BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Di era digital yang semakin maju, keamanan siber menjadi aspek yang sangat penting dalam menjaga keberlangsungan aktivitas pemerintahan, bisnis, dan kehidupan sosial masyarakat. Ketergantungan terhadap sistem informasi dan teknologi digital telah meningkatkan keterbukaan terhadap berbagai jenis ancaman siber, mulai dari serangan malware, pencurian data, hingga serangan yang menargetkan infrastruktur kritikal nasional [1]. Dalam konteks Indonesia, serangan siber bukan lagi sekadar isu teknis, tetapi telah menjadi tantangan serius bagi keamanan nasional, sebagai ancaman keamanan siber yang dapat melemahkan stabilitas dan kedaulatan negara.

Badan Siber dan Sandi Negara (BSSN) mencatat bahwa Indonesia merupakan salah satu negara yang sering menjadi target serangan siber. Berdasarkan laporan dari Direktorat Operasi Keamanan Siber BSSN melalui ID-SIRTII/CC, tercatat lebih dari 1,6 miliar anomali trafik atau potensi serangan siber terjadi sepanjang tahun 2021 di seluruh wilayah Indonesia. Jumlah ini menunjukkan tingginya intensitas ancaman digital yang dihadapi Indonesia. Bahkan, kasus kebocoran data pribadi yang diperjualbelikan secara ilegal di internet terus berulang setiap bulannya. Menurut pakar keamanan dari CISSReC, kondisi ini membuat keamanan siber nasional berada dalam status *Red Alert* atau tingkat kewaspadaan tinggi karena tingginya risiko peretasan terhadap data publik dan infrastruktur penting [2].

Fenomena tersebut menunjukkan bahwa serangan siber telah berkembang menjadi ancaman serius terhadap keamanan nasional. Menurut Fadhlurrahman et al.[3], keamanan nasional tidak hanya mencakup aspek militer, tetapi juga keamanan informasi, perlindungan data masyarakat, serta ketersediaan dan keandalan infrastruktur digital negara. Ancaman terhadap sistem digital yang mengelola data publik, layanan pemerintahan elektronik, serta sektor-sektor vital seperti keuangan, energi, dan transportasi, dapat menyebabkan kerugian besar, baik secara ekonomi maupun sosial.

Dampak dari meningkatnya intensitas dan kompleksitas ancaman, diperlukan sistem keamanan siber yang kuat, terintegrasi, dan adaptif terhadap

perubahan serangan yang terus berkembang [4]. Menyadari urgensi tersebut, pemerintah Indonesia membentuk Badan Siber dan Sandi Negara (BSSN) sebagai institusi yang berperan sentral dalam implementasi strategi keamanan siber nasional dan manajemen krisis siber. BSSN memiliki peran strategis untuk membangun, menjaga, dan mengembangkan ekosistem keamanan siber nasional secara menyeluruh.

Peran BSSN semakin krusial seiring dengan percepatan digitalisasi di berbagai sektor, khususnya dalam penyediaan layanan publik berbasis elektronik. Penguatan kebijakan dan infrastruktur keamanan informasi menjadi kepentingan nasional untuk menjaga keberlangsungan layanan digital yang aman dan andal. Namun dalam implementasinya, tantangan seperti kurangnya kesadaran keamanan informasi, keterbatasan sumber daya manusia, serta minimnya standar keamanan di berbagai instansi, masih menjadi hambatan dalam mewujudkan ketahanan siber yang menyeluruh.

Oleh karena itu, penting untuk terus meningkatkan kapasitas dan kesadaran akan keamanan siber di seluruh sektor, termasuk pemerintahan, industri, dan pendidikan. Penguatan literasi digital dan perlindungan informasi harus menjadi bagian dari strategi nasional [5]. Keamanan siber tidak bisa hanya dibebankan pada satu lembaga saja, melainkan harus menjadi tanggung jawab bersama seluruh komponen bangsa dalam menghadapi era digital yang semakin kompleks dan penuh risiko.

1.2 Maksud dan Tujuan Kerja Magang

Maksud dari pelaksanaan magang di BSSN pada tim Manajemen Risiko dan Keberlangsungan TIK adalah memperoleh pemahaman yang lebih mendalam mengenai penerapan prinsip-prinsip keamanan siber. Kegiatan magang ini dilakukan sebagai salah satu syarat akademik dalam menyelesaikan studi pada Program Studi Informatika Universitas Multimedia Nusantara (UMN). Program kerja magang ini memberikan pengetahuan strategi penguatan keamanan siber, baik dari sisi kebijakan maupun teknis. Aktivitas magang meliputi studi, observasi aktif, serta praktik seperti analisis ancaman, simulasi serangan, digital forensik, dan *penetration testing*. Pengalaman tersebut diharapkan menjadi dasar pengembangan keterampilan yang relevan dengan kebutuhan industri.

Adapun tujuan pelaksanaan kerja magang adalah untuk menganalisis dan mensimulasikan berbagai jenis ancaman keamanan siber melalui pendekatan studi

kasus dan praktik teknis. Kegiatan ini bertujuan untuk memahami penerapan prinsip-prinsip keamanan siber, mengenali metode serangan dan dampaknya, serta mengembangkan keterampilan dalam penggunaan *tools* keamanan siber dalam melakukan pengujian keamanan.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Kegiatan kerja magang di BSSN dimulai dengan pengiriman surat lamaran dan CV melalui email. Setelah tahap seleksi, jadwal wawancara ditetapkan dan dilaksanakan pada tanggal 9 Januari 2025. Pada tanggal 30 Januari 2025, izin untuk melaksanakan magang diberikan. Selanjutnya, pada tanggal 5 Februari 2025, kontrak magang ditandatangani di kantor BSSN yang berlokasi di Jl. Raya Muchtar No. 70 Bojongsari Lama, Bojongsari, Depok, Jawa Barat, 16518. Durasi magang terhitung mulai tanggal 1 Februari hingga 31 Mei 2025 atau sampai terpenuhinya 640 jam kerja, sesuai ketentuan MBKM Magang.

Penempatan magang dilakukan di Tim Manajemen Risiko dan Keberlangsungan TIK, Departemen Pusat Data dan Pengolahan Teknologi Informasi dan Komunikasi. Program ini dilaksanakan secara luring (*Work From Office*) selama kurang lebih lima bulan, yaitu sejak tanggal 1 Februari hingga 30 Juni 2025.

Jadwal kerja adalah hari Senin hingga Kamis dengan waktu kerja pukul 07.30 hingga 16.00 WIB, sedangkan pada hari Jumat, waktu kerja dimulai dari pukul 07.30 hingga 16.30 WIB. Hari libur nasional tidak dihitung sebagai hari kerja selama masa magang. Apabila terdapat kebutuhan mendesak yang mengharuskan izin tidak masuk, perizinan diajukan kepada pembimbing atau langsung kepada ketua tim.

Setelah proses administrasi dan penempatan divisi selesai, pembimbing lapangan yang ditunjuk oleh ketua tim akan mendampingi pelaksanaan kegiatan magang. Mahasiswa mengikuti orientasi awal untuk memahami alur kerja di Pusdatik BSSN, kemudian melaksanakan tugas yang diberikan sesuai arahan dari ketua tim melalui pembimbing lapangan. Selama magang, mahasiswa juga mengikuti sesi diskusi dan *sharing knowledge* bersama tim, serta mendokumentasikan seluruh kegiatan yang dijalani sebagai bahan penyusunan laporan akhir. Dengan prosedur tersebut, mahasiswa diharapkan dapat memperoleh pengalaman nyata serta mengembangkan keterampilan teknis dan non-teknis di lingkungan kerja.