transaksi online dan mencoba memanfaatkan pelanggan yang kurang berpengalaman (Setyawan, 2023: 2). Pada awal 2010-an, perkembangan media sosial menciptakan platform baru untuk berbagai jenis serangan, termasuk penyebaran berita palsu, penipuan online, dan kampanye *phising*. Ancaman siber mulai menciptakan dampak sosial dan politik yang signifikan.

Perkembangan serangan teroris siber di Indonesia menjadi sorotan dalam pertengahan 2010-an. Saat ini, dapat dikaji bagaimana perkembangan ancaman siber sendiri bertumbuh di Indonesia dan berdampak bagi Indonesia terlebih kepada aspek hubungan Indonesia di kancah Internasional, yang juga dapat digunakan dalam penelitian Hubungan Internasional mengenai dalam mendukung penelitian ini.

Ancaman siber sendiri telah berkembang pesat di Indonesia, dan perkembangan ini memiliki dampak signifikan dalam kerangka hubungan internasional. Ancaman siber tidak lagi hanya menjadi isu teknis, tetapi juga menjadi isu keamanan nasional, ekonomi, dan diplomasi yang mempengaruhi Indonesia dalam hubungannya dengan negara-negara lain.

Seiring dengan pertumbuhan pesat teknologi informasi dan digitalisasi di Indonesia, ancaman siber telah berkembang secara eksponensial. Ini mencakup serangan malware, serangan DDoS, peretasan data, *phising*, dan serangan siber

politik yang semakin sering terjadi. Perkembangan ini menciptakan kompleksitas tambahan dalam hubungan internasional Indonesia.

Dalam kerangka hubungan internasional, perkembangan ancaman siber memiliki lima dampak utama: (1) Keamanan Nasional; (2) Diplomasi Siber; (3) Hubungan Bilateral; (4) Hubungan Ekonomi; (5) Diplomasi Politik. Pada aspek keamanan nasional, ancaman siber telah menjadi faktor penting dalam perencanaan keamanan nasional Indonesia. Serangan terhadap infrastruktur kritis, seperti sistem kelistrikan dan telekomunikasi, dapat menciptakan ketidakstabilan nasional. Keamanan siber juga terkait dengan pertahanan militer dan komunikasi, yang membuatnya menjadi isu keamanan nasional yang serius (Ramadhan, 2022: 2). Diplomasi siber dipahami sebagai suatu kerja sama antar negara dalam bentuk diplomasi dalam mengatasi serangan siber, dengan tujuan menciptakan kerangka kerja yang efektif untuk menghadapi serangan siber. Diplomasi siber juga melibatkan upaya diplomatis untuk mengelola konflik yang mungkin timbul akibat serangan siber (Listyowati et al., 2022: 2).

Sedangkan pada konteks hubungan bilateral, perkembangan ancaman siber mempengaruhi hubungan bilateral suatu negara dengan negara-negara mitra. Serangan siber yang berasal dari atau melalui wilayah negara lain dapat menciptakan ketegangan diplomatik. Ancaman siber juga mempengaruhi hubungan ekonomi suatu negara dengan negara-negara mitra dagang. Kerentanannya terhadap serangan siber dapat mengganggu perdagangan dan investasi ekonomi (Moenardy, 2021: 4-6). Hal ini juga berlaku pada aspek diplomasi politik yang sudah terjalin dimana serangan siber politik dan upaya manipulasi politik melalui serangan siber

dapat menciptakan ketidakstabilan politik di Indonesia. Ancaman ini mempengaruhi diplomasi politik suatu negara dalam hubungannya dengan negara-negara lain. Upaya diplomatis diperlukan untuk memahami asal-usul serangan siber politik dan mengelola dampaknya terhadap stabilitas politik.

Dari konteks tersebut dapat dinilai perkembangan ancaman siber menciptakan tantangan baru dalam konteks hubungan internasional. Indonesia harus aktif berpartisipasi dalam diplomasi siber, bekerja sama dengan negara-negara mitra untuk mengatasi ancaman bersama, dan memastikan bahwa ancaman siber tidak menghambat hubungan bilateral, ekonomi, atau politik. Ancaman siber adalah isu global yang memerlukan kerja sama dan koordinasi antar negara untuk melindungi keamanan nasional dan kepentingan nasional. Dalam era digital ini, kebijakan luar negeri Indonesia harus mencerminkan realitas ancaman siber yang semakin mendalam dan kompleks..

Jika dikaji lebih dalam, ancaman siber di Indonesia telah berkembang sejalan dengan pesatnya pertumbuhan teknologi informasi dan penetrasi internet di negara ini. Serangan siber yang semakin sering dan beragam menciptakan ancaman signifikan terhadap keamanan nasional, ekonomi, dan diplomasi Indonesia. Dampak dari serangan ini dapat merugikan secara finansial, merusak reputasi, dan mengganggu stabilitas nasional. Oleh karena itu, penting bagi Indonesia untuk terus meningkatkan upaya perlindungan siber melalui kebijakan yang tepat, kerja sama internasional, dan pengembangan kapasitas teknis dalam menghadapi ancaman siber yang semakin kompleks.

Pembentukan BSSN diinisiasi oleh kesadaran bahwa ancaman siber bukan hanya masalah domestik, melainkan juga memiliki implikasi internasional. Sejak awal tahun 2000-an, serangan siber telah menunjukkan potensi merusak yang serius terhadap infrastruktur kritis, data pribadi, dan kepentingan nasional. Beberapa serangan bahkan dapat dilakukan dari luar negeri, melibatkan aktor-aktor internasional.

Langkah awal Indonesia adalah pembentukan Badan Siber dan Sandi Negara (BSSN) pada tahun 2018. Lembaga ini ditugaskan untuk mengkoordinasikan kebijakan keamanan siber dan berfungsi sebagai otoritas nasional dalam hal keamanan siber. Namun, kebijakan dan tugasnya masih terbatas.

Pada tahun 2020, pemerintah Indonesia membentuk Badan Siber dan Sandi Negara (BSSN) melalui Keputusan Presiden No. 133/2020. Langkah ini menunjukkan keseriusan pemerintah dalam menghadapi ancaman siber di era digital. Pembentukan BSSN juga mencerminkan upaya pemerintah untuk meningkatkan keamanan siber nasional. Selain itu, pemerintah mengakui kompleksitas tantangan siber dalam konteks hubungan internasional. BSSN diharapkan mampu merespons ancaman siber secara efektif dan menjaga stabilitas digital negara.

Oleh karena itu, memahami dan menganalisis fenomena global ancaman siber menjadi semakin penting. Dengan menyelidiki perkembangan dan dampak dari ancaman siber, kita dapat memahami lebih baik bagaimana transformasi ancaman siber saat ini mempengaruhi suatu negara, dan membuka jendela baru untuk melihat bagaimana teknologi mempunyai celah merugikan bagi masyarakat internasional.

Dalam konteks Indonesia, negara ini juga mengalami gelombang revolusi ancaman siber yang signifikan, membuka peluang dan tantangan yang perlu dianalisis lebih mendalam.

Dengan demikian, penelitian ini bertujuan untuk mengkaji upaya Indonesia memerangi *cyber attack* dengan strategi yang dihasilkan dan dilakukan oleh Badan Siber dan Sandi Negara, menghubungkan aspek global dari fenomena ini dengan realitas dalam negeri. Dengan memahami dinamika dan implikasi upaya Indonesia yang direalisasikan melalui pembentukan Badan Siber dan Sandi Negara, diharapkan akan muncul wawasan baru tentang bagaimana kebijakan dan strategi Indonesia dapat dirancang untuk mengoptimalkan manfaat dari fenomena global ini sambil tetap mempertimbangkan kedaulatan dan kepentingan nasional.

## 1.2 Rumusan Masalah

Maka Berdasarkan uraian latar belakang, maka terlihat timpangnya informasi dan data factual yang mengkaji mengenai upaya Indonesia memerangi *cyber attack* dari perspektif Hubungan Internasional oleh sebab itu peneliti mengangkat rumusan masalah dalam pertanyaan

**"Bagaimana Strategi Indonesia Melalui Badan Siber Dan Sandi Negara Dalam Menangani Ancaman Eskalasi Serangan Siber?"**

## 1.3 Tujuan Penelitian

Merujuk pada rumusan masalah yang telah disusun di atas, maka penelitian ini bertujuan untuk mengetahui untuk mengetahui bagaimana strategi BSSN berdasarkan kerangka kerja dan hasil yang telah dilakukan, serta tantangan dalam upaya pemberantasan serangan siber di Indonesia

## 1.4 Manfaat Penelitian

### 1.4.1 Manfaat Akademis:

Skripsi ini diharapkan dapat memberi manfaat akademis yang signifikan dalam konteks ilmu hubungan internasional yang berkaitan dengan keamanan (*security*) dan keamanan negara. Dalam era globalisasi dan interkoneksi digital, ancaman serangan siber telah menjadi prioritas penting bagi negara-negara untuk dipertimbangkan dalam kebijakan keamanan nasional mereka. Melalui analisis terhadap strategi keamanan siber yang diimplementasikan oleh Badan Siber dan Sandi Negara (BSSN) Indonesia, skripsi ini dapat memberikan kontribusi berharga dalam pemahaman tentang bagaimana negara-negara menghadapi tantangan baru dalam bentuk serangan siber dan upaya-upaya yang diambil untuk melindungi kepentingan nasional dalam domain *cyber*. Selain itu, skripsi ini juga dapat memperkaya wacana akademis tentang peran lembaga-lembaga keamanan dalam mengatasi ancaman siber, serta memberikan pemahaman yang lebih mendalam tentang dinamika hubungan internasional dalam konteks keamanan *cyber* di era digital saat in

### 1.4.2 Manfaat Praktis:

i. Perlindungan Keamanan Nasional

i. Rujukan untuk KOMINFO:

Memperkuat kerja sama antara Kementerian Komunikasi dan Informatika (KOMINFO) dengan Badan Siber dan Sandi Negara (BSSN) untuk meningkatkan pemahaman masyarakat tentang ancaman siber dan upaya mitigasi yang dilakukan pemerintah. Skripsi ini diharapkan dapat memberikan wawasan yang lebih mendalam tentang bagaimana kerja sama ini dapat diperkuat secara praktis.

ii. Rujukan untuk BSSN:

Memperjelas peran dan tanggung jawab Badan Siber dan Sandi Negara (BSSN) dalam melindungi infrastruktur informasi kritis Indonesia dari serangan siber, serta mengoptimalkan penggunaan teknologi dan sumber daya manusia untuk deteksi dini dan respons cepat terhadap ancaman tersebut. Skripsi ini diharapkan dapat memberikan panduan praktis dalam meningkatkan efektivitas tindakan BSSN dalam mengatasi ancaman siber.

iii. Rujukan untuk Kepolisian:

Mendorong koordinasi antara Badan Siber dan Sandi Negara (BSSN) dengan kepolisian untuk meningkatkan penegakan hukum terhadap pelaku kejahatan siber, termasuk penyediaan pelatihan dan peralatan yang diperlukan bagi aparat penegak hukum dalam menyelidiki dan menindaklanjuti kasus-kasus serangan siber. Skripsi ini diharapkan dapat memberikan rekomendasi konkret untuk memperkuat kerja sama antara BSSN dan kepolisian dalam penegakan hukum terhadap kejahatan siber.

iv. Rujukan untuk Penelitian Lanjutan:

Mengidentifikasi celah dan tantangan yang masih dihadapi dalam implementasi strategi keamanan siber Indonesia melalui Badan Siber dan Sandi Negara (BSSN), serta memberikan rekomendasi untuk pengembangan kebijakan dan teknologi yang lebih efektif dalam menghadapi ancaman siber yang terus berkembang. Skripsi ini diharapkan dapat menjadi landasan untuk penelitian lanjutan dalam mengatasi permasalahan yang diidentifikasi, serta memberikan

sumbangan konstruktif dalam pengembangan kebijakan dan teknologi keamanan siber.

Dengan mempertimbangkan manfaat-manfaat ini, Penelitian ini akan memberikan manfaat akademis dalam bentuk kontribusi pengetahuan dan pemahaman dalam bidang keamanan siber dan diplomasi siber, sementara juga memberikan manfaat praktis dengan menyediakan panduan bagi pemerintah dan lembaga terkait dalam memerangi serangan siber dan melindungi kepentingan nasional.

### 1.4.3 Sistematika Penelitian

Skripsi ini terdiri atas lima bab, dalam setiap bab terdapat sub-bab yang disesuaikan dengan bahasan penelitian

**BAB I** **PENDAHULUAN**

Bab pertama ini akan memperkenalkan latar belakang penelitian, memotret perkembangan ancaman siber yang bertumbuh dan perlahan mengakar di Indonesia, serta mengidentifikasi permasalahan yang relevan. Bab ini juga akan merinci tujuan penelitian, pertanyaan penelitian, dan struktur penelitian.

**BAB II** **KAJIAN PUSTAKA DAN METODE PENELITIAN**

Bab ini berisi tentang tinjauan pustaka, kerangka teoritik, kerangka pemikiran, dan argumen utama yang menjelaskan tentang teori atau konsep yang digunakan untuk memvalidasi penelitian ini serta adanya

perbandingan penelitian ini dengan penelitian sebelumnya. Bab ini juga memuat metode penelitian yang mendeskripsikan jenis, tipe, ruang lingkup, teknik analisa dan validasi yang digunakan pada penelitian ini

**BAB III** **PEMBAHASAN**

Bab ini berisi tentang mengenai temuan penelitian yang berkaitan mengenai perkembangan ancaman siber itu mulai berkembang di Indonesia itu sendiri, yang di sesuaikan dengan arah tujuan dan pandangan yang terdapat di kerangka teoritik, kerangka pemikiran, dan argumen utama yang menjelaskan tentang bagaimana dinamika dunia digital, terlebih Indonesia dalam era kemajuan teknologi termasuk bagaimana ancaman siber itu sendiri dapat mengakar dan memberikan pengaruhnya melalui serangan siber yang menginisiasi stratetegi Badan Siber dan Sandi Negara dan untuk memvalidasi penelitian disertakan data data yang mendukung.

**BAB IV** **PEMBAHASAN**

Bab ini berisi tentang mengenai sendiri bagaimana strategi upaya yang dilakukan oleh Indonesia melalui BSSN sebagai respon daripada ancaman siber dengan kacamata perspektif teori, yang rincikan menjadianalisis

upaya menggunakan Teori Sekuritisasi oleh Barry Buzan, keamanan siber dan termasuk diplomasi siber yang memuat relevansi yang signifikan dalam menjelaskan dan memahami bagaimana ancaman siber ditempatkan dalam kerangka keamanan nasional dan internasional beserta menilai strategi yang telah dilakukan oleh BSSN melalui indikator penilaian strategi BSSN menggunakan Diplomasi Siber dan juga yang indikator terkandung dalam *Global Cyber Security* Index. Ini membantu menjelaskan bagaimana serangan siber telah ditempatkan dalam kategori keamanan dan bagaimana negara-negara seperti Indonesia merespons ancaman tersebut dengan serius melalui strategi yang dilakukan oleh Badan Siber dan Sandi Negara.

**BAB V** **KESIMPULAN**

Bab penutup ini akan merangkum temuan penelitian dan memberikan kesimpulan akhir yang melibatkan pemahaman yang lebih dalam tentang upaya Indonesia memerangi *cyber attack* dan juga akan menyajikan rekomendasi kebijakan yang bagaimana seharusnya ancaman ini diperlakukan dan direspon secara efektif dan berkelanjutan. Selain itu, dapat mengidentifikasi

peluang rekomendasi untuk penelitian masa depan yang relevan dengan topik ini.