Data *Forgery* dan Cyber Espionage: Analisis Kejahatan Siber, Modus Operandi, dan Strategi Penanggulangan

Link Website Blog: https://webmakalah.vercel.app

Dosen Pengampu :

Fidya Eka Prahesti, M.T

Disusun Oleh

Kelompok 3 :

1. **Adhinata Nickola Wiratama (2413030040)**
2. **Inka Aulia Murdin Ningsih (2413030051)**
3. **Mukhammad Khoirul Aminin (2413030033)**
4. **Mochammad Fathur Rahman (2413030049)**
5. **Panji Satria Nurfadilla (2413030042)**
6. **Nanda Firstyanto Putra (2413030046)**

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS TEKNIK DAN ILMU KOMPUTER

UNIVERSITAS NUSANTARA PGRI KEDIRI

2025

KATA PENGANTAR

Puji syukur kami panjatkan kepada Tuhan Yang Maha Esa, karena atas limpahan rahmatnya penyusun dapat menyelesaikan makalah ini tepat waktu tanpa ada halangan yang berarti dan sesuai dengan harapan.

Ucapan terima kasih kami sampaikan kepada ibu Fidya Eka Prahesti, M.T sebagai dosen pengampu mata kuliah Etika profesi yang telah membantu memberikan arahan dan pemahaman dalam penyusunan makalah ini.

Kami menyadari bahwa dalam penyusunan makalah ini masih banyak kekurangan karena keterbatasan kami. Maka dari itu penyusun sangat mengharapkan kritik dan saran untuk menyempurnakan makalah ini. Semoga apa yang ditulis dapat bermanfaat bagi semua pihak yang membutuhkan.

Kediri, 18 Desember 2025

Kelompok 3

DAFTAR ISI

BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi pada era digital memberikan banyak manfaat bagi masyarakat , pemerintahan , dan sector industry. kemajuan ini juga diiringi oleh meningkatnya kejahatan siber yang semakin kompleks dan sulit dideteksi. Sejumlah penelitian mengungkap bahwa aktivitas kriminal di ruang digital tidak hanya meningkat jumlahnya, tetapi juga berkembang dalam bentuk yang lebih canggih, terutama manipulasi data dan spionase siber. Kedua kejahatan ini menimbulkan ancaman serius bagi integritas data, keamanan informasi, serta stabilitas nasional di berbagai negara. Salah satu bentuk kejahatan yang semakin marak adalah Data *Forgery*, yaitu tindakan pemalsuan atau manipulasi data elektronik dalam sistem komputer. Dalam jurnal yang ditulis Popal (2023), pemalsuan data dikategorikan sebagai salah satu bentuk *cybercrime* signifikan yang muncul akibat kemajuan teknologi, sejajar dengan carding, phishing, ransomware, hingga *cyber espionage*. Manipulasi data ini dapat merusak keakuratan informasi, mengganggu proses bisnis, dan menimbulkan kerugian finansial maupun reputasional bagi organisasi.

Selain itu *Cyber Espionage* atau spionase siber juga menjadi ancaman besar dalam konteks keamanan digital. Jurnal kebijakan spionase siber karya Sodiq pada (2024) menjelaskan bahwa spionase siber dilakukan dengan menembus jaringan komputer untuk memperoleh data sensitif seperti dokumen pemerintah, rahasia dagang, atau informasi strategis lain yang memiliki nilai politik maupun ekonomi. Serangan ini sering dilakukan oleh kelompok terorganisir bahkan aktor negara, sehingga memiliki dampak luas terhadap keamanan nasional. Penelitian lain menunjukkan bahwa Indonesia dan berbagai negara seperti Jerman menghadapi peningkatan dan industri strategis. Peningkatan kedua kejahatan ini semakin mengkhawatirkan karena melibatkan metode kompleks dan pelaku yang sulit dilacak. Kasus-kasus seperti penyadapan telekomunikasi, pencurian rahasia dagang, hingga pembobolan data industri farmasi menunjukkan bahwa spionase siber telah menjadi instrumen baru dalam kompetisi geopolitik dan ekonomi global.

Disisi lain, lemahnya pengawasan, kurangnya literasi digital, serta kelemahan kerangka hukum menjadikan banyak organisasi, terutama di negara berkembang, rentan terhadap ancaman ini.

Oleh karena itu, penting untuk melakukan kajian mendalam mengenai bagaimana Data *Forgery* dan *Cyber Espionage* terjadi, apa saja motif dan teknik yang digunakan pelaku, serta bagaimana dampaknya terhadap keamanan informasi. Berdasarkan urgensi tersebut, makalah berjudul **"**Data *Forgery* dan *Cyber Espionage*: Ancaman Keamanan Informasi di Era Digital dan Upaya Penanggulangan**"** disusun untuk memberikan pemahaman komprehensif, sekaligus menyoroti strategi pencegahan dan penanggulangan yang dapat diterapkan dalam menghadapi ancaman keamanan informasi di era digital.

B. Rumusan Masalah

Berdasarkan uraian latar belakang tersebut, maka permasalahan yang menjadi fokus penelitian adalah: Bagaimana bentuk ancaman Data *Forgery* dan *Cyber Espionage* terhadap keamanan informasi di era digital serta upaya penanggulangan yang dapat dilakukan untuk mengatasinya?

C. Tujuan Penulisan

Tujuan penelitian ini adalah untuk:

1. Menjelaskan bagaimana Data *Forgery* dan *Cyber Espionage* menjadi ancaman terhadap keamanan di era digital.
2. Menganalisis dampak yang ditimbulkan dari kedua pihak bentuk kejahatan siber tersebut.
3. Menguraikan upaya penanggulangan yang dapat dilakukan untuk mencegah dan meminimalkan ancaman Data *Forgery* dan Cyber Espionage.

D. Manfaat

Penelitian mengenai Data *Forgery* dan *Cyber Espionage* ini memberikan manfaat dalam bentuk pemahaman yang lebih mendalam mengenai karakteristik, modus, dan dampak kedua kejahatan siber tersebut terhadap keamanan informasi di era digital. Kajian ini juga berkontribusi secara praktis dengan memberikan gambaran mengenai langkah-langkah penanggulangan yang dapat diterapkan oleh organisasi, instansi, maupun masyarakat untuk meningkatkan kesiapsiagaan

terhadap ancaman pemalsuan data dan spionase siber. Selain itu, penelitian ini memiliki manfaat akademis karena dapat menjadi referensi tambahan dalam bidang studi keamanan siber dan sistem informasi, sekaligus memperkaya literatur yang dapat digunakan oleh mahasiswa dan peneliti dalam mengembangkan analisis atau penelitian lanjutan terkait isu-isu keamanan digital.

BAB II
TINJAU PUSTAKA

Tinjauan pustaka dalam penelitian ini disusun sebagai landasan konseptual untuk memahami permasalahan Data *Forgery* dan *Cyber Espionage* sebagai ancaman terhadap keamanan informasi di era digital. Teori-teori yang dibahas pada bab ini memberikan dasar pemikiran dalam menganalisis bentuk kejahatan siber, dampaknya terhadap data dan informasi strategis, serta upaya penanggulangan yang relevan. Penyusunan kajian teori ini mendukung pembahasan pada Bab III sesuai dengan rumusan masalah yang telah diuraikan pada Bab I.

1. Kemanan Informasi

Menurut Whitman dan Mattord (2021), keamanan informasi merupakan upaya perlindungan terhadap informasi dari akses, penggunaan, dan perubahan yang tidak sah. Keamanan informasi bertujuan menjaga informasi sebagai aset penting agar tetap aman dan dapat dipercaya. Stallings (2022) menjelaskan bahwa keamanan informasi didasarkan pada tiga prinsip utama, yaitu *confidentiality, integrity,* dan *availability*. Dalam konteks penelitian ini, Data *Forgery* berkaitan dengan pelanggaran integritas data, sedangkan *Cyber Espionage* mengancam kerahasiaan informasi strategis.

2. Kejahatn Siber (*Cybercrime*)

Menurut Popal (2023), *cybercrime* merupakan kejahatan yang memanfaatkan teknologi informasi dan jaringan komputer sebagai sarana atau sasaran. Kejahatan siber bersifat lintas batas, sulit dilacak, dan berdampak luas. Popal (2023) mengelompokkan *cybercrime* ke dalam berbagai bentuk, termasuk pemalsuan data dan spionase siber. Data *Forgery* dan *Cyber Espionage* termasuk kejahatan siber yang menargetkan data dan informasi, sehingga berpotensi besar mengganggu keamanan informasi di era digital.

3. Data *Forgery*

Menurut O’Brien dan Marakas (2021), Data *Forgery* adalah tindakan pemalsuan atau manipulasi data elektronik secara tidak sah dengan

tujuan tertentu, seperti memperoleh keuntungan atau menyesatkan pihak lain. Pemalsuan data dapat terjadi akibat lemahnya sistem pengamanan dan pengawasan internal. Popal (2023) menyatakan bahwa Data *Forgery* berdampak serius karena dapat merusak keandalan sistem informasi, menurunkan kepercayaan publik, serta menimbulkan kerugian finansial dan reputasi.

4. Cyber Espionage

Menurut Esty Pratiwi (2022), *Cyber Espionage* merupakan aktivitas pencurian informasi strategis melalui media siber yang dilakukan secara tersembunyi dan terencana. Informasi yang menjadi sasaran meliputi rahasia negara, kebijakan pemerintahan, serta rahasia dagang. Popal (2023) menjelaskan bahwa *cyber espionage* sering melibatkan aktor dengan kemampuan teknis tinggi dan berpotensi melemahkan keamanan nasional karena melanggar prinsip kerahasiaan informasi.

5. *Advanced Persistent Threat* (APT)

Menurut Sodiq dkk. (2024), *Advanced Persistent Threat* (APT) merupakan serangan siber yang bersifat terarah, canggih, dan berjangka panjang. APT digunakan dalam *cyber espionage* untuk menyusup ke sistem target dan mempertahankan akses dalam waktu lama melalui teknik seperti *phishing*, malware, dan eksploitasi celah keamanan. Keberadaan APT menunjukkan bahwa *cyber espionage* telah menjadi bagian dari strategi perang siber modern.

6. Kerangka Hukum dan Upaya Penanggulan

Menurut Esty Pratiwi (2022), penanggulangan *cyber espionage* dan kejahatan siber memerlukan dukungan kerangka hukum yang kuat. Di Indonesia, kejahatan siber diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta regulasi perlindungan data. Popal (2023) menekankan bahwa penanggulangan efektif harus dilakukan secara komprehensif melalui penguatan regulasi, peningkatan kesadaran keamanan siber, serta penerapan teknologi pengamanan informasi. Kerangka ini menjadi dasar analisis pada Bab III.

BAB III
PEMBAHASAN

Bab ini membahas analisis kasus Data *Forgery* dan *Cyber Espionage* sebagai bentuk kejahatan siber yang mengancam keamanan informasi di era digital. Pembahasan difokuskan pada gambaran umum kasus, motif pelaku, faktor penyebab, dampak yang ditimbulkan, serta upaya penanggulangan yang dapat dilakukan. Analisis pada bab ini disusun berdasarkan rumusan masalah serta landasan pustaka yang telah diuraikan pada bab sebelumnya.

1. Gambaran Umum

Perkembangan teknologi informasi yang semakin pesat telah mendorong peningkatan pemanfaatan sistem digital dalam berbagai sektor, baik pemerintahan, bisnis, maupun layanan publik. Namun, kondisi ini juga diikuti dengan meningkatnya ancaman kejahatan siber, salah satunya berupa Data *Forgery* dan Cyber Espionage. Data *Forgery* umumnya terjadi dalam bentuk pemalsuan atau manipulasi data elektronik, seperti perubahan data transaksi, dokumen digital, maupun informasi identitas. Sementara itu, *Cyber Espionage* dilakukan melalui penyusupan sistem untuk memperoleh informasi strategis secara ilegal dan tersembunyi.

Beberapa kasus yang dibahas dalam jurnal menunjukkan bahwa kedua bentuk kejahatan ini sering kali menargetkan institusi yang memiliki data bernilai tinggi, seperti lembaga pemerintahan, perusahaan teknologi, dan sektor keuangan. Serangan dilakukan dengan memanfaatkan kelemahan sistem keamanan informasi, baik dari sisi teknis maupun manajerial. Hal ini menunjukkan bahwa Data *Forgery* dan *Cyber Espionage* tidak berdiri sendiri, melainkan berkaitan erat dengan lemahnya pengelolaan keamanan informasi secara menyeluruh.

2. Motif Pelaku

Motif pelaku menjadi aspek penting dalam memahami terjadinya Data *Forgery* dan Cyber Espionage. Dalam kasus Data *Forgery*, motif ekonomi dan kepentingan pribadi sering menjadi faktor dominan. Pelaku

memalsukan atau memanipulasi data untuk memperoleh keuntungan finansial, menghindari tanggung jawab hukum, atau memengaruhi hasil keputusan tertentu. Dalam konteks organisasi, pemalsuan data juga dapat dilakukan untuk menutupi kelemahan sistem atau kesalahan manajerial.

Berbeda dengan Data *Forgery*, *Cyber Espionage* umumnya didorong oleh motif strategis jangka panjang. Pelaku *cyber espionage* tidak hanya mencari keuntungan langsung, tetapi berupaya mengumpulkan informasi rahasia yang bernilai tinggi, seperti kebijakan negara, teknologi strategis, atau rahasia dagang. Motif ini menjadikan *cyber espionage* sebagai ancaman serius karena sering dilakukan oleh kelompok terorganisir dengan sumber daya dan kemampuan teknis yang tinggi, bahkan melibatkan aktor negara.

3. Gambaran Umum

Terjadinya Data *Forgery* dan *Cyber Espionage* dipengaruhi oleh berbagai faktor yang saling berkaitan. Dari sisi teknis, lemahnya sistem keamanan informasi menjadi faktor utama, seperti penggunaan sistem yang tidak diperbarui, kurangnya mekanisme autentikasi yang kuat, serta minimnya pengawasan terhadap aktivitas sistem. Celah keamanan ini memberikan peluang bagi pelaku untuk memanipulasi data atau menyusup ke dalam sistem tanpa terdeteksi.

Selain faktor teknis, faktor non-teknis juga berperan besar. Kurangnya kesadaran pengguna terhadap pentingnya keamanan informasi, lemahnya budaya keamanan siber dalam organisasi, serta kurang optimalnya pengawasan internal turut meningkatkan risiko kejahatan siber. Di sisi lain, keterbatasan regulasi dan penegakan hukum, terutama dalam kasus lintas negara, menjadikan Data *Forgery* dan *Cyber Espionage* sulit dicegah dan ditindak secara efektif.

4. Dampak Terhadap Keamanan Informasi

Dampak yang ditimbulkan oleh Data *Forgery* dan *Cyber Espionage* tidak hanya bersifat teknis, tetapi juga berdampak luas secara ekonomi,

sosial, dan strategis. Data *Forgery* dapat menyebabkan kesalahan pengambilan keputusan karena informasi yang digunakan tidak akurat. Hal ini berpotensi menimbulkan kerugian finansial, menurunkan kepercayaan publik, serta merusak reputasi organisasi atau institusi yang terlibat.*Cyber Espionage* memiliki dampak yang lebih kompleks karena menyasar informasi strategis. Kebocoran data rahasia dapat melemahkan daya saing perusahaan, mengganggu stabilitas pemerintahan, serta mengancam keamanan nasional. Selain itu, keberhasilan serangan *cyber espionage* menunjukkan lemahnya sistem pertahanan siber, yang dapat dimanfaatkan kembali oleh pelaku untuk serangan lanjutan.

5. Upaya Penanggulangan

Upaya penanggulangan Data *Forgery* dan *Cyber Espionage* harus dilakukan secara terpadu melalui pendekatan teknis dan non-teknis. Dari aspek teknis, penguatan sistem keamanan informasi menjadi langkah utama, seperti penerapan kontrol akses yang ketat, enkripsi data, audit sistem secara berkala, serta penggunaan teknologi deteksi ancaman. Langkah-langkah ini bertujuan untuk mencegah manipulasi data dan mendeteksi aktivitas mencurigakan sejak dini. Dari aspek non-teknis, peningkatan kesadaran dan literasi keamanan siber bagi pengguna dan pengelola sistem menjadi faktor penting dalam pencegahan kejahatan siber. Selain itu, penguatan regulasi dan kerja sama lintas negara diperlukan untuk menghadapi karakteristik *cyber espionage* yang bersifat transnasional. Dengan sinergi antara aspek teknis, hukum, dan sumber daya manusia, ancaman Data *Forgery* dan *Cyber Espionage* dapat ditekan secara lebih efektif.

BAB III
KESIMPULAN

Berdasarkan pembahasan yang telah diuraikan pada bab-bab sebelumnya, dapat disimpulkan bahwa Data *Forgery* dan *Cyber Espionage* merupakan bentuk kejahatan siber yang berkembang seiring dengan meningkatnya ketergantungan terhadap sistem informasi digital. Kedua kejahatan tersebut memanfaatkan kelemahan sistem keamanan informasi dan tata kelola organisasi, sehingga berpotensi mengancam integritas, kerahasiaan, dan keandalan data sebagai aset strategis di era digital.diuraikan pada bab-bab sebelumnya, dapat disimpulkan bahwa Data *Forgery* dan *Cyber Espionage* merupakan bentuk kejahatan siber yang berkembang seiring dengan meningkatnya ketergantungan terhadap sistem informasi digital. Kedua kejahatan tersebut memanfaatkan kelemahan sistem keamanan informasi dan tata kelola organisasi, sehingga berpotensi mengancam integritas, kerahasiaan, dan keandalan data sebagai aset strategis di era digital.

Upaya penanggulangan Data *Forgery* dan *Cyber Espionage* tidak dapat dilakukan secara parsial, melainkan memerlukan pendekatan yang komprehensif. Penguatan sistem keamanan informasi melalui penerapan teknologi pengamanan yang memadai, peningkatan kesadaran dan literasi keamanan siber, serta dukungan regulasi dan penegakan hukum yang efektif menjadi langkah penting dalam meminimalkan risiko kejahatan siber. Dengan sinergi antara aspek teknis, sumber daya manusia, dan kebijakan hukum, ancaman Data *Forgery* dan *Cyber Espionage* diharapkan dapat ditekan sehingga tercipta lingkungan digital yang lebih aman dan terpercaya.

DAFTAR PUSTAKA

O’Brien, J. A., & Marakas, G. M. (2021). *Management information systems*. New York: McGraw-Hill Education.

Popal, M. (2023). Kejahatan siber dan implikasinya terhadap keamanan informasi di era digital. *Jurnal Keamanan Siber dan Teknologi Informasi*, 5(2), 45 58.

Pratiwi, E. (2022). Cyber espionage dan tantangannya terhadap keamanan nasional. *Jurnal Keamanan Informasi*, 4(1), 12–24.

Sodiq, A., dkk. (2024). Kebijakan dan strategi penanggulangan cyber espionage di era globalisasi digital. *Jurnal Kebijakan Keamanan Siber*, 6(1), 30–44.

Stallings, W. (2022). *Effective cybersecurity: A guide to using best practices and standards*. Boston: Pearson Education.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Boston: Cengage Learning.