SOSMANIORA (Jurnal Ilmu Sosial dan Humaniora)
https://journal.literasisains.id/index.php/sosmaniora
DOI: 10.55123/sosmaniora.v4i3.6424
ISSN 2829-234| p-ISSN 2829-2359
Vol. 4 No. 3 (Agustus 2025) 908-917
Submitted: July 09, 2025 | Accepted: August 25, 2025 | Published: September 10, 2025

Kebijakan Pemerintahan Joko Widodo dalam Menghadapi Ancaman Cyber di Sektor Infrastruktur Energi Indonesia

Baptista Pradevi[1*], Indra Wisnu Wibisono[2], Roberto OC Seba[3]
[1*]Program Studi Hubungan Internasional, Fakultas Ilmu Sosial Dan Ilmu Komunikasi, Universitas Kristen Satya Wacana, Sidorejo, Indonesia
[2,3]Departemen Hubungan Internasional, Fakultas Ilmu Sosial Dan Ilmu Komunikasi, Universitas Kristen Satya Wacana, Sidorejo, Indonesia
Email: [1*]372021018@student.uksw.edu, [2]indra.wibisono@uksw.edu, [3]robert.seba@uksw.edu

Abstrak

Infrastruktur energi merupakan sektor strategis bagi stabilitas ekonomi dan ketahanan nasional Indonesia. Namun, digitalisasi meningkatkan risiko serangan siber seperti malware dan peretasan sistem kontrol industri. Penelitian ini menganalisis efektivitas kebijakan keamanan siber pada era pemerintahan Joko Widodo dengan pendekatan kualitatif melalui studi literatur terhadap regulasi, laporan kelembagaan, dan kajian akademik. Hasil penelitian menunjukkan bahwa pemerintah telah membangun kerangka regulasi dan kelembagaan yang cukup kuat, seperti melalui Peraturan Presiden Nomor 53 Tahun 2017, Peraturan Presiden Nomor 82 Tahun 2022, dan Undang-Undang Nomor 27 Tahun 2022. Selain itu, upaya penguatan dilakukan melalui kerja sama PLN dan BSSN, pembentukan CSIRT, serta peningkatan kualitas SDM melalui pelatihan dan sertifikasi. Meskipun demikian, implementasi kebijakan masih menghadapi tantangan seperti keterbatasan tenaga ahli, kesenjangan standar keamanan, serta kerentanan digital akibat sistem yang belum sepenuhnya terintegrasi. Oleh karena itu, perlu penguatan kapasitas SDM, audit keamanan secara berkala, serta kebijakan yang lebih adaptif terhadap perkembangan teknologi global dan ancaman yang semakin kompleks.

Kata Kunci: Kebijakan Publik, Keamanan Siber, Infrastruktur Energi, Joko Widodo, Ancaman Digital.

Abstract

Energy infrastructure is a strategic sector for Indonesia's economic stability and national resilience. However, digitalization increases the risk of cyberattacks such as malware and the hacking of industrial control systems. This study analyzes the effectiveness of cybersecurity policies during the Joko Widodo administration using a qualitative approach through a literature review of regulations, institutional reports, and academic studies. The results show that the government has established a fairly robust regulatory and institutional framework, including Presidential Regulation No. 53 of 2017, Presidential Regulation No. 82 of 2022, and Law No. 27 of 2022. Furthermore, efforts to strengthen cybersecurity have been made through collaboration between PLN and BSSN, the establishment of CSIRT (Computer Security Incident Response Team), and improvements in human resource quality through training and certification. However, policy implementation still faces challenges such as limited expertise, gaps in security standards, and digital vulnerabilities due to partially integrated systems. Therefore, human resource capacity building, regular security audits, and more adaptive policies in response to global technological developments and increasingly complex threats are needed.

Keywords: *Energy Infrastructure, Cyber Security, Public Policy, Joko Widodo, Digital Threats.*

PENDAHULUAN

Globalisasi telah membawa transformasi digital yang masif dalam berbagai aspek kehidupan, termasuk tata kelola negara. Digitalisasi dalam sektor energi merupakan salah satu bagian dari transformasi digital yang lebih luas yang didorong oleh pemerintah. Terdapat beberapa aspek digitalisasi pada sektor

energi di Indonesia, yaitu smart grid, loT, layanan pelanggan digital, dsbnya. Digitalisasi pada sektor energi memiliki tujuan untuk meningkatkan efisiensi, produktivitas serta keberlanjutan sektor energi dan meningkatkan pelayanan kepada masyarakat. Urgensi digitalisasi energi terdapat pada kontribusi dalam mempercepat menuju transisi energi bersih, meningkatkan efisiensi serta produktivitas sistem kontrol, mengurangi emisi karbon, menekan biaya operasional, serta memperkuat ketahanan dan keamanan energi pada konteks sistem kontrol kelistrikan modern yang semakin kompleks. Penerapan teknologi digital memungkinkan optimasi pemanfaatan sumber daya, mendukung integrasi energi terbarukan secara lebih efektif, serta menyediakan mekanisme pemantauan sistem kontrol yang lebih akurat sehingga potensi pemborosan energi dapat diminimalisasi.

Selain itu, infrastruktur energi meliputi pengembangan dan penerapan energi terbarukan seperti teknologi penyimpanan energi, panel surya dan turbin angin. Ancaman siber menurut Pedoman Pertahanan Siber Kementerian Pertahanan Republik Indonesia (2014) merupakan sebuah entitas yang memiliki keinginan untuk melakukan sesuatu yang melanggar hukum dan norma yang dapat merugikan keamanan informasi, dan sebagainya. Ancaman siber pada sektor energi meliputi berbagai bentuk seperti *malware, ransomware, phishing*, DDoS, APT, dan pencurian data. Infrastruktur energi yang semakin terhubung secara digital menjadi target utama serangan siber, yang jika tidak ditangani dengan baik, dapat mengakibatkan gangguan signifikan pada perekonomian dan kesejahteraan masyarakat (Kemhan, 2014). Salah satu contoh ancaman nyata terjadi pada tahun 2021 ketika serangan ransomware terhadap Colonial Pipeline di Amerika Serikat menyebabkan kelangkaan bahan bakar di wilayah Pantai Timur selama beberapa hari (Gawazah et al., 2024). Kondisi tersebut dapat berdampak pada kenaikan harga barang dan jasa yang dapat menyebabkan inflasi, ketegangan sosial seperti demonstrasi, serta menghambat aktivitas masyarakat. Di Indonesia sendiri pada tahun 2020, ketika pertamina memiliki kerugian besar dikarenakan kondisi pasar global dan memiliki resiko terkenanya serangan *malware* dan *phising* (CNN, 2020). Selain itu tahun 2021, terjadi serangan serius bagi industri migas, yaitu serangan siber oleh *Advanced Persistent Threat* (APT). Serangan tersebut dapat menargetkan aset maupun infrastruktur vital, seperti Operasional Teknologi (OT) yang mengatur proses industri. Dengan ransomware yang menjadi salah satu ancaman utama sehingga hal tersebut dapat menjadi ancaman utama yang dapat mengganggu operasional ekonomi serta terjadinya peningkatan ancaman siber pada industri migas. Serangan-serangan yang terjadi ini tidak hanya berdampak pada operasional tetapi juga mengancam keamanan tenaga kerja dan infrastruktur vital. Dampak serangan tersebut menunjukkan bagaimana infrastruktur energi yang terhubung secara digital menjadi sangat rentan terhadap gangguan eksternal.

Di Indonesia, sektor energi yang terus berkembang dengan berbagai proyek kelistrikan dan pembangkit berbasis teknologi tinggi juga menjadi target potensial bagi ancaman siber. Lemahnya sistem kontrol keamanan siber di berbagai perusahaan energi dapat dimanfaatkan oleh peretas untuk mengakses dan mengontrol sistem vital, yang berpotensi mengganggu distribusi listrik atau operasional fasilitas energi. Pentingnya sektor energi bagi Indonesia tidak hanya sebatas penyediaan listrik bagi masyarakat, tetapi juga sebagai tulang punggung pertumbuhan ekonomi nasional. Sebagai negara berkembang dengan populasi lebih dari 284 juta jiwa (Saptoyo & Galih, 2025), kebutuhan energi Indonesia terus meningkat seiring dengan urbanisasi dan industrialisasi yang pesat.

Sektor energi juga menjadi sumber pendapatan negara yang signifikan melalui ekspor minyak, gas, dan batu bara. Ketergantungan ekonomi Indonesia pada sektor energi membuatnya menjadi salah satu sektor yang paling strategis dan harus dijaga keamanannya dari berbagai ancaman, termasuk ancaman siber. Jika terjadi serangan siber terhadap infrastruktur energi, dampaknya bisa sangat luas, mulai dari gangguan produksi industri hingga potensi krisis energi yang mempengaruhi kesejahteraan masyarakat. Kejadian pemadaman listrik massal di Jawa dan Bali pada tahun 2019 akibat gangguan teknis memberikan gambaran tentang bagaimana gangguan pada infrastruktur energi dapat menghambat aktivitas ekonomi, bisnis, dan kehidupan sehari-hari (Sumiyati et al., 2024). Ancaman siber yang lebih canggih berpotensi menyebabkan gangguan yang lebih besar, sehingga perlindungan terhadap sektor energi menjadi semakin mendesak.

Indonesia masih menghadapi berbagai tantangan dalam memperkuat keamanan siber di sektor energi. Salah satu tantangan terbesar adalah kurangnya kesadaran dan pemahaman terhadap ancaman siber, baik di tingkat pemerintah, perusahaan, maupun masyarakat umum. Tanpa adanya strategi yang komprehensif dan investasi yang memadai, sektor energi Indonesia akan tetap menjadi sasaran empuk bagi peretas ingin mengganggu stabilitas nasional. Terdapat beberapa laporan dari lembaga internasional seperti *International Energy Agency* (IEA) dan *World Economic Forum* (WEF) juga telah membahas risiko siber di sektor energi dan bagaimana negara-negara dapat meningkatkan pertahanan mereka. Hal ini menunjukkan bahwa Indonesia menjadi salah satu negara yang perlu mengadopsi praktik terbaik dari negara lain untuk memperkuat keamanan siber di sektor energinya. Meskipun berbagai penelitian telah membahas ancaman siber di sektor energi, masih terdapat kesenjangan dalam kajian yang secara spesifik menyoroti kebijakan

pemerintahan Joko Widodo dalam menghadapi ancaman ini. Banyak penelitian sebelumnya berfokus pada aspek teknis serangan siber atau tantangan umum dalam keamanan infrastruktur energi, tetapi belum banyak yang membahas bagaimana kebijakan pemerintah Indonesia diimplementasikan dalam konteks ancaman siber yang semakin kompleks (Wicaksono & Yasin, 2024). Selain itu, sebagian besar studi yang ada lebih menyoroti praktik global atau pendekatan di negara maju (Saeed et al., 2023), sementara kondisi Indonesia dengan karakteristik regulasi, teknologi, dan sumber daya manusia yang berbeda masih belum banyak dikaji secara mendalam. Faktor geopolitik dan ekonomi juga mempengaruhi dinamika ancaman siber di Indonesia, tetapi masih minim penelitian yang menganalisis hubungan antara kebijakan nasional dengan tantangan keamanan siber di sektor energi.

Kesenjangan lainnya terletak pada evaluasi efektivitas kebijakan yang telah diterapkan, karena belum ada kajian komprehensif yang membandingkan regulasi yang ada dengan implementasi nyata di lapangan. Urgensi penelitian ini semakin tinggi mengingat infrastruktur energi merupakan sektor yang sangat vital bagi ketahanan nasional, dan serangan siber dapat berdampak luas terhadap ekonomi, industri, dan kehidupan masyarakat. Indonesia yang tengah gencar melakukan transformasi digital di berbagai sektor harus memastikan bahwa keamanan siber menjadi prioritas utama dalam pembangunan infrastruktur energi. Sehingga, dengan meningkatnya jumlah serangan siber terhadap sektor energi di berbagai negara, Indonesia juga berisiko menghadapi ancaman serupa, terutama karena banyak perusahaan energi masih memiliki sistem kontrol keamanan yang lemah. Serangan terhadap jaringan energi dapat menyebabkan pemadaman listrik, gangguan distribusi bahan bakar, hingga sabotase sistem kontrol industri, yang dapat berujung pada instabilitas ekonomi dan sosial (Knapp, 2024). Pemerintah telah mengeluarkan berbagai kebijakan terkait keamanan siber, tetapi efektivitasnya masih perlu dievaluasi untuk memastikan bahwa regulasi tersebut benar-benar mampu menghadapi ancaman yang terus berkembang. Selain itu, ancaman siber tidak hanya datang dari individu atau kelompok kriminal, tetapi juga dari aktor negara yang memiliki kepentingan geopolitik, sehingga keamanan siber harus menjadi bagian dari strategi pertahanan nasional (Abdelkader et al., 2024).

METODE

Dalam penelitian ini menggunakan metodologi penelitian kualitatif dengan metode analisis. Menurut bakry 2016, metode analisis isi adalah salah satu teknik dalam penelitian kualitatif yang berfungsi untuk menganalisis dan mengkategorikan data. Tujuan dari metode ini adalah untuk menemukan pola, kolaborasi, serta efek suatu kebijakan. Maka dengan itu pengumpulan data ini dilakukan dengan melalui studi pustaka dan wawancara bersama para ahli di bidang cyber pada infrastruktur energi yang ada di Indonesia. Studi pustaka dilakukan dengan mempelajari dan memahami literatur terkait kebijakan-kebijakan siber pada masa pemerintahan Joko Widodo serta dokumen maupun artikel resmi dari pemerintah. Wawancara dengan para ahli dilakukan untuk mengetahui dan memahami. Selain itu, penelitian ini akan dibatasi dengan menjelaskan sejauh mana regulasi yang ada mampu melindungi sektor energi dari ancaman semakin kompleks.

Metode analisis data pada penelitian ini merupakan analisis isi (content analysis), yaitu menganalisis dan mengklasifikasikan data untuk mengidentifikasikan pola, kerjasama maupun hasil dari suatu kebijakan (Bakry, 2016). Validitas data dijaga dengan melalui triangulasi sumber sehingga dapat menjamin keakuratan dan konsistensi informasi yang diperoleh pada penelitian ini. Menurut Sugiyono 2026, pendekatan deskriptif dalam penelitian kualitatif merupakan suatu metode analisis yang bertujuan untuk menyajikan dan menggambarkan secara sistematis, faktual, serta tepat mengenai fakta-fakta, karakteristik, dan interaksi antara fenomena yang sedang diteliti. Penelitian ini menggunakan sumber sekunder, yaitu data yang dikumpulkan dari berbagai dokumen, berbagai literatur, artikel jurnal, jurnal, buku, serta sumber data website dan berita. Menurut Sugiyono (2016), data sekunder adalah informasi yang diperoleh oleh peneliti secara tidak langsung, melalui perantara seperti orang lain atau dokumen yang sudah ada sebelumnya.

HASIL DAN PEMBAHASAN

Pemerintah telah mengeluarkan regulasi seperti Perpres No. 53/2017, Perpres No. 82/2022, dan UU No. 27/2022, tantangan berupa keterbatasan SDM dan ketidakmerataan standar keamanan masih muncul akibat faktor struktural. Kebutuhan tenaga ahli di bidang keamanan siber industri (OT/ICS) tumbuh lebih cepat dibanding kapasitas pendidikan dan pelatihan nasional, sementara insentif karier di sektor publik kalah bersaing dengan swasta sehingga terjadi brain drain. Mekanisme rekrutmen birokratis dan distribusi talenta yang terkonsentrasi di kota besar juga membuat operator energi di daerah kekurangan tenaga profesional. Di sisi lain, standar keamanan seringkali tidak merata karena banyak infrastruktur energi masih

bergantung pada sistem kontrol industri lama yang sulit diintegrasikan dengan standar modern, serta kurangnya aturan teknis turunan dan mekanisme audit yang konsisten.

Hambatan ini diperparah oleh faktor birokrasi, alokasi anggaran, dan budaya organisasi. Fragmentasi kewenangan antar-kementerian dan lembaga memperlambat koordinasi, sementara anggaran keamanan siber seringkali tidak teralokasi secara khusus sehingga bergantung pada prioritas sisa. Dari sisi budaya, banyak organisasi energi masih lebih mengutamakan kontinuitas operasional dan efisiensi biaya daripada investasi proaktif di bidang keamanan. Kolaborasi PLN–BSSN dan pembentukan CSIRT memang menjadi langkah positif, namun sifatnya masih parsial dan belum merata ke semua entitas energi. Dengan demikian, efektivitas kebijakan hanya bisa tercapai jika diperkuat dengan insentif anggaran, roadmap pengembangan SDM, harmonisasi standar teknis, serta perubahan budaya organisasi agar keamanan siber benar-benar terintegrasi dalam manajemen infrastruktur energi.

Dinamika Ancaman Siber di Indonesia

Ancaman siber merupakan segala bentuk potensi yang dapat mengganggu, merusak, mencuri, maupun menyalahgunakan sistem kontrol informasi digital, data digital ataupun jaringan komputer (Kemenkes, 2025). Ancaman siber dapat menimbulkan dampak yang cukup signifikan seperti pencurian data pribadi atau lembaga yang dapat disalahgunakan, gangguan operasional yang dapat melumpuhkan layanan penting pemerintah maupun perusahaan swasta, kerugian secara ekonomi dapat ditimbulkan akibat pencurian uang maupun data keuangan, serta rusaknya reputasi dan psikologis dapat berdampak juga bagi korban akibat ancaman, siber yang terjadi. Situasi ini semakin meresahkan karena Indonesia dipandang rentan terhadap serangan siber akibat keterbatasan sumber daya manusia yang ahli serta rendahnya kesadaran masyarakat dan lembaga pemerintah maupun swasta dalam menjaga keamanan digital. Kelemahan tersebut diperburuk oleh sedikit dan lemahnya investasi dan tata kelola, tidak adanya pembaruan perangkat elektronik di tengah tingginya serangan, penggunaan aplikasi tanpa proteksi yang memadai, serta buruknya pengelolaan akun digital semakin memperbesar celah kejahatan siber di Indonesia (Salwa, 2024).

Ancaman siber di Indonesia semakin kompleks dan mengancam berbagai aspek kehidupan nasional. Pasca transformasi digital, sektor publik dan privat sangat bergantung pada teknologi informasi dan komunikasi (TIK). Namun, hal ini pada akhirnya menjadi membuat Indonesia rentan terhadap berbagai jenis serangan siber, seperti pencurian data, spionase, kontrol informasi, sabotase sistem kontrol, dan ransomware. Badan Siber dan Sandi Negara (BSSN) mencatat bahwa tren global, termasuk pada Indonesia, menunjukkan meningkatnya kontrol informasi, pencurian data, dan sabotase, terutama di sektor publik seperti PT PLN (Persero) yang kini masuk ke dalam infrastruktur informasi vital (IIV) negara. Insiden signifikan seperti kebocoran data eHAC pada Juli 2021 sebanyak 1,3 juta pengguna menjadi contoh konkret gangguan IIV pemerintah (Gian Ayu, 2022).

Studi dari Fourtrezz menyebut Indonesia peringkat ke-4 di ASEAN dalam jumlah kebocoran situs akibat ransomware, dan peringkat ke-49 dari 176 negara berdasarkan National Cyber Security Index (63,64/100) (CSIRT Indonesia, n.d.). Selain itu, masih banyak lembaga dan perusahaan yang belum memiliki Computer Security Incident Response Team (CSIRT) internal. Kurangnya sumber daya manusia yang kompeten di bidang keamanan siber juga memperlambat proses mitigasi dan penanganan insiden. Sektor energi (ESDM), mencakup pembangkitan, transmisi, distribusi, gas, migas, dan energi terbarukan, adalah tulang punggung PNBP dan infrastruktur vital nasional. Pada tahun 2017 Kementerian ESDM berkontribusi terhadap sebesar Rp 129,07 triliun atau sekitar 44% dari PNBP nasional (ESDM, 2018). Pada tahun 2018 Kementerian ESDM berkontribusi terhadap sebesar Rp 120,5 triliun atau sekitar 49,6% dari PNBP nasional (ESDM, 2018). Pada tahun 2024 Kementerian ESDM berkontribusi terhadap sebesar Rp 36,81 triliun atau sekitar 33,42% dari PNBP nasional (ESDM, 2024). Dengan besarnya ketergantungan pada sistem kontrol digital, serangan yang terjadi pada Industrial Control System (ICS) atau Operational Technology (OT) pada sektor energi dapat menyebabkan potensi blackout, kegagalan distribusi listrik, pelanggaran data pelanggan serta melemahkan kedaulatan negara (Kementerian Pertahanan Republik Indonesia, 2014). Pada aspek ini, aktor-aktor yang terlibat seperti BSSN sebagai koordinator nasional keamanan IIV dan pendamping pembentukan CSIRT sektoral di ESDM, ESDM CSIRT sebagai unit internal Kementerian ESDM yang memiliki fungsi preventive, responsive, helpdesk, dan sosialisasi keamanan siber (Kementerian ESDM RI, 2021), PLN yang menjalin MoU dengan BSSN sejak 2019/2022 untuk menguatkan kapabilitas intelijen siber dan SOC (PT PLN (Persero), 2022), serta adanya dukungan dari mitra teknologi dan korporasi dalam membangun kewaspadaan siber dan solusi canggih di sektor energi. Dengan demikian, peningkatan kapasitas SDM dan literasi siber nasional menjadi agenda mewujudkan ketahanan siber Indonesia. Ransomware & kebocoran data.

Kebijakan Pemerintahan Joko Widodo dalam Menghadapi Ancaman Siber pada Infrastruktur Energi

Sektor energi menjadi infrastruktur vital yang menjadi tombak perekonomian nasional dimana gangguan siber pada sektor tersebut dapat berdampak langsung pada layanan publik, stabilitas ekonomi, hingga pertahanan negara. Pada akhirnya, ancaman serangan siber menjadi semakin nyata dengan kasus peretasan terbesar pada tahun 2023 tercatat lebih dari 361 juta kasus terjadi dari peretasan siber yang diserang berbagai sektor kritis di Indonesia, termasuk energi. Pemerintah telah membentuk BSSN, melewat Peraturan Presiden No. 53 Tahun 2017, sebagai lembaga nasional yang bertanggung jawab atas keamanan siber, termasuk pada sektor energi. Selain itu, bersama BSSN, Kementerian ESDM sejak 2022 memang telah menyusun Cybersecurity Guideline for National Energy Infrastructure untuk menguatkan standar keamanan infrastruktur energi nasional. Melalui pernyataan ini, fakta tersebut menunjukkan bahwa urgensi penanganan serangan siber di sektor energi membutuhkan lebih kuatnya kebijakan, koordinasi, dan implementasi agar infrastruktur vital tetap terlindungi secara menyeluruh. Pemerintahan Joko Widodo telah menunjukkan komitmen dalam menangani ancaman siber melalui berbagai regulasi (Kementerian Pertahanan Republik Indonesia, 2017).

Beberapa regulasi telah diterbitkan, Peraturan Presiden No. 82 Tahun 2015 tentang SPBE, mendorong digitalisasi tata kelola pemerintahan (Badan Pembinaan Hukum Nasional, 2023) yang berarti transformasi digital melalui SPBE dapat meningkatkan ketergantungan pemerintah pada teknologi informasi dan komunikasi; Peraturan Presiden No. 53 Tahun 2017 tentang BSSN sebagai lembaga teknis nasional bidang keamanan siber (Kementerian Pertahanan Republik Indonesia, 2017), hal tersebut menjelaskan bahwa BSSN menjadi pilar kelembagaan bagi Indonesia dalam membangun kekuatan untuk berkoordinasi, mitigasi, serta penanggulangan ancaman siber nasional; Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) sebagai dasar hukum bagi keamanan data, standar operasional dan kewajiban dalam melindungi sistem elektronik nasional; Strategi Keamanan Siber Nasional (SKSN) oleh BSSN menjadi standar utama nasional dalam mencegah, mendeteksi serta merespon ancaman siber; Rencana Aksi Nasional Keamanan Informasi dan Siber (RAN KITS) memberikan arahan kebijakan agar keamanan siber dapat berjalan sistematis dan terintegrasi di berbagai sektor; dan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menjadi tonggak hukum utama bagi keamanan informasi digital, melindungi privasi masyarakat serta memperkuat data nasional. Dengan keenam kebijakan tersebut membentuk kerangka regulasi yang menyeluruh dalam pengelolaan keamanan siber, khususnya terhadap infrastruktur strategis seperti energi.

Namun, efektivitas implementasi kebijakan ini masih menghadapi sejumlah tantangan. Pertama, dari segi koordinasi, terjadi tumpang tindih fungsi antara lembaga-lembaga pemerintah pusat dan daerah serta antar instansi teknis. Dalam laporan BPK tahun 2023 terkait evaluasi SPBE, disebutkan bahwa belum semua kementerian/lembaga menerapkan standar interoperabilitas sistem kontrol digital nasional, termasuk dalam bidang energi (Badan Pembinaan Hukum Nasional, 2023). Ketidaksinkronan ini menyebabkan respon terhadap ancaman siber tidak dapat dilakukan secara cepat dan terkoordinasi. Kedua, dari aspek kelembagaan, meskipun BSSN telah berfungsi sebagai pusat komando keamanan siber nasional, kapasitas sumber daya manusia dan teknologi yang dimiliki masih terbatas. Berdasarkan Rencana Pembangunan Jangka Menengah Nasional (RPJMN) 2020–2024, penguatan SDM keamanan siber masih menjadi prioritas karena kurangnya ahli yang mampu menangani ancaman tingkat tinggi seperti ransomware atau APT (Bappenas, 2019). Ketiga, pada aspek teknis, PP Nomor 71 Tahun 2019 menetapkan standar keamanan sistem elektronik, tetapi belum semua perusahaan energi, terutama yang berstatus BUMN dan anak perusahaannya, memenuhi standar ini. Banyak diantaranya masih menggunakan sistem kontrol yang rentan dan belum memiliki cadangan data yang memadai atau prosedur pemulihan insiden (incident response protocol) yang cepat. Keempat, berdasarkan pengamatan dari Kementerian Komunikasi dan Informatika (Kominfo), terdapat peningkatan signifikan dalam jumlah serangan siber ke sektor energi sejak 2018, tetapi belum ada laporan publik resmi yang terintegrasi terkait mitigasi ancaman terhadap sektor ini (Lemhannas, 2020).

Hal ini memperlihatkan bahwa sistem pelaporan dan evaluasi keamanan belum sepenuhnya transparan. Namun, di sisi positif, terdapat sejumlah inisiatif yang dapat dianggap sebagai langkah maju dalam upaya mitigasi ancaman siber di sektor energi. Awalnya, BSSN telah melakukan cyber drill nasional setiap tahun sejak 2019 yang melibatkan sektor energi sebagai salah satu peserta utama. Tujuannya adalah meningkatkan kesiapsiagaan terhadap serangan simulatif seperti DDoS dan ransomware. Selanjutnya, Kementerian Energi dan Sumber Daya Mineral (ESDM) bekerja sama dengan BSSN untuk menyusun Cybersecurity Guideline for National Energy Infrastructure sejak 2022 (Kementerian Energi dan Sumber Daya Mineral, 2021). Panduan ini mengatur standarisasi sistem keamanan dan prosedur audit keamanan sistem energi. Selain itu, melalui Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan

Berbasis Elektronik, sektor energi juga didorong untuk mengintegrasikan keamanan data dan sistem digital ke dalam tata kelola perusahaan, termasuk melalui manajemen risiko dan audit TI internal (Badan Pembinaan Hukum Nasional, 2018). Evaluasi efektivitas juga dapat dilihat dari insiden serangan yang berhasil diminimalisasi. Dalam laporan tahunan BSSN 2022, disebutkan bahwa meskipun terjadi 300 juta anomali trafik siber di Indonesia, 70% potensi serangan terhadap infrastruktur energi berhasil dicegah berkat sistem kontrol pemantauan aktif dan kerja sama dengan pemilik sistem (Badan Siber dan Sandi Negara, 2023). Namun demikian, tantangan tetap ada. Serangan siber pada server Pertamina tahun 2022 yang diklaim melibatkan kelompok RansomEXX tetap berhasil menembus sistem, menunjukkan bahwa celah masih terbuka.

Menurut analisis sementara BSSN, penyebab utama adalah lemahnya autentikasi dua faktor dan keterlambatan dalam patch management. Dari sisi kebijakan publik, penguatan efektivitas tidak hanya bergantung pada regulasi, tetapi juga pada kesadaran dan kepatuhan industri. Perlu mekanisme compliance enforcement yang kuat agar perusahaan-perusahaan energi, terutama swasta dan anak usaha BUMN, benar-benar menerapkan sistem kontrol pertahanan siber yang sesuai standar nasional dan internasional. Di sinilah pentingnya evaluasi berkala dan penegakan hukum. UU PDP, misalnya, menetapkan sanksi administratif dan pidana atas kelalaian perlindungan data, tetapi implementasinya masih terbatas. Menurut PP No. 71 Tahun 2019, Penyelenggara sistem kontrol Elektronik harus memiliki manajemen risiko siber, tetapi audit publik secara berkala belum dilakukan secara luas (Badan Siber dan Sandi Negara, 2023; Badan Pembinaan Hukum Nasional, 2019). Secara keseluruhan, kebijakan era Joko Widodo telah membentuk fondasi yang kokoh dalam menghadapi ancaman siber di sektor energi, tetapi efektivitasnya masih menghadapi hambatan struktural dan operasional. Dibutuhkan penguatan dalam tiga hal utama: kapasitas teknologi dan SDM, konsolidasi kebijakan, dan evaluasi dan penegakan hukum.

Cyber Security sebagai bagian National Security pada infrastruktur energi dalam Era Pemerintah Joko Widodo

Menurut Pedoman Pertahanan siber Kementerian Pertahanan Republik Indonesia (2014), keamanan siber nasional merupakan sebuah upaya dalam menjaga infrastruktur dan informasi nasional tetap aman (Kementerian Pertahanan Republik Indonesia, 2014). Dalam keamanan nasional, cyber security merupakan suatu bagian yang penting dikarenakan perkembangan teknologi digital yang menjadikan cyberspace sebagai sektor baru selain luar angkasa, laut, darat, dan udara. Cyberspace adalah ruang yang dimana kelompok saling terhubung dengan menggunakan jaringan untuk kegiatan sehari-hari (Kementerian Pertahanan Republik Indonesia, 2014). Dikarenakan ancaman pada cyberspace dapat berdampak langsung pada stabilitas nasional, seperti mengganggu keamanan dan pertahanan nasional, merusak perekonomian nasional, melumpuhkan infrastruktur energi, serta menimbulkan ketidakstabilan sosial-politik. Oleh karena itu, banyak negara memposisikan cyber security sebagai bagian penting dalam strategi keamanan nasional. Indonesia pada era pemerintahan Joko Widodo melihat bahwa bahaya serangan cyber yang terdapat pada sektor energi merupakan hal yang utama dan strategis bagi keamanan sebuah negara. Masalah cyber tidak bisa dianggap sebagai sebuah masalah yang ringan, melainkan harus dianggap sebagai masalah yang serius sehingga dapat mengancam stabilitas, keamanan dan kedaulatan Indonesia. Melalui berbagai kebijakan pemerintah telah memasukan unsur digital dalam sektor keamanan untuk memperkuat pertahanan bangsa. Hal ini dapat terlihat melalui Peraturan Presiden Nomor 47 tahun 2023 mengenai strategi keamanan siber nasional dan manajemen krisis siber. Infrastruktur energi menjadi aspek penting bagi berbagai infrastruktur lainnya. Melalui penggabungan antara pendekatan digital dan pertahanan nasional, kebijakan pemerintah diperkuat serta pembentukan Badan Siber dan Sandi Negara (BSSN). BBSN bertugas sebagai koordinator seluruh sektor yang berkaitan dengan cyber security.

Kendala yang terjadi pada sektor energi dapat menimbulkan pemadaman listrik dan penyaluran bahan bakar yang dapat menyebabkan konflik sosial serta ketidakstabilan politik. Maka dari itu, perlindungan siber pada infrastruktur energi menjadi perhatian utama nasional yang harus dilindungi dengan peraturan dan memperkuat sistem keamanan. Pemerintah menjadikan cyber security sebagai landasan utama dalam menjaga stabilitas sektor energi nasional. Permasalahan yang terjadi pada PT Pertamina pada tahun 2020 dan Industri Migas pada tahun 2021 merupakan rentannya sektor energi terhadap ancaman digital. Permasalahan tersebut mengakibatkan kendala pada operasional yang signifikan serta mengancam pasokan energi nasional, sehingga berdampak langsung pada stabilitas ekonomi dan keamanan nasional. Hal tersebut menjelaskan pentingnya memperkuat sistem kontrol energi nasional dengan menggunakan pendekatan cyber yang komprehensif, baik dari teknologi maupun peraturan. Pemerintah menanggapi dengan meningkatkan kapasitas keamanan siber melalui edukasi, pelatihan, dan peningkatan pengetahuan bagi pihak terkait di sektor energi dan sumber daya alam (Diskominfo, 2022). Tindakan tersebut menunjukan bahwa pemerintah serius dalam menjaga keamanan sistem kontrol energi nasional dari ancaman cyber. Pemerintah juga memperkuat keamanan cyber dengan mengeluarkan Perpres No. 82 Tahun

2022 tentang Perlindungan Infrastruktur Informasi Vital yang mencakup sektor energi. Aturan tersebut menyatakan bahwa pentingnya sistem kontrol keamanan yang berlapis untuk infrastruktur energi yang menjadi infrastruktur vital nasional. BSSN memiliki peran yang penting untuk mengawasi peraturan pelaksanaan peraturan tersebut dan memastikan persiapan sektor energi dalam menghadapi ancaman siber yang terus berkembang (Komdigi, 2020). Selain itu melalui Peraturan Presiden Nomor 47 tahun 2023, pemerintah mengalokasikan anggaran dari APBN dan APBD untuk mendukung pelaksanaan strategi keamanan siber nasional. Anggaran tersebut penting bagi berkelanjutan perlindungan dan peningkatan kapasitas keamanan cyber pada sektor energi.

Tantangan dalam Implementasi Keamanan Siber di Sektor Energi

Implementasi keamanan siber terutama pada sektor energi harus menghadapi tantangan yang semakin kompleks dengan berkembangnya transformasi digital. Dalam konteks nasional, tantangan tersebut semakin relevan terkhususnya bagi PLN yang sebagai penyalur utama energi listrik di Indonesia. Pada tahun 2023 PLN telah melakukan pemerataan energi nasional. Digitalisasi telah diterapkan secara menyeluruh dari sektor pembangkit, transmisi, distribusi dan pelayanan banyak didukung dengan proses berbasis digital (PLN, 2023). Pada setiap aspek digitalisasi akan menjadi potensi bagi kejahatan siber diperkuat dengan peningkatan efisiensi dan kualitas layanan sehingga memperluas juga serangan siber yang harus dicegah. Maka dengan itu, peningkatan sistem keamanan siber menjadi kebutuhan yang mendesak bagi PLN. Kerjasama yang terjadi antara PLN dengan Badan Siber dan Sandi Negara (BSSN) menjadi landasan penting dalam stabilitas keamanan siber nasional. Kerjasama yang terjadi bukan hanya untuk pengembangan infrastruktur digital, melainkan meningkatkan kualitas SDM serta pembentukan Computer Security Incident Response Team (CSIRT) pada lingkungan PLN. Pada tahun 2022, kepala BSSN saat itu Hinsa Siburian menyampaikan bahwa PLN yang sebelumnya merupakan bagian dari Objek Vital Nasional sudah menjadi infrastruktur informasi vital nasional (PLN, 2022). Maka dengan itu, PLN perlu menerapkan perlindungan siber yang lebih tinggi.

Pada Agustus 2022, terjadi dugaan kebocoran data pelanggan PLN yang melibatkan ±17 juta akun pelanggan. Pemerintah melalui Kementerian Komunikasi dan Informatika memanggil manajemen PLN untuk dimintai keterangan dan mengevaluasi sistem keamanan data pelanggan.

Pembelajaran dari kasus ini:

1. Kurangnya prosedur internal dan kontrol teknis (access control, monitoring/log audit, proteksi enkripsi/backup yang memadai) memungkinkan data pelanggan bisa terekspos.
2. Karena keterbatasan SDM yang memahami aspek keamanan data dan regulasi perlindungan data, respons awal terhadap kebocoran kurang cepat dan sistematis.
3. Standar keamanan di unit-unit PLN yang berbeda tidak selalu sama — unit pusat mungkin punya sistem lebih baik, sedangkan unit cabang atau lokal mungkin masih menggunakan sistem lama atau tidak memiliki pelatihan keamanan yang memadai(Finansialku, 2022)

Hal tersebut sangat penting karena sektor energi merupakan salah satu yang akan berdampak pada stabilitas nasional jika terjadi serangan. Menurut Hinsa Siburian ancaman siber yang dihadapi PLN akan semakin beragam yaitu, kontrol informasi, spionase pencurian data serta sabotase (PLN, 2022). Dengan adanya digitalisasi layanan sehingga perlu membuat PLN mengelola data pengguna dalam skala besar, sehingga hal tersebut beresiko tinggi terjadinya kebocoran data dan penyalahgunaan informasi. Adanya tantangan tersendiri bagi penyelarasan perlindungan siber pada lapisan-lapisan infrastruktur yaitu, terdapat berbagai generasi teknologi di lapangan dalam penggunaan perangkat dan sistem yang ada. Jika terdapat serangan siber yang diarahkan kepada sistem kontrol industri maka hal tersebut dapat mengganggu persediaan listrik serta mengancam pertahanan energi nasional. Maka dari itu, PLN perlu mengembangkan teknologi keamanan serta audit secara berkala terhadap sistem digitalnya. Dengan adanya Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital sehingga hal tersebut menjadi tantangan tersendiri bagi PLN dikarenakan perlu menyesuaikan terhadap regulasi yang ada.

Regulasi tersebut mengharuskan PLN secara rutin memperbaharui kebijakan dan prosedur perlindungan siber. Langkah tersebut menuntut adanya koordinasi lintas divisi, pendanaan terhadap teknologi yang lebih modern serta peningkatan SDM karyawan PLN. Selain itu, PLN perlu memastikan bahwa seluruh badan usaha menerapkan standar keamanan yang sama. Jika terjadi kegagalan dalam penerapan ketentuan yang ada, hal tersebut dapat berdampak pada kepercayaan masyarakat dan sanksi dari pemerintah. Peningkatan kualitas SDM menjadi salah satu fokus utama dalam mempersiapkan keamanan siber di PLN. Tetapi dalam memastikan seluruh pekerja memiliki pengetahuan dan kapabilitas untuk mengidentifikasi dan merespon berbagai ancaman siber masih menjadi sebuah tantangan. Dengan bertambahnya ancaman yang bervariasi, pelatihan yang bersertifikasi menjadi hal yang wajib dilakukan. Dalam melindungi infrastruktur energi

nasional, tanpa adanya tenaga ahli yang memadai, investasi pada teknologi keamanan tidak dapat dipergunakan secara optimal.

KESIMPULAN

Berdasarkan penjelasan yang telah disampaikan, dapat disimpulkan bahwa ancaman siber semakin kompleks dan memiliki potensi merugikan dalam berbagai sektor nasional, terkhususnya pada sektor energi nasional yang merupakan infrastruktur vital negara. Ancaman siber di sektor energi Indonesia semakin kompleks dan berisiko tinggi, sehingga meskipun pemerintahan Joko Widodo telah membentuk BSSN, menerbitkan regulasi seperti Perpres No. 53/2017, Perpres No. 82/2022, serta UU No. 27/2022, dan memperkuat kolaborasi PLN–BSSN melalui pembentukan CSIRT, implementasi kebijakan masih terhambat oleh keterbatasan SDM, ketidakmerataan standar keamanan, serta lemahnya koordinasi dan pengawasan. Untuk memperkuat efektivitas kebijakan, diperlukan langkah konkret berupa program pelatihan bersertifikasi wajib bagi seluruh teknisi OT di perusahaan energi, audit eksternal berkala oleh BSSN minimal sekali setahun, alokasi anggaran khusus keamanan siber, pembentukan regional CSIRT/academy untuk meratakan kapasitas SDM, serta integrasi indikator keamanan siber dalam KPI manajemen PLN dan operator energi lainnya. Dengan rekomendasi tersebut, kebijakan yang ada dapat berfungsi tidak hanya sebagai fondasi normatif, tetapi juga instrumen praktis dalam meningkatkan ketangguhan infrastruktur energi Indonesia menghadapi ancaman siber yang semakin kompleks. Pemerintah telah meletakkan fondasi regulasi dan kelembagaan yang kokoh, masih diperlukan upaya lanjutan berupa penguatan kapasitas SDM, audit keamanan yang berkelanjutan, serta pengembangan kebijakan yang adaptif agar sektor energi Indonesia lebih tangguh dalam menghadapi ancaman siber yang semakin kompleks.

DAFTAR PUSTAKA

Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D. E. A., ... & Prokop, L. (2024). Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. Results in Engineering, 21, 102647.

Ali, J. Y. S. T. Y., & Idris, A. M. (2022). Analisis potensi ancaman asimetris berdasarkan kerentanan keamanan siber sektor industri energi baru terbarukan (EBT). Jurnal Kewarganegaraan, 6(2).

Aribowo, D., Damayanti, J., Sadewa, M., Nabila, S. R., & Sarnata, S. (2024). Risiko keamanan dan kerentanan jaringan transmisi listrik terhadap serangan siber pada infrastruktur energi terdistribusi. Jurnal Surya Teknika, 11(2), 710-716.

Ashari, K. (2020). Kamus Hubungan Internasional dan Diplomasi. Jakarta: PT Gramedia Pustaka Utama.

Badan Pembinaan Hukum. (2017). Peraturan Presiden (PERPRES) Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara. https://peraturan.bpk.go.id/Details/72920/perpres-no-53-tahun-2017

Badan Pembinaan Hukum. (2018). Peraturan Presiden (PERPRES) Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. https://peraturan.bpk.go.id/Details/96913/perpres-no-95-tahun-2018

Badan Pembinaan Hukum. (2019). Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019

Badan Pembinaan Hukum. (2022). Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Badan Pembinaan Hukum. (2023a). Peraturan Presiden (PERPRES) Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional. https://peraturan.bpk.go.id/Details/273981/perpres-no-82-tahun-2023

Badan Pembinaan Hukum. (2023b). Peraturan Menteri Sekretaris Negara Republik Indonesia Nomor 3 Tahun 2023 tentang Penerapan Sistem Pemerintahan Berbasis Elektronik Kementerian Sekretariat Negara. https://peraturan.bpk.go.id/Details/262146/permensesneg-no-3-tahun-2023

Badan Siber dan Sandi Negara. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) dalam menghadapi ancaman siber di Indonesia. http://download.garuda.kemdikbud.go.id/article.php?article=2425657&val=23177&titl e=Strategi%20Badan%20Siber%20dan%20Sandi%20Negara%20BSSN%20Dalam%2 0Menghadapi%20Ancaman%20Siber%20di%20Indonesia

Badan Siber dan Sandi Negara. (2023). BSSN: Serangan siber di tahun 2022 alami penurunan dibanding 2021. https://csirt.or.id/berita/bssn-paparkan-serangan-siber-alami-penurunan

Bappenas. (2019). Narasi RPJMN IV 2020–2024 (Revisi 14 Agustus 2019). https://perpustakaan.bappenas.go.id/e-library/file_upload/koleksi/migrasi-data-publik asi/file/RP_RKP/Narasi%20RPJMN%20IV%202020-2024_Revisi%2014%20Agustu s%202019.pdf

Erikha, A., & Hoesein, Z. A. (2025). Strategi pencegahan kebocoran data pribadi melalui peran Kominfo dan gerakan Siberkreasi dalam edukasi digital. Jurnal Retentum, 7(1), 48-64.

ESDM, K. (2018). Kontribusi PNBP Sektor ESDM Tahun 2018 Diperkirakan Lebih Besar. Kementerian Energi dan Sumber Daya Mineral, https://www.esdm.go.id/en/media-center/news-archives/kontribusi-pnbp-sektor-esdm- tahun-2018-diperkirakan-lebih-besar.

ESDM, K. (2018). Tahun 2017, Hampir 50 Persen PNBP Nasional Berasal dari Sektor ESDM. KEMENTERIAN ENERGI DAN SUMBER DAYA MINERAL REPUBLIK INDONESIA, https://www.esdm.go.id/id/media-center/arsip-berita/tahun-2017-hampir-50-persen-pn bp-nasional-berasal-dari-sektor-esdm.

ESDM, K. (2024). 20 Mei 2024, Realisasi PNBP Migas Capai Rp36,81 triliun. Kementerian Energi dan Sumber Daya Mineral Republik Indonesia, https://www.esdm.go.id/en/media-center/news-archives/20-mei-2024-realisasi-pnbp- migas-capai-rp3681-triliun.

Gawazah, L., Rondla, A., & Balhareth, M. S. A. (2024). To pay or not to pay: The US Colonial Pipeline ransomware attack. Thunderbird School of Global Management.

Humas. (2022). Presiden Terbitkan Perpres 82/2022 tentang Pelindungan Infrastruktur Informasi Vital. Sekretariat Kabinet Republik Indonesia, https://setkab.go.id/presiden-terbitkan-perpres-82-2022-tentang-pelindungan-infrastruktur-informasi-vital/#:~:text=Presiden%20RI%20Joko%20Widodo%20(Jokowi)%20 menetapkan%20Peraturan,dan%20transaksi%20elektronik%20yang%20 mengganggu%20ketertiban%20umum.

Ige, A. B., Kupa, E., & Ilori, O. (2024). Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources. International Journal of Science and Research Archive, 12(1), 2978-2995.

Katharina, R. (2021). Pelayanan publik & pemerintahan digital Indonesia. Yayasan Pustaka Obor Indonesia.

Kemhan. (2014). Pedoman Pertahanan Siber Kementerian Pertahanan Republik Indonesia. Kementerian Pertahanan Republik Indonesia , https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Ta hun-2014-tentang-Pertahanan-Siber.pdf.

Kementerian Energi dan Sumber Daya Mineral. (2021). Gandeng BSSN, Kementerian ESDM bentuk tim tanggap insiden siber. https://www.esdm.go.id/id/media-center/arsip-berita/gandeng-bssn-kementerian-esdm- bentuk-tim-tanggap-insiden-siber

Kementerian Komunikasi dan Digital. (2020). Pembentukan BSSN dan ancaman siber. https://www.komdigi.go.id/berita/pengumuman/detail/pembentukan-bssn-dan-ancaman-siber

Kementerian Pertahanan Republik Indonesia. (2014). Pedoman Pertahanan Siber. KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA, https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf.

Kementerian Pertahanan Republik Indonesia. (2017). Peraturan Sekretaris Jenderal Kementerian Pertahanan Nomor PS 133 Tahun

Kharisma, D., Tobing, W. T. M., Susanti, E., & Aprili, R. (2024). Evaluasi kebijakan perlindungan konsumen dalam transaksi digital di Indonesia: Studi kebijakan dan analisis SWOT. Perkara: Jurnal Ilmu Hukum dan Politik, 2(4), 565-578.

Knapp, E. D. (2024). Industrial network security: Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems. Elsevier.

Lemhannas. (2020). Anton Martin. http://lib.lemhannas.go.id/public/media/catalog/0010-092400000000029/swf/7803/015%20-%20Anton%20Martin.pdf

Nazari, Z., & Musilek, P. (2023). Impact of digital transformation on the energy sector: A review. Algorithms, 16(4), 211.

Popik, T. S. (2022). Preserving Ukraine's electric grid during the Russian invasion. Journal of Critical Infrastructure Policy, 3(1), 15-55.

PLN. (2025). AI Inovation in The Electricity Sector. Perusahaan Listrik Negara, https://plniconplus.co.id/news/AI-Inovation-in-The-Electricity-Sector.

RI, H. K. (2017). PEMBENTUKAN BADAN SIBER DAN SANDI NEGARA (BSSN). Kementerian

Koordinator Bidang Politik dan Keamanan RI, https://polkam.go.id/pembentukan-badan-siber-dan-sandi-negara-bssn/#:~:text=Selain%20itu%2C%20BSSN%20juga%20menjadi,turut%20serta%20 menjaga%20keamanan%20nasional.

RI, S. J., Anggaran, P. K., & Keahlian, B. (2022). Budget Issue Brief Politik dan keamanan . Berkas Dewan Perwakilan Rakyat RI, https://berkas.dpr.go.id/pa3kn/analisis-tematik-apbn/public-file/bib-public-112.pdf.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. Sensors, 23(15), 6666.

Saptoyo, R. D., & Galih, B. (2025). Jumlah Penduduk Indonesia 2025. Kompas, https://www.kompas.com/cekfakta/read/2025/03/04/100100582/jumlah-penduduk-indonesia- 2025

Sugiyono, (2016). Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif, Dan R&D. Bandung:alfabeta.

Sumiyati, A., Rahman, P. S., Gusti, M. H. C., Melkior, G. D. A., Hidayat, J., & Aribowo, D. (2024). Konsep dasar transmisi tenaga listrik: Klasifikasi, komponen serta gangguannya. Jurnal Surya Teknika, 11(2), 612-617.

Wicaksono, A. T., & Yasin, I. F. (2024). Criminal law reformulation through omnibus law as a solution to sectoral cyber protection: Reformulasi hukum pidana melalui omnibus law sebagai solusi perlindungan siber yang bersifat sektoral. Al-Jinayah: Jurnal Hukum Pidana Islam, 10(2), 237-261.

Yana, S., Nizar, M., & Yulisma, A. (2021). Prospek utama pengembangan energi terbarukan di negara-negara ASEAN. Jurnal Serambi Engineering, 6(2).