Jurnal Transformasi Humaniora

JTH, 8 (4), April 2025
ISSN: 21155640

DINAMIKA KEAMANAN SIBER: ANALISIS ANCAMAN SIBER TERHADAP PENYELENGGARAAN DIGITALISASI PEMERINTAHAN

Rizka Ramadhani [1], M. Hamdi Hs[2]
Email: rmdhnrzx940@gmail.com[1], hamdi.hs@unmuhjember.ac.id[2],
Universitas Muhammadiyah Jember

Abstrak: Pemanfaatan internet yang semakin masif di tengah masyarakat telah mendorong pemerintah untuk membuat perubahan tata kelola penyelenggaraan pemerintahan ke arah digitalisasi. Dalam upaya tersebut, semangat pemerintah dalam melakukan digitalisasi tata kelola harus diikuti oleh jaminan keamanan sektor siber. Indonesia adalah negara dengan jumlah pengguna internet yang cukup besar dan tentunya diikuti oleh penyelenggaraan pemerintahan yang semakin berbasis digital. Oleh karena itu, tulisan ini akan memaparkan analisis tentang ancaman terhadap keamanan siber yang berpotensi mengganggu penyelenggaraan pemerintahan. Tulisan menggunakan metode penelitian kualitatif dengan pendekatan Analisis data menggunakan Nvivo. Setelah elaborasi lebih lanjut, dapat diketahui bahwa semakin ke depan ancaman siber semakin kompleks sehingga membutuhkan adaptasi yang cepat oleh pemerintah. Aspek kepastian hukum, kelembagaan yang tidak tumpang tindih tupoksinya, hingga edukasi tentang ancaman siber terhadap pejabat pengambil keputusan pada khususnya dan masyarakat luas pada umumnya perlu diberikan fokus yang sama oleh pemerintah. Jaminan keamanan ruang siber dari potensi ancaman perlu diadakan untuk terlaksananya penyelenggaraan pemerintahan berbasis digital yang maksimal.
Kata Kunci: Ancaman; Keamanan; Siber; Penyelenggaraan Pemerintahan; Digitalisasi.

PENDAHULUAN

Perang siber merupakan jenis perang baru dalam beberapa dekade belakangan ini yang telah mengancam eksistensi semua negara. Indonesia sebagai negara dengan jumlah penduduk, cadangan sumber daya alam, dan porsi ekonomi global yang besar tentu membutuhkan jaminan pertahanan yang kuat di ruang siber. Dampak dari dinamika perang siber yang tidak mengenal lintas batas harus dapat dimitigasi apapun bentuk ancamannya yang dapat membahayakan penyelenggaraan pemerintahan, terutama dalam hal tata kelola yang ter-digitalisasi.

Kemajuan di bidang teknologi dan informasi telah memberi pengaruh besar dalam penyelenggaraan pemerintahan, mulai dari ekonomi, politik, sosial serta keamanan. Sifat alamiah dari ancaman dan keamanan adalah dinamis, terbukti bahwa ancaman dan keamanan bukanlah hal yang dapat selesai untuk dibicarakan, di diskusikan dan berhenti untuk diperbaharui. Pada abad ke-21, ancaman yang sering terjadi adalah ancaman yang bersifat tidak terlihat (intangible). Tingginya angka user aktif internet semestinya diimbangi oleh tingkat keamanan siber yang terjamin, sehingga arus informasi dan aktivitas masyarakat serta penyelenggaraan pemerintahan dapat terjaga keamanan dan kerahasiaannya. Sementara kondisi Indonesia dalam hal keamanan siber masih rendah dan lemah, hal tersebut yang mempengaruhi terjadi banyak peretasan data pribadi individu, seperti alamat, identitas sampai kartu debit nasabah bank. Selain menyasar data individu, kelemahan keamanan siber Indonesia juga menarget penyelenggaraan pemerintahan seperti kasus-kasus spionase, intelijen, hacking dan lain-lain (Makbull, 2022).

Pemerintah telah berupaya untuk menjamin keamanan siber dalam beberapa bentuk kebijakan, yaitu Capacity Building (program pelatihan dan pengembangan

keamanan siber dilaksanakan berkoordinasi dengan kelompok kerja Pusat Operasi Pertahanan Siber), dan UU Pidana Siber (beberapa pasal UU ITE) (Ariyaningsih, 2023). Adapun tujuan dari dilakukannya penelitian ini adalah untuk menganalisa bentuk-bentuk ancaman siber yang berpotensi mengganggu penyelenggaraan pemerintahan Indonesia, terutama dalam hal tata kelola yang terdigitalisasi. Sedangkan tujuan khusus dari penelitian ini adalah untuk menganalisa kesiapan Indonesia dalam menyelenggarakan tata kelola berbasis kolaborasi di era digital yang rawan terhadap ancaman dari perang siber yang tidak mengenal lintas batas.

METODE

Metode penelitian yang dipakai penulis dalam artikel ini adalah metode penelitian kualitatif. Menurut beberapa ahli, metode penelitian kualitatif memiliki definisi yang berbeda namun saling melengkapi. Menurut Hardani penelitian kualitatif adalah suatu penelitian yang pada dasarnya menggunakan pendekatan deduktif-induktif dan analisis data menggunakan Nvivo. Pendekatan tersebut berasal dari sebuah kerangka teori, gagasan para ahli atau pakar, serta pemahaman peneliti berdasarkan pengalamannya yang nantinya dikembangkan menjadi permasalahan-permasalahan berikut pemecahannya yang diajukan untuk mendapatkan sebuah pembenaran atau verifikasi dalam wujud dukungan data empiris di laporan.

Menurut Sugiyono penelitian kualitatif adalah metode penelitian yang didasarkan pada filsafat postpositivisme, dipakai untuk meneliti suatu kondisi obyek yang alamiah, (sebagai lawannya adalah eksperimen) di mana peneliti adalah sebagai instrumen penting atau kunci, teknik pengumpulan data dilakukan secara triangulasi (gabungan), analisis data bersifat induktif/kualitatif, dan hasil penelitian kualitatif lebih menekankan makna dari pada generalisasi. Penelitian kualitatif dapat dikatakan sebagai proses memahami pemaknaan orang atau komunitas yang berbeda tentang masalah sosial.

Penelitian ini mengambil jenis data sekunder dengan menggunakan teknik pengumpulan data berupa Studi Pustaka (Library Research), menurut Sugiyono teknik ini merupakan kajian teoritis, referensi serta literatur ilmiah lainnya yang berkaitan dengan budaya, nilai dan norma yang berkembang pada situasi sosial yang diteliti. Tulisan ini akan menganalisis penelitian terdahulu yang memang relevan dengan topik pembahasan. Pendekatan yang diambil dalam penelitian ini adalah pendekatan deskriptif, pendekatan yang menginterpretasikan bahan yang telah terkumpul untuk memperoleh gambaran umum tentang keadaan sebenarnya. Di mana tulisan ini akan menekankan pada fenomena dinamika perang siber yang tidak mengenal lintas batas yang berpotensi menjadi ancaman penyelenggaraan pemerintahan, terutama dalam hal tata kelola yang terdigitalisasi.

Penelitian ini juga memanfaatkan teknik analisis grounded theory, di mana teknik ini bertujuan mengembangkan teori secara induktif tentang sebuah fenomena melalui tahap pengkodean data, Axial Coding (mencari hubungan antar kategori dari hasil pengkodean data, dan Selective Coding (merumuskan teori baru setelah memahami kaitan setiap kategori data). Software NVivo dimanfaatkan dalam penelitian ini sebagai perangkat lunak untuk mengelola, menganalisis, dan melaporkan data kualitatif.

1. Coding Analysis:

Pengelompokan data berdasarkan kategori utama yang telah ditentukan. Dalam penelitian ini, dilakukan tahapan pengodean data yang mencakup:

a. Open Coding:

- Data yang diperoleh dari berbagai sumber dikategorikan ke dalam tema-tema utama seperti Ancaman Siber, Strategi Keamanan, dan Kebijakan Pemerintah.
- Setiap dokumen dianalisis untuk menemukan pola-pola yang berulang terkait tantangan keamanan siber.

b. Axial Coding

Hubungan antar kategori dianalisis untuk memahami bagaimana berbagai ancaman siber mempengaruhi penyelenggaraan pemerintahan digital

c. Selective Coding

Pada tahap ini, data yang telah dikodekan diintegrasikan untuk menghasilkan teori atau kesimpulan mengenai kesiapan pemerintah dalam menghadapi ancaman siber.

2. Word Frequency Analysis

Analisis ini dilakukan untuk mengidentifikasi kata kata yang paling sering muncul dalam sumber data yang telah dikaji.

a. Hasil analisis menunjukkan bahwa kata-kata berikut memiliki tingkat kemunculan tinggi:

Kata Kunci	Frekuensi Kemunculan
Keamanan	87 kali
Ancaman	72 kali
Pemerintah	65 kali
Digitalisasi	58 kali
Serangan Siber	47 kali
Regulasi	39 kali

b. Grafik Word Cloud yang dihasilkan oleh NVivo menunjukkan bahwa istilah "Keamanan" dan "Ancaman" mendominasi, mengindikasikan bahwa kedua aspek ini merupakan fokus utama dalam penelitian terkait keamanan siber pemerintahan.

3. Matrix Coding Query

Untuk menganalisis hubungan antara kategori data. Penelitian ini menemukan keterkaitan antara kebijakan pemerintah dengan jenis ancaman siber yang dihadapi.

Jenis Ancaman	Kebijakan yang Terkait	Kelemahan yang Ditemukan
Cybercrime	UU ITE, Regulasi BSSN	Kurangnya Perlindungan data pribadi dan lemahnya penegakan hukum
Cyber Terrorism	UU Terorisme, Keamanan Siber	Tidak ada sistem mitigasi yang cepat, dan kurangnya koordinasi antar lembaga
Cyber Warfare	Kerja Sama Internasional, TNI Cyber	Deteksi dini masih lemah, dan belum ada strategi nasional yang jelas

Temuan utama dari Matrix Coding Query:

a. Regulasi yang ada belum cukup kuat dalam menangani ancaman cybercrime
b. Ancaman cyber terrorism masih sulit diidentifikasi secara dini karena kurangnya koordinasi
c. Cyber Warfare memerlukan kebijakan strategis yang lebih jelas untuk meningkatkan kesiapan nasional.

HASL DAN PEMBAHASAN

Bentuk Ancaman Siber Bagi Indonesia

Dunia pertahanan keamanan telah membentuk sebuah persepektif baru, jika sebelumnya negara diposisikan sebagai unsur terpenting untuk dilindungi, maka persepktif baru yang muncul menempatkan manusia sebagai unsur paling penting. Persfektif tersebut dikenal dengan nama "human security". Kasus-kasus penyerangan lewat media internet terhadap banyak institusi pemerintahan di berbagai negara termasuk di Indonesia menggambarkan bahwa ancaman dan model perang yang ada antar negara saat ini berbeda bentuk dari perang generasi sebelumnya. Perang yang berbentuk konvensional dengan menggunakan kontak fisik tidak terlalu dominan, tetapi telah berubah menjadi ancaman dan perang dalam dunia teknologi dan informasi (Makbull, 2022).

Angka statistik digitalisasi yang dilakukan oleh pemerintah dalam mentransformasikan tata kelolanya, akan selalu menjadi target dari ancaman siber yang tidak mengenal lintas batas, jika negara tidak mengadakan pengamanan ruang siber. Indonesia dengan pertumbuhan pengguna internet yang terus meningkat akan selalu diikuti oleh kebutuhan jaminan pertahanan dan keamanan siber yang diselenggarakan oleh negara dengan lebih kompleks. Pemerintah sebagai penyelenggara negara perlu menganalisis dan mengedukasi masyarakat tentang bentuk ancaman-ancaman siber guna meningkatkan kolaborasi masyarakat dan pemerintah untuk menciptakan pertahanan dan keamanan ruang siber yang kuat.

Terdapat beberapa jenis ancaman siber yang dapat mengancam negara. Pertama adalah cyber crime atau kejahatan siber, hal ini terjadi di mana pelaku melakukan akses ilegal seperti transmisi ilegal dan manipulasi data untuk tujuan tertentu yang membahayakan keamanan. Misalnya adalah menciptakan gangguan dan mencari keuntungan finansial (pelakunya bisa individu atau sekelompok orang). Para pelaku kejahatan siber tentunya adalah orang yang sudah pakar dalam berbagai teknik peretasan, bahkan sering suatu aksi cyber crime dilakukan dari banyak tempat berbeda di waktu yang bersamaan. Banyak contoh aksi cyber crime yang masih sering terjadi dalam masyarakat, seperti pencurian identitas (identity theft), penipuan atau pembobolan kartu kredit (carding), memata-matai target tertentu (cyber espionage), penyebaran hoax dan lain-lain (Ariyaningsih, 2023).

Ancaman siber yang kedua adalah Cyber Terrorism. Ancaman ini berupa gerakan sejumlah jaringan atau kelompok teroris yang bertujuan untuk menggoyang stabilitas keamanan sosial, politik, serta ekonomi sebuah negara dengan memanfaatkan teknologi internet. Contohnya seperti menyerang website resmi pemerintah, melakukan penyadapan jaringan komunikasi strategis, meretas sumber data elektronik perbankan, dan lainnya. Gerakan terorisme siber ini akan sangat berbahaya jika disponsori oleh aktor negara atau pun non negara (kekuatan asing) yang memang mempunyai niat melumpuhkan stabilitas keamanan di Indonesia.

Ancaman siber yang ketiga adalah Cyber warfare. Ancaman ini adalah bentuk operasi siber (cyber operations) baik secara menyerang atau bertahan, yang dilakukan untuk tujuan membuat kerusakan atau kehancuran objek yang menjadi target operasi (Suharto and Maria Novita Apriyani 2021). Operasi siber biasanya melalui sebuah cyber attack dengan pendekatan beberapa metode yang umum, yaitu: pertama Dos (Denial of Service) atau sebuah metode kejahatan siber yang mencegah sistem komputer memenuhi permintaan akses pengguna yang berkepentingan sehingga tidak dapat digunakan layanan tersebut.

Metode serangan siber kedua adalah Injeksi SQL (Structured Query Language), merupakan jenis ancaman cyber security yang digunakan untuk mengambil kendali dan mencuri data dari pusat data. Pelaku biasanya memanfaatkan kerentanan dalam aplikasi basis data untuk memasukan perintah atau program kedalam basis data melalui pernyataan SQL. Aplikasi-aplikasi yang dibuat oleh pemerintah daerah sangat rawan karena hanya dibuat berdasarkan politik anggaran atau pembelanjaan anggaran tanpa melakukan design yang kuat. Metode ketiga adalah Social engineering. Sebuah serangan yang didasari oleh interaksi manusia yang dilakukan dengan manipulasi pengguna untuk memberikan informasi sensitive seperti . Biasanya operasi seperti ini dilakukan oleh intelijen asing yang memiliki kepentingan besar dari sebuah gejolak sosial yang terjadi.

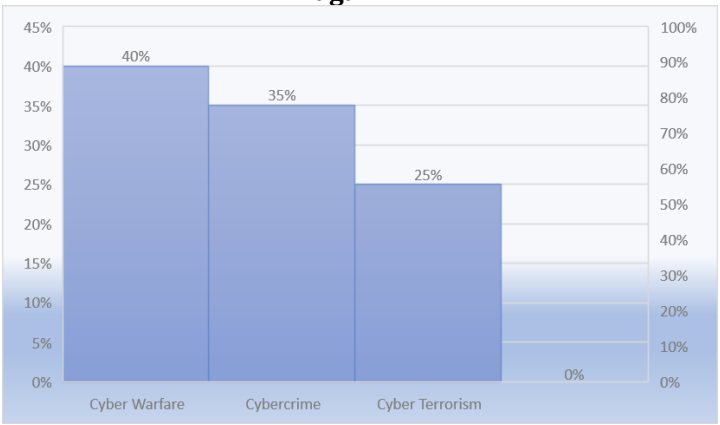
Metode serangan siber keempat adalah Malware. Berbentuk software yang diciptakan untuk membuat gangguan atau merusak komputer pengguna. Malware sering sekali menyebar melalui lampiran email atau unduhan yang terlihat sah dan sering menyasar pejabat pemerintahan yang berusia tua. Malware biasanya berbentuk Virus, Trojan, Spyware, Ransomware, Adware, dan Botnet (Ariningtiyas, 2023).

Analisis Ancaman Siber terhadap Penyelenggaraan Digitalisasi Pemerintahan (Analisis NVivo)

1. Identifikasi Kategori Ancaman Siber (Hasil Coding Analysis)

Hasil analisis menggunakan NVivo menunjukkan bahwa ancaman siber terhadap pemerintahan digital dapat dikategorikan sebagai berikut:

Bagan 1....



1. **Cybercrime – 35%**
   a. Meliputi peretasan data, pencurian informasi pribadi, dan penipuan daring.
   b. Mayoritas kasus yang ditemukan berkaitan dengan lemahnya keamanan sistem pemerintahan.
2. **Cyber Terrorism – 25%**
   a. Termasuk serangan terhadap infrastruktur pemerintah, penyebaran propaganda, dan sabotase digital.
   b. Target utama adalah lembaga pemerintahan dan infrastruktur strategis.
3. **Cyber Warfare – 40%**
   a. Melibatkan operasi ofensif dan defensif yang dilakukan oleh negara atau aktor non – negara.
   b. Pola serangan menunjukkan adanya keterlibatan kelompok yang memiliki kepentingan geopolitik.

2. Hasil Word Frequency Analysis

Hasil analisis frekuensi kata menggunakan NVivo mengkonfirmasi bahwa “Keamanan”, “Ancaman”, dan “Digitalisasi” adalah kata-kata yang paling sering muncul

dalam kajian keamanan siber.

Interpretasi temuan:

a. Menunjukkan bahwa aspek keamanan menjadi perhatian utama trasnsisi digital pemerintahan.
b. Perlu adanya kebijakan yang lebih ketat terkait mitigasi ancaman

3. Hubungan Kebijakan dan Ancaman Siber (Matrix Coding Query)

Jenis Ancaman	Hubungan dengan Kebijakan
Cybercrime	Regulasi masih lemah dan banyak celah hukum
Cyber Terrorism	Kurangnya sistem respons yang cepat
Cyber Warfare	Perlu strategi nasional yang lebih kuat

Langkah Pemerintah Indonesia Untuk Menghadapi Ancaman Siber

Indonesia dapat disebut masih sebagai negara yang berproses dalam pembentukan serta penguatan sistem keamanan dan pertahanan siber hingga sekarang. Dalam aspek kepastian hukum, Indonesia telah beberapa kali merancang dan melakukan perubahan terhadap aturan yang mengatur tentang bidang keamanan dan pertahanan siber republik Indonesia. Dari aspek struktur organisasi, pemerintahan Indonesia telah membentuk lembaga negara khusus yaitu BSSN. Pembentukan lembaga tersebut bisa diidentifikasi sebagai bentuk keseriusan pemerintah dalam mengamankan negara dari ancaman siber, baik dari aktor dalam maupun luar negara. Badan Siber dan Sandi Negara (BSSN) sendiri merupakan alat pemerintahan yang didirikan atas dasar tumpeng tindihnya kewenangan, tugas dan fungsi dari beberapa lembaga yang membidangi masalah siber sebelumnya seperti Kementerian Komunikasi dan Informasi (sekarang Komdigi), Badan Intelijen Negara (BIN), Kementerian Pertahanan (Kemhan), Polri dan institusi lainnya (Makbull, 2022).

Untuk proyeksi keamanan siber depannya, Markas Besar TNI sekarang masih menyusun rencana pembentukan angkatan keempat yaitu Angkatan Siber. Pembentukan angkatan keempat ini nantinya akan melengkapi tiga matra yang sudah ada di TNI. Meskipun TNI sekarang sebenarnya sudah memiliki Satuan Siber TNI (Satsiber TNI), tetapi satuan tersebut bertugas menyelenggarakan kegiatan dan operasi siber di lingkungan TNI dalam mendukung tugas pokok TNI saja (berkas.dpr.go.id). Melihat dari komposisi kabinet pemerintahan Presiden Prabowo yang banyak diisi oleh figur berlatar belakang militer, kemungkinan besar Presiden ke 8 tersebut akan sangat mempercayai dan mendukung TNI untuk membentuk angkatan siber sebagai angkatan keempat..

KESIMPULAN

Fenomena digitalisasi penyelenggaraan pemerintahan selalu diikuti oleh ancaman siber yang tidak mengenal lintas batas. Ancaman siber bagi pemerintahan sangat bersifat dinamis, sehingga tidak bisa berhenti untuk didiskusikan dan diperbarui upaya mitigasi dan penanganannya. Indonesia sebagai negara yang belum mapan dalam sektor keamanan siber diharapkan dapat lebih siap dalam menghadapi berbagai ancaman siber seperti: cyber crime, cyber terrorism, dan cyber warfare. Untuk menjamin keamanan siber, upaya memberi kepastian hukum, perubahan nomenklatur kementerian, hingga pembentukan lembaga khusus (BSSN) telah dilakukan terutama untuk menjamin keamanan dari penyelenggaraan pemerintahan.

Di era administrasi Presiden Prabowo saat ini, pelibatan militer di luar aspek pertahanan konvensional dinilai akan semakin masif. Termasuk isu tentang pembentukan angkatan siber sebagai angkatan keempat dalam matra TNI. Meskipun

BSSN sebagai lembaga yang diharapkan dapat mengatasi masalah tumpang tindih keamanan siber juga banyak diisi oleh orang berlatar belakang militer, namun administrasi Prabowo sangat meyakini bahwa untuk menjadikan Indonesia sebagai negara maju, maka membutuhkan militer yang kuat. Oleh sebab itu, aspek keamanan siber dinilai lebih terstruktur jika ada di bawah TNI.

SARAN

Besarnya jumlah pengguna internet di Indonesia yang diikuti oleh upaya digitalisasi penyelenggaraan pemerintahan telah menciptakan kebutuhan akan keamanan siber yang lebih terjamin. Secara kelembagaan dan kepastian hukum pemerintah Indonesia sangat fokus untuk menguraikan benang kusut dari dua aspek tersebut. Namun dari aspek edukasi yang bertujuan untuk memitigasi ancaman siber pemerintah kurang masif bergerak. Oleh sebab itu, pemerintah harus lebih aktif dalam mengedukasi masyarakat secara umum dan para pejabat atau pemangku kepentingan secara khusus tentang analisis ancaman siber terhadap keamanan Indonesia. Sekurang-kurangnya para pejabat yang mempunyai posisi pengambil keputusan harus memahami ancaman perang siber yang semakin kompleks di masa depan. Penyelenggaraan pemerintahan yang semakin terdigitalisasi perlu dijamin keamanannya oleh kolaborasi antara masyarakat sipil, pemerintah, dan khususnya kekuatan militer yang tangguh.

DAFTAR PUSTAKA

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. Justisia: Jurnal Ilmu Hukum, 1(1), 1-11.

Bovens, M. (2008). Public Accountability. In E. L. Edwards (Ed.), The Oxford Handbook of Public Management (pp. 182-208). Oxford University Press.

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). SAGE Publications.

Heeks, R. (2001). Building E-Government: International Practice and Theory. Routledge.

Klijn, E. H., & Koppenjan, J. F. M. (2000). Public Management and Policy Networks: Foundations of a Network Approach to Governance. Public Administration, 78(4), 657-674.

Kooiman, J. (2003). Governing as Governance. SAGE Publications.

Lansley, G. (2012). Cyber Security: The Role of the Government and the Private Sector. Palgrave Macmillan.

Listiyono, Y., Prakoso, L. Y., & Sianturi, D. (2022). Strategi Pertahanan Laut dalam Pengamanan Alur Laut Kepulauan Indonesia untuk Mewujudkan Keamanan Maritim dan Mempertahankan Kedaulatan Indonesia. Jurnal Education and Development, 10(2), 319-324.

Rizki, M. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi:-. Politeia: Jurnal Ilmu Politik, 14(1), 54-62.

Yin, R. K. (2009). Case Study Research: Design and Methods. SAGE Publications.