Jurnal Sosial dan Sains (SOSAINS)
p-ISSN 2774-7018 e-ISSN 2774-700x

Reformasi Tata Kelola Intelijen di Era Digital: Adaptasi Terhadap Ancaman Siber

Ramadhan Sofyan, Joko Sriwidodo , Edi Saputra Hasibuan
Universitas Bhayangkara Jakarta Raya, Indonesia
Email: fian.cicco@gmail.com, joko.sriwidodo@dsn.ubharajaya.ac.id,
hedihasibuan@yahoo.co.id

Abstrak

Transformasi digital kini menjadi fokus utama dalam merespons ancaman siber yang kian rumit di era modern. Penelitian ini menggunakan pendekatan kualitatif dengan memanfaatkan data sekunder untuk menganalisis serta mengeksplorasi tata kelola transformasi digital dan strategi dalam membangun ketahanan siber. Hasil penelitian ini menunjukkan bahwa tata kelola transformasi digital yang diterapkan oleh Badan Intelijen Negara (BIN) berperan dalam meningkatkan ketahanan siber nasional. Untuk menghadapi serangan siber yang terus berkembang, diperlukan penyesuaian struktural agar organisasi intelijen lebih responsif dan adaptif. Strategi ketahanan siber BIN meliputi penerapan kerangka kerja keamanan siber, peningkatan kapasitas sumber daya manusia, serta pengembangan kebijakan yang mendukung. Melalui Peraturan Presiden Nomor 73 Tahun 2017, BIN telah merestrukturisasi organisasi dengan fokus pada keamanan siber guna memperkuat pertahanan nasional. Selain itu, kolaborasi antara sektor publik dan masyarakat dalam meningkatkan kesadaran serta literasi digital menjadi elemen penting dalam menjaga keamanan siber negara. Dengan demikian, reformasi tata kelola intelijen dan adaptasi strategi ketahanan siber menjadi kunci utama dalam menghadapi ancaman digital.

Kata Kunci : Tata Kelola Digital, Ketahanan Siber, Badan Intelijen Negara

Abstract

Digital transformation is now a major focus in responding to increasingly complex cyber threats in the modern era. This study uses a qualitative approach utilizing secondary data to analyze and explore digital transformation governance and strategies for building cyber resilience. The results of this study indicate that the digital transformation governance implemented by the State Intelligence Agency (BIN) plays a role in increasing national cyber resilience. To deal with the ever-growing cyber attacks, structural adjustments are needed so that intelligence organizations are more responsive and adaptive. BIN's cyber resilience strategy includes the implementation of a cybersecurity framework, increasing human resource capacity, and developing supportive policies. Through Presidential Regulation Number 73 of 2017, BIN has restructured the organization with a focus on cybersecurity to strengthen national defense. In addition, collaboration between the public sector and society in increasing awareness and digital literacy is an important element in maintaining the country's cybersecurity. Thus, intelligence governance reform and adaptation of cyber resilience strategies are the main keys in dealing with digital threats.

Keywords: Digital Transformation, Cyber Resilience, State Intelligence Agency

PENDAHULUAN

Seiring dengan laju globalisasi, teknologi informasi menjadi sarana penting bagi manusia sebagai makhluk sosial dalam menjalin interaksi. Globalisasi membawa dampak besar terhadap perkembangan peradaban, termasuk dalam kemajuan teknologi informasi. Tidak dapat dipungkiri bahwa dalam beberapa dekade terakhir, teknologi informasi telah menjadi pusat perhatian dunia (Muadifah and B. Herawan Hayadi at.al 2024).

Perkembangan teknologi yang pesat di Indonesia turut memengaruhi dinamika sosial dan keamanan masyarakat. Tingginya penggunaan internet membuka peluang terjadinya kejahatan berbasis dunia maya. Di era globalisasi, ancaman siber tidak lagi terbatas pada upaya untuk menyerang negara, instansi pemerintahan, atau sektor militer semata, melainkan telah

merambah berbagai aspek kehidupan, seperti ekonomi, politik, budaya, dan keamanan nasional (M, 2014a).

Kemajuan pembangunan global yang terus meningkat berjalan seiring dengan pesatnya perkembangan teknologi yang kini telah menjadi bagian integral dari kehidupan manusia. Hampir seluruh aktivitas manusia kini dapat dilakukan dengan dukungan teknologi informasi, termasuk aktivitas kejahatan (Kalvet, 2012; Kitsing, 2011; M, 2014b; Welch, 2014). Kecanggihan teknologi tidak hanya digunakan untuk tujuan positif, tetapi juga dimanfaatkan untuk tindakan yang bersifat negatif, sehingga menimbulkan berbagai ancaman bagi pengguna, terutama melalui pemanfaatan ruang maya (*cyber space*).

Secara sederhana, *cyberspace* dapat dipahami sebagai ruang komunikasi berbasis komputer dalam sebuah realitas baru, yakni realitas virtual yang memanfaatkan dunia maya. Perkembangan ini membawa dampak signifikan terhadap perubahan tatanan sosial dan budaya. Kehadiran cyberspace juga mengubah konsep tentang masyarakat, komunitas, komunikasi, serta bentuk interaksi sosial dan budaya. Dengan semakin luasnya penggunaan internet, isu *cybercrime* menjadi tidak terlepas dari persoalan keamanan jaringan komputer dan keamanan informasi berbasis internet di era global, di mana tindak kejahatan dunia maya berkembang seiring pesatnya kemajuan teknologi informasi (Raharjo, 2002)

Kejahatan dunia maya merupakan sisi lain dari isu keamanan siber, yang mencakup berbagai aktivitas ilegal dan merusak dengan memanfaatkan komputer serta internet. Secara umum, *cybercrime* dapat dipahami sebagai setiap bentuk tindakan kriminal yang melibatkan komputer, perangkat digital, atau jaringan. Tingginya jumlah pengguna internet berdampak pada meningkatnya kerentanan terhadap tindak kejahatan di ruang maya. Bentuk kejahatan siber meliputi rekayasa sosial, pemanfaatan celah perangkat lunak, serangan terhadap jaringan, serta ancaman keamanan digital lainnya. Aktivitas kriminal ini mencakup pelecehan, pemerasan, pencucian uang, distribusi konten pornografi, promosi perjudian daring, dan berbagai tindakan ilegal lainnya.

Data dari inet.detik.com menunjukkan bahwa jumlah pengguna internet di Indonesia sangat besar. Pada awal 2025, pengguna internet di Indonesia tercatat mencapai 212 juta orang dari total populasi 285 juta jiwa, dengan tingkat penetrasi sebesar 74,6%. Laporan Digital 2025 Global Overview Report yang dirilis We Are Social melalui analisis Kepios juga menegaskan bahwa dalam setahun terakhir, pengguna internet di Indonesia bertambah 17 juta orang, atau meningkat 8,7% dibanding periode sebelumnya. Selain itu, tingkat adopsi internet (proporsi populasi yang menggunakan internet) juga naik relatif sebesar 7,9% (+543 basis poin) dalam periode yang sama (Agus Tri Haryanto, 2025).

Laporan GSMA Intelligence mencatat terdapat sekitar 365 juta pengguna ponsel di Indonesia. Angka ini menunjukkan bahwa sebagian individu memiliki lebih dari satu perangkat seluler, misalnya dengan memisahkan penggunaan untuk kepentingan kerja dan kebutuhan pribadi. Tren dari waktu ke waktu memperlihatkan bahwa jumlah sambungan seluler di Indonesia meningkat sebesar 5,7 juta atau 1,6% antara awal 2024 dan awal 2025. Selain itu, data GSMA Intelligence mengungkapkan bahwa 96,4% koneksi seluler di Indonesia sudah tergolong sebagai “broadband”, yang berarti terkoneksi melalui jaringan 3G, 4G, atau 5G. Tingginya jumlah pengguna internet juga sejalan dengan kepemilikan akun media sosial, di mana pada Januari 2025 terdapat 143 juta akun media sosial aktif, setara dengan 50,2% populasi Indonesia (Agus Tri Haryanto, 2025).

Dalam era digital yang semakin maju, reformasi tata kelola intelijen menjadi kebutuhan mendesak di berbagai negara. Transformasi teknologi informasi dan komunikasi telah mengubah wajah ancaman keamanan, khususnya dengan munculnya serangan siber yang semakin kompleks dan berteknologi tinggi. Kondisi ini menuntut adanya restrukturisasi intelijen yang lebih adaptif, efektif, dan responsif terhadap dinamika baru. Lebih jauh lagi, perkembangan teknologi digital membuka ruang bagi aktor negara maupun non-negara untuk melakukan aktivitas yang berpotensi mengancam keamanan nasional. Pemanfaatan teknologi mutakhir dalam operasi intelijen memang mendukung proses pengumpulan serta analisis data berskala besar, namun sekaligus menghadirkan tantangan terkait aspek privasi dan keamanan (Redaksi Indojpnn.net, 2024).

Era digital telah menandai fase baru dalam evolusi intelijen, di mana teknologi tidak lagi sekadar alat pendukung, tetapi menjadi fondasi utama restrukturisasi sistem intelijen modern. Pemanfaatan sensor pintar, platform media sosial, big data, hingga kecerdasan buatan memungkinkan pengumpulan dan analisis informasi berlangsung lebih cepat, akurat, dan adaptif terhadap dinamika ancaman. Transformasi ini bukan hanya meningkatkan efektivitas deteksi dan respons intelijen, tetapi juga membuka peluang kolaborasi lintas lembaga secara lebih integratif. Namun, percepatan digitalisasi juga membawa konsekuensi serius, terutama pada isu keamanan data dan perlindungan privasi. Oleh karena itu, integrasi teknologi dalam intelijen harus dijalankan secara bertanggung jawab dan berimbang, agar revolusi digital benar-benar memperkuat keamanan nasional tanpa mengorbankan hak-hak fundamental warga negara (Senopati, 2024).

Dalam situasi global yang semakin kompleks, ancaman terhadap keamanan nasional menjadi semakin beragam dan terus berubah. Untuk menghadapinya, dibutuhkan sistem intelijen yang adaptif, efisien, dan terintegrasi. Restrukturisasi intelijen serta penguatan kerja sama antar lembaga merupakan elemen penting dalam membangun sistem yang tangguh, sehingga mampu menyajikan informasi yang akurat dan tepat waktu bagi proses pengambilan keputusan strategis.

Restrukturisasi intelijen mencakup transformasi mendalam pada struktur organisasi, peran, serta pola koordinasi antar lembaga intelijen. Upaya ini bertujuan untuk mengoptimalkan efektivitas dalam proses pengumpulan dan analisis data, sekaligus memperkuat sinergi serta kolaborasi lintas institusi. Dalam kerangka kerja sama tersebut, restrukturisasi menjadi kunci untuk menciptakan sinergi serta mencegah terjadinya tumpang tindih tugas. Ada sejumlah faktor yang mendorong urgensi restrukturisasi intelijen, antara lain:

1. Munculnya berbagai ancaman baru yang kompleks, seperti terorisme, kejahatan lintas negara, dan perang siber, menuntut adanya pendekatan intelijen yang lebih terintegrasi serta kolaboratif.
2. Sistem intelijen konvensional belum mampu menyesuaikan diri dengan perkembangan pesat teknologi informasi dan komunikasi.
3. Diperlukan peningkatan efisiensi dan efektivitas dalam operasional lembaga intelijen.
4. Tumbuhnya tuntutan publik terhadap akuntabilitas dan transparansi dalam aktivitas badan intelijen.

Jika ditarik perbandingan, sebelum era digital mendominasi hampir seluruh aspek kehidupan, terdapat perbedaan yang cukup mencolok antara model intelijen lama dan model

intelijen setelah restrukturisasi. Hal ini sebagaimana dijelaskan oleh (Senopati, 2024) dalam artikelnya, yang menyebutkan bahwa:

Tabel 1. Restrukturisasi (Senopati, 2024)

Aspek	Model Intelijen Sebelum Restrukturisasi	Model Intelijen Sesudah Restrukturisasi
Organisasi	Struktur masih terpecah, dengan banyak lembaga intelijen bekerja secara independen.	Struktur lebih menyatu, dipimpin oleh lembaga utama dengan koordinasi yang kuat dan peran yang jelas.
Fungsi	Fokus pada pengumpulan data, namun analisis informasi belum terorganisir dengan baik.	Fokus pada pengumpulan sekaligus analisis informasi yang terstruktur dan terintegrasi, dengan penekanan pada prediksi serta evaluasi ancaman.
Koordinasi	Kerja sama antar lembaga lemah, mekanisme berbagi informasi belum efektif.	Koordinasi antar lembaga lebih solid, dengan mekanisme pertukaran informasi yang sistematis dan terstruktur.

Sumber: prabowocapres.com

Di Indonesia, transformasi digital memberikan dampak signifikan pada berbagai aspek kehidupan, termasuk sektor keamanan. Lembaga intelijen dituntut untuk segera menyesuaikan diri dengan perubahan ini guna merespons ancaman siber yang terus berkembang (Senopati, 2024). Meski demikian, proses adaptasi ke era digital juga menghadirkan persoalan etis dan sosial. Pemanfaatan teknologi mutakhir dalam pengumpulan, analisis, serta distribusi informasi memunculkan isu mengenai privasi, transparansi, dan akuntabilitas dalam praktik intelijen. Penggunaan data pribadi untuk kepentingan analisis intelijen berpotensi menimbulkan kekhawatiran terkait pelanggaran hak privasi individu. Karena itu, diperlukan jaminan bahwa proses pengumpulan dan pemanfaatan data pribadi dilakukan secara etis, sesuai hukum, dan penuh tanggung jawab.

Di sisi lain, transparansi dalam operasi intelijen menjadi semakin penting. Publik perlu memahami sejauh mana teknologi dimanfaatkan dalam kegiatan intelijen serta bagaimana perlindungan terhadap data pribadi dijalankan. Teknologi sebetulnya dapat menjadi instrumen untuk memperkuat akuntabilitas dan keterbukaan, misalnya melalui sistem audit dan pelacakan digital yang memastikan operasi berjalan sesuai regulasi dan norma etika. Namun, teknologi juga menyimpan potensi untuk disalahgunakan, baik dalam bentuk manipulasi informasi maupun penyalahgunaan kewenangan. Oleh karena itu, pemanfaatan teknologi harus dijalankan secara bijaksana dan bertanggung jawab agar tidak menimbulkan penyalahgunaan kekuasaan.

Perlindungan hak asasi manusia merupakan aspek krusial dalam reformasi tata kelola intelijen di era digital. Teknologi dapat dimanfaatkan untuk mendukung perlindungan HAM sekaligus mencegah penyalahgunaan kewenangan dalam praktik intelijen. Misalnya, analitik data dapat membantu mendeteksi dan mencegah tindak kejahatan seperti terorisme maupun perdagangan manusia. Meski demikian, pemanfaatan teknologi harus tetap memperhatikan prinsip penghormatan HAM. Algoritma yang digunakan perlu dirancang secara adil dan bebas dari bias, sementara sistem pengawasan harus memastikan perlindungan privasi serta hak-hak sipil.

Di sisi lain, penerapan pertahanan siber menjadi kebutuhan mendesak sekaligus kewajiban prioritas bagi negara dan seluruh institusi yang bergantung pada ruang digital. Tingkat urgensi pertahanan siber sejalan dengan tingginya ketergantungan terhadap teknologi di ruang maya. Oleh karena itu, dunia siber harus dilindungi secara memadai untuk mencegah risiko yang dapat merugikan individu, organisasi, maupun negara. Konsep pertahanan siber lahir sebagai respons untuk menghadapi ancaman dan gangguan yang muncul dari ruang maya.

Dalam skala global, negara-negara maju telah memanfaatkan teknologi mutakhir dalam menjalankan operasi intelijen. Contohnya, penerapan algoritma pembelajaran mesin untuk mendeteksi pola ancaman serta penggunaan teknologi enkripsi dalam menjaga kerahasiaan data sensitif. Kendati demikian, penerapan teknologi ini harus diseimbangkan dengan kebijakan yang menjamin privasi dan keamanan data. Penggunaan teknologi dalam intelijen perlu dilakukan secara etis dan bertanggung jawab, agar tidak melanggar hak individu serta tetap menjaga kepercayaan publik.

Di Indonesia, upaya reformasi tata kelola intelijen di era digital membutuhkan strategi yang menyeluruh. Hal ini meliputi penyusunan kebijakan yang tegas terkait pemanfaatan teknologi dalam aktivitas intelijen, peningkatan kompetensi sumber daya manusia di bidang teknologi informasi, serta penguatan landasan hukum mengenai privasi dan keamanan data. Selain itu, mekanisme pengawasan yang efektif harus dibangun guna mencegah potensi penyalahgunaan teknologi. Kerja sama antar lembaga intelijen dan keamanan juga sangat penting untuk menghadapi ancaman siber. Pemanfaatan teknologi dapat memperkuat efektivitas penggunaan sumber daya, meningkatkan sinergi antar lembaga, serta mengoptimalkan sistem peringatan dini, yang pada akhirnya berkontribusi pada penguatan keamanan nasional.

Selain itu, penting untuk meningkatkan kesadaran dan literasi digital di kalangan masyarakat. Masyarakat yang melek teknologi dapat berperan sebagai mitra dalam mendeteksi dan melaporkan ancaman siber (al-amri, 2024). Edukasi mengenai keamanan siber dan praktik terbaik dalam penggunaan teknologi dapat membantu mengurangi risiko serangan siber dan meningkatkan ketahanan nasional terhadap ancaman tersebut. Dalam menghadapi ancaman siber yang terus berkembang, reformasi tata kelola intelijen harus bersifat adaptif dan proaktif. Pengembangan strategi yang fleksibel dan responsif terhadap perubahan teknologi dan modus operandi pelaku ancaman menjadi kunci keberhasilan dalam menjaga keamanan nasional.

Penelitian ini bertujuan untuk menganalisis bagaimana reformasi tata kelola intelijen di Indonesia dikembangkan sebagai respons terhadap dinamika ancaman siber yang terus berkembang. Fokus utama diarahkan pada strategi-strategi yang diterapkan oleh BIN dalam memperkuat ketahanan siber nasional, baik dari sisi struktural, kebijakan, maupun pengembangan sumber daya manusia dan teknologi. Di samping itu, penelitian ini juga akan mengidentifikasi tantangan-tantangan utama dalam proses restrukturisasi kelembagaan intelijen di era digital serta bagaimana koordinasi lintas sektor dapat dioptimalkan.

Implikasi dari penelitian ini terbagi menjadi dua dimensi. Pertama, dari segi teoretis, kajian ini memberikan kontribusi terhadap pengayaan literatur mengenai tata kelola keamanan digital dan reformasi kelembagaan intelijen di negara berkembang, yang selama ini masih terbatas. Penelitian ini juga memperluas pemahaman mengenai penerapan prinsip governance dalam konteks keamanan siber dan intelijen negara. Kedua, dari segi praktis, temuan penelitian ini dapat menjadi rujukan strategis bagi pemerintah dan lembaga intelijen dalam merumuskan

kebijakan yang lebih adaptif, transparan, dan akuntabel di tengah kompleksitas ancaman siber modern.

Dengan demikian, reformasi tata kelola intelijen tidak hanya menjadi kebutuhan birokratis, tetapi juga bagian integral dari sistem pertahanan nasional yang proaktif dan tanggap terhadap transformasi digital global. Penguatan struktur kelembagaan, sinergi antarlembaga, serta investasi pada kapabilitas digital menjadi fondasi penting untuk membangun sistem intelijen yang andal dan berdaya saing tinggi di era siber saat ini.

METODE PENELITIAN

Penelitian ini menerapkan pendekatan kualitatif, yang dinilai efektif untuk memahami dan menganalisis reformasi tata kelola intelijen di era digital (Handoko et al., 2024). Melalui pendekatan ini, penulis dapat menggali secara mendalam dinamika internal maupun eksternal yang memengaruhi proses reformasi. Teknik yang digunakan mencakup wawancara mendalam, observasi partisipatif, serta analisis berbagai dokumen seperti jurnal, karya ilmiah, dan regulasi terkait. Penulis dapat mengungkap persepsi, pengalaman dan tantangan yang dihadapi oleh organisasi intelijen dalam upaya adaptasi terhadap ancaman siber (Faizah and Sashari R. A., 2023).

HASIL DAN PEMBAHASAN

1. Tata Kelola Transformasi Digital guna Menghadapi Ancaman Siber

Transformasi digital telah mengubah peta ancaman keamanan global, dengan serangan siber menjadi salah satu tantangan utama bagi lembaga intelijen dunia, termasuk Badan Intelijen Negara (BIN) Indonesia. Untuk menghadapi kompleksitas ancaman tersebut, BIN perlu melakukan penyesuaian struktur organisasi agar lebih lincah dan responsif terhadap perkembangan teknologi informasi.

Beberapa negara telah membuktikan bahwa integrasi transformasi digital dalam tata kelola dapat menghasilkan capaian besar. Estonia, Korea Selatan, dan India menjadi contoh nyata bagaimana digitalisasi mampu memperkuat efisiensi birokrasi, meningkatkan transparansi, membuka ruang partisipasi publik, sekaligus memperkuat strategi intelijen. Estonia bahkan dikenal sebagai pionir lewat program e-Estonia, yang menjadikannya salah satu negara dengan ekosistem digital paling maju di dunia. Keberhasilan tersebut ditopang oleh fondasi infrastruktur digital yang kuat, regulasi hukum yang jelas, serta fokus pada keamanan siber. Terobosan seperti e-Residency dan X-Road berhasil menyederhanakan layanan publik sekaligus mendorong lahirnya inovasi baru (Kalvet, 2012; Kitsing, 2011). Bagi Indonesia, pengalaman tersebut relevan sebagai pembelajaran bahwa infrastruktur digital yang andal serta dukungan regulasi merupakan kunci dalam membangun tata kelola digital yang efektif.

Transformasi digital di Korea Selatan tercermin melalui inisiatif e-government yang komprehensif. Pemerintah menekankan pembangunan infrastruktur internet berkecepatan tinggi serta peningkatan literasi digital masyarakat, yang berkontribusi pada peningkatan kualitas layanan publik dan partisipasi warga (Nam, 2012). Program *Government 3.0*, dengan fokus pada transparansi dan keterbukaan data, berhasil menciptakan tata kelola yang lebih inklusif dan efisien. Bagi Indonesia, penekanan serupa pada literasi digital dan keterbukaan informasi dapat membantu menutup kesenjangan digital sekaligus mendorong terciptanya model tata kelola yang lebih partisipatif.

Sementara itu, India menunjukkan keberhasilan transformasi digital melalui program *Digital India*, yang menyoroti digitalisasi skala besar. Implementasi sistem identifikasi biometrik *Aadhaar* serta perluasan layanan digital meningkatkan efisiensi sekaligus memperluas akses masyarakat terhadap layanan publik (Gelb & Metz, 2017). Pengalaman India menegaskan pentingnya penerapan solusi digital yang dapat diskalakan dan terintegrasi dengan sistem yang ada untuk mengatasi berbagai tantangan tata kelola. Bagi Indonesia, pemanfaatan solusi digital yang fleksibel dan luas berpotensi meningkatkan kualitas tata kelola secara signifikan.

Indonesia sendiri juga telah menunjukkan perkembangan berarti dalam upaya transformasi digital, terutama pada sektor publik. Program digitalisasi ini merupakan bagian dari strategi e-government yang bertujuan memperbaiki kualitas layanan publik, memperkuat transparansi, serta meningkatkan partisipasi warga negara. Beberapa langkah strategis yang menonjol antara lain penerapan Rencana Induk E-Government Indonesia (E-Gov MP) dan proyek smart city nasional (Rokhman, 2011). Selain itu, lahirnya berbagai platform daring untuk pelayanan publik, seperti National Single Window dalam fasilitasi perdagangan serta program One Data Indonesia yang berfokus pada standarisasi dan integrasi data lintas lembaga, telah berhasil meningkatkan efisiensi, aksesibilitas, transparansi, dan akuntabilitas (Priyono A. et al. 2020).

Meskipun demikian, proses transformasi digital di Indonesia masih menghadapi berbagai tantangan. Hambatan utama meliputi kesenjangan digital, keterbatasan infrastruktur teknologi di wilayah pedesaan, serta meningkatnya ancaman keamanan siber. Selain itu, adanya resistensi institusional di tubuh birokrasi pemerintah dan rendahnya literasi digital di sebagian kelompok masyarakat turut menghalangi pemanfaatan optimal dari transformasi digital.

Jika dibandingkan dengan pengalaman negara lain, terdapat sejumlah pelajaran berharga bagi Indonesia. Estonia, misalnya, berhasil membangun infrastruktur digital yang kokoh serta mengembangkan program e-residency yang aman, yang dapat dijadikan referensi untuk memperkuat tata kelola digital Indonesia (Adeodato & Pournouri, 2020). Pendekatan menyeluruh Estonia terhadap identitas digital dan keamanan data juga relevan untuk membantu Indonesia mengatasi isu terkait privasi dan perlindungan siber.

Hal serupa dapat dilihat pada Korea Selatan, yang menitikberatkan pada akses internet berkecepatan tinggi dan program literasi digital sebagai fondasi utama keberhasilannya. Strategi ini dapat diadopsi Indonesia untuk menutup kesenjangan digital serta memperluas partisipasi publik dalam tata kelola digital. Sementara itu, pengalaman India melalui inisiatif digitalnya menekankan pentingnya solusi yang skalabel dan integrasi teknologi dengan kerangka tata kelola yang ada. Pendekatan ini memberi inspirasi bagi Indonesia dalam meningkatkan layanan digital publik sekaligus menyesuaikan dengan kebutuhan masyarakat yang beragam.

Dalam Sidang Kabinet Paripurna pada masa pemerintahan Presiden Jokowi, beliau menekankan beberapa langkah strategis sebagai pedoman transformasi digital layanan pemerintah (Humas MENPANRB, 2024), yaitu:

a. Indonesia perlu segera memiliki layanan digital yang terintegrasi, tidak lagi terpecah-pecah sebagaimana kondisi sebelumnya.

b. Percepatan transformasi digital pemerintah dilakukan melalui perubahan struktural BUMN Peruri menjadi "GovTech" atau tim pengelola digital nasional.
c. Pentingnya membangun kerja kolaboratif di seluruh sektor.
d. Penegasan perlunya perlindungan data pribadi.
e. Penguatan koordinasi dalam pelaksanaan sembilan layanan prioritas yang akan dikonsolidasikan, mencakup layanan pendidikan, kesehatan, kepolisian, digital ID, digital payment, serta layanan aparatur negara.

2. Adaptasi Strategi Ketahanan Siber oleh Badan Intelijen Negara

Pertahanan siber merupakan langkah yang dilakukan untuk menghadapi serangan di dunia maya yang dapat mengganggu jalannya sistem pertahanan negara. Pentingnya pertahanan siber terletak pada kemampuannya untuk mengantisipasi ancaman serta serangan digital, sekaligus menggambarkan tingkat ketahanan yang ada saat ini. Oleh karena itu, diperlukan kesiapan, respons cepat, serta kemampuan pemulihan guna mengatasi dampak dari serangan siber.

Di Indonesia, strategi yang digunakan untuk melawan berbagai bentuk kejahatan siber adalah melalui penerapan keamanan siber (cyber security). Menurut Kaspersky, sebagaimana dikutip dalam (Lukiman, n.d.), keamanan siber adalah praktik melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari serangan berbahaya di ruang digital. Sementara itu, Cisco (dalam Lukiman, n.d.) menjelaskan bahwa keamanan siber merupakan upaya perlindungan terhadap beragam sistem jaringan dan perangkat lunak dari ancaman digital. Dari kedua definisi tersebut dapat disimpulkan bahwa keamanan siber adalah suatu sistem perlindungan informasi di dunia maya dari berbagai bentuk serangan.

Berdasarkan data terbuka dalam Lanskap Keamanan Siber 2023, yang mencakup hasil deteksi ancaman dari trafik internet Indonesia, pemantauan *cyber threat intelligence*, analisis kerentanan pada aplikasi berbasis internet yang diuji oleh BSSN, serta pengalaman dari penanganan insiden sebelumnya, diperkirakan terdapat sejumlah potensi ancaman siber yang berpotensi meningkat pada tahun 2024. Ancaman tersebut mencakup *Web Defacement*, *Malware Stealer* dan *Ransomware*, *Cyber Threat* berbasis *Artificial Intelligence (AI)*, serangan *Internet of Things (IoT)*, *Advanced Persistent Threat (APT)*, *Phishing*, hingga berbagai bentuk kejahatan siber lainnya. Identifikasi potensi ini didasarkan pada tren kenaikan signifikan dalam beberapa tahun terakhir, yang diprediksi akan terus berlanjut di tahun 2024.

Melihat potensi ancaman tersebut, Indonesia memerlukan strategi keamanan siber nasional. Jika keamanan dipahami sebagai kondisi bebas dari ancaman maupun bahaya, maka salah satu elemen utama dalam pengelolaan *cyber security* adalah bagaimana risiko di ruang siber dipahami dan direspon dengan solusi tepat. Tanpa langkah-langkah pertahanan yang memadai, kemungkinan meningkatnya ancaman akan semakin besar (Nam, 2012).

Pada tahun 2024, dinamika ruang siber baik di tingkat global maupun nasional yang dipengaruhi oleh perkembangan Teknologi Informasi dan Komunikasi (TIK) menunjukkan bahwa isu keamanan siber menjadi semakin esensial. Hal ini tidak hanya terkait dengan perlindungan data pribadi serta informasi sensitif, tetapi juga menyangkut stabilitas ekosistem digital demi mengoptimalkan potensi ekonomi digital Indonesia.

Berdasarkan ketentuan Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014, Kemhan (2014) mendefinisikan ruang siber (cyber space) sebagai wadah dimana

komunitas saling terhubung melalui jaringan, seperti internet, untuk melakukan berbagai aktivitas sehari-hari. Sejalan dengan itu, Bruce Sterling yang dikutip oleh Putri (2021) menyatakan bahwa:

"although it is not exactly "real" "cyber space" is a genuine place. Things happen there thar have veri genuine consequences. This place is not real, but it is serious, it is earnest. Tens of thousand of people have dedicated their lives to it, to the public service of public communication by wire and electronics."

Dengan demikian, ruang siber dapat dipahami sebagai ranah yang menghadirkan dampak ganda, baik positif maupun negatif. Walaupun transformasi digital membawa banyak manfaat, tantangan besar dalam bentuk ancaman keamanan siber juga turut menyertainya (Gelb A. D., 2017; Hinings T. and Greenwood R., 2018). Data dari Lanskap Keamanan Siber Indonesia 2024 menunjukkan bahwa total anomali trafik internet di Indonesia mencapai 403.990.813 kejadian, dengan jenis terbanyak berupa *Generic Trojan RAT* yang mengindikasikan adanya komunikasi *backdoor* menuju domain berbahaya yang terhubung ke *command and control server* milik aktor ancaman. Selain itu, terdeteksi pula 4.001.905 aktivitas *Advanced Persistent Threat (APT)* dan 1.011.209 aktivitas ransomware. Dari laporan yang diterima melalui layanan aduan siber, terdapat 1.417 aduan, dengan cyber crime mendominasi hingga 86% dari total kasus (BSSN, 2024).

Berdasarkan hasil evaluasi, **BSSN** melakukan **IT Security Assessment (ITSA)** terhadap berbagai sistem elektronik dan mengidentifikasi **2.860 kerentanan** pada **586 sistem**. Kerentanan paling kritis yang ditemukan adalah **Insecure Data Object Reference (IDOR)**, yang memungkinkan pihak-pihak tidak berwenang mengakses atau memodifikasi data tanpa melalui mekanisme validasi dan otorisasi yang memadai. Situasi ini menegaskan urgensi penerapan **kerangka kerja keamanan siber yang menyeluruh**, seperti *NIST Cybersecurity Framework*, yang menekankan praktik manajemen risiko komprehensif untuk melindungi infrastruktur vital. Mengingat meningkatnya skala dan kompleksitas ancaman siber, Indonesia harus memperkuat pertahanan siber secara berkelanjutan untuk menjamin keamanan data sensitif dan stabilitas sistem pemerintahan.

Pada akhirnya, sebagai langkah awal dalam menghadapi ancaman siber, pemerintah Indonesia mengeluarkan Peraturan Presiden Nomor 73 Tahun 2017 yang mengubah struktur organisasi BIN. Perubahan ini mencakup pembentukan Deputi VI yang bertanggung jawab atas intelijen siber. Deputi VI memiliki tugas merumuskan kebijakan dan melaksanakan kegiatan atau operasi intelijen siber, termasuk penyusunan rencana, pelaksanaan, pengoordinasian, pengendalian, dan penyusunan laporan terkait intelijen siber. Selain itu, dibentuk juga Deputi VII yang fokus pada intelijen di bidang komunikasi massa, komunikasi sosial, dan informasi. Deputi ini bertugas merumuskan kebijakan dan melaksanakan kegiatan intelijen terkait media dan informasi, yang merupakan aspek krusial dalam era digital.

Pembentukan kedua deputi ini menunjukkan upaya BIN untuk menyesuaikan struktur organisasinya dalam menghadapi ancaman siber dan dinamika informasi di era digital. Dengan adanya deputi khusus yang menangani intelijen siber dan komunikasi, BIN dapat lebih fokus dan terarah dalam mengantisipasi serta merespons berbagai ancaman yang muncul dari dunia maya. Selain penyesuaian struktur organisasi, BIN juga menekankan pentingnya pengembangan sumber daya manusia (SDM) yang kompeten di bidang siber. Langkah konkret yang diambil adalah melalui Sekolah Tinggi Intelijen Negara (STIN), yang menambahkan

program studi baru seperti S-2 Intelijen Medik dan rencana pengembangan program S-1 dan S-2 Intelijen Siber serta S-3 Intelijen Strategis. Upaya ini bertujuan untuk mencetak SDM berkualitas yang mampu menghadapi ancaman perang asimetris dan siber (Christianingrum et al., 2021).

BIN menempatkan **kolaborasi lintas instansi** sebagai salah satu strategi utama dalam memperkuat kapabilitas intelijen digital. Salah satu contohnya adalah kerja sama dengan **Kementerian PANRB** dalam mendorong transformasi digital, termasuk menjaga keamanan portal pemerintah dari potensi ancaman intelijen. Sebagai institusi intelijen utama, BIN dituntut untuk menjadi pihak pertama yang beradaptasi dengan dinamika teknologi digital yang terus berevolusi. Oleh karena itu, sinergi antara kompetensi sumber daya manusia, kemampuan teknis, dan penguasaan teknologi digital menjadi faktor kunci untuk menciptakan efektivitas dalam menangkal ancaman intelijen (Humas MENPANRB, 2024).

Di samping itu, BIN juga mendorong inovasi intelijen digital melalui pemanfaatan teknologi seperti pertahanan siber, serangan maya, pemanfaatan open-source intelligence, data science, hingga kecerdasan buatan (AI). Pendekatan multidisiplin tersebut penting untuk memperkuat sistem deteksi dini intelijen nasional. Namun, tantangan di masa depan menuntut langkah lebih jauh, yakni menghadirkan inovasi yang lebih terstruktur, cepat, dan sistematis.

Sejalan dengan pandangan (Djoyonegoro, 2023) dalam *antaranews.com*, ekosistem digital menghadirkan lonjakan besar volume data dalam dunia spionase yang saling terhubung, sekaligus memperlihatkan eskalasi ancaman siber dari pihak-pihak bermusuhan. Kondisi ini menuntut respons adaptif dari intelijen negara melalui inovasi berkelanjutan. Inovasi dipandang bukan sebagai titik akhir, melainkan proses tanpa garis finis; akhir dari satu inovasi selalu menjadi awal bagi inovasi berikutnya. Dengan demikian, kolaborasi dan keterbukaan internal menjadi syarat mutlak bagi badan intelijen dalam menghadapi dinamika ancaman digital yang terus berkembang.

Dengan struktur organisasi yang adaptif dan kolaboratif, serta pengembangan SDM yang kompeten di bidang siber, BIN dapat meningkatkan kemampuannya dalam menghadapi ancaman siber yang berkembang. Langkah-langkah ini sejalan dengan upaya transformasi digital yang tengah digalakkan oleh pemerintah Indonesia untuk meningkatkan keamanan nasional di era digital.

Namun, tantangan ke depan tetap ada, termasuk kebutuhan untuk terus memperbarui teknologi dan metode intelijen sesuai dengan perkembangan ancaman siber. Oleh karena itu, BIN perlu terus berinovasi dan beradaptasi agar tetap relevan dan efektif dalam menjalankan tugasnya melindungi keamanan negara.

KESIMPULAN

Transformasi digital telah mengubah lanskap ancaman keamanan, dengan ancaman siber menjadi tantangan utama bagi intelijen. Tata kelola transformasi digital yang diterapkan oleh Badan Intelijen Negara (BIN) Indonesia untuk meningkatkan ketahanan siber nasional. Ditemukan bahwa bibit tantangan baru, seperti serangan siber yang terus berkembang, memerlukan penyesuaian struktural dalam organisasi intelijen agar lebih responsif dan adaptif. Selain itu, strategi ketahanan siber yang dibangun oleh BIN mencakup penerapan kerangka kerja keamanan siber yang komprehensif, peningkatan kapasitas sumber daya manusia, dan pengembangan kebijakan yang mendukung. Melalui Peraturan Presiden Nomor 73 Tahun

2017, BIN telah merestrukturisasi organisasi dengan fokus pada keamanan siber, berupaya memperkuat pertahanan nasional dalam menghadapi ancaman digital. Penelitian ini menekankan pentingnya kolaborasi antara sektor publik dan masyarakat dalam membangun kesadaran serta literasi digital, sebagai bagian dari upaya kolektif untuk menjaga keamanan siber negara. Dengan demikian, reformasi tata kelola intelijen dan adaptasi strategi ketahanan siber menjadi kunci untuk menghadapi tantangan yang ada di era digital.

DAFTAR PUSTAKA

Agus Tri Haryanto. (2025). *Jumlah Pengguna Internet Indonesia Tembus 212 Juta di 2025*. Inet.Detik.Com. https://inet.detik.com/cyberlife/d-7816040/jumlah-pengguna-internet-indonesia-tembus-212-juta-di-2025

al-amri, F. S. (2024). Transformasi Digital Guna Menangkat Cyber Crime Dalam Rangka Optimalisasi Keamanan Nasional Negara Arab Saudi. In *Kertas Karya Ilmiah Perseorangan (TASKAP), Lembaga Ketahanan Nasional Republik Indonesia*.

Christianingrum, R., Aida, A. N., Riyono, T., & S., R. A. (2021). Budget Issue Brief Politik & Keamanan. In *Pusat Kajian Anggaran Badan Keahlian DPR RI* (Vol. 1, Issue 16).

Faizah and Sashari R. A., A. R. and S. and B. (2023). Resistensi Fixed Mindset Dalam Memengaruhi Kesadaran Masyarakat Terhadap Pendidikan. *Jurnal Riset Guru Indonesia*, *2*(2), 87–94. https://doi.org/10.62388/jrgi.v2i2.305

Gelb A. D., A. and M. (2017). *Identification Revolution: Can Digital ID Be Harnessed for Development?* Center for Global Development.

Handoko, Y., Wijaya, H. A., & L, A. (2024). *Metode Penelitian Kualitatif Panduan Praktis untuk Penelitian Administrasi Pendidikan*. PT. Sonpedia Publishing Indonesia.

Hinings T. and Greenwood R., B. and G. (2018). Digital innovation and transformation: An institutional perspective. *Information and Organization*, *28*(1), 52–61. https://doi.org/10.1016/j.infoandorg.2018.02.004

Kalvet, T. (2012). Innovation: a factor explaining e-government success in Estonia. *Electronic Government, an International Journal*, *9*(2), 142. https://doi.org/10.1504/EG.2012.046266

Kemhan, R. I. (2014). *Kementerian Pertahanan RI PEDOMAN PERTAHANAN SIBER*.

Kitsing, M. (2011). Success Without Strategy: E-Government Development in Estonia. *Policy & Internet*, *3*(1), 1–21. https://doi.org/10.2202/1944-2866.1095

M, E. K. N. (2014a). *Universitas Pertahanan Indonesia*. 1–132.

Muadifah and B. Herawan Hayadi and Furtasan Ali Yusuf and Suheti, A. (2024). Mengatasi Resistensi Terhadap Perubahan Dalam Wawasan, Intervensi Dan Strategi Untuk Adaptasi Organisasi. *Economic and Business Management International Journal*, *4*(1), 169–177.

Nam, T. (2012). Citizens' attitudes toward Open Government and Government 2.0. *International Review of Administrative Sciences*, *78*(2), 346–368. https://doi.org/10.1177/0020852312438783

Priyono A. and Putri V. N. A. O., A. and M. (2020). Identifying Digital Transformation Paths in the Business Model of SMEs during the COVID-19 Pandemic. *Journal of Open Innovation: Technology, Market, and Complexity*, *6*(4), 104. https://doi.org/10.3390/joitmc6040104

Putri, K. V. K. (2021). Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime. *Jurnal Hukum Lex Generalis*, *2*(7), 542–554. https://doi.org/10.56370/jhlg.v2i7.90

Raharjo, A. (2002). *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. Citra Aditya Bakti.

Redaksi Indojpnn.net. (2024). *Peran Teknologi dalam Restrukturisasi Intelijen di Era Digital*. Indojpnn.Net.

Rokhman, A. (2011). E-Government Adoption in Developing Countries; the Case of Indonesia. *Journal of Emerging Trends in Computing and Information Sciences*, *2*(5), 228–236. http://oru.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwXVy7CgIxEAzW2giKpT9wkuzmdfVhsDhBxP7Ia8vDwv_HzYkItlttNQ-YGSEQTrL7wwTjkraQXWJ-1dnoij5p5xRUW3OB1ncer3gb7Bj8ff3Dr7AVqzrvRAjnx3DpWmJsen5mGKY2jLwcvhGySRPmHqLK1hSQRXnmIkl9yeQwaY-4F5vYguPzaymYlYM4IrHDsDW

Senopati. (2024). *Peran Teknologi dalam Restrukturisasi Intelijen di Era Digital*. Prabowocapres.Com. https://prabowocapres.com/2024/08/22/peran-teknologi-dalam-restrukturisasi-intelijen-di-era-digital/

Welch, M. F. and N. K. and D. B. and M. (2014). Embracing Digital Technology: A New Strategic Imperative. *MIT Sloan Management Review*, *55*(2), 2.