Journal Education and Government Wiyata ISSN 2986-5131
Volume 4 Nomor 3, Agustus 2026 (1177-1195)
https://journal.wiyatapublisher.or.id/index.php/e-gov

PENGUATAN TATA KELOLA DAN KOORDINASI KEAMANAN SIBER DALAM MENINGKATKAN KETAHANAN SIBER NASIONAL

Cori Mentari Tambunan[1]
Kementerian Koordinator Bidang Politik dan Keamanan, Jakarta, Indonesia[1]
E-mail: corimentaritambunann@gmail.com[1]

ABSTRACT

Digital transformation in Indonesia has increased the use of electronic systems in government administration, public service delivery, and various societal activities. However, this has also increased the risk of cyber threats that may disrupt the continuity of public service delivery, compromise data security, and threaten the stability of the national digital system. This study aims to analyze issues in national cybersecurity governance and formulate policy alternatives to strengthen coordination among ministries and government agencies in addressing cyber threats in Indonesia. This study employs a qualitative approach with a policy analysis design through document analysis of official government reports, policy documents, laws and regulations, and relevant scientific publications. The analysis was conducted by prioritizing problems using the Urgency, Seriousness, and Growth (USG) method, identifying root causes through the Fishbone Diagram, and evaluating policy alternatives using McNamara Screening Analysis. The findings show that limited human resource capacity, weak coordination among ministries and government agencies, and suboptimal information-sharing mechanisms are the main factors hindering the effectiveness of national cybersecurity governance. The highest-priority policy alternative is the formulation of a national cybersecurity coordination policy by the Coordinating Ministry for Political and Security Affairs as a foundation for strengthening governance. This study recommends the development of an integrated policy that clarifies the division of authority, strengthens coordination mechanisms, enhances human resource capacity, and develops a cyber threat information-sharing system to support national cyber resilience and sustainable digital transformation in Indonesia.

Keywords: *Cybersecurity Governance; Collaborative Governance; Policy Analysis; Cyber Resilience; Whole-Of-Government*

ABSTRAK

Perkembangan transformasi digital di Indonesia telah meningkatkan pemanfaatan sistem elektronik dalam penyelenggaraan pemerintahan, pelayanan publik, serta berbagai aktivitas masyarakat. Di sisi lain, kondisi tersebut turut meningkatkan risiko ancaman siber yang berpotensi mengganggu keberlangsungan layanan publik, keamanan data, dan stabilitas sistem digital nasional. Penelitian ini bertujuan menganalisis permasalahan tata kelola keamanan siber nasional serta merumuskan alternatif kebijakan untuk memperkuat koordinasi antarkementerian

dan lembaga dalam menghadapi ancaman siber di Indonesia. Penelitian ini menggunakan pendekatan kualitatif dengan desain analisis kebijakan melalui studi dokumentasi terhadap laporan resmi pemerintah, dokumen kebijakan, peraturan perundang-undangan, serta publikasi ilmiah yang relevan. Analisis dilakukan melalui penentuan prioritas permasalahan dengan metode Urgency, Seriousness, dan *Growth* (USG)*, identifikasi akar penyebab dengan Fishbone Diagram, serta evaluasi alternatif kebijakan menggunakan Tapisan McNamara. Hasil penelitian menunjukkan bahwa keterbatasan kapasitas sumber daya manusia, lemahnya koordinasi antarkementerian dan lembaga, serta belum optimalnya mekanisme pertukaran informasi merupakan faktor utama yang menghambat efektivitas tata kelola keamanan siber nasional. Alternatif kebijakan yang memperoleh prioritas tertinggi adalah penyusunan kebijakan koordinasi keamanan siber nasional oleh Kementerian Koordinator Bidang Politik dan Keamanan sebagai dasar penguatan tata kelola. Penelitian ini merekomendasikan penyusunan kebijakan terpadu yang memperjelas pembagian kewenangan, memperkuat mekanisme koordinasi, meningkatkan kapasitas sumber daya manusia, serta mengembangkan sistem pertukaran informasi ancaman siber untuk mendukung ketahanan siber nasional dan keberlanjutan transformasi digital di Indonesia.*

Kata Kunci: *Tata Kelola Keamanan Siber; Collaborative Governance; Analisis Kebijakan; Ketahanan Siber; Whole-Of-Government*

PENDAHULUAN

Indonesia merupakan salah satu negara dengan populasi digital terbesar di dunia. Survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2026 mencatat 235,26 juta pengguna internet atau 81,72% dari total populasi nasional (APJII, 2026). Perkembangan tersebut mendorong transformasi digital pada pemerintahan, ekonomi, pendidikan, dan layanan publik (Athaillah et al., 2026; Alfi et al., 2023), tetapi sekaligus meningkatkan risiko *ransomware, phishing*, pencurian data, dan serangan terhadap infrastruktur kritis (Craigen et al., 2014; Herrera & Sebyar, 2023; Stallings, 2018). Dengan demikian, keamanan siber menjadi bagian penting dari ketahanan nasional dan keberlanjutan transformasi digital (Layode et al., 2024; Racionero-Garcia & Shaikh, 2024).

Urgensi tersebut terlihat dari meningkatnya ancaman terhadap sistem elektronik nasional. BSSN mencatat sekitar 5,5 miliar trafik anomali siber sepanjang 2025, meningkat 714% dibandingkan rata-rata periode 2020–2024, serta menemukan 44,7 juta kredensial pengguna Indonesia yang beredar di *darknet*. Hingga Triwulan I 2026, masih terdeteksi sekitar 604 juta trafik anomali siber (Syawaluddin et al., 2025). Serangan *ransomware* terhadap Pusat Data Nasional Sementara (PDNS) 2 pada 2024 yang berdampak pada 239 dari 282 instansi pengguna layanan pemerintah menunjukkan masih perlunya penguatan manajemen risiko, deteksi, respons, dan pemulihan insiden

siber (Kalderemidis et al., 2022; Kementerian Komunikasi dan Digital, *2024).* Kondisi tersebut menegaskan bahwa keamanan siber tidak hanya berkaitan dengan perlindungan teknologi informasi, tetapi juga dengan perlindungan data, keberlangsungan layanan publik, stabilitas ekonomi digital, dan kepercayaan masyarakat (Herera & Sebyar, 2023).

Namun, tantangan keamanan siber nasional tidak hanya bersifat teknis, tetapi juga merupakan persoalan administrasi publik yang berkaitan dengan tata kelola, kelembagaan, koordinasi lintas sektor, dan kebijakan publik. Penelitian terdahulu menunjukkan keterbatasan *digital talent*, infrastruktur TIK, pendanaan, dan kapasitas kelembagaan (Adma et al., 2023; Aji, 2022; Anwar et al., 2025; Anwary, 2022), kesenjangan regulasi dan implementasi (Alfath & Cahya, 2024; Maharani & Atman, 2025), serta lemahnya koordinasi, pertukaran informasi, monitoring, dan deteksi dini (Kalderemidis et al., 2022; Taufik et al., 2025).

Padahal, pengelolaan keamanan siber melibatkan kementerian/lembaga, pemerintah daerah, sektor swasta, perguruan tinggi, dan masyarakat sehingga membutuhkan kolaborasi dan pembagian peran yang jelas untuk memperkuat *cyber resilience* (Ikhssani et al., 2024; Intan & Intan, 2023; Ramli et al., 2026). Pemerintah telah menerbitkan berbagai regulasi dan membentuk Badan Siber dan Sandi Negara (BSSN), tetapi keberadaan regulasi dan kelembagaan belum sepenuhnya menjamin efektivitas implementasi tanpa dukungan kapasitas, koordinasi, dan mekanisme pertukaran informasi yang terintegrasi (Rusydi, 2025).

Penelitian sebelumnya telah membahas kapasitas sumber daya, regulasi, kelembagaan, koordinasi, dan *cyber resilience*, tetapi aspek-aspek tersebut masih banyak dikaji secara terpisah. Keterbatasan penelitian terdahulu terletak pada belum terintegrasinya identifikasi masalah, analisis akar penyebab, dan pemilihan alternatif kebijakan dalam satu kerangka analisis untuk memperkuat koordinasi keamanan siber nasional. Penelitian ini menawarkan kebaruan melalui integrasi perspektif *Cybersecurity Governance, Collaborative Governance,* dan *Whole-of-Government* dengan metode *Urgency, Seriousness, and Growth* (USG), *Fishbone Diagram*, dan Tapisan McNamara untuk menghasilkan prioritas masalah, akar penyebab, serta alternatif kebijakan secara sistematis.

Berdasarkan kesenjangan tersebut, penelitian ini menggunakan USG untuk menentukan prioritas masalah, *Fishbone Diagram* untuk mengidentifikasi akar penyebab, dan Tapisan McNamara untuk memilih alternatif kebijakan prioritas. Penelitian ini bertujuan menganalisis permasalahan tata kelola keamanan siber nasional, menentukan prioritas masalah, mengidentifikasi akar

penyebab, serta merumuskan alternatif kebijakan untuk memperkuat koordinasi keamanan siber nasional.

KAJIAN PUSTAKA

Keamanan Siber (*Cybersecurity*)

Keamanan siber (*cybersecurity*) merupakan upaya melindungi sistem informasi, jaringan, perangkat digital, dan data dari berbagai ancaman siber melalui penerapan proses, teknologi, dan praktik untuk menjaga integritas (*integrity*), ketersediaan (*availability*), dan kerahasiaan (*confidentiality*) informasi (Craigen et al., 2014; Stallings, 2018). Seiring meningkatnya transformasi digital, keamanan siber menjadi isu strategis tidak lagi bersifat teknis, yang berhubungan dengan perlindungan data, ketahanan nasional, dan keberlanjutan layanan publik. Oleh karena itu, pengelolaannya memerlukan integrasi teknologi, kebijakan, sumber daya manusia, dan manajemen risiko.

Tata Kelola Keamanan Siber (*Cybersecurity governance*)

Cybersecurity governance atau tata kelola keamanan siber merupakan bagian dari *enterprise governance* yang memastikan pengelolaan risiko keamanan siber selaras dengan tujuan organisasi melalui mekanisme evaluasi, pengarahan, dan pemantauan (ISACA, 2020). Dengan demikian, tata kelola keamanan siber mencakup kebijakan, struktur kelembagaan, akuntabilitas, proses pengambilan keputusan, dan koordinasi antarpemangku kepentingan. Menurut Von Solms dan Van Niekerk (2013), keamanan siber telah berkembang dari persoalan teknis menjadi isu tata kelola yang mencakup aspek kebijakan, SDM, koordinasi, dan proses organisasi. Sejalan dengan itu, OECD (2022) menekankan pentingnya penguatan tata kelola melalui koordinasi kelembagaan, pengelolaan risiko, dan pendekatan *whole-of-government* dalam menghadapi ancaman siber. Pendekatan tersebut juga didukung oleh Abrahams et al., (2024), Adma et al., 2023 dan Yamada (2024), yang menegaskan bahwa keamanan siber memerlukan kolaborasi lintas pemangku kepentingan dengan memanfaatkan pendekatan *whole-of-government* dan *whole-of-society*.

Dalam mendukung implementasi tata kelola keamanan siber, National Institute of Standards and Technology (NIST, 2018) Cybersecurity Framework mengidentifikasi lima fungsi utama, yaitu *Identify, Protect, Detect, Respond,* dan *Recover*, sebagai dasar pengelolaan risiko keamanan siber. Kerangka tersebut menunjukkan bahwa keamanan siber tidak hanya berfokus pada pencegahan serangan, tetapi juga pada kemampuan untuk mengidentifikasi risiko, melindungi sistem, mendeteksi ancaman, merespons insiden, dan memulihkan sistem secara berkelanjutan. Dalam konteks Indonesia, penguatan tata kelola keamanan siber masih menghadapi tantangan berupa fragmentasi kewenangan, lemahnya koordinasi antarkementerian dan lembaga,

keterbatasan kapasitas sumber daya manusia, serta belum optimalnya mekanisme pertukaran informasi ancaman siber (Adma et al., 2023; Alfath & Cahya, 2024; Maharani & Atman, 2025). Oleh karena itu, penelitian ini mengintegrasikan perspektif *Cybersecurity Governance, Collaborative Governance*, dan *Whole-of-Government* sebagai landasan konseptual untuk menganalisis penguatan koordinasi dalam tata kelola keamanan siber nasional.

Collaborative Governance

Collaborative Governance merupakan pendekatan tata kelola yang berkembang untuk menangani permasalahan publik kompleks melalui kolaborasi lintas organisasi dan sektor (Emerson & Nabatchi, 2015). Pendekatan ini relevan dalam keamanan siber karena ancaman siber bersifat dinamis, lintas sektor, dan tidak dapat ditangani satu institusi saja (Abrahams et al., 2024; Shah et al., 2023). Ansell dan Gash (2008) menyatakan bahwa *Collaborative Governance* merupakan proses formal, kolektif, dan berorientasi pada konsensus yang melibatkan aktor publik maupun nonpublik dalam pengambilan keputusan. Selanjutnya, Emerson dan Nabatchi (2015) menjelaskan bahwa keberhasilan kolaborasi dipengaruhi keterlibatan berlandaskan prinsip, motivasi bersama, dan kapasitas bertindak secara kolektif. Ketiga unsur tersebut dapat membangun kepercayaan, komitmen, dan kapasitas bersama antarpemangku kepentingan.

Dalam konteks keamanan siber nasional, kolaborasi tersebut melibatkan BSSN, Kementerian Komunikasi dan Digital, kementerian/lembaga, aparat penegak hukum, penyelenggara sistem elektronik, sektor swasta, perguruan tinggi, komunitas keamanan siber, dan masyarakat. Kompleksitas aktor tersebut menuntut mekanisme kolaborasi yang mampu mendukung koordinasi, pertukaran informasi, pengembangan kapasitas, serta penanganan insiden secara terpadu. Oleh karena itu, lensa analitis yang digunakan dalam penelitian ini adalah *Collaborative Governance* untuk mengkaji kolaborasi antarpemangku kepentingan dalam penguatan tata kelola keamanan siber nasional dan melengkapinya dengan pendekatan *Whole-of-Government* guna menjelaskan koordinasi serta integrasi antarkementerian dan lembaga pemerintah.

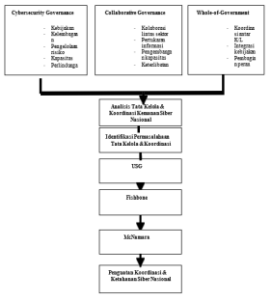
Sintesis Kajian Pustaka

Sejumlah penelitian sebelumnya cenderung membahas tata kelola keamanan siber dari perspektif regulasi, kelembagaan, atau aspek teknis secara terpisah sehingga belum memberikan pemahaman yang komprehensif mengenai pentingnya koordinasi lintas sektor dan integrasi antarlembaga dalam memperkuat tata kelola keamanan siber nasional (Adma et al., 2023; Alfath & Cahya, 2024; Maharani & Atman, 2025). Oleh karena itu, penelitian ini mengintegrasikan tiga perspektif teoritis, yaitu *Cybersecurity Governance, Collaborative Governance,* dan *Whole-of-*

Government, dalam mendapatkan pemahaman terkait dengan koordinasi dan tata kelola keamanan siber nasional yang lebih komprehensif.

Dalam kerangka analisis penelitian ini, *Cybersecurity Governance* diposisikan sebagai kerangka utama untuk mengidentifikasi dan menganalisis aspek tata kelola keamanan siber, meliputi kebijakan, kelembagaan, pengelolaan risiko, kapasitas, serta mekanisme perlindungan dan respons terhadap ancaman siber. *Collaborative Governance* digunakan untuk menganalisis kolaborasi antara pemerintah dan aktor nonpemerintah dalam mendukung koordinasi, pertukaran informasi, dan pengembangan kapasitas. Sementara itu, *Whole-of-Government* digunakan untuk menganalisis koordinasi dan integrasi antarkementerian/lembaga pemerintah, termasuk pembagian peran dan penyelarasan kebijakan (Abrahams et al., 2024; Adma et al., 2023; Yamada, 2024). Dengan demikian, *Cybersecurity Governance* menjelaskan aspek tata kelola yang dianalisis, *Collaborative Governance* menjelaskan dimensi kolaborasi lintas sektor, sedangkan *Whole-of-Government* menjelaskan dimensi koordinasi dan integrasi pemerintahan.

Berdasarkan hubungan tersebut, ketiga perspektif digunakan secara saling melengkapi sebagai lensa analitis penelitian. Aspek tata kelola keamanan siber diidentifikasi melalui perspektif *Cybersecurity Governance*, kemudian permasalahan yang berkaitan dengan keterlibatan dan kolaborasi lintas sektor dianalisis melalui *Collaborative Governance*, sedangkan permasalahan koordinasi dan integrasi antarkementerian/lembaga dianalisis melalui *Whole-of-Government*. Hasil analisis tersebut menjadi dasar dalam mengidentifikasi permasalahan prioritas, akar penyebab, dan alternatif kebijakan untuk memperkuat koordinasi serta ketahanan siber nasional.



Gambar 1. Kerangka Analisis Penelitian

METODE

Penelitian kualitatif dengan desain analisis kebijakan (*policy analysis)* ini bertujuan mengevaluasi tata kelola keamanan siber nasional, mengidentifikasi tantangan koordinasi antarkementerian dan lembaga, dan memberikan rumusan kebijakan alternatif yang memperkuat ketahanan siber nasional. Analisis kebijakan merupakan pendekatan sistematis dalam mengidentifikasi masalah publik, mengevaluasi alternatif kebijakan, serta merumuskan rekomendasi yang menjadi dasar dalam pengambilan keputusan (Dunn, 2018). Dalam

penelitian ini, analisis dilakukan dengan menggunakan perspektif *Collaborative Governance* dan *Whole-of-Government* sebagai lensa analitis untuk mengkaji mekanisme kolaborasi lintas pemangku kepentingan dan koordinasi kelembagaan dalam tata kelola keamanan siber nasional.

Data sekunder yang berupa dokumen kebijakan dan dokumen resmi terkait tata kelola keamanan siber nasional, meliputi peraturan perundang-undangan, dokumen kebijakan pemerintah, laporan Badan Siber dan Sandi Negara (BSSN), serta laporan Kementerian Komunikasi dan Digital digunakan dalam penelitian ini. Analisis dokumen dilakukan secara purposive berdasarkan relevansi dengan fokus penelitian, kemudian diklasifikasikan ke dalam tema ancaman keamanan siber, koordinasi antarlembaga, tata kelola keamanan siber, kapasitas sumber daya manusia, serta implementasi kebijakan keamanan siber nasional (Bowen, 2009). Selanjutnya, analisis kebijakan dilakukan melalui tiga tahapan, yaitu *Urgency, Seriousness, dan Growth* (USG) dalam menentukan prioritas permasalahan, kemudian digunakan Fishbone Diagram dalam mengidentifikasi akar penyebab permasalahan (Ishikawa, 1986) dan Tapisan McNamara untuk mengevaluasi serta menentukan alternatif kebijakan yang paling prioritas. Penilaian alternatif kebijakan dalam Tapisan McNamara dilakukan oleh peneliti berdasarkan hasil analisis dokumen dan temuan penelitian. Prosedur penilaian dilakukan dengan memberikan skor 1–5 pada setiap alternatif berdasarkan lima kriteria, yaitu efektivitas (K1), efisiensi (K2), kemudahan implementasi (K3), manfaat (K4), dan kesesuaian dengan tujuan kebijakan (K5). Dasar pemberian skor didasarkan pada tingkat kontribusi, relevansi, dan kesesuaian masing-masing alternatif terhadap permasalahan prioritas serta tujuan penguatan tata kelola dan koordinasi keamanan siber nasional. Skor 5 menunjukkan tingkat kontribusi dan kesesuaian yang sangat tinggi, sedangkan skor 1 menunjukkan tingkat yang sangat rendah. Nilai total setiap alternatif diperoleh dengan menjumlahkan skor kelima kriteria, kemudian alternatif dengan nilai total tertinggi ditetapkan sebagai alternatif kebijakan prioritas.

Tabel 1. Kriteria Penilaian Alternatif Kebijakan Menggunakan Tapisan McNamara

Kode	Kriteria	Indikator Penilaian
K1	Efektivitas	Kemampuan alternatif kebijakan dalam menyelesaikan permasalahan prioritas dan mencapai tujuan penguatan tata kelola keamanan siber.
K2	Efisiensi	Perbandingan antara sumber daya yang diperlukan dengan hasil atau dampak yang diharapkan dari implementasi kebijakan.
K3	Kemudahan Implementasi	Tingkat kemudahan penerapan kebijakan berdasarkan kesiapan kelembagaan, kewenangan, sumber daya, dan mekanisme pelaksanaan.
K4	Manfaat	Besarnya manfaat yang dapat diberikan kebijakan terhadap pemerintah, penyelenggara sistem elektronik, masyarakat, dan ketahanan siber nasional.
K5	Kesesuaian dengan tujuan kebijakan	Tingkat kesesuaian alternatif dengan tujuan penguatan tata kelola, koordinasi, dan ketahanan siber nasional.

Sumber: Diolah Penulis (2026)

Penilaian setiap kriteria menggunakan skala 1–5. Skor 5 menunjukkan tingkat kesesuaian atau kontribusi yang sangat tinggi terhadap kriteria yang dinilai, skor 4 menunjukkan tingkat tinggi, skor 3

menunjukkan tingkat sedang, skor 2 menunjukkan tingkat rendah, dan skor 1 merupakan skor terendah. Dengan demikian, semakin tinggi skor yang diperoleh, semakin besar tingkat kelayakan alternatif kebijakan berdasarkan kriteria yang digunakan.

Tabel 2 Skala Penilaian Tapisan McNamara

Skor	Interpretasi	Keterangan
5	Sangat Tinggi	Alternatif memiliki kontribusi dan kesesuaian yang sangat kuat terhadap kriteria serta sangat mendukung pencapaian tujuan kebijakan.
4	Tinggi	Alternatif memiliki kontribusi dan kesesuaian yang kuat terhadap kriteria serta mendukung pencapaian tujuan kebijakan.
3	Sedang	Alternatif memiliki kontribusi dan kesesuaian yang cukup terhadap kriteria, tetapi masih memerlukan penguatan atau penyesuaian dalam implementasinya.
2	Rendah	Alternatif memiliki kontribusi dan kesesuaian yang terbatas terhadap kriteria serta memerlukan penyesuaian yang cukup besar.
1	Sangat Rendah	Alternatif memiliki kontribusi dan kesesuaian yang sangat terbatas terhadap kriteria serta kurang mendukung pencapaian tujuan kebijakan.

Sumber: Diolah Penulis (2026)

HASIL DAN PEMBAHASAN

Identifikasi Permasalahan Prioritas dalam Tata Kelola Keamanan Siber Nasional

Identifikasi permasalahan prioritas dalam tata kelola keamanan siber nasional menggunakan metode USG (*Urgency, Seriousness, and Growth*) sebagai metode untuk menentukan masalah yang paling mendesak, memiliki dampak paling besar, serta memiliki potensi untuk berkembang jika tidak ditangani dengan segera melalui kebijakan publik (Dunn, 2018). Penilaian menggunakan skala 1–5 berdasarkan tingkat urgensi, potensi, serta dampak dari berkembangnya masalah. Hasil penilaian USG terhadap beberapa isu strategis keamanan siber nasional disajikan pada tabel berikut.

Tabel 3 Skor USG

Skor	Urgency	Seriousness	Growth
5	Sangat Mendesak	Sangat Serius	Sangat Berkembang
4	Mendesak	Serius	Berkembang
3	Cukup Mendesak	Cukup Serius	Cukup Berkembang
2	Kurang Mendesak	Kurang Serius	Kurang Berkembang
1	Tidak Mendesak	Tidak Serius	Tidak Berkembang

Tabel 4 Hasil Identifikasi Permasalahan Prioritas Menggunakan Metode USG

No	Isu Strategis	U	S	G	Total	Prioritas
1.	Rendahnya kesadaran keamanan siber pada organisasi	5	3	5	13	3
2.	Kurangnya integrasi dan berbagi informasi ancaman	5	5	4	14	2
3.	Ketergantungan pada teknologi dan produk pihak ketiga	4	4	4	12	4
4.	Keterbatasan Kapasitas SDM dan Koordinasi Antarinstansi	5	5	5	15	1
5.	Keterbatasan Monitoring dan Deteksi Dini Anomali	3	3	4	10	5

Sumber: Diolah Penulis (2026)

Berdasarkan hasil analisis USG pada Tabel 4, keterbatasan kapasitas sumber daya manusia dan koordinasi antarinstansi memperoleh skor tertinggi, yaitu 15, sehingga ditetapkan sebagai isu prioritas dalam penguatan tata kelola keamanan siber nasional. Temuan ini menunjukkan bahwa efektivitas penyelenggaraan keamanan siber nasional tidak hanya dipengaruhi oleh kesiapan teknologi, tetapi juga oleh kapasitas kelembagaan dan mekanisme koordinasi antar pemangku kepentingan (Alfath & Cahya, 2024; Qudus, 2025; Rusydi, 2025).

Hasil tersebut mengindikasikan bahwa tantangan keamanan siber di Indonesia memiliki karakter yang lebih luas daripada persoalan teknis dan teknologi. Keterbatasan kapasitas

sumber daya manusia dapat memengaruhi kemampuan organisasi dalam mengidentifikasi, mencegah, merespons, dan memulihkan diri dari insiden siber. Pada saat yang sama, lemahnya koordinasi antarkementerian dan lembaga dapat menghambat pertukaran informasi, pengambilan keputusan, serta respons terhadap ancaman yang bersifat lintas sektor. Oleh karena itu, penguatan tata kelola keamanan siber membutuhkan perhatian terhadap aspek kelembagaan serta koordinasi selain peningkatan infrastruktur teknologi.

Temuan tersebut sejalan dengan konsep *Cybersecurity Governance* yang menempatkan keamanan siber dalam bagian dari tata kelola organisasi yang mencakup kebijakan, kelembagaan, koordinasi, pengelolaan risiko, dan akuntabilitas (NIST, 2018). Dalam perspektif tersebut, efektivitas keamanan siber tidak ditentukan oleh kecanggihan teknologi saja, namun oleh kemampuan institusi dalam mengoordinasikan sumber daya, menetapkan mekanisme kerja yang jelas, dan membangun sistem respons terhadap insiden secara terintegrasi.

Temuan penelitian juga konsisten dengan penelitian Adma et al. (2023) dan Alfath dan Cahya (2024) yang mengidentifikasi lemahnya koordinasi dan fragmentasi tata kelola sebagai tantangan dalam penyelenggaraan keamanan siber di Indonesia. Oleh karena itu, hasil penetapan isu prioritas menjadi dasar untuk mengidentifikasi akar penyebab permasalahan agar alternatif kebijakan yang dirumuskan dapat menjawab faktor-faktor yang memengaruhi efektivitas koordinasi, kapasitas kelembagaan, dan penyelenggaraan keamanan siber secara nasional.

Analisis Akar Penyebab Permasalahan Tata Kelola Keamanan Siber

Berdasarkan hasil identifikasi permasalahan prioritas, analisis lebih lanjut dilakukan menggunakan *Fishbone Diagram* untuk mengidentifikasi faktor-faktor yang memengaruhi efektivitas tata kelola keamanan siber nasional. Analisis dilakukan berdasarkan enam dimensi, yaitu *man* (sumber daya manusia), *material* (dukungan kerja sama dan pertukaran informasi), *methods* (mekanisme koordinasi dan prosedur penanganan insiden), *measurement* (pengukuran dan evaluasi kinerja), *environment* (lingkungan organisasi dan budaya keamanan siber), serta *machine* (infrastruktur dan teknologi pendukung). Hasil identifikasi faktor-faktor penyebab disajikan pada Tabel 5.

Tabel 5. Hasil Analisis Penyebab Permasalahan Menggunakan Fishbone Diagram

No	Dimensi	Masalah Dimensi	Permasalahan
1.	*Man*	Keterbatasan kapasitas SDM keamanan siber	
2.	*Material*	Belum optimalnya Pertukaran informasi dan kerja sama keamanan siber antarnegara ataupun antarinstansi	Keterbatasan kapasitas SDM dan koordinasi antarinstansi
3.	*Methods*	Belum adanya mekanisme koordinasi dan respons insiden siber yang terintegrasi antarinstansi	
4.	*Measurement*	Belum tersedianya Indikator keberhasilan dan standar evaluasi penanganan insiden siber	
5.	*Environment*	Keterbatasan tenaga ahli keamanan siber dalam keamanan	
6.	*Machine*	Jaringannya terhadap teknologi dan sistem digital pihak ketiga	

Sumber: Diolah Penulis (2026)

Berdasarkan hasil analisis Fishbone Diagram, permasalahan tata kelola keamanan siber nasional dipengaruhi oleh enam kelompok faktor yang saling berkaitan. Faktor tersebut meliputi keterbatasan kapasitas sumber daya manusia keamanan siber, belum optimalnya mekanisme pertukaran informasi dan kerja sama antarinstansi, belum terintegrasinya mekanisme koordinasi serta penanganan insiden siber, belum tersedianya indikator evaluasi kinerja yang terstandarisasi, keterbatasan kapasitas organisasi dalam mendukung keamanan siber, serta ketergantungan terhadap teknologi dan sistem digital pihak ketiga.

Hasil menunjukkan akar permasalahan tidak berasal dari aspek teknologi saja, tetapi oleh faktor kelembagaan, sumber daya manusia, serta mekanisme tata kelola yang belum berjalan secara terpadu. Dengan demikian, tantangan utama keamanan siber nasional dapat dipahami sebagai persoalan *governance issue*, yaitu persoalan yang berkaitan dengan bagaimana berbagai institusi mengelola kewenangan, sumber daya, informasi, risiko, dan tanggung jawab secara bersama-sama. Hal tersebut menunjukkan bahwa penguatan koordinasi antarinstansi, peningkatan SDM, serta pengembangan mekanisme yang terintegrasi untuk tata kelola merupakan aspek yang esensial dan perlu dipertimbangkan dalam penyusunan alternatif kebijakan penguatan keamanan siber nasional (Alfath & Cahya, 2024; Khaw et al., 2024).

Temuan tersebut memperkuat hasil analisis USG bahwa kapasitas sumber daya manusia dan koordinasi antarinstansi merupakan persoalan yang perlu memperoleh perhatian utama. Keterbatasan kapasitas SDM dapat mengurangi kemampuan organisasi dalam menjalankan fungsi keamanan siber, sedangkan belum optimalnya pertukaran informasi dan mekanisme koordinasi dapat menghambat respons terhadap ancaman yang membutuhkan tindakan lintas lembaga. Kondisi ini menunjukkan bahwa peningkatan kapasitas individual tanpa diikuti dengan penguatan mekanisme kelembagaan dan koordinasi belum cukup untuk membangun tata kelola keamanan siber yang efektif.

Temuan relevan dengan Ansell dan Gash (2008), yang menyatakan penyelesaian permasalahan publik yang kompleks memerlukan keterlibatan berbagai aktor melalui proses kolaborasi yang formal, deliberatif, dan berorientasi pada konsensus yang semua tertuang dalam konsep *Collaborative Governance*. Dalam konteks keamanan siber nasional, kolaborasi tidak hanya melibatkan kementerian dan lembaga pemerintah, tetapi penyelenggara sistem elektronik, sektor swasta, perguruan tinggi, masyarakat yang merupakan pengguna layanan digital, serta komunitas keamanan siber.

Selanjutnya, Emerson dan Nabatchi (2015) menyatakan keberhasilan *Collaborative Governance*

Regime dipengaruhi oleh tiga komponen utama, yaitu keterlibatan yang berlandaskan prinsip, kapasitas untuk melakukan tindakan dan motivasi bersama. Hasil *Fishbone Diagram* menunjukkan bahwa ketiga aspek tersebut masih menghadapi tantangan dalam konteks tata kelola keamanan siber Indonesia. Belum optimalnya mekanisme pertukaran informasi, keterbatasan kapasitas sumber daya manusia, dan belum terbangunnya koordinasi lintas sektor secara sistematis menunjukkan bahwa kapasitas kolaboratif antarpemangku kepentingan masih perlu diperkuat.

Temuan penelitian ini juga konsisten dengan penelitian Shah et al. (2023) yang menegaskan pentingnya faktor manusia,
tata kelola organisasi, dan mekanisme koordinasi untuk meningkatkan ketahanan siber secara berkelanjutan. Dengan begitu, peningkatan sumber daya manusia, penguatan koordinasi antarinstansi, dan pengembangan mekanisme tata kelola yang terintegrasi menjadi aspek penting dalam penyusunan alternatif kebijakan penguatan keamanan siber nasional.

Penentuan Alternatif Kebijakan Prioritas dan Penguatan Koordinasi melalui Pendekatan *Whole-of-Government*

Berdasarkan hasil identifikasi akar permasalahan, dirumuskan enam alternatif kebijakan untuk memperkuat tata kelola keamanan siber nasional. Alternatif tersebut mencakup penyusunan kebijakan koordinasi keamanan siber nasional, penguatan mekanisme koordinasi dan pertukaran informasi ancaman siber antarinstansi, penguatan integrasi respons insiden siber nasional, penyusunan indikator evaluasi dan standar penanganan insiden siber, pengembangan kapasitas sumber daya manusia keamanan siber, serta modernisasi infrastruktur digital nasional. Keenam alternatif tersebut selanjutnya dievaluasi menggunakan Tapisan McNamara berdasarkan kriteria efektivitas, efisiensi, kemudahan implementasi, manfaat, dan dukungan terhadap pencapaian tujuan kebijakan. Hasil penilaian disajikan pada Tabel 6.

Tabel 6 Hasil Penilaian Alternatif Kebijakan Menggunakan Tapisan McNamara

No	Alternatif Solusi/Gagasan	Skor					Total Skor	Prioritas Gagasan
		K 1	K 2	K 3	K 4	K 5		
1	Penyusunan kebijakan koordinasi keamanan siber nasional oleh Kemenko Polkam	5	5	5	5	5	25	1
2	Penyusunan kerangka koordinasi dan pertukaran informasi ancaman siber antarinstansi i	5	4	4	3	4	20	2
3	Penguatan integrasi respons insiden siber antarlembag a nasional	3	3	3	4	3	16	3
4	Penyusunan indikator evaluasi dan standar nasional penanganan insiden siber	2	3	2	3	2	12	4
5.	Pengutatan kerja sama dan pengembaa gan kapasitas SDM keamanan siber nasional	2	2	3	2	2	11	5
6.	Modernisasi dan penguatan ketnandirian infrastruktur digital nasional	2	2	2	2	1	9	6

Sumber: Diolah Penulis (2026)

Prioritas tersebut menunjukkan bahwa persoalan koordinasi merupakan titik intervensi strategis dalam penguatan tata kelola keamanan siber nasional. Sebagai kementerian koordinator, Kemenko Polkam memiliki posisi strategis untuk menyelaraskan kebijakan, memperjelas pembagian kewenangan, dan memperkuat koordinasi antarkementerian dan lembaga dalam penyelenggaraan keamanan siber nasional. Kebijakan koordinasi juga

dapat menjadi landasan bagi pengembangan mekanisme integrasi respons insiden, peningkatan sumber daya manusia, pertukaran informasi ancaman siber dan penyusunan standar evaluasi dalam keamanan siber.

Temuan tersebut sejalan dengan penelitian Adma et al. (2023) dan Alfath dan Cahya (2024) yang menunjukkan bahwa lemahnya koordinasi dan fragmentasi tata kelola merupakan tantangan utama keamanan siber di Indonesia. Hasil ini

mendukung studi dari Abrahams et al., (2024) mengenai pentingnya kolaborasi dan pembagian peran yang jelas dalam meningkatkan efektivitas tata kelola keamanan siber. Abrahams et al., (2024) juga menunjukkan bahwa kepatuhan terhadap regulasi keamanan siber belum cukup untuk meningkatkan ketahanan siber apabila tidak didukung oleh koordinasi kelembagaan yang efektif.

Dalam konteks tersebut, pendekatan *Whole-of-Government* menjadi relevan untuk menjelaskan kebutuhan integrasi antarkementerian dan lembaga. Christensen dan Lægreid (2007) menekankan pentingnya koordinasi horizontal maupun vertikal antarlembaga pemerintah dalam menangani permasalahan publik yang kompleks. Pendekatan ini memandang bahwa efektivitas kebijakan tidak hanya ditentukan oleh kinerja masing-masing institusi, tetapi juga oleh kemampuan pemerintah membangun sinergi melalui penyelarasan kebijakan, pembagian kewenangan yang jelas, serta mekanisme koordinasi yang terintegrasi.

Dalam konteks keamanan siber nasional, pendekatan *Whole-of-Government* memungkinkan kementerian dan lembaga menjalankan fungsi dan kewenangannya dalam kerangka koordinasi nasional yang terpadu. Hal ini penting karena keamanan siber mencakup pencegahan dan identifikasi ancaman, deteksi, respons insiden, hingga pemulihan sistem. Integrasi antarlembaga dapat mempercepat pertukaran informasi, memperjelas pengambilan keputusan, dan meningkatkan efektivitas respons terhadap insiden lintas sektor.

Temuan tersebut juga memperkuat perspektif *Cybersecurity Governance* sebagaimana dijelaskan dalam *NIST Cybersecurity Framework* (2018), yang menempatkan fungsi *Identify, Protect, Detect, Respond,* dan *Recover* dalam suatu kerangka pengelolaan risiko yang didukung oleh tata kelola, kebijakan, pembagian tanggung jawab, dan mekanisme pengawasan. Dengan demikian, penguatan koordinasi bukan hanya berkaitan dengan hubungan administratif antarlembaga, tetapi merupakan bagian integral dari kemampuan nasional dalam mengelola risiko keamanan siber.

Secara keseluruhan, hasil USG, *Fishbone Diagram*, dan Tapisan McNamara menunjukkan pola yang konsisten. USG mengidentifikasi keterbatasan kapasitas SDM dan koordinasi antarinstansi sebagai

permasalahan prioritas; *Fishbone Diagram* menunjukkan bahwa permasalahan tersebut berakar pada faktor SDM, mekanisme koordinasi, pertukaran informasi, evaluasi, lingkungan organisasi, serta teknologi; sedangkan Tapisan McNamara menempatkan penyusunan kebijakan koordinasi keamanan siber nasional sebagai alternatif dengan prioritas tertinggi. Konsistensi ketiga hasil analisis tersebut memperkuat argumentasi bahwa intervensi kebijakan perlu diarahkan pada penguatan tata kelola dan koordinasi lintas institusi.

Implikasi dan Rekomendasi Kebijakan Penguatan Tata Kelola Keamanan Siber Nasional

Hasil analisis USG, *Fishbone Diagram*, dan Tapisan McNamara menunjukkan bahwa penguatan koordinasi antarkementerian dan lembaga merupakan prioritas kebijakan dalam memperkuat tata kelola keamanan siber nasional. Tantangan keamanan siber tidak hanya berkaitan dengan teknologi, tetapi juga koordinasi kelembagaan, kapasitas sumber daya manusia, dan pertukaran informasi antarinstansi. Oleh karena itu, diperlukan tata kelola yang mengintegrasikan kementerian dan lembaga, menyelaraskan kewenangan, serta memperkuat kolaborasi dan pengelolaan risiko secara terpadu untuk mendukung keberlanjutan transformasi digital nasional.

Berdasarkan temuan tersebut, penelitian ini merekomendasikan penyusunan Peraturan Menteri Koordinator Bidang Politik dan Keamanan tentang Pedoman Koordinasi serta Penguatan Keamanan Siber Nasional sebagai instrumen kebijakan untuk memperkuat tata kelola keamanan siber nasional. Regulasi tersebut perlu mengatur pembagian tugas dan kewenangan antarkementerian dan lembaga, mekanisme koordinasi dan respons insiden siber, pertukaran *cyber threat intelligence*, serta tata kelola keamanan SPBE berbasis manajemen risiko. Regulasi juga perlu mencakup audit keamanan informasi berkala, pengembangan *Security Operations Center* (SOC), mekanisme *backup* dan *disaster recovery*, serta monitoring dan evaluasi melalui indikator kinerja keamanan siber yang terstandarisasi. Rekomendasi ini sejalan dengan perspektif *Whole-of-Government* yang menekankan integrasi kebijakan, koordinasi lintas organisasi pemerintah, dan penyelarasan peran kelembagaan dalam menghadapi permasalahan publik yang kompleks (Christensen & Lægreid, 2007).

Penguatan regulasi perlu didukung peningkatan kapasitas kelembagaan dan sumber daya manusia melalui pelatihan, pendidikan sertifikasi profesi, dan *joint exercise* secara berkelanjutan. Upaya tersebut perlu disertai penerapan standar keamanan informasi, audit berkala, pengembangan SOC, serta penguatan *backup* dan *disaster recovery* untuk meningkatkan kesiapsiagaan organisasi. Selain itu, indikator kinerja dan sistem evaluasi

terstandarisasi diperlukan untuk memastikan efektivitas implementasi kebijakan secara berkelanjutan. Temuan ini mendukung konsep *Cybersecurity Governance* yang menempatkan keamanan siber sebagai bagian dari tata kelola organisasi melalui pengelolaan risiko, kapasitas kelembagaan, pengawasan, dan akuntabilitas, bukan semata aspek teknologi (NIST, 2018).

Penguatan tata kelola juga memerlukan kolaborasi dengan pemerintah daerah, sektor swasta, perguruan tinggi, komunitas keamanan siber, dan mitra internasional dalam pengembangan kapasitas SDM, pertukaran *cyber threat intelligence*, pelaksanaan *joint exercise*, serta riset dan inovasi keamanan siber. Kolaborasi ini diharapkan memperkuat ekosistem keamanan siber melalui pemanfaatan sumber daya dan kompetensi masing-masing pemangku kepentingan. Rekomendasi ini sejalan dengan perspektif *Collaborative Governance* yang menekankan keterlibatan aktor pemerintah dan nonpemerintah dalam membangun kapasitas bersama, kepercayaan, dan efektivitas implementasi kebijakan (Ansell & Gash, 2008; Emerson & Nabatchi, 2015).

Secara keseluruhan, penguatan tata kelola keamanan siber nasional memerlukan integrasi regulasi, peningkatan kapasitas SDM, koordinasi kelembagaan, dan kolaborasi lintas pemangku kepentingan. Temuan ini memperkuat konsep *Cybersecurity Governance, Collaborative Governance,* dan *Whole-of-Government* yang menempatkan tata kelola, koordinasi, dan kolaborasi sebagai faktor penting dalam meningkatkan efektivitas keamanan siber nasional. Secara praktis, rekomendasi tersebut dapat menjadi masukan bagi pemerintah dalam membangun kerangka koordinasi keamanan siber yang lebih terintegrasi untuk meningkatkan ketahanan siber, melindungi layanan publik digital, dan mendukung keberlanjutan transformasi digital Indonesia.

KESIMPULAN

Penelitian ini menunjukkan bahwa permasalahan utama tata kelola keamanan siber nasional terletak pada lemahnya koordinasi antarlembaga, keterbatasan kapasitas sumber daya manusia, dan belum optimalnya pertukaran informasi ancaman siber. Berdasarkan analisis USG, *Fishbone Diagram*, dan Tapisan McNamara, penyusunan kebijakan koordinasi keamanan siber nasional menjadi alternatif dengan prioritas tertinggi. Temuan ini menegaskan pentingnya tata kelola terintegrasi melalui penguatan koordinasi dan kolaborasi lintas kementerian dan lembaga serta pemangku kepentingan terkait. Secara akademik, penelitian ini mengintegrasikan perspektif *Cybersecurity Governance, Collaborative Governance,* dan *Whole-of-Government* sebagai kerangka analitis dalam penguatan tata kelola

keamanan siber dari perspektif kebijakan publik.

Secara praktis, penguatan tata kelola perlu diarahkan pada penyelarasan kewenangan, peningkatan pertukaran informasi ancaman siber, penguatan kapasitas sumber daya manusia, serta kolaborasi antara pemerintah, sektor swasta, perguruan tinggi, komunitas keamanan siber, dan mitra internasional. Upaya tersebut diharapkan mewujudkan tata kelola keamanan siber yang terintegrasi, adaptif, dan tangguh dalam mendukung transformasi digital Indonesia. Penelitian ini memiliki keterbatasan karena menggunakan data sekunder melalui studi dokumentasi sehingga belum menguji implementasi kebijakan secara operasional. Penelitian selanjutnya dapat menggunakan survei, wawancara, atau studi kasus pada kementerian, lembaga, pemerintah daerah, dan sektor strategis untuk menguji implementasi dan efektivitas kebijakan tata kelola keamanan siber.

DAFTAR PUSTAKA

Abrahams, T., Ewuga, S., Kaggwa, S., Uwaoma, P., Hassan, A., & Dawodu, S. (2024). Mastering compliance: A comprehensive review of regulatory frameworks in accounting and cybersecurity. *Computer Science & IT Research Journal*, *5*(1), 120–140. https://doi.org/10.51594/csitrj.v5i1.709

Adma, A., Surbakti, Y. M., & Sari, P. (2023). Transformasi sistem pertahanan siber Indonesia dengan BSSN sebagai poros dan motor penggerak menuju angkatan siber mandiri di masa depan. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(1), Article 7. https://doi.org/10.7454/jkskn.v6i1.10077

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis risiko keamanan siber dalam transformasi digital pelayanan publik di Indonesia. *Jurnal Ketahanan Nasional*, *6*(2), Article 5. https://doi.org/10.7454/jkskn.v6i2.10082

Aji, M. P. (2022). Sistem keamanan siber dan kedaulatan data di Indonesia dalam perspektif ekonomi politik (Studi kasus perlindungan data pribadi). *Jurnal Politica:* Asosiasi Penyelenggara Jasa Internet Indonesia. https://survei.apjii.or.id/home

Athaillah, C. D., Tupen, D., Sari, A. J., Adzzahra, F. C., & Indrawan, J. (2026). Tantangan cyber defense dalam menghadapi serangan siber terhadap infrastruktur pemerintah di Indonesia. *Governance: Jurnal Ilmiah Kajian Politik Lokal Dan Pembangunan*, *13*(2), 74-79. https://doi.org/10.56015/gjikplp.v13i2.653

Bowen, G. A. (2009). Document analysis as a *Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasio nal*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Alfath, T. P., & Cahya, W. (2024). Bridging the gap between policy and practice: Evaluating Indonesia's cybersecurity regulatory framework (2020–2023). *Data Journal of Information Systems and Management*, *2*(1), 14–24. https://doi.org/10.61978/data.v2i1.695

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, *18*(4), 543–571. https://doi.org/10.1093/jopart/mum032

qualitative research method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ090202

Christensen, T., & Lægreid, P. (2007). The whole-of-government approach to public sector reform. *Public Administration Review*, *67*(6), 1059–1066. https://doi.org/10.1111/j.1540-6210.2007.00797.x

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21.https://doi.org/10.22215/timreview/835

Anwar, M., Karolita, D., Areni, I. S., Wardhani, Dunn, W. N. (2018). Public policy analysis: An T. P. M., Syafar, F., & Syamsuddin, I. *integrated approach* (6th ed.).

Routledge. (2025). Cyber capacity buildingin

Emerson, K., & Nabatchi,T. (2015). Indonesia: A study of cyber security awareness in rural community. In G. Oliver,

V. Frings-Hessami, J. T. Du, & T. Tezuka (Eds.), *Sustainability and empowerment in the context of digital libraries* (Vol. 15494, pp. 250–259) Springer. https://doi.org/10.1007/978-981-96-0868-3_21

Anwary, I. (2022). The role of public administration in combating cybercrime: An analysis of the legal framework in Indonesia. *International Journal of Cyber Criminology*, *16*(2), 216–227. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/13 5

APJII. (2026). *Survei internet APJII 2026.Collaborative*

governance regimes. Georgetown University Press.

Herera, D. A., & Sebyar, M. H. (2023). Perlindungan hukum terhadap serangan siber: Tinjauan atas kebijakan dan regulasi terbaru. *Causa: Jurnal Hukum Dan Kewarganegaraan*, *1*(5). https://doi.org/10.3783/causa.v1i1.571

Ikhssani, A., Mudra, C., & Prasidya, F. G. (2024). Cybersecurity dan tata kelola intelijen. *Jurnal Kajian Stratejik Ketahanan Nasional*, *7*(1), Article 2. https://doi.org/10.7454/jkskn.v7i1.10086

Intan, A. A., & Intan, R. (2023). Case study: A review of cybersecurity policies and challenges in Indonesia. In P. Vasant, M. S.

Arefin, V. Panchenko, J. J. Thomas, E. Munapo, G. W. Weber, & R. Rodriguez-Aguilar (Eds.), *Intelligent computing and optimization: Proceedings of the 6th*

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce.

International Conference on Intelligent OECD. (2022). *OECD digital security policy Computing and Optimization 2023 (ICO2023)* (Vol. 3, pp. 266–273). Springer. https://doi.org/10.1007/978-3-031-50327-6_28

ISACA. (2020). *COBIT 2019: Governance and management objectives*. ISACA.

Ishikawa, K. (1986). *Guide to quality control* (2nd rev. ed.). Asian Productivity Organization.

Kalderemidis, I., Farao, A., Bountakas, P., Panda, S., & Xenakis, C. (2022). GTM: Game theoretic methodology for optimal cybersecurity defending strategies and investments. *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22)* , 1–9. https://doi.org/10.1145/3538969.35444

Kementerian Komunikasi dan Digital. (2024). *Laporan insiden Pusat Data Nasional Sementara (PDNS) 2 tahun 2024*. Komdigi.

Khaw, T., Amran, A., & Teoh, A. (2024). Building a thematic framework of cybersecurity: A systematic literature review approach. *Journal of Systems and Information Technology*, *26*(2), 234–256. https://doi.org/10.1108/JSIT-07-2023-0132

Layode, O., Naiho, H. N. N., Adeleke, G.S.,

Udeh, E.O., & Labake, T.T. (2024). The role of cybersecurity in facilitating sustainable

healthcare solutions: Overcoming challenges to protect sensitive data. *International Medical Science Research Journal*, *4*(6), 668–693. https://doi.org/10.51594/imsrj.v4i6.1228

Maharani, M. A., & Atman, W. (2025). Evaluasi strategi nasional keamanan siber Indonesia dalam menanggapi ancaman digital Indonesia. *Jurnal Integrasi Ilmu Sosial Dan*

framework: Towards a digital security strategy for prosperity. OECD Publishing. https://doi.org/10.1787/a69df866-en

Qudus, L. (2025). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. *Journal of Public Digital Governance*, *14*(1), 1146–1163. https://doi.org/10.30574/ijsra.2025.14.1.02 25

Racionero-Garcia, J., & Shaikh, S. A. (2024). Space and cybersecurity: Challenges and opportunities emerging from national strategy narratives. *Space Policy*, *70*. https://doi.org/10.1016/j.spacepol.2024.101 648

Ramli, A. M., Suseno, S., Mayana, R. F., Rajamanickam, R., & Rohmana, R. D. (2026). The urgency of regulating artificial intelligence in relation to cybersecurity and cyber resilience. *Cogent Social Sciences*, *12*(1), 2632977. https://doi.org/10.1080/23311886.2026.263 2977

Rusydi, M. T. (2025). Evaluating global cybersecurity laws: Effectiveness of legal frameworks and enforcement mechanisms in the digital age. *Walisongo Law Review (Walrev),* *6*(1), 71–83. https://doi.org/10.21580/walrev.2024.6.1.2 0960

Shah, M. U., Iqbal, F., Rehman, U., & Hung, P.

C. K. (2023). A comparative assessment of human factors in cybersecurity: Implications for cyber governance. *IEEE Access*, *11*, 87970–87984. https://doi.org/10.1109/ACCESS.2023.329 6580

Politik, *2*(3), 344-354. Stallings, W. (2018). *Effective cybersecurity: A* https://doi.org/10.62383/sosial.v2i3.2291 *guide to using best practices and standards.* Pearson.

Syawaluddin, A. S., Putra, A. F. H., & Putra, M.

A. (2025). Cyber security dan ketahanan nasional: Tantangan dan solusi di

era digital. *Jurnal Media Akademik*, *3*(6). https://doi.org/10.62281/v3i6.2422

Taufik, T., Sarinah, S., Amir, M., Liwaul, L., Azizah, N., Suaib, E., Nurhayati, S., Kartika, B., Rintaka, M. I. N. I., Rahman, R., Elwan,

L. O. M., Kadir, A., Sudirman, F. A., Rasmin, R., & Rijal, M. (2025). *Digital governance: Konsep, strategi dan implementasinya di Indonesia*. CV. Gita Lentera.

Von Solms, B., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Yamada, R. (2024). Impact of cybersecurity regulations on corporate compliance practices in Japan. *International Journal of Law and Policy*, *9*(2), 28–38. https://doi.org/10.47604/ijlp.2705