

BAB 1

PENDAHULUAN

1.1 LATAR BELAKANG

Masalah global dalam era digital ini semakin berkembang dengan pesatnya, di mana kejahatan siber menjadi ancaman yang tidak dapat diabaikan bagi semua negara di dunia. Fenomena ini menjadi semakin kompleks dengan adanya interkoneksi yang luas antar negara melalui internet. Di Indonesia, pemahaman tentang pentingnya menghadapi risiko keamanan siber masih belum merata. Ada kesalahpahaman bahwa kecepatan internet yang rendah tidak memerlukan perhatian serius terhadap keamanan siber, yang bisa menjadi kesalahan yang berakibat fatal (Satria et al., 2024). Sifat dunia digital yang saling berhubungan dan perkembangan teknologi baru telah menciptakan lanskap yang dipenuhi dengan potensi ancaman keamanan siber. Ancaman ini termasuk pencurian data, penipuan online, serangan malware, dan sabotase sistem komputer, yang memiliki implikasi serius bagi keamanan nasional dan stabilitas sosial (Sumadinata, 2023). Mengatasi tantangan ini membutuhkan kerja sama internasional, penegakan hukum yang kuat, dan harmonisasi hukum internasional. Membangun keamanan siber yang lebih baik dan menerapkan strategi pencegahan sangat penting dalam mengurangi dampak kejahatan dunia maya pada individu, organisasi, dan masyarakat (Sang & Trung, 2022).

Di tingkat yang lebih spesifik, pemerintah daerah juga dihadapkan pada tantangan yang serupa. Dengan meningkatnya ketergantungan pada infrastruktur teknologi informasi, seperti sistem basis data populasi, layanan online publik, dan sistem keuangan regional, keamanan siber menjadi aspek penting yang harus ditanggapi dengan serius. Serangan siber pada infrastruktur kota yang penting dapat menyebabkan pencurian informasi sensitif, penghancuran data, atau pengungkapan data pribadi, serta dapat mengakibatkan hilangnya waktu kerja dan penangguhan sistem, yang dapat memiliki konsekuensi serius bagi kelangsungan hidup kota. Strategi adopsi teknologi digital pemerintah daerah harus mencakup membangun

platform untuk partisipasi publik, pengembangan keterampilan karyawan, pengembangan pola pikir positif pembuat keputusan, mengenali peran pemain, memiliki tujuan dan prosedur yang jelas, regulasi yang tepat, dan menerima masukan pengguna (David et al., 2023). Tantangan yang dihadapi pemerintah daerah dalam menerapkan Sistem Pemerintahan Berbasis Elektronik (SPBE) meliputi topografi daerah, fasilitas, infrastruktur, sumber daya manusia, digitalisasi, dan kebijakan. Sistem Pemerintahan Berbasis Elektronik (SPBE) merupakan bentuk penyelenggaraan pemerintahan yang menggunakan teknologi informasi dan komunikasi untuk memberikan layanan kepada para pengguna SPBE. Sebelum diberlakukan Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, konsep ini lebih dikenal dengan istilah E-government atau Electronic Government (Rusdy & Flambonita, 2023). Transformasi digital menuntut kerja sama antara berbagai lapisan administrasi untuk mendukung digitalisasi pemerintah daerah yang efektif dan efisien, sementara itu juga mengatasi tantangan yang muncul dalam manajemen risiko keamanan siber dan perlindungan data (Nafi'ah, 2022). Untuk mengatasi tantangan ini, solusi yang perlu diadopsi adalah dengan mengimplementasikan Model Digital Forensic Readiness Index (DiFRI). Model ini memberikan panduan terstruktur untuk identifikasi, perlindungan, deteksi, respons, dan pemulihan terhadap insiden keamanan siber (Dheanda Absharina & Sutabri, 2023).

Dengan menggunakan model DiFRI, pemerintah daerah dapat secara sistematis menilai kesiapan forensik digital mereka dan mengukur tingkat kesiapsiagaan mereka. Model DiFRI juga dapat digunakan untuk mengukur tingkat kesiapan forensik digital organisasi siber. Menerapkan model DiFRI dapat membantu organisasi meningkatkan kesiapan forensik digital mereka dan secara efektif mencegah dan mengelola serangan siber (Panggabean, 2021).

Walaupun DiFRI telah diperkenalkan, ada beberapa tantangan dalam mengimplementasikannya, termasuk kurangnya kesadaran dan pemahaman tentang pentingnya keamanan siber di kalangan pejabat pemerintah daerah. Selain itu, keterbatasan sumber daya manusia, anggaran, dan infrastruktur teknologi informasi

yang tidak memadai juga dapat menghambat penerapan model ini secara efektif (Ramadhan et al., 2022).

Oleh karena itu, dalam penelitian ini disarankan untuk menerapkan *Digital Forensic Readiness Index* (DiFRI) sebagai langkah strategis untuk memperkuat sistem keamanan siber dalam menghadapi tantangan kejahatan siber. Namun, penting untuk mengidentifikasi faktor-faktor yang mempengaruhi keberhasilan penerapan model ini. Salah satu solusi yang dapat diajukan adalah meningkatkan kesadaran dan pemahaman tentang pentingnya keamanan siber di kalangan pejabat pemerintah daerah melalui pelatihan dan *workshop* yang terarah. Selain itu, perlu dilakukan alokasi sumber daya manusia, anggaran, dan peningkatan infrastruktur teknologi informasi yang sesuai dengan kebutuhan untuk mendukung efektivitas penerapan DiFRI. Dengan langkah-langkah ini, diharapkan Pemerintah Kota Yogyakarta dapat memperkuat kesiapannya dalam menghadapi ancaman kejahatan siber secara lebih efektif.

1.2 PERUMUSAN MASALAH

Meskipun forensik digital penting dalam menangani kejahatan siber, masih ada kesenjangan dalam pemahaman tentang kesiapan institusi pemerintahan dalam menghadapi tantangan ini. Model DiFRI diakui secara global untuk mengukur kesiapan forensik digital, namun penelitian yang menerapkannya pada institusi pemerintahan masih kurang.

Berdasarkan pernyataan di atas, terdapat beberapa point perumusan masalah dalam Penelitian ini, yaitu:

1. Tingkat kesiapan Pemerintah Kota Yogyakarta dalam menghadapi kejahatan siber berdasarkan model DiFRI.
2. Faktor-faktor yang mempengaruhi tingkat kesiapan Pemerintah Kota Yogyakarta dalam menghadapi kejahatan siber
3. Strategi yang dapat dilakukan untuk meningkatkan kesiapan Pemerintah Kota Yogyakarta dalam menghadapi kejahatan siber.

1.3 PERTANYAAN PENELITIAN

Adapun pertanyaan yang menjadi dasar penelitian yaitu:.

1. Bagaimana tingkat kesiapan Pemerintah Kota Yogyakarta dalam menghadapi kejahatan siber berdasarkan model *Digital Forensic Readiness Index* (DiFRI)?
2. Apa saja faktor-faktor yang mempengaruhi tingkat kesiapan Pemerintah Kota Yogyakarta dalam menghadapi kejahatan siber?
3. Strategi apa yang dapat dilakukan untuk meningkatkan kesiapan Pemerintah Kota Yogyakarta dalam menghadapi kejahatan siber?

1.4 TUJUAN PENELITIAN

Penelitian ini bertujuan untuk menganalisis kesiapan Pemerintah Kota Yogyakarta dalam menghadapi kejahatan siber dengan menggunakan Model *Digital Forensic Readiness Index* (DiFRI). Selain itu, penelitian ini juga mengevaluasi sejauh mana Pemerintah Kota Yogyakarta telah siap dalam menghadapi ancaman kejahatan siber, serta mengidentifikasi faktor-faktor yang mempengaruhi tingkat kesiapan tersebut. Rekomendasi konkret akan diberikan kepada Pemerintah Kota Yogyakarta untuk memperkuat sistem keamanan siber berdasarkan temuan analisis menggunakan DiFRI. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam meningkatkan kesiapan Pemerintah Kota Yogyakarta dalam menghadapi tantangan kejahatan siber di era digital saat ini.

1.5 MANFAAT HASIL PENELITIAN

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Peningkatan Kesadaran

Penelitian ini membantu meningkatkan kesadaran masyarakat dan pemerintah tentang pentingnya keamanan siber dan forensik digital. Dengan pemahaman yang lebih baik tentang risiko dan konsekuensi dari keamanan siber, pembaca dapat mempersiapkan diri dengan langkah-langkah pencegahan yang sesuai.

2. Perbaikan Kesiapan Forensik

Melalui *Digital Forensic Readiness Index* (DiFRI), instansi pemerintah dapat mengevaluasi tingkat kesiapan mereka dalam menghadapi insiden kejahatan

siber. Ini memungkinkan instansi pemerintah untuk mengidentifikasi kelemahan dan memperbaiki sistem keamanan mereka agar lebih efisien dalam mendeteksi, menangani, dan merespons serangan siber.

3. Kesiapsiagaan Serangan Siber

Dengan fokus pada strategi pencegahan sebelum serangan terjadi, penelitian ini membantu menciptakan pendekatan yang lebih proaktif. Dengan pemahaman mendalam tentang faktor-faktor yang mempengaruhi kemampuan organisasi dalam mengelola kesiapsiagaan serangan siber, instansi pemerintah dapat mengimplementasikan langkah-langkah yang lebih efektif untuk melindungi diri dari serangan.

4. Kontribusi pada Pengembangan Ilmu

Penelitian ini memberikan kontribusi penting bagi pengembangan forensik digital dengan memperkenalkan *Digital Forensic Readiness Index* (DiFRI) sebagai alat evaluasi yang dapat digunakan secara luas. Hal ini memperkaya pemahaman tentang forensik digital dan meningkatkan praktik dalam menghadapi kejahatan siber.

5. Penguatan Institusi Pemerintah

Dengan meningkatkan kesiapan institusi pemerintah dalam menghadapi kejahatan siber, Penelitian ini membantu memperkuat keamanan nasional dan melindungi kepentingan publik dari ancaman serangan yang dapat menyebabkan kerugian finansial dan pencurian data sensitif serta gangguan terhadap layanan publik yang penting.