BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

International Telecommunication Union (ITU) melaporkan bahwa pada tahun 2023, sekitar 5,4 miliar orang atau 67 persen populasi dunia telah menggunakan internet, meningkat 45 persen dibandingkan data tahun 2018 yaitu 1,7 miliar. Sayangnya, di era transformasi digital ini masih terdapat 2,6 miliar populasi yang belum mendapatkan akses dan manfaat dari internet. Jika dibandingkan dengan target di dalam *the United Nations Sustainable Development Goals* (SDG), semua orang perlu mendapatkan akses ke internet secara bermakna pada tahun 2030. Oleh sebab itu, perlu dibangun keterampilan digital bagi semua orang secara universal, termasuk keterampilan untuk mendapatkan pengalaman online yang aman [1] dan bebas dari serangan siber, yang disebut sebagai literasi keamanan siber (*cybersecurity literacy*).

Menurut laporan tahunan *Honeynet Project* 2023 yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN), Indonesia mengalami kenaikan jumlah serangan siber, yaitu menjadi lebih dari 600 juta serangan, meningkat lebih dari satu setengah kali lipat dibandingkan pada tahun sebelumnya yaitu 370 juta. Dari 1.76 juta alamat IP unik, yaitu 1,093 juta serangan *malware* dengan 6.7 ribu *malware* unik. Serangan siber tersebut diidentifikasi berasal dari dalam negeri Indonesia, dan luar negeri yaitu antara lain dari India, Amerika Serikat, Republik Rakyat Tiongkok, dan Vietnam. Pendeteksian serangan siber dilakukan melalui pemasangan perangkat Honeypot pada infrastruktur di 105 lokasi titik pemantauan yang disebar di 79 kantor Administrasi Pemerintahan, 3 lokasi sektor Teknologi Informasi Komunikasi, 3 sektor Keuangan, 2 sektor Kesehatan, 2 sektor Pertahanan, 1 sektor Pangan, 1 sektor Energi Sumber Daya Mineral, dan 14 sektor Lainnya (Pendidikan) [2].

Jenis-jenis serangan siber tersebut antara lain *Juice Jacking*, *Phishing* berbasis *WhatsApp* (perubahan tarif admin bank, foto kurir paket dan undangan nikah berkedok aplikasi Android), *Ransomware* dan vandalisme halaman web.

Beberapa peneliti sebelumnya telah menyajikan permasalahan umum keamanan siber di Indonesia antara lain sebagai berikut. Tingkat kesadaran digital (*digital literacy*) masih rendah. Kesadaran akan betapa vital-nya konsekuensi dari

ancaman siber internasional maupun nasional masih rendah, bahwa hal tersebut bahkan dapat melumpuhkan infrastruktur negara.

Banyak kasus kejahatan siber, seperti peretasan, pencurian data digital, dan *ransomware*, terjadi dalam waktu yang amat cepat. Akibatnya seringkali institusi yang diserang sulit untuk menanganinya dalam waktu singkat. Aspek hukum dari penanganan penyerangan siber kompleksitasnya tinggi, hal ini tercermin dari Undang-Undang (UU) Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang telah direvisi dua kali, menjadi UU No. 27 Tahun 2023. Demikian juga, pemahaman penyelenggara negara atau kelembagaan masih lemah terhadap *cybersecurity* karena seringkali *server*-nya berada di luar negeri.

GIS (Geography Information System) berisikan data geospasial, yaitu informasi tentang permukaan bumi yang sangat terperinci dengan presisi tinggi. Saat ini, struktur atau kerangka GIS umumnya terdapat pada asosiasi pemerintahan pusat, pemerintahan kota, organisasi militer, perusahaan, organisasi pengamanan bencana, organisasi pengamanan terbuka, masalah e-government, pembangkit tenaga listrik, sistem komputerisasi kota dan utilitas lainnya. Oleh karena itu, informasi geospasial harus didefinisikan dan diorganisasikan sesuai dengan kebutuhan khusus setiap klien[3].

Data-data yang disimpan di dalam tempat penyimpanan, seperti di *cloud*, penyimpanan lokal, dll. tetap penting untuk dilindungi, sama halnya dengan data geospasial. Data yang sensitif harus diamankan dari serangan siber karena mereka mengandung hal-hal pribadi, seperti nama lengkap, alamat, jumlah saldo bank, dst., demikian halnya juga dengan data geospasial yang mengandung batas wilayah negara, tata ruang pemukiman, koordinat letak kandungan sumber daya mineral dll. Dengan demikian, data geospasial juga tidak kalah pentingnya jika dibandingkan dengan data finansial, keduanya harus dilindungi dan dijaga kerahasiannya.

Tata kelola kelembagaan keamanan siber nasional masih terbatas. BSSN masih belum mempunyai Computer Security Incident Response Team (CSIRT) di semua kementerian, lembaga, institusi di segala sektor, juga ekosistem industri nasional pendukung keamanan siber dalam negeri masih lemah. Para pengembang yang mengembangkan perangkat lunak maupun perangkat keras guna mencegah dan menangani celah keamanan siber masih sedikit [4]. Keamanan siber juga krusial dalam proses pengambilan, penyimpanan dan pengelolaan, analisis data umum dan data geospasial sebagaimana akan dibahas melalui beberapa studi kasus yang terjadi di dalam negeri dan luar negeri didiskusikan di Bab 4. Pentingnya keamanan siber dalam pengelolaan data geospasial akan menjadi fokus masalah

dalam penelitian ini dengan perumusan masalah yang akan diuraikan pada sub bab selanjutnya.

1.2 Rumusan Masalah

Beberapa rumusan masalah pada penelitian ini adalah:

1. Apa penyebab utama penyerangan siber data geospasial.
2. Bagaimana menemukan teknik pencegahan dan mitigasi terhadap kejadian/insiden penyerangan siber data geospasial.
3. Bagaimana cara meningkatkan pengamanan akses dan data geospasial.

1.3 Batasan Permasalahan

Masalah yang dirumuskan di atas dibatasi ruang lingkupnya untuk sektor keamanan siber dalam data geospasial di konteks negara Indonesia dan pemangku kepentingan pembuat kebijakan/pemerintah, pelaku industri/ bisnis, akademisi/pakar keamanan siber, dan organisasi masyarakat sipil *(civil society organization)*.

1.4 Tujuan Penelitian

Penelitian yang berjudul "Pentingnya Keamanan Siber dalam Data Geospasial di Indonesia" memiliki beberapa tujuan:

1. Penelitian akan menganalisis penyebab utama serangan siber terhadap data geospasial.
2. Penelitian juga akan mengidentifikasi teknik/metodologi pencegahan dan mitigasi terhadap serangan siber pada data geospasial.

1.5 Manfaat Penelitian

Tugas akhir ini memiliki beberapa manfaat mengenai keamanan siber pada data geospasial, sebagai berikut:

1. Untuk memahami sistem informasi berbasis data serta pentingnya perlindungan data geospasial terhadap serangan siber.

2. Untuk mengidentifikasi penyebab-penyebab utama serangan siber terhadap data geospasial.

3. Untuk mengetahui teknik atau metodologi yang sesuai dalam upaya pencegahan dan mitigasi serangan siber pada data geospasial.

Secara praktis, penelitian bermanfaat juga bagi perusahaan atau lembaga dalam menerapkan langkah-langkah keamanan siber yang efektif, baik pengelolaan operator-nya (aspek sumber daya manusia/*human capital*) maupun pengelolaan perangkat (baik perangkat lunak/*software* ataupun perangkat keras/*hardware*) oleh karena pada saat ini data menunjukkan bahwa jumlah perangkat lebih banyak dibandingkan jumlah manusia, dan mengakibatkan peretas menjadi lebih inovatif [5].